Universidad Austral de Chile
Facultad de Ciencias de la Ingeniería
Escuela de Electricidad y Electrónica

ESTUDIO E IMPLEMENTACION DE DISPOSITIVO DE RED MULTIFUNCIONAL

Trabajo de Titulación para optar al
Título de Ingeniero Electrónico.

Profesor Patrocinante:
Sr. José Mardones Fernández
Ingeniero Electrónico

DENIS RICARDO CORTES PEREDO
ALVARO ANDRES VERA SCHAFER
VALDIVIA 2004

COMISION EXAMINADORA

Sr. Jose Mardones Fernández.
PROFESOR PATROCINANTE

Sr. Cristian Quiroga Acuña.
PROFESOR INFORMANTE

Sr. Francisco Moraga Quezada.
PROFESOR INFORMANTE

AGRADECIMIENTOS

Mis palabras de gratitud son para todas aquellas personas que de una forma u otra en el diario vivir me enseñaron a sortear y superar los obstáculos que nos depara la vida. Comenzando por mis padres que se esforzaron por darme la mejor educación y herramientas para poder así alcanzar mis metas, a mi hermana por ser mi amiga, a la Maita que nos acogió como uno mas de su familia y nos malacostumbraba peor que en nuestra propia casa.

Bueno y en especial a Jasna por su amor incondicional y motivación por ser cada día mejor. Finalmente gracias a Dios por acompañarme siempre.

DENIS RICARDO CORTES PEREDO.

Dedicado a:

La verdad es muy difícil agradecer a una determinada cantidad de personas ya que son muchos los que han colaborado en mi desarrollo profesional que incluye profesores y profesionales en general, además de aquellos que comenzaron como compañeros de carrera y con el tiempo se transformaron en grandes amigos con los cuales compartí buenos y malos momentos y que me ayudaron a superar esta importante etapa de mi vida, para todos ellos un fuerte abrazo.

Pero este trabajo esta dedicado de forma muy especial a mis padres - Heraclio Vera y Ana Maria Schafer - que hicieron posible se realice este sueño, los cuales con su apoyo incondicional han sido un pilar fundamental en mi desarrollo personal y profesional, ya que sin ellos y su esfuerzo es muy probable que no este escribiendo esto en este momento y sólo me queda decirles "**Muchas Gracias**" y tratar de retribuir en parte su cariño ya que es imposible devolver todo lo que he recibido de ellos.

Junto con ellos recordar muy cariñosamente a mi abuelita Enedina y mi tía Patricia a quienes agradezco de todo corazón su cariño y apoyo durante toda mi vida.

Y finalmente pero no menos importante: Joselin, que este sea el comienzo de una vida juntos.

ALVARO ANDRES VERA SCHAFER.

INDICE

RESUMEN

Este trabajo presenta el estudio de un dispositivo que cumpla con los requerimientos de toda red corporativa y tenga las características de: router, switch y seguridad de forma integrada y sin necesidad de adquirir 3 equipos diferentes, considerando sus distintas aplicaciones, configuración y comandos de trabajo.

Para realizar lo anterior es necesario asimilar conceptos relativos a funciones de enrutamiento, seguridad y conmutación de paquetes en redes IP.

Tomando en cuenta las ofertas existentes en el mercado, tomaremos como referencia el Private Internet eXchange (PIX) de un proveedor de equipos de conectividad, el cual presenta las características ya mencionadas.

Este documento se realizó primero en una etapa teórica recolectando información en la bibliografía existente en el mercado tanto para lo relacionado a conectividad como lo específico al firewall PIX. Una vez terminada la parte teórica, lograr una aplicación en forma práctica, implementado una pequeña red, la cual se configura de manera que se puedan usar los conceptos entregados en forma teórica, y además, en la cual el PIX sea el elemento central de provisión de funcionalidad, seguridad y gestión de la red.

SUMMARY

This work presents/displays the study of a device that fulfills the requirements of all corporative network and has the characteristics of: to router, switch and security of integrated form and with no need to acquire 3 different equipment, considering its different applications, configuration and commandos of work.

In order to make the previous thing it is necessary to assimilate concepts relative to routing functions, security and commutation of packages in networks IP.

Taking into account the existing supplies in the market, we will take like reference Private Internet eXchange (PIX) from a supplier from equipment from connectivity, which already presents/displays the mentioned characteristics.

This document was made as much first in a theoretical stage collecting information in the existing bibliography in the market for the related thing to connectivity like the specific thing to firewall PIX. Once finished part theoretical, to obtain application in form practical, implemented small network, which is formed so that the concepts given in theoretical form can be used, and in addition, in which the PIX is the central element of functionality provision, security and management of the network.

INTRODUCCION

Muchas organizaciones tienen una cantidad importante de computadores en operación y con frecuencia, alejadas entre sí. Para un rápido desarrollo y trabajo es muy importante compartir los recursos y hacer que los datos estén disponibles para cualquiera en esta organización, por esto los computadores, las redes e Internet afectan cotidianamente a nuestras vidas. Al principio, el número de personas involucradas en los avances de la computación, era relativamente pequeño y se sentían a gusto trabajando conjuntamente donde se confiaban los unos y los otros, en general, la seguridad era algo secundario.

Actualmente, Internet se compone de decenas de miles de redes conectadas entre sí. La seguridad en las redes resulta esencial en este entorno, ya que toda red organizada es accesible desde cualquier computadora de la red y, potencialmente, es vulnerable a las amenazas de personas que no necesitan acceso físico a ella.

En un sondeo reciente dirigido por el Computer Security Institute (CSI), el 70% de las organizaciones encuestadas declararon que las defensas de sus redes habían sido atacadas y el 60% afirmaba que los incidentes procedían de las propias empresas.

Aunque sea difícil dimensionar el número de empresas que tiene problemas de seguridad relacionados con Internet y las pérdidas financieras debidas a tales problemas, queda claro que los problemas existen.

Este trabajo ofrece información para el diseño, configuración y mantención de una red de área local (LAN) tomando como eje central un dispositivo que ofrece la posibilidad de conectar y comunicar los terminales en un organización y que además entregue la seguridad hacia el exterior, es decir, una conexión segura a Internet.

Debido a la amplia cantidad de recursos existentes en el mercado, se ha elegido el firewall CISCO PIX (Private Internet eXchange) por cumplir este con los requisitos planteados en los objetivos que son el entregar conectividad, conmutación y seguridad en intercambio de información hacia Internet.

Si bien es cierto, no existe una conexión totalmente segura a Internet, este trabajo entrega la información necesaria para trabajar en este equipo quien además de seguridad entrega aplicaciones como VPN (Virtual Private Network) la cual se usa para comunicar oficinas que están en lugares geográficos muy apartados.

La información aquí entregada se limita a aplicaciones de seguridad como listas de acceso y de conectividad, dejando de lado otras como contabilidad y estadísticas de ingreso.

Los antecedentes bibliográficos están basados en textos de apoyo de la editorial Pearson Educación con su serie de libros de estudios, CISCOPRESS, dedicados a todos los temas de redes y conectividad que este trabajo incluye.

Objetivos generales:

- Entregar a la pequeña empresa el análisis de un equipo que le permita comunicar y compartir una conexión a Internet de manera segura y efectiva.
- Lograr comunicar terminales de una red corporativa de manera eficiente y rápida.
- Generar un conjunto de reglas y procedimientos a cargar en el equipo analizado, con el objeto de proteger la red de ataques informáticos externos o internos limitando el acceso a datos confidenciales, evitando así el robo de información.
- Conocer, comprender y aplicar conceptos sobre conectividad en redes corporativas.

Objetivos específicos:

- Estudiar y aplicar un dispositivo multifuncional de conectividad de redes IP.
- Armar y operar una red local Ethernet cuyo fin es requerir de los servicios del PIX como elemento multifuncional de la red.
- Analizar el firewall CISCO PIX (Private Internet eXchange), generando una ficha técnica y de instalación para el análisis de parte de interesados en contar con sus servicios.
- Hacer una diferencia en calidad de servicio y costos de mantención e implementación entre CISCO PIX y algún otro equipo presente en el mercado.
- Conocer como se interconectan y comunican estos equipos entre si.
- Conocer los dispositivos y normas de seguridad en Internet, como protocolos más usados y aplicaciones.
- Conocer los distintos dispositivos de comunicación que se usan en una red IP.
- Estudiar conceptos de direccionamiento de números IP aplicables en una red corporativa.
- Estudiar conceptos de conectividad para luego aplicarlos de forma práctica.

CAPITULO I

Conceptos generales de Internetworking.

1.1. Definición de conceptos de red.

El objetivo de una red de datos consiste en facilitar la consecución de un incremento de la productividad vinculando todos los computadores, periféricos y redes de computadores de manera que los usuarios pueden tener acceso a la información con independencia del tiempo, ubicación y tipo de equipo informático.

1.1.1. Red de la organización.

Red que se ha creado enlazando recursos de computadores existentes dentro de la organización. Los recursos suelen estar ubicados en departamentos y/o grupos de trabajos independientes y que a menudo utilizan varias topologías de red y protocolos de comunicación.

Una red de empresa proporciona interoperabilidad entre sistemas autónomos y heterogéneos.

Objetivos perseguidos al construir una red:

- Integrar sistemas de comunicación incompatibles reduciendo el número de protocolos de comunicación que se utilizan en la organización.
- Aumentar la capacidad de la red para manejar más usuarios y archivos de datos de gran volumen, como los de multimedia.
- Permitir que los usuarios de distintas aplicaciones compartan información en diversos formatos y normas, sin que tengan por qué conocer dichas diferencias: transparencia.
- Mantener niveles de seguridad razonables sin hacer más engorrosa la utilización del sistema.
- Adaptar de forma rápida el sistema, a las necesidades cambiantes.

1.1.2. Conceptos de Redes:

Redes de comunicación, entre personas y/o sus equipos (teléfonos, fax, impresoras, computadores).

Una red de computadores es un sistema de comunicación de datos que enlaza dos o más computadores y dispositivos periféricos.

Los componentes típicos de software y hardware son:

- Sistema Operativo de red: módulos de software para el soporte funcional de red que complementan al sistema operativo local, y que permiten a los usuarios compartir archivos y periféricos con otros usuarios de la red. Incluyen los módulos de software, controladores o drivers, de las tarjetas de interfaz de red y los protocolos de comunicación. Un sistema operativo de red para una red dedicada se ejecuta en servidores autónomos, prestando servicios de:

- Servidor de archivos, pasarela de correo electrónico, de comunicaciones, de base de datos, de copia de seguridad y de almacenamiento, de fax, de impresión, de servicios de directorio.
- NIC: Network Interface Card o Tarjeta Interfaz de Red, token-ring o ethernet.
- Cableado :
    - Medio guiado: cables de par trenzado, coaxial, fibra óptica.
    - Medio no guiado o inalámbrico: infrarrojos, microondas, señales de radio.

1.1.3. Hardware de red

En términos generales, hay dos tipos de tecnologías de transmisión:

- Redes de difusión
- Redes punto a punto.

Las redes de difusión tienen un sólo canal de comunicación compartida por todas las máquinas de la red. Los mensajes (llamados **paquetes** en ciertos contextos) que envía una

máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a quién se dirige. Al recibir un paquete, una máquina verifica el campo de dirección. Si el paquete está dirigido a ella, lo procesa; si está dirigido a alguna otra máquina, lo ignora.

Como analogía, consideremos un anuncio en el aeropuerto, pidiendo a todos los pasajeros del vuelo 644 que se presenten en la puerta de embarque 12, sólo aquellos que tengan este vuelo se presentarán en la sala 12.

Los sistemas de difusión generalmente también ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Cuando se transmite un paquete con ese código, cada máquina en la red lo recibe y lo procesa. Este modo de operación se llama **difusión** (*broadcasting*). Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas, algo conocido como multidifusión. Un esquema posible consiste en reservar un bit para indicar multidifusión. Los restantes *n –1* bits de dirección pueden contener un número de grupo. Cada máquina se puede "suscribir" a cualquier grupo o a todos. Cuando se envía un paquete a cierto grupo, se entrega a todas las máquinas que se suscribieron a ese grupo.

En contraste, las redes **punto a punto** consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar primero una o más máquinas intermedias. A veces son posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de ruteo desempeñan un papel importante en estas redes. Como regla general, las redes pequeñas geográficamente localizadas tienden a usar la difusión, mientras que las redes más grandes suelen ser punto a punto.

1.1.4. Topologías

Mapa de la disposición del cableado

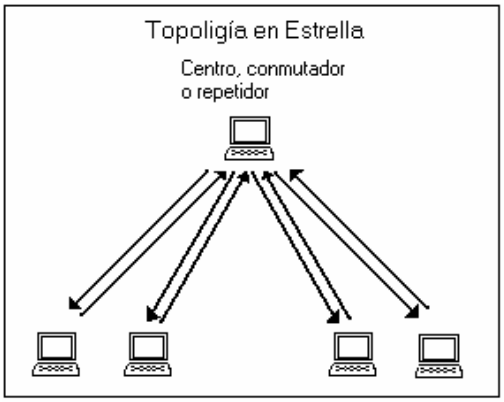


Figura 1.1. Estrella

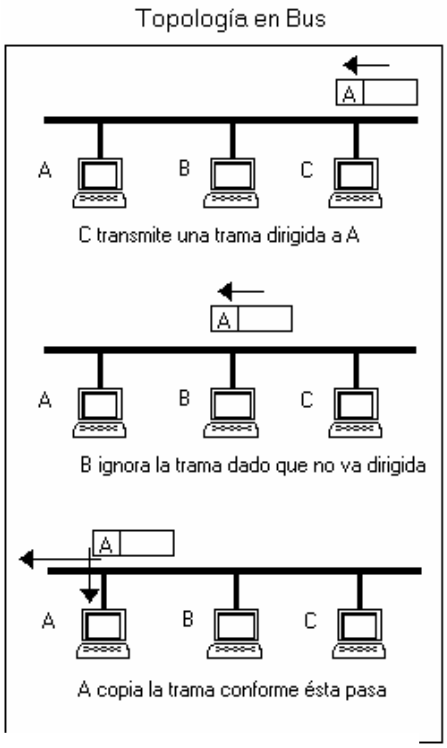


Figura 1.2. Bus.

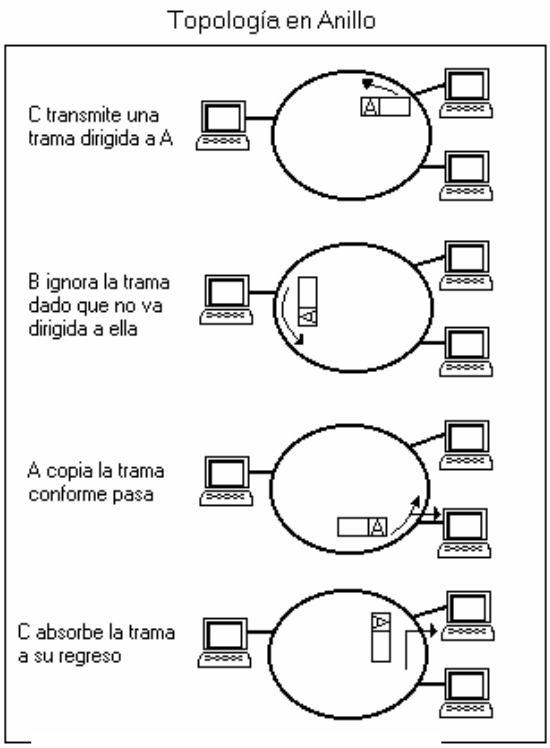


Figura 1.3. Anillo.

1.1.5. Arquitecturas de redes:

La comunicación es siempre entre, al menos, dos partes, los cuales establecen una “conversación” o sesión a través de las redes, requiriéndose que ambas partes estén de acuerdo en ciertas cosas básicas:

- En establecer la comunicación.
- En el formato de los datos.
- En la velocidad de transmisión de los datos.
- En definir direcciones.
- En definir numeración de los paquetes para mantener el orden y “ventanas” para el envío y recepción los paquetes.
- Otros mecanismos por ejemplo para el manejo de los errores de transmisión, desconexión, llamada cobro revertido, etc.

Es frecuente que estos sistemas de control se incorporen por software a cada uno de los dispositivos de la red. Bajo el concepto de Ingeniería de software, es común encontrar el software organizado en capas o layers en los cuales se agrupan “especializaciones” de la secuencia de tareas a realizar.

Al conjunto de capas y protocolos se le denomina arquitectura de red.

1.2. El modelo OSI

1.2.1. Introducción

En un principio, los computadores eran elementos aislados, constituyendo cada uno de ellos una estación de trabajo independiente, una especie de "isla informática". Cada computador precisaba sus propios periféricos y contenía sus propios archivos.

Se hizo necesario entonces implementar sistemas que permitieran la comunicación entre diferentes ordenadores y la correcta transferencia de datos entre ellos, surgiendo de esta forma el concepto de "redes de ordenadores" y de "trabajo en red" (networking).

El principal inconveniente de estos sistemas de comunicación en red fue que cada uno de ellos era propietario de una empresa particular, siendo desarrollados con hardware y software propios, con elementos protegidos y cerrados, que usaban protocolos y arquitecturas diferentes. Como consecuencia de ello, la comunicación entre ordenadores pertenecientes a distintas redes era imposible.

Para solucionar este problema, la Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y por lo tanto, elaboraron el modelo de referencia OSI en 1984.

En la actualidad, una adecuada interconexión entre los usuarios y procesos de una empresa u organización, puede constituir una clara ventaja competitiva. La reducción de costes de periféricos, o la facilidad para compartir y transmitir información son los puntos claves en que se apoya la creciente utilización de redes.

1.2.2. El Modelo OSI

El Modelo de Referencia de Interconexión de Sistemas Abiertos, OSI-RM (Open System Interconection-Reference Model) proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.

Para poder simplificar el estudio y la implementación de la arquitectura necesaria, la ISO dividió el modelo de referencia OSI en capas, entendiéndose por **capa** una entidad que realiza de por sí una función específica.

Cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI.

Los criterios que llevaron a este modelo de referencia fueron:

- Deberá crearse una nueva capa siempre que se precise un nuevo grado de abstracción.
- A cada capa deberá asignarse un número bien definido de funciones propias.
- La funcionalidad de cada capa deberá tener en cuenta la posibilidad de definir protocolos normalizados a nivel internacional.
- La frontera de las capas será tal que se minimice el flujo de información a través de la interfaz entre ambas.
- El número de capas será lo suficientemente grande como para no reunir en un nivel funcionalidades distintas y lo suficientemente pequeño para que el resultado final sea manejable en la práctica.

En el modelo de referencia OSI hay siete capas numeradas, cada una de las cuales ilustra una función de red particular. La división de la red en siete capas presenta las siguientes ventajas:

1. Divide la comunicación de red en partes más pequeñas y sencillas.
2. Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
3. Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida. Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
4. Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Una analogía del sistema de capas puede ser la forma en que una carta es enviada desde el emisor hasta el destinatario. En este proceso intervienen una serie de entidades o capas (carteros, oficinas postales, medios de transporte, etc.), cada una de las cuales realizan

una serie de funciones específicas, necesarias para el funcionamiento de las demás y para la entrega efectiva de la carta.

Las sietes capas OSI son:

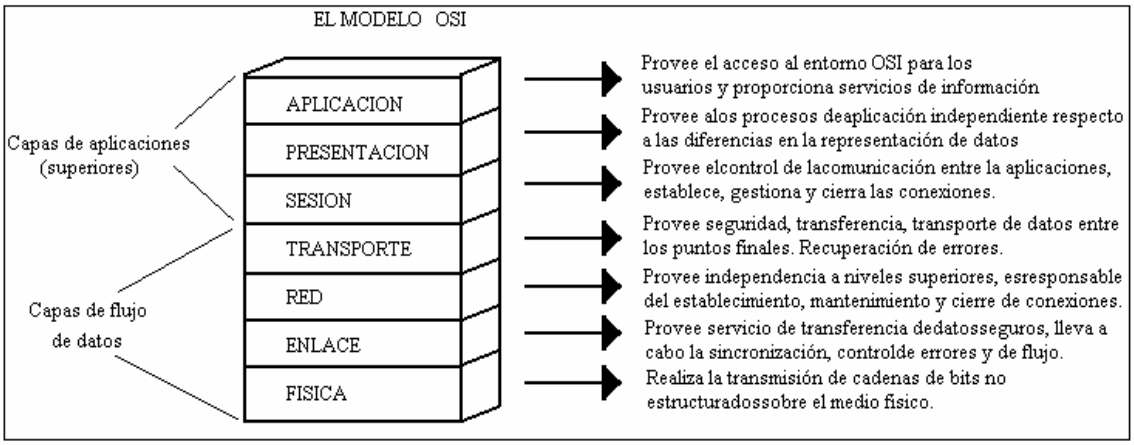


Figura 1.4 Modelo Osi

1.2.2.1. Capa 7: La capa de aplicación.

La **capa de aplicación** es la capa OSI más cercana al usuario. Proporciona servicios de red, como acceso a impresión de los ficheros para las aplicaciones del usuario. Difiere de otras capas en que no proporciona servicio a ninguna otra capa OSI, sino sólo a las aplicaciones externas al modelo OSI. La capa de aplicación establece la disponibilidad de socios de comunicación deseados. También sincroniza y establece un acuerdo en los procedimientos para la recuperación de errores e integridad en el control de datos. Ejemplos de aplicaciones de la capa 7 son Telnet y HTTP.

1.2.2.2. Capa 6: La capa de presentación.

La **capa de presentación** asegura que la información que se envía a la capa de aplicación de un sistema se va a poder leer por la capa de aplicación de otro sistema. Si es necesario, la capa de presentación traduce múltiples formatos de datos empleando un formato común. Una de las tareas más importantes de esta capa es el cifrado y el descifrado. Los estándares gráficos comunes de la capa 6 son PICT, TIFF y JPEG.

1.2.2.3. Capa 5: La capa de sesión.

Como su nombre indica, la **capa de sesión** establece, administra y finaliza las sesiones entre dos host de comunicación. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el dialogo entre las capas de presentación de los dos host y administra el intercambio de datos. Además de regular la sesión, la capa de sesión ofrece abastecimiento para una eficiente transferencia de datos, clase de servicio y, excepcionalmente, informa de problemas en las capas de sesión, presentación y aplicación. Ejemplos de protocolos de capa 5 son NFS (Network File System), sistema X-Window y ASP (AppleTalk session Protocol).

1.2.2.4. Capa 4: La capa de transporte.

La **capa de trasporte** segmenta los datos del sistema del host remitente y los reordena en un flujo de datos en el sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los de flujo de datos. Mientras que las capas de aplicación, presentación y sesión se preocupan por los temas de la aplicación, las cuatro capas inferiores se preocupan por los temas del transporte de datos.

La capa de transporte intenta proporcionar un servicio de transporte de datos que proteja a las capas superiores de los detalles de la implementación del transporte. Al proporcionar un servicio de comunicación, la capa de transporte establece, mantiene y finaliza adecuadamente los circuitos virtuales. Para suministrar un servicio fiable, se emplea la detección y recuperación de errores en el transporte y la información en el control de flujo. Ejemplos de protocolo de la capa 4 son TCP (Transmisión Control Protocol) UDP (User Datagram Protocol).

1.2.2.5. Capa 3: La capa de red.

La **capa de red** es una capa compleja que proporciona conectividad y una selección de ruta entre dos sistemas host que pueden estar ubicados en redes geográficamente separadas. Además, la capa de red se ocupa del direccionamiento lógico. Ejemplos de protocolos de la capa 3 son IP (Internet Protocol), IPX (Internet Packet Exchange) y AppleTalk

1.2.2.6. Capa 2: La capa de enlace datos.

La **capa de enlace datos** proporciona un tránsito de datos fiable a través de un enlace físico. De este modo, la capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

1.2.2.7. Capa 1: La capa física

La **capa física** define las especificaciones eléctricas, mecánicas, procedimientos y fundamentos para activar, mantener y desactivar el enlace físico entre sistemas finales. Características como niveles de voltaje, cronometraje de los cambios de voltaje, velocidad de los datos físicos, distancia máximas de transmisión, conectores físicos y otros atributos similares, se definen mediante las especificaciones de la capa física.

Esta capa solamente reconoce bits individuales.

1.3. Encapsulamiento

Si un computador ***A*** desea enviar datos a otro ***B***, en primer término los datos a enviar se deben colocar en paquetes que se puedan administrar y rastrear, a través de un proceso denominado **encapsulamiento**.

Cuando las aplicaciones de usuario envían los datos desde el origen, estos viajan a través de las diferentes capas. Las tres capas superiores (aplicación, presentación y sesión) preparan los datos para su transmisión, creando un formato común para la transmisión. Una vez pasados a este formato común, el encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tráfico de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.

El encapsulamiento consta de los cinco pasos siguientes:

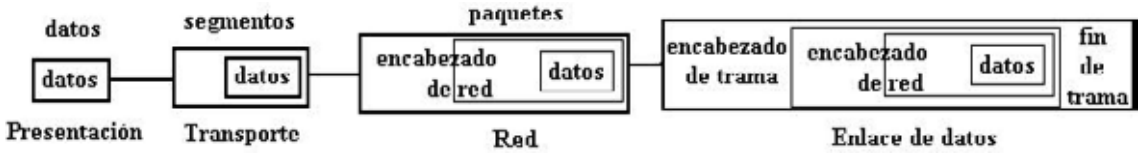


Figura 1.5 Etapas del encapsulamiento de datos.

1. **Crear los datos** (capa de presentación). Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la red.

2. **Empaquetar los datos** para ser transportados de extremo a extremo (capa transporte). Se dividen los datos en unidades de un tamaño que se pueda administrar (los segmentos), y se les asignan números de secuencia para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego los empaqueta para ser transportados por la red. Al utilizar segmentos, la función de transporte asegura que los hosts del mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.

3. **Agregar la dirección de red al encabezado** (capa de red). El siguiente proceso se produce en la capa de red, que encapsula el segmento creando un paquete o datagrama, agregándole las direcciones lógicas de red de la máquina origen y de la máquina destino. Estas direcciones ayudan a los enrutadores a enviar los paquetes a través de la red por una ruta seleccionada.

4. **Agregar la dirección local al encabezado** de enlace de datos (capa enlace de datos). En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama las direcciones MAC (número de la tarjeta de red, único para cada tarjeta) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

5. **Transmitir el tren de bits creado**. (Capa física). Por último, el tren de bits originado se transmite a la red a través de los medios físicos (cableado, ondas, etc.). Una función de

temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio, que puede variar a lo largo de la ruta utilizada.

Cuando los datos se transmiten en una red de área local (red LAN), se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el host origen hasta el host destino. Pero si se deben enviar los datos a un host de otra red interna o a través de Internet es necesario el uso de paquetes de datos que contengan las direcciones lógicas de las máquinas que se deben comunicar.

Las tres capas inferiores (red, enlace de datos, física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o de Internet.

1.4. Comunicación entre capas

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino. Esta forma de comunicación se conoce como **comunicaciones de par-a-par**. Las reglas y convenciones que controlan esta conversación se denominan **protocolo de la capa n**, y se ocupan del formato y significado de las unidades de datos intercambiadas.

Durante este proceso, cada protocolo de capa intercambia unidades de información entre capas iguales de las máquinas que se están comunicando, conocidas con el nombre de **unidades de datos de protocolo** (PDU). Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino.

También cada capa de un modelo o arquitectura de red recibe **servicios** a la capa que se encuentra debajo de ella y suministra servicios a la que está por encima en la jerarquía, siendo la implantación de estos servicios transparente al usuario. Hay dos tipos principales de servicios:

1. **Servicios orientados a la conexión**: En ellos la conexión es como un tubo a través del cual se envía la información de forma continuada, por lo que los mensajes llegan en el orden

que fueron enviados y sin errores. Proporcionan un servicio confiable de comunicación de datos. Una analogía es el sistema telefónico.

2. **Servicios sin conexión**: En los que cada mensaje lleva la dirección completa de su destino, la información no se envía de forma continuada y el ruteo de cada mensaje es independiente. El servicio no es entonces confiable, pues la capa de red ni garantiza el orden de los paquetes ni controla su flujo, y los paquetes deben llevar sus direcciones completas de destino. Una analogía sería el caso del sistema de correo convencional.

Otra clasificación posible de los servicios en la que distingue entre confiables y no confiables:

1. **Servicios confiables**: son aquellos en los que la transmisión de datos está controlada en cada momento, pudiéndose determinar el correcto envío y recepción de todos los datos transmitidos. Para ello la máquina receptora envía mensajes de acuse de recibo de las tramas recibidas a la máquina emisora.
2. **Servicios no confiables**: en estos no existe un control de los datos transmitidos, por lo que no se puede garantizar que se hayan recibido todos los datos. Una forma de contrarrestar esta debilidad es la implementación de un sistema de acuse de recibo de las unidades de datos.

En realidad, una capa de una máquina no puede transferir los datos de forma directa a su capa par de otra, si no que necesita los servicios de todas las capas que se encuentran por debajo de ella en la jerarquía de capas, pasándose la información hacia abajo hasta llegar al nivel físico, que es el que realiza el proceso de transferencia de datos.

Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le puede agregar cualquier encabezado e información final que la capa necesite para ejecutar su función. De esta forma, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicionales.

La capa de red presta un servicio a la capa de transporte, trasladando esos datos a través de la red. Para ello encapsula los datos y les agrega un encabezado específico (direcciones lógicas origen y destino), con lo que crea un paquete (PDU de la Capa 3).

La capa de enlace de datos suministra un servicio a la capa de red. Encapsula la información de la capa de red (paquetes) en una trama (la PDU de la Capa 2), cuyo encabezado contiene la información necesaria (direcciones físicas) para completar las funciones de enlace de datos.

La capa física también suministra un servicio a la capa de enlace de datos, codificando los datos de la trama de enlace de datos en un patrón de unos y ceros (trenes de bits) para su transmisión a través del medio (generalmente un cable).

1.5. Direcciones IP

Es el identificador de cada ordenador dentro de su red, la cual tiene una dirección de IP asignada que debe ser distinta a todas las direcciones que estén vigentes en ese momento.

Clasificación:

- **Direcciones IP públicas**. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

- **Direcciones IP privadas (reservadas)**. Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo.
- **Direcciones IP estáticas (fijas)**. Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.

- **Direcciones IP dinámicas**. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP.

Cada host y enrutador de Internet tiene una dirección IP, que codifica su número de red y su número de host. La combinación es única. Todas las direcciones de IP son de 32 bits de longitud y se usan en los campos de *dirección de origen y dirección de destino* de los paquetes IP. Los formatos usados para las direcciones IP se muestran en la figura 1.6. Aquellas máquinas conectadas a varias redes tienen direcciones de IP diferentes en cada red.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las **clases primarias A**, **B** y **C**. La **clase D** está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de **clase E** no se pueden utilizar (están reservadas).

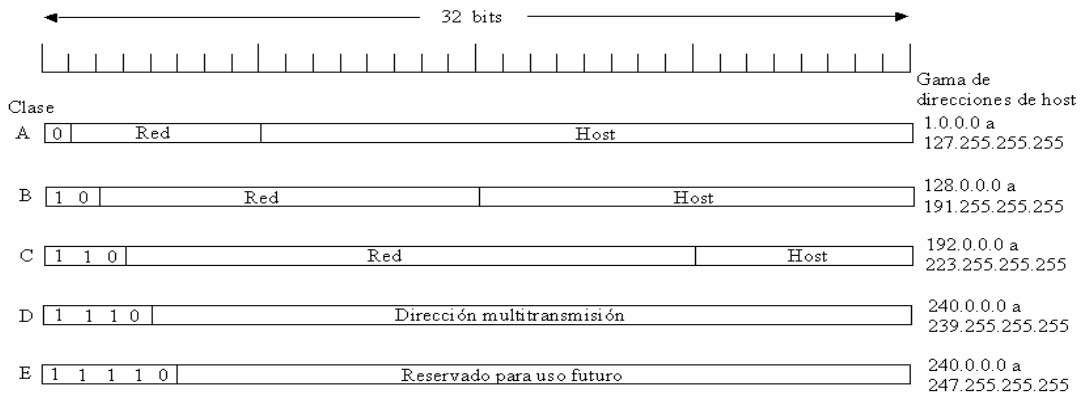


Figura 1.6 Formatos de dirección IP.

- Las direcciones de clase A usan 7 bits para el número de red permitiendo 126 posibles redes (veremos posteriormente que de cada par de direcciones de red y de host, dos tienen un significado especial). Los restantes 24 bits se emplean para el número de host, de modo que cada red tener hasta 16,777,214 hosts.
- Las direcciones de clase B usan 14 bits para el número de red, y 16 bits para el de host, lo que supone 16382 redes de hasta 65534 hosts cada una.

- Las direcciones de clase C usan 21 bits para el número de red y 8 para el de host, lo que supone 2,097,150 redes de hasta 254 hosts cada una.
- Las direcciones de clase D se reservan para multicasting o multidifusión, usada para direccionar grupos de hosts en un área limitada.
- Las direcciones de clase E se reservan para usos en el futuro

Los números de red los asigna el **NIC (***Network Information Center***, centro de información de redes**) para evitar conflictos.

Las direcciones de red, que son números de 32 bits, generalmente se escriben en **notación decimal con puntos**. En este formato, cada uno de los 4 bytes se escribe en decimal, de 0 a 255. Por ejemplo, la dirección hexadecimal C0290614 que en notación binaria seria se escribe como 192.41.6.20. La dirección de IP menor es 0.0.0.0 y la mayor 255.255.255.255.

Los valores 0 y –1 tienen significado especial, el valor 0 significa esta red o este host. El valor –1 se usa como dirección de difusión para indicar todos los host de la red indicada.

La dirección de IP 0.0.0.0 es usada por los host cuando están siendo arrancados, pero no se usa después. Las direcciones IP con 0 como número de red se refieren a la red actual. Estas direcciones permiten que las máquinas se refieran a su propia red sin saber su número (pero tiene que saber su clase para saber cuántos 0 hay que incluir). La dirección que consiste solamente en **"1"** permite la difusión en la red local, por lo común una LAN. Las direcciones con número de red propio y solamente **"1"** en el campo de host permiten que las máquinas envíen paquetes de difusión a LAN distantes desde cualquier parte de Internet. Por último, todas las direcciones de la forma 127.xx.yy.zz se reservan pruebas de realimentación. Los paquetes enviados a esa dirección no se colocan en el alambre; se procesan localmente y se tratan como paquetes de entrada. Esto permite que los paquetes se envíen a la red local sin que el transmisor conozca su número. Esta característica también se usa para la detección de fallas en el software de la red.

Los estándares para las direcciones IP se describen en RFC 1166 -- Números de Internet.

Las direcciones IP son usadas por el protocolo IP para definir únicamente un host en la red. Los datagramas IP(los paquetes de datos elementales intercambiados entre máquinas) se transmiten a través de alguna red física conectada a la interfaz de la máquina y cada uno de ellos contiene la *dirección IP de origen* y *la dirección IP de destino*. Para enviar un datagrama a una dirección IP de destino determinada la dirección de destino de ser traducida o mapeada a una dirección física. Esto puede requerir transmisiones en la red para encontrar la dirección física de destino(por ejemplo, en LANs el ARP("Adress Resolution Protocol", analizado en ARP("Address Resolution Protocol"), se usa para traducir las direcciones IP a direcciones físicas MAC).

1.5.1. DNS: Domain Name System

Para simplificar la referencia a máquinas, existe una base de datos distribuida global a la Internet, que hace una correspondencia entre direcciones IP y nombres de máquina.

Así podremos referirnos a una máquina de la Internet no sólo por su dirección IP sino también por su nombre dentro del DNS.

Los nombres de máquinas siguen una organización jerárquica por subdominios:

máquina.subdominio_2.subdominio_1.dominio_de_país

Ejemplos: a01-unix.uc3m.es yeti.dit.upm.es ftp.cica.indiana.edu

InterNIC: Organismo con autoridad para asignar direcciones IP: El InterNIC (Internet Network Information Center).

El InterNIC asigna direcciones de red, el administrador local las de máquina.

Tipos

Unicast: Representan a una sola máquina.
Multicast: Representan a un grupo de máquinas.

Broadcast: Representan a todas las máquinas de una subred.

Subredes.
En ocasiones, por razones organizativas o topológicas, se utilizan algunos bits de máquina como bits de subred, sobre todo con direcciones de clases A y B.

Dada una dirección de red otorgada por el InterNIC, el administrador decide si utilizará subredes, y el número de bits de máquina que utilizará para indicar la subred.

El número de bits con el que se indica la subred se denota con una máscara de subred: 32 bits, 1 para bits de red y subred, 0 para bits de máquina.

Ejemplo: Dirección 163.117.129.50 (clase B) con máscara 255.255.255.0 se interpreta como máquina 50 de la subred 129 de la red 163.117.

Al dividir una red en segmentos pequeños, o subredes, se consigue hacer un uso más eficiente de las direcciones de red. No se apreciará ningún cambio en la forma en que la red se ve desde el exterior pero, dentro de la propia organización, habrá una estructura adicional.

En la figura 1.7. la red 172.16.0.0 ha sido dividida en cuatro subredes, se ha usado el tercer octeto como dirección de subred en cada una de las direcciones. Los routers determinan la red de destino usando las direcciones de subred, limitando así la cantidad de tráfico en los demás segmentos de red.

Las subredes son una extensión del número de red. Los administradores de la red deciden el tamaño de las subredes basándose en las necesidades y crecimiento previsible de la organización.

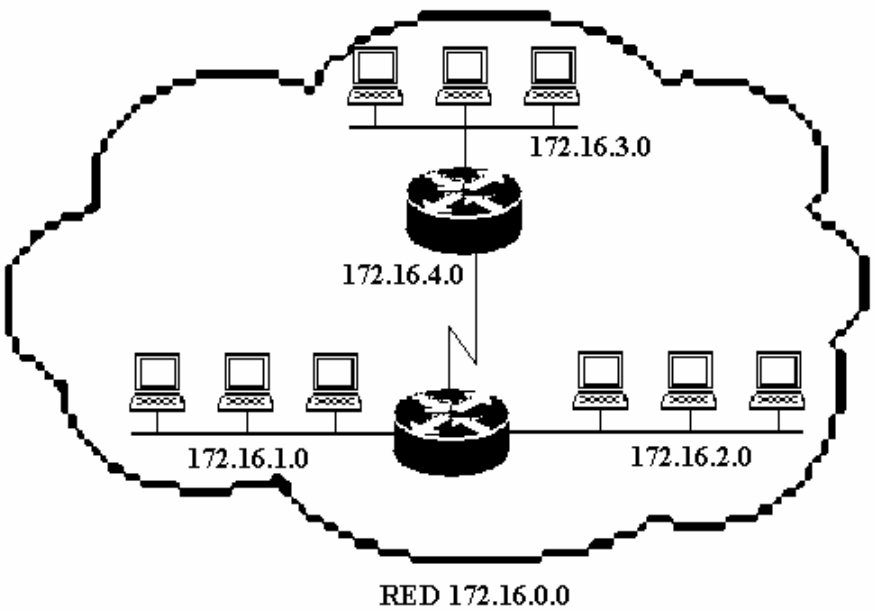


Figura 1.7 Direccionamiento con subredes.

Máscaras de subred: Un dispositivo de red utiliza una máscara de subred para determinar la parte de la dirección IP que se usa para la red, la subred y las direcciones de los dispositivos (host) como muestra la figura 1.7. Una máscara de subred es un valor de 32 bits que contiene una sucesión de unos para los ID de red y subred, y una serie de bits a 0 para el ID de host. Un dispositivo puede también determinar la clase de dirección que tiene asignada a partir de su propia dirección IP. La máscara de subred informa al dispositivo de donde se encuentra el limite entre los ID de subred y de host.

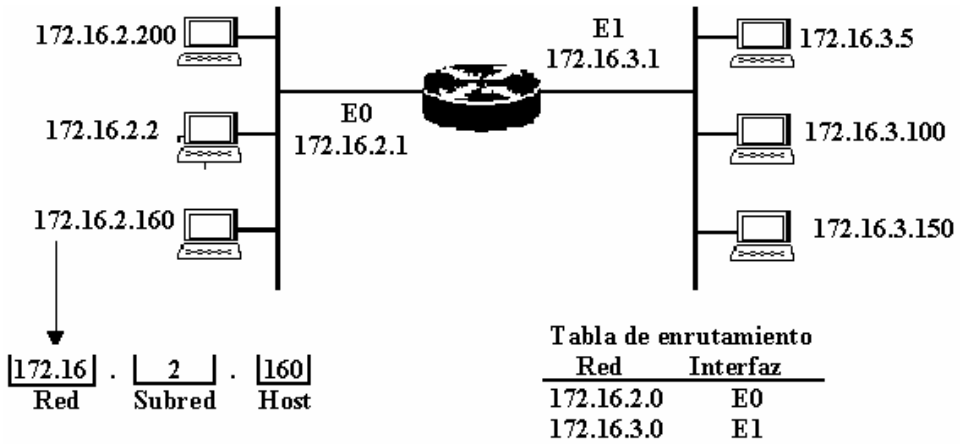


Figura 1.7. direccionamiento de subredes de routers.

El router y cualquiera de los host pueden determinar cuál es el segmento local realizando una comparación lógica con la máscara de subred, como se muestra en la figura 1.8.

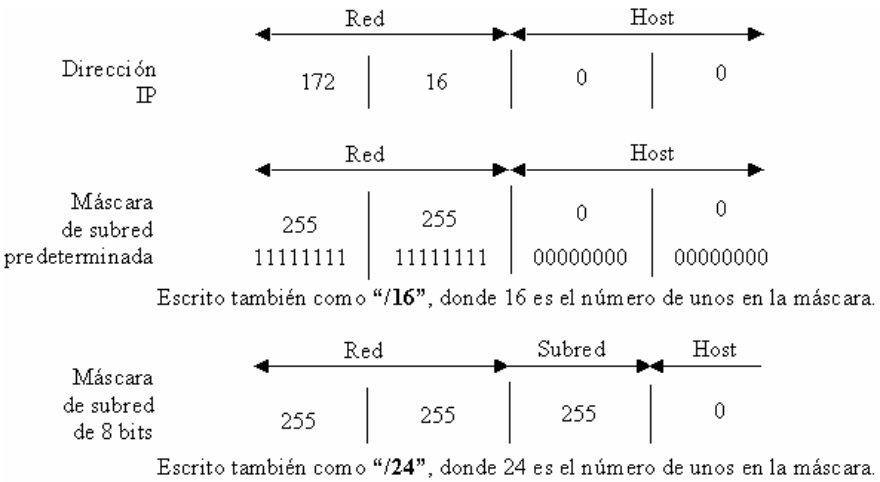


Figura 1.8 Máscara de subred.

Identificación de direcciones IP.

Dada una dirección IP y una máscara de subred, se puede usar el proceso mostrado en la figura 1.9. y que aparece descrito con más detalle en la lista que le sigue, para identificar la dirección de subred, la dirección de difusión, la primera y última dirección utilizable. Este método puede usarse para calcular el espacio de direcciones de las redes.

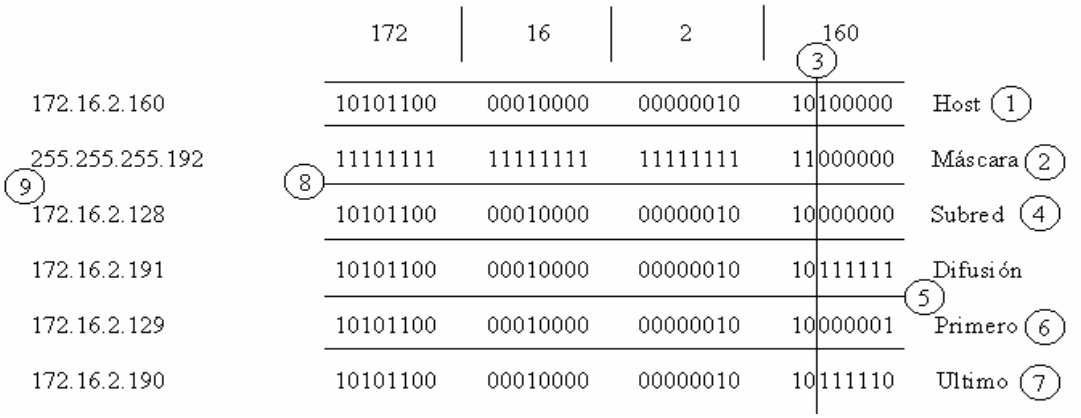


Figura 1.9 Cálculo del espacio de direcciones.

Lista de pasos a seguir para identificar la dirección de subred, la dirección de difusión, la primera y última dirección utilizable.

1. Escribir la dirección de 32 bits en notación binaria.
2. Escribir la máscara de subred en binario, justamente debajo de la anterior.
3. Trazar una línea vertical justamente después del último bit 1 de la máscara de subred.
4. En una fila inferior, colocar todos los bits a 0 para los restantes espacios libres (a la derecha de la línea vertical). Ésta es la subred.
5. En la siguiente fila, colocar a la derecha de la línea todo unos hasta alcanzar los 32 bits. Ésta es la dirección de difusión.
6. A la derecha de la línea en la fila siguiente, colocar todos los bits a 0 en los espacios libres restantes hasta llegar al último espacio libre. Colocar un 1 en dicho espacio. Esto dará la primera dirección utilizable.
7. En la fila siguiente, colocar a la derecha de la línea todos los bits a 1 en los espacios libres restantes hasta llegar al último espacio. Colocar un 0 en dicho espacio libre. Esto da la última dirección utilizable.
8. Copiar todos los bits escritos en el Paso 1 en los campos que hay a la izquierda de la línea vertical, en cuatro líneas.
9. Convertir las cuatro filas finales a notación decimal.

Con las subredes se puede seguir usando la fórmula 2^N-2 (donde N es el número de bits) para calcular el número de host.

Planificación de subredes.

El ejemplo de red que ilustra la figura 1.10. tiene asignada una dirección de Clase C 192.168.5.0. Supongamos que se necesitan 20 subredes, con 5 host por subredes. Subdivididas el último octeto en un parte de subred y una parte de host y determine cuál debe ser la máscara de subred.

Seleccione un tamaño de campo de subred que permite un número de subredes suficiente. En este ejemplo, eligiendo una máscara de 5 bits se tendría espacio para 20 subredes con 32 host cada una. Las direcciones de subred son múltiplos de 8, como

192.168.5.16, 192.168.5.32 y 192.168.5.48. Esto se debe a que hay 8 direcciones en cada red, incluidos el número de red y la dirección de difusión; por tanto, cada nueva subred será 8 unidades superior a la anterior.

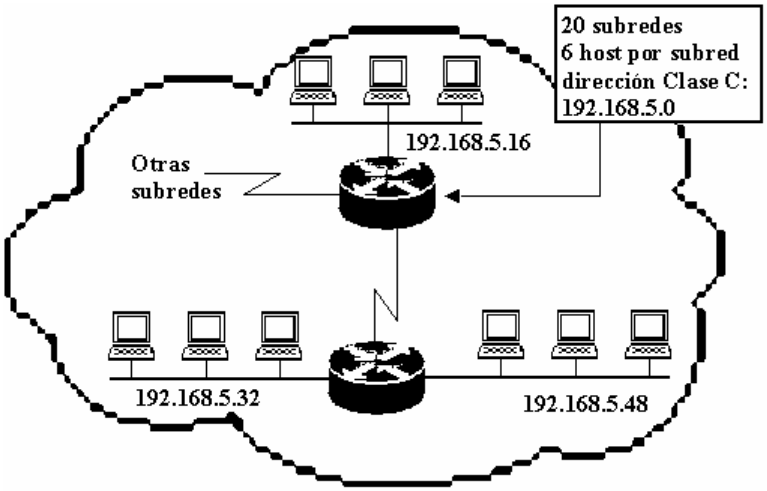


Figura 1.10 Planificación de subredes.

Los bits restantes en el último octeto se utilizan para el campo del host. Los 3 bits de nuestro ejemplo permiten un número de host suficiente para cubrir las necesidades iniciales de 5 host por cable. Los números de host disponibles son 1,2,3,4,5 y 6. La dirección 7 es la de difusión para esta red, y la siguiente subred tiene el valor 8.

La última dirección de host en una combinación de la dirección de inicio del “cable” de red/subred mas el valor de cada host. Los host de la subred 192.168.5.16 podrían ser direccionados como 192.163.5.17, 192.163.5.18, 192.163.5.19, 192.163.5.20, 192.163.5.21 y 192.163.5.22.

El número de host 0 está reservado para la dirección de “cable”, y el valor de host que consta sólo de unos esta también reservado, porque es el que permite seleccionar todos los host – una difusión.

En este ejemplo de planificación el número de subred extraído servirá de modelo para todas las subredes generadas durante este ejercicio. En la figura 1.11 se ven los números de subred, dirección de difusión y rangos inicial y final para el espacio de direcciones, correspondientes a la dirección 192.168.5.121 con una subred 255.255.255.248.

En la tabla siguiente se ha divido en subredes una red de Clase C para proporcionar 6 direcciones de host y 30 subredes.

	Red	Red	Red	Subred	Host
192.168.5.121:	11000000	10101000	00000101	01111	001
255.255.255.248:	11111111	11111111	11111111	11111	000
Subred:	11000000	10101000	00000101	01111	000
Difusión:	11000000	10101000	00000101	01111	111

Dirección de subred = 192.168.5.120
Dirección de host = 192.168.5.121 - 192.168.5.126
Dirección de difusión = 192.168.5.127
cinco bits para subredes

Figura 1.11 Ejemplo de planificación de subredes.

1.6. Protocolo IP

IP es el principal protocolo de la capa de red. Este protocolo define la unidad básica de transferencia de datos entre el origen y el destino, atravesando toda la red de redes. Además, el software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Se trata de un sistema de entrega de paquetes (llamados datagramas IP) que tiene las siguientes características:

Es no orientado a conexión debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.

Es no fiable porque los paquetes pueden perderse, dañarse o llegar retrasados.

CAPITULO II
DISPOSITIVOS DE COMUNICACIÓN

2.1 Cómo opera el router.

Una definición de router seria: Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa 2.

Los routers permiten dividir una red amplia en subredes lógicas, con ello, se consigue aislar el tráfico en cada subred, permitiendo así sacar el máximo partido al ancho de banda disponible.

2.1.1. Conceptos básicos del encaminamiento de datos.

Cuando la información tiene que pasar de una red a otra, el dispositivo de conexión entre redes que se encarga de mover los datos es el router. Para encaminar datos en una interconexión de redes es preciso que se produzcan dos eventos distintos: por un lado, que se determine la ruta apropiada para los paquetes y, por otro, que los paquetes se desplacen hasta su destino final.

Tanto la determinación de la ruta como el encaminamiento de los paquetes se producen en la capa 3 del modelo **OSI**. Otro evento importante que ocurre en esta capa es la resolución o conversión de las direcciones lógicas (como número IP cuando TCP/IP es el protocolo encaminado) en direcciones hardware.

2.1.2 Determinación de rutas IP.

Para que un router pueda enviar paquetes a una red, se debe determinar la ruta a seguir por dicho paquete. Las rutas se pueden determinar por medio de rutas estáticas o mediante protocolos de enrutamiento dinámico, como Protocolo de información de enrutamiento (RIP), Protocolo de enrutamiento de *gateway* interior (IGRP), Primero la ruta libre más corta (OSPF).

2.1.3 Generalidades sobre el enrutamiento.

Para que la información pueda viajar de una red a otra, es necesario que algún dispositivo sepa cómo transportar dicha información. El enrutamiento es el proceso por el cual un elemento pasa de una ubicación a otra. Hay muchos elementos que pueden ser objeto de enrutamiento, como el correo electrónico, las llamadas telefónicas. En *networking*, el dispositivo encargado de dirigir el tráfico es el router.

Para poder enrutar paquetes de información, un router (o cualquier otro elemento que se encargue de realizar el enrutamiento, como puestos UNÍS encargados de ejecutar el motor de enrutamiento, o switch de la capa 3), debe conocer lo siguiente:

- **Dirección de destino.** ¿Cuál es el destino (o dirección) del elemento que necesita ser enrutado? Esto es responsabilidad del host.
- **Fuentes de la información.** Desde qué fuente (otros routers) puede aprender el router las rutas hasta los destinos especificados.
- **Rutas posibles.** ¿Cuáles son las rutas iniciales posibles hasta los destinos perseguidos?
- **Rutas óptimas.** ¿Cuál es la mejor ruta hasta el destino especificado?
- **Mantenimiento y verificación de la información de enrutamiento.** Una forma de verificar que las rutas hasta los destinos conocidos son válidas y las más actualizadas.

La información de enrutamiento que el router aprende desde sus fuentes de enrutamiento se coloca en su propia tabla de enrutamiento. El router se vale de esta tabla para determinar los puertos de salida que debe utilizar para retransmitir un paquete hasta su destino. La tabla de enrutamiento es la fuente principal de información del router acerca de las redes. En la figura 2.1 puede verse cómo un router construye una tabla de enrutamiento.

Si la red de destino está conectada directamente, el router ya sabrá el puerto que debe usar para reenviar paquetes.

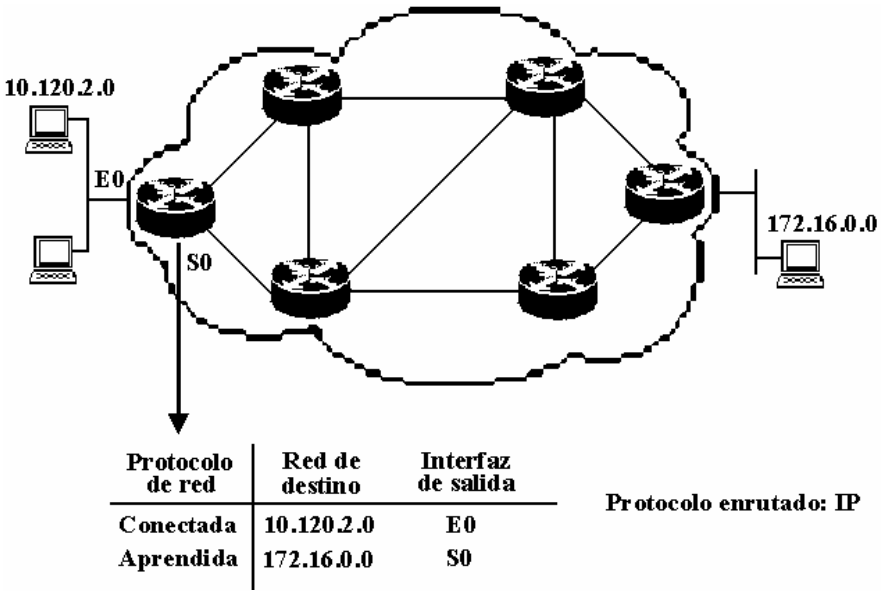


Figura 2.1 Routers conectados

Si las redes de destino no están conectadas directamente, el router debe aprender y calcular la ruta óptima a usar para reenviar paquetes a dichas redes. La tabla de enrutamiento se construye usando un de estos dos métodos:

- Manualmente, por el administrador de la red.
- A través de procesos dinámicos que se ejecutan en la red.

Estas son dos formas de informar a un router sobre dónde debe reenviar los paquetes que no están conectados directamente:

- Rutas estáticas. Rutas aprendidas por el router a través del administrador, que establece dicha ruta manualmente. En este caso, el administrador debe encargarse también de actualizar la entrada de las rutas estáticas cada vez que tenga lugar cualquier cambio en la topología del internetworking de redes, como cuando se produce algún fallo en un enlace.
- Rutas dinámicas. Rutas aprendidas automáticamente por el router, una vez que el administrador ha configurado un protocolo de enrutamiento que permite el aprendizaje de rutas. A diferencia de las rutas estáticas, en cuanto el administrador de la red habilita

el enrutamiento dinámico el conocimiento del router se actualiza automáticamente cada vez que se recibe información nueva sobre la topología de la red desde otros routers.

2.1.4 Conmutación de paquetes.

Cuando los paquetes llegan al router, se opera la conmutación de los mismos. Esto quiere decir que el router moverá los paquetes desde la interfaz de router por la que entraron y los conmutará hasta la interfaz de router conectada a la subred a la que deben dirigirse. Sin embargo, en determinados casos, es posible que los paquetes tengan que pasar por más de un router para alcanzar su destino final.

El encaminamiento de datos supone tanto el uso del direccionamiento lógico como del direccionamiento de hardware para transmitir paquetes desde una computadora emisora a otra computadora receptora. Todos los protocolos encaminados utilizan un esquema ligeramente distinto para resolver direcciones lógicas en direcciones de hardware.

2.1.5 Algunos tipos de router o designaciones que recibe:

2.1.5.1 Router de generación.

Router de una red AppleTalk que tiene el número de red o rango de cable incorporado en el descriptor de puerto. El router de generación define el número de red o el alcance de cable para otros routers de ese segmento de la red y responde a las consultas de configuración de los routers no generadores en la red AppleTalk conectada, permitiendo que esos routers confirmen o modifiquen sus configuraciones en consecuencia. Cada red AppleTalk debe tener al menos un router de generación.

2.1.5.2 Router designado.

Router OSPF que genera LSA para una red multiacceso y tiene otras responsabilidades especiales al ejecutar OSPF. Cada OSPF multiacceso que tiene por lo menos dos routers conectados tiene un router designado elegido por el protocolo Hello OSPF. El router designado permite una reducción en la cantidad de adyacencias requeridas en una red multiacceso, que a su vez reduce la cantidad de tráfico de protocolo de enrutamiento y el tamaño de la base de datos topológica.

2.1.5.3 Router fronterizo.

Router ubicado en los bordes, o al final, de la frontera de la red, que brinda protección básica contra las redes externas, o contra un área menos controlada de la red para un área más privada de la red.

2.1.5.4 Router no generador.

En AppleTalk, un router que primero debe obtener, y luego verificar, su configuración con un router de generación antes de poder comenzar a operar. Ver también router de generación.

2.1.5.5 Router vecinos.

En OSPF, dos routers que tienen interfaces a una red común. En redes multiacceso, el protocolo Hello OSPF detecta a los vecinos de forma dinámica.

Los routers operan en la capa de red registrando y grabando las diferentes redes aprendiéndose los números IP y eligiendo la mejor ruta para las mismas, colocan fronteras entre los segmentos de red porque éstos envían sólo tráfico que está dirigido hacia ellos, eliminando la posibilidad de "tormentas" de *broadcasts*, la transmisión de paquetes de protocolos no soportados y la transmisión de paquetes destinados a redes desconocidas.. Los

routers colocan esta información en una tabla de enrutamiento, que incluye los siguientes elementos:

- **Dirección de red.** Representa redes conocidas por el router. La dirección de red es específica del protocolo. Si un router soporta varios protocolos, tendrá una tabla por cada uno de ellos.
- **Interfaz.** Se refiere a la interfaz usada por el router para llegar a una red dada. Ésta es la interfaz que será usada para enviar los paquetes destinados a la red que figura en la lista.
- **Métrica.** Se refiere al coste o la distancia para llegar a la red de destino. Se trata de un valor que facilita al router la elección de la mejor ruta para alcanzar una red dada. Esta métrica cambia en función de la forma en que el router elige las rutas. Entre las métricas mas habituales figuran el número de redes que han de ser cruzadas para llegar al destino (conocido también como saltos), el tiempo que se tarda en atravesar todas las interfaces hasta una red dada (conocido también como retraso), o un valor asociado con la velocidad de un enlace (conocido también como ancho de banda).

Debido a que los router funcionan en la capa de red del modelo OSI, se utilizan para separar segmentos en dominios de colisión y de difusión únicos. Cada segmento se conoce como una red y debe estar identificado por una dirección de red para que pueda ser alcanzado por un puesto final. Además de identificar cada segmento como una red, cada puesto de la red debe ser identificado también de forma unívoca mediante direcciones lógicas. Esta estructura de direccionamiento permite una configuración jerárquica de la red, ya que está definida por la red en la que se encuentra, así como por un identificador de host. Para que los routers puedan operar en una red, es necesario que cada tarjeta este configurada en la red única que ésta representa. El router debe tener una dirección de host en esa red. El router utiliza la información de configuración de la tarjeta para determinar la parte de la dirección correspondiente a la red, a fin de construir una tabla de enrutamiento.

Además de identificar redes y proporcionar conectividad, los routers deben proporcionar conectividad, los routers deben proporcionar estas otras funciones:

- Los routers no envían difusiones de capa 2 ni tramas de multidifusión.

- Los routers intentan determinar la ruta óptima a través de una red enrutada basándose en algoritmos de enrutamiento.
- Los routers separan las tramas de capa 2 y envían paquetes basados en direcciones de destino de capa 3.
- Los routers asignan una dirección lógica de capa 3 individual a cada dispositivo de red; por tanto, los routers pueden limitar o asegurar el tráfico de la red basándose en atributos identificables con cada paquete. Estas opciones, controladas por medio de listas de acceso, pueden ser aplicadas para incluir o sacar paquetes.
- Los routers pueden ser configurados para realizar funciones tanto de puenteado como de enrutamiento.
- Los routers proporcionan conectividad entre diferentes LAN virtuales (VLAN) en entornos conmutados.
- Los routers pueden ser usados para desplegar parámetros de calidad de servicio para tipos específicos de tráfico de red.

Además de las ventajas que aporta su uso en un campus, los routers pueden utilizarse también para conectar ubicaciones remotas con la oficina principal por medio de servicios WAN. Los routers soportan una gran variedad de estándares de conectividad a nivel de la capa física, lo cual ofrece la posibilidad de construir WAN. Además, pueden proporcionar controles de acceso y seguridad que son elementos necesarios cuando conectan ubicaciones remotas.

2.2 Cómo opera un switch.

Cuando hablamos de *switch*, podemos estarnos refiriendo a:

- *Switch* capa de enlace de datos.
- *Switch* capa de red.
- *Switch* capa de transporte.

2.2.1 Switch de capa de enlace de datos.

Este es el tipo de switch de red de área local (LAN) más básico. Su antecesor es el bridge, por ello, muchas veces al switch se le refiere como un bridge multipuerto, pero con un costo más bajo, con mayor rendimiento y mayor densidad por puerto.

El switch capa 2 hace sus decisiones de envío de datos en base a la dirección MAC destino contenida en cada *frame*. Estos, al igual que los *bridges,* segmentan la red en diferentes dominios de colisión. Los Switch de la capa 2 poseen tres funciones principales que son: aprender direcciones, reenviar/filtar paquetes y evitar bucles.

Las funciones de conmutación son parecidas a las de los bridges Ethernet:

- Un Switch aprende las direcciones MAC de los dispositivos asociados a cada uno de sus puertos. Las asignaciones de direcciones a puertos se guardan en una base de datos MAC.
- Cuando un Switch Ethernet recibe una trama, consulta la base de datos MAC para determinar que puerto puede alcanzar el puesto identificado como destino en la trama. Si se localiza la dirección, la trama será retransmitida a través únicamente de ese puerto.
- Cuando la red conmutada incluye bucles de redundancia, un Switch Ethernet evita que estos bucles entren en la red, pero sin impedir vías de regreso en el caso de que se haya configurado un árbol de extensión.

La conmutación Ethernet incrementa el ancho de banda disponible en la red, deduciendo el número de usuarios por segmento o incluso permitiendo la existencia de segmentos dedicados e interconectados dichos segmentos.

2.2.1.1 La función de aprendizaje de direcciones.

Un switch Ethernet aprende direcciones y opera como un bridge transparente. El switch mantiene una tabla de direcciones MAC que se usa para registrar las ubicaciones de los dispositivos conectados al switch. A partir de aquí, utiliza dicha tabla para decidir qué paquetes deben ser enviados a otros segmentos.

El objetivo del switch es segmentar el tráfico de manera que los paquetes destinados a un host en un dominio de colisión determinado no se propaguen a otro segmento. El switch consigue esto “aprendiendo” las ubicaciones de los host. A continuación los pasos del proceso de aprendizaje y retransmisión.

- Cuando se inicializa un switch, la tabla de direcciones MAC del mismo está vacía.
- Con una tabla de direcciones MAC vacía, no es posible tomar decisiones relativas al filtrado o retransmisión basándose en direcciones, por lo que el switch de debe retransmitir cada trama a todos los puertos conectados, excepto a aquel donde se ha recibido la trama.
- Enviar una trama a todos los puertos conectados se denomina “inundar” la trama.
- Inundar es el medio menos efectivo de transmitir datos a través de un switch, pues se malgasta ancho de banda al enviar la trama a segmentos donde no se necesita.
- Debido a que los switch controlan el tráfico para múltiples segmentos al mismo tiempo, han de implementar memoria búfer para que puedan recibir y transmitir tramas independiente en cada puerto o segmento.

Para comprender el proceso de aprendizaje, la figura 2.2 muestra una transacción entre dos puestos que se encuentran en segmentos distintos.

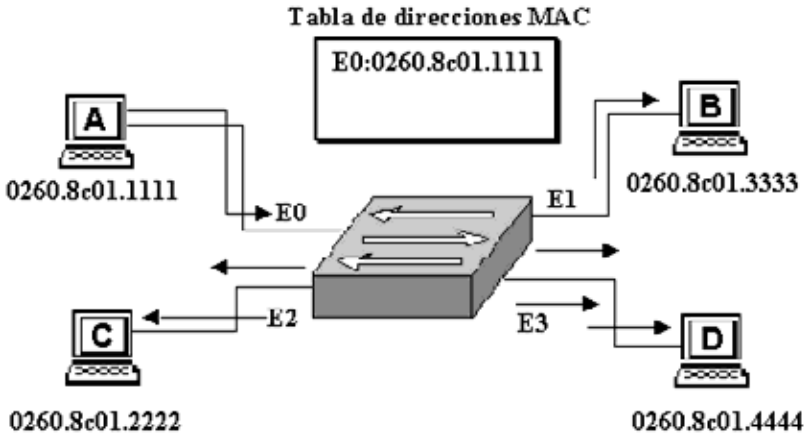


figura 2.2 Aprendizaje de direcciones: paquete inundado.

En la figura 2.2, el Puesto A con dirección Mac 0260.8c01.111111 desea enviar tráfico al Puesto C con dirección MAC 0260.8c01.2222. El switch recibe esta trama y lleva a cabo varias acciones:

1. La trama se recibe inicialmente a través del Ethernet físico y se almacena en un espacio de memoria temporal.
2. Debido a que el switch no conoce aún que interfaz está conectada al puesto de destino, se ve obligado a inundar la trama a través de todos los puertos.
3. Mientras se inunda la trama del Puesto A, el switch aprende la dirección de origen y la asocia al Puerto E0 en una nueva entrada de la tabla de direcciones MAC.
4. Una entrada de la tabla pasa a memoria caché. Si dicha entrada no se actualiza por una nueva trama en un periodo de tiempo determinado, la entrada es descartada.

Los switch y bridges resultan eficientes precisamente por su capacidad de aprendizaje. Conforme los puestos continúen enviando tramas de unos a otros, continuará el proceso de aprendizaje, como se muestra en la figura 2.3.

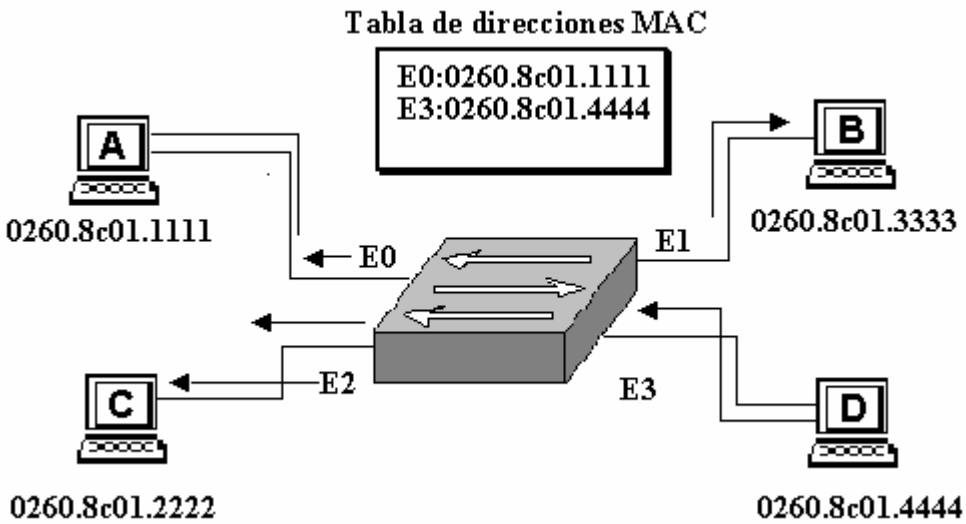


figura 2.3. Aprendizaje de direcciones : respuesta del puesto.

En la figura 2.3, el puesto D con dirección MAC 0260.8c01.4444 envía tráfico al puesto C, con dirección MAC 0260.8c01.2222. El switch realiza aquí varias acciones:

1. La dirección de origen, 0260.8c04.4444, se añade a la tabla de direcciones MAC.
2. La dirección de destino incluida en la trama transmitida, Puesto C, se compara con las entradas de la tabla de direcciones MAC.
3. Cuando el software determina que no existe aún asignación de puerto a dirección MAC para este destino, la trama es inundada a todos los puertos excepto a aquel a través el cual ha sido recibida.
4. Cuando el Puesto C envía de vuelta una trama al puesto A, el switch puede aprender también la dirección MAC del Puesto C, en el Puerto E2.
5. Cuando todos los puestos envíen tramas dentro del periodo de vigencia de la tabla de direcciones MAC, se irá construyendo una tabla de direcciones MAC completa. Estas entradas se usarán posteriormente para tomar decisiones inteligentes de retransmitir y filtrado.

2.2.1.2 **Decisiones de retransmisión/filtrado**.

Cuando una trama llega a una dirección de destino conocida, es transmitida sólo al puerto específico conectado a dicho puesto, y no a los demás puestos.

La secuencia de acciones para cuando el puesto A envía una trama al Puesto C es la siguiente:

1. La dirección MAC de destino incluida en la trama transmitida, 0260.8c01.2222, se compara con las entradas existentes en la tabla de direcciones MAC.
2. Cuando switch determina que la dirección MAC de destino puede ser alcanzada por medio del Puerto E2, retransmite la rama sólo a este puerto.
3. El switch no retransmite al Puerto E1 ni al Puerto E3, a fin de preservar el ancho de banda para estos enlaces. Esta acción se conoce filtrado de tramas.

Si uno de los Puesto envía una trama de difusión o multidifusión, la trama es retransmitida a todos los puertos excepto al puerto que la ha originado.

Las tramas de difusión o multidifusión constituyen un caso especial. Debido a que estas tramas pueden ser de interés para todos los puestos, el switch normalmente las inunda a todos

los puertos excepto al puerto de origen. Un switch nunca aprende direcciones de difusión o multidifusión, dado que las direcciones no aparecen en estos casos como direcciones de origen de la trama.

2.2.1.3 Evitación de bucles.

La tercera función del switch es evitar los bucles. Las redes puenteadas, que incluyen las redes conmutadas, están diseñadas por lo general con enlaces y dispositivos redundantes. Estos diseños eliminan la posibilidad de que un punto de fallo dé como resultado la pérdida de funcionalidad en toda la red conmutada. La figura 2.4 muestra una red conmutada diseñada con redundancia entre el segmento 1 y el segmento 2.

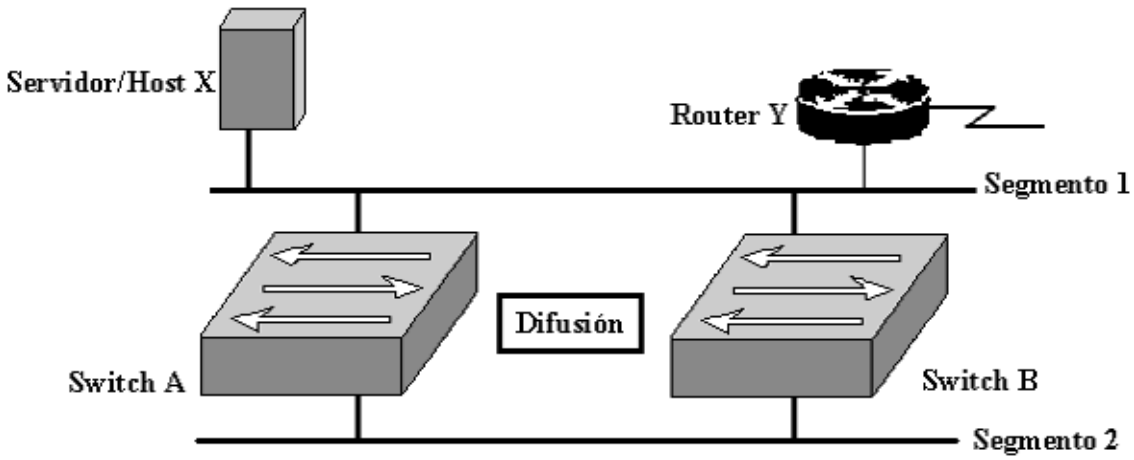


figura 2.4 Topología redundante para una red conmutada.

Aunque los diseños conmutados permiten eliminar un punto de fallo individual, originan al mismo tiempo varios problemas que deben ser tenidos en cuanta:

- Sin algún servicio de evitación de bucles implementado, cada Switch inundaría las difusiones en un bucle infinito. Esta situación se conoce habitualmente como bucle de puente. La propagación continua de estas difusiones a través del bucle produce una tormenta de difusión, lo que da como resultado un desperdicio del ancho de banda, así como impactos serios en el rendimiento de la red y del host.

- Podrían ser distribuidas múltiples copias de trama sin difusión a los puestos de destino. Muchos protocolos esperan recibir una sola copia de cada transmisión. La presencia de múltiples copias de la misma trama podría ser causa de errores irrecuperables.
- Una inestabilidad en el contenido de la tabla de direcciones MAC da como resultado que se reciban varias copias de una misma trama en diferentes puertos del switch. La retransmisión de datos podría quedar interrumpida cuando el Switch consume recursos al copiar direcciones innecesarias en la tabla de direcciones MAC.

En los siguientes apartados se describe como se pueden resolver todos estos problemas con la evitación de bucles.

2.2.1.4 Eliminación de tormentas de difusión.

Los Switch inundan tramas de difusión a todos los puertos excepto aquel de donde se ha recibido la trama. La figura 2.5 muestra el problema de las tormentas de difusión, en que los Switch propagan el tráfico de difusión de forma continua.

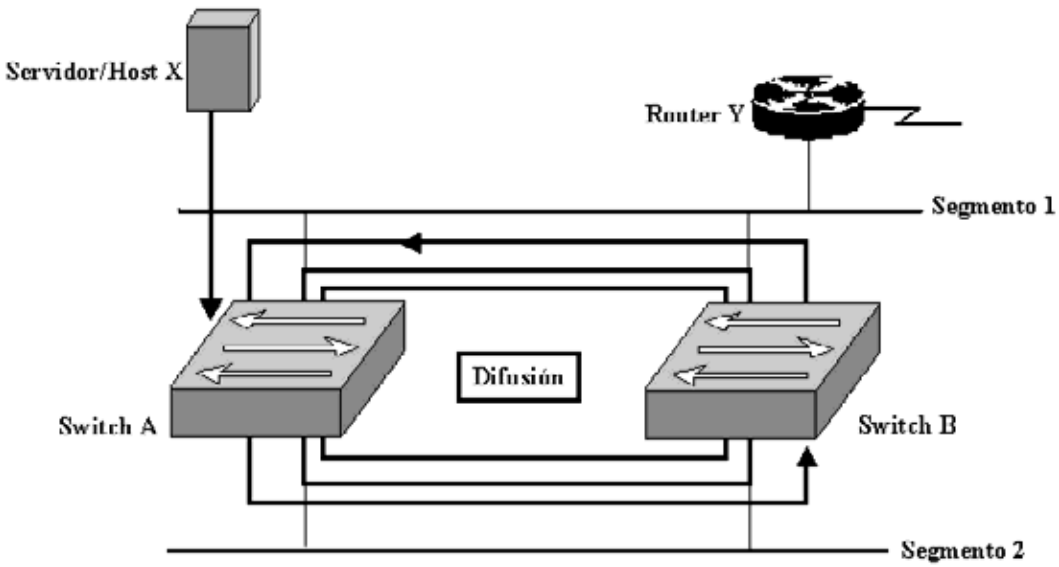


Figura. 2.5 Tormentas de difusión.

Una tormenta de difusión es una situación de extrema congestión debido a demasiadas difusiones en la red. Esto puede estar causado por un mal comportamiento de la carpeta NIC,

un diseño incorrecto de la red, o un bucle de puenteado/conmutación. La tormenta de difusión ilustrada en la figura anterior está causada por la siguiente secuencia de eventos:

1. Cuando el host X envía una trama de difusión (por ejemplo, un ARP para resolver su *gateway* predeterminada en el router Y) la trama es recibida por el Switch A.
2. El Switch A examina el campo que contiene la dirección de destino en la trama y determina que ésta debe ser inundada en el enlace Ethernet inferior. Segmento 2.
3. Cuando esta copia de la trama llega al Switch B, el proceso se repite y se transmite una copia de la trama al Ethernet superior. Segmento 1.
4. Debido a que la copia original de la trama llega al Switch B en el segmento 1 en algún momento posterior a su recepción por el Switch A, podría haber sido transmitido también por el Switch B al Segmento 2. en consecuencia, estas tramas viajarían alrededor de un bucle en ambas direcciones aunque el puesto de destino haya recibido ya una copia de la trama.

Una solución basada en la evitación de bucles eliminaría este problema impidiendo que una de las cuatro interfaces transmitiera o recibiera tramas durante operaciones normales.

2.2.1.5 Como se transmiten las tramas.

Para gestionas la conmutación de tramas se utiliza tres modos de operación primarios:

- **Guardar y retransmitir.** En el modo guardar y retransmitir, el switch debe recibir la trama completa para poder retransmitirla. Se leen las direcciones de origen y destino, se lleva a cabo la comprobación de redundancia cíclica (CRC), se aplican los filtros apropiados y se retransmite finalmente la trama. Si la CRC es incorrecta, la trama se descarta. La demora (o retraso) que tiene lugar en el switch depende de la longitud de la trama.
- **Modo de corte.** En el modo de corte, el switch verifica la dirección de destino (DA) en cuanto se recibe la cabecera y comienza de inmediato a enviar la trama. Dependiendo del protocolo de transporte de red utilizado (sin conexión u orientado a la conexión), existe una reducción significativa en el retardo entre el puerto de entrada y el de salida. El retardo en la conmutación basada en el modo de corte permanece constante con independencia del tamaño de la trama, debido a que en este modo, la retransmisión de la trama comienza en cuanto el

switch lee la dirección de destino. (En algunos switches, sólo se lee la dirección de destino.) La desventaja de este modo es que el switch podría retransmitir una trama de colisión o una trama con un valor CRC incorrecto. Algunos switches continúan leyendo la CRC y guardan un registro de errores. Si la tasa de error es demasiado alta, el switch puede ser configurado (de forma automática o manual) para utilizar el modo de guardar y retransmitir.

- **Sin fragmentos.** En el modo sin fragmentos (conocido también como modo de corte modificado), el switch lee los primeros 64 bytes antes de retransmitir la trama. Normalmente, la colisiones tienen lugar en los primeros 64 bytes de una trama. Al leer esos 64 bytes, el switch puede filtrar las tramas que están libres de colisiones.

2.2.1.6 Cómo dialoga el switch con otros dispositivos.

Un switch de red proporciona conectividad entre los dispositivos de la red. Una de las principales razones para colocar switches en una red es mejorar la conectividad. Como dispositivo intermedio entre otros dispositivos, el switch cuenta con varios modos de comunicación entre él y los dispositivos de destino. Los modos usados para establecer comunicaciones entre el switch y el dispositivo de destino, son half-duplex y full-duplex. Éstos son parámetros configurables que pueden afectar a la velocidad a la que un dispositivo puede enviar paquetes al switch para su retransmisión.

El modo de transmisión half-duplex implementa acceso múltiple con detección de portadora (carrier) y detección de colisiones (CSMA/CD). La LAN compartida tradicional opera en el modo half-duplex y es susceptible de colisiones de transmisión a través del cableado. Half-duplex es básicamente como un puente de un solo carril que cruza un río.

Ethernet full-duplex mejora significativamente el rendimiento de la red sin el gasto de instalar un nuevo medio. La transmisión full-duplex entre puestos se consigue usando conexiones Ethernet punto a punto y Fast Ethernet. Las tramas enviadas por dos nodos finales conectados no pueden colisionar, debido a que usan dos circuitos independientes de un cable de par trenzado. La conexión full-duplex consume un solo puerto.

Las conexiones de puertos full-duplex pueden usar medios 10BaseT y 100BaseFX para proporcionar enlaces punto a punto entre switches o nodos finales, pero no entre enlaces compartidos. Los nodos conectados directamente a un puerto de switch dedicado y con una tarjeta de red que soporte full-duplex pueden ser conectados a puertos de switch configurados para operar en el modo full-duplex. la mayoría de las tarjetas de red Ethernet y Fast Ethernet que se comercializan hoy día ofrece la posibilidad full-duplex. En el modo full-duplex, se desactiva el circuito de detección de colisiones.

Los nodos conectados a hubs, o los que comparten sus conexiones con un puerto de switch, deben operar en el modo half-duplex, debido a que los puestos finales deben ser capaces de detectar colisiones.

La eficiencia de la configuración Ethernet estándar se sitúa normalmente entre el 50 y 60 por cien del ancho de banda 10 Mbps. Ethernet full-duplex ofrece el 100 de cien de eficiencia en ambas direcciones (se transmite a 10 Mbps y se recibe a 10 Mbps).

2.2.2 Switch de capa de red.

Este tipo de *switches* integran *routing* y *switching* para producir altas velocidades. Este nuevo tipo de dispositivos es el resultado de un proceso de evolución natural de las redes de área local, ya que, combinan las funciones de los *switches* capa 2 con las capacidades de los routers.

Existen dos tipos de switches capa 3:

- *Packet-by-packet* (PPL3).
- *Cut-trough* (CTL3).

En ambos tipos de *switche*s, se examinan todos los paquetes y se envían a sus destinos. La diferencia real entre ellos es el rendimiento. PPL3 enruta todos los paquetes, en tanto que los *switches* CTL3 efectúan la entrega de paquetes de una forma un poco distinta, estos *switches* investigan el destino del primer paquete en una serie. Una vez que lo conoce, se

establece una conexión y el flujo es conmutado en capa 2 (con el consiguiente, rendimiento del *switching* de capa 2).

Funciones:

- Procesamiento de rutas: esto incluye construcción y mantenimiento de la tabla de enrutamiento usando RIP y OSPF.
- Envío de paquetes: una vez que el camino es determinado, los paquetes son enviados a su dirección destino. El TTL (Time-To-Live) es decrementado, las direcciones MAC son resueltas y el *checksum* IP es calculado.
- Servicios especiales: traslación de paquetes, prioritización, autenticación, filtros, etc.

2.2.3 Switch capa de transporte.

La información en los encabezados de los paquetes comúnmente incluyen direccionamiento de capa 2 y 3, tal como: tipo de protocolo de capa 3, TTL y *checksum*. Hay también información relevante a las capas superiores, como lo es el tipo de protocolo de capa 4 (UDP, TCP, etc.) y el número de puerto (valor numérico que identifica la sesión abierta en el host a la cual pertenece el paquete).

En el caso de los *switches* capa 3, éstos son *switches* capa 2 que utilizan la información del encabezado de capa 3. Lo mismo ocurre con los *switches* capa 4 , son *switches* capa 3 que procesan el encabezado de la capa. También son conocidos como switches sin capa (Layerless switches).

La información del encabezado de capa 4 permite clasificar de acuerdo a secuencias de paquetes manejados por aplicación (denominados "flujos"). Ahora bien, dependiendo del diseño del *switch*, éste puede prioritizar servicios o garantizar ancho de banda por "flujos". Algunos de los diseños de capa 4 son (Torrent, 1998):

Arquitectura basado en *Crossbard*: generalmente, sólo proveen prioritización por flujos porque tienen un esquema de *buffering* y de planificación muy compleja.

Switches con memoria compartida y cola de salida: son capaces de manejar múltiples niveles de prioridades. Resultando con problemas en proveer servicios cuando el número de flujos excede el número de colas disponibles.

Switches con colas por "flujos": son capaces de garantizar ancho de banda y manejar bien la congestión y pudiendo hacer la clasificación por flujos porque existe una cola por cada uno.

2.3 Algunas consideraciones acerca de switching y routing.

Los diseñadores y administradores de redes necesitan saber como y cuando usar las tecnologías de las que hemos hablado hasta ahora:

Colocar los *switches* capa 3 en puntos de concentración de la red o como *backbone* colapsado para eliminar "cuellos de botella".

Evitar enrutar en los *switches* capa 2 ubicados en los extremos o fronteras de la red.

Escoger *switches* capa 3 que tengan *buffers* con capacidad desde 50 hasta 100 paquetes por puerto y enviar millones de paquetes por segundo en la capa 3.

Evitar retardos excesivos, limitando los dominios de colisión entre 10 y 20 usuarios.

Cuando se escogen *switches* capa 2 con soporte de VLAN se debe tomar en cuenta que la comunicación *inter-vlan* se hace usando un *router* y que, éste puede convertirse en un "cuello de botella" si la red es muy grande.

2.4 Firewalls.

Una forma habitual de garantizar la integridad de la infraestructura es a través de los firewalls. Un firewalls, en su sentido más amplio, controla el flujo de tráfico. Se crean reglas para permitir o denegar los distintos tipos de tráfico y equilibrar las decisiones sobre enrutamiento tomadas. El permiso o la denegación del tráfico pueden incluir servicios de red

específicos. Generalmente, los Firewalls son implementados en los puntos de entrada y salida de la infraestructura de red, como se muestra en la figura 2.6.

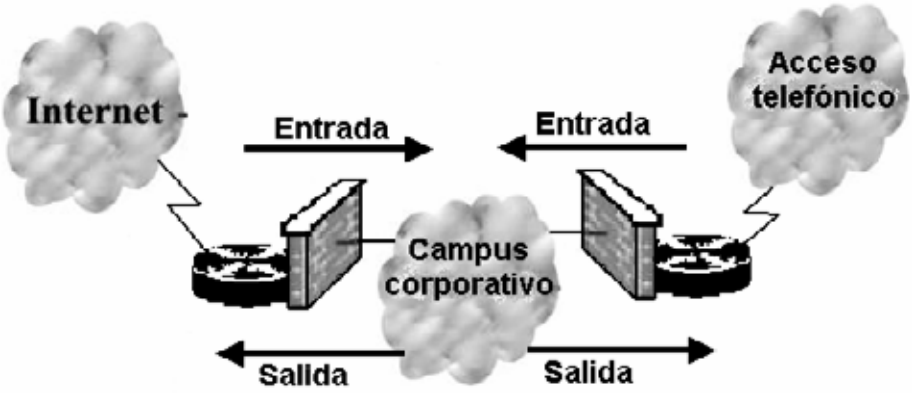


Figura 2.6 Implementación del Firewall.

2.4.1 Configuraciones comunes de Cortafuegos.

Firewall por hardware : Donde se sitúa en mi red.

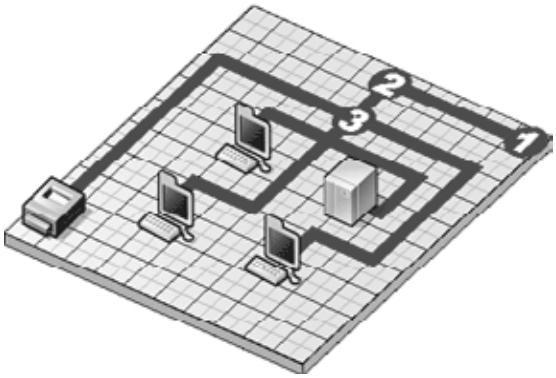


Figura. 2.7

1- Router (ADSL / FrameRelay / Cable / ...)

2 - Firewall (también llamado Cortafuegos en Castellano)

3 - Hub o Switch

2.4.2 Tipos de Firewalls

Podemos comprar un Firewall en forma de dispositivo de red que se conecta directamente al Switch/Hub por un lado y al Router por el otro, o podemos utilizar un PC y añadirle un software de Firewall.

El Firewall por hardware (el dispositivo) siempre es más sencillo de implementar y configurar que el Firewall basado en un PC con software especial. El Firewall por hardware también acostumbra a requerir mucho menos mantenimiento.

Figura. 2.8 Firewall (dispositivo)

No hay tantas diferencias entre los dos tipos como se podría pensar. Además las últimas tecnologías no aportan claridad para distinguirlas hasta el punto que no está claro cual es mejor y cual es peor. Pero en cualquier caso, se deberá prestar atención y poner mucho cuidado a la hora de instalar la que realmente se necesita en nuestra organización.
Firewall de nivel de red: filtrado de paquetes según:

- La dirección IP origen.
- La dirección IP destino.
- Campo de opciones IP.
- El protocolo a nivel de transporte

Cabecera IP

- El puerto origen y destino
- Banderas SYN/ACK (sólo TCP)

Cabecera TCP/UCP

Los Firewalls a nivel de red generalmente, toman las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP. Un simple router es un "tradicional" Firewall a nivel de red, particularmente, desde el momento que no puede tomar decisiones sofisticadas en relación con quién está hablando un paquete ahora o desde donde está llegando en este momento. Los modernos Firewall a nivel de red se han sofisticado

ampliamente, y ahora mantienen información interna sobre el estado de las conexiones que están pasando a través de ellos, los contenidos de algunos datagramas y más cosas. Un aspecto importante que distingue a los Firewall a nivel de red es que ellos enrutan el tráfico directamente a través de ellos, de forma que un usuario cualquiera necesita tener un bloque válido de dirección IP asignado. Los Firewalls a nivel de red tienden a ser más veloces y más transparentes a los usuarios.

2.4.3 Decisiones básicas al adquirir un Firewall.

Algunas de las decisiones básicas al adquirir un Firewall que hay que tratar en el momento de que una persona toma la responsabilidad (o se la asignan), de diseñar, especificar e implementar o supervisar la instalación de un Firewall.

El primero y más importante, es reflejar la política con la que la compañía u organización quiere trabajar con el sistema: ¿Se destina la Firewall para denegar todos los servicios excepto aquellos críticos para la misión de conectarse a la red? o ¿Se destina la Firewall para proporcionar un método de medición y auditoria de los accesos no autorizados a la red?

El segundo es: ¿Qué nivel de vigilancia, redundancia y control queremos? Hay que establecer un nivel de riesgo aceptable para resolver el primer asunto tratado, para ellos se pueden establecer una lista de comprobación de los que debería ser vigilado, permitido y denegado. En otras palabras, se empieza buscando una serie de objetivos y entonces se combina un análisis de necesidades con una estimación de riesgos para llegar a una lista en la que se especifique los que realmente se puede implementar.

El tercer asunto es financiero. Es importante intentar cuantificar y proponer soluciones en términos de cuanto cuesta comprar o implementar tal cosa o tal otra. Por ejemplo, un producto completo de red Firewall puede costar 100.000 dólares. Pero este precio se trata de una Firewall de alta resolución final. Si no se busca tanta resolución final, existen otras alternativas mucho más baratas. A veces lo realmente necesario no es gastarse mucho dinero en una Firewall muy potente, sino perder tiempo en evaluar las necesidades y encontrar una Firewall que se adapte a ellas.

En cuanto al asunto técnico, se debe tomar la decisión de colocar una máquina desprotegida en el exterior de la red para correr servicios proxy tales como telnet, ftp, news, etc. , o bien colocar un router cribador a modo de filtro, que permita comunicaciones con una o más máquinas internas. Hay sus ventajas e inconvenientes en ambas opciones, con una máquina proxy se proporciona un gran nivel de auditoria y seguridad en cambio se incrementan los coste de configuración y se decrementa el nivel de servicio que pueden proporcionar.

2.4.4 Firewall a nivel de aplicación.

Ordenador que ejecuta un software de servidor proxy cuyas características son:

- Conexión a nivel de aplicación.
- Depende del servicio.
- Requiere modificaciones de clientes.
- Suministran informes.

Los Firewalls a nivel de aplicación son generalmente, hosts que corren bajo servidores proxy, que no permiten tráfico directo entre redes y que realizan logines elaborados y auditan el tráfico que pasa a través de ellos. Los Firewall a nivel de aplicación se pueden usar como traductores de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro. Los primeros Firewalls a nivel de aplicación eran poco transparentes a los usuarios finales, pero los modernos Firewalls a nivel de aplicación son bastante transparentes. Los Firewalls a nivel de aplicación, tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad. Esto las hace diferenciarse de los Firewalls a nivel de red.

2.4.5 Arquitecturas más populares de Firewall.

Firewall a nivel de red:

- **“Screened host Firewall”** (Firewall mediante filtrado de host). En dicho Firewall, se accede a y desde un único host el cual es controlado por un router operando a nivel de

red. El host es como un bastión, dado que está muy defendido y es un punto seguro para refugiarse contra los ataques.

- **“Screened subnet Firewall”** (Firewall mediante filtrado de subred). En este Firewall se accede a y desde el conjunto de la red, la cual es controlada por un router operando a nivel de red. Es similar al Firewall indicado en el ejemplo anterior salvo que esta si que es una red efectiva de hosts protegidos.

Firewall a nivel de aplicación:

- **“Dual homed gateway”** (Firewall mediante host de doble conexión o gateway de dos dominios). Es un host de alta seguridad que corre bajo software proxy. Consta de 2 interfaces de red (uno a cada red) los cuales bloquean todo el tráfico que pasa a través del host.

El futuro de los Firewalls se encuentra a medio camino entre los Firewalls a nivel de red y los Firewalls a nivel de aplicación. El resultado final de los estudios que se hagan será un sistema rápido de protección de paquetes que conecte y audite datos que pasan a través de el. Cada vez más, los Firewalls (tanto a nivel de red como de aplicación), incorporan encriptación de modo que, pueden proteger el tráfico que se produce entre ellos e Internet. Los Firewalls con encriptación extremo-a-extremo (end-to-end), se puede usar por organizaciones con múltiples puntos de conexión a Internet , para conseguir utilizar Internet como una "central privada" donde no sea necesario preocuparse de que los datos o contraseñas puedan ser capturadas.

Actualmente, existen tres clasificaciones de los firewalls que abarcan distintas características de filtrado:

- **Filtrado de paquetes.** Estos firewalls se apoyan exclusivamente en las cabeceras TCP, UDP, ICMP e IP de los paquetes individuales para permitir o denegar el tráfico. El filtro de paquetes busca una combinación del sentido del tráfico (de entrada o de salida), el origen IP y la dirección de destino y los números de puerto de origen y de destino TCP y UDP.
- **Filtrado de circuitos.** Estos firewalls controlan el acceso manteniendo la información sobre el estado y reconstruyendo el flujo de datos asociados al tráfico. Un filtro de circuitos no pasa un paquete de un lado a otro a menos que forme parte de una conexión establecida.

- **Gateways de aplicación.** Estos firewalls procesa mensajes específicos y no pueden proteger el tráfico fácilmente utilizando protocolos más recientes.

Antes de determinar qué clasificaciones se adaptan mejor a su entorno, examine el flujo de tráfico que se pueda ejercer en el entorno. La mayor parte del control está basado en una combinación de las siguientes características:

- Sentido del tráfico.
- Origen del tráfico.
- Dirección IP.
- Números de puerto.
- Autentificación.
- Contenido de la aplicación.

- **Sentido del tráfico:** Que puede ser filtrado en sentido entrante o en sentido saliente. Por regla general, el tráfico **entrante** procede de un origen externo no fiable y se dirige a la red interna de confianza. El tráfico **saliente** procede del interior de la red fiable y se dirige a una red externa no fiable.

- **Origen del tráfico:** El hecho de que el tráfico se inicie desde la red interna (de confianza) o desde el exterior (no fiable) puede ser un factor a la hora de administrar el flujo del tráfico. Por ejemplo, podría optar por permitir que ciertos paquetes UDP se originaran desde el interior de la red de confianza (DNS), pero podría no permitir que las peticiones DNS entraran desde la red externa no fiable. Alternativamente, podría optar por limitar el tráfico TCP a las redes externas no fiables si la sesión TCP se inició desde la red interna de confianza.

- **Direcciones IP:** La dirección de origen o de destino se puede usar para filtrar cierto tipo de tráfico. Esta solución resulta útil a la hora de implementar los controles iniciales con el fin de evitar los ataques ilegales.

- **Número de puerto:** Los números de puerto de origen y destino TCP y UDP se usan para reconocer y filtrar distintos tipos de servicios.

- **Autentificación:** En ciertos puntos de ingreso a las redes de confianza, posiblemente quiera autenticar a los usuarios antes de que éstos puedan acceder a servicios concretos, como Telnet, FTP o HTTP. Los mecanismos de autentificación disponibles varían, pero todos ellos ayudan a la hora de controlar el uso y a la hora de auditar quién está accediendo a qué servicios. A mayor abundamiento, la autenticación también puede ayudar a los proveedores de servicios a generar información relativa a la facturación y la contabilidad.

- **Contenido de la aplicación:** Puede resultar útil examinar las aplicaciones y determinar ciertos controles. Es posibles que quiera examinar ciertos URL o filtrar tipos de contenido específicos.

2.4.6 Arquitectura avanzada de los Firewalls.

Aunque un router pantalla constituye un buen primer paso para proporcionar la seguir-dad de acceso a Internet, una solución más segura se apoya en una arquitectura de Firewall más robusta. Normalmente, esto se lleva a cabo con un router pantalla y con opciones de Firewall más intensas. Aparte de las opciones de filtrado primitivas, un Firewall suele proporcionar:

- Inspección avanzada paquete por paquete.
- Filtrado del contenido de la aplicación.
- Autenticación / autorización de la aplicación.
- Tecnología de cifrado.
- Traducción de direcciones de red (NAT).

Las opciones de filtrado del tráfico deberán incorporar información relativa al estado y también deberán ser capaces de filtrar en base al contenido de la aplicación. El escaneado de virus de correo electrónico, el filtrado de *applets* Java y el registro o el bloqueo URL son algunas de las funciones avanzadas que se suelen implementar en un Firewall.

A veces, estas funciones específicas de la aplicación son descargadas en dispositivos separados con el fin de guardar los ciclos de procesamiento de la CPU en el propio dispositivo del Firewall.

La autentificación y confidencialidad de los paquetes que utilizan el cifrado se está convirtiendo en un requisito vital. La implementación de esta funcionalidad de un modo ampliable a todos los fabricantes se ha generalizado con el advenimiento de los productos IPSec. Las opciones de autenticación y confidencialidad IPSec pueden ser aplicadas a muchas arquitecturas de acceso a Internet con el fin de proporcionar el flujo de tráfico confidencial y autenticado.

NAT también se usa mucho pero, “Consideraciones relativas a las normas de seguridad de un sitio”, es necesario usar una dirección legítima asignada por la NIC para evitar cualquier restricción de aplicación u opción en el futuro.

Capítulo III
Diseño de seguridad en redes.

3.1 Tecnologías de seguridad.

Hay una amplia gama de tecnologías de seguridad que proporciona soluciones para proteger el acceso a una red y los mecanismos de transporte de datos de la infraestructura de una red corporativa. Muchas de las tecnologías se pueden utilizar de modo indistinto a la hora de solucionar los problemas relacionados con la identidad del usuario o dispositivo, la integridad de los datos y la confidencialidad de los datos.

La autenticación es el proceso de validación de la identidad reivindicada por un usuario final o un dispositivo (como los clientes, los servidores, los switches, los routers, los Firewalls, etc.). La autorización es el proceso de concesión de derechos de acceso a un usuario, grupo de usuarios o sistema específico; el control de acceso limita el flujo de información de los recursos de un sistema a exclusivamente las personas o sistemas de la red.

3.1.1 Tecnologías de identidad.

La autenticación es un elemento fundamental, ya que todo se basa en la identidad de quién está tratando de obtener acceso a los recursos restringidos. El grado de infalibilidad del método de autenticación depende de la tecnología que se utilice.

3.1.1.1 Contraseñas seguras.

Aunque las contraseñas se suelen utilizar como prueba de la autenticidad de un usuario o dispositivo, es muy fácil descifrarlas si son fáciles de adivinar, si no son cambiadas con la suficiente frecuencia y si no transmitidas en texto claro por una red. Para que las contraseñas sean más seguras, hay métodos más robustos que cifran la contraseña o modifican el cifrado, de forma que el valor cifrado cambie cada vez. Éste es el caso de los esquemas de contraseñas de un solo uso, de entre los cuales los más comunes son el protocolo S/ley y de autenticación de contraseña por tokens.

3.1.1.1.1 El protocolo de contraseña S/Key.

El sistema de contraseña de un solo uso S/Key está diseñado para computar un ataque de reproducción cuando un usuario está tratando de iniciar sesión en un sistema. Un ataque de reproducción en el contexto del inicio de sesión se produce cuando alguien escucha fraudulentamente una conexión de red para obtener el ID de inicio de sesión y la contraseña de un usuario legítimo y que la usa posteriormente para acceder a la red.

El funcionamiento del protocolo S/Key está basado en una estructura cliente/servidor: el cliente suele ser un PC, mientras que el servidor suele ser UNÍS. Inicialmente, tanto el cliente como el servidor deberán estar configurados con la misma frase de paso y una cuenta de iteración. La cuenta de iteración específica cuántas veces se va a aplicar una determinada entrada a la función *hash*. El cliente inicia un intercambio S/Key enviando un paquete de inicialización; el servidor responde con un número de secuencia a una *seed*, como muestra la figura 3.1

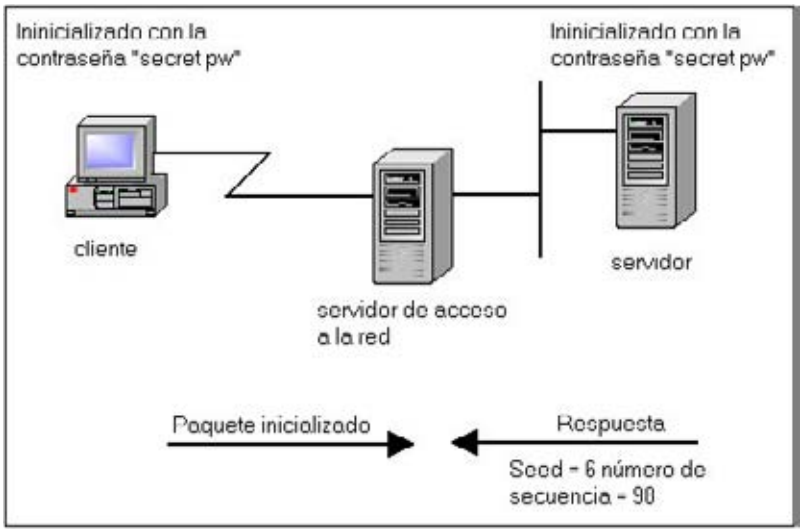


Figura 3.1 El intercambio S/Key inicial.

El cliente calcula la contraseña de un solo uso, proceso que implica tres pasos distintos: un paso de preparación, un paso de generación y una función de salida.

1. En el **paso de preparación**, el cliente introduce una frase de paso secreta. Esta frase de paso está concatenada con la *seed* que fue transmitida desde el servidor en texto claro.
2. El **paso de generación** se aplica múltiples veces a la función *hash* segura, generando una salida final de 64 bits.
3. La **función de salida** toma la contraseña de un solo uso de 64 bits y la muestra en un modo legible.

La última fase consiste en que el cliente pase la contraseña de un solo uso al servidor, donde puede ser verificada.

3.1.1.1.2 Esquema de autenticación de contraseña por tokens

Los sistemas de autenticación por token suelen requerir el uso de una tarjeta especial (llamada **tarjeta inteligente** o **tarjeta de token**), aunque ciertas implementaciones se ponen en práctica utilizando software para mitigar el problema de la pérdida de la tarjeta inteligente o tarjeta de tokens. Estos tipos de mecanismo de autenticación están basados en uno de estos dos esquemas: la **respuesta por desafío** y la **autenticación por sincronía**.

La solución de la respuesta por desafío aparece en la figura 3.2. Los siguientes pasos generan el intercambio de la autenticación:

1. El usuario llama a un servidor de autenticación, que emite una solicitud para un ID de usuario.
2. el usuario facilita el ID al servidor, que emite un desafío (un número aleatorio que aparece en la pantalla del usuario).
3. El usuario introduce ese número de desafío en la tarjeta de tokens, que es como un dispositivo para tarjetas de crédito, que cifra el desafío con la clave de cifrado del usuario y que muestra una respuesta.
4. El usuario escribe esta respuesta y la envía al servidor de autenticación. Mientras el usuario está obteniendo una respuesta del token, el servidor de autenticación calcula cuál deberá ser la respuesta adecuada de acuerdo con su base de datos de claves de usuario.

5. cuando el servidor recibe la respuesta del usuario, la compara con la que ha calculado.

Si las dos respuestas coinciden, el usuario tendrá acceso a la red. Si no coinciden, el acceso será denegado.

El esquema de autenticación por sincronía horaria es un algoritmo patentado que se ejecuta en el token y en el servidor para generar números idénticos que cambian periódicamente. El usuario llama al servidor para generar números idénticos que cambian periódicamente. El usuario llama al servidor de autenticación, que pide un código de acceso. El usuario introduce un número de identificación personal (PIN) en la tarjeta de tokens, y los dígitos aparecen en ese momento en el token. Estos dígitos representan la contraseña de un solo uso y son enviados al servidor. El servidor compara esta entrada con la secuencia generada; si coinciden, concederá acceso a la red al usuario.

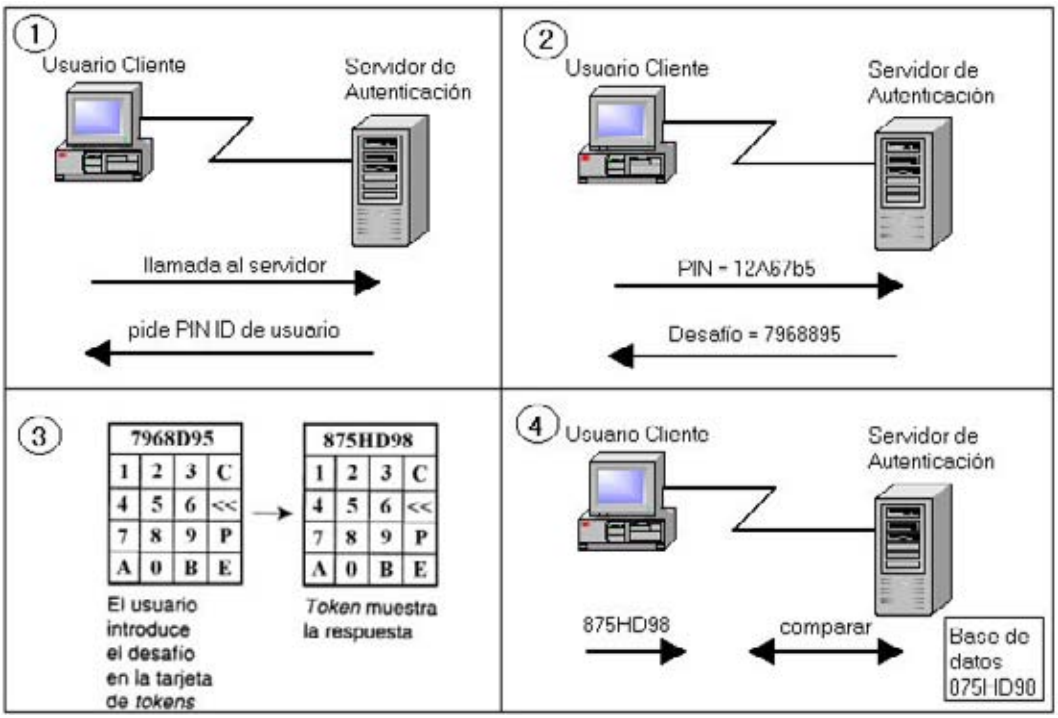


Figura 3.2 Autenticación de token con respuesta por desafío

El uso de los esquemas de respuestas por desafío o de contraseña de tokens con sincronía suele requerir que el usuario disponga de un dispositivo parecido al de los dispositivos

para tarjetas de crédito, que proporcione credenciales de autenticación. Esto puede suponer un problema para algunos usuarios, ya que tienen que acordarse de llevar el dispositivo, pero es lo suficiente flexible como para permitir un acceso autenticado casi seguro desde cualquier parte del mundo.

3.1.1.2 Protocolo de autenticación PPP.

Las contraseñas están incorporadas en muchos protocolos que proporcionan servicios de autenticación. En lo que respecta a las conexiones de acceso telefónico, se suele utilizar el protocolo punto a punto (PPP) para establecer una conexión de acceso telefónico sobre líneas serie RDSI. Entre los mecanismos de autenticación PPP se incluyen el protocolo de autenticación de contraseña (PAP), el protocolo de autenticación de intercambio de señales por desafío (CHAP) y el protocolo de autenticación extensible (EAP). En todos estos casos, es el dispositivo el que está siendo autenticado, en vez del usuario del dispositivo.

3.1.1.2.1 Negociaciones PPP.

Las negociaciones PPP se componen de la negociación LCP y de la negociación NCP. LCP es el encargado de establecer la conexión con ciertas opciones negociadas, manteniendo la conexión y proporcionando procedimientos que cierran la conexión. Para llevar a cabo estas funciones, el LCP está organizado en las cuatro fases siguientes:

1. Establecimiento de enlace y negociación de la configuración.
2. Determinación de la calidad del enlace.
3. Negociación de la configuración de protocolo de capa de red.
4. Finalización del enlace.

Para establecer las comunicaciones sobre el enlace punto a punto, cada extremo del enlace PPP deberá enviar paquetes LCP que configuren el enlace de datos durante la fase de establecimiento del enlace. Una vez establecido el enlace, PPP proporciona una fase de autenticación opcional antes de seguir en la fase del protocolo de capa de red. La fase NCP establece y configura los distintos protocolos de capa de red, como IP. Si se desea la autenticación del enlace, una implementación especificará la opción de configuración del protocolo de autenticación durante la fase de establecimiento del enlace. Estos protocolos de

autenticación están destinados a ser usados principalmente por hosts y routers que se conectan a un servidor de red PPP a través de circuitos conmutados o líneas e acceso telefónico, pero que también pueden ser aplicados a enlaces dedicados. El servidor puede usar la identificación del host o router de conexión en la selección de las opciones para las negociaciones de capa de red.

3.1.1.2.2 Protocolo de autenticación de contraseña PPP.

El **protocolo de autenticación de contraseña (PAP)** proporciona una manera muy sencilla de que un igual establezca su identidad ante el autenticador utilizando un intercambio de señales bidireccional. Esto sólo se hace en el establecimiento inicial del enlace. Hay tres tipos de trama PAP, como se ve en la figura 3.3.

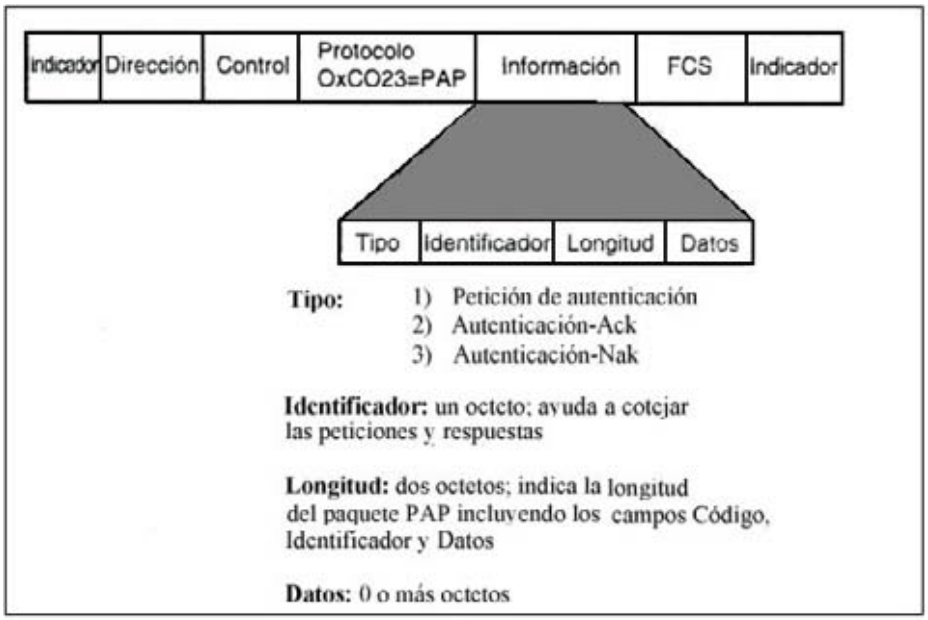


Figura 3.3 Los tres tipos de trama PAP de PPP.

Una vez completada la fase de establecimiento del enlace, se usa el paquete de petición de autenticación para iniciar la autenticación PAP. Este paquete contiene el nombre y la contraseña del igual, como se muestra en la figura 3.4.

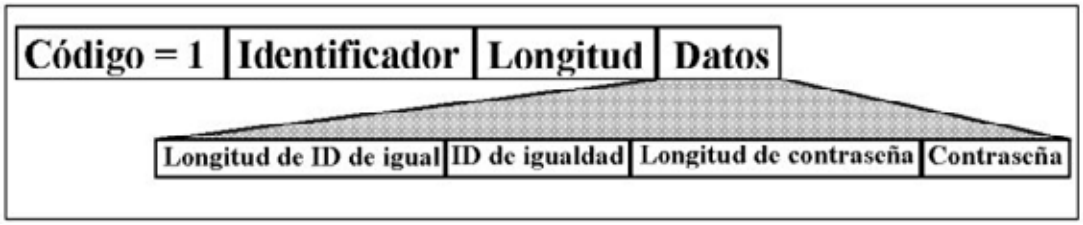


Figura 3.4 Petición de autenticación PAP de PPP

Este paquete de petición es enviado repetidas veces hasta que se recibe un paquete de respuesta válido o cuando expira un contador de reintentos opcional. Si el autenticador recibe un par ID de igual / Contraseña reconocible y aceptable, deberá responder con un acuse de recibo (ACK) de autenticación.

PAP no es un método de autenticación sólido. PAP sólo autentica al igual, y las contraseñas son enviadas sobre el circuito sin protección alguna. No existe protección frente a los frente a los ataques reiterados de prueba y error.

3.1.1.2.3 El protocolo de autenticación de intercambio de señales por desafío de PPP.

El **protocolo de autenticación de intercambio de señales por desafío de (CHAP)** de PPP se usa para verificar periódicamente la identidad de un *host* o usuario final utilizando un intercambio de señales de tres vías. El protocolo CHAP se ejecuta en el establecimiento del enlace inicial y puede ser repetido en cualquier momento posterior al establecimiento del enlace.

CHAP impone la seguridad de red requiriendo que lo iguales compartan un secreto en texto plano. Este secreto nunca se envía por el enlace. Se efectúa la siguiente secuencia de pasos:

1. Una vez completada la fase de establecimiento del enlace, el autenticador envía un mensaje de desafío al igual. El desafío se compone de un identificador (ID), un número aleatorio y o bien el nombre de *host* del dispositivo local o el nombre del usuario del dispositivo remoto.

2. El igual receptor calcula un valor utilizando una función *hash* unidireccional; el secreto es la entrada de la función *hash* unidireccional.
3. El igual envía la respuesta al desafío, que consta de:
    - Una versión cifrada del ID.
    - Una contraseña secreta (el valor *hash* calculado).
    - El número aleatorio.
    - El nombre de *host* del dispositivo remoto o el nombre del usuario del dispositivo remoto.
4. Cuando el autenticador recibe la respuesta al desafío, verifica el secreto buscando el nombre que hay en la respuesta y efectuando la misma operación de cifrado. El autenticador compara la respuesta con sus propios cálculos del valor *hash* esperado.
5. Si los valores coinciden, el autenticador confirmará la autenticación y enviará un mensaje de éxito, y el LCP establecerá el enlace.

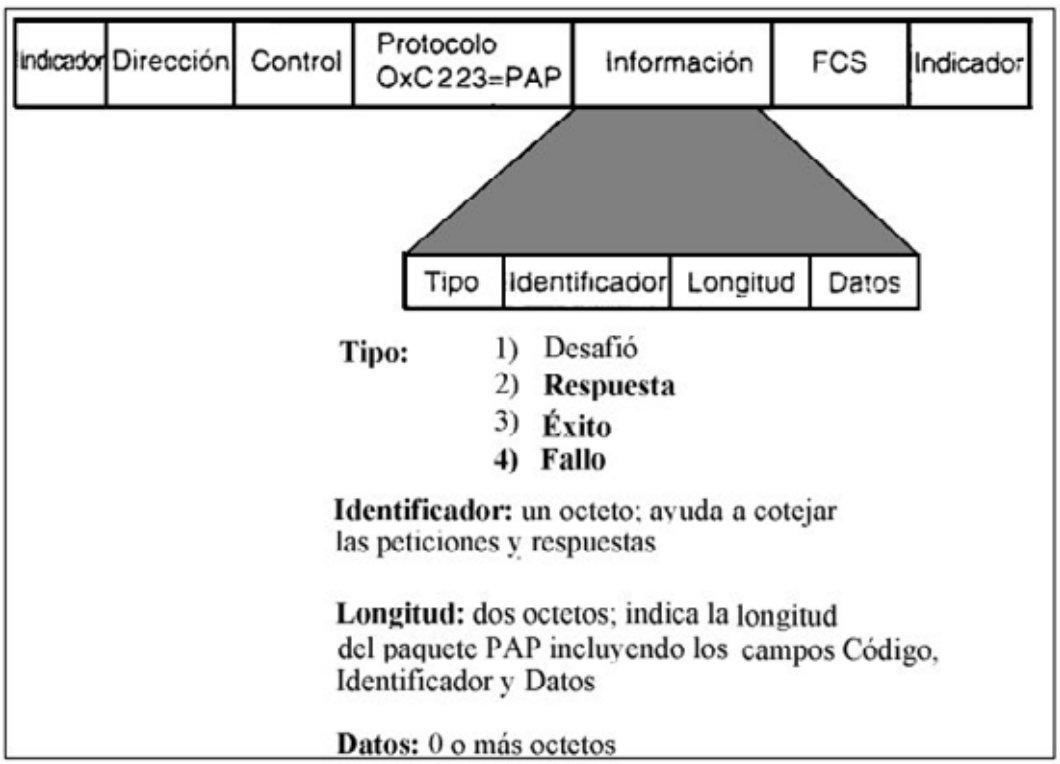


Figura 3.5 Tipos de trama CHAP de PPP.

CHAP proporciona protección frente al ataque de reproducción a través del uso de un identificador que cambia incrementalmente y de un valor de desafío variable. El uso de los

desafíos reiterados trata de limitar el tiempo de exposición ante un ataque. El autenticador es el que controla la frecuencia y la temporización de los desafíos.

3.1.1.2.4 El protocolo de autenticación extensible de PPP.

El **protocolo de autenticación extensible (EAP)** de PPP es un protocolo general que sirve para la autenticación PPP y que soporta múltiples mecanismos de autenticación. El protocolo EAP no selecciona un mecanismo de autenticación específico en la fase de control del enlace; más bien, aplaza la selección hasta la fase de autenticación, se forma que el autenticador pueda solicitar más información antes de determinar el mecanismo de autenticación específico. Esta disposición también permite utilizar un servidor *back-end*, que en realidad implementa los distintos mecanismo de autenticación, mientras que el autenticador PPP se limita a pasar el intercambio de autenticación.

En el caso que un router de una sucursal (el igual) está tratando de autenticarse ante el NAS (que es el autenticador), la secuencia de pasos es la siguiente:

1. Una vez completada la fase de establecimiento del enlace, el autenticador envía una o más peticiones para autenticar al igual. La petición posee un campo de tipo que indica lo que se está pidiendo. Entre los ejemplos de tipos de petición se incluyen la identidad, el desafío MD5, S/Key, la tarjeta de *token* genérica, etc. El tipo de desafío MD5 se corresponde directamente con el protocolo de autenticación CHAP.
2. El igual envía un paquete de respuesta contestando a cada petición. Al igual que el paquete de petición, el paquete de respuesta contiene un campo de tipo que se corresponde con el campo de tipo de la petición.
3. El autenticador finaliza la fase de autenticación con un paquete de éxito o de fallo.

El protocolo EAP incorpora más flexibilidad a la autenticación PPP y ofrece la posibilidad de usar nuevas tecnologías (como los certificados digitales).

3.1.1.2.5 Resumen de la autenticación PPP.

La autenticación PPP es necesaria para la conectividad de acceso telefónico. Es posible utilizar cualquiera de los mecanismo estándar disponibles (PAP, CHAP y EAP). La tabla 3.1 ofrece un resumen de las ventajas e inconvenientes de estos mecanismos.

Protocolo	Ventajas	Inconvenientes
PAP	Fácil de implementar	No posee una autenticación sólida; la contraseña se pasa sin protección entre el cliente y el servidor; no hay protección frente a la reproducción.
CHAP	Cifrado por contraseña	Debe haber una contraseña entre el cliente, almacenada en texto claro en el servidor; incorpora protección frente a la reproducción tanto en el cliente como en el servidor.
EAP	Soporte de autenticación flexible, más robusto.	Es nuevo; posiblemente no se haya generalizado todavía.

Tabla 3.1 Resumen de la autenticación PPP.

3.1.1.3 Protocolos que utilizan mecanismos de autenticación.

Muchos protocolos requieren la comprobación de la autenticación antes de proporcionar derechos de autorización y acceso al usuario o dispositivo. TACACS+ y RADIUS constituyen ejemplos de este tipo de protocolos, se suelen utilizar en entornos de acceso telefónico para proporcionar una base de datos de autenticación escalable, y pueden incorporar una serie de métodos de autenticación

3.1.1.3.1 El protocolo TACACS+

El protocolo TACACS+ es la última generación de TACACS. TACACS+ utiliza TCP como transporte. El demonio del servidor suele escuchar en el puerto 49, que es el puerto LOGIN asignado al protocolo TACACS. Este puerto está reservado en la RFC de números asignados

tanto UDP como para TCP. Las implementaciones actuales y extendidas de TACACS también utilizan el puerto 49.

TACACS+ es un protocolo cliente / servidor; el cliente TACACS+ suele ser un NAS y el servidor, suele ser un proceso de demonio que se ejecuta en un equipo UNÍS o NT. Un componente de diseño fundamental de TACACS+ es la separación de la autenticación, la autorización y la contabilidad.

3.1.1.3.1.1 Autenticación TACACS+

TACACS+ permite los intercambios de longitud arbitraria y de autenticación de contenido, lo cual permite a su vez usar cualquier mecanismo de autenticación con los clientes TACACS+ (incluyendo PAP, CHAP y EAP de PPP). La autenticación no es obligatoria; sino que es una opción configurada por el sitio. Algunos sitios no la requieren en ningún caso, mientras que otros sólo la requieren para ciertos servicios.

La autenticación TACACS+ contiene tres tipos de paquetes:

- START, que siempre es enviado por el cliente.
- CONTINUE, que siempre es enviado por el cliente.
- REPLY, que siempre es enviado por el servidor.

La autenticación comienza cuando el cliente envía un mensaje START al servidor. El mensaje START describe el tipo de autenticación que se va a ejecutar (por ejemplo, la contraseña de texto, PAP o CHAP), y puede contener el nombre de usuario y ciertos datos de autenticación. El paquete START sólo se envía como primer mensaje de una sesión de autenticación TACACS+, o como el paquete que sigue inmediatamente a un reinicio (el servidor puede solicitar un reinicio en un paquete REPLY). El número de secuencia del paquete START siempre es 1.

En respuesta a un paquete START, el servidor envía un mensaje REPLY. El mensaje REPLY indica si ha terminado la autenticación o si ésta debe continuar. Si el REPLY indica que la autenticación debe continuar, el mensaje también indicará que se solicita nueva información. El cliente recibe esa información y la devuelve en un mensaje CONTINUE. Este proceso se repite hasta que se recopila toda la información de autenticación, y el proceso se autenticación se termina.

3.1.1.3.1.2 Autorización TACACS+.

La autorización es la acción de determinar qué se le permite hacer a un usuario. Una petición de autorización puede indicar que el usuario no está autenticado (es decir, no se sabe quiénes son). En este caso, le compete al agente de autorización la acción de determinar si a un usuario no autenticado se le permite acceder a los servicios en cuestión.

Cuando la autenticación termina (si se usa),el cliente puede iniciar el proceso de autorización, si ésta es necesaria. Una sesión de autorización se define como un par sencillo de mensajes: un mensaje REQUEST seguido de un mensaje RESPONSE. El mensaje REQUEST de autorización contiene conjunto de campos fijos que describe la autenticidad del usuario o proceso, y un conjunto variable de argumentos que describe los servicios y las opciones para los que se solicita la autorización.

En TACACS+, la autorización no sólo proporciona respuestas sí o no, sino que también se puede personalizar el servicio para un usuario concreto.

3.1.1.3.1.3 Contabilidad TACACS+.

La contabilidad es la acción de registrar lo que un usuario está haciendo o ha hecho. La contabilidad en TACACS+ puede servir para dos cosas:

- puede ser utilizada para contabilizar los servicios utilizados, como en un entorno de facturación.

- Puede ser utilizada como herramienta de auditoria para servicios de seguridad.

TACACS+ soporta tres tipos de registros de contabilidad:

- Los **registros de inicio** indican que un servicio está a punto de iniciarse.
- Los **registros de parada** indican que un servicio acaba de terminar.
- Los **registros de actualización** son avisos intermedios que indican que un servicio sigue en ejecución.

Los registros de contabilidad TACACS+ contienen toda la información que se usa en los registros de autorización e información especifica de la contabilidad, como los momentos de inicio y parada (cuando sea necesario) e información relativa a la utilización de recursos.

3.1.1.3.1.4 Transacciones TACACS+.

Las transacciones entre el cliente TACACS+ y el servidor TACACS+ son autenticadas mediante el uso de un secreto compartido, que nunca es enviado por la red. Normalmente, el secreto se configura manualmente en ambas entidades. TACACS+ cifre todo el tráfico entre el cliente TACACS+ y el demonio del servidor TACACS+.

La figura 3.6 muestra la interacción entre un usuario de acceso telefónico y el cliente y el servidor TACACS+.

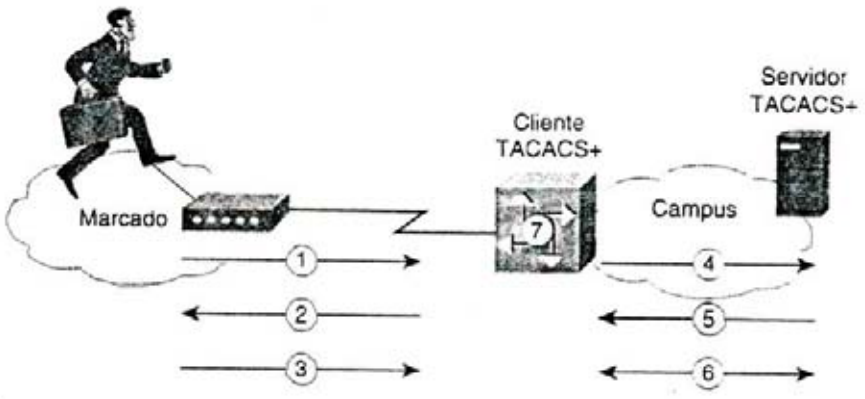


Figura 3.6 Un intercambio TACACS+.

1) El usuario inicia la autenticación PPP no NAS.
2) El NAS pide al usuario el nombre de usuario/contraseña (PAP) o desafío (CHAP).
3) El usuario responde.
4) El cliente TACACS+ envía un paquete cifrado al servidor TACACS+.
5) El servidor TACACS+ responde con el resultado de la autenticación.
6) El cliente y el servidor TACACS+ intercambian peticiones y respuestas de autorización.
7) El cliente TACACS+ actúa cuando se produce el intercambio de autorización.

3.1.1.3.2 El protocolo RADIUS.

El protocolo **Servicio de usuario de acceso telefónico mediante autenticación remota (RADIUS)** fue desarrollado como protocolo de autenticación y contabilidad de servidor de acceso.

RADIUS utiliza UDP como transporte. Por regla general, el protocolo RADIUS está considerado como un servidor sin conexión. Los temas relacionados con la disponibilidad, la retransmisión y los tiempos de espera del servidor son gestionados por los dispositivos RADIUS, y no por el protocolo de transmisión.

RADIUS es un protocolo cliente/servidor. El cliente RADIUS suele ser NAS; el servidor RADIUS suele ser un proceso de demonio que se ejecuta en un equipo UNÍS o NT. El cliente es el responsable de pasar información de usuario a los servidores RADIUS designados y de actuar frente a la respuesta devuelta. Los servidores RADIUS son los responsables de recibir las peticiones de conexión del usuario, de autenticar al usuario y de devolver toda la información sobre configuración necesaria para enviar el servidor al usuario.

3.1.1.3.2.1 Autenticación RADIUS.

El servidor RADIUS puede soportar una serie de métodos para la autenticación de un usuario. Cuando el servidor recibe el nombre de usuario y la contraseña original del usuario,

puede soportar los protocolos PAP o CHAP de PPP, el inicio de sesión UNÍS y otros mecanismos de autenticación. Lo que se soporte dependerá de lo que haya implementado el fabricante.

Normalmente, un inicio de sesión de usuario consta de una consulta (petición de acceso) del nas al servidor RADIUS y una respuesta (concesión de acceso o denegación de acceso) del servidor. El paquete de petición de acceso contiene el nombre de usuario, la contraseña cifrada, la dirección IP del NAS y el puerto. El formato de la petición también proporciona información acerca del tipo de sesión que el usuario desea iniciar.

Cuando el servidor RADIUS recibe el paquete de petición de acceso del NAS, busca el nombre de usuario en una base de datos. Si el nombre de usuario no existe en la base de datos, o bien se cargará un perfil predeterminado o bien el servidor RADIUS enviará inmediatamente un mensaje de denegación de acceso. Este mensaje puede ir acompañado de un mensaje de texto opcional, que puede indicar el motivo de la denegación.

3.1.1.3.2.2 Autorización RADIUS.

En RADIUS, las funcionalidades de autenticación y autorización están emparejadas. Si se encuentra el nombre de usuario, y la contraseña es correcta, el servidor RADIUS devolverá una respuesta de aceptación del acceso, incluyendo una lista de pares atributo/valor que describen los parámetros que se van a usar para esta sesión. Entre los parámetros más habituales se encuentran el tipo de servicio, el tipo de protocolo, la dirección IP a asignar al usuario (estática o dinámica), la lista de acceso a aplicar, o una ruta estática a instalar en la tabla de enrutamiento del NAS. La información sobre configuración del servidor RADIUS define lo que se va a instalar en el NAS.

3.1.1.3.2.3 Contabilidad RADIUS.

Las funciones de contabilidad del protocolo RADIUS se pueden usar de manera independiente de la autenticación o la autorización RADIUS. Las funciones de contabilidad RADIUS permiten que los datos sean enviados al principio y al final de las sesiones, indicando

el número de recursos (como el tiempo, los paquetes, los bytes, etc.) que hayan sido utilizados durante la sesión. Un proveedor de servicios de Internet (ISP) podría usar software de control de acceso y contabilidad RADIUS para satisfacer ciertas necesidades especiales de seguridad y facturación.

3.1.1.3.2.4 Transacciones RADIUS.

Las transacciones entre el cliente y el servidor RADIUS son autenticadas mediante el uso de un secreto compartido, que no se envía nunca por la red. Además, las contraseñas de usuario (si las hay) se envían de forma cifrada entre el cliente y el servidor RADIUS con el fin de eliminar la posibilidad de que alguien que accediera ilegítimamente a una red no segura pudiera determinar la contraseña de un usuario.

La Figura 3.7 muestra el proceso de inicio de sesión y autenticación de RADIUS.

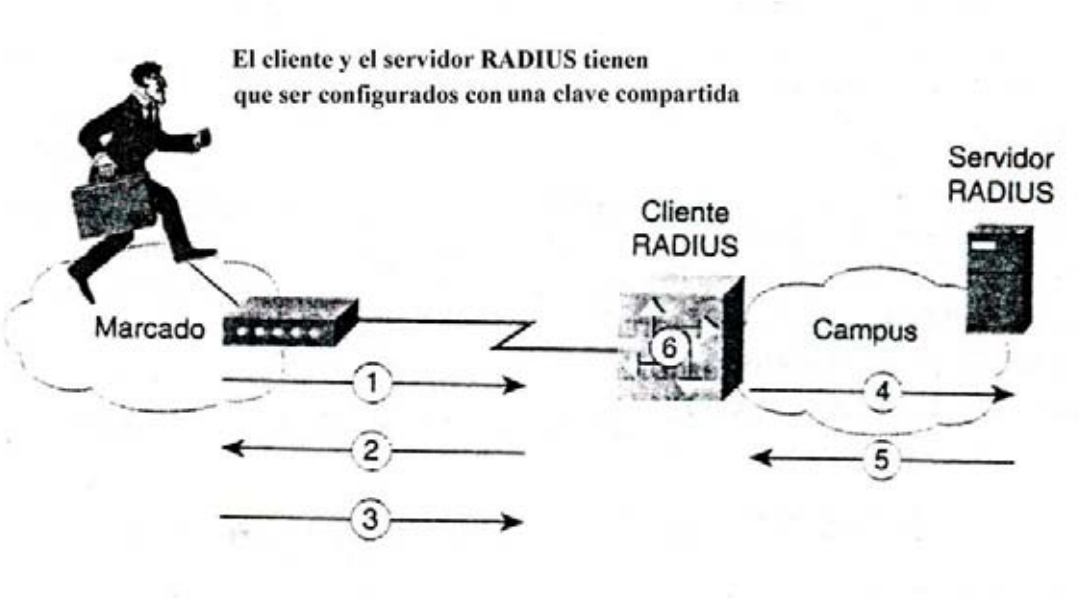


Figura 3.7 Inicio de sesión y autenticación RADIUS

1) El usuario inicia la autenticación PPP con el NAS.
2) El NAS pide al usuario el nombre de usuario/contraseña PAP o desafío (CHAP)
3) El usuario responde.

4) El cliente RADIUS envía el nombre de usuario y la contraseña cifrada al servidor RADIUS.
5) El servidor RADIUS responde con la aceptación, la denegación o el desafío.
6) El cliente RADIUS actúa cuando hay servicios y parámetros de servicios con aceptación/denegación.

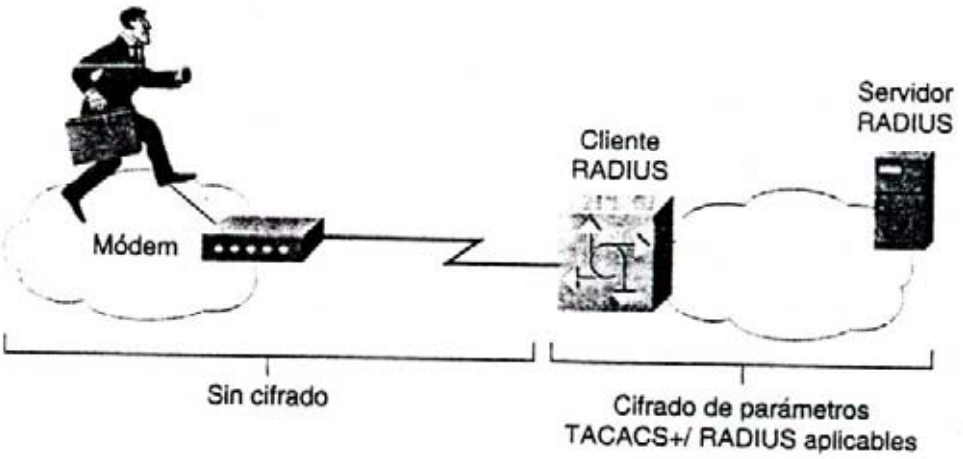


Figura 3.8 Cifrado TACACS+ / RADIUS

3.1.2 Tecnologías de seguridad de las redes privadas de acceso telefónico virtual.

Las **redes privadas de acceso telefónico virtual (VPDN)** permiten a las grandes empresas ampliar sus redes privadas a través de las líneas de acceso telefónico. En vez de invertir mucho en seguridad llamando a un sitio de campus desde cualquier parte del mundo o de reducirla llamando localmente y utilizando Internet como medio de transporte para acceder al campus empresarial principal, las nuevas tecnologías permiten que los sitios y los usuarios remotos se conecten de forma segura con la infraestructura de la empresa utilizando el acceso telefónico a Internet.

Actualmente, existen tres protocolos similares que cumplen este fin:

- El protocolo de reenvió de capa 2 (L2F).

- El protocolo de tunneling punto a punto (PPTP).
- El protocolo de tunneling de capa 2 (L2TP).

3.1.2.1 El protocolo de reenvío de capa 2.

El **protocolo de reenvío de capa 2 (L2F)** permite el tunneling de la capa de enlace, es decir, las tramas Control de enlace de datos de alto nivel (DIC), utilizando tales túneles, es posible desacoplar la ubicación del servidor de acceso telefónico inicial de la ubicación en la que se termina la conexión del protocolo de acceso telefónico y donde se proporciona el acceso a la red. Estos túneles también activan aplicaciones que requieren soporte para el acceso telefónico IP de direcciones privadas, IPX y AppleTalk utilizado SLIP/PPP en la infraestructura Internet existente.

3.1.2.2 El protocolo de tunneling punto a punto.

El **protocolo de tunneling punto a punto (PPTP)** fue iniciado por Microsoft. Es una arquitectura cliente/servidor que permite canalizar el protocolo punto a punto (PPP) a través de una red IP y que desacopla las funciones que hay en los NAS activos.

Cómo desacoplar la funcionalidad NAS tradicional.

Tradicionalmente, un NAS implementa las siguientes funciones:

- Proporcionar una interfaz física nativa a las redes PSTN o RDSI y controlar los adaptadores externos de módem o de terminal.
- Proporcionar la terminación lógica de una sesión LCP de un Protocolo punto a punto (PPP).
- Participar en los protocolos de autenticación PPP.
- Proporcionar la agragación y la administración para el protocolo multienlace PPP.
- Llevar a cabo la terminación lógica de los distintos Protocolos de control de red (NCP) de PPP.
- Llevar a cabo el enrutamiento y el puenteado multiprotocolo entre las interfaces NAS.

PPTP divide estas funciones entre dos entidades:

- **Concentrador de acceso PPTP (PAC).** Este dispositivo está conectado a una o más líneas PSTN o RDSI capaces de funcionar con PPP y de manipular el protocolo PPTP.
- **Servidor de red PPTP (PNS).** Este dispositivo administra el lado del servidor del protocolo PPTP. Dado que PPTP se fundamenta exclusivamente en TCP/IP y que es independiente del hardware de interfaz, el PNS puede usar cualquier combinación de hardware para interfaz IP, incluyendo los dispositivos LAN y WAN.

El PAC es el responsable de proporcionar la interfaz física a las redes PSTN y RDSI y de proporcionar la terminación lógica de las sesiones LCP de PPP. La participación en los protocolos de autenticación PPP puede ser parte del PAC o del PNS. El PNS es el encargado de la agregación de canales, la terminación lógica de los NCP de PPP, así como del enrutamiento y el puenteado multiprotocolo entre las interfaces NAS. El protocolo que se usa para ejecutar las unidades de datos del protocolo (PDU) de PPP entre el PAC y el PNS, aparte de los temas relativos al control de llamada y a la administración, son dirigidos por PPTP.

3.1.2.2.1 Panorámica del protocolo.

PPTP está orientado a la conexión. El PNS y el PAC mantienen información sobre la conexión para cada usuario que esté conectado a un PAC. Se crea una sesión cuando se intenta una conexión PPP de extremo a extremo entre un servidor de acceso telefónico y el PNS. Los datagramas que estén relacionados son enviados por el túnel entre el PAC y el PNS.

Un túnel viene definido por un par PNS-PAC. El túnel transporta datagramas PPP entre el PAC y el PNS. En un solo túnel se multiplexan muchas sesiones. Una conexión de control que funciona sobre TCP administra el establecimiento, la liberación y el mantenimiento de las sesiones y del propio túnel.

Existen dos componentes paralelos de PPTP:

- Una conexión de control entre cada par PAC-PNS que funciona sobre TCP.

- Un túnel IP que funciona entre el mismo par PAC-PNS, que se usa para transportar paquetes PPP con encapsulamiento GRE para las sesiones de usuario que haya entre el par.

3.1.2.2.2 La conexión de control.

Es necesario establecer una **conexión de control** entre el par PNS-PAC antes de que se pueda producir el tunneling PPP entre ellos. La conexión de control es una sesión TCP estándar sobre la cual se pasa la información de control de llamada y de administración PPTP. La sesión TCP para la conexión de control se establece iniciando una conexión TCP con el puerto 1723. la sesión de control está asociada de forma lógica, pero separada, de las sesiones que se están canalizando a través de un túnel PPTP.

El primer conjunto de mensajes de conexión de control se usa para mantener la propia conexión de control.

La conexión de control es iniciada por el PNS o por el PAC una vez éstos establecen la conexión TCP subyacente. La conexión de control es la encargada del establecimiento, la administración y la liberación de la sesión que se transporta a través del túnel. Es la forma de notificar la llamada entrante a un PNS dentro de un PAC asociado, así como la forma de instruir a un PAC para que realice una llamada de acceso telefónico saliente. Una vez que se establece la conexión de control, el PAC o el PNS puede iniciar sesiones requiriendo llamadas salientes o respondiendo a peticiones entrantes.

La propia conexión de control es mantenida por mensajes de eco de actividad.

3.1.2.2.3 El protocolo de túnel.

PPTP requiere el establecimiento de un túnel para cada par PNS-PAC que se comunique. Este túnel se usa para transportar todos los paquetes PPP de sesión de usuario para las sesiones que impliquen un par PNS-PAC determinado.

Los datos de usuario que transporta el protocolo PPTP son paquetes de datos PPP. Los paquetes PPP son transportados entre el PAC y el PNS, encapsulados en paquetes GRE, que a su vez son transportados sobre IP.

Los paquetes PPP encapsulados son, en esencia paquetes de datos PPP que carecen de elementos de entramado específicos de los medios.

La figura 3.9 muestra la estructura general de paquetes que se transmite sobre los túneles que hay entre un PAC y un PNS:

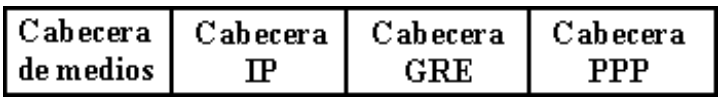


Figura 3.9 La estructura de un paquete con tunneling PPTP.

3.1.2.3 El protocolo de *tunneling* de capa 2.

Dado que L2F y PPTP proporciona una funcionalidad similar, también existe lo que se denomina **Protocolo de tunneling de capa 2 (L2TP)**. Este protocolo está considerado un trabajo en desarrollo que satisface los siguientes requisitos de usuario final:

- Transparencia de sistema final. Ni el sistema final remoto ni los host de sitio doméstico necesitarán software especial para utilizar este servicio de un modo seguro.
- La autenticación viene proporcionada por los protocolos CHAP, PAP, EAP de PPP de acceso telefónico, u otros diálogos (como un intercambio textual sobre V.120 antes de iniciar PPP). Esto incluye soluciones TACACS+ y RADIUS, y soporta también las tarjetas inteligentes y las contraseñas de un solo uso. La autenticación deberá ser administrable por el usuario independientemente del ISP.
- El direccionamiento tendrá que ser tan manipulable como las soluciones de acceso telefónico dedicadas. La dirección deberá ser asignada por el sitio doméstico, y no por el ISP.
- La autorización deberá ser administrada por el sitio doméstico, como en el caso de una solución de acceso telefónico directo.

- La contabilidad deberá ser ejecutada tanto por el ISP (con fines de facturación) como por el usuario (con fines de cobro revertido y de auditoría).

3.1.2.3.1 Panorámica del protocolo.

De una forma similar a PPTP, L2TP define dos entidades:

- **Concentrador de acceso L2TP (LAC).** Este dispositivo está conectado al tejido de una red conmutada (por ejemplo, PSTN o RDSI) o coubicada en un sistema final PPP capaz de soportar L2PT. El LAC sólo tiene que implementar los medios sobre los cuales funcionan L2TP para pasar el tráfico a uno o más LNS. El LAC puede canalizar (tunelar) todos los protocolos que sean transportados dentro de PPP. El LAC es el iniciador de las llamadas salientes y el receptor de las llamadas entrantes.
- **Servidor de red L2TP (LNS).** Este servidor funciona en toda plataforma que soporte PPP. El LNS se encarga del lado del servidor del protocolo L2TP. Dado que L2TP se apoya exclusivamente en el único medio sobre el que llegan los túneles L2TP, el LNS puede tener una sola interfaz LAN o WAN pero ser capaz de terminar las llamadas que lleguen en cualquier intervalo completo del LAC de las interfaces PPP (ASYNC, RDSI síncrono, V.120, etc.). El LNS es el iniciador de las llamadas salientes y el receptor de las entrantes.

Existen dos componentes paralelos de L2TP que funcionan sobre un túnel concreto: los mensajes de control entre cada par LAC-LNS y los paquetes de sobrecarga entre el mismo par LAC-LNS. Estos últimos se usan para transportar los paquetes PPP con encapsulación L2TP para las sesiones de usuario entre el par.

3.1.2.4 Cómo utilizar las tecnologías VPDN.

Aunque el protocolo es estándar, las implementaciones L2F y PPTP van a seguir vigentes en una serie de fabricantes. Efectivamente, las tres tecnologías soportan una funcionalidad similar. Sin embargo, L2TP probablemente tenga más soporte de fabricante, ya

que es estándar. Cuando se decide implementar cualquiera de las tecnologías de red privada de acceso telefónico virtual (VPDN) en un entorno de red corporativa, hay que tener en cuenta las diferencias entre el servicio de acceso a Internet estándar y el servicio de acceso telefónico virtual. Existen diferencias significativas con respecto a la autenticación, autorización, asignación de direcciones y contabilidad.

Los detalles acerca de las diferencias entre estos servicios y los problemas que plantean se describirán en las próximas secciones. Los mecanismos que se usan para el servicio de acceso telefónico virtual están ideados para que coexistan con mecanismos más tradicionales; el POP de un ISP deberá prestar un servicio simultáneo a los clientes ISP y a los clientes de acceso telefónico virtual.

3.1.2.4.1 Autenticación.

En un escenario de acceso telefónico tradicional, un ISP que utiliza un NAS conjuntamente con un servidor de seguridad sigue un proceso de seguridad desafiando al usuario remoto en relación al nombre de usuario y la contraseña. Si el usuario remoto supera esta fase, la fase de autorización podrá comenzar.

En lo que respecta al servicio de acceso telefónico virtual, el ISP persigue la autenticación hasta que se descubra la identidad aparente del usuario. En este punto no se lleva a cabo la interacción de la contraseña.

Tan pronto como se determina el *gateway* corporativo, se inicia una conexión con la información de autenticación recopilada por el ISP. El *gateway* corporativo completa la autenticación o bien aceptando o bien rechazando la conexión. Una vez aceptada la conexión, el *gateway* corporativo podrá proseguir con otra fase de autenticación de la capa PPP. Estas actividades de autenticación adicionales quedan fuera del alcance de la especificación, pero pueden incluir extensiones PPP patentadas o desafíos textuales implementados en una sesión Telnet TCP/IP.

3.1.2.4.2 Autorización.

Cuando se proporciona un servicio de acceso telefónico tradicional, es necesario que el ISP mantenga perfiles de usuario que definan la autorización. Por tanto, un servidor de seguridad podría interactuar con el NAS para proporcionar el uso basado en normas para conectar a los usuarios en base a sus autenticaciones. Estas normas pueden ser desde filtros sencillos origen/destino hasta algoritmos complejos que determinan aplicaciones concretas, el acceso de la hora del día, y una larga lista de destinos permitidos o denegados. Este proceso puede resultar problemático para el ISP, especialmente si está proporcionando acceso a los usuarios remotos en nombres de corporaciones que requieran cambios constantes en estas normas.

En lo que respecta al servicio de acceso telefónico virtual, la tarea de proporcionar una autorización detalla basada en instrucciones de normas se asigna directamente a la empresa del usuario remoto. Al permitir la conectividad de extremo a extremo entre usuarios remotos y el *gateway* corporativo, la autorización puede llevarse a cabo como si los usuarios remotos hubieran llamado directamente a la ubicación corporativa. Esta configuración exonera al ISP de tener que mantener una base de datos grande de perfiles de usuario individuales de muchas empresas distintas.

3.1.2.4.3 Direccionamiento.

En un servicio de Internet tradicional, el usuario acepta que la dirección IP pueda ser asignada dinámicamente a partir de un conjunto de direcciones del proveedor de servicios. Con frecuencia, este modelo implica que los usuarios remotos tienen poco acceso (o ninguno) a los recursos de sus redes corporativas, ya que los Firewalls y las normas de seguridad deniegan a las direcciones IP externas el acceso a la red corporativa.

En lo que respecta al servicio de acceso telefónico virtual, el *gateway* corporativo puede existir por detrás del Firewall corporativo y asignar direcciones que sean internas. Dado que los túneles L2TP operan exclusivamente en la capa de la trama, las normas de tal administración de direcciones serán irrelevantes a la hora de corregir el servicio de acceso telefónico virtual;

para la manipulación de protocolos PPP, es como si el usuario de acceso telefónico se hubiera conectado con el *gateway* corporativo.

3.1.2.4.4 Contabilidad.

El requisito de que tanto el NAS como el *gateway* corporativo proporcionen datos sobre contabilidad puede significar que pueden contar paquetes, octetos y tiempos de inicio y detención de la conexión.

Dado que el acceso telefónico virtual es un servicio de acceso, los intentos de contabilidad de la conexión (concretamente, los intentos fallidos de conexión) tienen mucha importancia. El *gateway* corporativo puede rechazar las nuevas conexiones en base a la información sobre autenticación recopilada por el ISP, con el registro correspondiente. En los casos en que el *gateway* corporativo acepte la conexión y prosiga con la autenticación, el *gateway* corporativo podrá desconectar al cliente. En tales escenarios, la indicación de desconexión del ISP también puede incluir el motivo de la desconexión.

Dado que el *gateway* corporativo puede declinar una conexión en base a la información sobre autenticación recopilada por el ISP, la contabilidad puede distinguir fácilmente entre una serie de intentos fallidos de conexión y una serie de conexiones breves satisfactorias. Como carece de esta utilidad, el *gateway* corporativo deberá siempre aceptar peticiones de conexión e intercambiar numerosos paquetes PPP con el sistema remoto.

3.1.2.4.5 Ventajas del uso de las VPDN.

La tabla 3.2 muestra las ventajas de un servicio de acceso telefónico virtual.

Prestaciones	Ventajas
Soporte multiprotocolo	El ISP puede proporcionar servicios multiprotocolo sobre un *backbone* sólo para IP, utilidades de apoyo, técnicas de administración, personal y formación aplicada de la infraestructura activa.
Autenticación de usuario realizada en la empresa del usuario remoto	ElISP no tiene por qué mantener una base de datos de autenticación de usuarios. El ISP no tiene por qué responder a los cambios organizativos de la ubicación corporativa. Las empresas no tienen por qué “confiar” en los procedimientos de autenticación del ISP.
Autorización de usuario realizada en la empresa del usuario remoto	El ISP no tiene por qué mantener listas de acceso de los distintos usuarios. Administración simplificada de Firewalls. Las empresas pueden implementar sus propias normas de seguridad.
Soporte simultáneo para el acceso local	El ISP puede usar el NAS para el acceso a Internet estándar y el servicio de acceso telefónico virtual, reduciendo los costes, el equipo y los requisitos de infraestructura.
Asignación de direcciones realizada por la empresa del usuario remoto	El ISP no tiene por qué mantener el espacio de direcciones de la empresa dentro de la red ISP. Con esto se minimiza la tabla de enrutamiento del ISP, mejora la escalabilidad y se soporta el uso corporativo de direcciones no registradas en Internet y en las redes públicas.
Independencia de los medios	El ISP puede utilizar cualquier medio (Frame Relay, ATM, punto a punto, X.25) en el *backbone* para soportar el servicio de acceso telefónico virtual.
Túnel dinámico	Los túneles son iniciados en base a la administración L2TP. Esta configuración proporciona una solución escalable, ya que los túneles sólo se inician cuando el tráfico del usuario está activo.

Las sesiones múltiples de usuarios remotos son multiplexadas a través de un solo túnel L2TP	Ésta es una solución escalable, ya que minimiza el número de túneles que tienen que estar abiertos en un momento concreto. Las infraestructuras de *backbone* basada en PVC, como Frame Relay, necesitan un solo PVC entre el NAS y el *gateway* corporativo para administrar sesiones de múltiples usuarios remotos.
La seguridad del túnel mantiene números de clave y secuencia aleatorios	El establecimiento del túnel implica un proceso de autenticación desde el NAS (ISP) hasta el *gateway* corporativo para proteger frente a los ataques. Además, L2TP combate las intrusiones utilizando números de secuencia.
No existen dependencias de protocolo de enrutamiento	Ni el ISP ni el cliente corporativo tienen por qué administrar el dominio de enrutamiento del otro para proporcionar acceso y servicios, liberándolos para que usen el protocolo de enrutamiento que mejor se adapte en cada caso.

Tabla 3.2 Ventajas de los servicios VPDN.

3.1.2.4.6 Consideraciones adicionales.

Con cualquiera de las tecnologías VPDN, la autenticación PPP se usa para autenticar a los usuarios o los dispositivos; los puntos finales del túnel pueden reautenticarse de forma periódica. Sin embargo, no existe protección para los paquetes individuales (de datos o de control) que atraviesen el túnel establecido. Existen trabajos en curso que proponen el uso del modo de transporte IPSec para proteger el tráfico del túnel VPDN. Además, en el caso de los paquetes de datos individuales que recorran el túnel VPDN, los servicios de seguridad (entre los cuales se incluyen la autorización, la integridad, la protección de la reproducción y la confidencialidad), pueden ser proporcionados conjuntamente con L2F, PPTP o L2TP.

3.2 Diseño e implementación de las normas de seguridad corporativas.

El diseño y la implementación de una normas de seguridad corporativas es específicas del sitio. Una vez identificados los activos vitales y analizados los riesgos, es el momento de

diseñar las normas definiendo las directrices y los procedimientos a seguir por el personal corporativo.

Para ser efectivos, los procedimientos deberán ser concisos. Los detalles relativos a la implementación técnica no deberán incluirse, ya que cambian con el tiempo. Si ya existe una infraestructura de red corporativa, podría tener que modificar *ad hoc* los procedimientos de seguridad existentes con el fin de adaptarse más fácilmente a las normas recién creada. El diseño de las normas requiere una planificación meticulosa para garantizar que se incluyen adecuadamente todos los temas relacionados con las seguridad.

Los siguientes puntos son los principales que se deben tener en cuenta antes de diseñar unas normas de seguridad para el entorno de *networking* corporativo:

- Definición de los controles de seguridad física.
- Definición de los controles de seguridad lógica.
- Definición de la integridad del sistema y de los datos.
- Garantía de la confidencialidad de los datos.
- Desarrollo de normas y procedimientos para el equipo encargado de la red corporativa.
- Desarrollo de un aprendizaje adecuado para los usuarios de la red corporativa.

3.2.1 Controles de seguridad física.

Los **controles de seguridad física** son los controles relacionas con las infraestructura física, la seguridad de los dispositivos físicos y el acceso físico. ¿Qué grado de facilidad o dificultad experimentan los intrusos a la hora de obtener acceso físico a los dispositivos más importantes de la infraestructura de red? Si todavía no se ha creado la red corporativa en el sitio, deberá considerar que los controles de seguridad física están en su fase de planificación.

En lo que respecta a las redes existentes, si se crean o adoptan unas normas de seguridad para adaptarse a los entornos cambiantes, podría ser necesario cambiar la infraestructura física o las ubicaciones de algunas de las partes más importantes del equipamiento para garantizar una implementación más simple de las normas de seguridad.

3.2.1.1 Infraestructura de la red física.

La **infraestructura de la red física** abarca la selección del tipo de medio adecuado y la ruta al cableado físico (la topografía de la red). Lo deseable es que ningún intruso sea capaz de escuchar ilegalmente los datos que recorren la red y que todos los sistemas importantes posean un alto grado de disponibilidad.

3.2.1.1.1 Selección de los medios físicos.

Desde un punto de vista de la seguridad, el tipo de cable que se elija en las distintas partes de la red puede depender del grado de importancia de la información que recorre ese cable. Los dos tipos de cable más comunes que se usan en las infraestructuras de *networking* son el par trenzado y la fibra óptica. La fibra óptica se suele utilizar en entornos de ancho de banda alto. A diferencia del par trenzado, la fibra óptica no energía y, por tanto, proporciona un grado muy elevado de seguridad frente a las escuchas ilegales.

A veces es posible detectar los accesos utilizando herramientas que calculan la atenuación física del cable. Normalmente, se utiliza un reflectómetro óptico de dominio temporal (OTDR) para comprobar el cable de fibra óptica. Este dispositivo se suele usar para calcular la atenuación de la señal y la longitud de una base de cable instalada; sin embargo, a veces, también pueden detectar los acceso ilegales.

Una de las cosas que el escuchador ilegal necesita a la hora de acceder a un cable óptico es un **divisor óptico**. La inserción de un divisor óptico en un cable óptico permite realizar el acceso, pero también afecta al nivel de señal del medio. Este nivel puede ser calculado. Si hay un nivel de señal óptica de prueba de características en varios puntos de la topología de una red de medio óptico, se podrá observar cualquier acceso óptico convencional que se inserte en la red. La figura 3.10 muestra un rastro de cable de fibra óptica OTDR inicial entre 2 edificios.

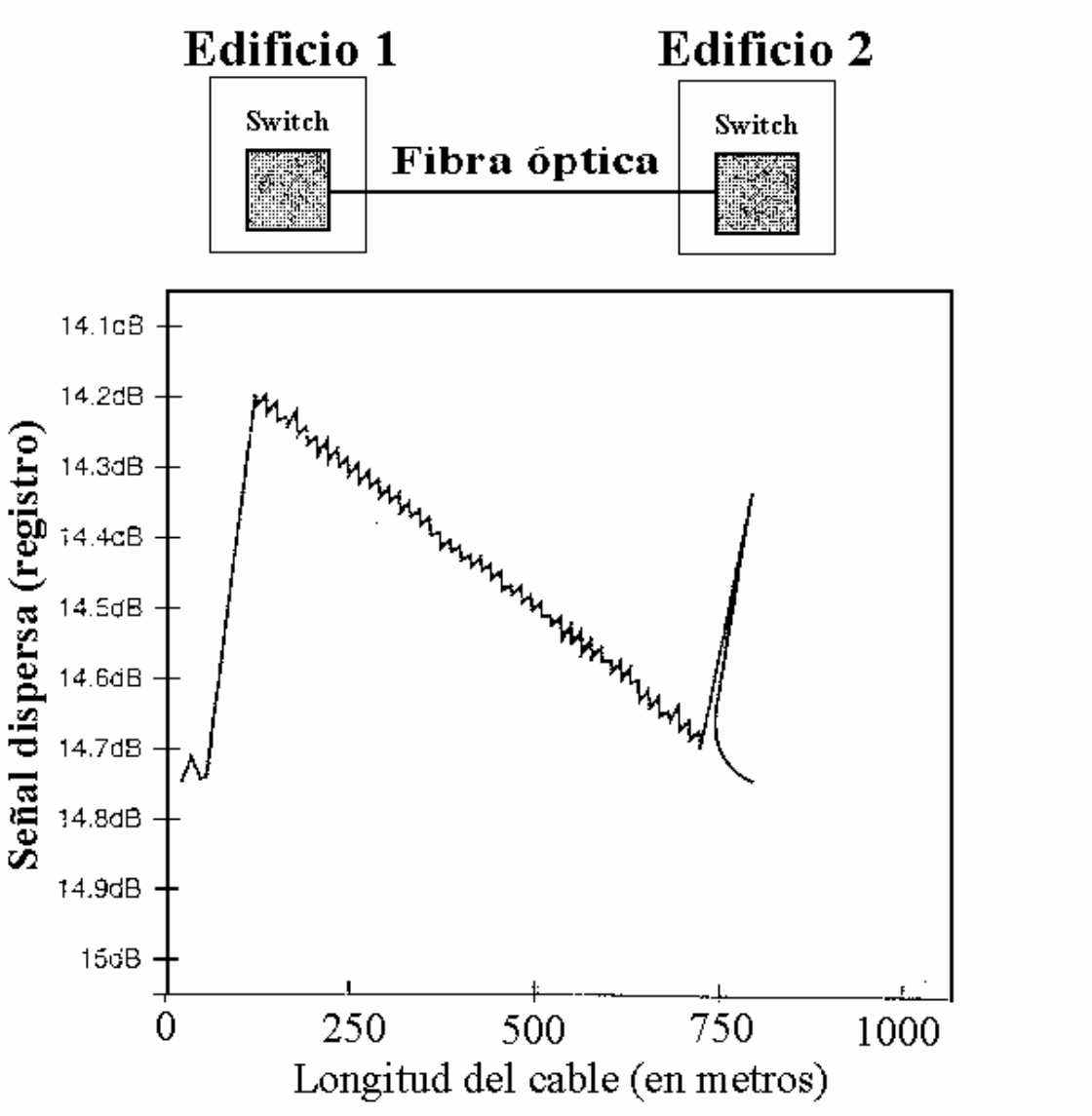


Figura 3.10 Rastro de cable de fibra óptica OTDR

La figura 3.11 muestra el rastro de fibra óptica que se toma después de que se haya insertado un divisor óptico en la longitud del cable de fibra óptica.

Aunque estos tipos de rastros pueden ser una indicación de la posible existencia de un acceso, son más útiles para la detección de problemas de degradación del cable.

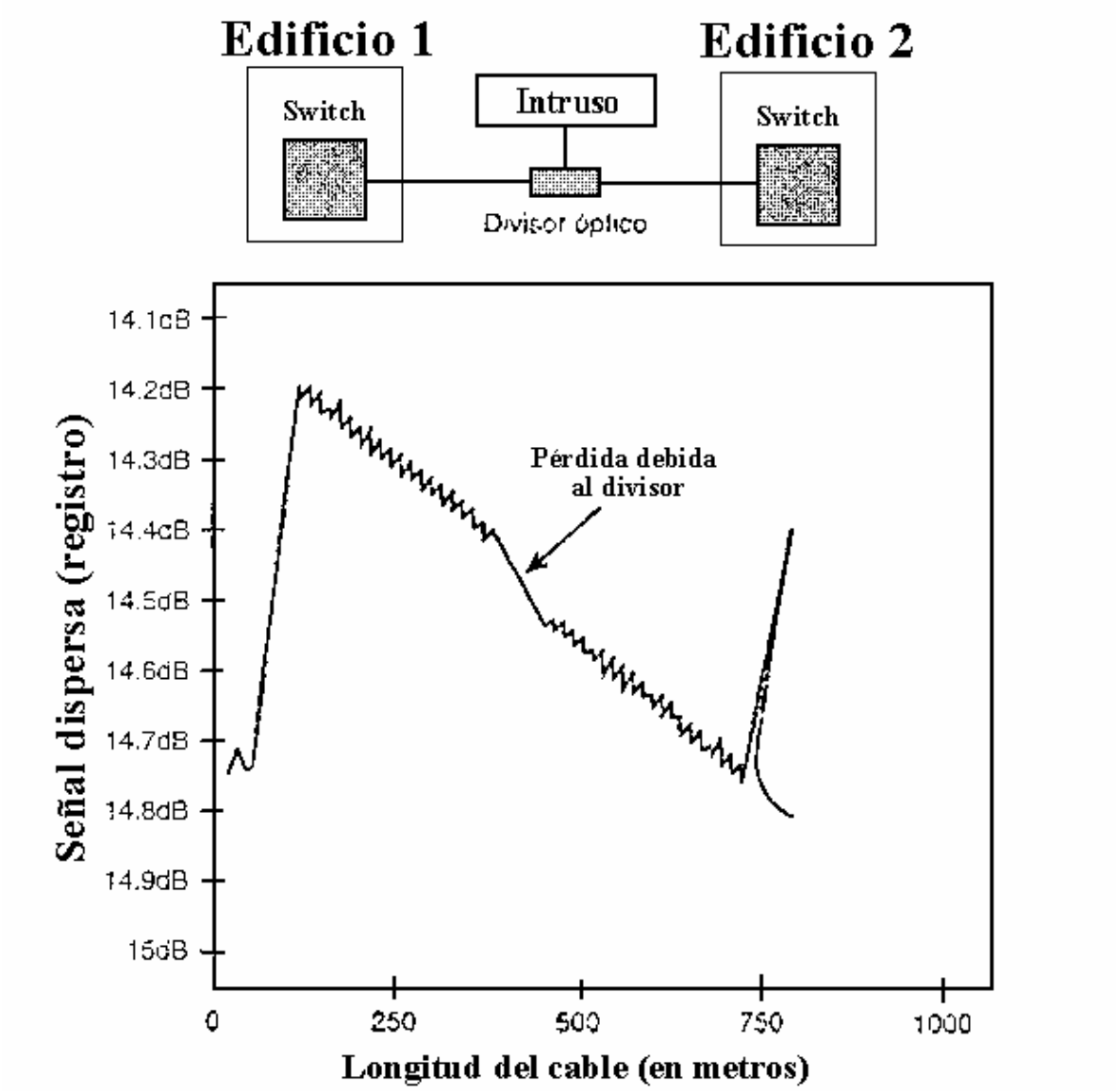


Figura 3.11 El cálculo ODTR una vez insertado el divisor de fibra óptica.

3.2.1.1.2 Topografía de red.

La ruta física de los medios, que también se conocen como **topografía de red**, constituye una preocupación para la disponibilidad de la red y los dispositivos que tenga conectados. Alude a la fiabilidad y la seguridad de la infraestructura. Es importante que haya un sistema de cableado estructurado que minimice el riesgo de tiempo de inactividad.

Imagínese un entorno de campus grande con múltiples edificios. Si la topografía de infraestructura del backbone de la red no es un verdadera red en estrella con conductos comunes en la base de la estrella, alguien provisto de una retroexcavadora podría destruir grandes partes de la red (véase figura 3.12). Sin embargo, si se colocan rutas físicas alternativas (es decir, si se crea una verdadera red en estrella), sólo quedarían inaccesibles las partes más pequeñas de la red si fallara el cable físico (véase figura 3.13).

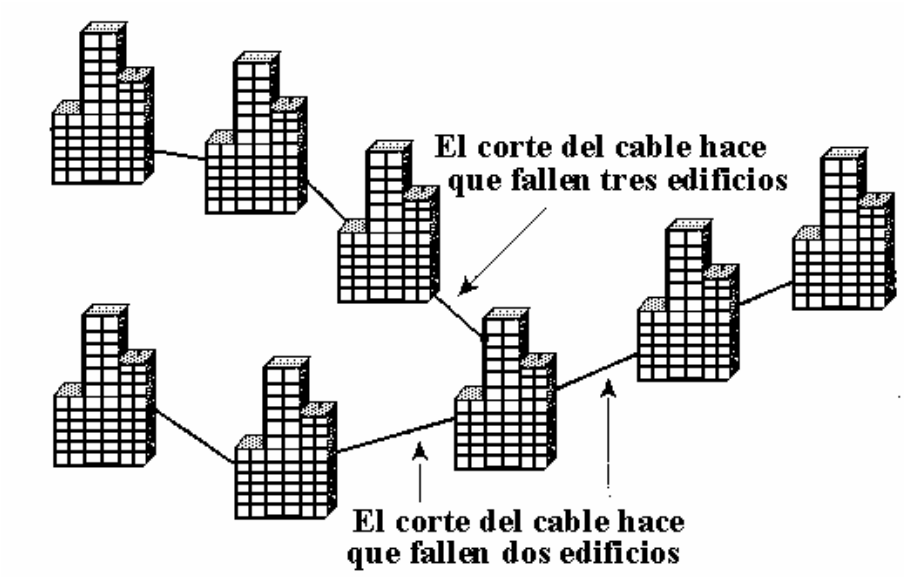


Figura 3.12 Una topografía física de ejemplo.

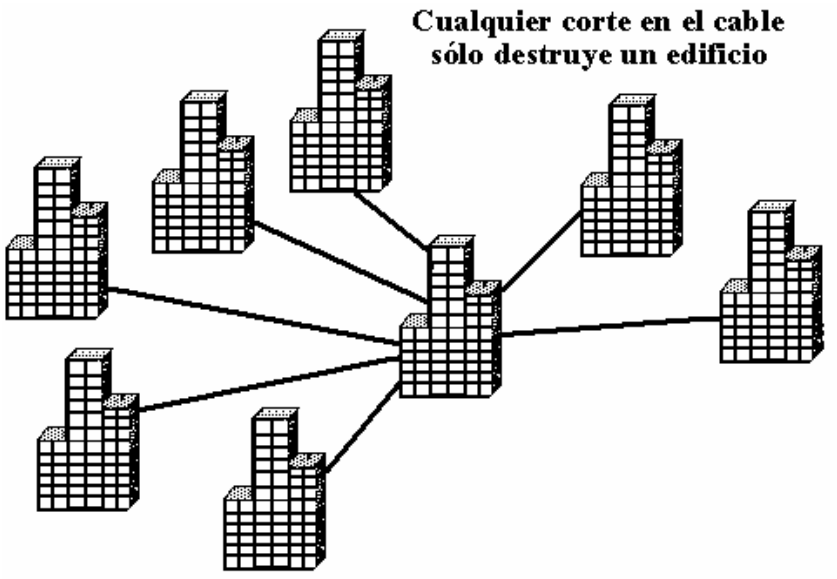


Figura 3.13 Una verdadera topografía física en estrella.

3.2.1.2 Seguridad de los dispositivos físicos.

La **seguridad de los dispositivos físicos** se suele subestimar. Los intrusos con suficiente motivación pensarán que pueden obtener lo que desean. La seguridad de los dispositivos físicos incluye la identificación de la ubicación de los dispositivos, la limitación del acceso físico y la instauración de las protecciones del entrono adecuadas.

3.2.1.2.1 Ubicación física.

La ubicación de los recursos vitales de la red es de capital importancia. El equipo de la infraestructura de red deberá estar físicamente ubicado en áreas de acceso restringido, a fin de eliminar la posibilidad de que haya un acceso no autorizado imputable a la proximidad física.

3.2.1.2.2 Acceso físico.

¿Quién tiene acceso a los armarios de conexión y a las ubicaciones restringidas? Los requisitos de acceso físico a las áreas controladas son determinados en gran medida por los resultados del análisis de riesgos o una encuesta de seguridad. Conviene restringir el acceso físico a los armarios de conexión y a las ubicaciones más importantes del equipo de la infraestructura de red. El acceso a estas áreas no deberá estar permitido a menos que la persona éste específicamente autorizada o requiera acceso para llevar a acabo sus tareas.

Parte de las normas de seguridad físicas deberán prever la contratación de personal de mantenimiento o que otras personas que no estén autorizadas a acceder libremente sean escoltadas por una persona autorizada o que firmen antes de acceder al área controlada.

3.2.1.2.3 Protecciones del entorno.

Es preciso instalar e implementar protecciones del entorno apropiadas con el fin de proteger los recursos de red vitales. La importancia del sistema determina si la seguridad es o no “adecuada”. Cuanto más importante sea un sistema, más protecciones deberán implantarse para asegurar que el recurso está disponible a cualquier coste. Como mínimo, deberá considerar las siguientes protecciones del entorno:

- Prevención, detección, supresión y protección contra incendios.
- Prevención, detección y control de inundaciones.
- Protección del suministro eléctrico.
- Control de la temperatura.
- Control de la humedad.
- Protección frente a desastres naturales provocados por terremotos, rayos, tormentas, etc.
- Buenos procedimientos de limpieza para la protección contra la suciedad y el polvo.

3.2.2 Infraestructura e integridad de los datos.

En la infraestructura de red, conviene asegurarse de que todo el tráfico de la red es válido. El **tráfico válido** es el que puede clasificarse como tráfico de red esperado, como el siguiente:

- Servicios soportados.
- Tráfico legal.
- Datos que no han sido alterados.

Los *Firewalls* controlan el flujo de tráfico entre redes y se suelen usar para controlar el flujo de los servicios de red soportados, la autenticación de los datos en la infraestructura de red proporciona una seguridad razonable frente a los paquetes alterados. La colocación de protecciones para implementar métodos cuyo fin sea el de impedir ataques puede evitar el tráfico ilegal.

Para mayor información respecto al trabajo de los *Firewalls* diríjase al punto 2.4 de la sección de firewalls.

3.2.2.1 Servicios de red.

La elección de que servicios y protocolos se van a soportar puede resultar una tarea desalentadora. Una solución sencilla pasa a permitir todo y denegar lo necesario. Esta política es fácil de implementar, ya que basta con que se activen los servicios y que se permita que todos los protocolos crucen los límites de la red. Cuando se pongan de manifiesto agujeros en la seguridad, deberá restringir o parchar tales servicios tanto a nivel de *host* como nivel de red.

Esta solución es muy sencilla, pero también es vulnerable a múltiples ataques. Una solución más segura consiste en denegar todo y permitir lo necesario. Este modelo suele ser más seguro que el anterior, pero requiere más trabajo para ser implementado con éxito. También requiere entender mejor los servicios. Si sólo permite los servicios conocidos, proporcionará un análisis más óptimo de un servicio o protocolo concretos y podrá diseñar un mecanismo de seguridad acorde con el nivel de seguridad del sitio.

En la mayoría de los casos, los servicios proporcionados por un sitio tendrán niveles de necesidad de acceso y modelos de confianza distintos. Los servicios esenciales para la seguridad o el funcionamiento correcto de un sitio funcionan mejor en un equipo dedicado con un acceso muy limitado.

Los servicios proporcionados en el mismo equipo pueden interactuar de forma catastrófica. Por ejemplo, permitir el FTP anónimo en el mismo equipo que el servidor WWW podría dar vía libre a que un intruso colocara un archivo en el área del FTP anónimo y hacer que el servidor http lo ejecutara. En la medida de lo posible, cada servicio deberá ejecutarse en un equipo distinto. Esta medida ayuda a aislar los intrusos y a limitar el daño potencial.

3.2.2.2 Datos autenticados.

Para garantizar una cantidad razonable de integridad de los datos, deberá autenticar la mayor parte del tráfico que atraviesa la red. En aras de la integridad de la infraestructura de red, el tráfico que sea específico para el funcionamiento de una infraestructura segura (como las actualizaciones de enrutamiento) también deberá ser autenticado.

3.2.2.2.1 Actualizaciones de enrutamiento.

Si no autentica las actualizaciones de enrutamiento, las actualizaciones d enrutamiento no autorizadas o deliberadamente maliciosas podrán poner en peligro la seguridad del tráfico de red. Esto puede ocurrir si una parte no amistosa desvía o analiza el tráfico de la red. Por ejemplo, un *router* no autorizado podría enviar una actualización de enrutamiento ficticia para convencer al *router* de que enviará tráfico a un destino incorrecto. Este tráfico desviado podría ser analizado para conocer la información confidencial acerca de su empresa, o simplemente detraer la capacidad de la empresa para comunicarse eficientemente por medio de la red.

Las **sumas de comprobación** protegen contra la inyección de paquetes espúreos, aunque el intruso tenga acceso directo a la red física. Combinado con un número de secuencia u otro identificador único, una suma de comprobación también puede protegerle frente a **ataques de reproducción**, mientras que una actualización de enrutamiento antigua podría ser retransmitida por un intruso o un *router* cuyo comportamiento fuera erróneo. La seguridad máxima se proporciona por medio del cifrado completo de las actualizaciones de enrutamiento secuenciadas o identificadas de forma exclusiva. Esta solución impide que un intruso determine la topología de la red. La desventaja del cifrado es la estructura necesaria para el procesamiento de las actualizaciones.

3.2.2.3 Frenos más comunes a los ataques.

La mayoría de los ataques de *networking* más comunes pueden resultar más difíciles de ejecutar con los productos tipo *Firewalls*.

3.2.2.3.1 Ataques contra los hosts aleatorios protegidos por el Firewalls.

En muchos casos, los ataques contra *hosts* aleatorios protegidos por el *Firewalls* pueden ser completamente evitados, dependiendo de cómo haya configurado el *Firewall*. La configuración más conservadora permite que el tráfico no alcance los *hosts* internos, a menos

que éstos inicien una conexión saliente de algún tipo. Si lo hace de este modo, podrá evitar una serie de ataques.

3.2.2.3.2 Ataques contra servicios expuestos.

Los servidores web, los servidores de correo, los servidores FTP, etc., protegidos por el *firewall* presentan el máximo riesgo, puesto que cualquiera de los hosts de la red puede enviarles ciertos tipos de paquetes que cualquier momento. Lo normal es colocar estos servicios expuestos en una zona desmilitarizada (DMZ) de la red, en vez de en la red interna. También deberá asegurarse de que el propio servidor está protegido. Los *firewalls* hacen varias cosas para proteger los servicios expuestos, pero sigue siendo aquí donde se sitúan los riesgos más elevados.

3.2.2.3.3 Ataques contra los *hosts* cliente internos.

Si los *host* cliente internos han formado conexiones salientes, se estarán exponiendo a cierto tráfico de retorno. Por regla general, los ataques contra clientes internos sólo pueden ser dirigidos por el servidor con el que se haya conectado el cliente (incluyendo alguien que se hace pasar por ese servidor por medio del falseamiento IP). Para suplantar al servidor al servidor, el atacante tiene que saber con qué servidor se ha conectado el cliente.

En un ataque concreto, la protección suele ser completa para *hosts* que no estén comunicándose activamente con la red, parcial para *hosts* que se estén comunicando activamente con la red, y mínima para servicios expuestos.

Sin embargo, la seguridad depende de cómo esté configurado el sistema.

3.2.2.3.4 Ataques de falseamiento.

Ningún producto, aunque esté configurado correctamente, podrá protegerle completamente frente a los *hosts* externos si se presuponen las direcciones de los *hosts*

internos. No hay forma de que un *firewall*, o cualquier otro dispositivo, pueda determinar si la dirección de origen de un paquete IP no autenticado es válida (aparte de examinar la interfaz a la que haya llegado ese paquete). Por tanto, ningún *firewall* podrá protegerle frente al caso general de un *host* externo que engaña a otro. Si hay algo que tiene que confiar en la dirección de un *host* externo, deberá controlar la ruta de red completa a ese *host*, y no un solo punto de acceso.

Cualquier producto de internetworking puede hacer que los ataques de falseamiento sean más difíciles de realizar haciendo que sea más difícil para el atacante saber qué nodos son los más ventajosos para el falseamiento en cada momento. Esta protección no es completa; un atacante que pueda husmear la red en sus puntos estratégicos, o que pueda aprovecharse de los patrones de tráfico, podrá sortear el producto de internetworking.

Las listas siguientes proporcionan un ejemplo de la infraestructura y la sección de integridad de los datos de las normas de seguridad de una universidad.

3.2.2.3.4.1 Seguridad de la infraestructura.

- El acceso a los puertos LAN y a las interfaces del router quedará desactivado cuando no se use.
- La funcionalidad del firewall se utilizará en los **puntos de entrada**; éstos se definen como las conexiones que proporcionan acceso desde cualquier parte del campus principal de la universidad.
- Sólo se soportarán los servicios de red que sean necesarios. Estos servicios serán definidos por el grupo de dirección de operaciones de red.

3.2.2.3.4.2 Integridad de los datos.

- El software no relacionados con el trabajo no se usará en ningún computador que forme parte de la infraestructura de red y los servicios más importantes.
- Todas las imágenes de software y sistemas operativos deberán usar un esquema de verificación de suma de comprobación antes de que la instalación confirme su integridad.
- Todas las actualizaciones de enrutamiento y actualizaciones VLAN deberán ser autenticadas entre los dispositivos de emisión y recepción.

3.3 Confidencialidad en Redes.

a) Cifrado de Enlaces de datos (link encrypton): Se cifran todos los datos de una ruta realizado por el proveedor de servicios de comunicación.

   Ventajas: transparente para los usuarios, permite protegerse bien contra ataques de intercepción y análisis de tráfico.

   Desventajas: los paquetes deben ser varias veces cifrados y descifrados para permitir su encaminamiento (routers intermedios). Si un nodo se compromete, se compromete todo el tráfico que fluye por el nodo. El usuario individual pierde el control sobre los algoritmos usados.

b) Cifrado Terminal (end-to-end): El cifrado y descifrado se realiza en los puntos finales de la comunicación y es usado por las organizaciones que son usuarios finales.
   Ventajas: Se evita comprometer la información debido a nodos intermediarios no confiables.
   Desventajas: La información de encaminamiento permanece visible (cabeceras).

3.3.1 Enfoques de Seguridad TCP/IP.

Seguridad IP: Se provee al nivel de protocolo de red, siendo transparente para usuarios finales y aplicaciones.

- Es solución de propósitos generales
- IPSec (IP Security) sigue este enfoque

Seguridad de transporte: Se implementa justo sobre TCP, siendo solución de propósito general relativo.

- Esquemas mas conocidos son SSL(Secure Socket Layer) y TLS (Transport Layer Security), donde TLS está basado en SSL
- Existen dos alternativas de implementación:

1.- Integrado al protocolo inferior y transparente para las aplicaciones.

2.- Incluido en paquetes de software como Netscape y Explorer.

Seguridad Específica a la Aplicación: Seguridad incluida en una aplicación en particular.

Ventajas: Los servicios están hechos a la medida de acuerdo a necesidades de la aplicación.

Desventajas: El servicio no puede ser compartido entre aplicaciones

3.3.2 Protocolos de seguridad de la capa de transporte.

3.3.2.1 IPSec.

Se enfoca a tres áreas funcionales:

- Autenticación: Asegura que un paquete recibido fue transmitido por la parte que se identifica como origen en la cabecera del paquete y que no ha sido alterado durante su transmisión.

- Confidencialidad: Este habilita a los nodos para cifrar paquetes, enviando que éstos sean leídos por terceros.
- Gestión de claves: Permite el intercambio seguro de claves.

Aplicaciones de IPSec:

1.- Asegura conectividad de oficinas o sucursales a través de Internet a través de VPN.

2.- Asegura acceso remoto a través de Internet(a través de ISP) a la red de la empresa.

3.- IPSec en un firewall o un router asegura el tráfico, sin incluir en un overhead extra dentro de la red.

4.- IPSec en un firewall es resistente a bypass si el firewall IP es único punto externo de conexión.

5.- IPSec esta bajo la capa de transporte, siendo transparente su uso para aplicaciones y usuarios.

6.- Permite proveer seguridad a usuarios individuales

7.- Permite asegurar arquitectura de routing.

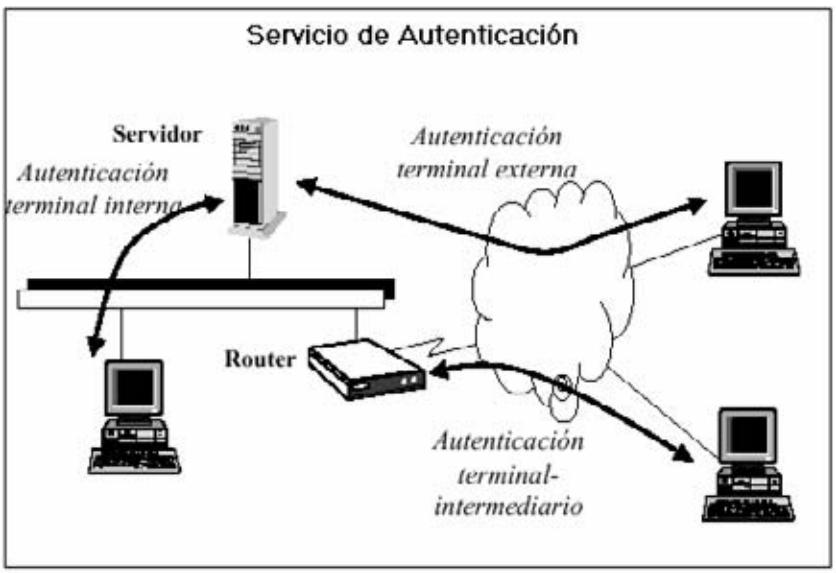


Figura 3.14 Servicio de Autenticación.

3.3.2.2 Protocolo SSH.

SSH (o Secure Shell) es un protocolo para crear conexiones seguras entre dos sistemas usando una arquitectura cliente/servidor.

El protocolo SSH proporciona los siguientes tipos de protección:

- Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
- El cliente transmite su información de autenticación al servidor usando una encriptación robusta de 128 bits.
- Todos los datos enviados y recibidos durante la conexión se transfieren por medio de encriptación de 128 bits, lo cual los hacen extremamente difícil de descifrar y leer.

Ya que el protocolo SSH encripta todo lo que envía y recibe, se puede usar para asegurar protocolos inseguros. El servidor SSH puede convertirse en un conducto para convertir en seguros los protocolos inseguros mediante el uso de una técnica llamada reenvío por puerto, como por ejemplo POP, incrementando la seguridad del sistema en general y de los datos.

3.3.2.2.1 Capa de transporte.

El papel principal de la capa de transporte es el de facilitar una comunicación segura entre dos hosts a la hora de y después de la autenticación. Normalmente ejecutado a través de TCP/IP, la capa de transporte logra hacer esto ocupándose de la encriptación y descifrado de datos, verificando que el servidor sea el equipo correcto para la autenticación, y proporcionando protección a la integridad de los paquetes de datos al momento de ser enviados y recibidos. Además, la capa de transporte también puede proveer la compresión de los datos, acelerando así la transmisión de la información.

Al contactar un cliente a un servidor por medio del protocolo SSH, se negocian varios puntos importantes para que ambos sistemas puedan construir la capa de transporte correctamente:

- Intercambio de claves
- El algoritmo de la clave pública que hay que usar
- El algoritmo de la encriptación simétrica que hay que usar
- El algoritmo de la autenticación de mensajes que hay que usar
- El algoritmo de hash que hay que usar

3.3.2.2.2 Autenticación.

Cuando la capa de transporte haya construido un túnel seguro para transmitir información entre los dos sistemas, el servidor le dirá al cliente de los diferentes métodos de autenticación soportados, como el uso de firmas privadas codificadas con claves o la inserción de una contraseña. El cliente entonces intentará autenticarse ante el servidor mediante el uso de cualquiera de los métodos soportados.

Ya que los servidores se pueden configurar para que concedan varios tipos de autenticación, este método proporciona a cada parte un control óptimo. Luego el servidor podrá decidir qué métodos de encriptación soportará basado en su pauta de seguridad, y el cliente puede elegir el orden en que intentará utilizar los métodos de autenticación entre las opciones a disposición. Gracias a la naturaleza segura de la capa de transporte de SSH, hasta métodos de autenticación que parecen inseguros, como la autenticación basada en el host, son en realidad seguros.

La mayoría de los usuarios que requieren de una shell segura se autenticarán por medio de una contraseña. En contraste con otros esquemas de seguridad por medio de autenticación, la contraseña se transmite al servidor en texto sin cifrar. Sin embargo, ya que la contraseña entera va cifrada al pasar por la capa de transporte, puede ser enviada a través de cualquier red sin problemas de seguridad.

3.3.2.3 Protocolo SNMP.

Protocolo Simple de Gestión de Red. Este protocolo ha sufrido varios cambios evolutivos ya que como las redes de datos se van haciendo cada ves más complejas; entonces se ha tenido que ir mejorando deficiencias funcionales y herramientas de seguridad principalmente para dar los pasos desde la versión 1 hasta la versión 3.

Es una herramienta sencilla para la gestión de red, esta define una base de información y gestión (MIB) limitada y fácil de implementar de variables escalares y tabla de dos dimensiones, y define un protocolo para permitir a un gestor obtener y establecer variables MIB y para permitir a una agente emitir notificaciones no solicitadas llamadas interrupciones traps.

La esencia de SNMPv2 es un protocolo que se utiliza para intercambiar información de gestión. Cada encargado en un sistema de gestión de red mantiene una base de datos local de la información relevante de gestión de red, conocida como base de información de gestión.

SNMPv2 no proporciona gestión de red, en lugar de eso SNMPv2 proporciona un marco de trabajo en el que se pueden construir aplicaciones de gestión de red.

El estándar SNMPv2 define la estructura de esta información y los tipos de datos permitidos; esta definición se conoce como estructura de información de gestión (SMI, Structure of Management Information), el estándar también contribuye varias MIB que son generalmente útiles para la gestión de red.

Al menos un sistema de la configuración debe de ser responsable de la gestión de red. Es aquí donde se debe instalar cualquier aplicación de gestión de red. Es recomendable que exista más de una estación de gestión, para que proporcione redundancia o divida el trabajo en una red grande. La mayoría del resto de los sistemas actúa con un papel de agente. Un agente recoge la información localmente y la almacena para accesos posteriores de un gestor, la información incluye datos sobre el mismo sistema y también pueden incluir información del tráfico de la red o a redes a las que está conectado con el agente.

Ejemplo de una infraestructura de gestión de red con SNMPv2.

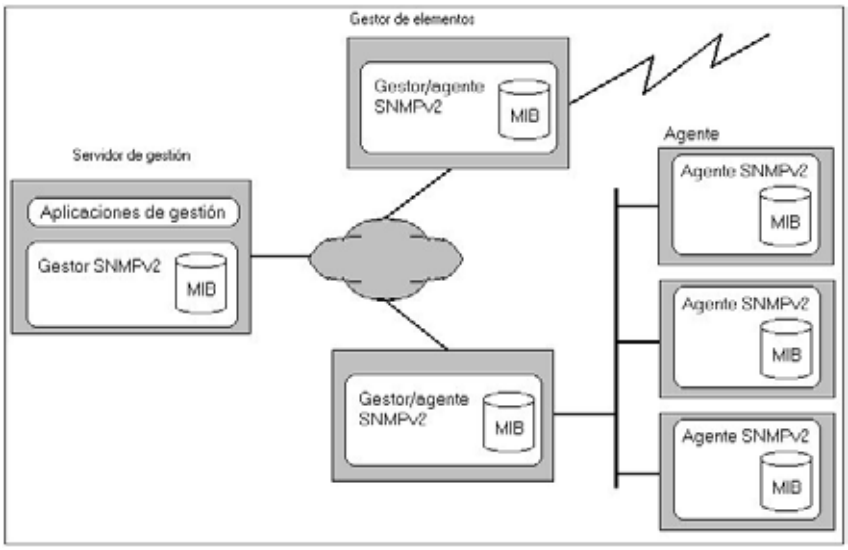


Figura 3.15 Configuración gestionada por SNMPv2.

3.3.2.4 Protocolo sencillo de gestión de red versión 3 (SNMPv3)

SNMPv3 proporciona tres servicios importantes: autentificación, privacidad y control de acceso. Los dos primeros forman parte del modelo de Seguridad Basada en Usuarios (USM, user-based security) y el último se define en el Modelo de Control de Acceso Basado en Consideraciones (VACM). Los servicios de seguridad están gobernados por la identidad del usuario que solicita el servicio; esta identidad se expresa como un director, que puede ser un individuo o una aplicación o un grupo de individuos o aplicaciones.

3.3.2.5 Cronología de la evolución de seguridad en SNMP.

SNMPv1 constituye la primera definición e implementación del protocolo SNMP(año 1988), estando descrito en las RFC 1155, 1157 y 1212 del IETF (*Internet Engineering Task Force).* El rápido crecimiento de SNMP dio paso a sus debilidades, principalmente su imposibilidad de especificar de una forma sencilla la transferencia de grandes bloques de datos y la ausencia de mecanismos de seguridad.

SNMPv2 apareció en 1993, estando definido en las RFC 1441-1452. SNMPv1 y SNMPv2 tienen muchas características en común, siendo la principal mejora la introducción de tres nuevas

operaciones de protocolo: *GetBulk* para que el gestor recupere de una forma eficiente grandes bloques de datos, tales como las columnas de una tabla; *Inform* para que un agente envíe información espontánea al gestor y reciba una confirmación; y *Report* para que el agente envíe de forma espontánea excepciones y errores de protocolo. SNMPv2 también incorpora un conjunto mayor de códigos de error y más colecciones de datos. En 1995 apareció una revisión de SNMPv2, denominada SNMPv2c y descrita en las RFC 1901-1910, añadiendo como mejoras una configuración más sencilla y una mayor modularidad; pero manteniendo el sencillo e inseguro mecanismo de autentificación de SNMPv1 y SNMPv2.

SNMPv3 refuerza las prestaciones de seguridad, incluyendo autentificación, privacidad y control de acceso; y de administración de protocolo, con una mayor modularidad y la posibilidad de configuración remota. SNMPv3 apareció en 1997, estando descrito en las RFC 1902-1908 y 2271-2275. Cabe destacar que SNMPv3 no se trata de un estándar que reemplaza a SNMPv1 y/o SNMPv2, sino que define una serie de capacidades adicionales de seguridad y administración a ser utilizadas en conjunción con SNMPv2 o SNMPv1. El modelo de seguridad basado en usuario o USM (*User-Based Security Model*) proporciona los servicios de autentificación y privacidad en SNMPv3. El mecanismo de autentificación en USM asegura que un mensaje recibido fue, de hecho, trasmitido por la entidad indicada en el campo correspondiente a la fuente en la cabecera del mensaje; y además, que el mensaje no fue alterado durante su tránsito y que no fue artificialmente retardado o repetido. Para conseguir la autentificación, el gestor y el agente que desean comunicarse deben compartir la misma clave de autentificación secreta configurada previamente fuera de SNMPv3 (no es almacenada en la MIB y no es accesible mediante SNMP). El protocolo de autentificación utilizado puede ser el HMAC-MD5-96 o el HMAC-SHA-96. Para asegurarse de que los mensajes llegan dentro de una ventana temporal razonable que descarte el posible retardo de mensajes y el ataque mediante mensajes repetidos, se utilizan mecanismos de sincronización entre emisor y receptor y el chequeo de la ventana temporal constituida por el momento de emisión del mensaje y su momento de recepción. Por otro lado, la facilidad de privacidad de USM posibilita a los gestores y a los agentes encriptar mensajes para prevenir que sean analizados por intrusos.

CAPITULO IV
Firewall PIX de CISCO Secure.

4.1 Tipo de Tecnología de Firewall.

La tecnología firewall existe desde el momento que surgió la necesidad de los firewalls en el sector de las computadoras. Dentro de esto a los firewalls los podemos definir por su pertenencia a una de estas tres categorías:

4.1.1 Filtro de Paquete.

Analiza el tráfico en la capa de transporte o en la capa de red de la pila de protocolo TCP/IP, siempre y cuando los datos que fluyan por la red estén basados en TCP/IP estándar. La información analizada por un filtro de paquete es la información estática de la cabecera del paquete.

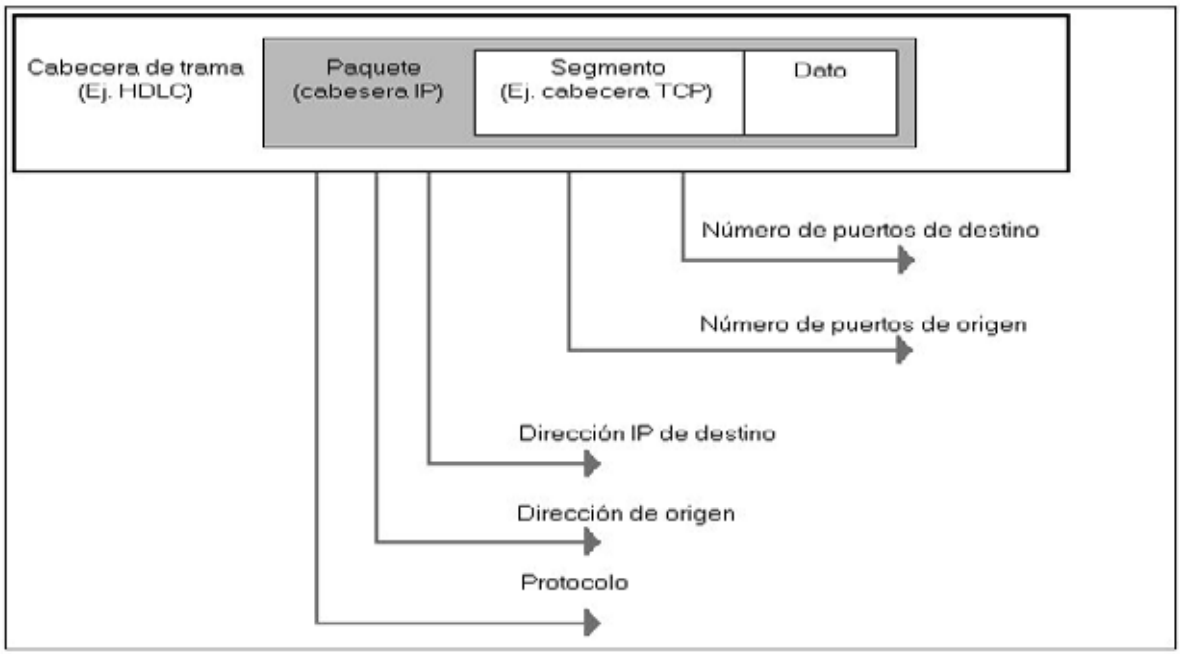


Figura 4.1 Comprobación de paquetes con listas de acceso.

Un filtro de paquete crea reglas que utilizan el criterio de origen y/o destino específico. Como se ilustra en la figura 4.1 un filtro de paquete puede autorizar o denegar información en base a uno o más de los siguientes criterios:

Dirección IP de origen; Dirección IP de destino; Protocolos; Puerto de origen; Puerto de destino.

Un aspecto importante de un filtro de paquetes con estado es que no guarda información con estados, ya que cuando el filtro de paquetes ha procesado el paquete, no guarda información a cerca del paquete concreto.

4.1.2 Filtro Proxy: Es un dispositivo firewall que examina los paquetes en las capas superiores del modelo OSI (de la capa 4 a la 7). Al examinar detalladamente la sesión refuerza mucho un filtro Proxy, pero el rendimiento extremo a extremo se reciente.

Una forma de funcionamiento de un firewall de filtro Proxy consiste en exigir que el usuario del interior o área de confianza del firewall construya una sesión en el propio firewall, el usuario debe autenticarse. En base al ID de usuario y la contraseña, al usuario se le permite tener un acceso específico al exterior y se construyen dos sesiones únicas (una desde el usuario al Proxy y otra desde el Proxy hasta el destino).

Problemas del filtro Proxy:

- Un filtro Proxy crea un único punto de fallo, lo que significa que si se pone en peligro el acceso al firewall, también se pondrá en peligro toda la red.
- Un firewall Proxy funciona mas lentamente bajo tensión.
- Un firewall Proxy generalmente se construye sobre un sistema operativo conocido de propósitos generales , ya que tiene que usar algunos de los servicios del SO para llevar a cabo los procesos del Proxy. Esto da origen a problemas de estructura y de menor rendimiento y vulnerabilidad del SO a atacar, ya que es bien conocido.

4.1.3 Filtros de Paquetes con Estados: Combina lo mejor de las tecnologías de filtrado de paquetes y de las de filtrado de proxies. Un filtro de paquete con estado mantiene una información completa del estado de sesión para cada sesión que se construya en el firewall. Cada vez que se establece una conexión IP para una conexión entrante o saliente, la información queda registrada en una tabla de flujo de sesión con estado. El filtrado de paquete con estado es el método que utilizan los firewall de alto desempeño como los PIX de Cisco.

La tabla de flujo de sesión con estado contiene las direcciones de origen y destino, los números de puertos, información de las secuencias TCP e indicadores adicionales para cada conexión TCP/UDP que esté asociada con una determinada sesión. Cuando se inicia una sesión a través del firewall, se crea un objeto de conexión y, consecuentemente se comparan todos los paquetes entrantes y salientes con los flujos de sesión de la tabla de flujo de sesión con estado. Sólo si hay una conexión apropiada que valide el paso se autoriza el paso de los datos a través del firewall.

Algunos beneficios del filtrado de paquetes con estado:

- Funciona con paquetes individuales y los compara con las conexiones establecidas.
- Funciona a un nivel de rendimiento superior que el de filtrado de paquetes o que el filtro Proxy.
- Graba los datos en una tabla por cada transacción con conexión o sin conexión que se produzca. Esta tabla sirve como punto de referencia para determinar si los paquetes pertenecen a una conexión existente o proceden de un origen no autorizado.

4.1.4 La lógica de lo firewall PIX.

PIX es un firewall de hardware / software dedicado que proporciona una seguridad de alto nivel y que tiene menos repercusión sobre el rendimiento de red de otros firewalls. Está considerado un sistema híbrido, ya que incorpora tecnologías de filtrado de paquetes, filtrado de proxies y filtrado de paquetes con estado.

El firewall PIX Cisco Secure ofrece las siguientes ventajas y características:

- **Sistema integrado seguro y en tiempo real.** A diferencia de los filtros de proxy normales, que lleva a cabo mucho procesamiento en cada paquete de datos, el firewall PIX utiliza un sistema integrado seguro y en tiempo real que mejora la seguridad de la red. El entorno operativo PIX es un entorno patentado y bien protegido que no está expuesto a ninguna de las vulnerabilidades de sistema operativo conocidas.

- **Algoritmo de seguridad adaptable (ASA).** Implementa el control de la conexión con estado a través del firewall PIX de Cisco. Este filtro de paquetes con estado es un método seguro de análisis de paquetes de datos, que coloca en una tabla mucha información acerca de un paquete de datos. Para que sea considerado “establecido” (la respuesta a la solicitud), la información de ese paquete deberá coincidir con la información de la tabla.

- **Proxy por método de corte.** Un método de autenticación basado en el usuario para conexiones entrantes y salientes.

- **Recuperación ante fallos con estado/reserva en caliente.** El firewall PIX de Cisco le permite configurar dos unidades de firewall PIX de Cisco en una topología completamente redundante

El núcleo del firewall PIX es el ASA. El ASA es la parte del sistema operativo patentado que habilita la inspección de paquetes con estado y la retención del flujo de sesión, y que mantiene los perímetros seguros entre las redes que controla el firewall. El diseño ASA con estado, orientado a la conexión, crea flujos de sesión basados en direcciones de origen y destino.

Cada vez que se establece una conexión TCP para las conexiones entrantes y salientes a través del firewall PIX, la información sobre la conexión queda registrada en una tabla de flujo de sesión con estado. Para que se establezca una sesión, la información sobre la conexión deberá coincidir con la información almacenada en la tabla. Con esta metodología, los filtros con estado actúan sobre las conexiones y no sobre los paquetes haciendo que sea un método de seguridad más estricto.

Utilizando el ASA, el PIX lleva a cabo los siguientes procesos de filtrado de paquetes con estado:

- Obtiene los parámetros de identificación de la sesión, como las direcciones IP y los puertos de cada conexión TCP.
- Registra los datos en una tabla de conexión con estado y crea un objeto de sesión.
- Compara los paquetes entrantes y salientes frente a los objetos de sesión de la tabla de conexión.
- Permite que los paquetes de datos fluyan a través de firewall PIX sólo si existe una conexión adecuada que valide su paso.
- Cuando concluye la conexión, se elimina la información relativa a la conexión y a los objetos de sesión.

La función de proxy por método de corte del firewall PIX de Cisco es un método patentado de verificación transparente de la identidad de los usuarios del firewall y de autorización o de denegación del acceso a cualquier aplicación basada en TCP o UDP.

Cuando se usa la autenticación con el firewall PIX, es preciso autenticar las conexiones con un ID de usuario y una contraseña antes de poder establecerlas. El ID de usuario y la contraseña se introducen a través de una conexión inicial http, Telnet o FTP. Se autentica al usuario frente a una base de datos que está basada en el sistema de control de acceso al TAC (TACACS+) o en el servicio de usuario de acceso telefónico mediante autenticación remota (RADIUS) y se comprueba la norma. A continuación, el firewall PIX cambia el flujo de la sesión, y todo el tráfico subsiguiente fluye rápida y directamente entre las dos partes sin mantener el estado de la sesión. El proxy por método de corte del PIX influenciar los servicios de autenticación, autorización y contabilidad del servidor de control de acceso de Cisco Secure.

4.2 Modelos de firewall PIX

A continuación se relacionan cinco de los modelos existentes de firewalls PIX, en esta oportunidad no se hará mención al PIX 501 ya que más adelante se estudiará con mayor detalle.

- **El PIX 506 de Cisco Secure.** El más pequeño de los cinco modelos, el PIX 506 está pensado para pequeñas empresas/oficinas domesticas (SOHO) y su rendimiento es de 10 Mbps.
- **El PIX 515 de Cisco Secure.** Concebido para empresas pequeñas y medianas e implementaciones de oficina remota, tiene un rendimiento de 120 Mbps y capacidad para manejar hasta 125.000 sesiones simultáneas.
- **El PIX 520 de Cisco Secure.** Concebido para empresas grandes y complejas y entornos de mucho tráfico. Tiene un rendimiento de hasta 370 Mbps y capacidad para manejar 250.000 sesiones simultáneas.
- **El PIX 525 de Cisco Secure.** Pensado para empresas y proveedores de servicios, tiene un rendimiento de 370 Mbps y capacidad para manejar hasta 280.000 sesiones simultáneas.
- **El PIX 535 de Cisco Secure.** La última adición (y la más grande) a la serie PIX 500, está pensado para empresas y proveedores de servicios, tiene un rendimiento de 1Gbps y capacidad para manejar hasta 500.000 sesiones simultáneas.

La tabla 4.1 enumera las especificaciones y características de la gama de productos PIX.

	PIX 506 de Cisco Secure	PIX 515 de Cisco Secure	PIX 520 de Cisco Secure	PIX 525 de Cisco Secure	PIX 535 de Cisco Secure
Tamaño (RU [unidad de bastidor] = 1,73 pulgadas	1	1	3	2	3
Procesador Intel Pentium (MHz)	200	200	350	600	1 GHz
Máximo de interfaces	2	6	6	8	10
Recuperación ante fallos	No	Sí	Sí	Sí	Sí
Conexiones	400	125.000	250.000	280.000	500.000

Tabla 4.1. Especificaciones y características de la gama de productos PIX.

4.2.1 Controles, conectores y características del panel frontal/posterior.

Los conectores y los controles del PIX varían según el modelo. Todos los modelos utilizan la misma convención de nombres, pero debido a las diferencias de tamaño y distribución, el diseño físico es distinto. Es por esto que sólo se hará referencia a los modelos PIX 515 y PIX 535.

4.2.1.1 Firewall PIX de Cisco modelo 515.

En el panel posterior del PIX 515 se incluyen los conectores Ethernet RJ-45, un puerto de consola, una conexión de recuperación ante fallos, los LED y el interruptor de encendido. La figura 4.2 muestra el panel posterior del PIX 515-R.

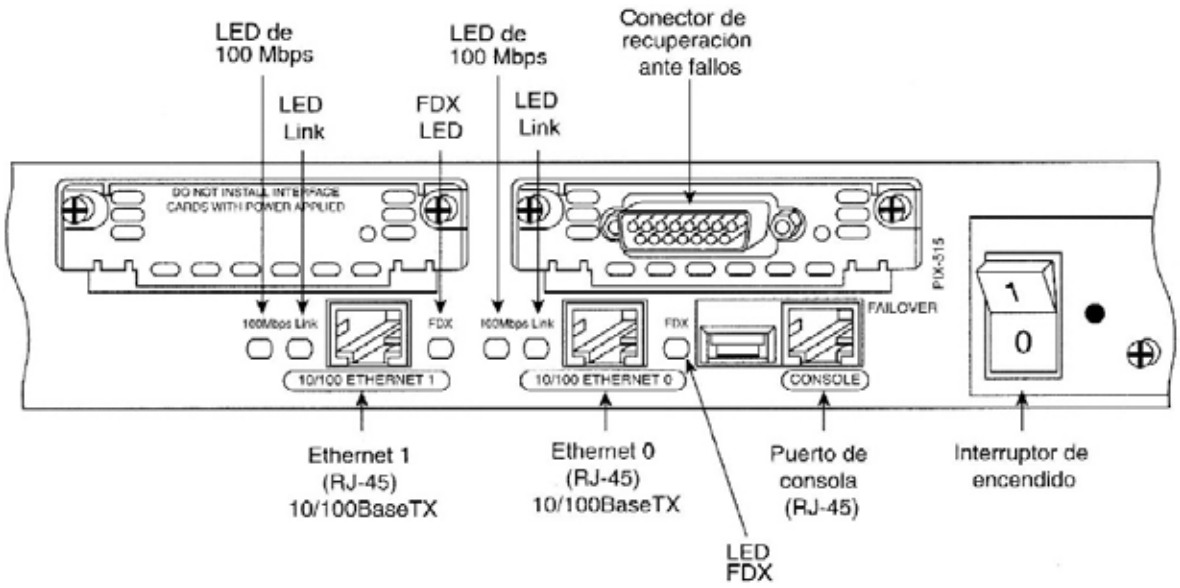


Figura 4.2 El PIX 515.

La lista que sigue detalla las opciones del panel posterior del PIX 515 de la figura 4.2.

- **Conexión Ethernet.** Ethernet 1 es la conexión de red interna. Ethernet 0 es la conexión de red externa. (A partir de la versión de software 5.2x: Ethernet 0 no tiene por qué ser la interfaz externa).

- **Puerto de consola.** Se utiliza para conectar un terminal (por ejemplo, un PC que ejecuta Windows a través de la aplicación Hyperterm) en el firewall PIX para las operaciones de consola.
- **Conexión de recuperación ante fallos.** Se usa para conectar cable de recuperación ante fallos entre dos firewalls PIX.
- **LED de 100 Mbps.** Las comunicaciones 100BaseTX de 100 Mbps del correspondiente conector. Si la luz está apagada, el firewall PIX 515 utilizará un intercambio de datos de 10 Mbps.
- **LED LINK.** Indica que los datos están pasando por la red a la que está enlazada el conector.
- **LED FDX.** Indica que la conexión utiliza el intercambio dúplex de datos; los datos pueden ser transmitidos y recibidos simultáneamente. Si la luz está apagada, estará habilitado semidúplex.
- **Interruptor de encendido.** Controla el encendido del firewall PIX.

El puerto USB que hay a la izquierda del puerto de consola y la placa desmontable que hay por encima del conector Ethernet 1 (Figura 4.2) son futuras mejoras en el firewall PIX.

A continuación se relacionan los indicadores LED de la parte frontal del PIX 515.

- **POWER.** Cuando el firewall PIX está activado, la luz está encendida.
- **ACT.** Si el firewall PIX se utiliza en una configuración autónoma, la LUZ estará encendida. Cuando el firewall PIX esté configurado para operaciones de recuperación ante fallos, la luz se encenderá en firewall PIX activo.
- **NETWORK.** La luz se enciende cuando el menos una interfaz de red está pasando tráfico.

Existen dos ranuras para la expansión del PIX 515. El número máximo de interfaces permitidas es de seis. Para conseguir el máximo de seis puertos, se inserta una tarjeta de cuatro puertos en la ranura superior (véase figura 4.3). Cuando se actualiza el PIX a un firewall de seis puertos, la licencia de software también se deberá actualizar.

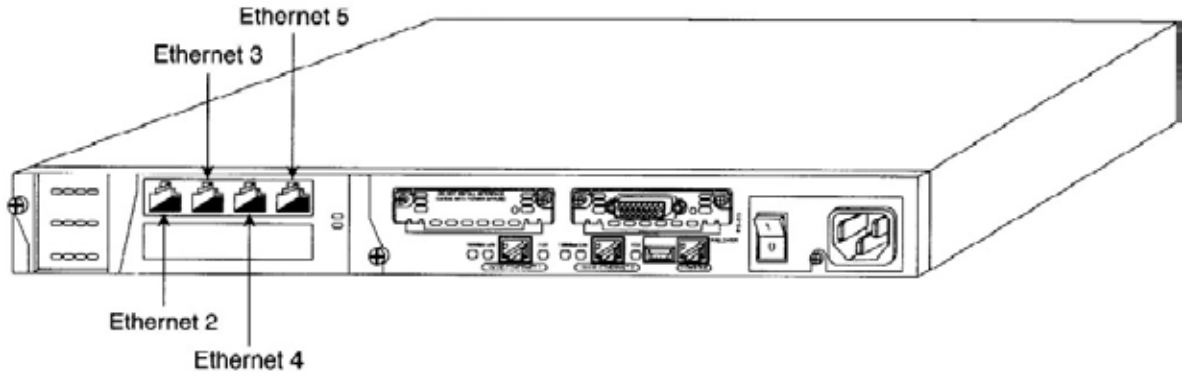


Figura 4.3 Cómo agregar una tarjeta de expansión de cuatro puertos.

Al actualizar algunas características del firewall PIX, incluyendo el aumento del numero de conexiones, la instalación de recuperaciones ante fallos, la instalación de IPSec o la adición de interfaces adicionales, podría ser necesario actualizar una licencia restringida a una no restringida.

El número de ranuras se puede ampliar de dos a tres o de tres a cuatro, si el firewall PIX 515 posee una o dos tarjetas Ethernet de puerto único adicionales en el ensamblado auxiliar, situado en el extremo izquierdo del firewall, las tarjetas se numerarán de arriba abajo para que la tarjeta superior sea Ethernet 2 y la inferior Ethernet 3.

Para configurar y administrar el PIX de forma local, debe establecerse una conexión entre el PIX y un terminal de computador a través del puerto de consola. Para instalar el cable serie entre el PIX y el computador de consola, tendrá que usar el cable serie que incluye el PIX.

Para instalar el cable serie entre el firewall PIX 515 y el computador de consola, siga estos pasos:

Paso 1 Localice el ensamblaje del cable serie del kit de accesorio que se incluye en el firewall PIX.

Paso 2 Conecte uno de los conectores RJ-45 con el puerto de consola PIX.

Paso 3 Conecte el otro conector RJ-45 y un conector DB9 o DB-25 al conector correspondiente de la interfaz del terminal.

En el PIX 520 hay cuatro ranuras de interfaz. Si se conectan cables de red con cuatro tarjetas de interfaz de puerto único en el PIX 520, la tarjeta de interfaz de red deberá estar en la ranura 0, que es la ranura disponible que hay más a la izquierda. En la configuración, esta ranura se conoce como Ethernet 0.

Observe la diferencia en las secuencia de numeración.

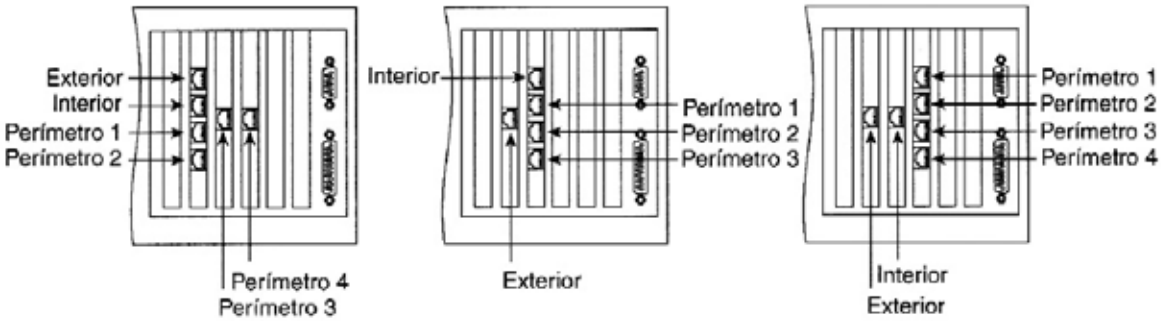


Figura 4.2.3 La tarjeta cuadrangular del firewall PIX 520.

4.2.1.2 Firewall PIX de Cisco modelo 535.

Actualmente, el firewall PIX más grande es el modelo 535. Este modelo incorpora rendimiento de clase de carrier para satisfacer las necesidades de las redes de las grandes empresas, así como las de los proveedores de servicios.

El modelo 535 soporta tarjetas de interfaz Ethernet de 10 MB, 100 MB y 1 GB. También se soporta el cifrado DES de 56 bits y el cifrado 3DES de 168 bits.

El panel frontal consta de los mismos indicadores LED **POWER** y **ACT** que el modelo 525.

Existen tres buses separados para las ocho ranuras de interfaz en la parte posterior del PIX 535. Las ranuras y los buses (figura 4.5) están configurados de esta forma:

- Ranuras 0 y 1. Bus 0 de 64 bits / 66 MHz.
- Ranuras 2 y 3. Bus 1 de 64 bits / 66 MHz.
- Ranuras 4 a 8. Bus 2 de 32 bits / 33 MHz.

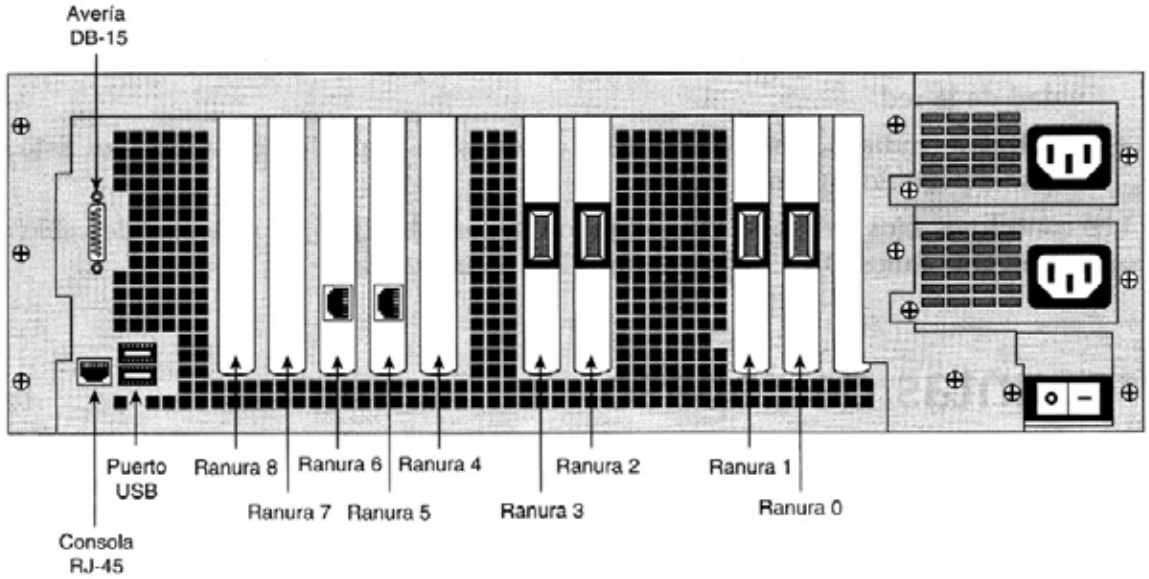


Figura 4.5 El firewall PIX 535.

Para conseguir el máximo rendimiento de las tarjetas de circuito de interfaz, deberá seguir estas recomendaciones.

- Es posible configurar un total de seis tarjetas de circuito de interfaz con la licencia restringida y un total de ocho con la licencia no restringida.
- Las tarjetas de circuito PIX-1 GE-66 (66 MHz) pueden instalarse en cualquiera de las ranuras, pero primero deberán instalarse en el bus de 64 bits / 66 MHz. Es posible instalar hasta ocho tarjetas de circuito PIX-1 GE-66.
- La tarjeta de circuito FE (33 MHz) puede instalarse en cualquier bus o ranura. Es posible instalar hasta un máximo de ocho tarjetas de circuito FE de puerto único o hasta cuatro tarjetas de circuito FE de cuatro puertos.
- No mezcle las tarjetas de circuito de 33 MHz con las tarjetas de circuito GE de 66 MHz en el mismo bus de 64 bits / 66 MHz (bus 0 o bus 1). La velocidad total del bus se verá reducida por la tarjeta de circuito de menor velocidad.

- Sólo se debe instalar el acelerador VPN en el bus de 32 bits / 33 MHz.

Los siguientes LED se encuentran en el panel posterior, junto a las interfaces 100BaseTx:

- **LED de 100 Mbps.** Este indicador está situado en el panel posterior, junto al puerto. Si el LED está activo, el puerto estará empleando 100Mbps. Si la luz está apagada mientras la red está activa, ese puerto estará usando 10 Mbps para el intercambio de datos.
- **ACT.** Este indicador está en el panel posterior, junto al puerto. Muestra la actividad de la red.
- **LINK.** Este indicador muestra que los datos están pasando por la interfaz. Está en el panel posterior, junto al puerto.

Los conectores fijos del panel posterior son la consola RJ-45, el conector de cable de recuperación ante fallos DB-15 y la interfaz USB no utilizada.

4.3 Imagen y actualización del software para PIX.

Cuando se trabaja con cualquier dispositivo Cisco, la interfaz de línea de comandos (CLI) es la interfaz que se usa principalmente para configurar, controlar y mantener ese dispositivo. La CLI interactiva es la interfaz de usuario que más se utiliza para todos los productos Cisco. Los modos administrativos básicos que utilizan los dispositivos Ciscos en el EXEC de usuario, el EXEC privilegiado y los distintos modos de configuración. Cuando se está en modo EXEC de usuario, es posible llevar a cabo consultas básicas, pero no es posible hacer cambios.

4.3.1 La línea de comandos PIX.

El firewall PIX contiene un conjunto de comandos parecidos, pero no idénticos en lo que a la sintaxis se refiere, al conjunto de comandos de Cisco IOS. Cuando acceda a un comando

concreto, deberá estar en el modo apropiado si quiere acceder a ese comando concreto, el PIX proporciona cuatro modos administrativos de acceso:

- **Modo no privilegiado**: está disponible la primera ves que se accede al firewall PIX , también se denomina modo EXEC de usuario. Este modo permite ver un subconjunto de todos los comandos disponibles, ya que un usuario no puede realizar cambios en la configuración si el modo no privilegiado es el único modo accesible.
- **Modo Privilegiado**: este modo permite cambiar la configuración actual, una ves que se ha accedido al modo privilegiado, se tiene acceso al modo de configuración
- **Modo configuración**: Permite cambiar la configuración del sistema, en este modo funcionan todos los comandos no privilegiados, privilegiados y de configuración.
- **Modo de monitor**: Le permite llevar a cabo determinadas tareas que de otro modo sería imposible ejecutar. Una de estas labores consiste en actualizar una imagen a través de la red. Estando en el modo monitor, puede introducir comandos para especificar la ubicación del servidor TFTP y la imagen binaria a descargar.

Modo	Indicador
Modo no privilegiado	pixfirewall>
Modo privilegiado	pixfirewall#
Modo de configuración	pixfirewall(config)#
Modo de monitor	monitor>

Tabla 4.2. Los distintos indicadores PIX para los modos administrativos.

En cada modo de acceso, es posible abreviar la mayoría de los comandos hasta la longitud mínima necesaria para hacerlos únicos. Por ejemplo, es posible escribir **wr t** para ver la configuración en vez de escribir el comando completo, **write terminal**. Otros ejemplos pueden ser **en** lugar de **enable** para iniciar el modo privilegiado y **co t** en vez de **configuration terminal** para iniciar el modo de configuración.

La información de ayuda está disponible en la línea de comandos del firewall PIX introduciendo **help** o **?** para enumerar todos los comandos. Si escribe **help** o **?** detrás de un comando (por ejemplo, **route?**), aparecerá la sintaxis del comando. El número de comandos que aparece cuando se usa el comando **help** (**?**) difiere en función del modo de acceso, de

forma que el modo no privilegiado ofrece el menor número de comandos, mientras que el modo de configuración ofrece el mayor número de comandos. Además, es posible introducir cualquier comando en la lista de comandos y pulsar Intro para ver la sintaxis del comando.

Con un editor de textos, es posible crear un archivo de configuración mientras se está en modo sin conexión. Un usuario podría copiarlo y pegarlo en la configuración PIX.

El PIX permite introducir una configuración completa de esta forma o línea. Siempre deberá comprobar la configuración después de pegar información, a fin de asegurarse de que todo ha sido copiado correctamente. Otra opción a la hora de configurar el PIX consiste en usar un servidor TFTP.

4.4 Modos de Configuración de un Firewall.

Cuando se configura el Firewall PIX es importante tener en cuenta que ya sea de dos interfases o de seis interfases la configuración es exactamente de la misma forma, esto se debe que el ASA (algoritmo de seguridad adaptable) utiliza el concepto de niveles de seguridad.

El nivel de seguridad designa el hecho de que la interfaz sea interna (fiable) o externa (no fiable) con respecto a otra interfaz. Se considera que una interfaz está dentro con respecto a otra interfaz si su nivel de seguridad es mayor que el nivel de seguridad de la otra interfaz y se considera que es externa con respecto a otra interfaz si su nivel de seguridad es más bajo que el nivel de seguridad de la otra interfaz.

Nivel de Seguridad ASA

Los niveles de seguridad van de 0 a 100 y las reglas para estos niveles son las siguientes:

- Nivel de seguridad 100: es el nivel mas alto de una interfaz, se utiliza en la interfaz interna del firewall dado que es el nivel de seguridad mas fiable, y la red de la organización debe estar configurada detrás de esta interfaz.

- Nivel de seguridad 0: Es el nivel de seguridad mas bajo, este nivel se usa para la interfaz externa del firewall la cual se encuentra predeterminada y no se puede modificar. Ya que 0 es el nivel de seguridad de la interfaz menos confiable. A los dispositivos del exterior se les permitirá el acceso a través del firewall sólo si este está configurado para ello. Esta interfaz sirve para conectarse a Internet.

- Nivel de seguridad 1 – 99: Estos niveles de seguridad pueden ser asignados a las interfases de perímetro que están conectadas con el firewall.

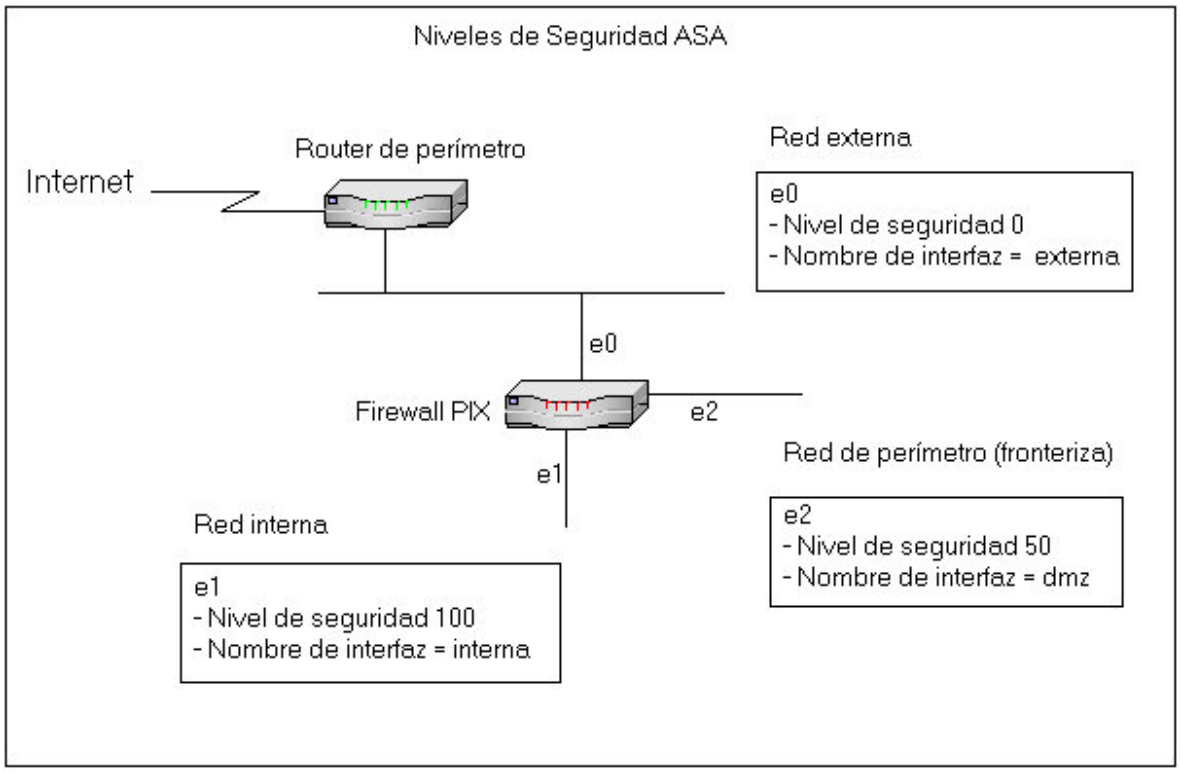


Figura 4.6 Niveles de seguridad PIX.

Mediante algunas entradas de configuración básica, mostraremos algunos ejemplos de las distintas conexiones de interfaz entre el firewall PIX y otros dispositivos de perímetro.

- Los datos que viajan desde una interfaz más segura hacia una interfaz menos segura, necesitaran que haya una conversión estática o dinámica para permitir el tráfico de dicha interfaz hacia una de menor seguridad.
- Los datos que viajan desde una interfaz menos segura hasta una interfaz mas segura deberán cumplir con dos cosas: primero una conversión estática y segundo un conducto o una lista de acceso que permita el tráfico deseado.
- No existe flujo de tráfico entre dos interfases con el mismo nivel de seguridad.
- Los datos que viajan desde una interfaz más segura hasta una interfaz menos segura: Es necesario que haya una conversión estática o dinámica para permitir el tráfico desde una interfaz de seguridad alta hasta otra baja.
- Los datos que viajen desde una interfaz menos segura a una más segura: Es necesario una conversión estática y un conducto o una lista de acceso que permita el tráfico deseado.
- Los datos que viajan a través de dos interfaces con el mismo nivel de seguridad: No existe flujo de tráfico entre dos interfaces con el mismo nivel de seguridad, aunque sea posible configurar dos o más interfaces con el mismo nivel de seguridad ASA.

4.4.1 Comandos Básicos para la configuración del firewall PIX.

Antes de revisar los comandos se explicarán las convenciones sobre la sintaxis de comandos.

Las convenciones utilizadas para presentar las sintaxis de comandos de este libro son las mismas que se usaron en la CISCO IOS Command Referente las cuales se describen como:

- Las barras verticales (|) separan elementos alternativos, que se excluyen entre sí.
- Los corchetes [ ] indican los elementos opcionales.
- Las llaves { } indican una opción necesaria.
- Las llaves dentro de los corchetes [{ }] indican una opción necesaria con un elemento opcional.
- La **negrita** indica comandos y palabras clave que son introducidas literalmente. En los ejemplos y resultados de configuración reales (y no en la sintaxis general de comandos),

la negrita indica comandos que son introducidos manualmente por el usuario (como el comando **show**).

- La *cursiva* indica argumentos a los que se proporcionan valores reales.

Nota: Cada opción/argumento será explicado en la tabla 4.3 que aparece mas abajo.

- Comando **nameif:** Asigna un nombre a cada interfaz del firewall y especifica su nivel de seguridad (exceptuando las interfases externas e internas que por defecto tienen su nombre).

  Sintaxis: **Nameif** id_hardware nombre_if nivel_seguridad

- Comando **interface:** se identifica el tipo de hardware , especifica la velocidad del hardware que van desde 10baset hasta 1000basesx y activa interfaz.

  Sintaxis: **Interface** id_hardware velocidad_hardware **[shutdown]**

- Comando **IP address:** Es para asignarle a cada interfaz una dirección IP.

  Sintaxis: **IP address** nombre_if dirección_ip [máscara_de_red]

- Comando **nat:** La traducción de direcciones de red Nat impide que las redes externas conozcan las direcciones IP internas.

  Sintaxis: **nat** (nombre_if) id_nat ip_local [mascara_de_red]

- Comando **global:** Al enviar datos de una red fiable a otra no fiable, se suelen convertir las direcciones IP de origen. El PIX lo puede hacer por medio de dos comandos, el primero es el nat que define las direcciones de origen fiables que se van a convertir. El comando que se usa para definir la dirección o intervalo de direcciones en que se convertirá la dirección de origen es el comando global.

Sintaxis: **global** (nombre_if) id_nat **interface** | ip_global [-ip_global] [**netmask** mascara_global]

- Comando **route:** Define una ruta estática para una interfaz, esta instrucción puede tener un destino específico o también puede crear una ruta estática predeterminada.

Sintaxis: **route** nombre_if dirección_ip máscara_de_red ip_gateway [métrica]

Comando	**Descripción del argumento/opción**
id_hardware	Especifica una interfaz de perímetro y su ubicación física.
Nombre_if	Asigna un nombre a la interfaz del perímetro física.
nivel_seguridad	Indica el nivel de seguridad de la interfaz de perímetro.
velocidad_hardware	Determina la velocidad de conexión. Introduzca **auto** para que el firewall pueda detectar la velocidad necesaria para el dispositivo.
shutdown	Cierra la interfaz definitivamente.
direccion_ip	La dirección IP asignada de interfaz.
máscara_de_red	Máscara de red de la dirección IP local, si no se especifica, se supondrá la máscara de red con clase: Clase A: 255.0.0.0 Clase B: 255.255.0.0 Clase C: 255.255.255.0
id_nat	Identifica el pool global y lo compara con su respectivo comando **global**.
id_local	La dirección o direcciones IP signadas a los dispositivos de la red interna.
interface	Hace que el PIX convierta todas las direcciones IP que especifique el comando **nat** para la interfaz especificada.
ip_global	Direcciones IP únicas o la dirección IP de inicio de un intervalo de direcciones IP globales.
-ip_global	Un intervalo de direcciones IP globales.
netmask máscara_global	La máscara de red de la dirección IP global.

Tabla 4.3 Descripción de los argumentos.

4.5 Conversión de firewall PIX.

La encapsulación tiene lugar al principio de una sesión, cuando los datos de la aplicación se combinan con la información de a capa de transporte para crear un segmento. El PIX busca la información específica que hay dentro de una trama para tomar decisiones importantes acerca del flujo del tráfico.

4.5.1 Protocolos de transporte.

Una sesión de red principalmente se lleva a cabo sobre uno de estos dos protocolos en la capa de transporte:

4.5.1.1 Protocolo de control de transmisión (TCP).

Este protocolo esta orientado a conexión, entonces cuando inicia una sesión desde un host en la interfaz mas segura del firewall PIX , éste crea una entrada en una tabla de estado de sesión.

El firewall PIX extrae la información de sesión de la red del flujo de red y verifica su validez en tiempo real, este filtro con estado mantiene los parámetros de cada conexión de red y comprueba la información subsiguiente.

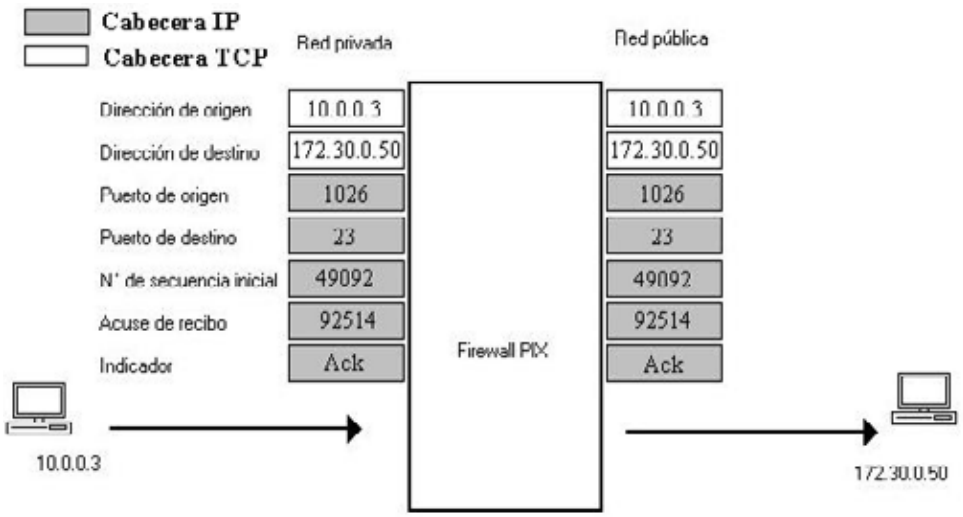


Figura 4.7 Inicialización TCP, del interior al exterior.

4.5.1.2 Protocolo de datagrama de usuario (UDP):

Este es un protocolo sin conexión, con lo que el firewall tendrá que adoptar otras medidas pata garantizar la seguridad . Las aplicaciones que utiliza UDP son difíciles de proteger ya que no existe intercambio de señales ni secuencia. El firewall PIX crea una ranura de conexión UDP cuando un paquete UDP es enviado desde una interfaz más segura hacia otra menos segura. El firewall PIX acepta paquetes UDP entrantes siempre que después de haber visto un paquete UDP saliente desde la misma dirección IP de origen y destino.
Características de UDP:

- Es un protocolo no fiable pero eficiente
- No garantiza la entrega ya que no existe configuración ni finalización de la conexión .
- Carece de administración o prevención de congestión.

4.5.2 Conversión del firewall PIX.

Cuando se configura la conversión de direcciones con el firewall PIX existen dos opciones la conversión estática y la conversión dinámica.

4.5.2.1 Conversión estática de direcciones:

Con este tipo de conversión se logra que las direcciones internas puedan convertirse a una dirección global específica. Esta conversión se utiliza cuando hay que convertir un host a la misma dirección cada ves que se construya una sesión saliente en el PIX. También se utiliza para lograr que las direcciones IP de las interfaces de seguridad alto estén accesibles para los niveles de seguridad bajo.

El comando **static** tiene la siguiente sintaxis:

Static [(nombre_if_interno, nombre_if_externo)] ip_global ip_local [**netmask** máscara_red] [conexiones_máx [límite_em]] **[norandomseq]**

4.5.2.2 Conversión dinámica de direcciones

Se utiliza para convertir un intervalo de direcciones locales a un intervalo de direcciones globales o a una dirección global única. La conversión de un intervalo de direcciones locales a un intervalo de direcciones globales se denomina Traducción de direcciones de red NAT. La traducción de un intervalo de direcciones locales a una dirección global única se denomina Traducción de direcciones de puerto (PAT).

La conversión dinámica de direcciones utiliza NAT, los host locales deberán definidos con el comando nat. El pool de direcciones deberá ser definido con el comando global. El pool para la asignación de direcciones se elige en la interfaz saliente en base al id_nat que se haya seleccionado con el comando nat.

Al utilizar PAT todas las direcciones locales son traducidas a una única dirección global. La configuración PAT es similar a NAT, la única diferencia es que la instrucción global contiene solo una dirección IP.

PAT no funciona con aplicaciones H.323. Las aplicaciones multimedia pueden entrar en conflicto.

PAT funciona con DNS, FTP, http y RCP entre los mas importantes.

4.6 Configuración de Acceso a través del Firewall.

Para configurar el acceso desde el exterior hasta el interior existen dos formas de proceder en el PIX desde un dispositivo menos fiable hasta un dispositivo más fiable.

4.6.1 Métodos para operar en el PIX.

4.6.1.1 Respuesta a una petición válida

Cuando un usuario del interior crea una conexión con un dispositivo del exterior, la respuesta a esa petición se permite por defecto a través del PIX y todas las conexiones internas y externas poblarán la tabla de conversión del PIX.

Si el dispositivo externo responde a la petición, el firewall comprueba la tabla de conversión para verificar si existe una línea de conversión para esa petición concreta. Si esta existe, el firewall permitirá que la respuesta continúe.

Una vez terminada la sesión se inicia el temporizador de inactividad de esa determinada línea de conversión, el tiempo dependerá de la versión del software que se esté utilizando, por ejemplo la versión 5.1 es de tres horas.

4.6.1.2 Configuración de un conducto.

Se utiliza para canalizar internamente una comunicación externa.. Se debe configurar la traducción static o global y nat, también se configura el conducto que define la dirección o conjunto de direcciones de origen y / o el puerto o intervalos de puertos TCP/UDP de destino al que se permite que fluya por el firewall.

4.6.2 Comandos static y conduit.

4.6.2.1 Static

Crea una asignación estática entre una dirección IP interna y una dirección global externa. El uso de este comando permite establecer una dirección IP global permanente para esta dirección IP interna concreta. Esto configura la capacidad de crear una entrada para las interfaces especificadas con el nivel de seguridad bajo en la interfaz especificada con el nivel de seguridad alto.

4.6.2.2 Conduit

Este comando se utiliza después de crear la asignación estática entre la dirección IP interna y la dirección IP externa, ya que la conexión desde la interfaz externa hacia la interfaz interna seguirá estando bloqueada por el ASA del firewall PIX.

Entonces este comando se utiliza para permitir el flujo entre una interfaz con un nivel de seguridad bajo con uno de seguridad alto. Conduit crea las excepciones en el ASA del firewall PIX.

Ejemplo: Utilización del comando static para convertir de forma estática la IP 10.0.1.10 a 192.168.1.101 y el comando conduit permitirá que solo http sea el que acceda al host convertido.

Pixfirewall (config)# static (inside, outside) 192.168.1.101 10.0.1.10 netmask 255.255.255.255
Pixfirewall (config)# conduit permit tcp any eq www host 172.16.1.1

Sintaxis del comando conduit:

Conduit permit | deny protocolo ip_global máscara_global [puerto operador [puerto]] ip_externa máscara_externa [puerto operador [puerto]]

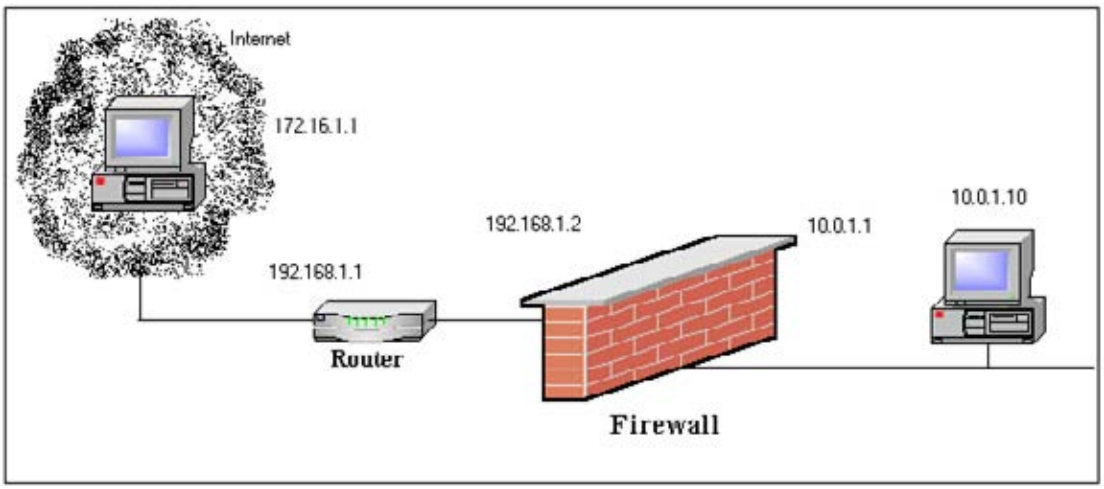


Figura 4.8 El comando conduit.

4.6.3 Métodos de accesos a través del PIX.

NAT (Traducción de Direcciones de Red) es el método de acceso mas común desde el interior hacia el exterior. NAT permite convertir un intervalo de direcciones del interior a un intervalo de direcciones cuando se accede a los dispositivos del exterior.

NAT 0 permite desactivar la conversión de direcciones, de forma tal que las direcciones IP internas sean visibles para el exterior sin la conversión de direcciones.

PAT (Traducción de Direcciones de Puerto) convierte un intervalo de direcciones internas a una sola dirección global. PAT es una combinación de una dirección IP y un número de puerto de origen que crea una sesión única. El firewall traduce cada dirección local a la misma dirección global, pero asigna un puerto de origen único mayor que 1024.

- PAT y NAT se pueden usar conjuntamente.
- Es posible usar una dirección IP global para un máximo de 64.000 hosts internos, esto es un límite al tamaño del campo del puerto de 16 bits.
- Asignar solo un número de puerto a una sola dirección IP significa alquilar menos direcciones IP a un proveedor de servicios, esto reduce considerablemente los costos de la red.
- No utilizar PAT cuando se ejecuten aplicaciones multimedia a través del firewall, porque es posible que tengan que acceder a puertos específicos y entren en conflicto con los puertos reservados por PAT.

4.6.3.1 Protocolo FIXUP.

El comando Fixup permite a un usuario ver, cambiar, activar o desactivar el uso de un servicio o protocolo a través del firewall PIX. Los puertos que especifica el comando fixup son los servicios que escuchará el firewall PIX. Puede cambiar el valor de puerto de cada servicio, a excepción de RSH.

Algunas aplicaciones como FTP , requiere que el Firewall PIX entienda las propiedades especiales de la aplicación, de forma que se permitan las conexiones que formen parte legítima

de la aplicación. Durante la transferencia FTP desde el interior hasta el exterior, el firewall PIX deberá tener en cuenta el segundo canal de datos que se abre desde el servidor hasta la estación de trabajo de inicio.

El firewall identifica las aplicaciones mediante el número de puertos TCP o UDP contenidos en los paquetes IP, por ejemplo reconoce FTP mediante el puerto número 21, SMTP con el puerto 25 y http mediante el puerto 80.

En general, no es necesario cambiar estos números de puerto, pero en circunstancias especiales, es posible que haya un servicio escuchando en un número de puerto no estándar. Por ejemplo , podría haber un servidor http escuchando en un puerto 5000. El firewall no reconocería que está usando el puerto 5000 para http y bloquearía la conexión de datos http devueltas desde el servidor. Este problema se puede solucionar agregando el puerto 5000 al comando fixup protocol: pixfirewall (config)# fixup protocol http 5000

Este comando permite al firewall reconocer que las conexiones al puerto 5000 deben ser tratadas de la misma forma que las conexiones al puerto 80.

4.6.3.2 Soporte Multimedia.

Las aplicaciones multimedia pueden ser problemáticas para un firewall, ya que los distintos protocolos que utiliza abren dinámicamente distintos puertos para la conexión.

Características de multimedia del firewall PIX.

- Abre y cierra dinámicamente puertos UDP para las conexiones multimedia seguras.
- Soporta multimedia con o sin NAT. Las aplicaciones multimedia que soportan actualmente son:
- Intel Internet Video Pone, Microsoft NetMeeting (basado en estandar H323), White Pine Meeting Point, Microsoft NetShow, White Pines CuSeeMe, VDOnet VDOlive, Real Networks Real Audioy Real Video, Vxtreme WebTheatre, Xing Stream Works y VocalTech Internet Phone.

4.6.4 Configuración de múltiples interfaces.

Un firewall como dispositivo de seguridad que contenga sólo 2 interfaces suele ser suficiente, con lo cual actúa como gateway seguro para el tráfico que entra y sale de la red, sin embargo este escenario normalmente no es suficiente.

El modelo PIX 535 soporta hasta ocho interfaces de perímetro adicionales (para un total de 10) lo cual permite diferenciar sectores privados de los sectores de acceso público como la zona desmilitarizada (DMZ), lo cual entrega mayor seguridad al estar separada físicamente.

Cuando el firewall PIX esté equipado con tres o más interfaces, utilice las siguientes directrices para configurarlo al tiempo que emplea NAT:

- A partir de la versión 5.2X del SO del PIX, es posible asignar un nuevo nombre a la interfaz, pero el valor predeterminado es “outside”. A esta interfaz no se le puede asignar un nivel de seguridad distinto.
- Un interfaz siempre está “fuera” respecto a otra interfaz, si tiene un nivel de seguridad bajo.
- Utilice una instrucción de tuta predeterminada única a la interfaz externa. Establezca la ruta predeterminada con el comando **route**.
- Utilice el comando **nat** para permitir a los usuarios de las correspondientes interfaces iniciar conexiones salientes.

4.7 Mensajes Syslog.

El firewall PIX genera mensajes syslog pata eventos del sistema, como por ejemplo, las alertas y la disminución de recursos. Es posible usar los mensajes syslog que recibe un servidor syslog para crear alertas de correo electrónico y archivo de registro o mostrarlos en la consola de un host syslog determinado.

El firewall PIX puede enviar mensajes syslog a cualquier servidor syslog. En caso de que todos los servidores o host syslog se encuentren desconectados, el firewall PIX almacenará hasta 100 mensajes en su memoria.

Los mensajes subsiguientes que lleguen sobrescribirán el búfer desde la primera línea. Esta opción sólo está disponible cuando el PIX está usando TCP como transporte para syslog. El firewall envía mensajes syslog para documentar los siguientes eventos:

- **Seguridad.** Paquetes UDP derivados y conexiones TCP denegadas.
- **Recursos.** Notificación de la conexión y la disminución de líneas de conversión.
- **Sistema.** Inicios y cierres de sesión de consola y Telnet, y momentos en los que se reinicia el firewall PIX.
- **Contabilidad.** Byte transferidos por conexión.

4.8 Configuración AAA en los Firewalls PIX de Cisco.

La mayoría de las implementaciones de normas de seguridad están diseñadas en base a una solución por capas. En otras palabras, una medida de seguridad no basta para que las normas de seguridad sean satisfactorias. Una solución multidisciplinar, que es más general**,** es aquella que emplea muchos métodos de seguridad. Uno de los aspectos de una norma de seguridad podría ser la exigencia de que usuario introdujera un ID de usuario y una contraseña para acceder a servicios específicos (o a todos los servicios). Esto se denomina **autenticación basada en usuario.** La autenticación podría no tener nada que ver con un usuario concreto, sino con la autenticación de un dispositivo de red otro., 'La autenticación podría ser la prueba de que una entidad de red (dispositivo, cliente, servidor) que no fuera un usuario es en realidad la entidad que dice ser.

4.8.1 Definición de AAA.

La autenticación determina la identidad de un usuario y verifica la información. La autenticación tradicional utiliza un nombre (o un identificador único) y una contraseña fija. El acceso a un dispositivo o una red con un ID de usuario define la identidad del usuario. Una vez

autenticado el usuario, el servidor de autenticación podría ser configurado para permitir la autorización específica, en base al ID de usuario y la contraseña. La **autorización** define lo que el usuario puede hacer. Cuando un usuario ha iniciado sesión y está accediendo a un servicio, *host* o red, podría conservarse un registro de lo que ese usuario estuviera haciendo. La **contabilidad** constituye la acción de controlar lo que un usuario hace. Es muy útil tener un registro contable de los accesos de red. Si se presentan problemas en la red, el hecho de mantener un historial de los registros puede ayudar a identificar y rectificar estos problemas. Los registros contables también pueden ser usados para facturar, analizar y planificar.

El firewall PIX utiliza la Autenticación, autorización y contabilidad (Authentication, Authorization, and Accounting), o AAA, para identificar la identidad del usuario, lo que puede o no hacer y lo que hizo. Los controles de acceso básico al propio PIX están basados en direcciones IP y puertos. Estos controles de acceso no proporcionan ningún mecanismo para identificar usuarios individuales y controlar el flujo de tráfico en base a ese usuario. La autenticación es válida sin autorización. La autorización no es válida sin autenticación.

AAA, cuando se usa con el PIX, suele procesarse de la siguiente forma:

1. El cliente solicita el acceso a algún servicio. El PIX, como gateway entre el cliente y el dispositivo en el que existe el servicio (en base a la petición y la configuración del PIX) requiere que el cliente reenvíe un ID de usuario y una contraseña.

2. El PIX recibe esa información y la reenvía a un servidor AAA, que confirma si se permite o se deniega. Un servidor es una entidad lógica que proporciona cualquiera de las tres funciones AAA. El servidor AAA puede mantener la base de datos de ID de usuario y contraseñas para confirmar que un cliente puede acceder al servicio solicitado.

El hecho de que haya un servidor AAA aparte (estos procesos residen en un dispositivo distinto) reducirá la carga (CPU) del firewall, simplificará la configuración y la administración del firewall e incrementará la escalabilidad.

Es posible permitir que ciertos usuarios autenticados sean los únicos que accedan a una red. Un ejemplo podría ser permitir exclusivamente a aquellos que estuvieran provistos de un

ID de usuario y una contraseña válidos acceder desde la red interna, a través del firewall PIX, hasta Internet. También es posible limitar la autorización (las aplicaciones a las que se puede acceder) de los usuarios autenticados. Configurando el PIX y el servidor AAA, un administrador puede limitar los servicios accesibles a FTP, HTTP, Telnet o cualquier otra aplicación (o combinación de aplicaciones). Un servidor AAA es un servidor de autenticación que puede ser configurado con software para Servidor de control de acceso de Cisco Secure (CSACS) que auténtica y autoriza a los usuarios controlando el acceso. El servidor AAA también puede hacer un seguimiento de los registros contables.

Otro escenario podría ser el de permitir a un usuario que accediera exclusivamente al servicio FTP a través del PIX. La petición la hace el usuario final, y el PIX intercepta la petición y pide un nombre de usuario y una contraseña. Cuando el usuario introduce la información, el PIX la pasa al servidor AAA. Cuando el usuario es autenticado por el servidor AAA, el usuario puede realizar peticiones adicionales. El PIX recibe cada una de las peticiones (de modo transparente para el usuario final), las cuales pasan al servidor AAA para la autorización.

Un usuario puede autenticarse con el firewall PIX utilizando uno de estos tres servicios: FTP, Telnet o HTTP. Cada uno de ellos posee mecanismos de autenticación en línea dentro del propio servicio. Esto no limita las aplicaciones que el PIX puede permitir. Lo que un usuario vea dependerá del servicio al que se esté accediendo. La figura 4.9 ilustra lo que un usuario debe introducir en función del servicio al que esté accediendo.

- **Telnet**. El firewall PIX genera un indicador. Cada usuario tiene cuatro oportunidades de iniciar sesión. Si el nombre de usuario o la contraseña no son válidos después del cuarto intento, el firewall PIX cerrará la conexión. Si la autenticación y la autorización son satisfactorias, se le pedirá al usuario un nombre de usuario y una contraseña, siempre que lo exija el servidor de destino.

- **FTP**. El programa FTP genera un indicador. Si se introduce una contraseña incorrecta, la conexión se cierra inmediatamente. Si el nombre de usuario o la contraseña de la base de datos de autenticación difiere del nombre de usuario o contraseña del *host* remoto al que se está accediendo a través de FTP, introduzca el nombre de usuario y la contraseña en el siguiente formato:

- aaa_username@remote_username
- aaa_password@remote_password

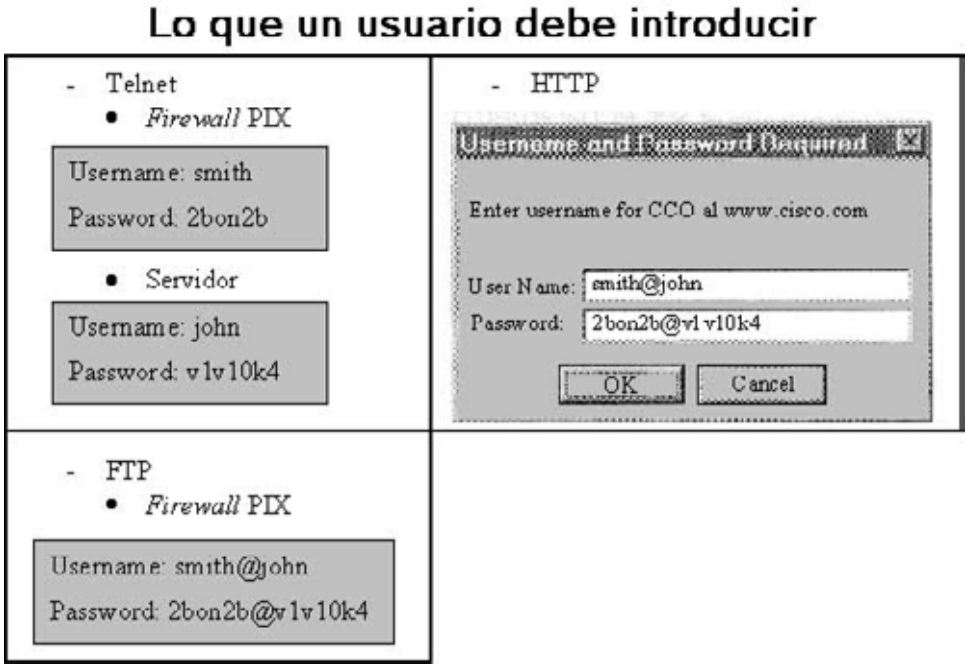


Figura 4.9 Lo que un usuario debe introducir.

- **HTTP.** El navegador genera una ventana emergente con un nombre de usuario y una contraseña. Si se introduce una contraseña incorrecta, se preguntará nuevamente. Es posible desactivar una cuenta después de un número de intentos fallidos.

El firewall PIX soporta nombres de usuario de autenticación (AAA) de hasta 127 caracteres y contraseñas de hasta 63 caracteres. Debido al tratamiento especial que recibe el inicio de sesión con FTP o HTTP al tiempo que se usa AAA, una contraseña o nombre de usuario no pueden contener el símbolo "arroba" (@) como parte de la cadena de la contraseña o del nombre de usuario

4.8.2 Funcionamiento del proxy por método de corte.

El proxy por método de corte del firewall PIX funciona determinando que una sesión requiere la autenticación basada en usuario, la habilitación de un desafío de nombre de usuario/contraseña adecuado, y la autenticación del usuario frente a la base de datos

TACACS+ o RADIUS estándar. Una vez comprobada la norma, el firewall PIX cambia el flujo de sesión y todo el tráfico fluye directa y rápidamente entre el servidor y el cliente, al tiempo que se mantiene la información del estado de la sesión.

Un diseño típico para el uso de esta tecnología es un usuario de Intemet que accede a un servidor HTTP de una DMZ de empresa. En la figura 4.10 se muestra al usuario de Intemet que accede al URL correspondiente para entrar en el servidor web XYZ. El requisito AAA del PIX obliga al usuario a introducir un nombre de usuario y una contraseña. El usuario introduce la información, que se pasa al PIX en texto claro, y el PIX reenvía la información al servidor AAA, que en este caso está ejecutando software CSACS. Si está autenticado, al usuario se le permite interactuar con el destino. Si el servidor web de destino también requiere autenticación, como en la figura 4.10, se pasará la contraseña y el nombre de usuario remotos.

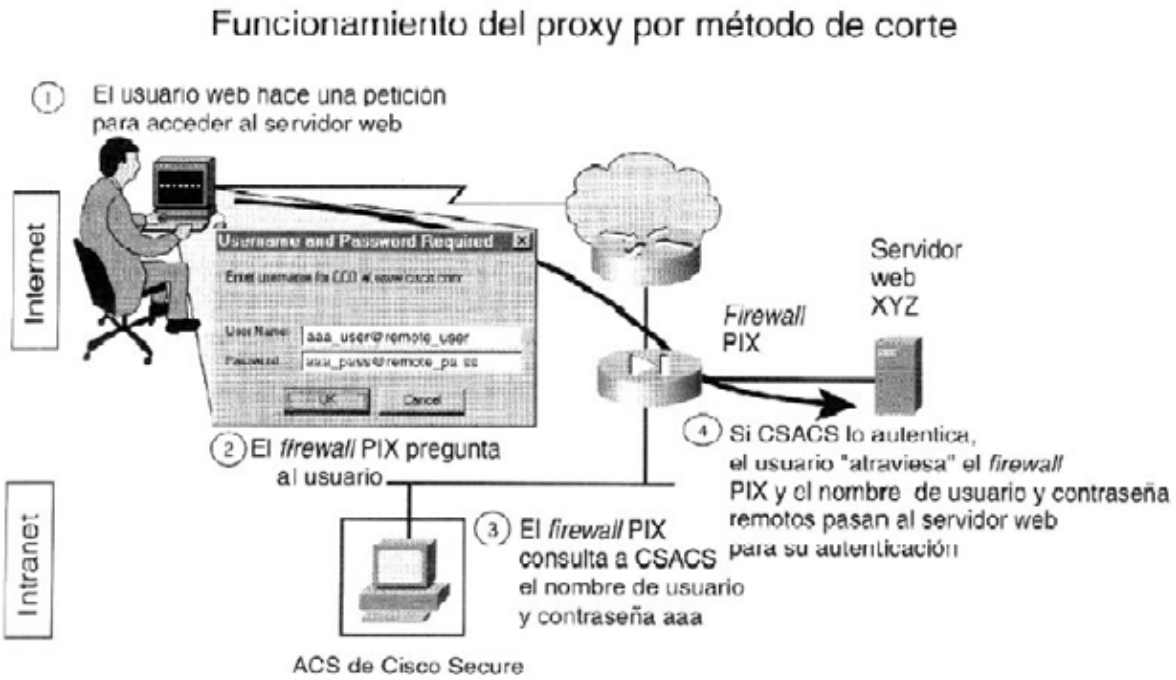


Figura 4.10 Funcionamiento del *proxy* por método de corte.

4.8.3 Servidores AAA soportados.

El firewall PIX soporta los siguientes protocolos y servidores AAA:

- Sistema de control de acceso al TAC Plus (TACACS+).

- Servidor de control de acceso de Cisco Secure (CSACS) para Windows NT (CSACS-NT).
- ACS de Cisco Secure para UNIX (CSACS-UNIX).
- Freeware TACACS+.

- Servicio de usuario de acceso telefónico con autenticación remota (RADIUS).
  - ACS de Cisco Secure para Windows NT (CSACS-NT).
  - ACS de Cisco Secure para UNIX (CSACS-UNIX).
  - Livingston (ahora parte de Lucent Technologies).
  - Merit, de Interlink Network.
  - Steel Belted Radius, de Funk Software.

4.8.4 Instalación de CSACS para Windows NT.

CSACS es una aplicación que proporciona servicios AAA. CSACS proporciona un control centralizado para AAA a partir de una interfaz web gráfica. Con ACS, el administrador puede gestionar y administrar el acceso del usuario a través del firewall PIX.

Para instalar CSACS para Windows NT, siga estos pasos (cierre todas las aplicaciones de Windows antes de ejecutar la configuración):

Paso 1 Inicie sesión en el servidor NT como administrador del sistema.

Paso 2 Inserte el CD-ROM CSACS en la unidad de CD-ROM. CSACS posee una opción de ejecución automática; por tanto, se abrirá la ventana de instalación.

Paso 3 Seleccione Instala. Se abrirá la ventana Software License Agreement.

Paso 4 Lea el contrato. Seleccione Accept para aceptar los términos y condiciones de la licencia. Se abre la ventana Welcome.

Paso 5 Seleccione Next. Se abre la ventana Before You Begin.

Paso 6 Verifique que se cumple cada condición, y seleccione la casilla de verificación de cada elemento. Seleccione Next.

NOTA: Si se trata de una instalación nueva, vaya directamente al Paso 9.

Paso 7 (Opcional) Si CSACS ya está instalado, se abrirá la ventana Previous Installation. Se le pedirá al usuario que elimine la versión anterior y que guarde la información de la base de datos existente. Para conservar los datos existentes, seleccione Yes, keep the existing database y seleccione Next. Para usar una nueva base de datos, anule la casilla de verificación y haga clic en Next. Si se mantiene la base de datos existente, la configuración hará una copia de seguridad de la configuración existente y eliminará los archivos antiguos. Una vez eliminados los archivos, seleccione OK.

Paso 8 Si Setup localiza una configuración existente, el usuario tendrá la opción de importar la configuración. Para conservar la configuración existente, seleccione Yes, import configuration y seleccione Next. Para usar una nueva configuración, anule la casilla de verificación y seleccione Next.

Paso 9 Se abre la ventana Choose Destination Location. Para instalar el software en el directorio predeterminado, haga clic en Next. Para usar un directorio distinto, haga clic en Browse e introduzca el directorio que vaya a usar. Si el directorio no existe, se le pedirá al usuario que cree uno. Seleccione Yes. Se abre la ventana Authentication Database Configuration.

Paso 10 En este punto, el usuario puede optar por autenticarse ante la base de datos CSACS o ante CSACS primero y luego comprobar la base de datos de usuarios de Windows NT (haga clic en Explain para ver más información acerca de los elementos enumerados. Si no se cumple alguna de las condiciones, seleccione Cancel para salir de Setup).

Para limitar el acceso telefónico exclusivamente a aquellos usuarios especificados en el Administrador de usuarios de Windows NT, seleccione la configuración Yes, reference Grant dialin permission to user. Seleccione Next. Se abre la ventana Network Access Server Details.

Paso 11 Complete la siguiente información de la ventana Network Access Server Details (véase la figura 4.11):

- Authenticate Users Using. Tipo de protocolo de seguridad que se va a usar. TACACS+ (Cisco) es el valor predeterminado.
- Access Server Name. Nombre del servidor de acceso a la red (NAS) que usará los servicios CSACS. Cuando se instala conjuntamente con un PIX, el nombre del NAS es el nombre de host del PIX.

- Access Server IP Address. Dirección IP del NAS que usará los servicios CSACS. Cuando se instala conjuntamente con un PIX, la dirección IP del servidor de acceso es la dirección IP del PIX.
- Windows NT Server IP Address. Dirección IP de este servidor Windows NT.
- TACACS+ or RADIUS Key. Secreto compartido del NAS y ACS de Cisco Secure. Estas contraseñas deberán ser idénticas a fin de asegurar la función y comunicación correctas entre el NAS y CSACS. Los secretos compartidos discriminan entre las mayúsculas y minúsculas. Setup instala los archivos CSACS y actualiza el Registro. Seleccione Next.

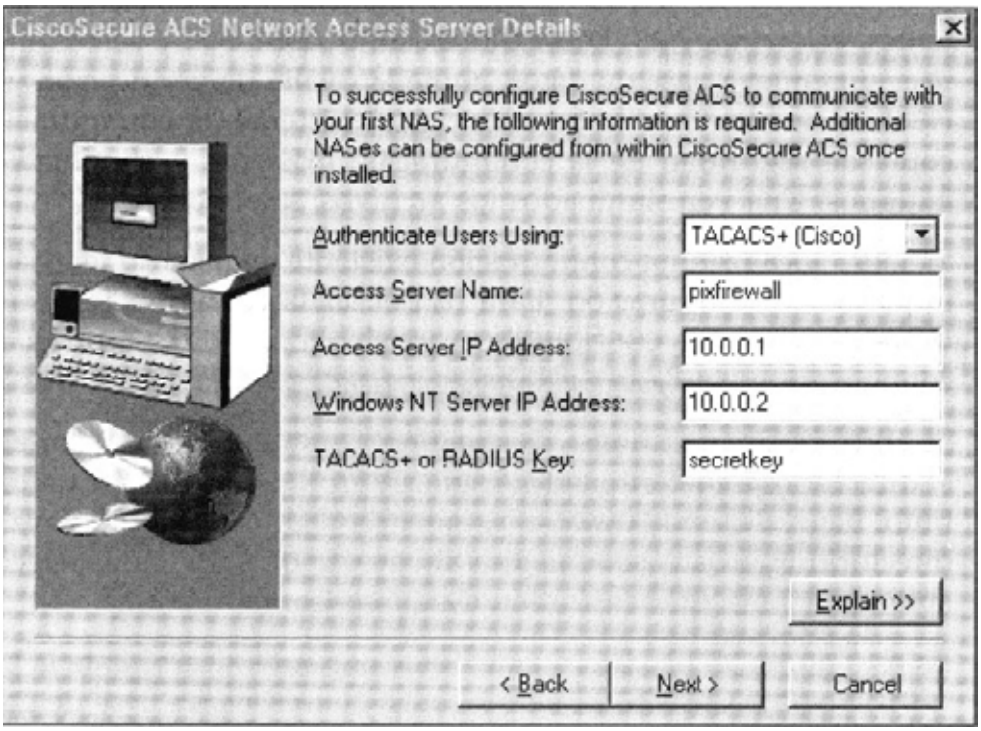


Figura 4.11 Configuración de detalle del NAS.

Paso 12 Se abre la ventana Advanced Options. Las opciones Advanced Options están desactivadas por defecto. Seleccione la casilla de verificación para activar alguna o todas las opciones que aparecen. Seleccione Next.

Paso 13 Se abre la ventana Active Service Monitoring. Para activar el servicio de control CSACS, CSMon, seleccione la casilla de verificación Enable Log-in Monitoring y seleccione un script para que se ejecute cuando el proceso de inicio de sesión no supere la prueba:

- No Remedial Action. Deje que CSACS funcione tal y como está.

- Reboot. Reinicie el sistema en el que se está ejecutando CSACS.
- Restart All (la configuración predeterminada). Reinicia todos los servicios CSACS.
- Restart RADIUS/TACACS+. Sólo reinicia RADIUS, TACACS+, o ambos protocolos.

Paso 14 Para que CSACS genere un mensaje de correo electrónico cuando se produzcan los eventos de administrador, marque la casilla de verificación Enable Mail Notifications e introduzca la siguiente información:

- SMTP Mail Server. El nombre y el dominio del servidor de envío de correo (por ejemplo, server1.company.com):
- Mail account to notify. La dirección electrónica completa del destinatario previsto (por ejemplo, msmith@company.com).

Paso 15 Seleccione Next. Se abre la ventana Cisco Secure ACS Service Initiation. Si no se ha configurado un NAS a partir del Setup, seleccione Next. Para configurar ahora un NAS, seleccione Yes, I want to configure Cisco IOS now. Seleccione Next.

Paso 16 Se abre la ventana Cisco Secure ACS Service Initiation. El administrador tiene ahora la opción de iniciar el servicio CSACS, abriendo el navegador de administración de CSACS y repasando el archivo readme.

4.8.4.1 Cómo agregar usuarios a CSACS-NT.

La base de datos de usuarios que utiliza CSACS puede residir dentro de la propia aplicación o puede ser una base de datos externa (como una base de datos de usuarios de Windows NT). Para agregar usuarios a CSACS NT, siga estos pasos:

Paso 1 En la barra de navegación, seleccione User Setup. Se abre la ventana Select. La Figura 8.5 muestra la ventana User Setup del CSACS.

Paso 2 Introduzca un nombre en el campo User.

El nombre de usuario puede contener hasta 32 caracteres. Los nombres no pueden contener los siguientes caracteres especiales: # ? " * > <. Los espacios iniciales y finales no están permitidos.

Paso 3 Haga clic en Add/Edit. Se abre la ventana Edit. El nombre de usuario que se haya agregado o modificado aparecerá en la parte superior de la ventana. La Figura 4.12 muestra la ventana Edit cuando se agrega un nuevo usuario.

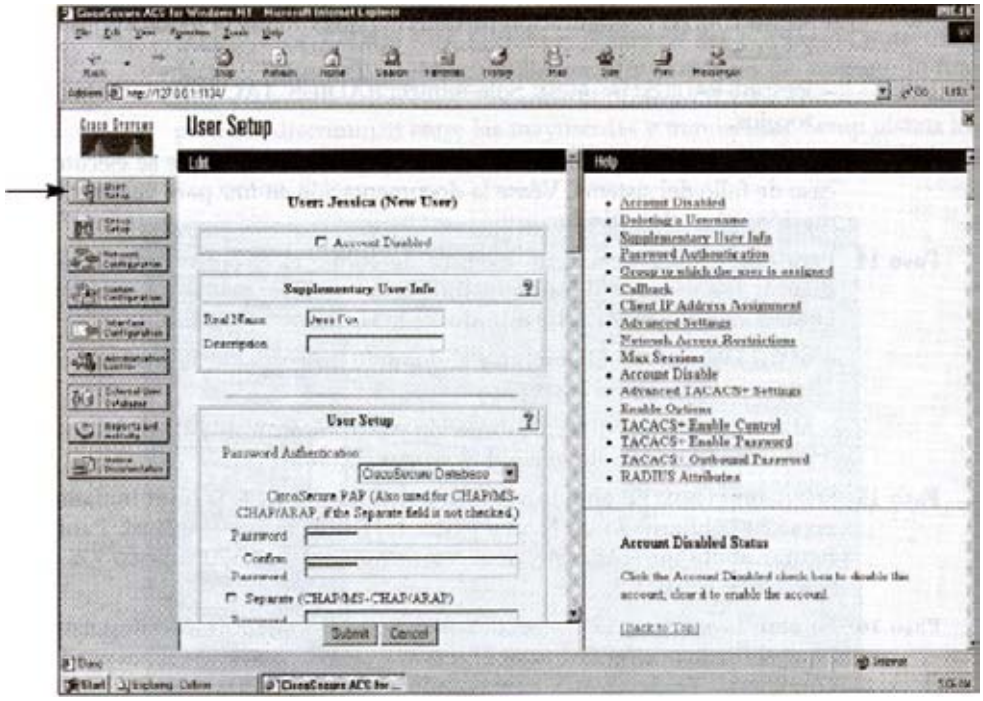


Figura 4.12 Cómo agregar usuarios CSACS-NT.

En la ventana Edit, el administrador puede modificar las siguientes opciones:

- ACCOUNT Disable. Seleccione la casilla de verificación ACCount Disabied para denegar el acceso a este usuario. Observe que debe hacer clic en Submit para que esta acción surta efectos.
- Supplementary User Information (Opcional). Introduzca la siguiente información:
  - Real Name. Si el nombre de usuario no es el verdadero nombre del usuario, introduzca aquí ese nombre.
  - Description. Introduzca una descripción detallada del usuario.

Este elemento puede contener hasta cinco campos configurabas por el usuario. El administrador puede seleccionar interface Configuration en la barra de navegación. Seleccione

User Data Configuration, Coloque una marca de verificación en los números 3, 4 y 5 de Field ID. Con esto se añaden tres User Fields adicionales a la ventana Edit de User Setup.

- User Setup. Modifica o introduzca la siguiente información para el usuario (donde proceda):
  - Password Authentication. Seleccione el tipo de autenticación en el menú desplegable.
  - Cisco Secure Database. Auténtica un usuario desde la base de datos CSACS local.
  - Windows NT. Auténtica a un usuario con una cuenta en la base de datos de usuarios Windows NT ubicada en el mismo equipo que el servidor de Cisco Secure. También existe una entrada en la base de datos CSACS que se usa para otros servicios CSACS. Este tipo de autenticación sólo aparecerá en la interfaz de usuario si esta base de datos de usuarios externos ha sido configurada en External User Databases: Database Configuration.
- Password and Confirm Password. Introduzca y confirme la contraseña del Protocolo de autenticación de contraseña (PAP) que vaya a usar.
- Separate CHAP/MS-CHAP/ARAP. Esta opción no se usa con el firewall PIX.
- Group to which the user is assigned. En este menú desplegable, seleccione el grupo al que vaya a asignar el usuario. El usuario hereda los atributos y las operaciones asignadas al grupo. Por defecto, los usuarios son asignados a Default Group. Los usuarios que se autentiquen a través del método Unknown User que no se encuentren en un grupo existente también serán asignados a Default Group.
- Callback. No se usa con el firewall PIX.
- Client IP Address Assignment. No se usa con el firewall PIX.
- Account Disable. Defina las circunstancias bajo las cuales la cuenta de este usuario quedará desactivada.
- Never. Haga clic para mantener la cuenta del usuario siempre activada. Éste es el valor predeterminado.
- Disable account if. Haga clic para desactivar la cuenta en las circunstancias especificadas en los siguientes campos:

- Date exceeds. En los menús desplegables, seleccione la fecha y la hora en la que desea desactivar la cuenta. El valor predeterminado es de 30 días después de que se agregue el usuario.
- Failed attempts exceed. Haga clic en la casilla de verificación e introduzca el número de intentos consecutivos infructuosos permitidos antes de desactivar la cuenta. El valor predeterminado es de cinco.
- Failed attempts since last successful login. Este contador muestra el número de intentos de inicio de sesión infructuosos desde la última vez que este usuario inició sesión sin éxito.
- Reset current failed attempts count on submit. Si una cuenta está desactivada porque se ha superado el número de intentos fallidos, marque esta casilla de verificación y haga clic en Submit para restablecer el contador de intentos fallidos a 0 y reponer la cuenta.

Haga clic en Submit cuando haya efectuado todas las selecciones.

4.8.5 Cómo configurar la autenticación.

Una vez configurado CSACS, es necesario introducir en la configuración del PIX la correspondiente entrada para el servidor AAA. Existen muchas opciones diferentes que un administrador puede configurar en relación con AAA y el PIX. En primer lugar, hay que crear un grupo AAA y especificar un protocolo de autenticación. A continuación, se crea el servidor AAA y se asigna para que sea parte del grupo AAA. Es posible definir múltiples servidores AAA para que formen parte del mismo grupo AAA. Esto permite el fallo de acceso al servidor. Si no se puede alcanzar el primer servidor AAA, tendrá lugar una petición al próximo servidor AAA definido.

Utilice el comando aaa-server para especificar grupos de servidores AAA. Con el firewall PIX, un administrador puede definir grupos separados de servidores TACACS+ o RADIUS para especificar distintos tipos de tráfico, como un servidor TACACS+ para el tráfico entrante y un servidor TACACS+ distinto para el tráfico saliente. El comando AAA hace

referencia a la etiqueta del grupo para dirigir la autenticación, la autorización y la contabilidad al servidor AAA adecuado.

Un administrador puede tener hasta 16 grupos de etiquetas, y cada grupo puede tener hasta 16 servidores AAA, para que haya un total de hasta 256 servidores TACACS+ 0 RADIUS. Al especificar múltiples servidores AAA, un administrador puede habilitar una reserva en caliente. Cuando un usuario inicia sesión, accede a los servidores uno a uno, empezando por el primer servidor que se especifique en el conjunto de etiquetas, hasta que responda un servidor.

La configuración predeterminada proporciona dos protocolos de servidor AAA. Los dos siguientes parámetros de configuración estarán por defecto en el archivo de configuración.

- aaa-server tacacs+ protocol tacacs+
- aaa-server radius protocol radius

Las versiones antiguas del SO del PIX no requerían la creación de un grupo AAA. La ventaja de que estos dos parámetros sean los parámetros predeterminados es que se crea un grupo predeterminado. Esto significa que cuando se actualiza una versión antigua con una más reciente (que requiere el grupo AAA), no se descartarán los demás comandos AAA.

El firewall PIX utiliza los puertos 1645 y 1646 para RADIUS. Si el servidor RADIUS utiliza los puertos 1812 y 1813, será necesario reconfigurarlo para que use los puertos 1645 y 1646.

La sintaxis del comando aaa-server es la siguiente:

aaa-server etiqueta_grupo (nombre_if) host servidor_ip clave timeout segundos aaa-server etiqueta_grupo protocol protocolo-autenticación.

La tabla 4.3 describe la sintaxis del comando aaa-server.

Parámetro del comando aaa-server	**Descripción**
etiqueta-grupo	Una cadena alfanumérica que es el nombre del grupo del servidor. Utilice la etiqueta del grupo del comando aaa para asociar las instrucciones de comando aaa authentication y aaa accounting con un servidor AAA.
nombre-if	El nombre de la interfaz en la que reside el servidor.
host ip-servidor	La dirección IP del servidor TACACS+ o RADIUS.
Clave	Una palabra clave alfanumérica que discrimina entre las mayúsculas y minúsculas compuesta de hasta 127 caracteres que tiene el mismo valor que la clave del servidor TACACS+. Se omitirán todos los caracteres introducidos más allá de los 127 permitidos La clave se utiliza entre el cliente y el servidor para cifrar los datos que hay entre ellos. La clave deberá ser la misma en los sistemas cliente y servidor. En la clave no se permite que haya espacios, pero sí otros caracteres especiales. Si no se especifica la clave, el cifrado no tendrá lugar.
timeout seconds	Un temporizador de retransmisión que especifica la duración con la que el firewall PIX reintenta el acceso cuatro veces al servidor AAA antes de elegir el siguiente servidor AAA. La configuración predeterminada es de cinco segundos. El máximo es de 30 segundos. Por ejemplo, si el valor de tiempo de espera es de 10 segundos, el firewall PIX retransmitirá durante 10 segundos, y si no recibe acuse de recibo alguno, lo intentará tres veces más para un total de 40 segundos para retransmitir los datos antes de que se seleccione el siguiente servidor AAA.
protocol protocolo-autenticación	El tipo de servidor AAA, tacacs+ o radius.

Tabla 4.3 Descripción del comando aaa-server.

El Ejemplo 4.1 muestra el comando aaa-server. La primera instrucción del ejemplo crea el grupo y asigna el protocolo de autenticación. El nombre del grupo es MYTACACS y el protocolo de autenticación es TACACS+. La segunda instrucción del ejemplo asigna el servidor al grupo MYTACACS, asigna la interfaz con la que el servidor AAA se comunicará con el PIX (en el interior), define la dirección IP del servidor AAA (10.0.0.2), asigna una clave (secretkey), y define un tiempo de espera (10 segundos).

Ejemplo 4.1. Especificación de grupos de servidores AAA.

```
pixfirewall(config)# aaa-server MYTACACS protocol tacacs+
pixfirewall(config)# aaa-server MYTACACS (inside) host 10.0.0.2 secretkey timeout 10
```

Después de configurar el comando aaa-server, es el momento para que el administrador configure authentication. El comando aaa authentication activa o desactiva los servicios de autenticación de usuarios. Cuando un usuario inicia una conexión a través de Telnet, FTP o HTTP, se pide al usuario un nombre de usuario y una contraseña. Un servidor AAA, designado anteriormente con el comando aaa-server, verifica si el nombre de usuario y la contraseña son los correctos.

El comando aaa authentication no está pensado para exigir una norma de seguridad. Los servidores AAA determinan si un usuario puede acceder o no a un sistema, y a qué servicios y direcciones IP. El firewall PIX interactúa con Telnet, FTP y HTTP para mostrar los indicadores de registro. Es posible configurar un PIX para especificar que sólo sea un servicio el que utilice la autenticación, pero éste deberá estar de acuerdo con el servidor AAA para garantizar que tanto el firewall como el servidor están de acuerdo.

El firewall PIX sólo permite un tipo de protocolo de autenticación por red. Por ejemplo, si una red se conecta internamente a través del firewall PIX por medio de TACACS+, la misma red no se podrá conectar internamente a través del firewall PIX por medio de RADIUS; sin embargo, si una red se conecta internamente a través del firewall PIX por medio de TACACS+, una red distinta se podría conectar internamente a través del firewall PIX por medio de RADIUS.

La sintaxis del comando aaa authentication es la siguiente:

aaa authentication include | exclude servicio_autenticación inbound | outbound | nombre_if ip_local máscara_local ip_externa máscara_externa etiqueta_grupo

La tabla 4.4 describe la sintaxis del comando aaa authentication.

Parámetro del comando aaa authentication	**Descripción**
Authentication	Activa o desactiva la autenticación de usuarios, pide al usuario el nombre de usuario y la contraseña, y verifica información con el servidor de autenticación. Cuando se usa con la opción consola, activa o desactiva el servicio de autenticación para que acceda a la consola del firewall PIX sobre Telnet o desde el conector de consola de la unidad de firewall PIX. El uso del comando aaa authentication requiere que se haya configurado el comando aaa-server para designar un servidor de autenticación.
Include	Crea una nueva regla con el servicio especificado a incluir.
exclude	Crea una excepción a una regla declarada previamente excluyendo el servicio especificado de la autenticación con el host especificado. El parámetro exclude mejora la opción except anterior permitiendo al usuario especificar un puerto a excluir con un host o hosts específicos.
Servicio_autenticacíón	La aplicación con la que un usuario está accediendo a una red. Utilice any, ftp, http o telnet. El valor any permite la autenticación de todos los servicios TCP. Para que se pida a los usuarios credenciales de autenticación, éstos deberán usar FTP, HTTP o Telnet (HTTP sirve para la Web y sólo se aplica a los navegadores web que puedan pedir un nombre de usuario y una contraseña).

inbound	Autentica conexiones entrantes. inbound implica que la conexión se origina en la interfaz externa y que se dirige a la interfaz interna.
outbound	Autentica conexiones salientes. Outbound implica que la conexión se origina en la interfaz interna y que se dirige a la interfaz externa.
nombre_if	Nombre de la interfaz desde la cual los usuarios requieren autenticación. Utilice nombre_if en combinación con la dirección ip_local y la dirección ip_externa para determinar dónde se busca el acceso y por parte de quién. La dirección ip_local siempre es la interfaz de nivel de seguridad más alto, mientras que ip_externa siempre se sitúa en el nivel más bajo.
ip_local	La dirección IP del host o red de hosts a autenticar. Esta dirección puede ser establecida a 0 para incluir a todos los hosts y permitir que el servidor de autenticación decida qué hosts se van a autenticar.
máscara_local	Máscara de red de local ip. Especifique siempre un valor de máscara específico. Utilice 0 si la dirección IP es 0. Utilice 255.255.255.255 para un host.
ip_externa	La dirección IP de los hosts que van a acceder a la dirección ip-local. Utilice 0 para incluir a todos los hosts.
máscara_externa	Máscara de red de ip_externa. Especifique siempre un valor de máscara específico. Utilice 0 si la dirección IP es 0. Utilice 255.255.255.255 para un host.
etiqueta_grupo	La etiqueta de grupo que se establece con el comando aaa_server.

Tabla 4.4 Descripción del comando aaa authenticatión.

El Ejemplo 4.2 muestra cómo configurar el comando aaa authentication y enlazar la instrucción con el comando aaa server mediante el nombre de grupo MYTACACS. Toda dirección IP o red que se establezca a 0 será el equivalente de any o de all hosts.

Ejemplo 4.2. Cómo configurar la autenticación AAA y enlazarla con el servidor AAA.

```
pixfirewall(config)# aaa-server MYTACACS protocol tacacs+
pixfirewall(config)# aaa-server MYTACACS (inside) host 10.0.0.2 secretkey timeout 10
pixfirewall(config)# aaa authentication include any inbound 0.0.0.0   0.0.0.0   0.0.0.0   0.0.0.0
MYTACACS
pixfirewall(config)# aaa authentication include telnet outbound 0.0.0.0   0.0.0.0   0.0.0.0   0.0.0.0
MYTACACS
pixfirewall(config)# aaa authentication include ftp dmz 0.0.0   0.0.0.0   0.0.0.0   0.0.0.0
MYTACACS
pixfirewall(config)# aaa authentication exclude any outbound 10.0.0.33     255.255.255.255
0.0.0.0   0.0.0.0  MYTACACS
```

Las opciones include y exclude no son compatibles con las versiones del firewall PIX anteriores a la versión 5.1. Si se retrotrae a una versión anterior, las instrucciones de comando aaa serán eliminadas de la configuración.

4.8.5.1 Autenticación de otros servicios.

El firewall PIX auténtica a los usuarios a través de Telnet, FTP o HTTP. También es posible autenticar otros servicios. Por ejemplo, es posible configurar el PIX de forma que se necesite autenticación para acceder a un servidor de archivos Microsoft en el puerto 139. Cuando los usuarios deseen acceder a servicios que no sean Telnet, FTP o HTTP, tendrán que hacer una de estas cosas:

- Opción 1. Autenticarse primero accediendo a un servidor Telnet, FTP o HTTP antes de acceder a otros servicios.
- Opción 2. Autenticarse frente al servicio Telnet virtual del firewall PIX antes de acceder a otros servicios.

Cuando no haya servidores Telnet, FTP o HTTP frente a los cuales autenticarse, o para simplificar la autenticación del usuario, el firewall PIX tiene una opción de autenticación a través de Telnet o HTTP virtuales. Esto permite al usuario autenticarse directamente con el firewall PIX frente a la dirección IP del Telnet o HTTP virtuales.

4.8.5.2 Telnet virtual.

La opción Telnet virtual proporciona una forma de preautenticar a los usuarios que soliciten conexiones a través del firewall PIX utilizando servicios o protocolos que no soporten la autenticación.

La autenticación del usuario también es general cuando no hay ningún servidor Telnet, FTP o HTTP que lleve a cabo la autenticación. Es posible usar la dirección IP de Telnet virtual para la autenticación de entrada y salida del firewall PIX.

Cuando un usuario no autenticado hace un telnet a la dirección IP virtual, al usuario se le pide un nombre de usuario y una contraseña. Es el servidor TACACS+ o RADIUS el que auténtica al usuario. Una vez autenticado, el usuario ve el mensaje "Authentication Successful" y las credenciales de autenticación son colocadas en la caché del firewall PIX durante el timeout uauth. El firewall PIX restablece entonces la sesión telnet.

Si un usuario desea finalizar la sesión para borrar la entrada de la caché uauth del firewall PIX, el usuario deberá hacer un nuevo telnet a la dirección virtual. Al usuario se le pide un nombre de usuario y una contraseña, el firewall PIX elimina de la caché uauth las credenciales asociadas, y el usuario recibe un mensaje "Logout Successful". El Ejemplo 4.3 muestra un inicio de sesión y una finalización de sesión satisfactorios.

Ejemplo 4.3. Inicio y finalización de sesión satisfactorios.

```
! Authenticating Login

>telnet 192.168.0.5
LOGIN Authentication
Username: aaauser
Password: ********
Authentication Successful

! Authenticating Logout
```

>telnet 192.168.0.5
LOGOUT Authentication
Username: aaauser
Password: ********
Logout Successful

La sintaxis del comando virtual telnet es la siguiente:

virtual telnet dirección-ip

En lo que se refiere al uso saliente de Telnet virtual, la dirección IP deberá ser una dirección enrutada al firewall PIX

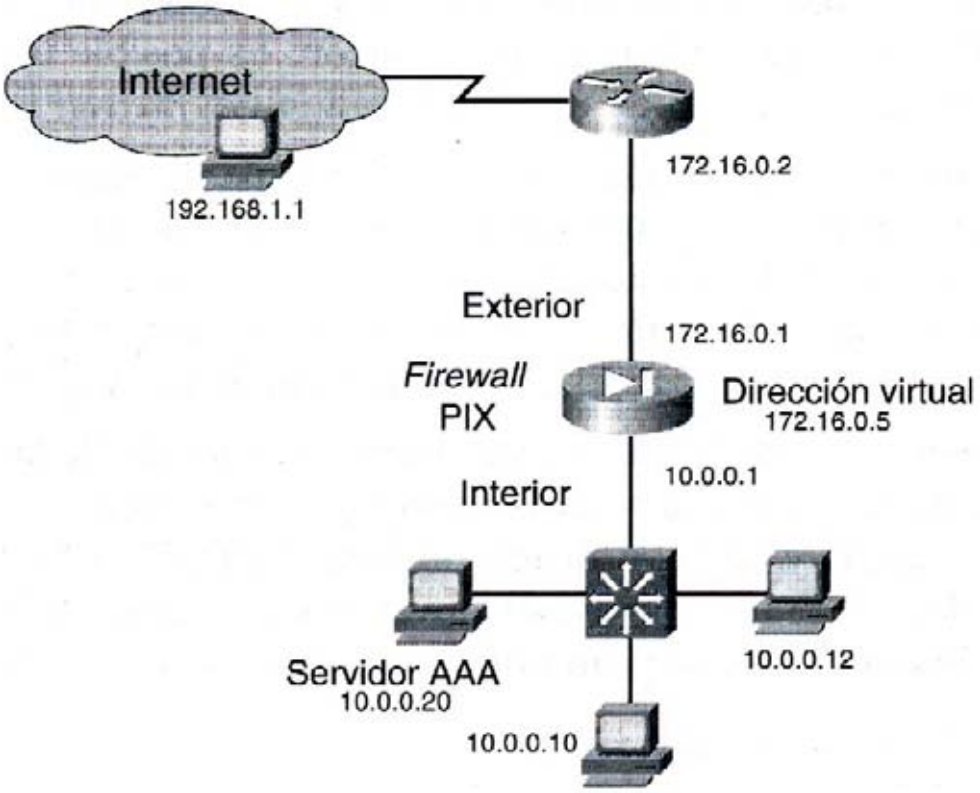


Figura 4.13 Telnet Virtual.

Utilice una dirección que no esté siendo utilizada por ninguna interfaz. En el ejemplo de la figura 4.13, el PIX se configura para pedir autenticación para el acceso saliente del puerto TCP 49. El cliente interno 10.0.0.10 posee un gateway predeterminado que está establecido a la interfaz interna del firewall PIX en 10.0.O.I. La dirección Telnet virtual es 172.16.0.5. El cliente interno, 10.0.0.10, hará Telnet a la dirección virtual 172.16.0.5. El PIX pedirá al cliente que se autentique. Una vez autenticado, se derivará la sesión del cliente con el PIX. El cliente podrá entonces acceder al PIX por medio del puerto TCP 49.

El Ejemplo 4.4 muestra una configuración parcial del PIX.

Ejemplo 4.4. Telnet virtual saliente.

pixfirewall(config)# **ip address outside 172.16.0.1**
pixfirewall(config)# **ip address inside 10.0.0.1**
pixfirewall(config)# **global(outside)l 172.16.0.30-172.16.0.50 netmask 255.255.255.0**
pixfirewall(config)# **nat(inside)l 0 0 0**
pixfirewall(config)# **aaa-server foxserver protocol TACACS+**
pixfirewall(config)# **aaa-server foxserver (inside)host 10.0.0.20 s**ecretkey timeout 10
pixfirewall(config)# **aaa authentication include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 foxserver**
pixfirewall(config)# **aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 foxserver**
pixfirewall(config)# **virtual telnet 172.16.0.5**

Utilizando la misma figura (4.13), un ejemplo de un Telnet virtual saliente podría ser que a un usuario del exterior (192.168.1.1) se le pidiera que accediera al puerto TCP 49 del host interno, 10.0.0.10. 10.0.0.10 está asignado estéticamente a la dirección 172.16.0.25. El cliente, 192.168.1.1, hace primero un telnet a la dirección virtual 172.16.0.5. El PIX le solicita que se autentique. Una vez autenticado, la sesión se cierra. El cliente puede entonces acceder al puerto TCP 49 del host 172.16.0.25 (10.0.0.10).

El Ejemplo 4.5 muestra una configuración parcial del PIX.

Ejemplo 4.5. Telnet virtual entrante.

```
pixfirewall(config)# ip address outside 172.16.0.1
pixfirewall(config)# ip address inside 10.0.0.1
pixfirewall(config)# global(outside)l 172.16.0.30-172.16.0.50 netmask 255.255.255.0
pixfirewall (config)# nat(inside) l 0 0 0
pixfirewall(config)# aaa-server foxserver protocol TACACS+
pixfirewall(config)# aaa-server foxserver   (inside)host 10.0.0.20 secretkey timeout 10
pixfirewall(config)# aaa authentication include telnet inbound 0.0.0.0   0.0.0.0   0.0.0.0   0.0.0.0
foxserver
pixfirewall(config)# aaa authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
foxserver
pixfirewall(config)# virtual telnet 172.16.0.5
pixfirewall(config)# static(inside,outside)172.16.0.25 10.0.0.10 netmask 255.255.255.255   0   0
pixfirewall(config)# conduit permit tcp host 172.16.0.5 eq telnet any
pixfirewall(config)# conduit permit tcp host 172.16.0.25 eq 49 any
```

Es importante recordar que para hacer un telnet a la dirección Telnet virtual, deberá cerrar la sesión Telnet virtual autenticada.

4.8.5.3 HTTP virtual.

Si se pide una autenticación en sitios que estén fuera del PIX, así como en el propio PIX, a veces el navegador puede comportarse de forma poco habitual. Dado que los navegadores colocan en la caché el nombre de usuario y la contraseña, podría parecer que la autenticación no está teniendo lugar. Para evitar esto, un administrador puede implementar HTTP virtual. El navegador apunta a la dirección virtual. Después de que se produzca la autenticación con la dirección IP virtual, el navegador recibe el mensaje "Error: 501 Not Implemented'. En este punto, con el navegador, solicite ir al sitio web de destino más allá del PIX. No habrá reautenticación adicional del PIX durante el timeout uauth.

Con la opción de HTTP virtual, los navegadores web funcionan correctamente con la autenticación HTTP del firewall PIX. El firewall PIX presupone que la base de datos del servidor AAA es compartida con un servidor web y proporciona la misma información automáticamente al servidor AAA y al servidor web. La opción HTTP virtual funciona con el firewall PIX para autenticar al usuario, separar la información del servidor AAA de la petición URL del cliente web y dirigir al cliente web al servidor web. El HTTP virtual redirigirá la conexión inicial del navegador web a una dirección IP, que reside en el firewall PIX, autenticando al usuario y redirigiendo el navegador al URL solicitado originariamente por el usuario. Esta opción se llama así porque accede a un servidor HTTP virtual del firewall PIX, que en realidad no existe.

Esta opción es especialmente útil en el caso de la interoperabilidad del firewall PIX con Microsoft IIS, pero también resulta útil para otros servidores de autenticación. Cuando se usa la autenticación HTTP en un sitio que ejecute Microsoft IIS y que tenga activados "Basic text authentication" o "NT Challenge", el servidor Microsoft IIS podría denegar el acceso a los usuarios. Esto tiene lugar porque el navegador anexa la cadena: "Authorization: Basic=Uuhjksdkflik==" a los comandos HTTP GET. Esta cadena contiene las credenciales de autenticación del firewall PIX. Los servidores Microsoft IIS de Windows NT responden a las credenciales y presuponen que un usuario de Windows NT está tratando de acceder a las páginas privilegiadas del servidor. A menos que la combinación de nombre de usuario y contraseña del firewall PIX sea exactamente la misma que una combinación de nombre de usuario y contraseña válidos de Windows NT del servidor Microsoft IIS, se denegará el comando HTTP GET.

Para resolver este problema, el firewall PIX redirige la conexión inicial del navegador a su dirección IP de HTTP virtual, auténtica al usuario y redirige el navegador al URL solicitado originariamente por el usuario.

Atención: No establezca la duración de timeout uauth a 0 segundos cuando utilice la opción HTTP virtual. Esto impediría que hubiera conexiones HTTP con el verdadero servidor web

La sintaxis del comando virtual http es la siguiente:
virtual http dirección ip [warn].

Para el uso saliente, la dirección IP deberá ser una dirección enrutada al firewall PIX.

En lo que respecta al uso entrante, la dirección IP deberá ser una dirección global no utilizada. Un comando access-list o un par de comandos conduit y static deberán proporcionar acceso a ip_address, así como una instrucción de comandos aaa authentication.

Por ejemplo, como uso saliente, si un cliente interno de 192.168.0.100 posee un gateway predeterminado establecido a la interfaz interna del firewall PIX en 192.168.0. 1, la dirección IP establecida con el comando virtual http podrá ser cualquier dirección IP que no esté siendo utilizada en ese segmento, como 192.168.0.120.

La opción warn alerta a los usuarios del comando virtual http que el comando ha sido redirigido. Esta opción sólo es aplicable a los navegadores basados en texto, en los que el redireccionamiento no puede producirse de forma automática.

4.8.5.4 La autenticación del acceso de consola.

El comando aaa authentication consola puede ser utilizado para requerir que la autenticación acceda a las consolas serie, de activación y Telnet del firewall PIX. Las opciones de la consola serie también registran en un servidor syslog todos los cambios que se realicen a través de la consola serie.

El acceso autenticado a la consola del firewall PIX posee distintos tipos de indicadores, dependiendo de la opción elegida. Mientras que la opción de activación permite que haya tres intentos antes de detenerse con un mensaje de acceso denegado, las opciones serie y Telnet hacen que se le pregunte continuamente al usuario hasta lograr el inicio de sesión.

La autenticación de la consola serie crea una situación potencial de bloqueo si no se contestan las peticiones del servidor de autenticación y el acceso a la consola es necesario para intentar hacer el diagnóstico. Si la petición de inicio de sesión de la consola expira, un usuario puede acceder al firewall PIX desde la consola serie introduciendo el nombre de usuario y la contraseña de activación del firewall PIX. El nombre de usuario del firewall PIX es "pix" si no se puede acceder al servidor TACACS+ o RADIUS.

La longitud máxima de la contraseña para acceder a la consola es de 16 caracteres.

La sintaxis del comando aaa authentication consola es la siguiente:
aaa authentication [serial | enable | telnet] console etiqueta_grupo

La tabla 4.4 describe los parámetros de este comando.

Argumento/Opción de comando	**Descripción**
serial	Pide un nombre de usuario y una contraseña antes del indicador de línea de comandos de la conexión de consola serie.
Enable	Pide un nombre de usuario y una contraseña antes de acceder al modo privilegiado para las conexiones serie o Telnet.
telnet	Obliga al usuario a especificar un nombre de usuario y una contraseña antes del primer indicador de línea de comandos de una conexión de consola Telnet.
Consola	Especifica que el acceso a la consola del firewall PIX solicite la autenticación y, opcionalmente, registra los cambios realizados en la configuración en un servidor syslog.
etiqueta_grupo	La etiqueta de grupo que se establece con el comando aaa-server.

Tabla 4.4 Descripción del comando aaa authentication.

El Ejemplo 4.6 muestra cómo configurar el comando aaa authentication con respecto a la consola.

El comando telnet permite al administrador especificar qué hosts pueden acceder a la consola del firewall PIX con Telnet. Anteriormente al sistema operativo 5.0, el Telnet a la consola del firewall PIX sólo estaba disponible desde la interfaz interna y no desde la interfaz externa. Ahora existe la posibilidad de activar Telnet con el firewall PIX en todas las interfaces. Sin embargo, el firewall PIX obliga a que todo el tráfico Telnet con la interfaz externa esté protegido con IPSec. Por tanto, para activar una sesión Telnet con la interfaz externa, configure IPSec en la interfaz externa para incluir el tráfico IP generado por el firewall PIX y activar telnet

en la interfaz externa. El tráfico de vuelta al cliente Telnet es el único que se envía a través del túnel IPSec, y no todo el tráfico generado por la interfaz externa.

Ejemplo 4.6. Autenticación del acceso de consola.

```
pixfirewall(config)# aaa authentication serial console MYTACACS
pixfirewall(config)# aaa authentication enable console MYTACACS
pixfirewall(config)# aaa authentication telnet console MYTACACS
```

4.8.5.5 Cómo cambiar los tiempos de espera de la autenticación.

Utilice el comando timeout uauth para especificar la duración de la caché posterior a la inactividad de las conexiones de usuario. El valor del comando timeout deberá ser cómo mínimo de dos minutos. Utilice el comando clear uauth para eliminar todas las cachés de autorización de todos los usuarios, lo que les obligará a reautenticarse la siguiente vez que creen una conexión. El comando timeout uauth puede ser establecido a 0 (cero) para desactivar la caché.

La sintaxis del comando timeout uauth es la siguiente:

```
timeout uauth [hh:mm:ssl [absolute | inactivity]
```

La tabla 4.8 describe los parámetros de este comando.

Argumento/Opción de comando	**Descripción**
uauth [hh:mm:ss]	Plazo de expiración de la caché de autenticación y autorización que tiene el usuario para reautenticar la siguiente conexión. Esta duración deberá ser menor que los valores xlate. Establézcala a 0 para desactivar la caché. No la establezca a 0 si se usa FTP pasivo en las conexiones.

Absolute	Ejecuta continuamente el temporizador uauth, pero una vez éste se termina, espera para volver a preguntar al usuario hasta que éste inicia una nueva conexión, como, por ejemplo, cuando hace clic en un vínculo de un navegador web. El temporizador uauth predeterminado es absolute. Para desactivar absolute, establezca el temporizador uauth a 0 (cero).
Inactivity	Inicia el temporizador UaUth cuando una conexión pasa al estado de inactividad.

Tabla 4.5 Descripción del comando timeout uauth.

Los cualificadores inactivity y absolute obligan a los usuarios a reautenticarse transcurrido un periodo de inactividad o una duración absoluta. El temporizador de inactividad se inicia cuando una conexión pasa al estado de inactividad. Si un usuario establece una nueva conexión antes de que expire el temporizador de inactivitidad, el usuario no deberá reautenticarse. Si un usuario establece una nueva conexión una vez expirado el temporizador de inactividad, el usuario deberá reautenticarse.

El temporizador absoluto se ejecuta de forma continua, pero no pregunta al usuario hasta que éste inicia una nueva conexión, como, por ejemplo, cuando hace clic en un vínculo una vez que el temporizador absoluto ha expirado. Si el temporizador expira y el usuario hace clic en un nuevo vínculo, se le pedirá que se reautentique. El temporizador absoluto deberá ser menor que el temporizador xlate; de otro modo, se le podría preguntar al usuario después de haber finalizado su sesión.

El temporizador de inactividad proporciona a los usuarios el mejor acceso a Internet, ya que no se les exige que se reautentiquen de forma regular. Los temporizadores absolutos proporcionan un mayor nivel de seguridad y administran mejor las conexiones del firewall PIX. Cuando se pide a los usuarios que se reautentiquen de forma regular, éstos tienden a administrar mejor el uso de los recursos. Otra ventaja es que cuando se pregunta otra vez, disminuye el riesgo de que alguien trate de usar el acceso de otro usuario si éste abandona su estación de trabajo, como, por ejemplo, una computadora de prácticas de una universidad. La

mejor solución puede ser el uso de un temporizador absoluto durante los picos y un temporizador de inactividad el resto del tiempo.

El temporizador de inactividad y el temporizador absoluto pueden funcionar al mismo tiempo. El temporizador absoluto deberá ser configurado para un periodo más prolongado que el temporizador de inactividad. Si el temporizador absoluto es menor que el temporizador de inactividad, este último no se producirá. Por ejemplo, si el temporizador absoluto se configura a 10 minutos y el de inactividad a una hora, el primero volverá a preguntar al usuario cada 10 minutos, y el segundo nunca se iniciará.

Si el temporizador de inactividad se configura a una duración concreta y el temporizador absoluto a cero, los usuarios serán reautenticados únicamente cuando expire el temporizador de inactividad. Si ambos temporizadores son establecidos a cero, los usuarios tendrán que reautenticarse en cada nueva conexión.

No establezca la duración de timeout uauth a 0 segundos cuando utilice la opción HTTP virtual, ya que esto impide que haya conexiones HTTP con el verdadero servidor web (de destino).

El Ejemplo 4.7 muestra la configuración de los periodos de tiempo de espera de los temporizadores absoluto y de inactividad.

Ejemplo 4.7. Configuración de los periodos de tiempo de espera

```
pixfirewall(config)# timeout uauth 3:00:00 absolute
pixfirewall(config)# timeout uauth 0:30:00 inactivity
```

4.8.5.6 Cómo cambiar la petición de autenticación.

Utilice el comando auth-prompt para crear un texto de desafío AAA para el acceso HTTP, FTP y Telnet. Este texto muestra en la parte superior las peticiones de nombre de usuario y contraseña cuando se inicia sesión. También es posible cambiar el texto de rechazo y aceptación de la autenticación.

La sintaxis del comando auth-prompt es la siguiente:

auth-prompt [accept | reject | prompt] *cadena*

La tabla 4.6 describe los parámetros de este comando.

Argumento/Opción de comando	**Descripción**
Accept	Si una autenticación de usuario a través de Telnet es aceptada, se muestra la cadena de petición.
Reject	Si una autenticación de usuario a través de Telnet es rechazada, se muestra la cadena de petición.
Prompt	La cadena de petición de desafío AAA sigue a esta palabra clave. Esta palabra clave es opcional por la compatibilidad retrospectiva.
Cadena	Una cadena de hasta 235 caracteres alfanuméricos. No conviene usar caracteres especiales; sin embargo, los espacios y los signos de puntuación están permitidos. Introduciendo un signo de interrogación o pulsando la tecla Intro se termina la cadena (el signo de interrogación aparece en la cadena).

Tabla 4.6. Descripción del comando auth-prompt

El Ejemplo 4.8 muestra las tres peticiones de autenticación.

Ejemplo 4.8. Cómo cambiar la petición de autenticación.

pixfirewall(config)# auth-prompt prompt Please Authenticate to the Firewall

pixfirewall(config)# auth-prompt reject Authentication Failed, Try Again
pixfirewall(config)# auth-prompt accept You 've been Authenticated

NOTA

Microsoft Internet Explorer muestra hasta 37 caracteres en una petición de autenticación, Netscape Navigator hasta 120 caracteres, y Telnet y FTP hasta 235 caracteres.

4.8.6 Cómo configurar la autorización.

El firewall PIX utiliza los servicios de autorización TACACS+ con un servidor de control de acceso para determinar a qué servicios puede acceder un usuario autenticado. En lo que respecta a la autorización de FTP, Telnet y HTTP, es posible usar el nombre de la aplicación en el comando aaa authorization. Es importante recordar que los servicios no especificados están autorizados de forma implícita. Si la intención es la de crear una excepción a una regla declarada con anterioridad, utilice el parámetro exclude.

La sintaxis del comando aaa authorization es la siguiente:

aaa authorization include | **exclude** *servicio-autorización* **inbound** | **outbound** | *nombre_if ip_local máscara_local ip_externa máscara_externa*

La tabla 4.9 describe los parámetros de este comando.

Argumento/Opción de comando	***Descripción***
authorization	Activa o desactiva la autorización TACACS+ para los servicios. El servidor de autenticación determina a qué servicios puede acceder el usuario.
include	Crea una nueva regla con el servicio especificado a incluir.

exclude Crea una excepción a una regla previamente declarada excluyendo el servicio especificado de la autenticación, autorización o contabilidad del host especificado. El parámetro exclude mejora la opción except anterior permitiendo al usuario especificar un puerto a excluir de un host o hosts específicos.

servicio_autorizacíón Los servicios que requieren autorización. Utilice any, ftp, http, telnet o protocolo/puerto. Los servicios que no estén especificados se autorizarán de forma implícita. Los servicios que estén especificados en el comando aaa authentication no afectarán a los servicios que requieran autorización.

Para protocolo/puerto:

protocolo. El protocolo (6 para TCP, 17 para UDP, 1 para ICMP, etc.). puerto. El puerto o intervalo de puertos TCP o UDP de destino. El puerto también puede ser el tipo ICMP; es decir, 8 para el eco ICMP o ping. Un valor de puerto de 0 (cero) significa todos los puertos. Los intervalos de puerto sólo se aplican a los protocolos TCP y UDP, y no a ICMP. En lo que respecta a los protocolos que no sean TCP, UDP e ICMP, el puerto no es aplicable y no deberá utilizarse. A continuación vemos una especificación de puerto de ejemplo.

aaa authorization include udp/53-1024 inside 0 0 0 0

servício_autorización Este ejemplo concede autorización para búsquedas DNS a la interfaz interna para todos los clientes, y sólo autoriza el acceso a cualquier otro servicio que tenga los puertos situados en el intervalo entre 53 y 1024.

La especificación de un intervalo de puertos puede generar resultados inesperados en el servidor de autorización. El firewall PIX envía el intervalo de puertos al servidor como cadena esperando que el servidor los analice sintácticamente como puertos específicos. No todos los servidores hacen esto. Además, la intención podría ser la de autorizar a usuarios de servicios específicos, lo que no se producirá si se acepta un intervalo.

inbound	Autentica o autoriza conexiones entrantes. inbound significa que la conexión se origina en la interfaz externa y que se dirige a la interfaz interna.
outbound	Autentica o autoriza conexiones salientes. outbound significa que la conexión se origina en la interfaz interna y que se dirige a la interfaz externa.
nombre_if	Nombre de interfaz desde la cual los usuarios requieren autenticación. Utilice nombre_if en combinación con la dirección ip_local y la dirección ip_externa para determinar dónde se busca el acceso y por parte de quién. La dirección ip_local siempre está en el nivel de seguridad más alto, mientras que ip_externa siempre está en el más bajo.
ip_local	La dirección IP del host o red de hosts que se va a autenticar o autorizar. Esta dirección podría establecerse a 0 para incluir a todos los hosts y permitir que sea el servidor de autenticación el que decida qué hosts se van a autenticar.
máscara_local	Máscara de red de local ip. Especifique siempre un valor de Máscara específico. Utilice 0 si la dirección IP es 0. Utilice 255.255.255.255 para un host.
ip_externa	La dirección IP de los hosts que van a acceder a la dirección ip_local. Utilice 0 para incluir a todos los hosts.
máscara_externa	Máscara de red de ip_externa. Especifique siempre un valor de máscara específico. Utilice 0 si la dirección IP es 0. Utilice 255.255.255.255 para un host

Tabla 4.9 Descripción del comando aaa authorization

El Ejemplo 4.9 muestra un ejemplo de los parámetros include y exclude.

Ejemplo 4.9. Autorización enable.

pixfirewall(config)# aaa authorization include ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS

pixfirewall(config)# aaa authorization exclude ftp outbound 10.0.0.33 255.255.255.255 0.0.0.0 0.0.0.0 MYTACACS

4.8.6.1 Cómo agregar una regla de autorización a CSACS-NT.

En CSACS se puede conceder a un grupo concreto el acceso exclusivo a un servicio. Si, por ejemplo, de lo que se trata es de que un usuario sólo sea autorizado para FTP, tendrá que seguir estos pasos en el CSACS (véase la figura 4.14) y el usuario deberá formar parte del grupo que se esté modificando.

Paso 1 En la barra de navegación, seleccione Group Setup. Se abre la ventana Group Setup.
Paso 2 Seleccione el grupo a modificar y seleccione Edit Settings.
Paso 3 Desplácese por Group Setup hasta IOS Commands.
Paso 4 Seleccione IOS Commands colocando una marca de verificación en el cuadro que hay junto a IOS Commands.
Paso 5 En Unmatched Cisco IOS commands, seleccione Deny.
Paso 6 Seleccione Command colocando una marca de verificación en el cuadro que hay junto a Command.
Paso 7 Introduzca el servicio permitido en el cuadro que hay debajo de Command: ftp.
Paso 8 Deje el campo Arguments vacío.
Paso 9 Seleccione Permit (Unlisted arguments).
Paso 10 Haga clic en Submit para agregar más reglas, o haga clic en Submit + Restart cuando termine.

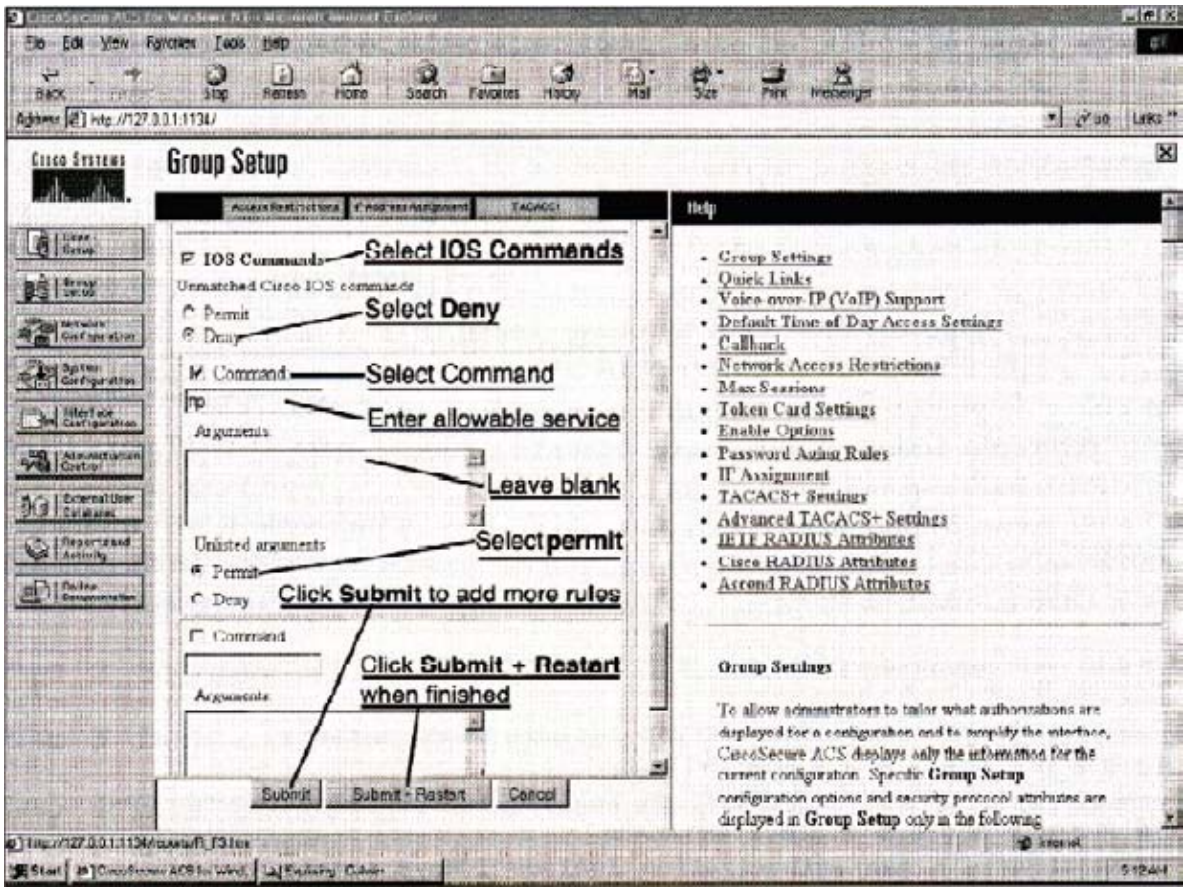


Figura 4.14 Reglas de autorización que permite servicios específicos.

Si de lo que se trata es de que sólo se autorice al usuario a que haga FTP a dos direcciones IP de destino específicas (172.27.27.45 y 10.1.1.10), habrá que dar estos pasos dentro del CSACS (utilice la figura 4.15 para ver este ejemplo) y el usuario deberá formar parte del grupo que se esté modificando.

Paso 1 En la barra de navegación, seleccione Group Setup. Se abre la ventana Group Setup.

Paso 2 Seleccione el grupo a modificar y seleccione Edit Settings.

Paso 3 Desplácese por Group Setup hasta IOS Commands.

Paso 4 Seleccione IOS Commands colocando una marca de verificación en el cuadro que hay junto a IOS Commands.

Paso 5 En Unmatched Cisco IOS commands, seleccione Deny.

Paso 6 Seleccione Command colocando una marca de verificación en el cuadro que hay junto a Command.

Paso 7 Introduzca el servicio permitido en el cuadro que hay debajo de Command: ftp.

Paso 8 En el campo Arguments, introduzca las direcciones IP de destino permitidas:

permit 172.27.27.45

permit 10.1.1.10

Paso 9 En los argumentos Unlisted, seleccione Deny.

Paso 10 Haga clic en Submit para agregar más reglas, o haga clic en Submit + Restart cuando haya terminado.

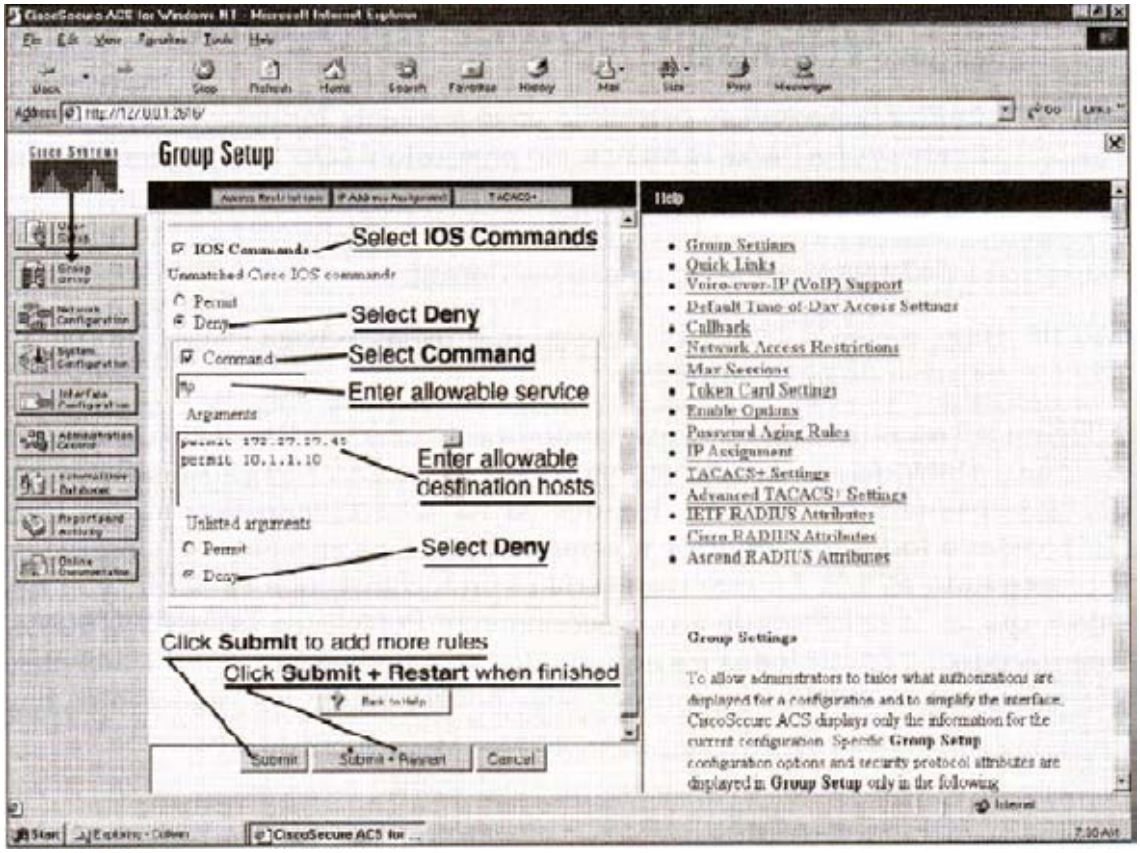


Figura 4.15 Reglas de autorización que dan servicio a hosts específicos.

4.8.6.2 Autorización de otros servicios.

Para autorizar servicios que no sean Telnet, FTP o HTTP, la sintaxis del comando aaa authorization es algo distinta. Para autorizar Telnet, FTP o HTTP, es posible usar el nombre de la aplicación. Para autorizar otros servicios, es necesario especificar el número de protocolo y de puerto. Éste se especifica en el formato protocolo/puerto. Cuando especifique el protocolo,

utilice el número de protocolo, como 6 para TCP, 17 para UDP y 1 para ICMP. Cuando especifique el puerto, utilice el número de puerto que se especifica en la RFC 1700, como 23 para Telnet y 25 para SMTP. Para el protocolo ICMP, utilice el tipo de mensaje en vez del número de puerto. El puerto no se usa para los protocolos que no sean TCP, UDP e ICMP. El Ejemplo 4.10 muestra el uso del comando aaa authorization

Ejemplo 4.10. Autorización del tráfico que no es Telnet, FTP o http.

pixfirewall(config)# aaa authorization include udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS

pixfirewall(config)# aaa authorization include tcp/30-100 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS

pixfirewall(config)# aaa authorization include icmp/8 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS

La primera línea del Ejemplo 4.10 autoriza el acceso a todas las aplicaciones UDP (designadas por Udp/O). La segunda línea del Ejemplo 4.10 autoriza los puertos TCP 30 a 100 (que vienen designados por tcp/30-100). Sólo es posible especificar intervalos de puerto para los protocolos TCP y UDP.

La tercera línea del Ejemplo 4.10 autoriza solicitudes de eco ICMP (designadas por icmp/8, una solicitud de eco es del tipo 8).

Para configurar reglas de autorización para servicios específicos que no sean Telnet, FTP o http en el CSACS para NT, siga estos pasos:

Paso 1 En la barra de navegación, seleccione Group Setup. Se abre la ventana Group Setup.
Paso 2 Seleccione el grupo a modificar y seleccione Edit Settings.
Paso 3 Desplácese en Group Setup hasta IOS Commands.
Paso 4 Seleccione IOS Commands colocando una marca de verificación en el cuadro que hay junto a IOS Commands.

Paso 5 En Unmatched Cisco IOS commands, seleccione Deny.

Paso 6 Seleccione Command colocando una marca de verificación en el cuadro que hay junto a Command.

Paso 7 Introduzca el servicio permitido en el siguiente formato: protocolo/puerto (donde protocolo es el número de protocolo y puerto el número de puerto).

Paso 8 Deje el campo Arguments vacío.

Paso 9 En Unlisted arguments, seleccione Permit.

Paso 10 Haga clic en Submit para agregar más reglas, o haga clic en Submit + Restart cuando haya terminado.

La figura 4.16 muestra cómo hay que configurar la ventana Group Setup del CSACS. Al seleccionar Deny dentro de Unmatched Cisco IOS commands, los usuarios podrán acceder únicamente a los servicios listados (si ha seleccionado Permit, los usuarios podrán acceder a todos los servicios no enumerados específicamente). Observe que el servicio permitido es 1/8. En este caso sería el protocolo 1, que es ICMP, y el tipo de mensaje 8, que es la solicitud de eco. Seleccionando Permit (en Unlisted arguments), los usuarios pueden emitir todos los argumentos no enumerados específicamente (si se hubiera seleccionado Deny, los usuarios sólo podría emitir los argumentos enumerados).

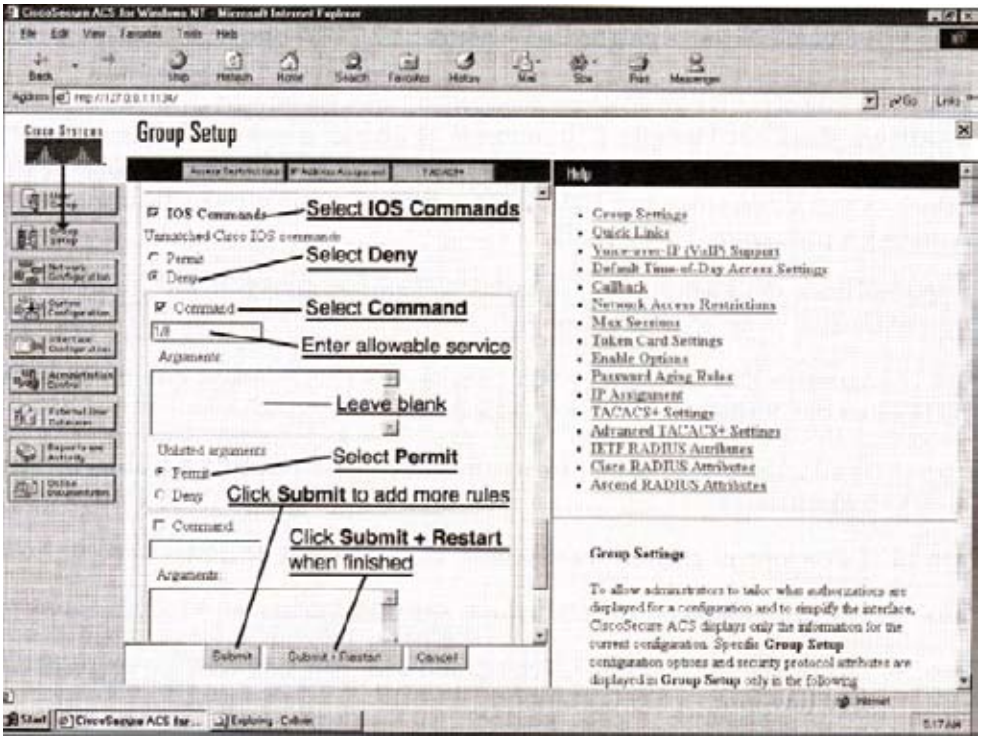


Figura 4.16 Autorización del tráfico que no es Telnet, FTP o http en CSACS-NT.

4.8.7 Cómo configurar la contabilidad.

Una vez configuradas la autenticación y la autorización, suele ser necesario configurar también la contabilidad. La información sobre contabilidad puede utilizarse para hacer un seguimiento de quién está accediendo a un *host* o aplicación específicos. Los registros de contabilidad pueden reflejar el tiempo que el usuario está conectado. También pueden mostrar la cantidad de información que se transmite y recibe. Esta información puede utilizarse con fines de facturación.

La sintaxis del comando aaa accounting es la siguiente:

aaa accounting include | exclude servicio_contabilidad **inbound | outbound |** nombre_if ip_local máscara_local ip_externa máscara_externa etiqueta_grupo

La tabla 4.10 describe los parámetros de este comando:

Argumento/Opción de comando	***Descripción***
accounting	Activa o desactiva servicios de contabilidad con el servidor de autenticación. El uso de este comando requiere haber configurado previamente el comando aaa-server para designar un servidor de autenticación.
include	Crea una nueva regla con el servicio especificado a incluir.
exclude	Crea una excepción a una regla declarada con anterioridad excluyendo el servicio específico de la autenticación, autorización o contabilidad del *host* especificado. El parámetro exclude mejora la opción anterior except permitiendo al usuario especificar un puerto a excluir de un *host o hosts especí*ficos.
Servicio_contabilidad	El servicio de contabilidad. Este servicio se facilita a todos los servicios, si bien el administrador puede limitarlo a uno o más servicios. Los valores posibles son any, ftp, http, telnet o *protocolo/puerto.* Utilice any para proporcionar contabilidad a todos los servicios TCP. Para proporcionar contabilidad a los servicios

	UDP, utilice la forma *protocolo/puerto.* En lo que respecta a *protocolo/puerto,* el protocolo TCP aparece como 6, el protocolo UDP como 17, etc. *puerto* es el puerto de destino TCP o UDP. Un valor de puerto de 0 (cero) incluye a todos los puertos. En lo que respecta a protocolos que no sean TCP ni UDP, el puerto no es aplicable y no se debe usar.
inbound	Autentica o autoriza conexiones entrantes. inbound implica que la conexión se origina en la interfaz externa y que se dirige a la interfaz interna.
outbound	Autentica o autoriza conexiones salientes. outbound significa que la conexión se origina en la interfaz interna y que se dirige a la interfaz externa.
nombre_if	Nombre de la interfaz desde la cual los usuarios requieren autenticación. Utilice *nombre_if* en combinación con la dirección *ip_local* y la dirección *ip_externa* para determinar dónde se busca el acceso y por parte de quién. La dirección ip_local siempre está en la interfaz de nivel de seguridad más alto, mientras que *ip_externa* siempre está en el nivel más bajo.
ip_local	La dirección IP del *host* o red de *hosts* que se va a autenticar o autorizar. Puede establecerse a 0 para incluir a todos los *hosts* y permitir que sea el servidor de autenticación el que decida qué *hosts* se van a autenticar.
máscara_local	Máscara de red de ip_local. Especifique siempre un valor de máscara específico. Utilice 0 si la dirección IP es 0. Utilice 255.255.255.255 para un host.
ip_externa	La dirección IP de los hosts que van a acceder a la dirección ip_local. Utilice 0 para incluir a todos los hosts.
máscara_externa	Máscara de red de ip_externa. Especifique siempre un valor de máscara específico. Utilice 0 si la dirección IP es 0. Utilice 255.255.255.255 para un host.
Etiqueta_grupo	La etiqueta de grupo que se establece con el comando aaa-server.

Tabla 4.10. Descripción del comando aaa accounting.

El Ejemplo 4.11 muestra dos usos del comando aaa accounting. El primer ejemplo muestra un requisito para contabilizar todo el tráfico saliente autenticado. La segunda instrucción configura una exclusión de contabilidad para la dirección IP específica 10.0.0.33

Ejemplo 4.11. Cómo configurar la contabilidad AAA.

pixfirewall(config)# **aaa accounting include any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS**
pixfirewall(config)# **aaa accounting exclude any outbound 10.0.0.33 255.255.255.255 0.0.0.0 0.0.0.0 MYTACACS.**

La primera instrucción muestra un requisito para contabilizar todo el tráfico saliente autenticado. La segunda instrucción configura una exclusión de contabilidad para la dirección IP específica 10.0.0.33.

4.8.7.1 Cómo ver registros de contabilidad con CSACS-NT.

Siga estos pasos para ver los registros de contabilidad después de haber activado la contabilidad en el PIX y una vez instalada la aplicación CSACS.

Paso 1 En la barra de navegación, seleccione Reports and Activity.

Paso 2 En Reports, seleccione primero TACACS+ Accounting y luego TACACS+ Accounting active.csv, encuadrados bajo Select a TACACS+ Accounting file, para mostrar los registros de contabilidad, como se ve en la figura 4.17.

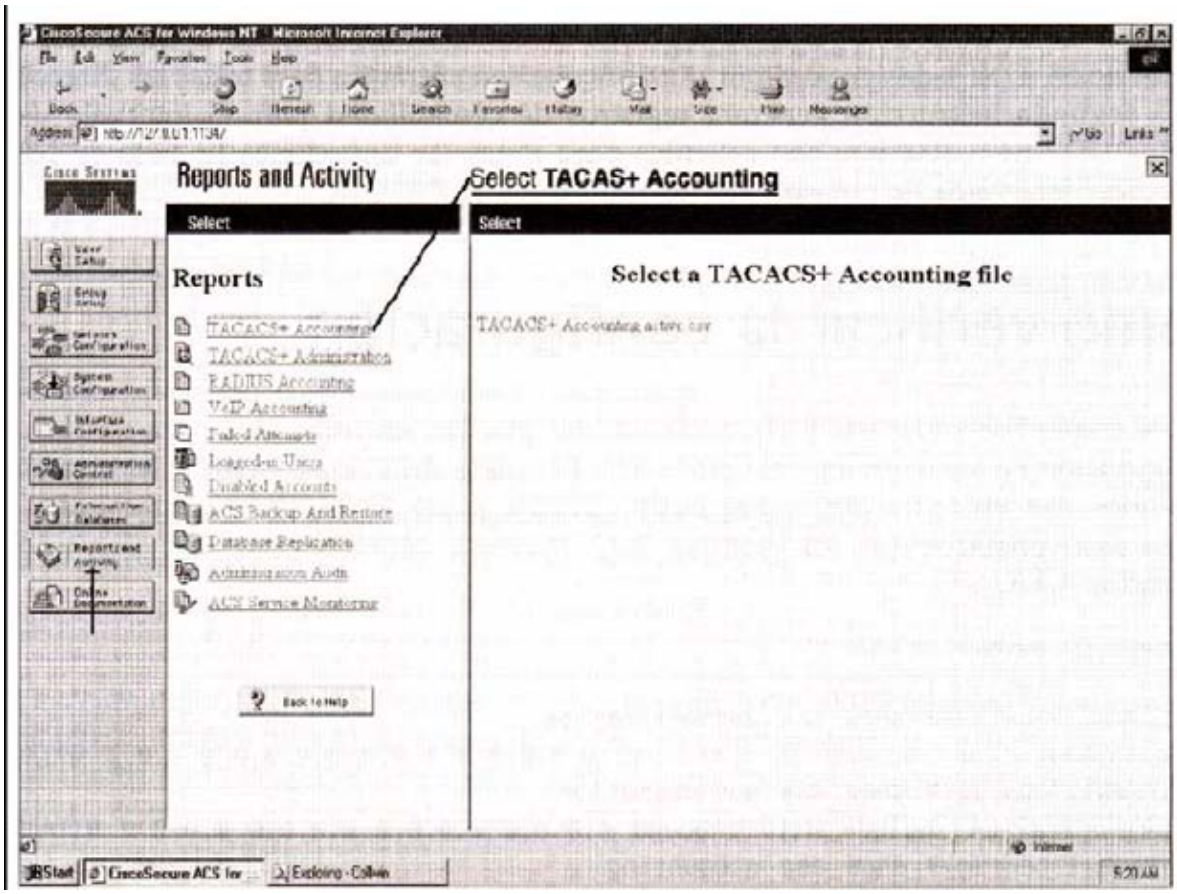


Figura 4.17 Cómo ver registros de contabilidad.

4.8.7.2 Contabilidad de otros servicios.

Cuando se configura aaa accounting para el tráfico que no sea Telnet, FTP o HTTP, la sintaxis del comando será algo distinta a la del tráfico específico Telnet, FTP o HTTP. Al igual que ocurre con aaa authorization, cuando se configuran la contabilidad para Telnet, FTP o HTTP, es posible usar el nombre de la aplicación. Cuando se configuran servicios de contabilidad que no sean Telnet, FTP o HTTP, la sintaxis de *servicio_contabilidad se* especificará en el formato *protocolo/puerto.* Cuando especifique el protocolo, utilice el número de protocolo, como 6 para TCP y 17 para UDP. Cuando especifique el puerto, utilice el número de puerto especificado en la RFC 1700, como 23 para Telnet y 25 para SMTP. El puerto no se usa para los protocolos que no sean TCP y UDP.

El ejemplo 4.12 muestra un ejemplo de la configuración de la contabilidad AAA del tráfico no procedente de Telnet, FTP o http.

Ejemplo 4.12. Cómo configurar la contabilidad AAA para el tráfico no procedente de Telnet, FTP o http.

pixfirewall(config)# aaa accounting include udp/53 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS
pixfirewall(config)# aaa accounting include udp/54-100 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS.

La primera instrucción generará registros de contabilidad para las aplicaciones UDP del puerto 53 (DNS), designadas por udp/53, que son entrantes para todas las direcciones IP. La segunda instrucción generará registros de contabilidad para el intervalo de los puertos UDP 54 a 100, que son salientes para todas las direcciones IP. Sólo es posible especificar intervalos de puerto para los protocolos TCP y UDP

4.8.8 Cómo verificar la configuración

Los comandos show aaa y show aaa-server pueden ser utilizados para confirmar la configuración de los distintos comandos aaa. La salida del comando show aaa repasa los comandos aaa authentication, aaa authorization y aaa accounting configurados que hayan sido introducidos. El ejemplo 4.13 muestra cómo revisar uno por uno los comandos AAA.

Ejemplo 4.13. Revisión de AAA.

pixfirewall(config)# **show aaa authentication**
aaa authentication include http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 **MYTACACS**
pixfirewall(config)# **show aaa authorization**
aaa authorization include http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 **MYTACACS**
pixfirewall(config)# **show aaa accounting**
aaa accounting include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 **MYTACACS**
pixfirewall(config)# **show aaa**

aaa authentication include http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS
aaa authentication telnet console **MYTACACS**
aaa authorization include http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 **MYTACACS**
aaa accounting include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 **MYTACACS**

El comando Show aaa-server detalla los comandos aaa-server configurados, como se muestra en el ejemplo 4.14. Las dos primeras líneas son los parámetros predeterminados de la configuración PIX.

Ejemplo 4.14. Revisión de AAA.

pixfirewall(config)# **show aaa-server**
aaa-server **TACACS+** protocol tacacs+
aaa-server **RADIUS** protocol radius
aaa-server **MYTACACS** protocol tacacs+
aaa-server **MYTACACS** (inside) host **10.1.1.4** secretkey timeout **5**

Para eliminar los comandos aaa authentication, aaa authorization y aaa accounting, utilice los comandos no aaa authentication y no aaa accounting. La autenticación no aaa authentication eliminará los comandos aaa authorization correspondientes. El comando clear aaa también eliminará de la configuración las instrucciones del comando aaa.

Para eliminar el comando aaa-server MYTACACS (inside) host 10.1.1.4 secretkey timeout 5, utilice el comando no aaa-server MYTACACS (inside) host 10.1.1.4 secretkey timeout 5.

Para eliminar el comando aaa-server MYTACACS protocol tacacs+, utilice el comando clear aaa-server MYTACACS protocol tacacs+.

Para poder verificar el comando auth-prompt configurado con anterioridad, es posible emitir el comando show auth-prompt, tal y como muestra el ejemplo 4.15.

Ejemplo 4.15. Verificación de las peticiones de autorización.

pixfirewall(config)# **show auth-prompt.**

auth-prompt prompt prompt Authenticate to the Firewall
auth-prompt prompt accept You 've been Authenticated
auth-prompt prompt reject Authentication Failed.

Dos comandos show adicionales son el comando show timeout uauth y el comando show virtual [http | telnet]. El comando show timeout muestra los valores del temporizador uauth (autenticación de usuario) activos para todos los usuarios autenticados. El comando show virtual http y el comando show virtual telnet muestra la configuración de HTTP virtual y Telnet virtual.

El ejemplo 4.16 muestra una salida de ejemplo de cada comando.

Ejemplo 4.16. Verificación de las peticiones de autorización.

pixfirewall(config)# **show virtual**.

virtual http 192.168.0.2

virtual telnet 192.168.0.2

pixfirewall(config)# **show timeout uauth**

timeout uauth 3:00:00 absolute uauth 0:30:00 inactivity

Dentro del comando show timeout, timeout uauth 3:00:00 muestra la duración (en horas:minutos:segundos) antes de que expire la caché de autenticación y autorización. En este ejemplo, es de tres horas.

absolute uauth 0:30:00 hace que el PIX ejecute continuamente el temporizador uauth, pero cuando el temporizador expira (en este caso, transcurridos 30 minutos), espera a volver a preguntar al usuario hasta que éste inicia una nueva conexión, como, por ejemplo, cuando hace clic en un enlace con un navegador web. El temporizador uauth predeterminado es absolute. Para desactivar absolute, establezca el temporizador uauth a 0 (cero).

El parámetro inactivity indica que el PIX deberá iniciar el temporizador uauth después de que una conexión se vuelva inactiva.

4.9 Manejo Avanzado de Protocolos y protección ante ataque en un firewall PIX.

La manipulación avanzada de protocolos se lleva a cabo a través de un mecanismo llamado protocolo de reparación. El cual actúa haciendo un seguimiento del canal de control de una aplicación para evitar las violaciones de protocolos y permitir que el PIX responda dinámicamente a una necesidad legítima de un protocolo de abrir de forma segura una conexión entrante hacia una excepción temporal en el ASA. Cuando la excepción ya no es necesaria, el protocolo de reparación se cierra.

4.9.1 La necesidad de la manipulación avanzada de protocolos.

Un buen firewall debe inspeccionar los paquetes que hay sobre la capa de red y llevar a cabo las siguientes operaciones en función de lo que requiera el protocolo o la aplicación:

- Abrir y cerrar de forma segura direcciones IP o puertos negociados para las conexiones cliente / servidor legitima a través del firewall.
- Utilizar las instancias de Traducción de direcciones de red NAT de las direcciones IP que hay dentro de un paquete.
- Utilizar las instancias Traducción de direcciones de puerto PAT de los puertos que hay dentro de un paquete.

4.9.1.1 FTP Estándar o clásico.

Utiliza dos canales para la comunicación: cuando un cliente protegido por un firewall inicia una conexión FTP desde su host, abre un canal TCP estándar desde uno de sus puertos de orden superior (TCP>1023) hasta el puerto TCP 21 de destino del servidor externo. Esta conexión recibe el nombre de canal de control. Cuando el cliente solicita datos del servidor, le indica que envíe los datos a un puerto concreto de orden superior. El servidor acusa recibo de la petición e inicia una conexión entrante desde su propio puerto 20 hasta el puerto de orden superior solicitado por el cliente. Esta conexión se denomina canal de datos.

El firewall administra FTP para las conexiones salientes y entrantes de la siguiente forma:

- Conexión saliente: Cuando el cliente solicita datos, el firewall PIX abre un conducto entrante temporal que sirve para permitir el canal de datos del servidor. Este conducto se cierra inmediatamente después de que los datos hayan sido enviados.
- Conexión entrante: Si hay un conducto que permita las conexiones entrantes a un servidor FTP, y si todo el tráfico TCP saliente se permite de forma implícita, no es necesario que haya una administración especial, ya que el servidor inicia el canal de datos desde el interior.

La figura 4.18 muestra el intercambio de señales TCP de tres vías y el establecimiento del canal de control FTP (puerto TCP 21).

Figura 4.18 Transacciones FTP cliente/servidor estándar.

4.9.1.2 FTP pasivo.

FTP pasivo también utiliza dos canales para las comunicaciones. El canal de control funciona igual que en una conexión FTP estándar, pero la configuración del canal de datos funciona de forma distinta. Cuando solicita datos del servidor, el cliente le pregunta al servidor si acepta conexiones PASV. Si las acepta, enviará al cliente un número de puerto de orden superior para que lo utilice en el canal de datos. A continuación, el cliente iniciará la conexión de datos desde su puerto de orden superior hasta el puerto enviado por el servidor.

La figura 4.19 muestra las transacciones entre el cliente y el servidor con el FTP pasivo. La mayoría de los navegadores web utilizan por defecto el FTP pasivo.

En lo que respecta al tráfico FTP pasivo, el firewall PIX se comporta de la siguiente gorma en le caso de las conexiones PASV entrantes y salientes:

- Conexión PASV saliente: Si se permite de forma implícita todo el tráfico TCP saliente, no será necesario que haya una administración especial, ya que será el cliente el que inicie los canales de comando y de datos desde el interior. Si no se permite de forma implícita todo el tráfico TCP saliente, el firewall PIX abrirá un conducto temporal para el canal de datos desde el cliente. Este conducto se cierra después que los datos hayan sido enviados.
- Conexión PASV entrante: Si existe un conducto que permite las conexiones de control FTP entrantes con un servidor PFTP, el firewall abrirá un conducto entrante temporal para el canal de datos iniciado por el cliente. Este conducto se cierra inmediatamente de que los datos hayan sido enviados.

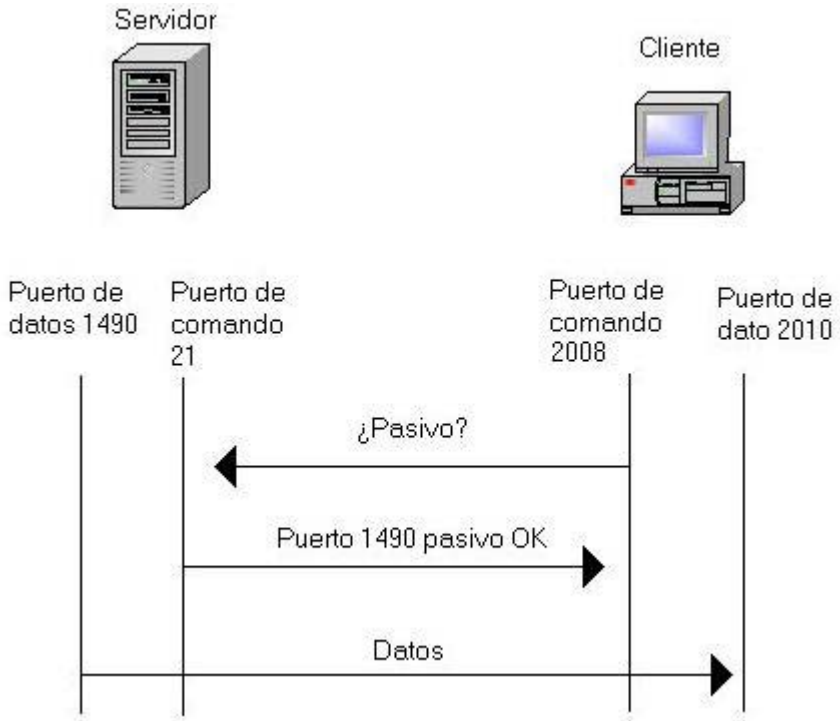


Figura 4.19 Transacciones FTP cliente/servidor pasivas.

4.9.1.3 Comando fixup protocol FTP.

La sintaxis del comando fixup protocol ftp es la siguiente:

Fixup protocol ftp puerto [-puerto] [strict]

Donde puerto [-puerto] es el puerto o intervalo de puertos que el firewall PIX inspeccionará para las conexiones FTP, la opción **strict** hace que el comando exiga que cada petición FTP acuse recibo antes que se permita un nuevo comando, e impide que los navegadores web incrusten comandos en las peticiones FTP.

El comando fixup protocol ftp permite que el firewall PIX realice en el puerto indicado las siguientes operaciones para el tráfico FTP:

- Implementar NAT o PAT en la sobrecarga de paquetes.
- Crear dinámicamente conductos para las conexiones de datos FTP.

- Registrar comandos FTP.

El uso del comando clear fixup protocol ftp sin argumentos hace que el firewall PIX borre todas las asignaciones fixup protocol ftp anteriores y establezca el puerto 21 como valor predeterminado.

4.9.1.4 Shell Remoto (rsh).

El demonio rsh se ejecuta en un host UNIX o Windows proporciona utilidades de ejecución remota con una autenticación basada en números de puertos privilegiados desde hosts de confianza. Principalmente el demonio comprueba la dirección IP y el puerto de origen del cliente. El puerto de origen deberá situarse en el intervalo entre 512 y 1023, si no se cumple el servicio deberá cancelar la conexión.

Posteriormente se crea una segunda conexión desde el demonio rsh hasta el puerto especificado del equipo del cliente. A continuación, el demonio rsh valida el nombre del host / cliente comprobando los archivos, si la comprobación falla, la conexión quedará cancelada y se devolverá un mensaje de diagnóstico.

Ejemplo:

Se muestran las transacciones entre el cliente y el servidor para rsh. El comando FIXUP protocol rsh permite que el firewall PIX proteja las peticiones rsh de la siguiente forma:

- Conexión saliente: Cuando el servidor envía mensajes de error estándar, el firewall PIX abre un conducto entrante temporal para este canal. Este conducto se cierra cuando ya no es necesario.
- Conexión Entrante: Si hay un conducto que permita conexión entrante en un servidor rsh, y si todo el tráfico TCP saliente se permite de forma implícita, la administración no será necesaria, ya que el servidor iniciará el canal de errores estándar desde el interior. Si hay un conducto que permita que haya conexiones entrantes en un servidor rsh , y si no se permite de forma implícita todo el tráfico TCP saliente, el firewall abrirá un conducto temporal para el canal de errores estándar desde el servidor. Este conducto se cerrará cuando todos los mensajes hayan sido enviados.

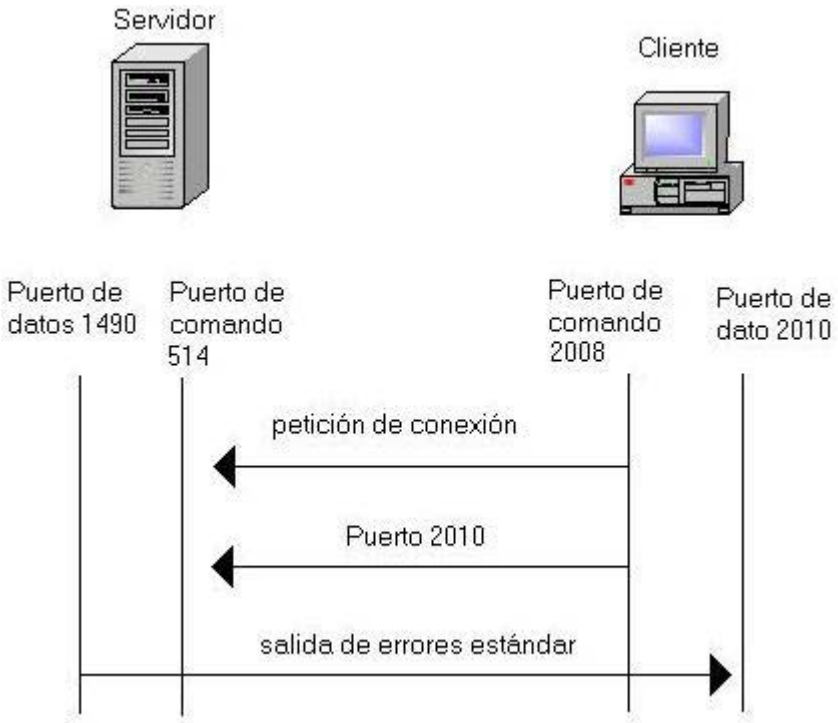


Figura 4.20 Transacciones rsh cliente/servidor.

4.10 Configurar IPSec para los PIX.

4.10.1 El firewall PIX de Cisco Secure puede crear una VPN segura.

Una red privada virtual (VPN) es un servicio que ofrece una conectividad segura y fiable sobre una infraestructura de red pública compartida, como puede ser Internet. Dado que la infraestructura es pública, la conectividad suele ser menos costosa que si se utilizan redes privadas dedicadas.

El firewall PIX es un activador de servicios VPN muy potente. El alto rendimiento del firewall PIX, la compatibilidad con los estándares abiertos y la facilidad de configuración lo convierten en un gateway VPN muy versátil. La VAC (tarjeta aceleradora VPN) ofrece un rendimiento 3DES de 100 Mbps sin necesidad de software adicional y sin tener que modificar la configuración del PIX.

El firewall PIX crea VPN en varias topologías, tal y como se muestra en la figura 4.10.1 y como se describe en la siguiente lista.

- **De PIX a gateway VPN seguro de PIX.** Dos o más firewalls PIX pueden habilitar una VPN, que protege el tráfico entre los dispositivos colocados detrás de los firewalls PIX. La topología de gateways VPN seguros impide que el usuario tenga que implementar dispositivos o software VPN dentro de la red, haciendo que el gateway seguro sea transparente para los usuarios.

- **De PIX a gateway VPN seguro de router Cisco IOS.** El *firewall* PIX y el *router* Cisco, que ejecutan software VPN de Cisco Secure, pueden interactuar para crear un gateway VPN seguro entre redes.

- **De cliente VPN de Cisco a PIX a través. del acceso telefónico**. El *firewall PIX* puede convertirse en un punto final para el cliente VPN de Cisco a través de una red de acceso telefónico. La red de acceso telefónico puede estar formada por RDSI, la red pública de telefonía conmutada (PSTN), y canales de comunicación por módem analógico o por línea de suscriptor digital (DSL).

- **De cliente VPN de Cisco a PIX a través de red**. El *firewall* PIX puede convertirse en un punto final VPN para el cliente VPN 3000 de Cisco Secure a través de una red IP.

- **De productos de otros fabricantes a PIX**. Los productos de otros fabricantes pueden conectarse con el *firewall* PIX si se adaptan a los estándares VPN abiertos.

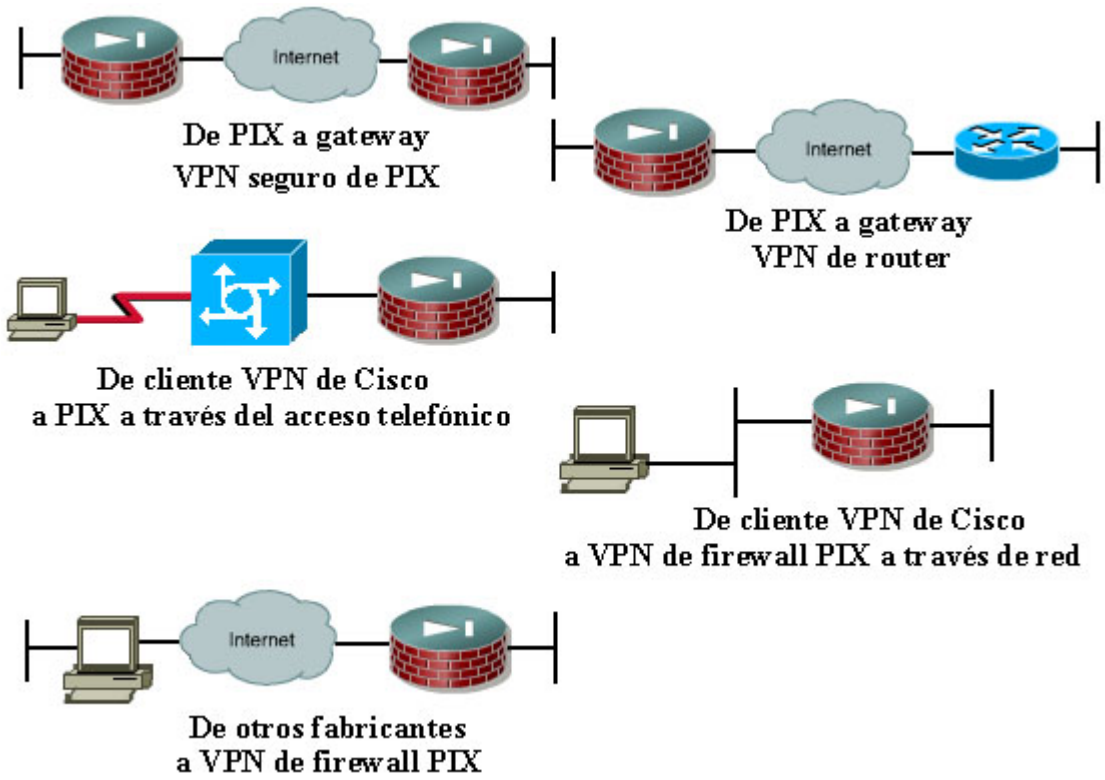


Figura 4.21 Las distintas topologías VPN.

La compatibilidad IPSec con productos que no sean Cisco deberá probarse minuciosamente, ya que ser 'compatible con IPSec' no garantiza la interoperabilidad.

Una VPN puede construirse en varios escenarios. Los más comunes son los siguientes:

- **VPN de Internet.** Un canal de comunicaciones privado sobre Internet.

Este tipo de VPN puede dividirse en:

- La conexión de oficinas remotas a través de Internet.
- La conexión de usuarios de acceso telefónico remoto a sus *gateways domésticos* a través de un proveedor de servicios de Internet (ISP).

- **VPN de intranet.** Un canal de comunicaciones privado de una empresa u organización que pueda o no contener el tráfico que atraviesa una WAN.

- **VPN de extranet.** Un canal de comunicaciones privado entre dos o más entidades separadas donde los datos recorren Internet o alguna otra WAN.

En todos los casos, la VPN o túnel consta de dos puntos finales que pueden ser *firewalls PIX, routers* Cisco, estaciones de trabajo cliente que ejecuten el Cliente VPN de Cisco o los productos VPN de otros fabricantes que se adapten a los estándares abiertos.

4.10.1.1 PIX, VPN e ipsec.

Cualquier firewall PIX que ejecute el SO 5.0 y posterior del PIX utiliza el conjunto de protocolos de Seguridad IP (IPSec) para activar las opciones VPN avanzadas. La implementación de IPSec en el PIX está basada en la IPSec Cisco IOS que se ejecuta en los *routers Cisco.*

IPSec proporciona un mecanismo para proteger la transmisión de datos por redes IP, garantizando la confidencialidad, la integridad y la autenticidad de las comunicaciones de datos sobre redes no protegidas, como Internet.

IPSec permite las siguientes opciones VPN en los *firewalls* PIX:

- **Confidencialidad de los datos.** El remitente IPSec puede cifrar los paquetes antes de transmitirlos por una red.

- **Integridad de los datos.** El receptor IPSec puede autenticar iguales y paquetes IPSec enviados por el remitente IPSec con el fin de garantizar que los datos no se han alterado durante la transmisión.

- **Autenticación del origen de los datos.** El receptor IPSec puede autenticar el origen de los paquetes IPSec enviados. Este servicio depende del servicio de integridad de datos.
- **Antireproducción.** El receptor IPSec puede detectar y rechazar paquetes reproducidos, ayudando a impedir los ataques.

IPSec es un conjunto de protocolos y algoritmos de seguridad que se usa para proteger los datos en la capa de red.

IPSec y los protocolos relacionados con la seguridad cumplen los estándares abiertos promulgados por la IETF, así como las RFC documentadas y los borradores de la IETF. IPSec puede utilizarse para escalar desde redes pequeñas hasta redes muy grandes.

El *firewall* PIX soporta los siguientes estándares IPSec:

- IPSec (Seguridad del protocolo IP).
- Intercambio de clave de Intemet (IKE).
- Estándar de cifrado de datos (DES).
- Triple DES (3DES).
- Diffie-Hellman (D-H).
- Message Digest 5 (MD5).
- Secure Hash Algorithm-1 (SHA-1).
- Firmas Ravist-Shamir-Adelman (RSA).
- Autoridades de certificados (CA).
- Asociación de seguridad (SA).

Ahora que ya conoce parte del vocabulario IPSec, las siguientes secciones definen los términos y los dotan de contexto.

4.10.1.2 IPSec.

IPSec es una estructura de estándares abiertos que proporciona confidencialidad, integridad de datos y autenticación de datos entre iguales que participan en la capa IP. IPSec se puede usar para proteger uno o más flujos de datos entre iguales IPSec.

La implementación general de IPSec está presidida por la RFC 2401, "Security Architecture for the Internet Protocol". IPSec se compone de estos dos protocolos principales:

- **Cabecera de autenticación (AH).** Un protocolo de seguridad que proporciona servicios opcionales de autenticación y de detección de la reproducción. El protocolo AH actúa como firma digital para garantizar que la totalidad del paquete IP no ha sido manipulado. Con la excepción de los campos que cambian en tránsito, como la suma de comprobación y el tiempo de existencia, AH proporciona autenticación no sólo a la sobrecarga de datos, sino a la totalidad del paquete. La IANA asignó al protocolo AH el número de protocolo IP 51. AH no proporciona servicios de cifrado y descifrado. AH puede ser usado por sí solo o con la Sobrecarga de seguridad del encapsulado (ESP).

- **Sobrecarga de seguridad del encapsulado (ESP).** Un protocolo de seguridad que proporciona confidencialidad y protección de los datos, así como servicios de autenticación y detección de la reproducción opcionales. El *firewall* PIX utiliza ESP para cifrar la sobrecarga de datos de los paquetes IP. ESP puede ser usado por sí solo o conjuntamente con AH. La IANA asignó a ESP el número de protocolo IP 50.

4.10.1.3 IKE

IKE es un protocolo híbrido compuesto por estándares ISAKMP y Oakley, que proporciona servicios de utilidad para IPSec: la autenticación de iguales IPSec, la negociación de asociaciones de seguridad IKE e IPSec y el establecimiento de claves para los algoritmos de cifrado que utiliza IPSec. IKE funciona en el puerto UDP 500.

4.10.1.4 SA

El concepto de asociación de seguridad (SA) es fundamental para IPSec. Una SA es una conexión entre iguales IPSec que determina los servicios IPSec disponibles entre iguales, similares a un puerto TCP o UDP. Cada igual IPSec mantiene en la memoria una base de datos SA que contiene los parámetros de la SA. Las SA se identifican de forma unívoca por la dirección del igual IPSec, el protocolo de seguridad y el índice de parámetro de seguridad (SPI). En el *firewall* PIX es necesario configurar los parámetros de la SA y controlar las SA.

4.10.1.5 DES

DES hace referencia al Estándar de cifrado de datos, que fue publicado en 1977. DES cifra y descifra los datos de los paquetes. DES es utilizado por IPSee e IKE. DES utiliza una clave de 56 bits, que garantiza un cifrado de alto rendimiento.

Desde la aparición de las computadoras de sobremesa rápidas, DES ya no está considerado un cifrado fuerte. Para proteger los datos de producción, Cisco recomienta utilizar 3DES.

4.10.1.6 3DES

3DES es una variante de DES, que se repite tres veces con tres claves separadas, doblando la capacidad de DES. IPSec utiliza 3DES para cifrar y descifrar el tráfico de datos y utiliza una clave de 168 bits, lo que garantiza la fortaleza del cifrado.

4.10.1.7 D-H

Diffle-Hellman es un protocolo de cifrado de clave pública que permite que las dos partes establezcan una clave secreta compartida sobre un canal de comunicaciones inseguro. D-H se usa en el IKE para establecer claves de sesión. En el *firewall* PIX se soportan grupos D-H de 768 bits (Grupo 1) y de 1024 bits (Grupo 2). El segundo grupo es más seguro. En el *firewall* PIX, IKE utiliza un intercambio D-H para derivar claves secretas simétricas en cada igual IPSec que sea utilizado por algoritmos de cifrado. El intercambio D-H puede ser autenticado con RSA (o con claves precompartidas).

4.10.1.8 MD5

Message Digest version 5 (MD5) es un algoritmo *hash* (de dispersión) que auténtica los datos de los paquetes. Un *hash* es un algoritmo de cifrado de sentido único que toma un mensaje de entrada de longitud arbitraria y genera un conjunto de mensajes de salida de longitud fija. IKE, AH y ESP pueden usar MD5 para la autenticación. MD5 procesa su entrada en bloques de 512 bits y genera un conjunto de mensajes de 128 bits.

4.10.1.9 SHA-1

Secure Hash Algorithm (SHA) es un algoritmo *hash* que firma y autentica los datos de los paquetes. El *firewall* PIX utiliza la variante HMAC de SHA-1, que proporciona un nivel adicional de dispersión. IKE, AH y ESP pueden usar SHA-1 para la autenticación.

4.10.1.10 Firmas RSA

RSA es un sistema de cifrado de clave pública que sirve para la autenticación. En la criptografía de clave pública, cada usuario posee una clave pública y una clave privada. La clave pública se hace pública, mientras que la clave privada permanece en secreto. El cifrado se lleva a cabo con la clave pública, mientras que el descifrado se lleva a cabo por medio de la clave privada. El criptosistema de clave pública RSA es la forma más conocida de criptografía de clave pública. RSA significa Rivest, Shamir y Adleman, que son los inventores del criptosistema RSA.

4.10.1.11 CA

El hecho de que el firewall PIX dé soporte de una Autoridad de certificados (CA) posibilita que se pueda escalar la red protegida por IPSec proporcionando el equivalente de una tarjeta de identificación digital a cada dispositivo. Estas tarjetas ID digitales se llaman certificados digitales. Cuando dos iguales IPSec desean comunicarse, lo que hacen es intercambiar certificados digitales para probar sus identidades (con lo que se elimina la necesidad de intercambiar manualmente las claves públicas con cada igual o de especificar manualmente una clave compartida en cada igual). Los certificados digitales se obtienen de una CA. El soporte CA del *firewall* PIX utiliza firmas RSA para autenticar el intercambio CA.

4.10.2 Cómo configurar el soporte IPSec en el *firewall PIX.*

Esta sección muestra cómo configurar la IPSec básica en el *firewall* PIX por medio de claves precompartidas para la autenticación. Presenta una panorámica de las tareas y los pasos necesarios para configurar IPSec, proporciona detalles acerca de los comandos relacionados con IPSec dentro del *firewall* PIX y muestra ejemplos de comandos.

El objetivo de esta sección consiste en configurar *firewalls* PIX para que funcionen como *gateways* IPSec seguros que cifrarán y protegerán los flujos de tráfico de las redes protegidas por los *firewalls* PIX, utilizando claves precompartidas para la autenticación. El uso de claves precompartidas IKE para la autenticación de sesiones IPSec es relativamente fácil de configurar, aunque no escala bien cuando hay un gran número de iguales IPSec; en cuyo caso, habrá que utilizar certificados digitales.

La figura 4.22 muestra la topología simplificada de la empresa XY que se usa en los ejemplos de esta sección.

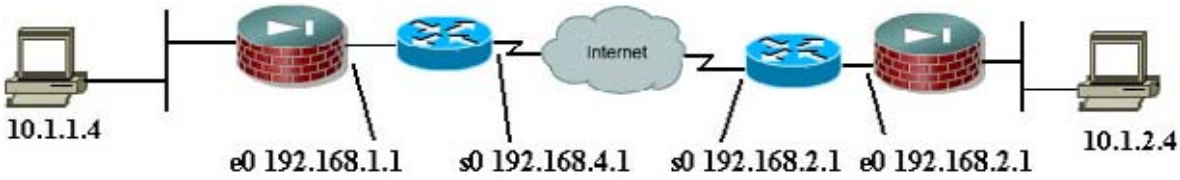


Figura 4.22 Topología de la empresa XYZ para el IPSec de firewall PIX.

A la hora de configurar el cifrado IPSec en el *firewall* PIX utilizando claves precompartidas, hay que llevar a cabo cuatro tareas:

- **Tarea 1: preparación para IPSec.** Supone determinar con detalle las normas de cifrado, incluyendo la identificación de los *hosts* y las redes que se desea proteger, la elección de un método de autenticación, la determinación de los detalles acerca de los iguales IPSec, la identificación de las opciones IPSec necesarias y la garantía de que las listas de acceso existentes permiten el tráfico IPSec. Si hay un *router* de perímetro de filtrado frente al *firewall* PIX, éste deberá permitir los protocolos IP 50 y 51 y el puerto UDP 500.

- **Tarea 2: configuración del Intercambio de clave de Internet (IKE) para las claves precompartidas.** Implica la activación del IKE, la creación de normas IKE, el establecimiento del modo de identidad y la validación de la configuración.

- **Tarea 3: configuración de IPSec.** Incluye la creación de listas de acceso de cifrado, la definición de conjuntos de transformación, la creación de entradas de mapas de cifrado y la aplicación de conjuntos de mapas de cifrado a las interfaces.

- **Tarea 4: comprobación y verificación de la configuración IPSec.** Esta tarea implica el uso de los comandos show, debug y otros comandos relacionados para probar y verificar que el cifrado IPSec funciona y para solucionar problemas.

A continuación se abordan más detalladamente cada una de estas tareas de configuración.

4.10.2.1 Tarea 1: preparación para IPSec.

Paso 1 Determinación de las normas IKE (Fase 1 del IKE, o modo principal) entre iguales IPSec en base al número y la ubicación de los iguales.

Paso 2 Determinación de las normas IPSec (Fase 2 del IKE, o modo rápido), incluyendo detalles del igual IPSec, como las direcciones IP y los conjuntos y modos de transformación IPSec.

Paso 3 Comprobación de la configuración activa utilizando write terminal, show isakmp, show isakmp policy, show crypto map y otros comandos show.

Paso 4 Asegurarse de que la red funciona sin cifrado para eliminar problemas básicos utilizando el comando ping y ejecutando el tráfico de prueba antes de probar el cifrado.

Paso 5 Asegurarse de que las listas de acceso existentes en el *router* de perímetro y en el *firewall* PIX permiten el tráfico IPSec, o el tráfico deseado será filtrado.

4.10.2.2 Tarea 2: configuración del IKE para las claves precompartidas.

Consiste en configurar los parámetros del IKE reunidos anteriormente. Observe que en los comandos de configuración PIX, ISAKMP es sinónimo de IKE.

Deberá empezar esta tarea definiendo las necesidades y la estrategia de seguridad generales basándose en las normas de seguridad de la empresa.

Paso 1 Activación o desactivación del IKE con el comando isakmp enable.

Paso 2 Creación de las normas IKE con los comandos isakmp policy.

Paso 3 Configuración de las claves precompartidas con el comando isakmp key y los comandos asociados.

Paso 4 Verificación de qué método va a utilizar el IKE para verificar su igual de cifrado. Cuando dos iguales utilizan el IKE para establecer asociaciones de seguridad IPSec, cada igual enviará su identidad ISAKMP al igual remoto. Enviará su dirección IP o su nombre de *host* en función de cómo esté establecida la identidad ISAKMP de cada uno. Por defecto, la identidad ISAKMP de la unidad del *firewall* PIX está establecida a la dirección IP. Como regla general, establezca el *firewall* PIX y las identidades de sus iguales de la misma forma para evitar un fallo en la negociación del IKE. Este fallo podría ser debido al *firewall* PIX o al igual que no está reconociendo su identidad. Para determinar el método que va a utilizar el PIX para verificar la identidad del igual, utilice el comando show isakmp identity. La identidad predeterminada es la dirección IP.

Paso 5 Verificación de la configuración IKE con el comando show isakmp [policy].

Las siguientes secciones describen detalladamente estos pasos.

4.10.2.2.1 Paso 1: Activación o desactivación del IKE.

El primer paso a la hora de configurar el IKE consiste en activar o desactivar el IKE en las interfaces que se usan para terminar los túneles IPSec. El IKE se activa o desactiva en interfaces individuales por medio del comando isakmp enable. El IKE está activado por defecto, y hay que usar la forma no del comando para desactivarlo. La sintaxis del comando es la siguiente:

isakmp enable nombre-intertaz
pixfirewall#(config) **isakmp enable outside**

El argumento *nombre-ínterfaz* especifica el nombre de la interfaz en la que se va a activar la negociación IKE.

4.10.2.2.2 Paso 2: Creación de las normas IKE.

El siguiente paso a la hora de configurar el soporte IKE en el *firewall* PIX consiste en definir un paquete de normas IKE. El objetivo de definir un paquete de normas IKE es el de establecer el IKE entre dos puntos finales IPSec. Utilice los detalles relativos a las normas IKE reunidos durante la tarea de planificación.

Utilice el comando isakmp policy para definir unas normas IKE. Las normas IKE definen una serie de parámetros que se van a usar durante la negociación IKE. Utilice la forma no de este comando para eliminar unas normas IKE. La sintaxis del comando es la siguiente:

pixfirewall#(config) **isakmp policy 10 authentication pre-share**
isakmp policy *príoridad* encryption {**des** | **3des**}
pixfirewall#(config) **isakmp policy 10 encryption 3des**
isakmp policy *prioridad* {**group1** | **group2**}
pixfirewall#(config) **isakmp policy 10 group2**
isakmp policy *prioridad* hash {**md5** | **sha**}
pixfirewall#(config) **isakmp policy 10 hash sha**
isakmp policy *prioridad* **lifetime** *segundos*

pixfirewall#(config) **isakmp policy 10 lifetime 86400**

La tabla 4.11 describe los parámetros del comando.

Parámetro del comando	Descripción
policy prioridad	Identifica únicamente las normas IKE y les asigna una prioridad. Utilice un entero entre 1 y 65.534, siendo el 1 la prioridad más alta y 65.534 la más baja
authentication pre-share	Especifica las claves precompartidas como método de autenticación.
authentication rsa-sig	Especifica las firmas RSA como método de autenticación.
encryption des	Especifica DES-CBC de 56 bits como el algoritmo de cifrado que se va a usar en las normas IKE. Es el valor predeterminado.
encryption 3des	Especifica que hay que usar el algoritmo de cifrado Triple DES en las normas IKE.
group 1	Especifica que hay que usar el grupo Diffie-Hellman de 768 bits en las normas IKE. Es el valor predeterminado.
group 2	Especifica que hay que usar el grupo Diffie-Hellman de 1024 bits en las normas IKE
hash md5	Especifica MD5 (variante de HMAC) como el algoritmo *hash* que se va a usar en las normas IKE.
hash sha	Especifica SHA-1 (variante de HMAC) como el algoritmo *hash* que se va a usar en las normas IKE. Es el algoritmo *hash* predeterminado
lifetime segundos	Especifica el número de segundos que debe existir cada asociación de seguridad antes de expirar. Utilice un entero entre 60 y 86.400 segundos (un día). Normalmente, puede dejar este valor como el predeterminado (86.400).

Tabla 4.11 Parámetros del comando isakmp policy.

Si no especifica uno de estos comandos para unas normas, se usará el valor predeterminado de ese parámetro. Utilizando la forma no del comando, puede restablecer un

valor a su valor predeterminado. Por ejemplo, para restablecer a DES como método de cifrado establecido anteriormente a 3DES, utilice el comando no isakmp Policy 100 encryption.

4.10.2.2.3 PASO 3: Configuración de las claves precompartidas.

El siguiente paso a la hora de configurar el soporte IKE en el *firewall* PIX consiste en establecer opcionalmente el modo de identidad y configurar las claves precompartidas, como veremos en las siguientes secciones.

4.10.2.2.3.1 Cómo establecer el modo de identidad

Los iguales IPSec se autentican entre sí durante las negociaciones IKE utilizando la clave precompartida y la identidad IKE. La identidad puede ser o bien la dirección IP del igual o su nombre de *host.* El *firewall* PIX utiliza por defecto el método de identidad de la dirección IP. Si opta por utilizar el método de identidad de la dirección, deberá especificar el método con el comando isakmp identity. Utilice la forma no de este comando para restablecer la identidad del IKE al valor predeterminado (nombre de *host).* La sintaxis del comando es la siguiente:

isakmp identity {address | hostname}

La palabra clave address establece la identidad IKE a la dirección IP de la interfaz que se comunica con el igual remoto durante las negociaciones IKE de las claves precompartidas. Este palabra clave se suele utilizar cuando el igual utiliza únicamente una interfaz para las negociaciones IKE y cuando se conoce la dirección IP.

La palabra clave hostname establece la identidad IKE al nombre de *host* que esté concatenado con el nombre de dominio (por ejemplo, myhost.domain.COM). Esta palabra clave se deberá usar si se usa más de una interfaz del igual para las negociaciones IKE, o si no se conoce la dirección IP de la interfaz (como ocurre en el caso de las direcciones IP asignadas dinámicamente).

4.10.2.2.3.2 Cómo configurar las claves precompartidas.

Las claves de autenticación precompartidas se configuran con el comando de configuración isakmp key. Esta clave se deberá configurar siempre que se especifiquen claves precompartidas en unas normas IKE. Utilice la forma no de este comando para eliminar una clave de autenticación precompartida. La sintaxis del comando es la siguiente:

isakmp key cadenaclave **address** dirección-igual **[netmask** máscara]

La tabla 4.12 describe los argumentos y opciones de comando para esta secuencia de comandos.

Parámetro de comando	Descripción
Cadenaclave	Especifica la clave precompartida. Utilice cualquier combinación de caracteres alfanuméricos hasta un máximo de 128 bytes. Esta clave precompartida deberá ser idéntica en ambos iguales.
Address	Especifica que se ha establecido la identidad IKE del igual remoto con su dirección IP.
dirección-igual	Especifica la dirección IP del igual remoto. Es posible introducir como *wildcard* la dirección 0.0.0.0, indicando que cualquier igual IPSec que tuviera una clave coincidente podría usar la clave.
nombredehost-igual	Especifica el nombre de *host* del igual remoto. Es el nombre de *host* del igual concatenado con su nombre de dominio (por ejemplo, myhost.domain.com).
netmask máscara (opcional)	Especifica la máscara de red. Es posible introducir como *wildcard la* máscara de red 0.0.0.0 junto con una dirección de 0.0.0.0, indicando que cualquier igual que no tuviera una clave asociada con su dirección IP específica podría usar la clave.

Tabla 4.12 Argumentos y opciones del comando isakmp key

Es posible configurar una dirección *wildcard* de igual y una máscara de 0.0.0.0 0.0.0.0 con el fin de que muchos iguales compartan la clave precompartida. Sin embargo, Cisco recomienda usar una clave única para cada igual.

Al igual que ocurre con cualquier igual IPSec que use calves precompartidas, se deberá configurar la misma clave precompartida en cada par de iguales IPSec a la hora de usar claves precompartidas para la autenticación IKE. Se recomienda que se configure una clave precompartida distinta en cada par de iguales IPSec. El uso de la misma clave precompartida en más de un par de iguales IPSec supone un riesgo para la seguridad.

4.10.2.2.4 Paso 4: Verificación de la configuración IKE.

Puede usar el comando show isakmp [policy] para mostrar las normas configuradas y predeterminadas. El comando Show isakmp muestra las normas configuradas tal y como aparecerían con el comando write terminal. El comando write terminal muestra las normas configuradas.

4.10.2.3 Tarea 3: Configuración de IPSec.

La siguiente tarea a la hora de configurar IPSec en el *firewall* PIX consiste en configurar los parámetros IPSec recopilados anteriormente.

Paso 1 Configuración de las listas de acceso de cifrado con el comando access-list.

Paso 2 Configuración de paquetes de conjuntos de transformación con el comando crypto ipsec transform-set.

Paso 3 (Opcional) Configuración de los tiempos de existencia globales de las asociaciones de seguridad IPSec con el comando crypto ipsec security-association lifetime.

Paso 4 Configuración de los mapas de cifrado con el comando crypto map.

Paso 5 Aplicación de los mapas de cifrado a la interfaz de terminación/origen con el comando crypto map map-name interface.

Paso 6 Verificación de la configuración IPSec con los comandos show disponibles.

4.10.2.3.1 Paso 1: configuración de las listas de acceso de cifrado

Las listas de acceso de cifrado definen qué tráfico IP va a ser protegido por IPSec. Estas listas realizan las siguientes funciones para IPSec:

- Seleccionan el tráfico saliente que IPSec va a proteger.
- Procesan el tráfico entrante para filtrar y descartar el tráfico que tendría que haber sido protegido por IPSec.
- Determinan si van a aceptar peticiones para las asociaciones de seguridad IPSec con respecto a los flujos de datos solicitados a la hora de procesar negociaciones IKE.

Las listas de acceso de cifrado identifican los flujos de tráfico que es necesario proteger. Aunque la sintaxis de las listas de acceso de cifrado es la misma que la de las listas de acceso normales, los significados son distintos de las listas de acceso de cifrado: permit especifica que es necesario cifrar los paquetes coincidentes, mientras que deny especifica que no se va a cifrar en los paquetes coincidentes. Las listas de acceso de cifrado se comportan de modo parecido a una lista de acceso aplicada al tráfico saliente de una interfaz del *firewall PIX.*

Para configurar una lista de acceso de cifrado, utilice el comando de configuración access-list. Para eliminar una sola línea de una lista de acceso, utilice la forma no del comando. Para eliminar toda la lista de acceso y su comando access-group asociado, utihce el comando clear access-list. La sintaxis del comando es la siguiente:

access-list nombre_acl **[deny | permit]** protocolo dirección-origen máscara-origen [operador puerto [puerto]] dirección_destíno máscara_destino [operador puerto [puerto]]

La tabla 4.13 describe los argumentos y las opciones de esta secuencia de comandos.

Parámetro del comando	Descripción
Nombre_acl	Especifica el nombre o número de una lista de acceso.
deny	No selecciona un paquete para la protección IPSec. Impide que IPSec proteja el tráfico IPSec en el contexto de una entrada de mapa de cifrado concreta.
permit	Selecciona un paquete para la protección IPSec. Hace que IPSec proteja todo el tráfico IP que coincida con las condiciones especificadas, utilizando las normas descritas por la correspondiente entrada de mapa de cifrado.
protocolo	Especifica el nombre o el número de un protocolo IP. Puede ser una de las palabras clave ICMP, ip, tcp o udp, o un entero situado en el intervalo entre 1 y 254 que represente un número de protocolo IP. Para que coincida con cualquier protocolo de Internet, utilice la palabra clave ip.
dirección_origen dirección_destino	Especifica la dirección de la red o del *host* desde el que se está enviando el paquete o desde donde se ha recibido. Existen otras tres formas de especificar el origen o el destino: Utilice una cantidad de 32 bits en formato decimal con puntos de cuatro partes. Utilice la palabra clave any como abreviatura de un origen y máscara de red de origen y una máscara de red de 0.0.0.0 0.0.0.0. Utilice el origen de *host* o el destino de *host* como abreviatura para un origen y máscara de

	red de origen de 255.255.255.255 o un destino y una máscara de red de destino de 255.255.255.255.
máscara_origen máscara_destino	Especifica los bits de máscara de red (máscara) a aplicar al origen o al destino. Existen otras tres formas de especificar la máscara de red de origen o de destino: Utilice una cantidad de 32 bits en formato decimal con puntos de cuatro partes. Coloque ceros en las posiciones de bit que desee omitir. Utilice la palabra clave any como abreviatura para un origen y máscara de red de origen o un destino y máscara de red de destino de 0.0.0.0 0.0.0.0. Esta palabra clave no se recomienda. Utilice el origen de *host* o el destino de *host* como abreviatura para un origen y máscara de red de origen de 255.255.255.255o un destino y máscara de red de destino de 255.255.255.255.
operador (opcional)	Especifica un puerto o intervalo de puertos para comparar puertos de origen o de destino. Entre los posibles operandos se incluye lt (menor que), gt (mayor que), eq (igual a), neq (no igual a) y range (intervalo inclusivo). El operador range requiere dos números de puerto. Cada uno de los operadores restantes requiere un solo número de puerto.
puerto	Servicio o servicios IP permitidos en base al protocolo TCP o UDP. Especifique los puertos o bien mediante un nombre o bien a través de un número situado entre 0 y 65.535.

Tabla 4.13 Opciones y argumentos del comando access-list

Se desviará todo el tráfico entrante no protegido que coincida con una entrada de permiso en la lista de acceso de cifrado para una entrada de mapa de cifrado marcada como IPSec.

Se recomienda que evite el uso de la palabra clave any para especificar direcciones de origen o de destino. Además, podría experimentar un mayor uso de la CPU y una degradación del rendimiento de la red.

Trate de ser lo más exacto posible a la hora de definir en una lista de acceso de cifrado qué paquetes proteger. Si debe usar la palabra clave any en una instrucción permit, deberá anteponer a esa instrucción una serie de instrucciones deny con el fin de filtrar el tráfico que desee proteger.

Es imperativo que configure imágenes espejo de las listas de acceso de cifrado para que IPSec las utilice. Las listas de acceso de cifrado de cada igual deberán ser simétricas.

La no creación de listas de acceso simétricas en ambos iguales de cifrado redunda en la incapacidad de formar una SA.

Por ejemplo, los criterios de origen de PIX 1 deberán se exactamente iguales que los criterios de destino de PIX 2, y los criterios de destino de PIX 1 deberán ser exactamente iguales que los criterios de origen de PIX 2. En cada *firewall* PIX, el tráfico entrante y el tráfico saliente es evaluado frente a la misma lista de acceso IPSec saliente. Los criterios de la lista de acceso son aplicados hacia delante al tráfico que sale del *firewall* PIX y en sentido contrario al tráfico que entra en el *firewall* PIX. Cuando un *firewall* PIX recibe paquetes cifrados de un igual IPSec, utiliza la misma lista de acceso para determinar qué paquetes entrantes descifrar visualizando las direcciones de origen y de destino de la lista de acceso en sentido contrario.

4.10.2.3.2 Paso 2: configuración de paquetes de conjuntos de transformación.

El siguiente paso para configurar IPSec en el *firewall* PIX consiste en usar las normas de seguridad para definir un conjunto de transformación. Un conjunto de transformación es una combinación de transformaciones IPSec individuales que habilitan unas normas de seguridad para el tráfico. Los conjuntos de transformación combinan los siguientes factores IPSec:

- Un mecanismo para la autenticación de paquetes: la transformación AH.
- Un mecanismo para el cifrado y la autenticación opcional de la sobrecarga: la transformación ESP.
- El modo IPSec, transporte o túnel.

Un conjunto de transformación se define con el comando crypto ipsec transform-set. Para eliminar un conjunto de transformación, se usa la forma no del comando. La sintaxis del comando es la siguiente:

crypto ipsec transform-set *nombre-conjunto-transformación transtormación1 [transformación2 [transformación3]]*

La tabla 4.14 describe los argumentos del comando crypto ipsec transform-set.

Parámetro de comando	Descripción
nombre-conjunto-transformación	Especifica el nombre del conjunto de transformación a crear (o modificar).
transformacíón1 *transformacíón2* *transformacíón3*	En un conjunto se pueden especificar hasta tres transformaciones. Las transformaciones definen los protocolos y algoritmos de seguridad IPSec. Cada transformación representa un protocolo de seguridad IPSec (ESP, AH o AH más ESP, o AH más ESP y ESP-HMAC) más el algoritmo que desee usar

Tabla 4.14 Argumentos del comando crypto IPSec transform-set.

En un conjunto puede haber hasta tres transformaciones. El modo predeterminado de cada transformación es *túnel.* Los conjuntos están limitados a una transformación AH y a dos transformaciones ESP. Asegúrese de que la configuración de los conjuntos de transformación coinciden entre iguales IPSec.

Cuando no se usa el IKE para establecer asociaciones de seguridad, es preciso usar un solo conjunto de transformación. El conjunto de transformación no se negocia. Si especifica un protocolo ESP en un conjunto de transformación, podrá especificar simplemente una transformación de cifrado ESP o una transformación de cifrado ESP y una transformación de autenticación ESP.

La tabla 4.15 muestra las transformaciones IPSec que soporta el firewall PIX

Transformación	**Descripción**
ah-md5-hmac	Transformación AH-md5-hmac que se usa para la autenticación.
ah-sha-hmac	Transformación AH-sha-hmac que se usa para la autenticación.
esp-des	Transformación ESP que utiliza el cifrado DES (56 bits).
esp-3des	Transformación ESP que utiliza el cifrado 3DES (168 bits).
esp-md5-hmac	Transformación ESP con autenticación HMAC-MD5 que se usa con una transformación esp-des o esp-3des para proporcionar integridad adicional a los paquetes ESP.
esp-sha-hmac	Transformación ESP con autenticación HMAC-SHA que se usa con una transformación esp-des o esp-3des para proporcionar integridad adicional a los paquetes ESP.

Tabla 4.15 transformaciones IPSec soportadas por el PIX

4.10.2.3.3 PASO 3: configuración de los tiempos de existencia globales de las asociaciones de seguridad IPSec.

El tiempo de existencia de la asociación de seguridad IPSec determina el tiempo durante el que las SA IPSec mantienen su validez antes de ser renegociadas. El *firewall* PIX soporta un valor de tiempo de existencia global que se aplica a todos los mapas de cifrado. El valor del tiempo de existencia global puede ser reemplazado por una entrada de mapa de cifrado.

Los tiempos de existencia sólo se aplican a las asociaciones de seguridad que estén establecidas a través del IKE. Las asociaciones de seguridad establecidas manualmente no expiran. Cuando una asociación de seguridad expira, se negocia una nueva sin interrumpir el flujo de datos.

4.10.2.3.3.1 Un conjunto de transformación negociado a través de iguales IPSec.

Puede cambiar los valores del tiempo de existencia global de la asociación de seguridad utilizando el comando de configuración crypto ipsec security-association lifetime. Para restablecer un tiempo de existencia al valor predeterminado, utilice la forma no del comando. La sintaxis del comando es la siguiente:

crypto ipsec security-association lifetime {seconds *segundos* | **kilobytes** *kilobytes}*

donde el parámetro seconds segundos especifica el número de segundos que existirá una asociación de seguridad antes de expirar. El valor predeterminado es de 28.800 segundos (8 horas). El parámetro kilobytes kilobytes especifica el volumen de tráfico (en kilobytes) que puede pasar entre iguales IPSec utilizando una asociación de seguridad determinada antes de que expire. El valor predeterminado es de 4.608.000 KB (10 MBps durante una hora).

Cisco recomienda el uso de los valores de tiempo de existencia predeterminados. Las SA se configuran por medio de mapas de cifrado.

El tiempo de existencia que se configura para ISAKMP es independiente del tiempo de existencia IPSec que se acaba de ver.

4.10.2.3.4 Paso 4: creación de los mapas de cifrado.

Es necesario crear entradas de mapa de cifrado para que IPSec configure las SA para los flujos de tráfico que deban ser cifrados. Las entradas de mapa de cifrado creadas para IPSec configuran parámetros de asociación de seguridad, ensamblando las distintas partes que se configuran para IPSec, entre las que se incluyen las siguientes:

- El tráfico que debe ser protegido por IPSec (lista de acceso de cifrado).
- La granularidad del tráfico que una serie de asociaciones de seguridad va a proteger.
- Dónde debe ser enviado el tráfico protegido con IPSec (quién es el igual IPSec remoto).
- La interfaz local que se va a usar para el tráfico IPSec.
- Qué protocolo de seguridad IPSec debe ser aplicado a este tráfico (conjuntos de transformación).
- El hecho de que las asociaciones de seguridad sean establecidas manualmente o a través del IKE.
- El tiempo de existencia de la asociación de seguridad IPSec.
- Otros parámetros que podrían ser necesarios para definir una asociación de seguridad IPSec.

Las secciones siguientes tienen en cuenta los parámetros de los mapa de cifrado, examinan el comando crypto Map, le enseñan a configurar mapas de cifrado y le presentan ejemplos de ellos.

4.10.2.3.4.1 Parámetros de mapa de cifrado.

Sólo es posible aplicar un conjunto de mapas de cifrado a cada interfaz. Este conjunto puede incluir una combinación de IPSec utilizando IKE e IPSec con entradas SA configuradas manualmente.

Múltiples interfaces pueden compartir el mismo conjunto de mapas de cifrado si desea aplicar las mismas normas a múltiples interfaces.

Si crea más de una entrada de mapa de cifrado para una determinada interfaz, utilice el número de secuencia (núm-sec) de cada entrada de mapa para clasificar las entradas de mapa; cuanto menor sea el número de secuencia, mayor será la prioridad. En la interfaz que tiene el conjunto de mapas de cifrado, el tráfico se evalúa primero frente a las entradas de mapa de prioridad más alta. Deberá crear múltiples entradas de mapa de cifrado para una interfaz concreta si se da alguna de estas condiciones:

- Que iguales IPSec distintos manipulen distintos flujos de datos.

- Que se desee aplicar una seguridad IPSec distinta a los distintos tipos de tráfico (para los mismos iguales IPSec o para iguales IPSec diferentes). Por ejemplo, si desea que se autentique el tráfico entre un grupo de subredes y que se autentique y se cifre el tráfico entre otro grupo de subredes. En este caso, se deberán definir los distintos tipos de tráfico en dos listas de acceso separadas, y se deberá crear una entrada de mapa de cifrado distinta para cada lista de acceso de cifrado.
- Que no se esté usando IKE para establecer un determinado grupo de asociaciones de seguridad, y que se desee especificar múltiples entradas de lista de acceso. Deberá crear listas de acceso separadas (una por cada entrada de permiso) y especificar una entrada de mapa de cifrado aparte para cada lista de acceso.

4.10.2.3.4.2 Cómo hacer copias de seguridad de los *gateways.*

Es posible definir múltiples iguales remotos utilizando mapas de cifrado que permitan la redundancia de *gateways.* Si un igual falla, seguirá siendo una ruta protegida. El igual al que se envían los paquetes viene determinado por el último igual que escuchó el *firewall* PIX (del que haya recibido tráfico o una petición de negociación) en un determinado flujo de datos. Si el intento es fallido con el primer igual, el IKE probará con el siguiente igual de la lista de mapas de cifrado.

4.10.2.3.4.3 Cómo configurar los mapas de cifrado.

El comando de configuración crypto Map se usa para crear o modificar una entrada de mapa de cifrado. Las entradas de mapa de cifrado se configuran haciendo referencia a los mapas de cifrado dinámicos como las entradas de prioridad más baja dentro de un conjunto de mapas de cifrado (es decir, los que tienen los números de secuencia más altos). Utilice la forma no de este comando para eliminar una entrada o conjunto de mapas de cifrado. La sintaxis del comando es la siguiente:

crypto map *nombre-mapa núm-sec* **{ipsec-isakmp** | **ipsec-manual}[dynamic** *nombre-mapa-dinámico]*

crypto map *nombre-mapa núm-sec* **match address** nombre_acl

crypto map *nombre-mapa núm-sec* **set peer** *{nombredehost* | *dirección-ip}*

crypto map *nombre-mapa núm-sec* **set pfs [group1** | **group2]**

crypto map *nombre-mapa núm-sec* **set security-association lifetime {seconds** *segundos* | **kilobytes** *kilobytes}*

crypto map *nombre-mapa núm-sec* **set transform-set** *nombre1-conjunto-transformación [nombre6-conjunto-transformación]*

crypto map *nombre-mapa* **client authentication** *nombre-servidor-aaa*

crypto map *nombre-mapa* **client configuration** *dirección* **{initiate** | **respond}**

La tabla 4.16 muestra los argumentos y las opciones de la secuencia de comandos crypto map.

Parámetro de comando	**Descripción**
nombre-mapa	Asigna un nombre a un conjunto de mapas de cifrado.
núm-sec	Asigna un número a la entrada de mapa de cifrado.
ipsec-manual	Indica que no se va a usar el IKE para establecer que las asociaciones de seguridad IPSec protejan el tráfico especificado por esta entrada de mapa de cifrado.
ipsec-ísakmp	Indica que se va a usar el IKE para establecer que las asociaciones de seguridad IPSec protejan el tráfico especificado por esta entrada de mapa de cifrado.
nombre-acl	Identifica la lista de acceso de cifrado con nombre. Este nombre deberá coincidir con el argumento con nombre de la lista de acceso de cifrado con nombre que se esté cotejando.
match address	Especifica una lista de acceso para una entrada de mapa de cifrado.

set peer	Especifica un igual IPSec de una entrada de mapa de cifrado. Especifica múltiples iguales repitiendo este comando. El igual es la interfaz de terminación del igual IPSec.
Nombredehost	Especifica un igual por su nombre de *host.* Es el nombre de *host* del igual concatenado con su nombre de dominio, como myhost.example.com.
dirección-íp	Especifica un igual por su dirección IP.
set pfs	Especifica que IPSec debe pedir el PFS (Perfect Forward Secrecy). En lo que respecta al PFS, cada vez que se negocia una nueva asociación de seguridad, se produce un nuevo intercambio Diffie-Hellman. El PFS proporciona una seguridad adicional para la generación de claves secretas a costa de un procesamiento adicional.
group 1	Especifica que IPSec deberá usar el grupo de módulos primarios Diffle-Hellman de 768 bits al ejecutar el nuevo intercambio Diffie-Hellman. Se utiliza con las transformaciones esp-des o esp-3des.
group 2	Especifica que IPSec deberá usar el grupo de módulos primarios Diffie-Hellman de 1024 bits al ejecutar el nuevo intercambio Diffle-Hellman.
set transform-set	Especifica qué conjuntos de transformación pueden utilizarse con la entrada de mapa de cifrado. Enumere múltiples conjuntos de transformación en orden de prioridad, colocando primero la transformación de prioridad más alta (más segura).
nombre-conjunto-transformacíón	Especifica el nombre del conjunto de transformación. En el caso de una entrada de mapa de cifrado ipsec-manual, sólo podrá especificar un conjunto de transformación. En el caso de un ipsec-isakmp o una entrada de mapa de cifrado dinámico, podrá especificar hasta seis conjuntos de transformación.

kilobytes *kilobytes*	Especifica el volumen de tráfico (en kilobytes) que puede pasar entre iguales que utilicen una asociación de seguridad concreta antes de que expire la SA. El valor predeterminado es de 4.608.000 KB. El tiempo de existencia de la asociación de seguridad de una entrada de mapa de cifrado reemplaza al valor de tiempo de existencia global de la asociación de seguridad.
seconds *segundos*	Especifica el número de segundos que va a existir una asociación de seguridad antes de expirar. El valor predeterminado es de 3600 segundos (una hora).
dynamic (opcional)	Especifica que esta entrada de mapa de cifrado hace referencia a un mapa de cifrado estática preexistente. Si utiliza esta palabra clave, no estará disponible ninguno de los comandos de configuración del mapa de cifrado.
nombre-mapa-dinámico (opcional)	Especifica el nombre del conjunto de mapas de cifrado que se deberá usar como plantilla de normas.
nombre-servídor-aaa	Especifica el nombre del servidor AAA que autenticará al usuario durante la autenticación IKE. Las dos opciones de servidor AAA que están disponibles son TACACS+ y RADIUS.
Initiate	Indica que el *firewall* PIX trata de establecer direcciones IP para cada igual.
respond	Indica que el *firewall* PIX acepta peticiones de direcciones IP de cualquier igual que lo pida.

Tabla 4.16 Argumentos y opciones del comando crypto map

He aquí algunas directrices adicionales que sirven para configurar los mapas de cifrado:

- Identifique el mapa de cifrado con un nombre de mapa de cifrado y un número se secuencia únicos.
- Utilice ipsec-isakmp para el soporte de servidor CA.

- Después de definir entradas de mapa de cifrado, podrá asignar el grupo de mapas de cifrado a las interfaces que utilicen el comando crypto map *nombre-mapa interna nombre-ínterfaz.*

Las listas de acceso de entradas de mapa de cifrado que contengan ipsec-manual se encuentran restringidas a una sola entrada permit, y las entradas subsiguientes son ignoradas. Las asociaciones de seguridad que estén establecidas por esa entrada crypto map concreta sólo sirven para un solo flujo de datos. Para soportar múltiples asociaciones de seguridad establecidas manualmente en distintos tipos de tráfico, defina múltiples listas de acceso de cifrado y luego aplique cada una a una entrada de mapa de cifrado ipsec-manual aparte. Cada lista de acceso deberá incluir una instrucción permit que defina qué tráfico se va a proteger.

4.10.2.3.4.4 Cómo establecer claves manualmente.

Puede configurar las SA IPSec manualmente y no usar el IKE para configurar la SA. Cisco recomienda que use el IKE para configurar las SA, ya que es muy difícil garantizar que los valores de las SA coincidan entre iguales, y D-H es un método más seguro para garantizar claves secretas entre iguales. Si se ve obligado, puede usar los comandos crypto map para especificar manualmente las claves de sesión IPSec y otros parámetros SA de una entrada de mapa de cifrado.

Las asociaciones de seguridad que se establezcan a través del comando crypto map no expiran (a diferencia de las asociaciones de seguridad que se establezcan a través del IKE). Las claves de sesión de un igual deberán coincidir con las claves de sesión del igual remoto. Si cambia una clave de sesión, se eliminará y reinicializará la asociación de seguridad que utilice la clave.

4.10.2.3.5 Paso 5: aplicación de los mapas de cifrado a las interfaces.

El último paso del proceso de configuración real de IPSec consiste en aplicar el conjunto de mapas de cifrado a una interfaz. Aplique el mapa de cifrado a la interfaz del fire*wall* PIX que esté conectada a Internet a través del comando crypto map en modo de configuración. Utilice la forma no del comando para eliminar el mapa de cifrado de la interfaz. La sintaxis del comando es la siguiente:

crypto map *nombre-mapa* **interface** *nombre-interfaz*

donde *nombre-mapa* especifica el nombre del conjunto de mapas de cifrado y el parámetro interface *nombre-interfaz* especifica la interfaz que va a ser usada por el *firewall* PIX para identificarse a sí mismo ante los iguales. Si el IKE está activado y está usando una CA para obtener certificados, ésta deberá ser la interfaz cuya dirección esté especificada en los certificados CA.

Es posible terminar túneles IPSec en cualquier interfaz del *firewall* PIX. Esto no significa que el tráfico procedente del exterior termine en la interfaz interna. El tráfico que termina en la interfaz interna es el tráfico de la red interna. El tráfico que termina en el exterior es el tráfico procedente del exterior. El tráfico que termina en una DMZ es el tráfico procedente de la DMZ.

Tan pronto como aplique el mapa de cifrado, la base de datos de asociaciones de seguridad deberá inicializarse en la memoria del sistema. Las SA estarán disponibles para ser configuradas cuando se transmita o reciba el tráfico definido por la lista de acceso de cifrado.

A una interfaz sólo se le puede asignar un conjunto de mapas de cifrado. Si múltiples entradas de mapa de cifrado poseen el mismo nombre de mapa, pero un número de secuencia distinto, se considerará que forman parte del mismo conjunto y todas ellas se aplicarán a la interfaz. La entrada de mapa de cifrado que tenga el número de secuencia más bajo será considerada como la de más alta prioridad y se evaluará primero.

El siguiente es un ejemplo de como aplicar un mapa de cifrado a una interfaz externa.

crypto map mymap interface outside

4.10.2.3.6 Paso 6: verificación de la configuración IPSec.

El último paso a la hora de configurar IPSec en el *firewall* PIX consiste en verificar la configuración IPSec utilizando los comandos SHOW que estén disponibles.

Puede ver todas las listas de acceso configuradas con el comando show access-list. En el ejemplo siguiente, el valor hitcnt=0 muestra que no se ha evaluado tráfico ante esta lista de acceso.

Pix2# show access-list
access-list 101 permit ip host **192.168.2.9** host **192.168.1.9** (hitcnt=0)

Con el comando show crypto ipsec transform-set podrá ver los conjuntos de transformación que estén definidos en ese momento. Este comando tiene la siguiente sintaxis:

show crypto ipsec transform-set [tag *nombre-conjunto-transformación]*

donde el parámetro opcional tag *nombre-conjunto-transformación* sólo muestra los conjuntos de transformación con el *nombre-conjunto-transformación* especificado.

Si no se usa ninguna palabra clave, aparecerán todos los conjuntos de transformación que estén configurados en el *firewall PIX.*

Puede usar el comando show crypto map para ver la configuración del mapa de cifrado. Si no se utiliza ninguna palabra clave, aparecerán todos los mapas de cifrado que estén configurados en el *firewall* PIX. La sintaxis del comando es la siguiente:

show crypto map [interface *intertaz* | **tag** *nombre-mapa]*

donde el parámetro interface *interfaz* sólo muestra el conjunto de mapas de cifrado que se haya aplicado a la interfaz especificada.

El siguiente ejemplo muestra los mapas de cifrado de PIX 1 y PIX 2. Observe cómo el mapa de cifrado consigue unir los seis valores relacionados con IPSec.

```
Pix1(config)# show crypto map
Crypto Map "peer2"10 ipsec-isakmp
        Peer = 192.168.2.2
        access-list 101 permit ip host 192.168.1.10 host 192.168.2.10 (hitcnt=0)
        Current peer: 192.168.2.2
        Security association lifetime:4608000 kilobytes/28800 seconds
        PFS (Y/N) : N
        Transform sets={ pix2, }
Pix2(config)# show crypto map
Crypto Map "peerl"10 ipsec-isakmp
        Peer =192.168.1.2
        access-list 101 permit ip host 192.168.2.10 host 192.168.1.10 (hitcnt=0)
        Current peer: 192.168.1.2
        Security association lifetime:4608000 kilobytes/28800 seconds
        PFS (Y/N):N
        Transform sets={ pix1, }
```

4.10.2.4 Tarea 4: comprobación y verificación de la configuración IPSec.

El último paso a la hora de configurar IPSec para claves precompartidas consiste en verificar que los valores IKE e IPSec fueron configurados correctamente y que todo funciona bien. El *firewall* PIX contiene una serie de comandos show, clear y debug que resultan útiles para probar y verificar IKE e IPSec, que se resumen en esta sección.

4.10.2.4.1 Cómo probar y verificar la configuración IKE.

Puede usar los comandos que se resumen en la tabla 4.17 para observar la configuración y el funcionamiento del IKE.

Comando	Descripción
Show isakmp	Muestra las normas IKE configuradas en un formato similar a un comando write terminal.
Show isakmp policy	Muestra las normas predeterminadas y las normas que se hayan configurado en el IKE.

Tabla 4.17 Comandos que se usan para observar el IKE.

4.10.2.4.2 Cómo probar y verificar la configuración IPSec.

Puede probar y verificar la configuración IPSec del *firewall* PIX con los comandos de la tabla 4.18.

Comando	Descripción
show access-list	Enumera las instrucciones de comando access-list de la configuración. Se emplea para verificar que las listas de acceso de cifrado seleccionan el tráfico interesante. Muestra el número de paquetes que coinciden con la lista de acceso.
show crypto map	Muestra las listas de acceso de cifrado que están asignadas a un mapa de cifrado. Muestra los parámetros del mapa de cifrado configurado.
show crypto ipsec transform-set	Muestra los conjuntos de transformación IPSec configurados.
show crypto ipsec security-association lifetime	Muestra los valores correctos del tiempo de existencia global de las SA IPSec.

Tabla 4.18 Comandos que sirven para observar IPSec.

4.10.2.4.3 Cómo controlar y administrar las comunicaciones IKE e IPSec.

Puede observar la configuración IKE e IPSec y controlar y administrar las comunicaciones IKE e IPSec entre los iguales *firewall* PIX e IPSec con los comandos de la tabla 4.19.

Comando	Descripción
show isakmp sa	Muestra el estado actual de las asociaciones de seguridad del IKE.
show crypto IPSec sa	Muestra el estado actual de las asociaciones de seguridad IPSec. Sirve para garantizar que el tráfico está siendo cifrado. También muestra el número de paquetes cifrados y descifrados sobre esa SA.
clear crypto isakmp sa	Borra las asociaciones de seguridad IKE.
clear crypto ipsec sa	Borra las asociaciones de seguridad IPSec.
debug crypto isakmp	Muestra las comunicaciones IKE entre los igualesfirewall PIX e IPSec.
debug crypto ipsec	Muestra las comunicaciones IPSec entre los igualesfirewall PIX e IPSec.

Tabla 4.19 Comandos que sirven para observar el IKE.

El comando Show isakmp sa sirve para ver todas las SA IKE activas de un igual, como se ve en el ejemplo siguiente:

Pix1# **show isakmp sa**

dst	src	state	conn-id	slot
192.168.1.2	192.168.2.2	QM-IDLE	93	0

El comando clear isakmp borra las conexiones IKE activas.

4.10.3 Cómo escalar las VPN en el *firewall* PIX.

El uso de claves precompartidas para la autenticación IKE sólo funciona cuando hay unos pocos iguales IPSec. Las CA permiten ampliarla a un gran número de iguales IPSec.

Otros métodos de autenticación IKE requieren la intervención manual para generar y distribuir las claves a un igual cada vez. El proceso de inscripción del servidor CA puede automatizarse mucho, por lo que se escala bien en implementaciones muy grandes. Cada igual IPSec se inscribe de forma individual en el servidor CA y obtiene un certificado digital compatible con otros iguales que estén inscritos en el servidor.

4.10.3.1 El firewall PIX con inscripción CA.

Los iguales se inscriben en un servidor CA siguiendo una serie de pasos en los que se generan claves específicas y luego se intercambian con el *firewall* PIX y el servidor CA para formar un certificado firmado. Los pasos necesarios para la inscripción pueden ser resumidos de esta forma:

Paso 1 El *firewall* PIX genera un par de claves RSA.

Paso 2 El *firewall* PIX obtiene el certificado de la CA, que contiene la clave pública de la CA.

Paso 3 El *firewall* PIX pide un certificado firmado de la CA que utilice las claves RSA (públicas) generadas y la clave/certificado públicos del servidor CA.

Paso 4 El administrador CA verifica la petición y envía un certificado firmado.

4.11 Control de Acceso Basado en Contexto del Firewall Cisco IOS.

4.11.1 Introducción al firewall cisco IOS.

El Firewall Cisco IOS es una opción específica de seguridad del software. Integra una funcionalidad para firewalls CBAC, el proxy de autenticación y la detección de intrusos para cada perímetro de la red, y amplía las opciones de seguridad actuales, como la autenticación, cifrado y la recuperación ante fallos, el bloqueo de Java y las alertas en tiempo real.

4.11.1.1 Control de Acceso Basado en Contexto.

El motor Control de acceso basado en contexto CBAC del Firewall proporciona un control de acceso por aplicación en todos los perímetros de la red. El CBAC mejora la seguridad de las aplicaciones TCP y UDP que utilizan puertos bien conocidos, como por ejemplo, tráfico FTP y de correo electrónico, examinando las direcciones de origen y de destino, permitiendo a los administradores de red aplicar soluciones integradas.

El CBAC filtra de forma inteligente los paquetes TCP y UDP basándose en la información de sesión del protocolo de capa de aplicación. Puede inspeccionar el tráfico de las sesiones que se originan en cualquiera de las interfaces del router. El CBAC inspecciona el tráfico que viaja a través del Firewall para descubrir y administrar información sobre el estado de sesiones TCP y UDP. Esta información sobre el estado crea aberturas temporales dentro de las listas de acceso del Firewall para permitir la devolución del tráfico y las conexiones de datos adicionales durante las sesiones.

4.11.1.2 Proxy de Autenticación

Anteriormente, la identidad del usuario y el acceso autorizado relacionado eran determinados por dirección IP fija de usuario, o había que aplicar una norma de seguridad a la totalidad de un grupo de usuarios. Con proxy de autenticación las normas por usuarios pueden ser descargadas dinámicamente en el router a partir de un servidor de autenticación TACACS+

o RADUS utilizando los servicios de autenticación, autorización y contabilidad (AAA) del software del sistema operativo.

Con la opción proxy de autenticación, los usuarios inician sesión en la red o acceden a internet a través del protocolo de transferencia de hipertexto HTTP, y sus perfiles de acceso específico son recuperados y aplicados de forma automática desde un servidor de control de acceso ACS o un servidor de autenticación RADIUS o TACACS+. Los perfiles están activos solo cuando hay tráfico activo de los usuarios autenticados, además el proxy de autenticación es compatible con otras opciones de seguridad como por ejemplo el traductor de direcciones de red NAT, el cifrado IPSec y software de cliente VPN.

4.11.1.3 Detección de Intrusos.

Los sistemas de detección de intrusos IDS proporcionan un nivel de protección que va mas allá del Firewall protegiendo a la red de ataques y amenazas internos y externos. La tecnología IDS del Firewall Cisco IOS mejora la protección del firewalls de perímetro actuando sobre los paquetes y flujos que violan las normas de seguridad o que representan una actividad sospechosa.

La opción de detección de intruso del firewalls resulta ideal para proporcionar una visibilidad adicional en los perímetros de internet, extranet y de sucursal en internet.

4.11.2 Control de Acceso basado en contexto de acción.

Primero es preciso abordar los conceptos básicos de lista de control de acceso (ACL). Una ACL proporciona filtrado de paquetes. Existe un deny all implícito al final de la ACL, si no se configura o aplica una ACL a una interfaz, permite todas las conexiones. Sin el CBAC, el filtrado del tráfico está limitado a las implementaciones de listas de accesos que examinan los paquetes de la capa de red o, a lo sumo, de la capa de transporte.

Con el CBAC, se enlaza las reglas de inspección específicas del protocolo y una lista de acceso a la interfaz interna, especificando los intervalos de direcciones que se desea proteger

con el CBAC. En la interfaz que actúa como externa se crea una lista de acceso que "idealmente" bloquea todo el tráfico entrante, pero probablemente se necesite el protocol de enrutamiento e ICMP. La lista de acceso de la interfaz externa se modifica dinámicamente para permitir el tráfico de retorno y se elimina inmediatamente cuando se cierra sesión.

4.11.2.1 Configuración del CBAC.

Tareas necesarias para configurar el CBAC:

- Establecer controles de auditoría y alerta
- Establecer tiempos de espera y umbrales globales
- Definir la asignación de puerto a aplicación PAM
- Definir las reglas de inspección
- Aplicar las reglas de inspección y ACL a las interfaces
- Probar y verificar

1.- Establecer controles de auditoria y alerta: Activa los controles de inicio de sesión y auditoría con el fin de proporcionar un registro del acceso de red a través del Firewall, incluyendo los intentos de acceso ilegítimos y los servicios entrantes y salientes. Utiliza los comandos "ip inspect audit.-trail y no ip inspect alert-off" para permitir respectivamente, el control de auditoría y alerta.

2.- Establecer tiempos de espera y umbrales globales: Esta sección examina como configurar los siguientes tiempos de espera y umbrales.

-Tiempo de espera TCP, SYN y FIN
-Tiempos de inactividad TCP, UDP Y DNS
-Protección DoS de inundación TCP

El CBAC utiliza tiempos de espera y umbrales para determinar cuánto tiempo administrar información sobre el estado de una sesión y para determinar cuándo eliminar las sesiones que no se establezcan por completo.

Para definir el tiempo que el software va a esperar hasta que una sesión TCP llegue al estado establecido antes de cerrar sesión, utilice el comando"ip inspect tcp synwait-time" en

configuración global, utilice la forma “no” de este comando para restablecer el tiempo de espera al valor predeterminado, la duración predeterminada es de 30 segundos.
Para definir el tiempo que se va a administrar una sesión TCP una ves que el Firewall detecta un intercambio FIN, con el comando “ip inspet tcp finwait-time”predeterminada es de 5 segundos.

3.- Definir la asignación de puertos a aplicaciones PAM: permite personalizar los números de puertos TCP o UDP para los servicios o aplicaciones de red. La PAM emplea esta información para dar soporte a entornos de red que ejecutan servicios que utilizan puertos distintos de los puertos registrados o bien conocidos que están asociados a una aplicación. La PAM permite a los administradores de red personalizar el control de acceso de red para aplicaciones y servicios específicos. La asignación de puertos específicos de host o subred se realiza por medio de ACL estándar.
Para establecer la PAM, se utiliza el comando ip port-map, la sintaxis del comando es la siguiente: ip port-map *nombre-aplicación* port *número-puerto* [list *núm-acl*]

4.- Definir las reglas de inspección: Son necesarios para especificar el tráfico IP que va a ser inspeccionado por el CBAC en la interfaz. Normalmente hay que definir una regla de inspección, la única excepción podría producirse si se desea activar el CBAC en dos direcciones en una misma interfaz del firewall, en este caso se deben configurar dos reglas una por cada dirección.
Una regla de inspección deberá especificar cada protocolo de capa de aplicación que se quiera inspeccionar, así como el TCP genérico o UDP genérico. Entre las reglas de inspección se incluyen las opciones de control de mensaje de alerta y de comprobación de la fragmentación de los paquetes IP. Para definir un conjunto de reglas de inspección se utiliza el comando de configuración global ip inspect name.

5.- Aplicación de las reglas de inspección y ACL a las interfaces del Router: Para aplicar un conjunto de reglas de inspección a una interfaz, se utiliza el comando de configuración de interfaz ip inspect *nombre-inspección (in/out)* . Para que el firewall sea efectivo, es necesario aplicar estratégicamente las reglas de inspección y las ACL a todas las interfaces del router.
Reglas generales para evaluar la lista de acceso IP en el Firewall:

- En la configuración Básica: Una configuración inicial básica permite que todo el tráfico de red fluya desde las redes protegidas hasta las no protegidas, a la ves que bloquea el tráfico de red procedente de cualquier red desprotegida.
- Permitir que el tráfico CBAC deje la red a través del Firewall: Todas las listas de acceso que evalúan el tráfico que abandona la red protegida deberán permitir el tráfico que vaya a inspeccionar el CBAC.
- Utilizar listas de acceso extendidas para denegar el tráfico de retorno CBAC que accede a la red a través del Firewall.

4.11.3 Ejemplo, Firewall de tres interfaces.

Se configura un router para que sea un Firewall entre tres redes: la interna, externa y DMZ. Las normas de seguridad que se implementan son las siguientes: permitir que todo el tráfico UDP y TCP general se inicie en el interior desde la red 10.0.0.0 para acceder a Internet y al host DMZ 172.16.0.2. también se permite el tráfico ICMP desde la misma red hasta Internet y hasta el host DMZ. Otras redes del interior no están definidas, entonces deberán ser denegadas. En lo que respecta al tráfico que se inicia en el exterior, permita el acceso exclusivamente a ICMP y http en el host DMZ 172.16.0.2 y el resto del tráfico debe ser denegado.

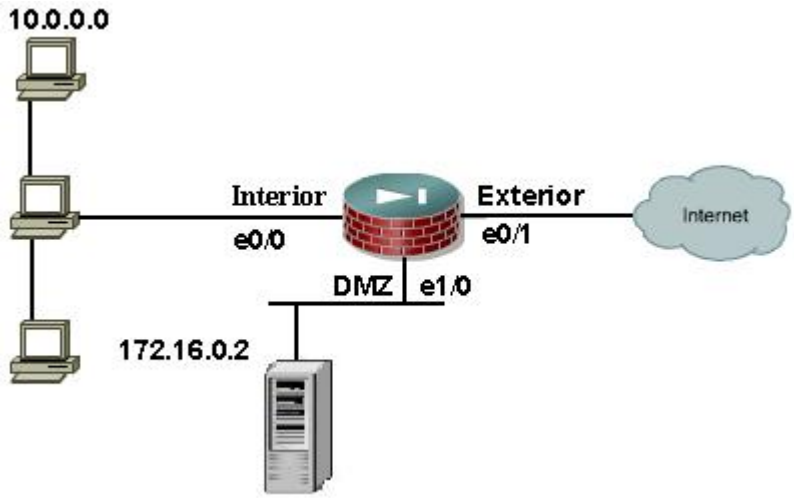


Figura 4.23 Normas para Firewalls de tres interfaces.

4.11.3.1 Tráfico saliente.

- Establecer las reglas que inspeccionen el tráfico TCP y UDP

Router(config)# ip inspect name outbound tcp
Router(config)# ip inspect name outbound udp

- Escribir una ACL que permita el tráfico IP desde la red 10.0.0.0 hasta cualquier destino

Router(config)# access-list 101 permit ip 10.0.0.0 0.255.255.255 any

- Aplicar la regla de inspección y ACL a la interfaz interna en sentido entrante

Router(config)# interface e0/0
Router(config-if)# ip inspect outbound in
Router(config-if)# ip access-group 101 in

4.11.3.2 Tráfico entrante.

- Regla que inspeccione el tráfico TCP:

Router(config)# ip inspect name inbound tcp

- Escribir una ACL que permita exclusivamente el tráfico ICMP y http desde Internet hasta el host 172.16.0.2

Router(config)# access-list 102 permit icmp any host 172.16.0.2
Router(config)# access-list 102 permit tcp any host 172.16.0.2 eq www

- Aplicar la regla de inspección y la ACL a la interfaz externa en sentido entrante

Router(config)# interface e0/1
Router(config-if)# ip inspect inbound in
Router(config-if)# ip access-group 102 in

4.11.3.3 Tráfico entrante a la DMZ.

Establecer una ACL que sólo permita que se inicie tráfico ICMP desde el host DMZ y que responda a una petición http

```
Router(config)# access-list 103 permit icmp host 172.16.0.2 any
Router(config)# access-list 103 permit tcp host 172.16.0.2 eq www any
```

Establecer una ACL que permita exclusivamente el tráfico ICMP y http desde cualquier red hasta el host 172.16.0.2

```
Router(config)# access-list 104 permit icmp host 172.16.0.2 any
Router(config)# access-list 104 permit tcp host 172.16.0.2 eq www any
```

Aplicar las ACL a la interfaz DMZ

```
Router(config)# interface e1/0
Router(config-if)# ip access-group 103 in
Router(config-if)# ip access-group 104 out
```

4.12 Configuración del Firewall PIX para detección de intrusos.

El sistema de detección de intrusos (IDS) es muy limitado en cuanto a su alcance dentro del contexto más amplio de protecciones que ofrece el IDS de Cisco Secure. La opción IDS del PIX no debe ser concebida como una solución integral, sino como unincremento a la eficiencia de la detección de intrusos.

El IDS de Cisco Secure es una opción exclusiva para IP que ofrece al administrador del PIX la flexibilidad necesaria para personalizar el tipo de tráfico que requiere ser auditado, registrado y eliminado.

Las opciones son las siguientes:

- Auditoria del tráfico. Las firmas de nivel de aplicación sólo se auditan como parte de una sesión activa. La auditoria deberá estar asignada a una interfaz.
- Soporte para las distintas normas de auditoria. El tráfico que coincida con una firma desencadena una serie de acciones configurables.
- Posibilidad de desactivar la auditoria de la firma.
- Posibilidad de activar el IDS y desactivar selectivamente las acciones de una clase de firma (informativa, de ataques)

La auditoria se lleva a cabo examinando los paquetes IP a la medida que llegan a una interfaz de entrada. Si un paquete desencadena una firma y la acción configurada no elimina el paquete, ese mismo paquete podrá desencadenar otras firmas.

El Firewall PIX soporta la auditoria en la entrada de todas las interfaces. Es posible configurar individualmente las interfaces con distintas firmas, así como las acciones predeterminadas que se tomarán al coincidir una firma configurada.

4.12.1 Elementos de la configuración para la detección de intrusos

La base del sistema IDS del PIX es el comando ip audit.. Este comando se utiliza para crear las normas de auditoria globales del PIX, aquí se muestran las dos formas del comando global de ip audit:

ip audit. Attack
ip audit. Info

En cada caso, el comando ip audit especifica las acciones predeterminadas que se tomarán cuando coincida una firma de ataque o informativa. Si no hay nada configurado, la acción predeterminada para las firmas de ataque e informativas se reducirá exclusivamente al dar la alarma y se permitirá que el paquete pase o se elimine en función de cómo se haya configurado el PIX. En todos los comandos ip audit., actino puede ser cualquier combinación de alarm, drop y reset.

La sintaxis del comando ip audit. Attack es la siguiente:
ip audit. Attack [[action] [alarm] [drop] [reset]]

La sintaxis del comando ip audit info es la siguiente:
ip audit. Info [[action] [alarm] [drop] [reset]]

4.12.1.1 Configuración de las normas de auditoria sobre una base de interfaz.

Cada interfaz del PIX puede tener un máximo de dos normas de auditoria enlazadas, una para las firmas informativas y otra para las firmas de ataque. En primer lugar ,se utiliza el comando ip audit. name para definir las normas de auditoria de las firmas de ataque e informativas.

La sintaxis del comando ip audit. name attack es la siguiente:

ip audit name *nombre_auditoria* Attack [[action] [alarm] [drop] [reset]]

La sintaxis del comando ip audit. name info es la siguiente:

ip audit name *nombre_auditoria* info[[action] [alarm] [drop] [reset]]

Ahora que se ha creado las normas de auditoria, se procede a la utilización del comandoip audit. interface para enlazar a la interfaz o interfaces que se deseen proteger.

La sintaxis del comando ip audit. interface es la siguiente:

Ip audit. interface *nombre_if nombre_auditoria*

4.12.1.2 Desactivación selectiva de las firmas IDS de las normas de auditoria.

Es posible que sea necesario en un determinado entorno desactivar selectivamente las firmas IDS de las normas de auditoria, se utiliza el comando ip audit. signature disable para desactivar las firmas por número de firma. También a la inversa se utiliza el comando no ipaudit signature *número_ firma* para reactivar una firma previamente desactivada.

La sintaxis del comando ip audit. signature es la siguiente:

ip audit. signature *número_firma* disable

Se utiliza el comando show ip audit. signature para mostrar una lista de las firmas IDS desactivadas.

4.13 Forma de configurar el protocolo de configuración dinámica del host (DHCP) en el Firewall PIX.

El protocolo de configuración dinámica del host (DHCP) es un mecanismo que sirve para automatizar la configuración de as computadoras que usan TCP/IP. DHCP se puede utilizar para asignar direcciones IP de forma automática, para enviar parámetros de configuración TCP/IP, como una máscara de subred y un gateway predeterminado, y para proporcionar otra información de configuración, como las direcciones IP para los servidores DNS.

4.13.1 El servidor DHCP.

La opción del servidor DHCP del PIX fue diseñado para ser utilizado con el PIX 506 ya que fue concebido para entornos de oficinas pequeñas. Como DHCP, el Firewall PIX asigna parámetros de configuración de red a los clientes DHCP. Estos parámetros de configuración proporcionan un cliente DHCP con los elementos utilizados para acceder a la red, como la dirección IP, el gateway predeterminado y el servidor DNS.

El número de direcciones IP que soporta el Firewall PIX depende de a versión del SO del PIX y se muestra en la tabla 4.20

Versión del SO del PIX	PIX 506	El resto de plataformas PIX
5.2	10	10
5.3	32	32
6.0	32	256

Tabla 4.20 Direcciones IP según versión de SO.

4.13.2 El Cliente DHCP.

La opción del cliente DHCP del Firewall PIX está diseñada para ser usada en entornos pequeños, donde el PIX está conectado directamente a DSL o a un módem por cable que soporta la función de servidor DHCP. Con la opción de cliente DHCP activada en el PIX, éste funciona como un cliente DHCP y es capaz de obtener y configurar los siguientes parámetros en base a los datos recibidos del ISP:

- Ruta predeterminada
- Dirección y mascara de subred de la interfaz.

Para activar la opción cliente DHCP en el Firewall PIX, se hicieron las siguientes mejoras en el comando ip address:

ip addres *nombre_if* dhcp [setroute]
show ip address *nombre_if* dhcp

Se señalan nuevos comandos debug, como se muestra aquí:

debug dhcp packet
debug dhcp detail
debug dhcp error

El comando ip address dhcp permite la opción de cliente DHCP en la interfaz especificada del Firewall PIX para adquirir dinámicamente su dirección ip en unservidor DHCP ISP. Elargumento opcional *setroute* le indica le indica al PIX que establezca una ruta

predeterminada utilizando el parámetro del gateway predeterminado que devuelve el servidor DHCP. El uso de la opción *setroute* no es necesario si ha configurado manualmente una ruta predeterminada con el comando *route*.

Los comandos debug dhcp proporcionan herramientas de solución de problemas para las opción de cliente DHCP activada.

4.13.3 Configuración del PIX como servidor DHCP: dirección externa estática.

(configura ambas interfaces “activadas” a 10 Mb, semiduplex)
interface ethernet0 10baset
interface ethernet1 10baset
(configurar interfaces internas y externas con direcciones IP estáticas)
ip address outside 220.26.55.63 255.255.255.0
ip address inside 192.168.111.1 255.255.255.0
(enseña al PIX a usar la dirección IP de la interfaz externa para PAT)
global (outside) 1 interface
(permite que todos los usuarios del interior se conviertan en direcciones PAT)
nat (inside) 1 0.0.0.0 0.0.0.0
(indica al PIX donde se encuentra el gateway predeterminado)
route outside 0.0.0.0 0.0.0.0 220.26.55.1 1
(crea un pool de direcciones en la interfaz interna para asignar usuarios internos)
dhcp address 192.168.111.5-192.168.111.10 inside
(deja que el PIX especifique hasta dos direcciones IP para los servidores DNS)
dhcp dns 192.108.254.12 192.108.254.27
(predeterminado: establese el lease DHCP a 3600 segundos)
dhcp lease 3600
(deja que el PIX configure la denominación de dominio del cliente)
dhcpdomain mydomain.com
(activa el servidor DHCP en la interfaz interna)
dhcp enable incide

4.14 Configuración de el protocolo Shell seguro (SSH) en el Firewall PIX.

SSH (Shell seguro) es un programa que se registra en otras computadoras de una red, que sirve para ejecutar comandos en un equipo remoto y para mover archivos de un equipo a otro. Proporciona una autenticación robusta y comunicaciones seguras en redes no seguras.
El uso de SSH ofrece una alternativa más segura que Telnet, que envía todos los datos en texto plano. En una sesión SSH, todos los datos, incluyendo el registro y la introducción de contraseña iniciales, estan cifrados con el cifrado DES o 3DES. La clave de sesión simétrica es encriptada por el cliente SSH utilizando el cifrado RSA y es enviada de modo seguro al servidor SSH.

4.14.1 Como configurar el PIX para el acceso SSH.

Existen dos conjuntos de tareas que hay que realizar con el fin de utilizar SSH para acceder al PIX:

4.14.1.1 Configurar el PIX para que acepte conexiones SSH.

Paso 1 Asignar un nombre de host y un nombre de dominio al PIX. Esto es necesario para generar el conjunto de claves RSA.

Pixfirewall(config)# hostname percival
Percival(config)# domain-name cisco.com

Paso 2 Generar un par de claves RSA y guarde la clave en la memoria flash.

Percival(config)# ca generate rsa key 2048

Paso 3 Visualice la clave pública RSA recién creada.

Percival(config)#show ca mypubkey rsa
% key pair ……..

Paso 4 Una vez generadas las claves, deberá guardar la memoria flash. Si no se sigue este paso, se borrarán las claves en la siguiente carga.
Percival(config)# ca save all

Paso 5 Especifique que hosts están permitidos para SSH en el PIX y establezca el tiempo de espera de inactividad SSH. En este caso limitará el acceso SSH a un solo host y finalizará las sesiones transcurridas una hora de inactividad.
Percival(config)# ssh 192.168.111.7 255.255.255.0 inside
Percival(config)# ssh timeout 60

Paso 6 Establezca la contraseña de activación y la contraseña de Telnet. Se le pedirá que introduzca la contraseña Telnet para autenticar su sesión SSH
Percival(config)# enable password hardgue$$
Percival(config)# password Ace$$D3n13d

4.14.1.2 Configurar el cliente SSH para que se conecte con el PIX.

Antes de poder conectarse con el PIX por medio de SSH, se tendrá que instalar un cliente SSH que sea compatible con su plataforma. Para visualizarlo mas claramente se realiza el siguiente ejemplo.

En este ejemplo se usa uncliente SSH de SSH Comunications.

Paso 1 Iniciar el software de cliente SSH

Paso 2 Seleccionar Setting en el menú de edit.

Paso 3 hacer clic en el elemento Conection de la lista profile Setting del panel de izquierdo. En el campo hostname, ingresar la dirección Ip del PIX. Escribir pix en el campo User name. A continuación, en el panel Authentication Methods, hacer clic en password.

Paso 4 hacer clic en el elemento Cipher List . Anular las marcas de todos los cifrados, a excepción del que vaya a usar. Una vez seleccionado el cifrado, utilizar la flecha hacia arriba para trasladar el cifrado elegido a la parte superior de la lista.

Paso 5 Para no introducir esta información cada vez que inicie el cliente SSH, elija Save Setting en el menú file.

Paso 6 Abrir el cuadro emergente de inicio de sesión haciendo clic en el boton de Quick Connect.

Paso 7 debido a los potenciales puntos débiles de la versión 1 de SSH, este cliente SSH le avisa hacer clic en el botón Yes para continuar.

Paso 8 Si es la primera ves que se ha conectado con el PIX con SSH, deberáintercambiar claves públicas para cifrar la sesión. El cliente SSH le insta a que acepte la clave pública del PIX.

Paso 9 Una vez guardada la clave pública del Pix, elcliente SSH le preguntará la contraseña de Telnet.

Paso 10 Ya se creó una conexión segura con el firewall PIX.

CAPITULO V

Caso practico con PIX 501

5.1 Características básicas de CISCO PIX.

Dado que la serie de Firewalls Cisco PIX, son “todos iguales”, en el sentido de tipo de administración, características básicas como protocolos IPSec manejables, características de Firewall, etc. La diferencia radica en la robustez como máquina, licencias firewall o VPN IPSec soportados, vamos a presentar las características básicas de PIX 501.

5.1.1 CISCO PIX 501.

Dentro de la serie de firewalls Cisco PIX, este es el más pequeño, está orientado a un segmento SOHO, su método de seguridad Firewall se basa en el método Stateful Packet Firewall usando el algoritmo ASA (Adaptive Security Algoritm).

Su administración local y remota se basa en línea de comandos y PDM (administración por https).Antes de administrarlo via https es necesario habilitar este modo via consola y además indicar cual de sus interfaces y segmento de red estará autorizado para ingresar a PDM.

Cisco PIX 501	
Versión de Firmware	PIX Versión 6.3
Procesador	AMD 133 Mhz
RAM	16Mb
Flash	8Mb
Troughput Firewall	10 Mbps cleartext firewall
Número de usuarios Firewall	10 (opcional con licencia 50 usuarios)
Números de túneles IPSec concurrentes.	Con ver. IOS 6.1 (3) hasta 5. Con ver. IOS 6.3 hasta 10
Troughput VPN	3Mbps (3DES – SHA 1)

IPSec	
Encriptación	CBC – 3DES (recientemente vienen habilitados de fabrica con 3des)
Autenticación	HMAC – MD5 – SHA
Modos Configuración VPN	Preshared key – Certificados
Perfec Forward Secrecy – Diffi hellman Group	1 -2

Los métodos de configuración VPN soportados son en Preshared Key y Certificados, no soporta Manual Key.

El número de usuarios o licencias Firewall de este equipo es de 10, 50 o ilimitados.

5.1.2 Configuración por defecto.

Podemos dividir las características de fábrica de este equipo, en los tres ítems que se presentan a continuación:

- **General.** El equipo viene de fábrica, con IP Default y las interfaces Inside y Outside ya definidas, aunque viene sólo con la herramienta básica de administración y configuración como lo es consola, tampoco viene con DHCP habilitado, ni con Internet settings definidas (PPPoE, DHCP cliente o IP fija). También por defecto viene denegado el ping, por ello es necesario habilitarlo si es necesario, con el comando conduit.

- **Firewall**. Por defecto viene con todo el tráfico WAN >> LAN Bloqueado, es decir que no permite abrir sesiones desde Internet, hacia la interfaz Inside. Respecto al tráfico en sentido inverso al anterior, es decir LAN >> WAN, viene todo habilitado.

- **VPN IPSec** Con versión de IOS 6.3 el PIX 501 puede soportar hasta 10 túneles IPSec, esto significa que puede tener en conjunto, entre VPN Lan to Lan y remote Access o VPN cliente, hasta 10.

También de fábrica estos equipos tienen licencia o vienen habilitados para hacer 3DES, DES, SHA, Diffie Hellman 1 y 2, MD5, pueden autenticar a un (o más) usuario (para el caso de VPN Remote Access), en forma local sin necesidad de contar con un servidor AAA Radius o Tacacs.

Para el caso de los softwares VPN Remote Access, sólo es necesario tener una cuenta CCO para poder bajarlos de la página Web de Cisco.

5.2 Configuración básica de CISCO PIX.

Nos referimos a configuración básica de Cisco PIX, a la configuración que se debe hacer antes de iniciar el levantamiento de una VPN o configuración Firewall, es decir para dejar operativo el firewall y con conectividad a nivel Outside e Inside.

5.2.1 Configuración Básica Cisco PIX 501.

Para comenzar a configurar este equipo se puede usar consola (y en realidad este es el método principal para hacerlo en forma local), o usando https, aunque igual se debe habilitar antes este método, por lo que comenzaremos por consola.

Al igual que cualquier router Cisco, ingresaremos al Firewall con Hyperterminal y con las settings acostumbradas, es decir bits por segundo 9600, bits de datos 8, paridad none, bits de parada 1, control de flujo none.

Por defecto el Cisco PIX 501 no viene con password enable, por lo que un enter bastará. También cabe mencionar que los comandos y el modo de ayuda de los PIX difiere un poco de los routers habituales.

Suponiendo que el equipo está con la configuración de fábrica, comenzaremos con la configuración de las respectivas IP.

5.2.1.1 Configuración de IP y conectividad a nivel LAN y WAN.

Vamos a suponer que tenemos una IP pública estática asignada, con la correspondiente máscara, Default Gateway, etc. Y que los host de la red interna, saldrán hacia Internet haciendo PAT, por último la versión de IOS con la que trabajaremos será 6.3.

Para configurar conectividad básica del equipo siga la siguiente línea de comandos en modo de configuración global:

<*estos comandos son equivalentes al no shutdown de los routers*>

interface ethernet0 10baset
interface ethernet1 10full

<para asignar ip a la interface trust o lan, por ejemplo en el segmento 192.168.x.x. Usaremos esta IP sólo como ejemplo en esta y las sgtes. Líneas de comando>

ip address inside 192.168.x.x 255.255.255.0

<*habilitar nat en todas en todas la ip inside y global para habilitar port address translation en la interface outside. En este caso 1, representa el ID del nat*>

nat 1 0.0.0.0 0.0.0.0
global 1 interface

<*colocar ip a la interface outside. Nótese que sólo como ejemplo hemos colocado 200.72.X.X, la IP Outside puede ser cualquier IP pública.* >

ip address outside 200.72.x.x 255.255.255.248

<Define una ruta por default y además habilita el ping >

route outside 0.0.0.0 0.0.0.0 200.72.x.x 1
conduit permit icmp any any

< Configura al PIX para que sea DHCP server hacia la interface Inside. Esta línea de comandos es opcional.>

dhcp address 192.168.x.x-192.168.x.x inside
dhcp enable inside
dhcp dns 200.72.1.5 200.72.1.11

<habilitar PDM, Pix Device manager, administración por GUI o https >

http server enable
http 192.168.x.0 255.255.255.0 inside

<habilitar telnet >

telnet 192.168.X.X 255.255.255.0 inside

<Habilitar administración Remot*a. Si no se ejecuta esta línea de comandos, no será posible ingresar al Firewall desde Internet, aunque se haya habilitado un VPN cliente con este objetivo. >*

management-access inside

<Guardar los cambios >

wr mem

Esta es nuestra primera etapa y el Cisco PIX ya debería estar conectado hacia Internet y con los host internos también conectados y pasando por el PIX.

5.2.1.2 Crear cuentas de usuario (para PDM, VPN Client, Telnet, etc.).

Cisco PIX, puede ocupar una base de datos local para autenticar usuarios, o también definir un servidor TACACS o RADIUS externo, para que autentique a los usuarios que en uno u otro escenario deben ingresar User y Password, como por ejemplo para VPN Client, PDM, telnet, etc. (esto cuando se indica al Firewall que los usuarios deben autenticarse para usar estas herramientas).

Antes de continuar con la explicación de cómo configurar cuentas de usuario, es necesario indicar algunas consideraciones:

a) Como se vio anteriormente, se debe ingresar el comando *management-access*, para permitir el acceso a la administración del Firewall usando VPN Client. Si no se tiene cuidado en proporcionarle los derechos de acceso apropiados a cada cuenta, entonces podemos encontrarnos fácilmente con usuarios remotos que pueden ingresar al Firewall a hacer algún tipo de configuración.

b) Existen 3 niveles de autorización para cada cuenta:
   Admin – nivel 15 – Lectura y escritura
   Read only- nivel 5 – Sólo lectura
   Monitor only – nivel 3 – Sólo monitorización del firewall

c) Los 3 niveles de administración del Firewall, no tienen relación con que este va a filtrar o bloquear protocolos en uno u otro caso, o permitir o denegar acceso a una u otra red, sino que solamente tiene relación con los niveles de autorización cuando el cliente ingresa al PDM, telnet, etc. del Firewall.

d) Dado lo anterior, todo usuario que tenga un software VPN Client en su PC, y luego se conecte al Firewall, podrá acceder a la herramienta PDM, telnet,, con la misma cuenta que se autentica para realizar la conexión VPN Cliente hacia su red corporativa. Que esta cuenta tenga derecho a sólo lectura, es responsabilidad del administrador del mismo equipo.

Para crear cuentas de usuarios vamos a utilizar PDM en esta ocasión, para ello siga las instrucciones que a continuación se indican:

a) Ingrese al PDM de PIX, usando https, por ejemplo si la IP Inside del equipo es 192.168.1.1, entonces usando su web browser, coloque en la barra de direcciones: https://192.168.1.1. Para ingresar a PDM debe contar con algunos requisitos mínimos, como por ejemplo JDK instalado para el browser

b) Si ya entró a PDM debería estar ubicado directamente en el Home y ver la pantalla de la figura 5.1.

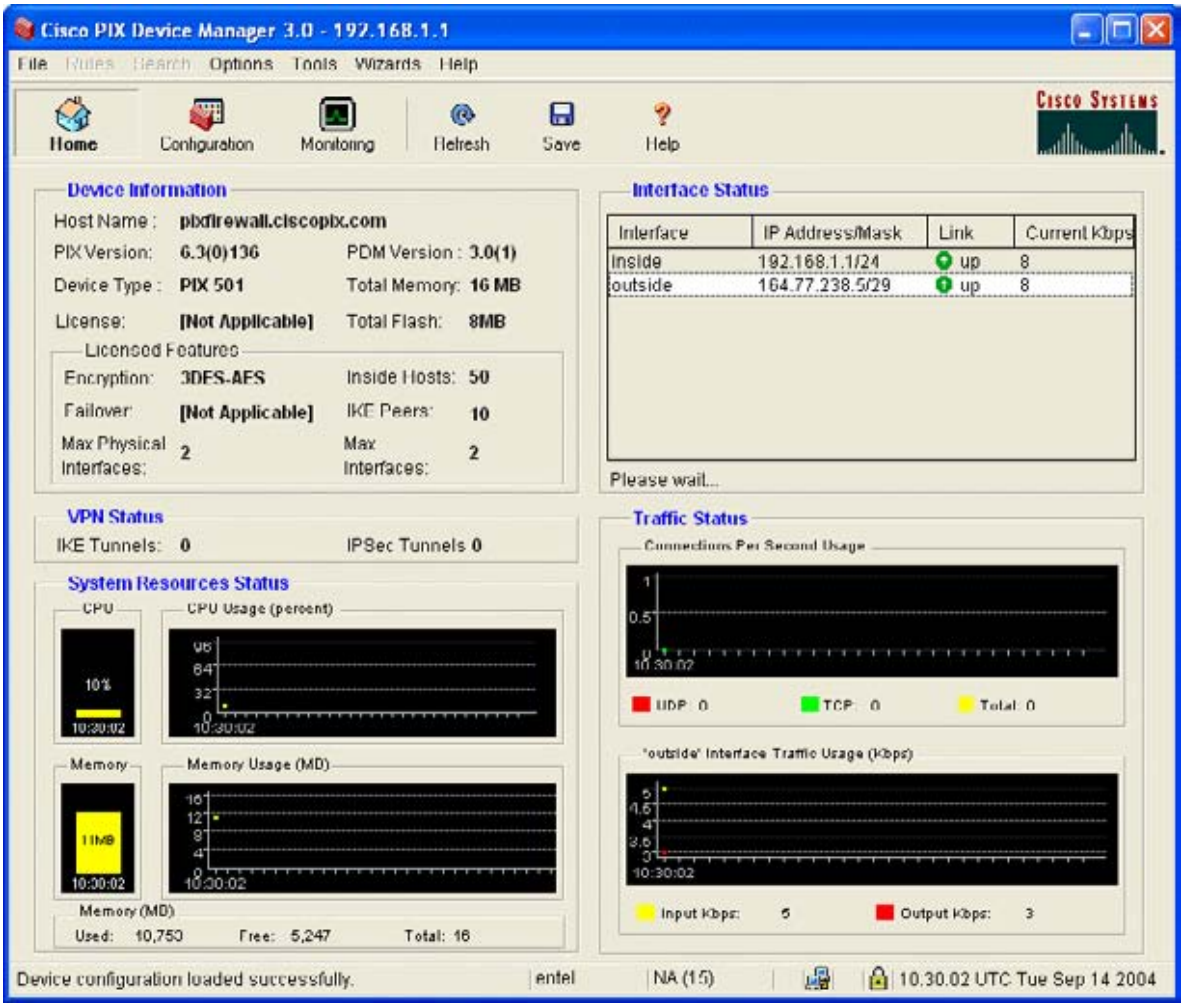


Figura 5.1. Vista principal de cisco PDM (ver 3.0). Se observa que existe una gráfica de los Recursos utilizados en el equipo, como por ejemplo porcentaje de CPU, RAM, tráfico.

c) Para continuar debe hacer click sobre el icono **Configuration** , luego sobre el menú **Administration - User Accounts** . (Figura 5.2)

Figura 5.2. Agregando un nuevo usuario a la base de datos local.

d) Click sobre el botón **Add** , luego ingrese el **User, Password** y **level privileges** respectivos. En este caso vamos agregar el usuario admin con password admin, level privilege 15, para que sea usado por la unidad de provisión o mantención. Para el caso de usuarios remotos que usen VPN Client, el level privilege debe ser de nivel 3 o 5.

e) Click en el botón Ok, luego en Apply, luego en el icono , para guardar los cambios a la flash.

f) Siga el mismo procedimiento para agregar al menos 2 usuarios, con **level privileges 5** , para ser usados en la configuración de VPN Remote Access.

5.2.1.3 Habilitar autenticación para ingresar a PDM, telnet y consola.

Para evitar que cualquier persona ingrese a las herramientas de administración del Firewall y consecuentemente tener métodos de seguridad mínimos respecto a esto, se recomienda habilitar el acceso a estas herramientas con prompts de autenticación (en forma adicional puede habilitar password enable para CLI).

Para hacer esto se usan las mismas cuentas creadas en el apartado anterior para cualquier operación que involucre acceso a las herramientas de administración de PIX.

Para habilitar autenticación cuando un usuario trate de ingresar a PDM, telnet, consola, etc, debe seguir el procedimiento:

a) Ingrese a PDM, luego click en icono **Configuration** , diríjase al menú **Administration – Authentication/Authorization** .

b) Tache todas las opciones que aparecen en el lado derecho de la ventana (y seleccione la autenticación LOCAL), para que PIX pida autenticación para el uso de cada una de las herramientas de administración. Click en el botón **Apply** para aplicar los cambios. Es probable que aparezca una nueva ventana mientras se aplican los cambios, preguntando si desea que PDM asocie cada comando disponible a los niveles de privilegio por defecto para Admin, Monitor Only y Read Only, click en botón **Yes** .

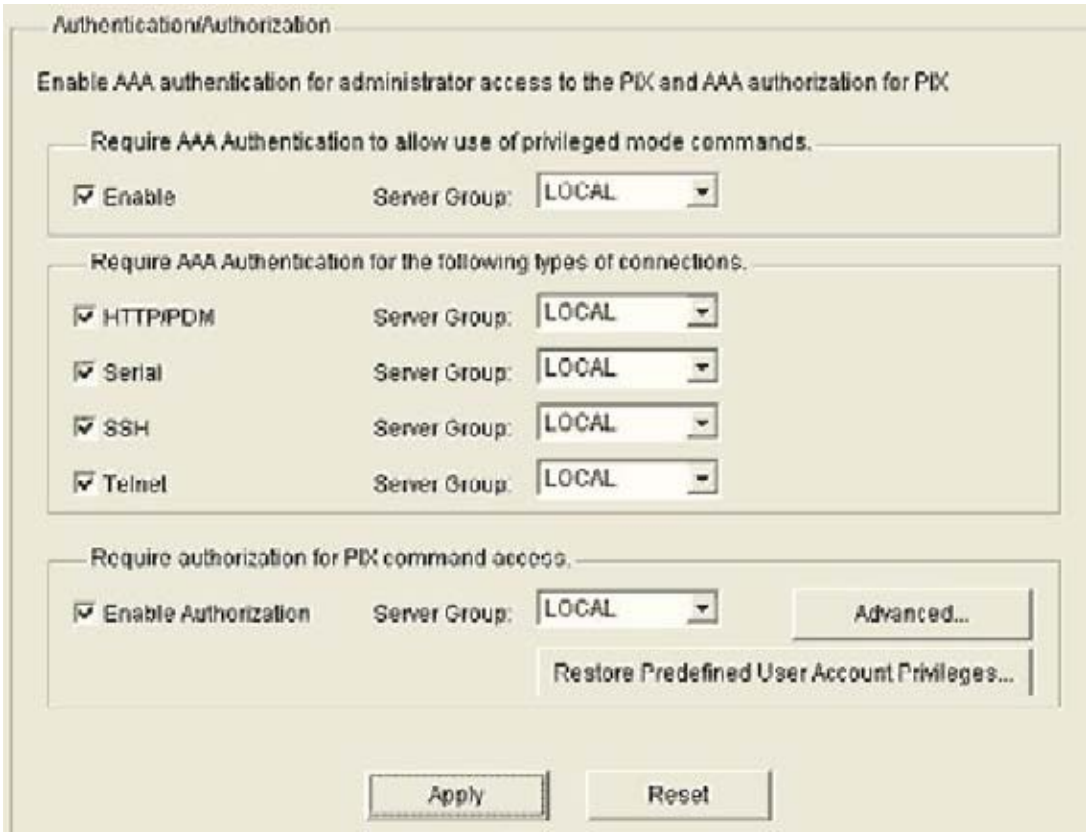


Figura 5.3. Habilitando autenticación para acceso a herramientas de administración.

5.2.1.4 Administración SSH, telnet y PDM (Gestión Remota).

Para administrar en forma remota el Firewall Cisco PIX, existen dos métodos básicos, los cuales son el uso de VPN Client, para ingresar en forma remota al Firewall. De esta forma se puede acceder a la herramienta GUI (Graphical User Interface) PDM y telnet (CLI), en esta última sólo se tendrá acceso a configuración por comandos, por lo que Cisco recomienda usar la primera alternativa y como opcional SSH.

Usando la topología de para mantención remota, el administrador debe contar con el software VPN Client (3.X o 4.X) instalado en su PC, un acceso Internet, luego de esto se debe conectar a la IP Outside del Firewall y finalmente usar telnet o PDM apuntando a la IP Inside del Firewall. Por ello entes de ejecutar esta operación es necesario que el instalador habilite una VPN Client en PIX para hacer mantención sobre el mismo equipo

Para habilitar las herramientas de administración del Firewall Vamos a suponer que la IP del PIX es la 192.168.168.1/24

a) Telnet

Para configurar telnet y habilitarlo a la interface Inside, en modo de configuración global se escriben los siguientes comandos:

telnet 192.168.168.x 255.255.255.0 Inside

Donde la IP 192.168.168.x y la correspondiente máscara corresponden a la IP que tiene el PC que estará autorizado a usar telnet o también puede quedar habilitado a toda la red (192.168.168.0). Si quiere configurar el tiempo timeout permitido para esta conexión, puede usar el comando

telnet timeout (minutos).

b) PDM.

Para configurar el acceso a la administración del equipo por PDM, es necesario habilitar el “servidor” http e indicar cual de las interfaces o IP estará autorizada para ingresar.

http server enable
http 192.168.168.x 255.255.255.0 inside

Los comentarios son los mismos que para telnet. Además considerar que PDM se trata de configuración del firewall usando web seguro o http de un browser.

Para el caso gestión remota por telnet y PDM, es necesario después configurar un Túnel IPSec para lograr ingresar por la interfase Outside y además usar el comando Management-access.

c) SSH.

Para configurar ssh y administrar el firewall en forma remota, es necesario antes colocar un hostname al equipo, luego generar un certificado (RSA key – pair) y guardar el key-pair resultante usando el comando ca save all.

Para usar SSH, es necesario que el PIX venga habilitado con DES o 3DES, pero esto no es problema ya que de fábrica este equipo viene activado para hacer 3DES, además para acceder al firewall por SSH, se debe ingresar como Username pix y como password, el password de telnet (por defecto el password de telnet es cisco).

5.3. Configuración de VPN.

5.3.1 Introducción.

Para configurar una VPN, podemos tener 3 escenarios posibles, el primero una VPN Lan to Lan punto a punto, el segundo una VPN Lan to Lan Multipunto (que a su vez se puede dividir en full meshed o partial meshed) y el último una VPN cliente.

A modo de ejemplo y para explicar las posibles configuraciones de los firewalls, podemos graficar estos escenarios en las siguientes figuras:

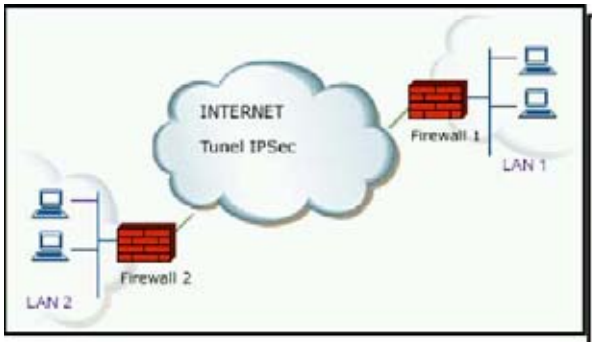


Figura 5.4. VPN Lan to Lan

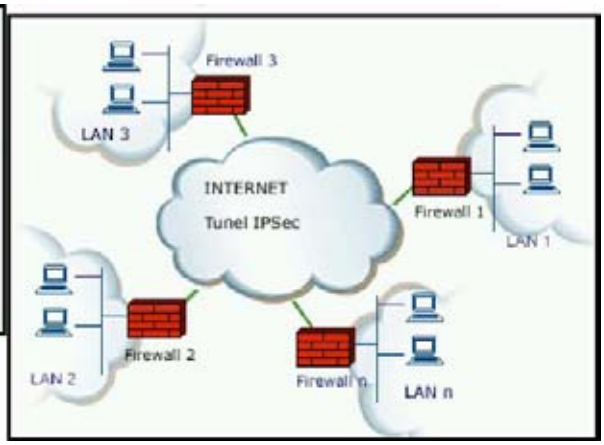


Figura 5.5. VPN Lan to Lan Multipunto

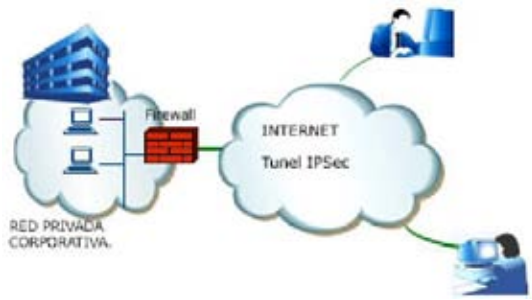


Figura **5.6**. VPN cliente (o remote access)

En esta oportunidad veremos el VPN cliente por ser el mas usado para mantención remota.

5.3.2 Configuración VPN Remote Access.

5.3.2.1 Configuración VPN Remote Access en Firewall.

En este caso usamos la interface de administración por https o PDM, antes de comenzar con la configuración del Remote Access o VPN cliente, obviamente debe estar habilitado el *http server* (via comandos) del firewall y además que al menos la IP del PC que se destina para hacer la configuración, esté autorizado a usar esta herramienta

Recordar que esta configuración también es válida para acceder al equipo en forma remota y lograr administrarlo, salvo que para este último caso es necesario habilitar la administración a través del comando *management-access* y que además la cuenta del usuario que se autentica por VPN tenga *Privilege level 15*.

Se configurará un VPN Remote Access (o VPN Cliente), con versión de PDM 3.0 (PIX Device Manager) y en el caso del software usado para el cliente Remoto, un VPN Remote Access 3.6. El Software VPN de Cisco es gratuito y se puede bajar desde la página de Cisco, Existen versiones para Windows 9X, 2000, XP, etc. Para descargar software VPN cliente, debe loggearse en la página Cisco, luego ingresar al sgte link: http://www.cisco.com/cgi-bin/tablebuild.pl/vpnclient-3des

Para configurar el acceso de un cliente VPN remoto, o Remote Access, siga el sgte. procedimiento:

a) Ingrese a la administración por PDM (PIX Device manager o administración por https), click en el Menú Wizards – VPN Wizards. Click botón Next.

Figura 5.7. Abriendo el Wizard que permite configurar VPN.

b) Ahora de la nueva ventana que aparece, seleccionar la opción **Remote Access VPN** y además la interface que se habilitará para esta VPN, en este caso **Outside**. Click botón **Next**.

c) Seleccione el software VPN cliente que usará el cliente remoto, en este caso seleccionamos **Release 3.X or Higher**. Click botón **Next**.

d) En el siguiente paso se configura un nombre para el Group VPN, en este caso usamos para **Group Name TESIS** y como **preshared Key (Group password)**, entel123. Click botón **Next**.

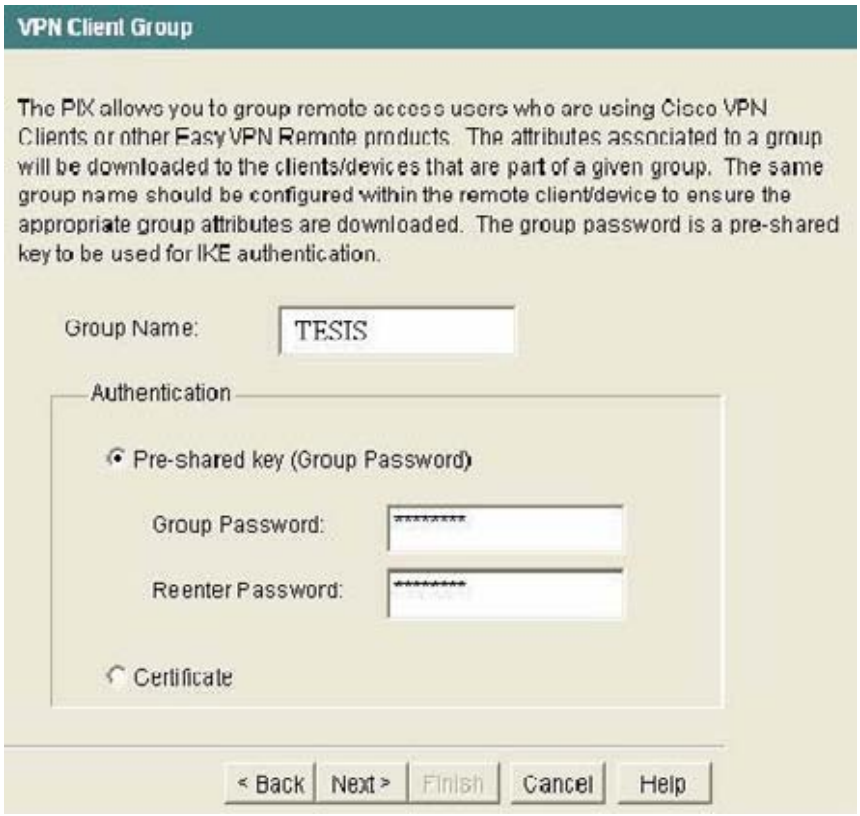


Figura 5.8. Configuración del Group name y Preshared-Key.

e) Ahora se debe habilitar la autenticación local (también se podría usar un AAA Radius o Tacacs interno en la red del cliente) para ello tache la opción **Enable Client Extended Authentication**, y para la opción Extended Authentication for Group TESIS, seleccione **LOCAL**. Click botón **Next**.

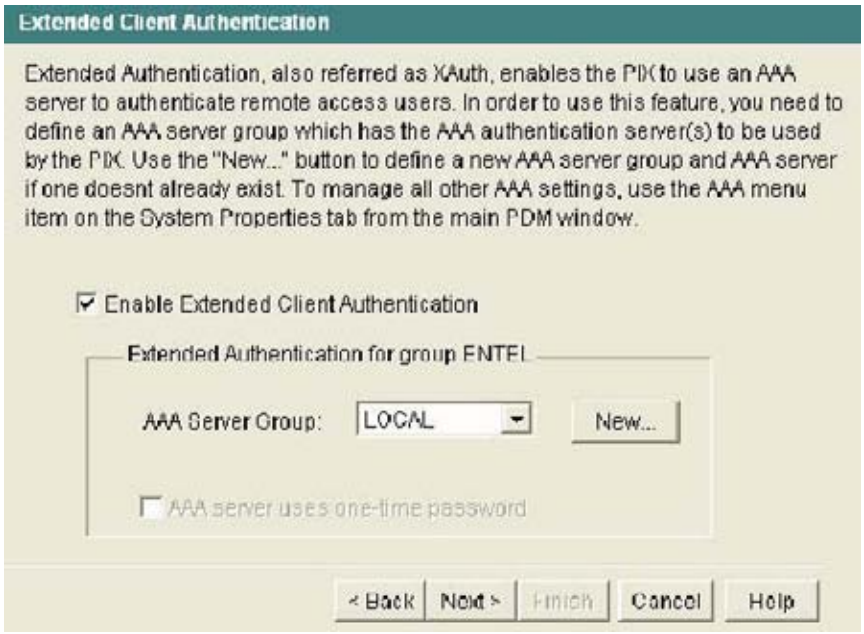


Figura 5.9. Habilitación de Xauth, con autenticación interna.

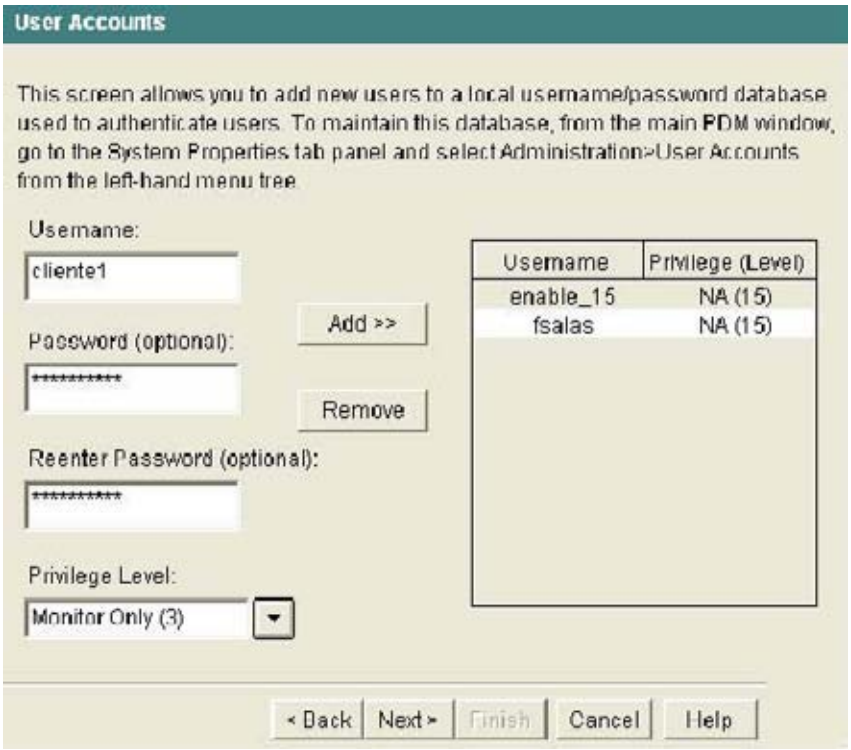


Figura 10. Configuración de usuario para ser autenticado en forma local una vez que trate de conectarse a la red privada con el VPN Remote Access. Observar que para el caso de usuarios que no deben tocar la configuración del Firewall, el Privilege Level debe ser 3 o 5.

f) Es necesario crear un usuario que será autenticado en forma local una vez que se conecte con el software VPN (figura 10). En este caso creamos un usuario con **Username** cliente1, y **Password** cliente123, en **Privilege Level**, lo dejamos con el menor de los privilegios posibles ya que no necesitamos que este usuario haga algún tipo de configuración en el equipo. Click en el botón **Add >>** para agregar este usuario. Click botón **Next**.

g) Para agregar un Pool de IP dentro del cual se le asignará IP al cliente, usamos un rango que permita al cliente Remoto obtener una dentro del mismo segmento de red a la que quiere acceder (en este caso la red privada usa el rango 192.168.168.0/24). Click botón **Next**.

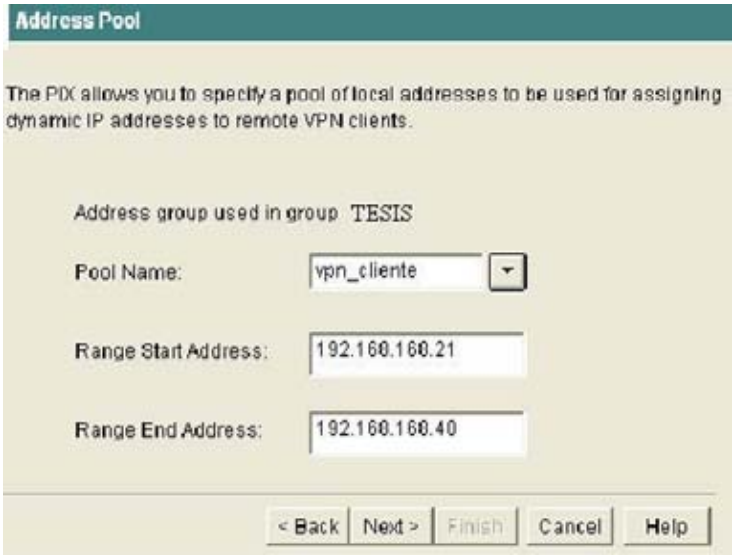


Figura 5.11 Configuración de Pool de IP de los que obtendrá IP el usuario VPN Remote Access.

h) La información que solicita el Wizard en este paso es opcional, básicamente pregunta por los DNS y WINS server que se asignarán al VPN Remote Access. Click botón **Next**.

i) Llega la configuración de protocolos IPSec para la negociación IKE (Fase1), en este caso seleccionamos para **Encryption** 3DES , **Authentication** SHA, **DH Group** Group 2 (1024 bits), esta combinación de protocolos seleccionados se considera muy seguro. Click botón **Next**.

j) Para fase 2 o protocolos del túnel IPSec, seleccionamos **Encryption** 3DES , **Authentication** SHA. Click botón **Next**.

k) La última parte de este Wizard nos pide indicar que segmento de red (Interna), no se aplicará NAT cuando los usuarios ingresen por Remote Access. Para este caso seleccionamos el segmento de red interno (Inside) y luego click en el botón **>>**, para agregarlo, luego se **debe tachar** la opción **Enable Split Tunneling …** para permitir a los usuarios remotos ingresar a su sitio corporativo y además mantener la conexión a Internet, finalmente click en botón **Finish**.

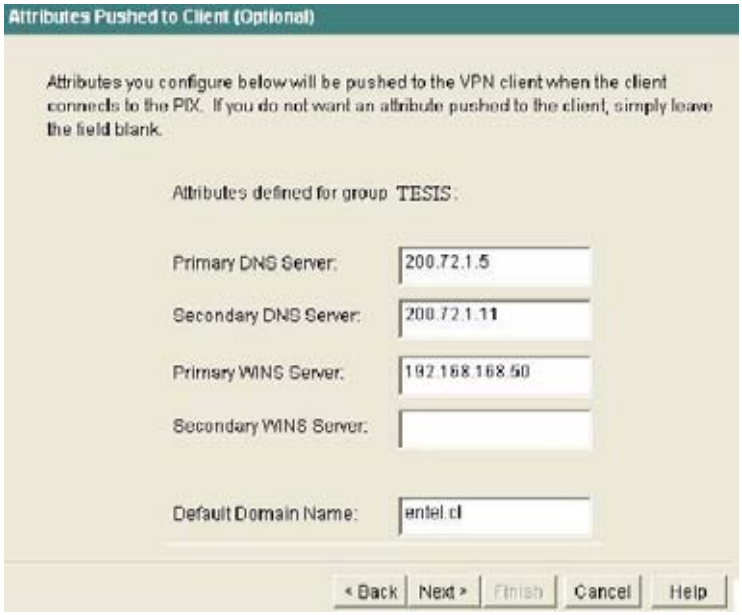


Figura 5.12.Configuración de IP de red adicional y opcional para el VPN Remote Access.

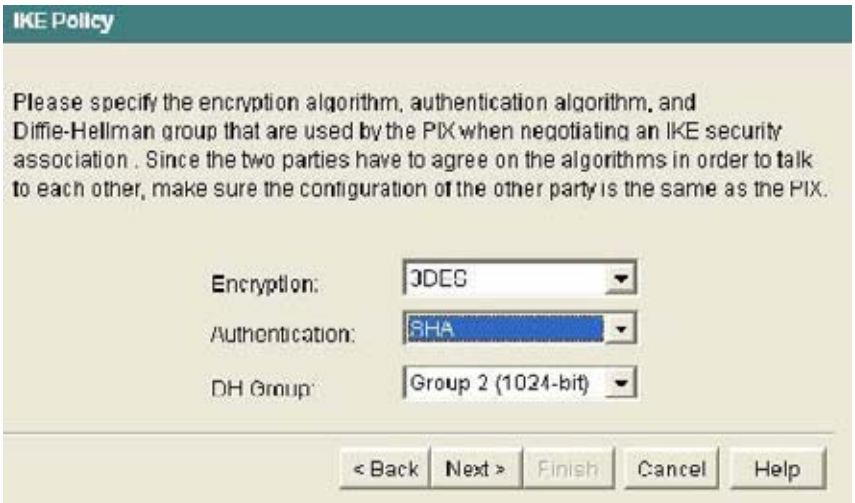


Figura 5.13. Configuración de protocolos IPSec para la fase 1 IKE.

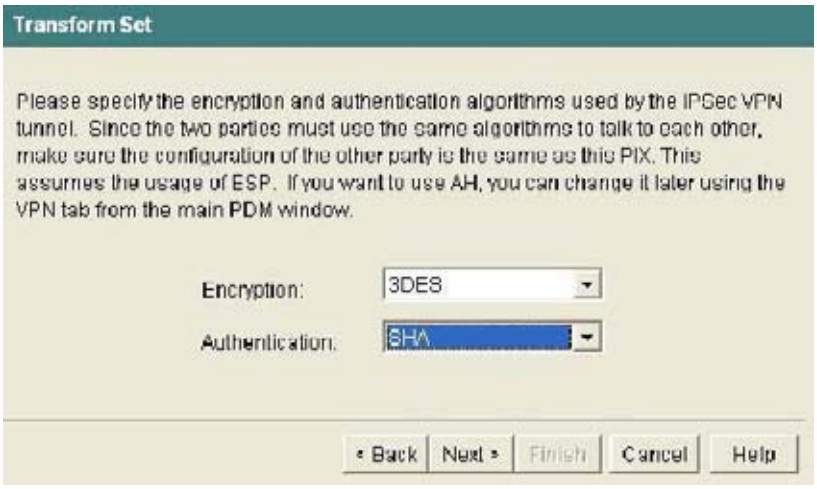


Figura 5.14. Configuración de protocolos de encriptación y Autenticación para la fase 2.

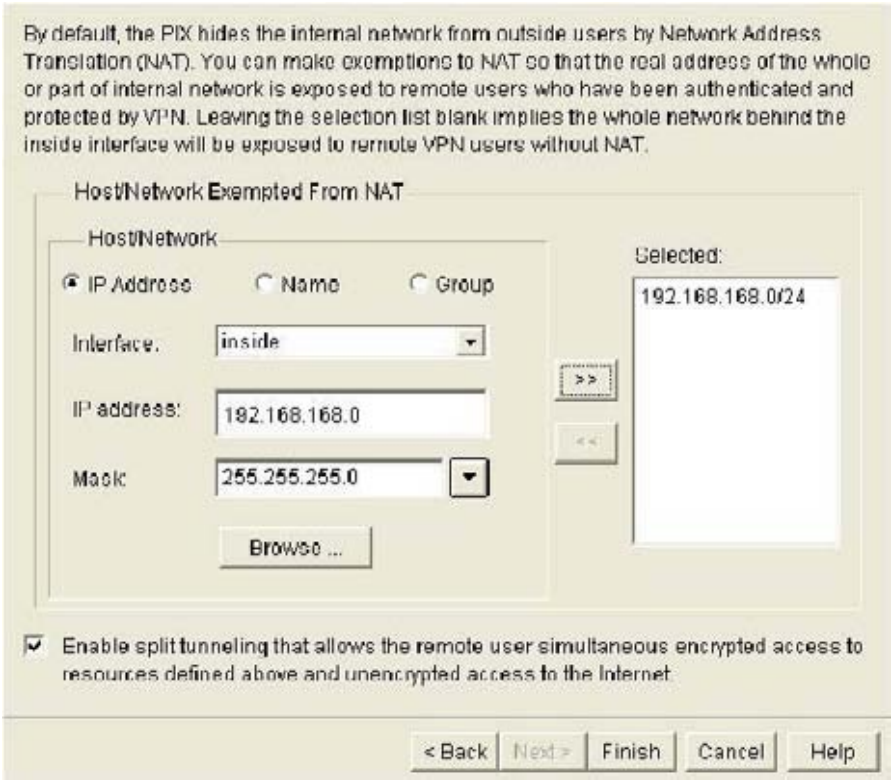


Figura 5.15. Parte final.

La figura 5.15 muestra la parte final del Wizard, nos pide indicar que segmento de red interno no se aplicará NAT, al momento que ingrese un usuario via Remote Access. Además se debe habilitar split tunneling para que el usuario remoto no pierda su conexión a Internet una vez que ha levantado el túnel VPN con su Sitio Central.

5.3.2.2 Configuración del software VPN client.

5.3.2.2.1 VPN Client 3.6.

Una vez que ya se configuró el Firewall para recibir el requerimiento de negociar las llaves y luego levantar túnel IPSec desde Internet, podemos configurar el software en el PC que hará este requerimiento al PIX.

Figura 5.16. Vista principal del VPN cliente 3.6 de Cisco.

Para comenzar veremos la configuración necesaria en el software VPN cliente de Cisco versión 3.6. Para configurar una conexión Remote Access al firewall, siga los sgtes. Pasos:

Figura 5.17. Ingresando texto descriptivo para la conexión VPN.

a) Abra el programa VPN cliente 3.6 (Archivos de programa).

b) Click en el botón **New**, luego en la casilla que pide un nombre descriptivo para la entrada, ingrese conexión 1 o algo similar, idem en la descripción de la entrada, click en botón **Siguiente**.

c) Ingrese la IP Outside del Firewall PIX al que se conectará el cliente (en este caso colocamos 164.77.238.5). Clic en botón **Siguiente**.

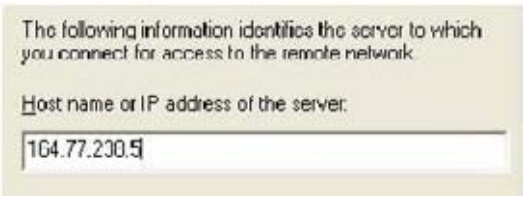


Figura 5.18. Ingresando IP Outside del Firewall PIX.

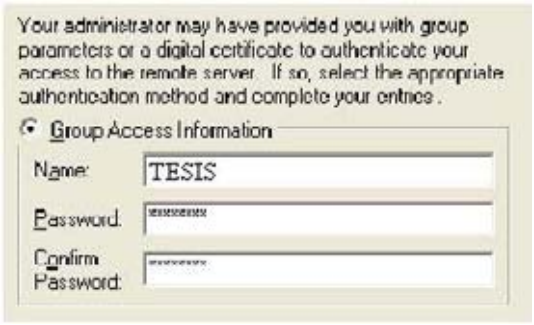


Figura 5.19. Configurando preshared Key o Group Access Information.

d) Ahora debe colocar el **Group Access Information**, esto significa usar el mismo nombre del grupo configurado en el firewall (en configuración anterior del firewall usamos Group Name: TESIS y Group password: entel123).

e) Click finalmente en el botón **Finalizar**.

f) Como podrá observar ahora ya se encuentra configurado nuestro acceso a la red o lugar de trabajo, para conectarse, sólo debe seleccionar la entrada creada y luego hacer click en botón **Connect**.

Una vez que el software se encuentra en proceso de conexión hacia el firewall (obviamente se debe iniciar una conexión hacia Internet antes), 1 o 3 segundos después aparece una pequeña ventana que pide ingresar user y password del cliente que está tratando de conectarse y que anteriormente también se configura en el PIX (en la configuración anterior agregamos el usuario cliente1 y password cliente123), luego al momento de aparecer esta ventana el cliente debería usar en este caso el user: cliente1 y password: cliente123.

Si se ha conectado exitosamente, se puede ver en propiedades de conexión de red o en las estadísticas del software que el PC cliente ha obtenido IP del rango que se ha especificado en la configuración Remote Access del firewall.

Finalmente se observa que para el caso de la configuración del Software VPN client, no se configuran protocolos IPSec ni de autenticación ni de encriptación, esto significa que el software negocia junto con el firewall el protocolo a usar, de hecho al hacer un debug en el firewall, se observa que ambos extremos comienzan sus propuestas mutuas de protocolos a usar, comenzando por los de mayor nivel de encriptación hasta el menor.

En laboratorio, se hicieron pruebas tratando de configurar un VPN Remote Access usando encriptación DES, aunque los softwares sean capaces de Trabajar con 3DES (3.6 y 4.0), esto dio como resultado que en la negociación de protocolos, tanto el firewall como el software no llegaran a acuerdo y por lo tanto el VPN Remote Access no funcionara. Como resumen y conclusión se deduce que tanto el VPN client 3.6 y 4.0 sólo trabajarán con encriptación 3DES.

5.3.2.2.2 VPN Client 4.0.

Para el caso del VPN client 4.0, el procedimiento de configuración es muy similar al 3.6, por lo que no entraremos tanto en detalle esta vez.

Para configurar una entrada en forma similar a la anterior, debe abrir este software, luego hacer click en el icono o botón **New**, luego ingresar todos los parámetros necesarios, como se observa en la figura 18, finalmente click en el botón Save y luego se selecciona la entrada creada para luego hacer click en el botón **Connect**.

Figura 5.20. Ingresando los parámetros necesarios para la nueva entrada.

Figura 5.21. Se observa la conexión nueva en la ventana principal del VPN client. Para conectarse al sitio remoto, sólo basta (antes se debe tener conexión a Internet) con seleccionar "Mi Conexión 1" y luego hacer click en el botón Connect.

5.3.2.2.3 Importar o rescatar una configuración hecha.

Respecto a la configuración, aunque como queda claro la configuración en el software es bastante sencilla, es posible importar una entrada ya creada y agregarla como si la hubiésemos creado en forma manual.

Por ejemplo en el caso de la configuración hecha con el VPN Client 3.6, podríamos rescatar la entrada si nos dirigimos a la carpeta "Archivos de programa\Cisco Systems\VPN Client\Profiles", luego copiamos el archivo (cada configuración pesa aprox. 1 kb) a algún directorio o unidad de memoria, y finalmente la importamos desde el programa abierto con la opción Import.

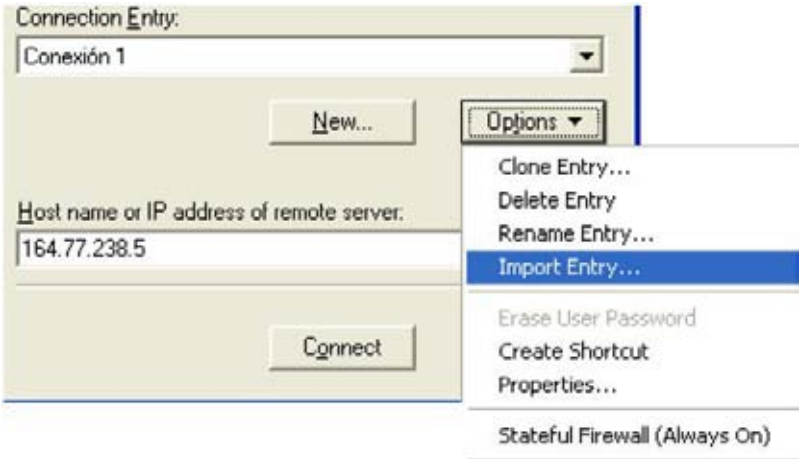


Figura 5.22 Importar una entrada VPN

Es posible importar una entrada VPN remote Access, Usando la opción del software que dice Import, como indica la figura 5.22. Una vez que hacemos click en esta opción navegamos hasta la ubicación del archivo con extensión “.pcf”.

5.4 Configuración firewall.

5.4.1 Fundamentos Firewall PIX.

PIX protege el segmento de red Inside (Trust o LAN) de accesos no autorizados desde la interfaz Outside (o Internet) ya en su configuración por defecto. La mayor parte de la serie PIX desde el 515 hacia arriba, pueden proteger además, uno o más perímetros de red, también llamados Demilitarized Zones (DMZs). El acceso al segmento DMZ, es típicamente menos restringido que el acceso desde la interfaz Ouside, pero más restringido que el acceso desde Inside.

El firewall PIX, aparte de proteger la red interna o Inside, de ataques externos desde la red Outside, puede proteger uno o un grupo de usuarios Intranet entre si. Para todos los PIX exceptuando el 501 y 506 que no tienen DMZ, se puede configurar la interface perimetral (o DMZ) para que sea tan segura como la Inside, o con variaciones en los niveles de seguridad como sea necesario. Estos niveles de seguridad en cada Interfaz, se representan con números de 0 a 100, donde 0 es la interfaz de menor seguridad, es decir con mayor riesgo y el 100 es la interface de mayor seguridad o la menos riesgosa.

Por ejemplo se puede ver el número o nivel de seguridad en cada interface, con el comando *nameif.*

MELV(config)# sh nameif
nameif ethernet0 outside security0
nameif ethernet1 inside security100

Se observa entonces que por ejemplo en el caso de un PIX 501, con este comando se pueden ver las dos interfaces y su respectivo nivel de seguridad asignado por defecto, donde ethernet0 corresponde a la interfaz Outside y ethernet1 a la Inside.

En el caso de la interface DMZ o perimetral los niveles de seguridad pueden ir desde el 1 al 99.

Ambas interfaces, Inside y Perimetral son protegidas con el algoritmo ASA de Cisco (PIX Firewall´s Adaptive Security Algoritm). La interface Inside, Outside y Perimetral, pueden escuchar RIP routing updates y todas las interfaces pueden hacer broadcast RIP con su default route si es necesario.

5.4.2 Configuración Firewall PIX.

Aunque ya se mencionó anteriormente, por defecto estos equipos vienen sin PDM ni telnet habilitados, por lo que aconsejamos antes de configurar las políticas de seguridad habilitar al menos PDM para tener una herramienta de configuración por CLI y otra por GUI.

Respecto a los requerimientos de Hardware y Software en la estación que hará uso de PDM, algunos de los requerimientos mínimos son:

Tipo de recurso - Hardware	**Requerimientos**
Procesador	Pentium III o equivalente a 450 Mhz
RAM	256 Mb
Resolución de pantalla	1024 x 768 px y 256 colores
Conexión de red	
Velocidad de conexión	56 Kbps; 384 Kbps (DSL o cable)

Sistema Operativo – Plataformas soportadas	Browser	JVM
Windows 98 Windows NT 4.0 (Service Pack 4 o superior) Windows 2000 (Service Pack 3) Windows ME Windows XP	Internet Explorer 5.5 o 6.0	Native JVM (VM 3167 o superior)
	Internet Explorer 5.5 o 6.0	Java 1.3.1, 1.4.0, or 1.4.1
	Netscape 4.7x	Native JVM 1.1.5
	Netscape 7.0x	Java Plug-in 1.4.0 or 1.4.1
Plataformas recomendadas		
Windows 2000 (Service Pack 3) Windows XP	Internet Explorer 6.0.2600	JRE S.E. (Standard Edition) 1.4.2
	Internet Explorer 6.0	Native1 JVM (VM 3809) o Java Plug-in 1.4.1_02
	Netscape 7.0x	Java Plug-in 1.4.1_02

Para habilitar PDM debe usar dos comandos:

http 192.168.x.x 255.255.255.0 inside
13. http server enable

Donde la IP 192.168.x.x 255.255.255.0, representa la Red o IP que estará habilitada a usar PDM (si es un único host se debe usar máscara 32 y la IP del PC que se destina a administrar el firewall por PDM).

Si necesita ingresar por PDM en forma remota usando un túnel VPN, entonces aparte de la IP o red que estará autorizada a usar PDM, se debe agregar el comando.

management-access inside

Esto siempre y cuando el usuario VPN Cliente haya obtenido una IP del segmento de red Inside, al conectarse en forma remota al firewall.

5.4.2.1 Configuración Access List.

Como se menciona anteriormente este comando se ocupa básicamente para configurar acceso desde la Interface de menor seguridad a la de mayor seguridad (Outside a la Inside).

También se mencionó que por defecto PIX permite tráfico desde el nivel de mayor seguridad (ej Inside), al de menor seguridad, esta es una access list implícita y que se puede ver en PDM, aunque no es posible editarla. Para limitar tráfico Outbound (saliente) se puede ocupar el comando ***Outbound,*** o usar PDM.

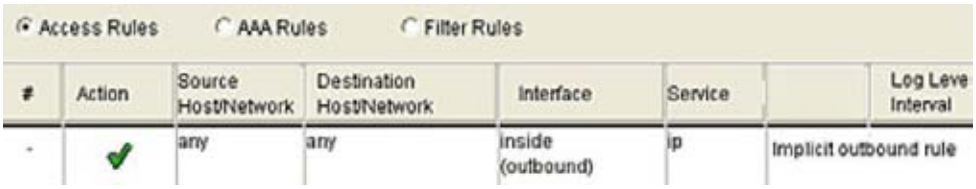


Figura 5.23. Vista de la access list implícita que permite todo tipo de tráfico desde la Inside a la Outside. Esta access list no se puede editar.

La configuración de access-list en PIX, tiene un orden de acuerdo a la categoría en la que se encuentre esta, es decir, depende de los objetivos con que se crea una access-list, esta irá acompañada o en combinación de otros comandos.

Por ejemplo para comenzar, la sintaxis con que se configura una access-list es la siguiente:

access-list *acl_ID* [**deny** | **permit**] *protocol* {*source_addr* | *local_addr*} {*source_mask* | *local_mask*} *operator port* {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} *operator port*

Vamos a ver algunos ejemplos de access-list, tanto para el caso en que se usen o no con el comando access-group o para cuando van en combinación con los crypto access-list, o nat 0 access-list.

La siguiente access-list, por ejemplo no tiene el final la opción operador definida ni tampoco el puerto, lo que indica y así es asumido por el PIX, que se trata de todos los protocolos IP y todos los puertos.

access-list acl_out permit tcp any host 209.165.201.1

En esta ACL el operador es **eq** (sólo igual a) y el puerto se ha definido por el nombre literal del servicio.

access-list acl_out deny tcp any host 209.165.201.1 eq ftp

En el sgte caso el operador es **lt** que significa que la access list se aplicará a todos aquellos puertos menores que el que se ha especificado. Por ejemplo se usa en este caso **lt 1025** para permitir o denegar el acceso a todos los puertos Well Known ports (1 a 1024).

access-list acl_dmz1 permit tcp any host 192.168.1.1 lt 1025

Se puede usar el operador **gt** junto al número de puerto para permitir/denegar todos aquellos puertos superiores al que se ha especificado, por ejemplo **gt 42** permite/deniega todos los puertos superiores a 43 (43 a 65535).

access-list acl_dmz1 deny udp any host 192.168.1.2 gt 42

El operador **neq** y un número de puerto indica que la ACL se aplicará a todo el conjunto de puertos exceptuando al que se indica. Por ejemplo **neq 10** permite/deniega acceso a todos los puertos excepto el 10, es decir de 1-9 y del 11 al 65535.

access-list acl_dmz1 deny tcp any host 192.168.1.3 neq 10

Se puede usar **range** junto a un rango de puertos para permitir/denegar acceso mediante la ACL, a todos los puertos del rango indicado, por ejemplo si se indica **range 10 1024** la ACL permite o deniega el acceso al rango de puertos especificado, es decir desde el 10 al 1024.

Para el caso en que las ACL sean usadas en combinación con los comandos crypto maps, o nat 0 …, esto significa que existe una política IPSec de por medio o la configuración de algún túnel.

Por ejemplo para el caso en que exista alguna configuración VPN IPSec, es necesario asociar una access-list por cada túnel, la primera indica al firewall que deje pasar tráfico ip entre las dos redes privadas (VPN Lan to Lan o Site to Site que es lo mismo) y que a su vez será utilizada con el comando crypto map, por ejemplo, se puede ver la definición de la ACL y su relación con los comandos para el túnel IPSec asociado.

access list acl1 permit ip 192.168.20.0 255.255.255.0 10.0.0.0 255.255.255.0

crypto map map1 10 match address acl1

nat (inside) 0 access-list acl1

en la primera línea se define la ACL, (la red 192.168.20.0 es la red local al PIX y la red 10.0.0.0, es la red interna del peer remoto) donde se define que el firewall dejará pasar tráfico entre estos dos segmentos de red, la segunda línea corresponde al grupo de comandos crypto map y en la línea mostrada se indica que el tráfico que coincida con los segmentos de red definidos en la ACL, será sometida a encriptación, de acuerdo a los transform set usados en el mismo crypto map map1.

El comando nat (inside) 0 access-list acl1, indica al firewall que los hosts del peer remoto ingresarán a la red interna sin hacer nat.

5.4.2.2 Configuración comando Outboud/Apply.

Este comando se usa principalmente para controlar el uso de Internet, la sintaxis se observa en las sgtes. Líneas:

[**no**] **apply** [**(***if_name***)**] *list_ID* **outgoing_ src** | **outgoing_dest**

clear apply

[**no**] **outbound** *list_ID* **permit** | **deny** *ip_address* [*netmask* [*port*[**-***port*]] [*protocol*]

[**no**] **outbound** *list_ID* **except** *ip_address* [*netmask* [*port*[**-***port*]] [*protocol*]

clear outbound

show outbound

show apply

5.4.2.3 Configuración de Access Rules genéricas con PDM.

Para denegar el acceso de los hosts internos a un servidor internet determinado y con servicios determinados, se hace la sgte configuración (vamos a suponer que el servicio a denegar es ftp).

En este caso la IP inside del Firewall es la 10.0.0.1/24 y los hosts internos en el respectivo segmento de red.

a) Asumiendo que ya ingresó a la interface PDM, diríjase a Configuration – Access Rules.
b) Click con el botón derecho sobre las reglas creadas y luego click en Add. También, para agregar una regla de acceso, puede hacer click en el icono  , ubicado en la parte superior izquierda de PDM.
c) De la nueva ventana emergente en el menú desplegable **Select an Action**, seleccione deny, en el campo Source Host/Network, Inside , Destination Host/Network, Outside, en Destination Port haga click en el botón  , para seleccionar el servicio ftp, en resumen la configuración debería quedar como se indica en la figura 5.25.

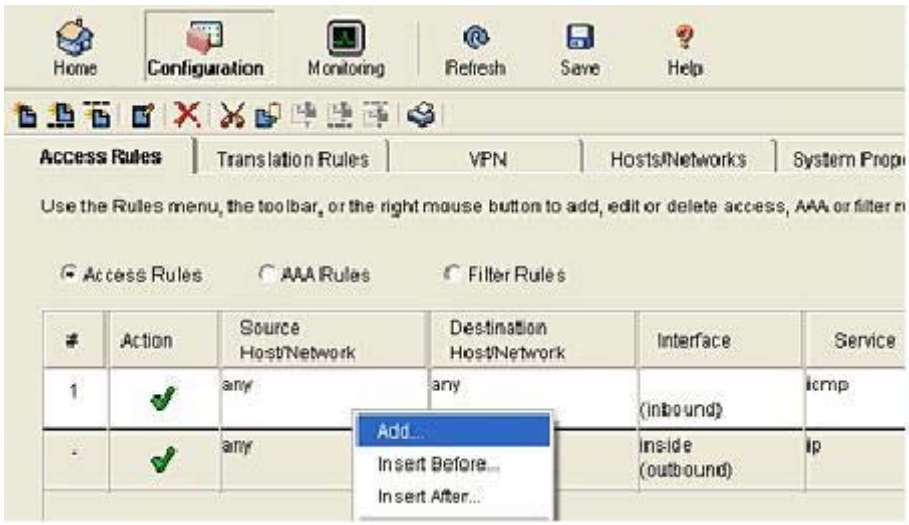


Figura 5.24. Agregando una regla de acceso (Outbound) usando PDM.

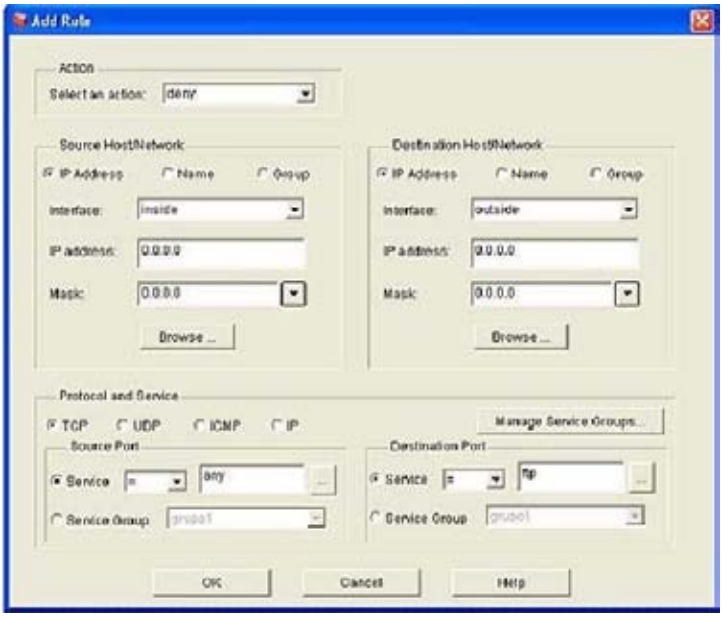


Figura 5.25. Configurando una Access Rule con PDM. En este caso se está negando el servicio FTP para todos los usuarios internos.

d) Click en botón **Ok**, luego en el botón **Apply**, para aplicar los cambios y finalmente para guardar los cambios en la flash, haga click en el icono  ubicado en la parte inferior.

También para guardar los cambios en la flash puede dirigirse al menú **File – Save running configuration to flash**.

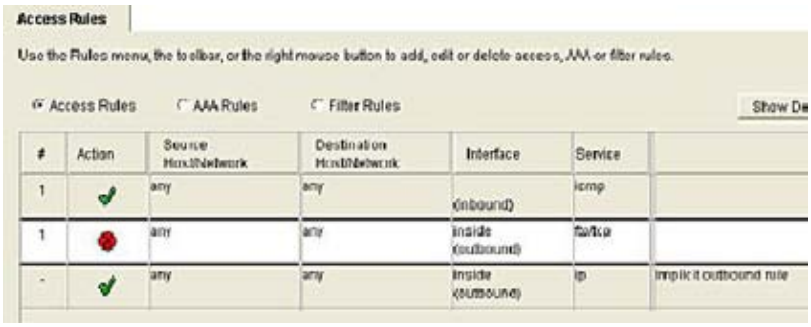


Figura 5.26. Desde la primera regla hasta la última tenemos, permitir ping, denegar el acceso a cualquier servidor ftp y por último la regla implícita que permite tráfico desde el nivel de seguridad mayor al menor (Inside to outside).

Figura 5.27. Vista de algunos de los servicios predeterminados por PDM PIX.

Ahora veremos como el PDM genera la configuración para CLI, respecto a la regla recién configurada. Entonces entrando por consola vemos la siguiente configuración:

MELV(config)# sh Outbound
outbound 1 deny 0.0.0.0 0.0.0.0 21 tcp
MELV(config)# sh apply
apply (inside) 1 outgoing_src

En primer lugar tenemos el comando outbound que tiene un List Id = 1, además deniega el acceso y que la IP fuente es cualquiera de la interface Inside, con puerto destino 21 y protocolo TCP.

Luego está el respectivo comando apply que habilita a outbound y que además le dice al firewall que se trata de una regla por dirección fuente Inside, observar además que el comando apply hace referencia al mismo list ID que el comando Outbound, en este caso 1.

En el caso que se necesite denegar el acceso a una IP específica, es necesario antes definir el host, en el caso de PDM recurriendo a **Configuration – Hosts / Networks**. En el caso de hacerlo por consola, se usa el comando **name <ip_address> <name>.**

5.4.2.4 Denegar Sitios Web Internet con PDM.

Continuando, en este caso vamos a denegar el acceso a alguna página web no deseada, para ello primero debemos descubrir la IP que tiene el sitio con un ping por ejemplo, luego la definimos como un Host (una etiqueta en la configuración del PIX que permite identificar cual es el sitio destino que se aplicará la regla en este caso) y finalmente se configura la regla que denegará el acceso.

Ahora bien, como ejemplo, vamos a bloquear el acceso al sitio web de playboy, para hacerlo siga los siguientes pasos:

a) Diríjase a **Configuration – Hosts / Networks**, luego defina la IP Outside de playboy, como se observa en la sgte. figura.

b) Diríjase a **Access Rules** y haga click en el icono  , para agregar una nueva regla.

c) De la nueva ventana que aparece, observar la figura 26, como es especificado el segmento de red fuente, el destino (en este caso por el nombre antes definido) y el puerto y protocolo destino.

d) Click el botón **Ok**, luego **Apply** y finalmete click en el icono  , para guardar los cambios en la flash.

Figura 5.28. Configuración de la IP Outside que se usará en la nueva regla de acceso.

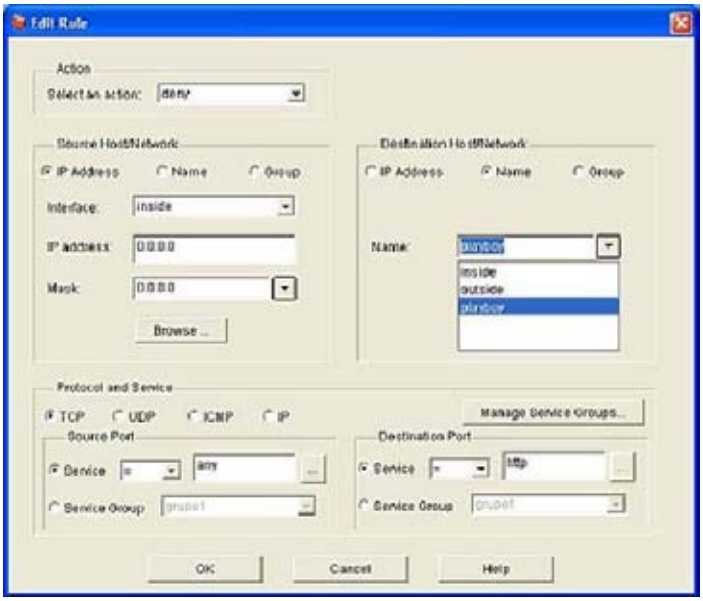


Figura 5.29. Denegando el servicio www a la IP de playboy.

Una forma más sofisticada de filtrar contenido de páginas web, sería teniendo acceso a un servidor Websense, edición para PIX, o en su defecto un N2H2 que también proporciona filtro de contenido. Por defecto PIX no tiene licencia para hacer uso de un servidor de este tipo.

5.4.2.5 Bloquear/habilitar el acceso Internet a distintos usuarios internos.

Vamos a plantear el escenario en que sea necesario habilitar sólo a 5 usuarios internos la salida hacia Internet y todo el resto sean denegados.

Para ello lo primero que debemos hacer, es configurar una regla de acceso como en los casos anteriores, sólo que esta vez denegaremos el acceso hacia Internet de cualquier servicio

para todos los usuarios internos (Inside), luego será necesario definir en **Configuration – Hosts / Networks**, o con el comando name, cada uno de los PC que estarán autorizados a usar Internet, luego el paso siguiente es habilitar Internet para cada PC que se definió antes.

- Como se puede pensar en este momento se tienen 2 reglas que se contradicen una a otra (una regla que deniega la salida a todos los usuarios Inside y la otra que permitirá también a usuarios Inside salir hacia Internet), sin embargo, al existir coincidencia en este caso de los hosts (unos definidos por segmento de red y los otros por PC individual), el firewall omite la regla o el comando Outbound deny, frente al Outbound permit.
- Cuando se usan múltiples reglas para filtrar el mismo paquete, entonces la regla que mejor calza, o que es más específica con las condiciones configuradas, es la que finalmente aplica el Firewall.
- PIX procesa en orden secuencial todas la reglas de acceso por su List ID, por ejemplo una lista de acceso con un List ID 1, es procesada antes que una List ID 2.

Para hacer la configuración respectiva seguimos los sgtes. Pasos:

a) Primero agregamos una regla de acceso denegando todo tipo de tráfico de salida desde la interfaz Inside hacia la Outside.

b) Luego nos dirigimos a **Configuration – Hosts / Networks,** para configurar y dar un nombre a cada cliente o IP que si estará autorizada a salir a Internet. En este caso vamos a permitir desde la IP 10.0.0.2 – 10.0.0.6, para ello configuramos cada IP en forma individual. Click en **Next**, luego seleccionamos la opción **Dynamic** y finalmente **Finish.**

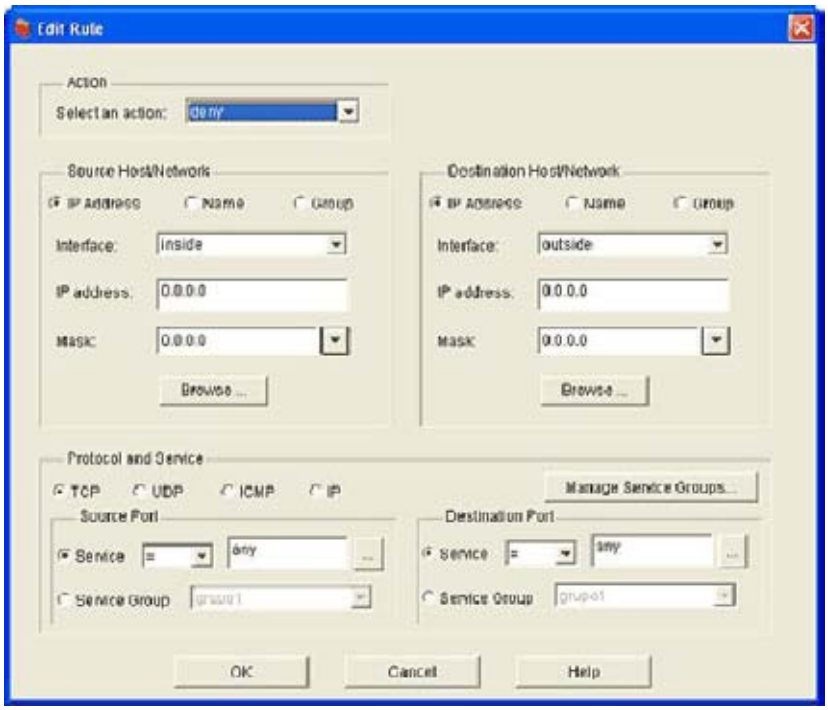


Figura 5.30. Agregando una regla de acceso que deniega toda salida hacia internet de los usuarios Inside.

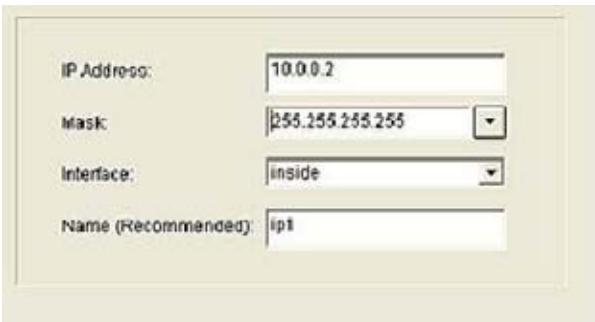


Figura 5.31. Configuración de cada IP que luego usaremos para identificar el host autorizado a salir a Internet.

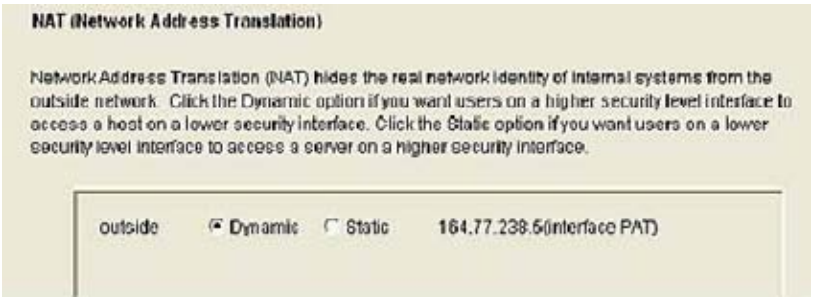


Figura 5.32. Configuración individual para cada IP autorizada a salir a Internet.

c) Luego para cada IP que se configura en el paso anterior, debemos configurar una regla de acceso que permita el acceso hacia la Interfaz Outside, como se observa en la figura 5.33.

d) Click **Ok**, luego el botón **Apply**.

e) Siga el resto del procedimiento hasta terminar con la última IP, una vez que finalice haga click sobre el icono  para guardar los cambios en la flash.

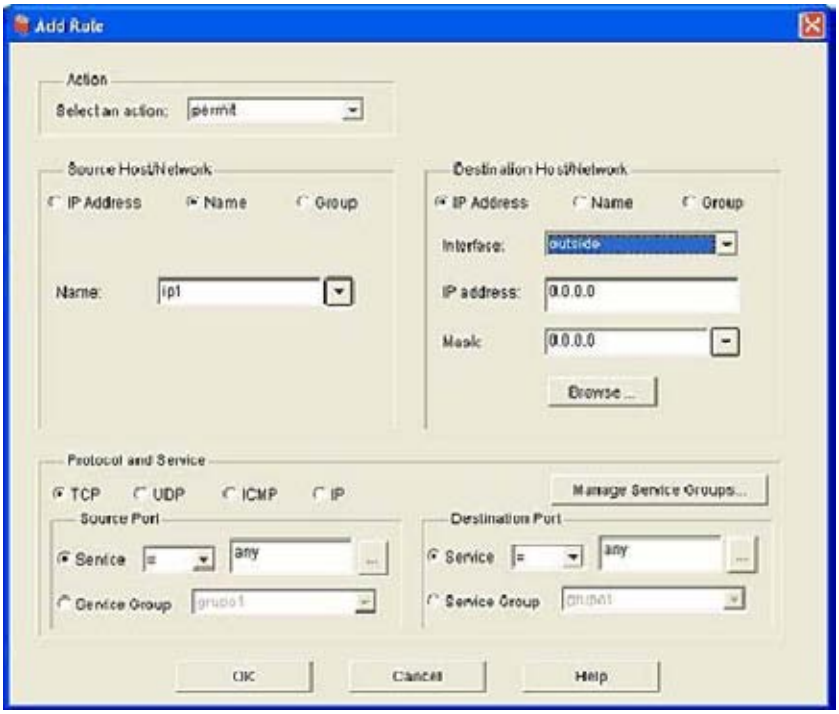


Figura 5.33. Configuración de regla de acceso que permite la salida de cada IP autorizada.

Una vez que terminó todo se puede observar que los usuarios en este caso desde la IP 10.0.0.2 – 10.0.0.6 lograrán navegar por Internet, en tanto el resto estará todo denegado.

La configuración planteada podría lucir como en la figura 5.34:

Figura 5.34. Vista de todas las reglas de acceso configuradas.

Si entramos via consola al firewall, podemos ver que se ha generado la siguiente línea de comandos:

MELV(config)# sh outbound
outbound 1 deny 0.0.0.0 0.0.0.0 0 tcp
outbound 1 permit 0.0.0.0 0.0.0.0 21 tcp
outbound 1 permit ip1 255.255.255.255 0 tcp
outbound 1 permit ip5 255.255.255.255 0 tcp
outbound 1 permit ip2 255.255.255.255 0 tcp
outbound 1 permit ip3 255.255.255.255 0 tcp
outbound 1 permit ip4 255.255.255.255 0 tcp
outbound 2 permit playboy 255.255.255.255 80 tcp
MELV(config)# sh apply
apply (inside) 1 outgoing_src
apply (inside) 2 outgoing_dest
MELV(config)# sh name
name 209.247.228.201 playboy
name 10.0.0.0 segmento1
name 10.0.0.6 ip5
name 10.0.0.5 ip4
name 10.0.0.4 ip3
name 10.0.0.3 ip2
name 10.0.0.2 ip1
MELV(config)#

5.4.2.6 Configuración Filtros Activex, Applet Java.

PIX tiene un filtro especial para aplicaciones o pequeños programas que corren sobre html o páginas web. Objetos ActiveX y java applets representan riesgos de seguridad para conexiones salientes (desde interfaz Inside), ya que pueden contener código malicioso con el propósito de atacar servidores o hosts.

Usando este feature de PIX, se puede bloquear y filtrar ActiveX y java applets. Para el caso en que un cliente considere que algunos URL o sitios ftp, son maliciosos para el acceso desde su red, es posible hacer uso de herramientas adicionales como por ejemplo Web sense o N2H2 (N2H2 sólo soporta http Filtering), aunque esto implica costos adicionales, y la instalación de un servidor en paralelo con el firewall con software de Websense u otro.

Para configurar este tipo de filtro, diríjase a **Access Rules - Filter Rules**, luego en forma similar a las configuraciones que hicimos en páginas anteriores, ahora es necesario indicar la IP fuente, destino, etc.

Para hacer un ejemplo de esta configuración, vamos a bloquear los applets java del sitio www.eldiario.cl, para hacerlo seguimos los pasos:

a) Primero defina la IP del servidor donde está alojada la página del diario financiero y coloque una etiqueta para identificarlo, como se observa en la figura 5.35.

b) Luego nos dirigimos a **Access Rules - Filter Rules** y hacemos click sobre el icono , para agregar una nueva regla.

c) De la ventana emergente, seleccionamos en **Select an Action,** Filter Java Applet, la interface **Inside**, como fuente, el nombre definido anteriormente “eldiario”, como destino y los puertos donde se aplicará el filtro de applet java que en este caso son desde el 80 - 80.

d) Click en el botón **Ok**, luego **Apply** y finalmente en el icono  para guardar los cambios en la flash.

Figura 5.35. Definición de la IP pública donde está alojada la página del diario.

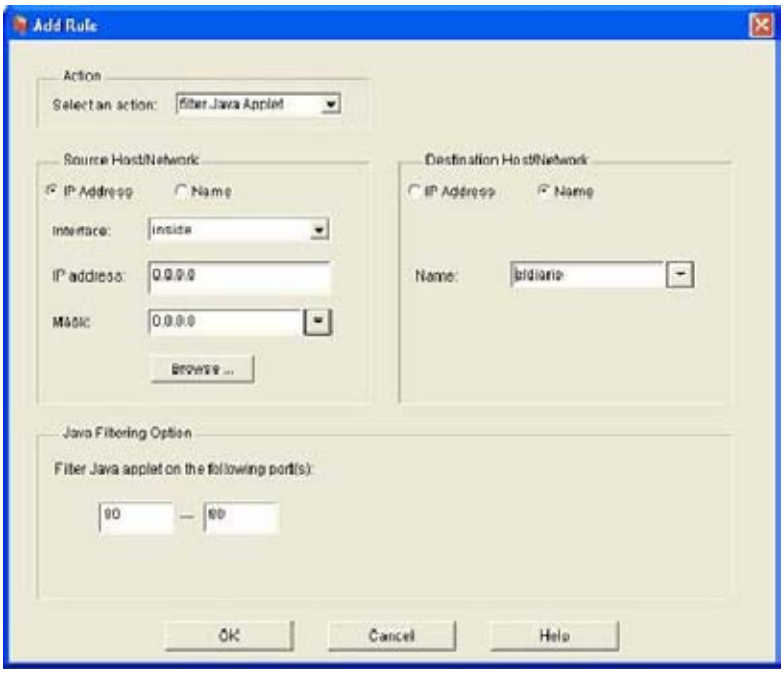


Figura 5.36. Aplicando filtro para applets java dentro del código html, en un sitio en particular.

Aplicar estos filtros no significa que bloquearemos acceso a la página web en particular, sino que solamente los applet java incrustados en el código html, no se ejecutarán y el sitio se podrá ver pero sin las funcionalidades que le aportan los mismos applet.

También con esta funcionalidad de PIX se pueden filtrar controles Activex, que son homólogos a los applet, pero de Microsoft, URL (con websense o N2H2), FTP entre otros.

Figura 5.37. Vista de todas las alternativas de filtro que tiene PIX, en capas superiores.

5.4.2.7 Configuración de acceso desde Internet a Servidor interno.

Este tipo de configuración permite acceder a un servidor con IP Inside, desde Internet. Para lograr esto, se debe contar con una IP pública adicional a la IP Outside del Firewall.

La configuración en el Firewall, se debe hacer en el sgte. orden:

a) Configurar un nombre descriptivo para el servidor interno, junto a su IP Inside.
b) Configurar un NAT estático uno a uno usando la IP pública disponible.
c) Configurar una Access Rule que permita el acceso al servidor interno, apuntando al (los) protocolo específico, con (el o los) puerto específico.

Para entrar en el detalle de la configuración, usaremos como ejemplo, la habilitación de un servidor Web con IP Inside 10.0.0.5 y con un NAT estático usando la IP 164.77.238.4.

Para configurar el servidor interno que dará servicios hacia Internet, debe proceder de la siguente forma:

a) Ingrese a PDM, luego diríjase a Hosts – Networks, enseguida seleccione la interface Inside para agregar una nueva entrada, click en el botón Add. En la nueva ventana que aparece, ingrese IP Inside, máscara (32 bits) y el nombre que hace referencia al servidor. Click en el botón Next para configurar el NAT estático.

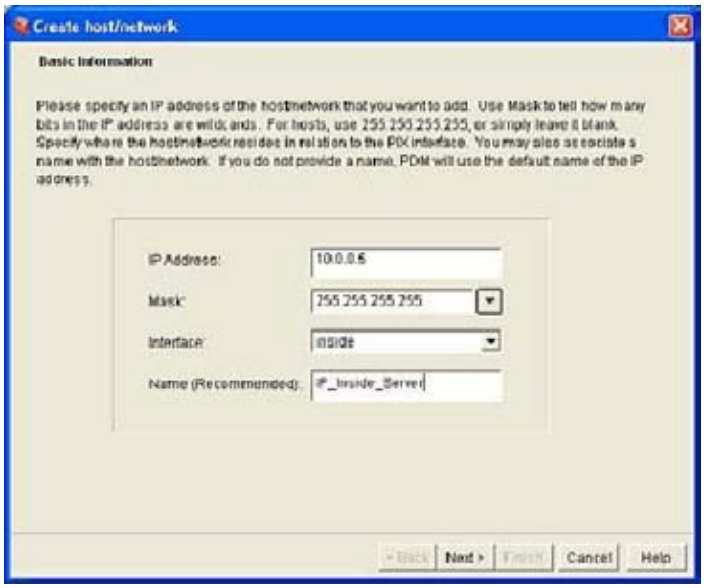


Figura 5.38. Configuración de nombre descriptivo para servidor Interno, versus su IP Inside.

b) Es necesario ahora configurar el NAT estático que mencionamos antes, para ello en la nueva ventana, debe seleccionar la opción **Static** y a continuación la IP pública que se usará para hacer la traducción (en este caso la 164.77.238.4). Click en botón **Finish**.

Figura 5.39. Configuración de Nat estático para el servidor Interno.

Puede ver el conjunto de reglas de traducción de IP Inside, inclusive la que acaba de agregar, en **Translation Rules**.

c) Click en el botón **Apply** para aplicar los cambios.

d) Es necesario ahora crear la regla de Acceso que permitirá levantar una sesión desde Internet al servidor interno, para ello haga click sobre **Access Rules**, luego click sobre el icono , para agregar la nueva regla.

e) Siga la misma metodología que ha sido usada para configurar la mayor parte de las reglas Firewall hechas anteriormente. En este caso la red Fuente debería ser Outside any, dirección destino IP Inside de servidor (en este caso tiene la etiqueta *IP_Inside_Server*), protocolo y puerto fuente TCP any y Protocolo y puerto destino en este caso www. Click en botón **Ok**, luego en **Apply** para aplicar los cambios.

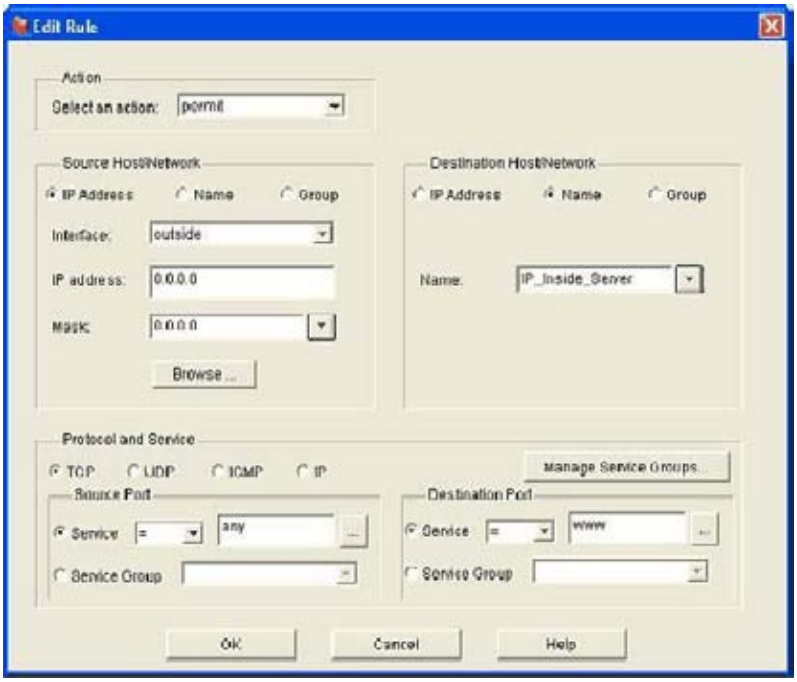


Figura 5.40. Configuración de la Access Rule que permite el acceso al servidor interno desde Internet.

f) Para finalizar guarde los cambios en la flash.

5.4.2.8 Configuración de autenticación para uso de servicios Internet.

Es posible configurar Cisco PIX para que pida a los usuarios Inside (a un grupo o un único host), que se autentiquen para así autorizarlos a utilizar servicios como por ejemplo:

- ftp
- http

- https
- telnet

Para proceder con este objetivo debe antes definir si los usuarios serán autenticados con servidor Radius, Tacacs o usando la base de datos local del Firewall, luego definir las cuentas, identificar aquellas IP que deben autenticarse y por último configurar la regla que indicará al Firewall que pida autenticación si un host Inside hace un Request a alguno de los servicios mencionados anteriormente.

Para crear esta regla debe dirigirse a **Configuration – Access Rules – AAA Rules**, luego clic sobre el icono de crear una nueva regla. Por ejemplo se muestra en la sgte pantalla, la configuración de un regla que indica al Firewall, que debe pedir a un usuario (en este caso con IP inside 10.0.0.10) autenticarse antes de iniciar una sesión (hacia Internet) http.

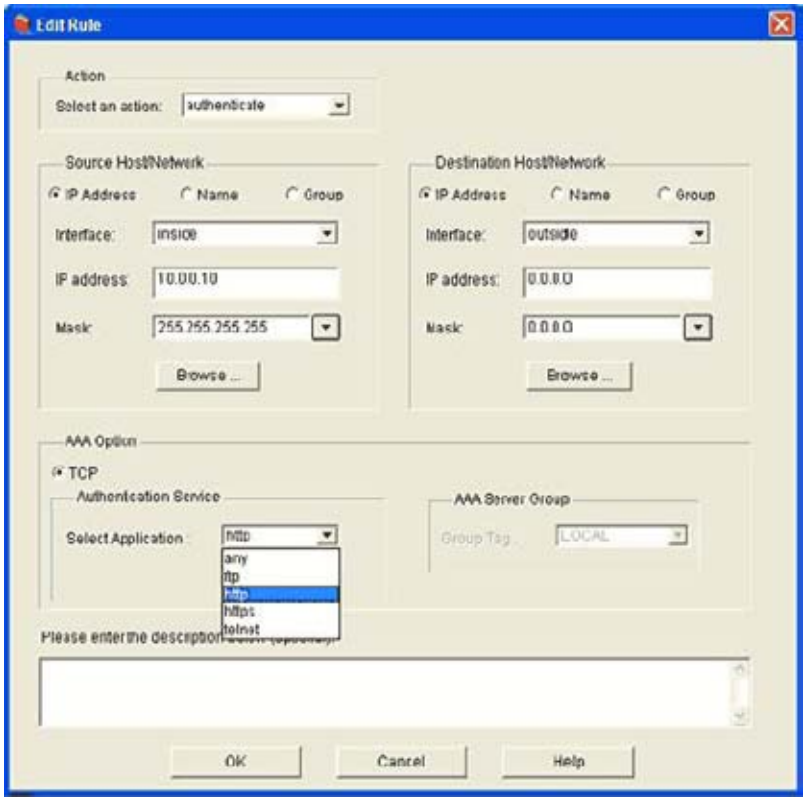


Figura 5.41. Regla que permite al Firewall pedir autenticación a un host Inside ante el requerimiento de un servicio Internet específico.

CONCLUSIONES

La configuración usada para VPN cliente en la mayor parte de los firewalls (exceptuando a PIX 501), es muy similar a la usada o requerida para configurar una VPN Lan to Lan (Punto a Punto a Multipunto) y tal vez la única diferencia que se puede apuntar es que el cliente VPN no tiene una IP pública estática, por lo que en la configuración de los equipos IPSec, se debe indicar en la configuración que el IPSec Gateway o peer remoto, tendrá una IP del tipo 0.0.0.0. Al igual que en el caso de configurar una VPN Multipunto (más de dos peers), no existiría diferencia respecto a la configuración que se ha indicado para configurar una Punto a Punto.

Dentro de todos los tipos de configuración que se han manejado en este documento, podemos indicar que existen diferencias en cuanto a seguridad requerida, velocidad o Troughput VPN, cantidad de procesamiento, como parámetros más relevantes.

Respecto a la seguridad requerida: se subdivide a su vez en seguridad aportada por las características de los protocolos usados y por el tipo de configuración usada (Manual Key o preshared Key).

Dentro de los protocolos que usan para encriptación tenemos que de mayor a menor encriptación tenemos: 3DES, AES, DES. De los protocolos de autenticación, de menor a mayor nivel de seguridad: SHA1, MD5. De los protocolos Diffie Hellman Group, de mayor a menor seguridad: Grupo 2, Grupo 1.

Por las características de configuración se tiene que de los métodos de configuración que hemos visto para VPN, tenemos de Mayor a menor seguridad: Preshared Key, Manual Key. Esto ya que en el caso de la primera configuración, la SA, son establecidas en forma automática y renegociadas cada cierto tiempo, de acuerdo a lifetime configurado.

Velocidad o Troughput VPN: tiene directa relación además al nivel de seguridad configurado, además de la cantidad de túneles en uso, es decir a mayor seguridad tendremos menor troughput para el tráfico de datos, mientras que a menor grado de seguridad, mayor troughput.

Cantidad de procesamiento en el equipo: La cantidad de procesamiento en el firewall o la cantidad de carga a la que se expone, tiene directa relación con el grado de encriptación que debe procesar o la complejidad de los algoritmos de autenticación, o de intercambio de llaves, etc.

Por los parámetros aludidos anteriormente, debe existir una previa política y balance entre la sobrecarga de los firewalls (y su respectivo troughput de fábrica), la seguridad y el nivel de seguridad comprometido en la VPN. Por ejemplo en el caso de una VPN Lan to Lan, generalmente estas están permanentemente conectadas, por lo que el grado de seguridad dependerá exclusivamente de las políticas que necesite el cliente y del tipo de tráfico que pasará por el túnel.

También en el caso de los VPN cliente, se puede decir que esta no es una conexión VPN permanente, por lo que un grado de seguridad medio-bajo, podría ser recomendable.

Para el caso de Cisco PIX 501, puede suceder que luego de un tiempo la VPN (sobre todo cuando no hay tráfico), se haya deshabilitado, es decir que las llaves negociadas entre ambos peers hayan caducado, esto no debería ser mayor problema, ya que el PIX si no detecta tráfico VPN entre él y otro peer, entonces deshabilita la VPN. Esto puede cambiar de situación si PIX detecta que se produce tráfico nuevamente y que hay requerimientos de intercambio IKE.

Otra situación que puede ocurrir con PIX es que no se produzca conectividad VPN por el número de prioridad que tengan las isakmp policy, intente dar mayor prioridad en algunos casos, o ajuste los valores Lifetime en un valor idéntico para ambos firewalls.

De todos los equipos con los que hemos trabajado, no hay alguno que posea una herramienta de reportes o logs completo y que permita identificar la fuente de los problemas en caso que no se produzca la conectividad después de configurar una VPN. La mayor parte de los equipos al no producirse conexión con otros peers, arrojan logs muy genéricos, como por ejemplo *SA mismatch* , o *IPSec Gateway unreachable*, etc.

Para el caso en que se quiera limitar tráfico con este firewall, se aconseja comenzar con el comando Outbound (Usando PDM o consola) y en casos donde sea necesario usar access-list.

WatchGuard es una plataforma poderosa y relativamente fácil de utilizar, pero hay que tener mucho cuidado en asignar las reglas que sean necesarias ya que puede tornarse inestable y lento en actualizar el estado de conexiones y VPN. Una falencia importante que se detecta: es que en el momento que la consola realiza REFRESH (actualización de los datos) todas las conexiones se alarman por un intervalo de unos pocos segundo llegando así hasta a ocultar una posible falla real. También se detecta pero de forma no tan frecuente la perdida de administración de una determinada VPN, en este caso se debe reasignar la ruta asociada a la VPN.

Cisco PIX es una plataforma menos amistosa, pero para administradores de redes que configuren de forma avanzada Router y Switch Cisco notaran las similitudes, solo difieren en una gama de comandos específicos de seguridad.

Cisco PIX resultó mas estable en desempeño y por ende menor utilización de los recursos de sistema, pero WatchGuard a su ves tiene la facultad de bloquear elementos en forma mas precisa, como por ejemplo una palabra cualquiera asociándolo a un servicio.

REFERENCIA BIBLIOGRAFICA

- REDES DE COMPUTADORAS 3^{era} Ed, Andrew S. Tanenbaum, Traducción: David Morales Peaje. Prentice Hall.

- COMUNICACIONES Y REDES DE COMPUTADORES, William Stalling, Prentice Hall.

- COMUNICACIONES Y REDES DE COMPUTADORES, 6ta Ed, William Stallings, Prentice Hall.

- DISEÑO DE SEGURIDAD EN REDES, Merike Kaeo, traducción: Santiago Fraguas Berasain. Cisco Press. Pearson Educación.

- ROUTERS CISCO, Joe Habraken, traducción: Beatriz Paredes, Prentice Hall.

- INTERCONEXIÓN DE DISPOSITIVOS DE RED CISCO, Steve McQuerry, Traducción: Clave Informatica I+D, S.A. Cisco Press. Pearson Educación.

- ACADEMIA DE NETWORKING DE CISCO SYSTEM, GUIA DEL PRIMER AÑO, 3era Ed. CISCO System Inc, Traducción KME Sistemas, S.L. Cisco Press. Pearson Educación.

- FIREWALL PIX DE CISCO SECURE, David W. Chapman Jr, Andy Fox, Tradución: Ruth Vázquez Llorente. Cisco Press. Pearson Educación.

- Installation Guide for the Cisco Secure PIX Firewall. http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_installation_guide_book09186a0080108d27.html

ANEXO 1

Guia rápida de inicio.

Ficha técnica de instalación y mantención.

De los aspectos físicos y lógicos.

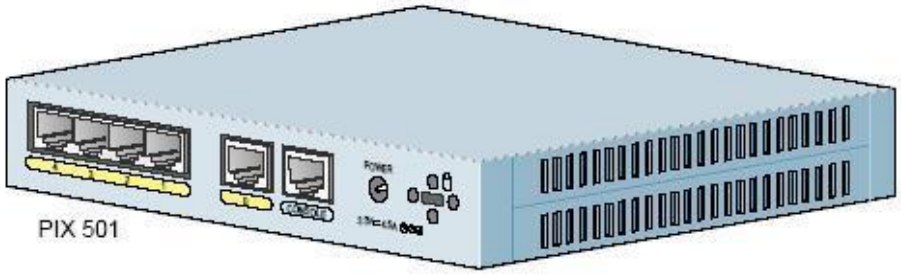
El PIX 501 entrega la seguridad de la empresa para las pequeñas oficinas en una confiable aplicación de plug-and-play. Ideal para asegurar alta velocidad "siempre en" los ambientes de banda ancha, el PIX 501, parte de la serie del cortafuego de Cisco proporciona capacidades robustas de la seguridad, características pequeñas del establecimiento de una red de la oficina, y capacidad de gran alcance de la gerencia alejada en un acuerdo, solución toda junta:

- La seguridad de la inspección de estado basado en Adaptive Security Algorithm (ASA).
- Soporta sobre 100 aplicaciones, servicios y protocolos predefinidos para un control de acceso flexible.
- El establecimiento de una red privada virtual (VPN) para el acceso seguro a uno red remota usando los estándares de IKE/IPSec.
- Protección contra sobre 55 diferentes ataques por intrusos.
- Filtros URL de salidas de tráfico web.
- Switch integrado que permite a múltiples usuarios compartir una única conexión de banda ancha.

Características de Hardware.	**Características de Software.**
• Compacto chasis de escritorio. • Fuente de energía externa. • Procesador de 133 Mhz. • 16 MB Ram y 8 MB flash. • 1 puerto 10BaseT Ethernet (half duplex) para una conexión externa hacia Internet (port 0).	• Soporta version 6.1 o superior del software firewall PIX, sistema operativo incluido. • Incluye por defecto configuración de plug-and-play para una instalación simplificada.

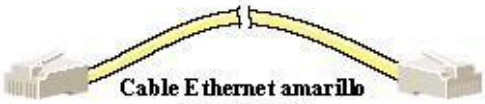
- Switch integrado de 4 puertos 10/100 Mbps Ethernet para una LAN privada interna (puertos 1 al 4).
- Puerto de consola serial para acceso administrativo.
- Abertura para añadir seguridad fisica.
- Panerl frontal de LEDs para aplicaciones y estados de enlaces.
- Firewall con canal de 10Mbps de texto plano.
- Canal VPN de 3 Mbps (3DES/SHA1).
- Incluye Cisco Pix Device Manager (PDM) para una administración intuitiva basada en navegador web.
- Soporta 10 host activos ampliables a 50 host con la licencia opcional de 50 usuarios.
- Servidor DHCP interno que soporta 32 direcciones DHCP ampliables a 128 direcciones DHCP con la licencia opcional de 50 usuarios.

Artículos incluidos.

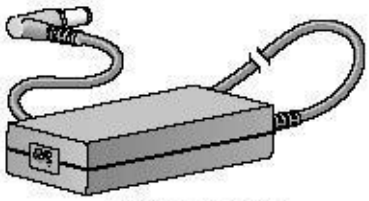


Terminal adaptador a PC
(74-0495-01)

Cable consola azul
(72-1259-01)



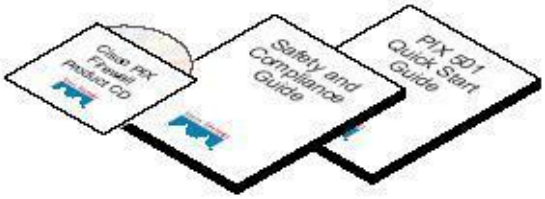
Cable Ethernet amarillo
(72-1482-01)



Fuente de energia
(341-0008-01)

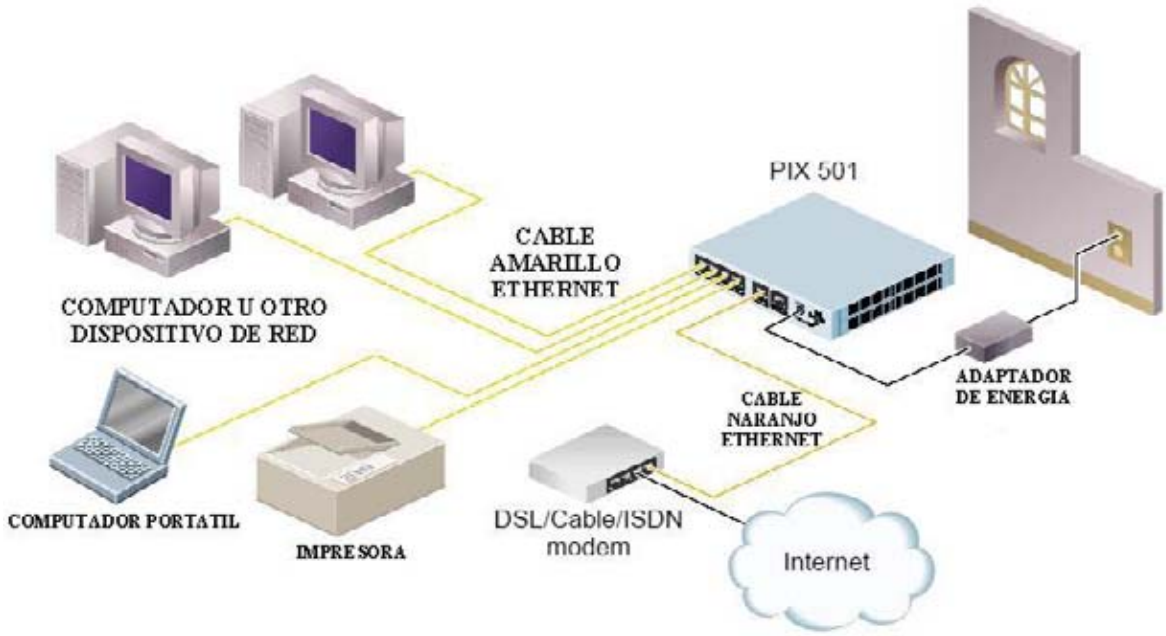
Ethernet naranjo
Crossover cable
(72-3515-01)

Cable de poder
(72-0259)



Documentación

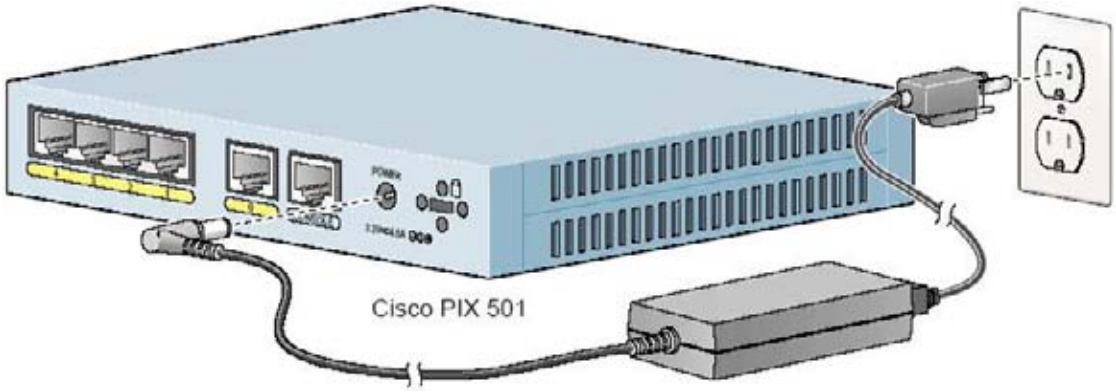
Instalación del PIX 501.



Para conectar los cables, siga los siguientes pasos:

1. Sitúe el chasis en una superficie plana y estable, el chasis no es montable en un rack.
2. Conecte el puerto 0, el puerto Ethernet de salida, a la red pública que puede ser Internet.
    a. Use el cable Ethernet amarillo para conectar el dispositivo a un switch o hub.
    b. Use el cable cruzado Ethernet naranjo para conectar el dispositivo a un cable/DSL/ISDN modem.
3. Conecte su PC u otro dispositivo de red con un cable etherneta uno de los cuatro puertos internos del switch (enumerados del 1 al 4).

Asegúrese que uno de los PC tenga instalado TCP/IP y se este configurado para obtener automáticamente una dirección IP a través de DHCP. Esto permite al PC comunicarse con el PIX 501 y con Internet así también como con el PIX Device Manager (PDM) Startup Wizard.



Siga los siguientes pasos para encender el firewall PIX.

1. Conecte la fuente de energía (341-0008-01) con el cable de poder (72-0259) y el conector pequeño redondo de la fuente de energía al conector "**power**" en el panel trasero y el cable de poder a la fuente de corriente eléctrica.
2. Revise que la luz de "**power**" este encendida con un color verde sólido, entonces el equipo estará encendido.

El PIX 501 no tiene interruptor de encendido, por lo cual al completar el paso 2 el equipo estará encendido.

Si desea mantener el dispositivo funcionando se recomienda una fuente de energía autónoma como una UPS en caso de cortes por la empresa proveedora de energía eléctrica.

Configuración del PIX 501.

El Cisco PIX 501 viene con una configuración por defecto lo cual significa que requiere, en su mayoría, de un ambiente de red con banda ancha, esta configuración protege la red interna contra cualquier tráfico no solicitado, además de usar DHCP en las interfaces de salida que requieren estas direcciones IP. Un grupo de direcciones IP están incluidas para host en la interfaz interna.

En las siguientes situaciones puede ser necesario hacer cambios en la configuración por defecto:

- Crear una contraseña administrativa y de telnet (altamente recomendada para asegurar la seguridad en la administración del firewall PIX)
- Configurar Point-to-Point Protocol over Ethernet (PPPoE) o Ip estáticas para las interfaces de salida.
- Configurar VPN y características de auto actualización.

El PIX 501 contiene de forma integrada la utilidad llamada **PIX Device Manager** (PDM) la cual es una configuración de ayuda basada en navegador web y designada para ayudar en la configuración inicial, monitoreo y cambios en el PIX. Para acceder a PDM asegurese que tiene habilitado el JavaScript en su navegador y para mejor desempeño recomendamos Microsoft Internet Explorer 5.5 o superior.

PDM versión 2.0 o superior incluye un **startup wizard** para la configuración inicial, para usar esta ayuda siga los siguientes pasos.

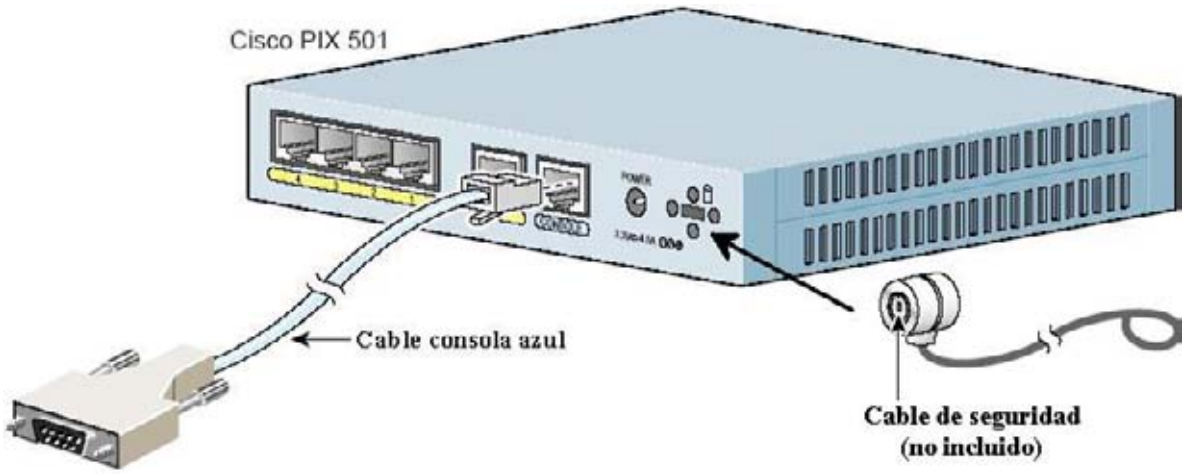
1. Use un cable ethernet y conecte su PC en uno de los 4 puertos de switch (enumerados del 1 al 4) del panel trasero del firewall PIX.
2. Configure su PC para usar DCHP (para recibir automáticamente una dirección IP) o asigne una dirección estática dentro de la red 192.168.1.0, excepto la dirección 192.168.1.1 que es la que trae la interfaz interna por defecto.
3. Revise el **link LED** para verificar que su PC tiene conectividad con uno de los puertos internos, cuando esto ocurra el **link LED** del panel frontal se estabilizará en un color verde sólido.
4. Para entrar en el **startup wizard**, en su navegador web ingrese la dirección **https://192.168.1.1/startup.html**

Nota: recuerde añadir la “s” a “https” o la conexión fallará. HTTPS (HTTP over SSL) provee una conexión segura entre su navegador y el PIX cuando usa PDM para configurar o monitorear.

5. Presione **enter** tanto para el username como para el password.
6. Acepte los certificados y siga las instrucciones. Para ayuda en línea pinche el icono **help** en la base de la ventana del **startup wizard**.

Maneras alternativas para acceder al PIX.

Usted puede acceder a la interfaz de linea de comandos (command-line interface – CLI) para administración usando el puerto de consola de su firewall PIX. Para esto usted debe correr un emulador de terminal serial en su PC como por ejemplo hiperterminal que viene con Windows.



Siga los siguientes pasos para conectarse al puerto de consola para acceso a administración local.

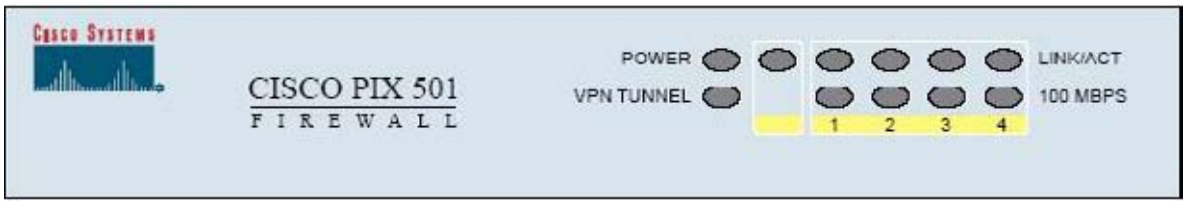
1. Conecte el terminal adaptador a PC (74-0495-01) en el puerto serial de 9 pines.
2. Conecte una de las puntas del cable de consola azul (72-1259-01) en el terminal adaptador de PC.
3. Conecte la otra punta de cable de consola azul en el puerto de consola del PIX 501.
4. Configure el software emulador de terminal serial en su PC para 9600 Baud, 8 bits de datos, sin paridad y 1 bit de parada.

Seguridad física, instalación de cable con candado.

El PIX 501 incluye una abertura que acepta un cable con candado estándar que brinda seguridad física para pequeños equipos portátiles como los computadores portátiles o notebook. Este articulo no viene incluido.

Para instalar este cable con candado, siga las instrucciones del fabricante e inserte el candado en la abertura en el panel trasero del Firewall PIX.

Chequeando los LEDs.



La tabla siguiente indica los estados y descripciones de cada LED.

LED	**Estado**	**Descripción**
POWER	Verde	El dispositivo esta encendido.
	Apagado	El dispositivo esta apagado.
LINK/ACT	Verde parpadeante	Actividad de Red está presente, como Internet.
	Verde	Correcto uso del cable, y conectado a un equipo de energía.
	Apagado	Enlace no establecido. Nota: si este LED no esta encendido, posiblemente esta usado un cable Ethernet o el cable esta dañado, pruebe cambiando el cable.
VPN TUNNEL	Verde	Uno o más Túneles VPN IKE/IPSec están en uso
	Apagado	No hay túnel VPN activo. La configuración por defecto no incluye VPN. Estos LEDs no se enciendienden cuando se establecen túneles PPTP/L2TP.
100 MBPS	Verde	La interfaz a negociado a 100Mbps en half o full duplex.
	Verde parpadeante	La interfaz esta funcionando a 10Mbps en half o full duplex.

Como obtener documentación de asistencia técnica.

Cisco provee cisco.com como punto de partida para toda la asistencia técnica, consumidores y socios pueden obtener documentación, consejos para resolver problemas y ejemplos de configuración en línea usando el centro de asistencia técnica (Technical Assistance Center -TAC). Remítase a los siguientes sitios en Internet.

www.cisco.com/techsupport
www.cisco.com/tac

Para asistencia técnica en español contáctese a:

tac@cisco.com

ANEXO 2

Donwloads e información general.

Los siguientes link en Internet proporcionan descargas de software para PIX, PDM, VPN Client, así como información relevante como por ejemplo requisitos para usar PDM, requerimientos mínimos para instalar VPN client, etc.

Software.

Versiones Software PIX y PDM para descargar.	http://www.cisco.com/cgi-bin/tablebuild.pl/pix
VPN cliente software (3.6, 3.7, 4.0, etc.), para versiones de sistemas operativos: Win 9X, Win 2000, Win XP, MAC OS, Linux, Solares, entre otros.	http://www.cisco.com/cgi-bin/tablebuild.pl/vpnclient-3des
Link para upgradear PIX de DES a 3DES (para usuarios con cuenta CCO)	http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl
Link para upgradear PIX de DES a 3DES (para usuarios sin cuenta CCO)	http://www.cisco.com/pcgi-bin/Software/FormManager/formgenerator.pl

Información.

Usando el Firewall PIX	http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0b3.html
Información general acerca de cómo upgradear Software para Cisco Secure PIX Firewall y PIX Device Manager.	http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/products_tech_note09186a0080094a5d.shtml#downloads
Cisco PIX series Firewall data Sheets	http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheets_list.html

Command reference (CLI) desde la A - Z	http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_chapter09186a00800ec9e6.html
Configuración Básica VPN	http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0b2.html#wp1025148
Ejemplo de configuración VPN cliente	http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_user_guide_chapter09186a00800898ed.html
Requerimientos mínimos para instalar VPN Client	http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide09186a00800bd982.html
Configuración en detalle de VPN Client 3.X	http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide09186a00800bcd40.html#35296
Troubleshooting acerca de PDM	http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_20/pdmig/pdm_trb.htm#25143
Requerimientos mínimos para usar PDM 3.0	http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdmrn30.htm#49070
Well Known Ports	http://www.iana.org/assignments/port-numbers

ANEXO 3

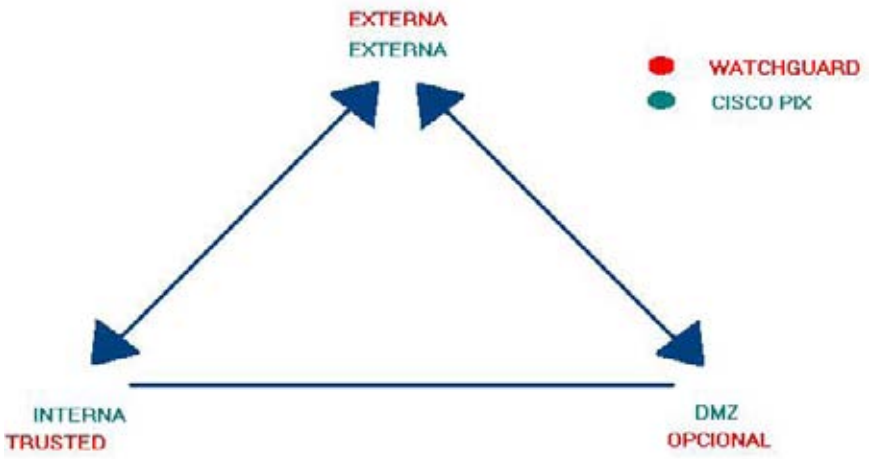
Comparación de dos de los más eficientes y comunes Firewalls utilizados actualmente : FIREWALL PIX DE CISCO Y FIREWALL WATCHGUARD.

Para llegar a estas conclusiones se ha trabajado con ambos equipos realizando una configuración estándar para ambos:

Primero comenzaremos con las similitudes:

Ambos trabajan bajo los conceptos de Estancia y Precedencia: el primero significa que el principio de todo lo que no está implícito en una regla, por defecto está negado. La Precedencia es el orden en que se deben ejecutar cada una de las reglas.

Los dos equipos tiene la misma cantidad de interfaces con el mismo propósito, ya sea que varíen sus nombres. Como se ejemplifica a continuación.



Tanto el firewall PIX como el GuatchGuard tienen la opción de utilizar los mismos algoritmos de autenticación (generalmente se utiliza IPSEC para la comunicación) SHA para autenticación y triple DES para encriptación.

Diferencias.

A pesar que ambos poseen interfaz gráfica propietaria, en el caso de PIX de Cisco es “PIX DEVICE MANAGER”: la cual cumple la función de poder adherir reglas a la configuración del equipo y de monitorear el tráfico, los túneles VPN, ocupación de CPU y memoria entre lo principal. (Nota: no se pueden colocar todo tipo de reglas de configuración a través de esta interfaz gráfica. Para esto se debe realizar a través del puerto serial muy similar a como se efectúa para configurar cualquier Router Cisco.

Esta interfaz gráfica se ejecuta y se monitorea a través de la web por HTTPS: en forma segura ya que además pide autenticarse como si fuese una VPN, es sencilla y amistosa de utilizar y carga automáticamente la configuración del firewall existente.

En el GuatchGuard se llama “WATCHGUARD FIREBOX SYSTEM” En esta interfaz se realizan todas las reglas de configuraciones que se pueden realizar en el firewall, ya sea desde bloquear puertos o servicios hasta crear VPN móvil o estáticas. Además también se utiliza para monitorear las conexiones seguras.

Esta interfaz gráfica se ejecuta y se monitorea a través de un programa previamente instalado propietario de WatchGuard que a su ves es amistoso de instalar ya que va guiando la instalación con las diferentes alternativas muy similar como instalar cualquier programa. Cuando se carga esta interfaz grafica pide buscar el archivo con la configuración del firewall y en ese momento pide autenticarse a modo de seguridad.

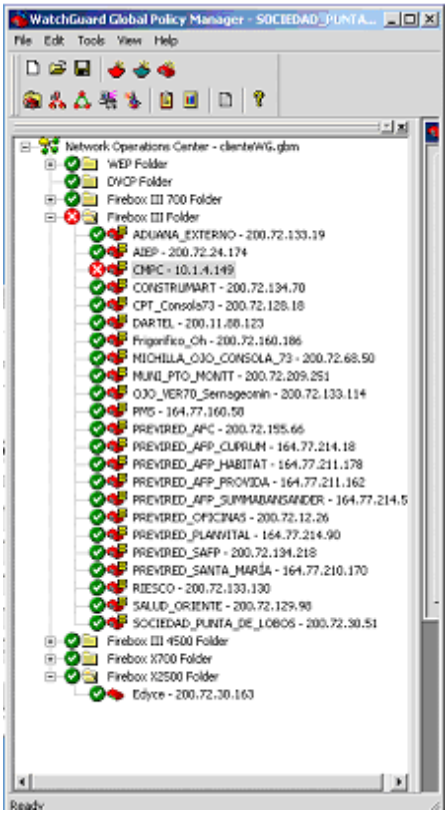
A modo de conclusión de las dos herramientas de interfaz gráfica ambas tienen buenas herramientas de monitoreo, por ejemplo es bueno destacar en el PIX el uso de la CPU y memoria, también la configuración de sus interfaces y su estado que se encuentran. En el ámbito de VPN es un poco mas débil pero muestra de buena forma los túneles IPSEC e IKE.

En WatchGuard es todo al revés, es destacable con respecto a VPN, pero tiene falencias con respecto de las interfaces del equipo.

En la creación de VPN son similares ya que cada uno tiene software propietario para el punto remoto y así poder establecer la conexión virtual en forma segura.

WatchGuard posee la flexividad de también realizar una VPN utilizando herramientas de Windows en ves del software remoto haciendo que sea mas económico ya que no es necesario adquirir una nueva licencia.

A continuación se muestran ambas interfaces gráficas:



Análisis de Hardware:

Tanto PIX de Cisco como WatchGuard poseen distintos tamaños y rendimiento de equipos, dependiendo de el propósito, desde equipos orientados a una Lan de tamaño regular hasta equipos más poderosos.

En esta parte WatchGuard posee una ventaja con la línea de equipos nuevos con los FIEBOX III, ya que todo sus modelos son idénticos en hardware y a través de la licencia que se adquiere se va liberando mas RAM y mas rendimiento, evitando cambiar de equipo.

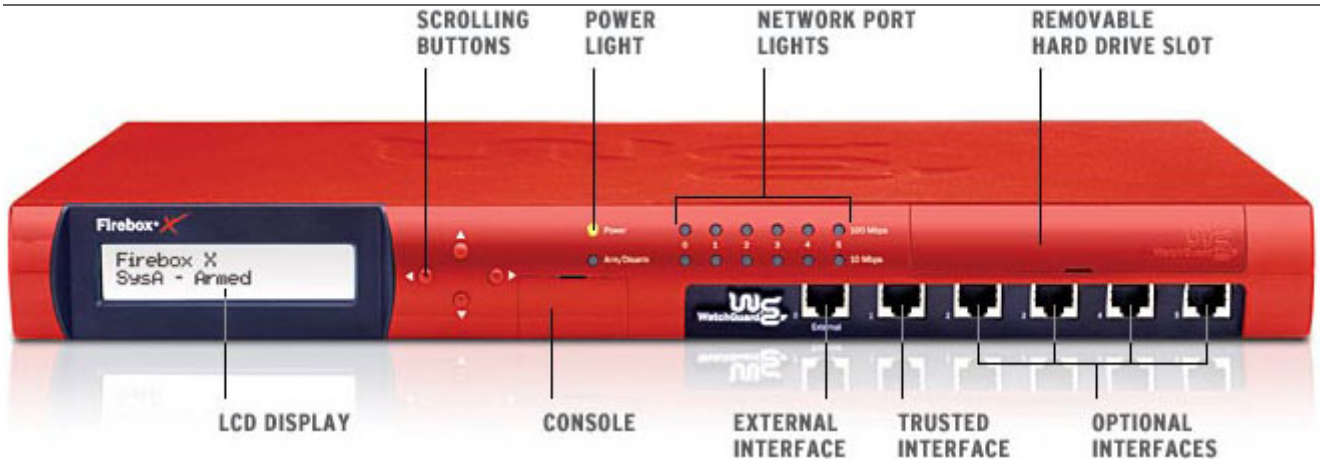
En el PIX cada una de las versiones viene en distinto Hardware.

Inicialización de equipos:

Cisco PIX: Este equipo viene de fábrica con un sistema operativo mínimo para arrancar, motivo por lo cual la IOS se tiene que descargar desde un servidor tftp o bien rescatar la IOS desde un PC portátil previamente guardado.

En WatchGuard el equipo de fábrica también arranca con un sistema mínimo, pero para cargar la IOS viene incorporada en la memoria del firewall.

Firebox® X700 Front Panel Detail



–Ficha técnica de los equipos.

En la marca WatchGuard tomamos como referencia al FIREBOX X700

Modelo Firebox®	**Firebox® X700**
Ideal para.	Creada para una mediana empresa de 50-200 usuarios que requieran una seguridad integrada.
Hardware	
Interfaces	6 10/100 Fast Ethernet 3 10/100 active w/purchase 3 10/100 upgradeable w/license key purchase Up to 4 DMZs
Securidad	
Deep Application Inspection	SMTP, HTTP, FTP, DNS
Intrusion Prevention	✔
NAT	Dynamic, Static, One-to-one
User Authentication	✔
VPN Authentication	✔
Performance	
Firewall Throughput	150 Mbps
VPN Throughput	40 Mbps
Concurrent Sessions	50,000
VPN Tunnels	
Total VPN Tunnels (Max.)	200
Branch Office VPN Tunnels (Max.)	100
Mobile User VPN Tunnels (Max.)	100
Mobile User VPN Client Licenses (Bundled)	10

- Procesador a 233 MHz AMD K6-IIE
- 64 MB SDRAM
- 8 MB flash disk
- 100-240 VCA, 50/60 Hz

• 15,5” (39.3 cm) de ancho, 2,85” (7.2 cm) de largo, 10,5” (26.6 cm) de fondo.

Precios y contacto con distribuidores oficiales en Chile.

Nota: los precios son solo referenciales ya que pueden sufrir fluctuaciones.

WatchGuard FIREBOX X500:	Precio: $1.511.300 + IVA o US$ 2.540 + IVA
WatchGuard FIREBOX X700:	Precio: $2.422.840 + IVA o US$ 4.0072 + IVA

Cisco PIX 515E:	Precio: US$ 4.269 hasta 5.690
Cisco PIX 535:	Precio: US$ 17.492

Distribuidor Oficial: MAGENTA Telefono: (2)2408100
Dirección: Reyes Lavalle 3350, Las Condes, Santiago de Chile.