ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

IMPLEMENTACIÓN DE MEJORAS DE CALIDAD DE SERVICIO DE INTERNET EN LA RED DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO

SR. CARLOS ALBERTO PASPUEL SUAREZ

SANGOLQUI- ECUADOR
2008

CERTIFICACION

Por parte del Ing. Carlos Romero e Ing. Fabián Sáenz certifican que la elaboración del proyecto IMPLEMENTACION DE MEJORAS DE CALIDAD DE SERVICIO DE INTENET EN LA RED DE LA ESCUELA POLITECNICA DEL EJERCITO fue realizado bajo su dirección.

_____	_____
Ing. Carlos Romero	Ing. Fabián Sáenz
DIRECTOR	CODIRECTOR

RESUMEN

En este trabajo se realizo el monitoreo del trafico de la ESPE, a fin de encontrar debilidades en torno a la seguridad de la red. La herramienta que se utilizo fue el Analizador de Protocolos Optiview Experta, que nos entrega de forma inmediata el tráfico de la red en un esquema de capas, desde la capa de enlace de datos hasta la capa de aplicación, al culminar el monitoreo se realizo un análisis de los datos obtenidos y se encontró algunas debilidades de la red con relación a las políticas de seguridad, a su segmentación de red y direccionamiento ip. Se recomiendo el criterio para la nueva segmentación de red y direccionamiento ip y las mejoras en las políticas de seguridad en el Cisco PIX Firewall.

DEDICATORIA

Este trabajo se lo dedico a mi madre Mercedes, a mi padre German y a mi hermana Mónica, que a lo largo de mi estudio universitario siempre estuvieron a mi lado dándome su apoyo, cariño, y todo su esfuerzo para darme la oportunidad de graduarme en la Escuela Politécnica del Ejército.

AGRADECIMIENTO

Un especial agradecimiento a Director de la tesis, el Ing. Carlos Romero que gracias a la guía y orientación que me brindo fue posible el desarrollo y culminación de este trabajo.

Además al departamento de UTIC de la ESPE a cargo de la Ing. Patricia Nogales y demás miembros del departamento, que brindaron la información necesaria de la red, que fue la base para el planteamiento de la tesis.

PROLOGO

El Campus de la ESPE cuenta con un promedio de 1000 usuarios, siendo el acceso al Internet un punto de gran concurrencia, por esta razón se realizo un monitoreo del trafico, a fin de encontrar posibles debilidades en torno a la seguridad de la red.

El Cisco Pix Firewall, es el centro de Seguridad de la red, además el punto de conexión con las demás sedes, siendo la administración de este equipo bastante delicada razón por la cual es el centro de desarrollo de la tesis.

INDICE DEL CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

GLOSARIO

ACS user database.- base de datos del ACS, para realizar el proceso de autorización.

Cache web.- Se llama caché web al caché que almacena documentos web (es decir, páginas, imágenes, etcétera) para reducir el ancho de banda consumido, la carga de los servidores y el retardo en la descarga.

Cisco Secure ACS.-servidor que ayuda al control de acceso a la red, este control lo realiza por medio de la autenticación, autorización y administración de cuentas (AAA).

Broadcast.-, en castellano difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Ftp.- es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor.

Firewall.- un elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.

Fingerprint scanning.- consiste es realizar un escaneo de la yema de los dedos y obtener la huella digital.

Gateway.- en informática, equipos para interconectar redes.

Hash.- En informática, Hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.,

Host.- El término host (equipo anfitrión) en informática o computación puede referirse a: Aquel ordenador de la red que ofrece servicios a otros ordenadores conectados a dicha red o una máquina conectada a una red de ordenadores y que tiene un nombre de equipo

Http.- El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW).

Https.- es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

Hub.- Un concentrador o hub es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

Icmp.- es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP).

Modem.- es un dispositivo que sirve para modular y demodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada portadora mediante otra señal de entrada llamada moduladora.

Multicast.- es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

Nat.- es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

Ping .- (Packet Internet Grouper) se trata de una utilidad que comprueba el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (definidos en el protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o enrutadores IP.

Radius.-protocolo que proporciona servicios de autenticación, autorización y administración de cuentas.

Router.- ruteador o encaminador es un dispositivo de hardware para interconexión de red de computadoras que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.
Snmp.- es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red

Spanning tree.- (STP) es un protocolo de red de la segunda capa OSI. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes

Switch.- en castellano "conmutador" es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Tcp.- en español Protocolo de Control de Transmisión es uno de los protocolos fundamentales en Internet.
Tipping point.-

Tacacs.- es un protocolo de autenticación remota que se usa para comunicarse con un servidor de autenticación comúnmente usado en redes Unix.

Udp.- es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

Web.- o Red Global Mundial es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet.

Wireless.- La comunicación inalámbrica (inglés wireless, sin cables) es el tipo de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión.

CAPITULO 1

INTRODUCCION

1.1 SEGURIDAD EN REDES

Las computadoras, las redes e Internet afectan cotidianamente la vida del ser humano. El mundo tecnológicamente depende cada vez más de las computadoras y de las redes.

Al principio de la ola tecnológica, mucha gente dudaba de este fenómeno, y el número de personas involucradas era relativamente reducido, en este entorno las personas confiaban unos en otros y trabajaban con toda libertad sin ningún temor. En este ambiente la seguridad de las computadoras y el software no eran prioritarios.

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

Una *internetwork* se compone de varias redes conectadas entre sí. Cuando se accede a información en un entorno *de internetwork*, hay que crear áreas seguras, el dispositivo que crea estas zonas se denomina *firewall.*

1.2 FIREWALL

Un *firewall* es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red privada y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Trabaja como un filtro que controla todas las comunicaciones que pasan de una red a la otra, en función de lo que se permite o deniega su paso. Para permitir o denegar una comunicación el *firewall* examina el tipo de servicio al que corresponde, como pueden ser el *web*, el correo, ftp, etc. Dependiendo del servicio el *firewall* decide si lo permite o no. Además, el *firewall* examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un *firewall* puede permitir desde una red local hacia Internet servicios de *web*, correo y *ftp*. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor *web* y queremos que accesible desde Internet). Dependiendo del *firewall* que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un *firewall* puede ser un dispositivo software o hardware, es decir, un aparato que se conecta entre la red y la conexión a Internet, o bien un programa que se instala en la máquina que tiene el *modem* que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con software específico que lo único que hacen es monitorizar las comunicaciones entre redes.

Cuando el *firewall* es de hardware, este dispositivo suele tener un mínimo de tres interfases, creando un mínimo de tres redes, cumpliendo cada una de ellas; las siguientes funciones:

Interior: es el área de confianza de la *internetwork*. Los dispositivos que están en el interior forman las redes privadas de la organización.

DMZ (Zona desmilitarizada): es una red o redes aisladas, a la que pueden acceder los usuarios del exterior. Es necesario configurar el *firewall* para permitir el acceso desde el exterior o interior hasta la DMZ. La creación de esta DMZ posibilita que una empresa ponga la información y servicios a disposición de los usuarios del exterior dentro de un entorno seguro y controlado, sin permitir el acceso al interior.

Exterior: es el área de no confianza de la *internetwork.* El *firewall* protege los dispositivos del interior y la DMZ de los dispositivos del exterior.

Los servidores que residen en la DMZ, suelen denominarse *host* bastión, el mismo que se está actualizando constantemente con respecto a su sistema operativo, lo que garantiza que sea menos vulnerable a los ataques.

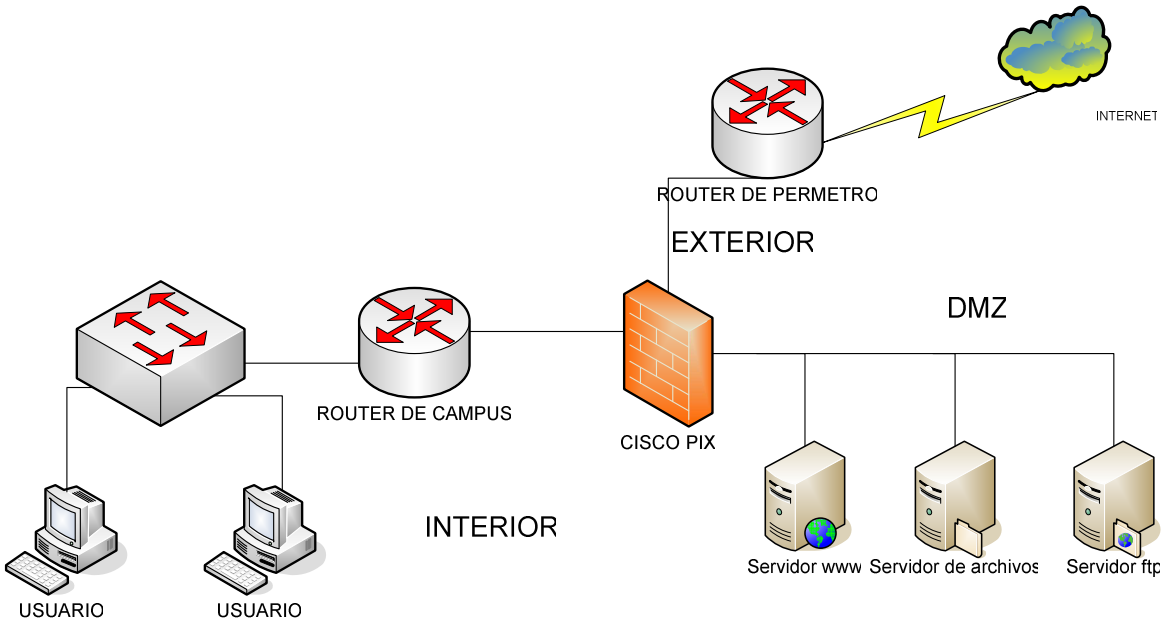


Figura 1.1 firewall, seguridad perimetral de la red

Las funciones básicas de un *firewall* son:

- ✓ No permitir acceso desde el exterior al interior.
- ✓ Permitir un acceso limitado desde el exterior a la DMZ.
- ✓ Permitir todo el acceso desde el interior hasta el exterior.
- ✓ Permitir un acceso limitado desde el interior hasta la DMZ.

1.3 TIPOS DE ATAQUES

Podemos definir como ataques, todas aquellas acciones que suponen una violación de la seguridad de nuestro sistema, confidencialidad, integridad o disponibilidad.

Estas acciones se pueden clasificar de modo genérico según los efectos causados, como:

Interrupción: cuando un recurso del sistema es destruido o se vuelve no disponible.

Intercepción: una entidad no autorizada consigue acceso a un recurso.
Modificación: alguien no autorizado consigue acceso a una información y es capaz de manipularla.
Fabricación: cuando se insertan objetos falsificados en el sistema.

También se pueden ordenar por modalidades de ataque según la forma de actuar:

Ataque de reconocimiento: un intruso trata de descubrir sistemas, servidores y puntos débiles.

Ataque de acceso: un intruso ataca las redes o sistemas para recuperar datos, obtener acceso o incrementar sus privilegios de acceso personales.

Ataque de negación de servicio: un intruso ataca la red de tal forma que daña o corrompe el sistema computacional, o impide que otros usuarios autorizados pueden acceder a sus redes, sistemas o servicios.

El ataque de reconocimiento tiene lugar cuando un usuario no autorizado trata de descubrir dispositivos y puntos débiles del sistema de red, también se conoce como recopilación de información y en la mayoría de los casos, precede de un acceso real o un ataque de denegación de servicio.

El intruso suele barrer la red con *pings* para determinar qué dirección IP están activas y responden. De esta forma puede determinar los servicios o puertos activos en las direcciones IP, y al reconocer los puertos de la aplicación podrá determinar el tipo y la versión de la aplicación, así como el tipo y la versión del sistema operativo que se está ejecutando en el *host* destino.

Un ataque de acceso puede materializarse como recuperación y manipulación no autorizada de datos, un acceso al sistema o un incremento de privilegios. Estos ataques también se pueden utilizar para obtener el control de un sistema e instalar y ocultar software para que los intrusos lo utilicen con posterioridad.

La recuperación no autorizada de datos consiste en escribir, copiar o trasladar archivos a los cuales el intruso no puede acceder.

Un atacante del acceso al sistema ocurre cuando obtiene acceso a un sistema sin autorización, el incremento no autorizado de privilegios, por lo general ocurre por los usuarios legítimos con niveles de privilegios muy bajos.

La denegación de servicio ocurre cuando un atacante desactiva o corrompe las redes, los sistemas o los servicios para denegar el servicio de los usuarios. Suele implicar que el sistema se colapse hasta el punto que sea inutilizable.

1.4 POLÍTICAS DE SEGURIDAD

Los riesgos que se enfrentan ha llevado a que muchos desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Definición de Políticas de Seguridad Informática

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que los mismos establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

Elementos de una Política de Seguridad Informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

Objetivos de la política y descripción clara de los elementos involucrados en su definición.

Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.

Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.

Definición de violaciones y sanciones por no cumplir con las políticas.

Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos.

Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

Parámetros para Establecer Políticas de Seguridad

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.

Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.

Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos de su área.

Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.

Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Razones que Impiden la Aplicación de las Políticas de Seguridad Informática

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para juguetes del Departamento de Sistemas".

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y

necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

CAPITULO 2

SITUACION ACTUAL DE LA RED

2.1 TOPOLOGIA DE RED

La topología que utiliza la red la ESPE, esta compuesta por el PIX, como seguridad perimetral para proteger tanto la red interna y servidores. Estos servidores están separados en una red denominada anteriormente DMZ (zona desmilitarizada).

Dentro de la DMZ, tenemos los servidores Web, ftp, y dns.

En la red interna tenemos los siguientes servidores Ret Hat Linux Interprise, Microsoft Isa Server 2006, Windows Server 2003

Cave mencionar que el PIX posee un failover que sirve de redundancia en caso de algún fallo del PIX.

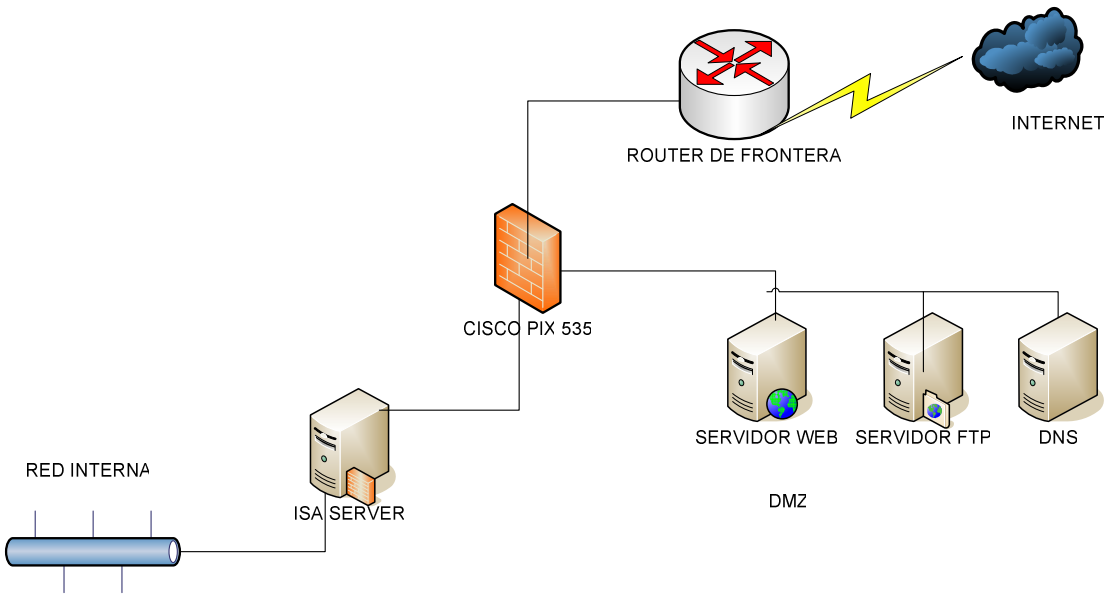


figura. 2.1. topología de la RED de la ESPE

2.2 DIRECCIONAMIENTO IP

Pix Y Failover:

	Red	Dirección IP	mascara
Red Interna	192.168.1.16	192.168.1.18	255.255.255.248
Red Externa	192.168.58.32	192.188.58.33	255.255.255.224
DMZ	192.168.58.160	192.188.58.162	255.255.255.224
Sedes	192.168.58.192	192.188.58.193	255.255.255.248
Failover externa		192.188.58.62	255.255.255.224
Failover interna		192.168.1.19	255.255.255.248
Failover DMZ		192.188.58.190	255.255.255.225
Failover sedes		192.18.58.197	255.255.255.248

Servidores En La Dmz:

	Red	Dirección IP	mascara
	192.168.58.160		255.255.255.224
Dns		192.188.58.163	255.255.255.224
WEB(pagina espe)		192.188.58.167	255.255.255.224
Protocol Tranfer File		192.188.58.170	255.255.255.224

Red interna:

	Red	mascara	
Administración	10.1.100.0	255.255.252.0	Vlan 1
Usuarios	10.1.0.0	255.255.252.0	Vlan 7
	10.1.4.0	255.255.252.0	Vlan 8
	10.1.8.0	255.255.252.0	Vlan 9
	10.1.12.0	255.255.252.0	Vlan 10
	10.1.16.0	255.255.252.0	Vlan 11
	10.1.20.0	255.255.252.0	Vlan 12
Telefonía IP	10.1.24.0	255.255.252.0	Vlan 50

Servidores Red Interna:

	Red 10.1.0.0	Dirección IP	mascara
Dhcp		10.1.0.2	255.255.252.0
Dns Primario		10.1.0.104	255.255.252.0
Dns Secundario		10.1.0.110	255.255.252.0
Isa Server		10.1.0.112	255.255.252.0
Antivirus		10.1.0.252	255.255.252.0
Servidor de Correo Profesores		10.1.0.114	255.255.252.0
Servidor de Correo Alumnos		10.1.0.115	255.255.252.0

2.3 POLÍTICAS DEL ISA SERVER

ISA Server 2006 es un *gateway* integrado de seguridad perimetral que contribuye a la protección del un entorno de TI frente a amenazas procedentes de Internet, y además ofrece a los usuarios un acceso remoto rápido y seguro a sus aplicaciones y datos corporativos. ISA Server 2006 puede utilizarse en tres escenarios principales de uso:

Publicar aplicaciones de forma segura.-esta funcionalidad de ISA Server 2006 permite que las organizaciones puedan disponer de acceso a sus servidores Exchange, *SharePoint* u otras aplicaciones Web de forma segura desde fuera de la red corporativa.

Gateway para redes de oficina.-las organizaciones pueden utilizar ISA Server 2006 como *gateway* para enlace de oficinas remotas, facilitando su conexión y seguridad, y aprovechando al máximo el ancho de banda disponible

Protección de acceso al Internet.-este servicio de ISA Server 2006 permite proteger los entornos corporativos frente a amenazas basadas en tecnologías de Internet, procedentes del exterior o de la propia red corporativa.

Las políticas del servidor ISA son las siguientes:

- ✓ Permitir trafico Dns desde servidores de control de dominio y servidores de correo de alumnos hacia la red externa
- ✓ Permitir Conexiones de clientes VPN desde la red externa hacia la red interna.

- ✓ Permitir tráfico desde el *Tipping Point* hacia la red externa.
- ✓ Bloquear Radio y televisión desde la red interna hacia la externa.
- ✓ Permitir acceso a páginas internas desde la red interna a la red externa.
- ✓ Bloquear páginas prohibidas y pornográficas desde la red interna hacia la externa.
- ✓ Bloquear el Internet a usuarios en particular.
- ✓ Permitir bajar de Internet archivos ejecutables, como presentaciones, etc
- ✓ Bloquear Messenger a todos los usuarios de la red interna
- ✓ Permitir el acceso *ftp* y *http* desde los administradores al *switch core.*
- ✓ Permitir el tráfico de Internet a usuarios de la red *wirelees.*
- ✓ El Isa Server además esta trabajando como *Web Cache*

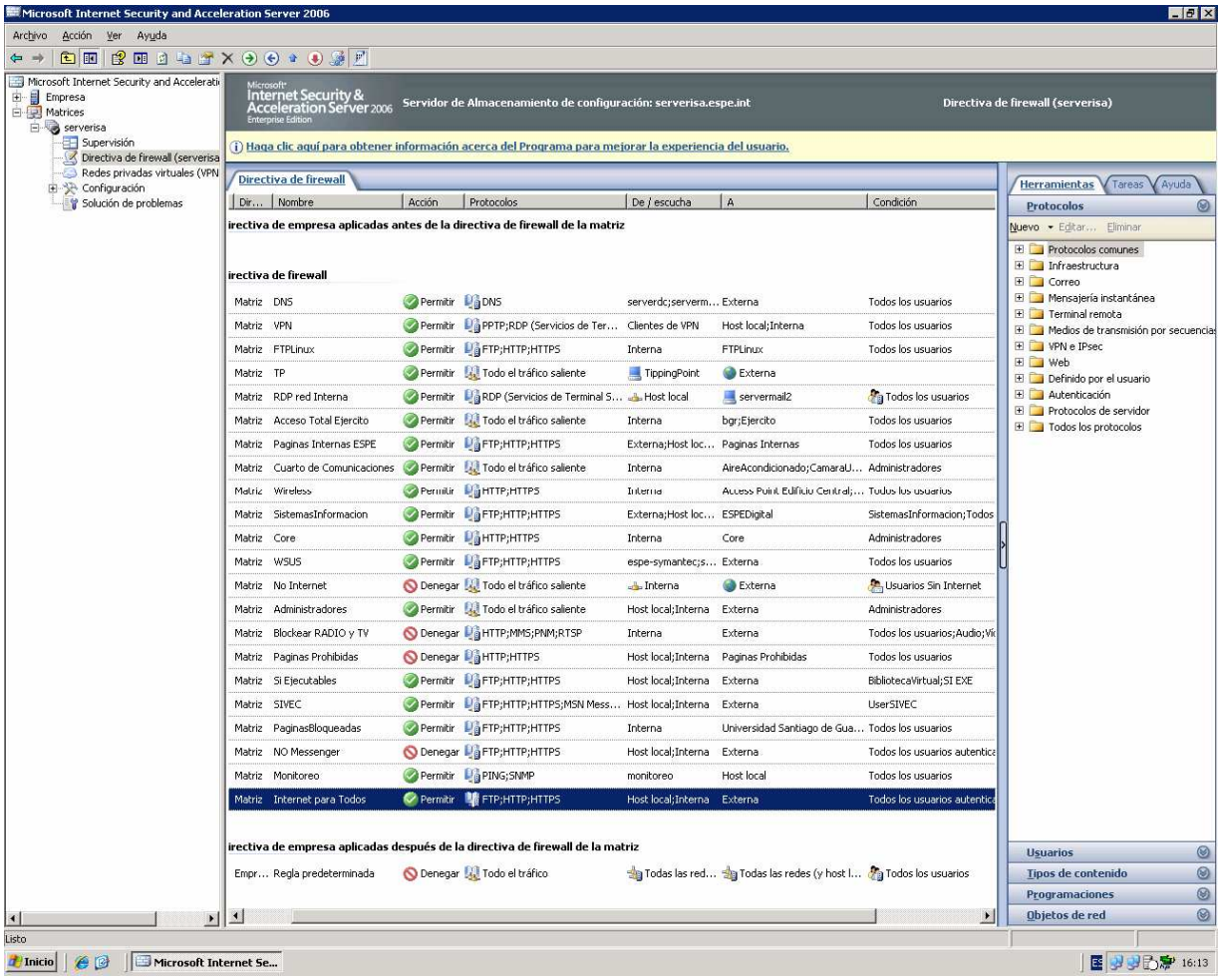


figura. 2.2. políticas de seguridad del isa server

2.4 MONITOREO DE LA RED MEDIANTE ANALIZADOR DE PROTOCOLOS

Miércoles, 21 de mayo 2008.

TRAFICO DE INTERNET

tabla. 2. 1. ancho de banda Internet 1

HORA	ANCHO DE BANDA(Mbps)
7:30	6,5
8:30	7,5
9:30	10
10:30	12
11:30	15
12:30	15
13:30	14
14:30	12
15:30	10
16:30	10

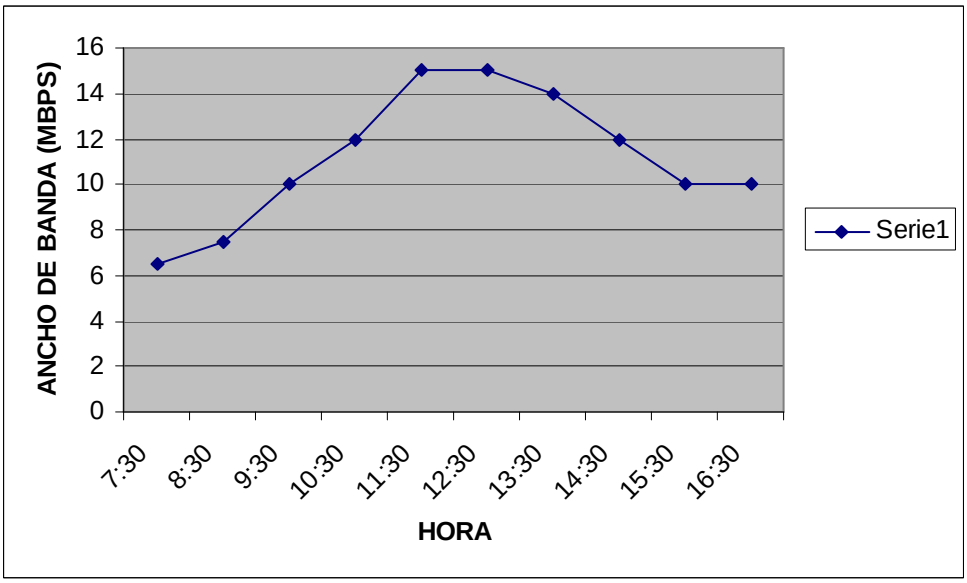


figura. 2.3. ancho de banda de Internet vs. Hora (1)

ANCHO DE BANDA PICO 15Mbps
HORA 11:30

Jueves, 22 de Junio 2008

TRAFICO DE INTERNET

tabla. 2. 2. ancho de banda Internet (2)

HORA	ANCHO DE BANDA(MBPS)
8:00	11,8
9:00	11,6
10:00	11
11:00	11
12:00	12
13:00	10
14:00	10
15:00	11
16:00	7,5
17:00	7
18:00	7,5
19:00	7
20:00	6
21:00	8
22:00	7
23:00	0

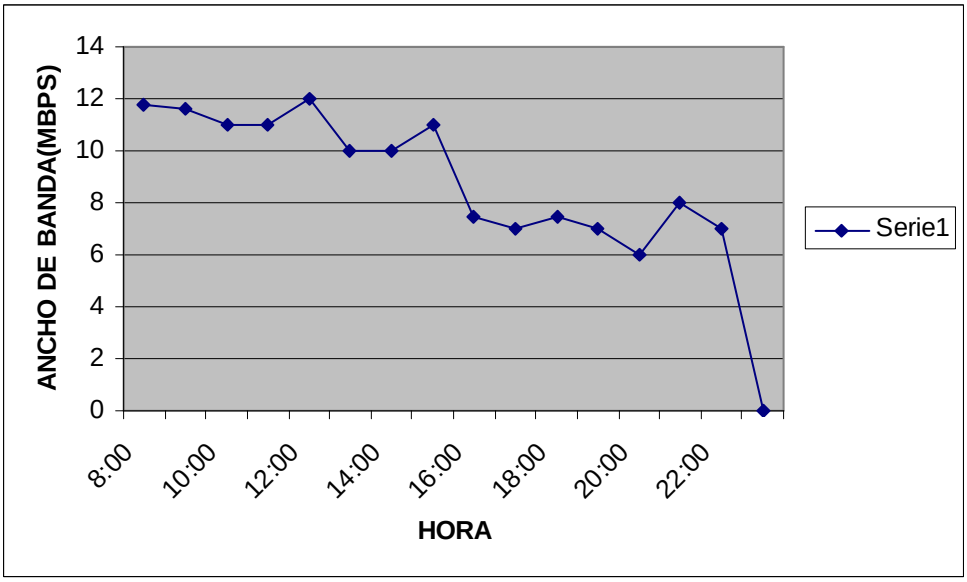


figura. 2.4. ancho de banda de Internet vs. Hora (2)

ANCHO DE BANDA PICO 12Mbps
HORA 12:00

Lunes, 2 de junio 2008

TRAFICO DE INTERNET

tabla. 2. 3. ancho de banda Internet (3)

HORA	ANCHO DE BANDA(MBPS)
7:30	6,2
8:30	7,5
9:00	8,5
9:30	7,2
10:00	4,2
10:30	5,2
11:00	6
11:30	15
12:00	8
12:30	7,3
13:00	7,1
13:30	6,7
14:00	5,8
14:30	6,3
15:00	6,2
15:30	6,1
16:00	5
16:30	5,5

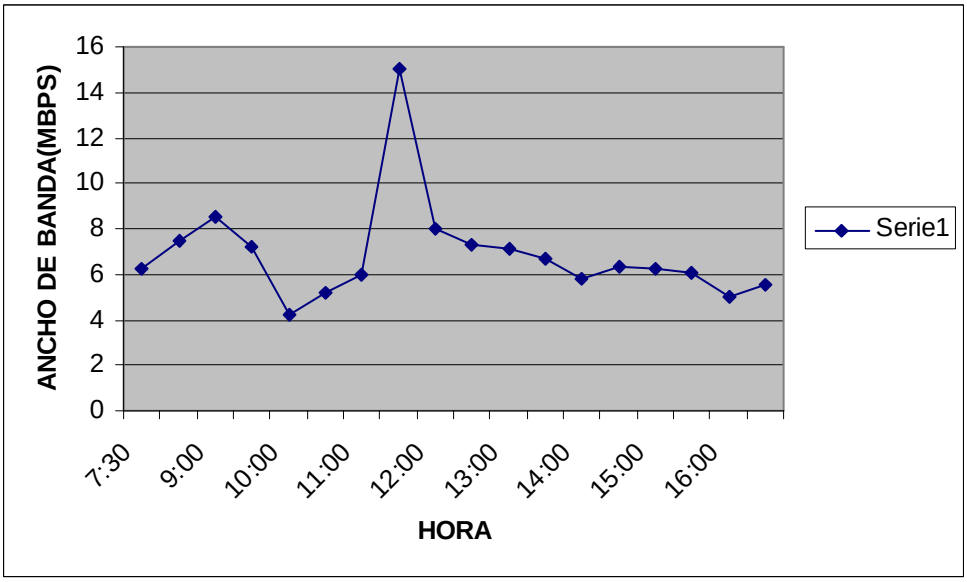


figura. 2.5. ancho de banda de Internet vs. Hora (3)

ANCHO DE BANDA PICO	15Mbps
HORA:	11:30

Martes, 3 de junio 2008

TRAFICO DE INTERNET

tabla. 2. 4. ancho de banda Internet (4)

HORA	ANCHO DE BANDA(MBPS)
7:30	8
8:30	7,6
9:00	4
9:30	2,8
10:00	2,4
10:30	1,6
11:00	1,6
11:30	15
12:00	22
12:30	20
13:00	18
13:30	17
14:00	16
14:30	16,2
15:00	16,2
15:30	16,2
16:00	14
16:30	10,8

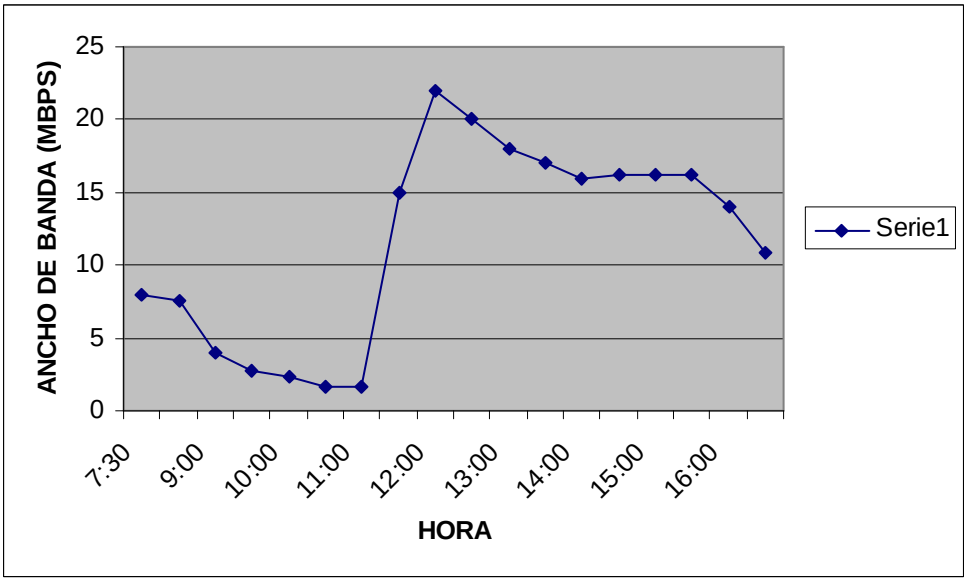


figura. 2.6. ancho de banda de Internet vs. Hora (4)

ANCHO DE BANDA PICO	22Mbps
HORA	12:00

Miércoles, 4 de junio 2008

TRAFICO DE INTERNET

tabla. 2. 5. ancho de banda Internet (5)

HORA	ANCHO DE BANDA(MBPS)
14:00	15,5
14:30	11,7
15:00	9
15:30	10
16:00	9,3
16:30	8,3
17:00	7,8
17:30	8
18:00	8,1
18:30	7,7
19:00	7,3
19:30	7,3
20:00	7,3

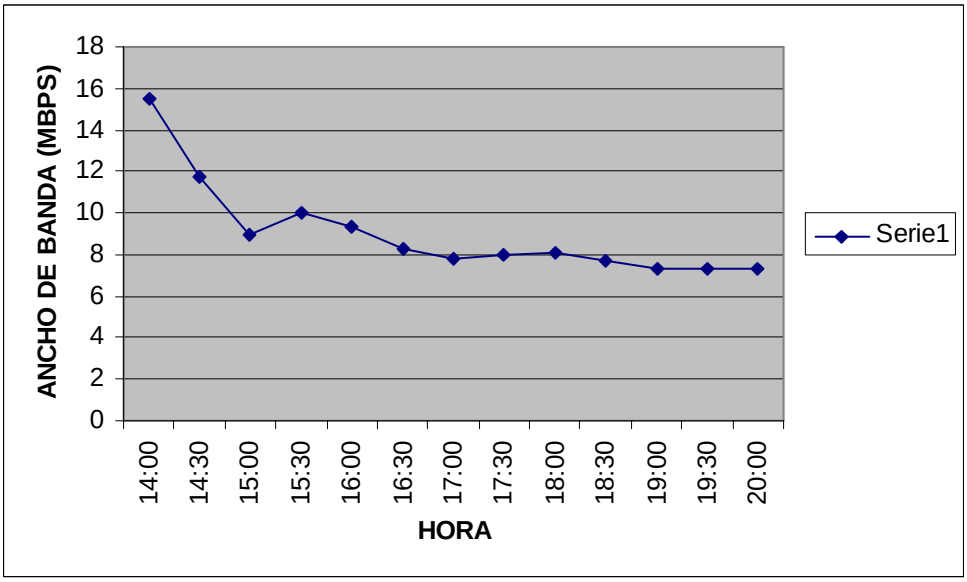


figura. 2.7. ancho de banda de Internet vs. Hora (5)

ANCHO DE BANDA PICO	15,5 Mbps
HORA	14:00

Jueves, 5 de junio 2008

TRAFICO DE INTERNET

tabla. 2. 6. ancho de banda Internet (6)

HORA	ANCHO DE BANDA(MBPS)
7:30	2,5
8:00	2,6
8:30	2,6
9:00	10
9:30	11
10:00	12
10:30	12
11:00	12
11:30	12,5
12:00	13,8
12:30	7,3
13:00	11,8
13:30	7,1
14:00	22
15:00	15
15:30	9,1

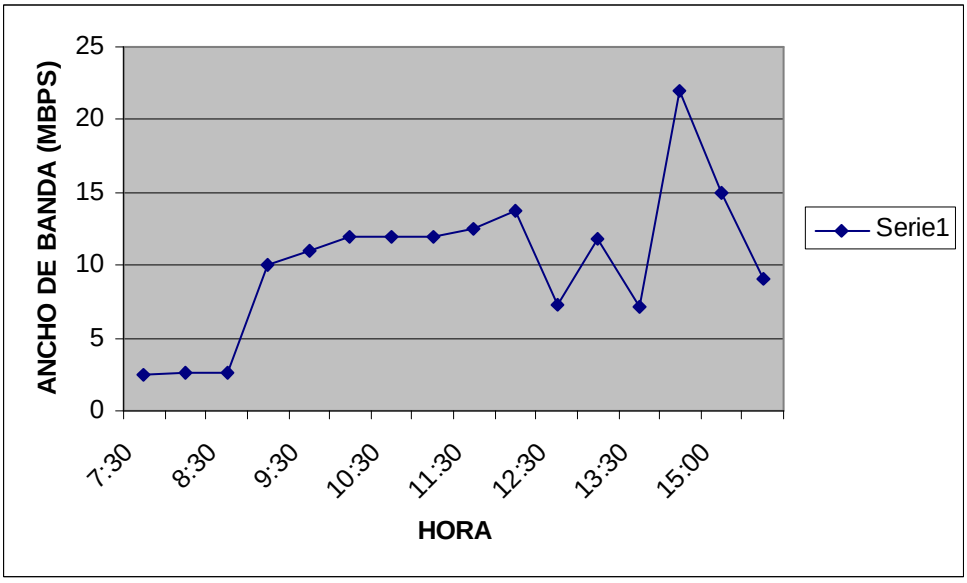


figura. 2.8. ancho de banda de Internet vs. Hora (6)

ANCHO DE BANDA PICO	22Mbps
HORA	14:00

2.4.1 Tipos De Protocolos Que Transitan La Red

tabla. 2. 7.protocolos que transitan la red

PROTOCOLO	VALOR PORCENTUAL
ARP	9,76
802.1D	0,5
IPv6	1,6
http	2
ICMP	12,5
DHCP	0,6
WWW	57,3
NETBIOS	6
SMB	2,5
LDAP	1,3
Otros	5,9

2.4.2 Ancho De Banda Utilizado Por Cada Protocolo

Grafico Porcentual

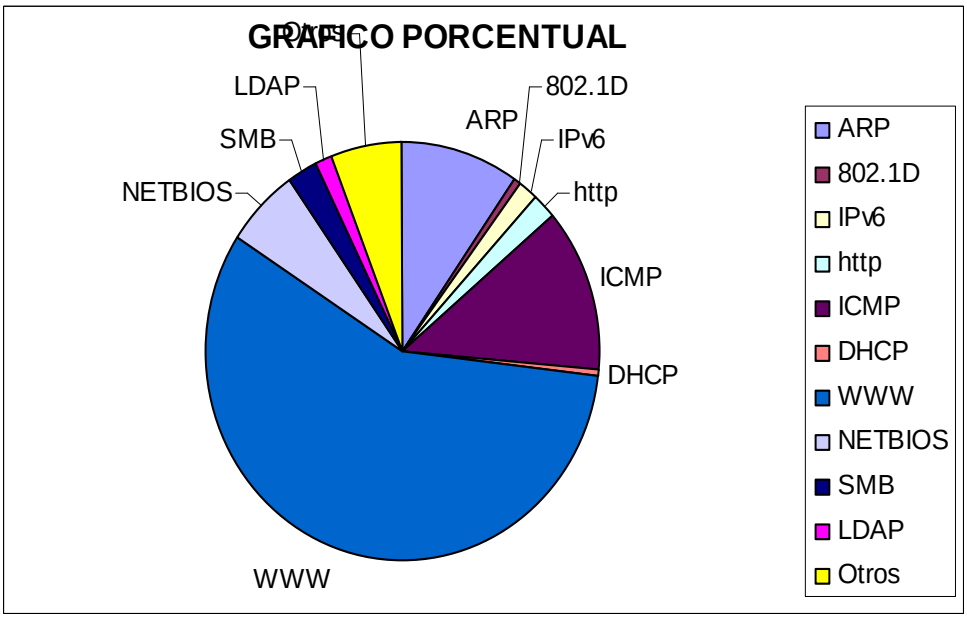


figura. 2.9. gráfico porcentual del trafico de la red

SERVER MESSAGE BLOCK.- SMB es un Protocolo de red (que pertenece a la capa de aplicación en el modelo OSI) que permite compartir archivos e impresoras (entre otras

cosas), entre nodos de una red. Es utilizado principalmente en ordenadores con Microsoft Windows y DOS.

NETBIOS .-Es un protocolo de resolución de nombres que puede ser encapsulado sobre TCP/IP. NetBIOS funciona a nivel de la capa de aplicación, dando una apariencia uniforme a todas las redes Windows independientemente de los protocolos que se hayan utilizado para las capas de red y transporte. Permite compartir archivos e impresoras así como ver los recursos disponibles en Entorno de red.

ARP.-Es un protocolo de nivel de red responsable de encontrar la dirección hardware (*Ethernet MAC*) que corresponde a una determinada dirección IP. Para ello se envía un paquete (*ARP request*) a la dirección de multidifusión de la red (*broadcast* (MAC = ff ff ff ff ff ff)) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (*ARP reply)* con la dirección *Ethernet* que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección *Ethernet*, pero esto sólo funciona si todas las máquinas lo soportan.

ICMP.-El Protocolo de Mensajes de Control de Internet (por sus siglas de *Internet Control Message Protocol*) es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un *router* o *host* no puede ser localizado

802.1D.- es el estándar de IEEE para *bridges* MAC (puentes MAC), que incluye *bridging* (técnica de reenvío de paquetes que usan los *switches)*, el protocolo *Spaning Tree* y el funcionamiento de redes 802.11, entre otros.

DHCP.- significa Protocolo de configuración de *host* dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma *dinámica* (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

HTTP.- El protocolo de transferencia de hipertexto (*HyperText Transfer Protocol*) es un protocolo del nivel de aplicación usado para la transferencia de información entre sistemas, de forma clara y rápida. Este protocolo ha sido usado por el World-Wide Web desde 1990.

WWW.- trafico de Internet en la red interna de la ESPE, a través del servidor ISA, puerto de aplicación 8080.

2.5 DETECCIÓN DE PROBLEMAS EN LA RED DE LA ESPE

A partir del análisis del tráfico de la red de la Espe se detectaron los siguientes problemas:

- ✓ Demasiado trafico ARP en la red
- ✓ Constante duplicación de direcciones IP
- ✓ Dominio de *broadcast* muy grande, en promedio de 800 a 1000 usuarios
- ✓ Exceso de trafico *icmp* desde la red externa al servidor Proxy de Internet

CAPITULO 3

FUNCIONAMIENTO DEL CISCO PIX FIREWALL

3.1 ALGORITMO ADAPTATIVO DE SEGURIDAD

Todas las interfases del *firewall* se configuran de la misma forma, esto se debe a que el ASA (Algoritmo de seguridad adaptativo), utiliza el concepto de niveles de seguridad.

Entre dos interfases, una estará a un nivel más alto y otra a un nivel mas bajo. Por lo tanto el nivel de seguridad designa el hecho de que una interfaz sea interna (fiable) o externa (no fiable) con respeto a otra interfaz.

La regla principal de los niveles de seguridad es que los datos pueden acceder al PIX a través de una interfaz con un nivel de seguridad más alto, pasar por el PIX y salir a través de una interfaz con un nivel de seguridad mas bajo. Por lo contrario si deseamos que los datos pasen a través de una interfaz con un nivel de seguridad bajo y salir a una interfaz con un nivel de seguridad alto, esto solo es posible por medio de listas de acceso.

Los niveles de seguridad están comprendidos de 0 a 100, y sus reglas son las siguientes:

Nivel de seguridad 100.- es el nivel de seguridad mas alto de una interfaz, por lo tanto se utiliza para la interfaz interna del PIX, es decir la red de la organización deberá estar configurada detrás de esta interfaz, así nadie podrá acceder a los datos de la red a menos que se le otorgue un permiso, el mismo que deberá estar configurado en el PIX.

Nivel de seguridad 0.- es el nivel de seguridad mas bajo, siempre se le asignara para la interfaz externa, esta interfaz nos sirve para conectarnos al Internet.

Nivel de seguridad 1-99.- estos niveles de seguridad se las asigna a las interfases del perímetro que están conectadas al PIX. Es muy habitual conectar a estas interfases a una red que actué como zona desmilitarizada (*DMZ*). Una *DMZ* es un entorno al que pueden acceder los usuarios desde la red externa, y separadamente de la red interna.

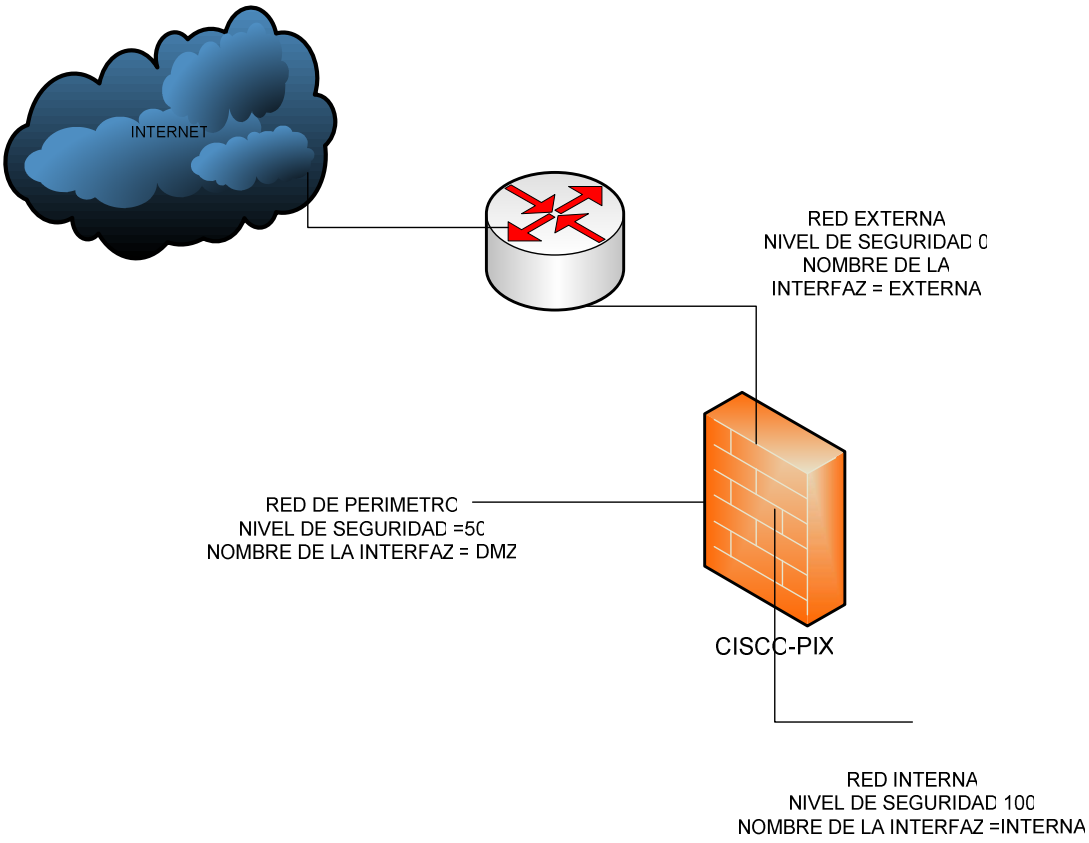


Figura. 3.1. niveles de seguridad

3.2 FLUJO DE SESIONES

La encapsulación tiene lugar al principio de una sesión, estos datos al combinarse con la información de la capa de transporte pasan a conformar un segmento, estos a su vez se encapsulan con la información de capa de red para formar un paquete, finalmente estos datos llegan la capa de enlace de datos y forman las tramas.

El PIX busca información específica en la trama para tomar decisiones importantes acerca del tráfico que fluirá a través de la red.

En la figura 3.2 se ilustra la encapsulación de un maquina con dirección IP 10.0.0.3 que inicia la sesión con el comando telnet 172.30.0.50

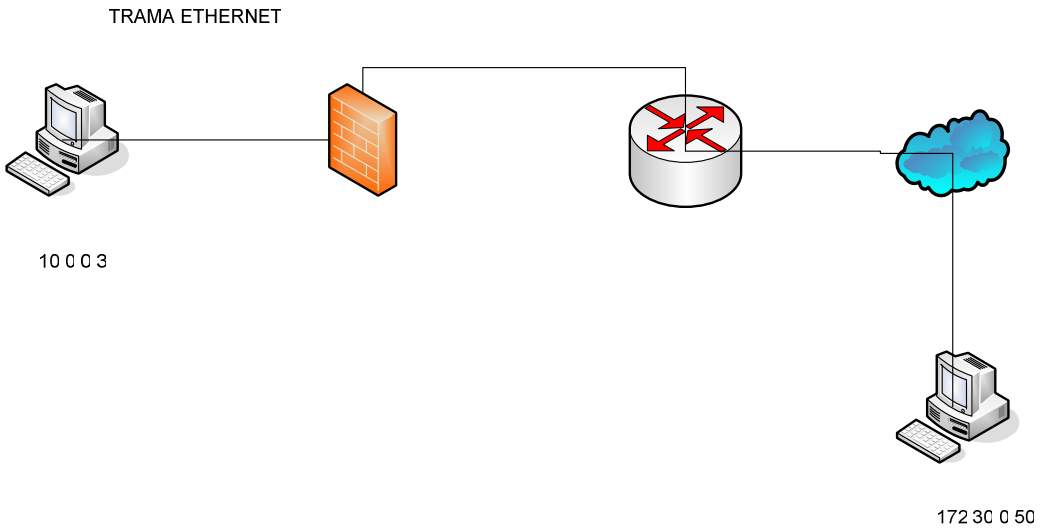


Figura. 3.2. flujo de sesion

El término saliente indica que las conexiones se han iniciado desde el lugar de máxima seguridad de la red o más fiable, hasta uno menos fiable; y las conexiones entrantes son las que se han iniciado desde un lugar menos fiable del PIX, hasta una interfaz más fiable.

Para tratar de una forma más comprensible como trata el PIX las conexiones entrantes y salientes, tenemos que referirnos a los principales protocolos de transporte; TCP y UDP.

Una sesión de red se establece por medio de estos protocolos:

- TCP (Protocolo para el control de Transmisión) que es de fácil inspección.
- UDP (Protocolo da datagrama de usuario) que su inspección resulta difícil para el PIX.

PROTOCOLO DE CONTROL DE TRANSMISION

TCP es un protocolo orientado a conexión, al iniciarse una conexión desde un *host* que se encuentra en la red interna o confiable, el PIX crea una entrada en su tabla de estado de conexión.

El PIX es capaz de extraer la información de sesión de red del flujo de red y verificar su validez en tiempo real, este filtro mantiene la información de cada conexión de red y

comprueba la información subsiguiente como el número de puerto origen y destino, dirección IP. Al iniciar TCP una sesión a través del PIX, este graba el flujo de red y busca un acuse de recibo desde el dispositivo de destino, permitiendo el intercambio de señales en tres vías.

A continuación se indica los pasos que ocurren al establecerse una sesión TCP a través del PIX.

Al recibir el PIX un paquete IP desde el interior, comprueba si no hay una línea de conversación, en caso de que no existiera, este la creará. Una línea de conversación es la dirección IP interna y la dirección IP globalmente única. Esta información se graba en memoria y puede ser cotejada por el flujo de información subsiguiente.

En el ejemplo anterior 10.0.0.11 se convierte a 192.168.0.20, inmediatamente se utiliza la información de la capa de transporte para crear la ranura de conexión.

El PIX convierte el número de secuencia inicial (49091) de la conexión interna y reenvía el paquete por la interfaz saliente.

A continuación espera del host destino, un paquete SYN/ ACK, compara el paquete recibido con la ranura de conexión, calcula la información se secuencia y reenvía el paquete al host interno.

El *host* interno completa el intercambio en tres vías, con un acuse de recibo. La ranura de conexión está marcada como activa y se transmiten los datos. Es en este momento cuando se reinicia el contador embrionario de esta conexión.

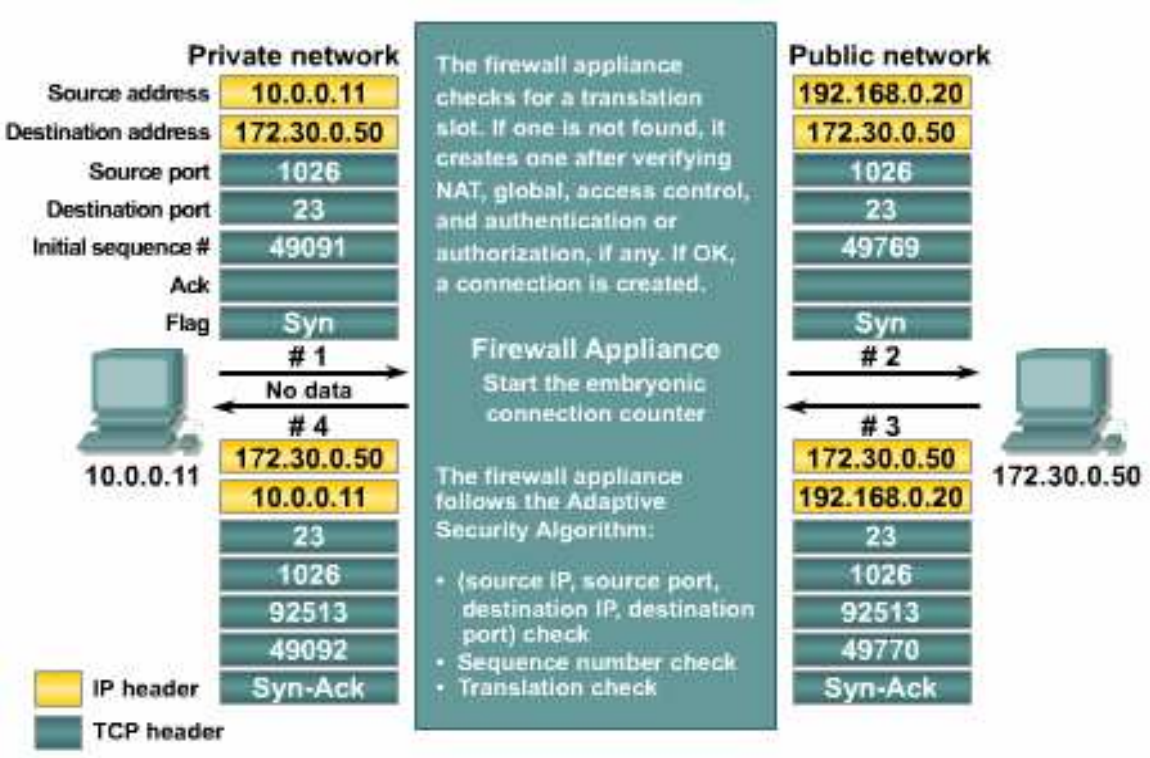


Figura. 3.3 Iniciación TCP, del interior al exterior

PROTOCOLO DE DATAGRAMA DE USUARIO

UDP es un protocolo no orientado a conexión, por lo que resulta difícil garantizar su seguridad, ya que no existe intercambio de tres vías ni secuenciación, de igual manera resulta difícil mantener una conexión ya que no tiene ni un inicio, ni un estado de flujo.

Lo único que garantiza el PIX es crear una ranura de conexión UDP, cuando un paquete UDP es enviado desde una interfaz mas segura hasta una interfaz menos fiable, los paquetes devueltos con posterioridad que coincidan con la ranura de conexión serán reenviados la red interna.

Cuando la ranura de conexión permanezca inactiva más del tiempo configurado, se eliminará de la tabla de conexión.

Algunas características de UDP se indican a continuación:

- ✓ UDP no garantiza la entrega
- ✓ UDP carece de administración o prevención de la congestión
- ✓ No existe configuración o finalización de la conexión.

- ✓ UDP es un protocolo de transporte no fiable, pero eficiente.

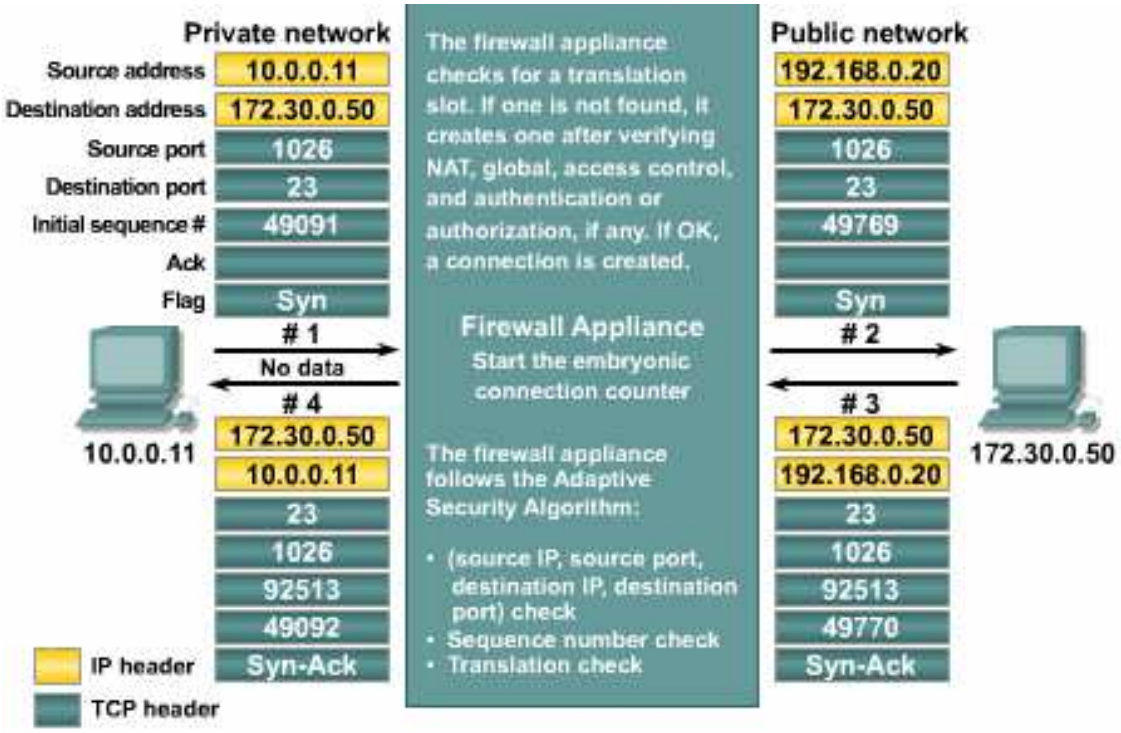


Figura. 3.4 Sesión UDP en el Firewall

CAPITULO 4

CONFIGURACION DEL FIREWALL

4.1 INTRODUCION

En este capítulo detallamos los comandos de configuración básica del PIX, utilizados para asignar nombre al PIX, dirección IP a la interfaz, nivel de seguridad a cada interfaz, nombre para identificar a la interfaz, lista de acceso para permitir el tráfico y las capacidades de enrutamiento del PIX.

Se explica los conceptos de conversión estática y conversión dinámica, que son utilizados en conjunto para dar diferentes tipos de accesos a través del PIX.

El acceso desde la parte interna hacia la externa por medio de los comandos *nat*, *pat* y global y la sintaxis de cada uno de ellos.

De la parte externa hacia la interna con el comando *access-list*, y una detallada explicación de los diferentes parámetros que podemos utilizar. Se revisa también algunos de las opciones del comando show, para verificar el estado y configuración del PIX.

En la parte final se realiza un ejemplo de configuración de múltiples interfases del PIX.

4.2 CONFIGURACIÓN BÁSICA

Los siguientes son los comandos básicos para la configuración del *firewall:*

hostname.-asigna un nombre al PIX.

interfase.-asigna el tipo y la capacidad de cada interfase de perímetro.

nameif.-asigna un nombre a cada interfase

ip address.-asigna una dirección ip a la interfaz

security level.-asigna un nivel de seguridad a cada interfaz

speed.-asigna la velocidad de conexión

4.2.1 Comando Hostname

En todos los PIX el nombre por defecto es pixfirewall. En redes de varios PIX es recomendable asignar un nombre a cada PIX. El comando utilizado es hostname.

El nombre asignado al PIX puede tener 16 caracteres alfanuméricos, mayúsculas o minúsculas.

Sintaxis:

```
pixfirewall(config)#hostname frw1
frwl(config)#
```

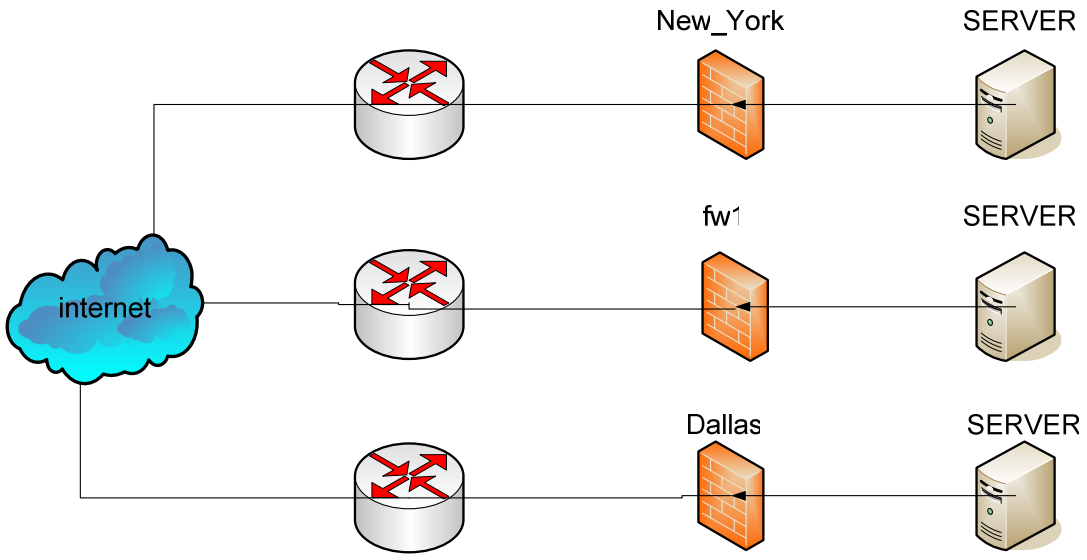


Figura. 4.1 comando hostname

4.2.2 Comando interfase

Este comando identifica a la interfaz y al *slot* de ubicación, con respecto PIX. Las interfase son numeradas como 0/0, 0/1 ,0/2, el primer número representa el *slot* y el segundo a la interfaz.

Después de ingresar este comando en el CLI, el *prompt* cambia a modo de interfaz, siendo en este modo capaz de cambiar nivel de seguridad, nombre de interfaz, dirección ip, velocidad entre otros.

Para una interfaz que a estado sin tráfico, los comandos *nameif, ip address, security level* y *no shutdown* son necesarios, para interfases físicas el estado por defecto es *shutdown*, siendo necesario el comando *no shutdown* para habilitar la interfaz, los niveles de seguridad por defecto pueden ser utilizados o cambiados.

Sintaxis:

```
Pixfirewall(config)#interfase ethernet0
Pixfirewall(config-if)
```

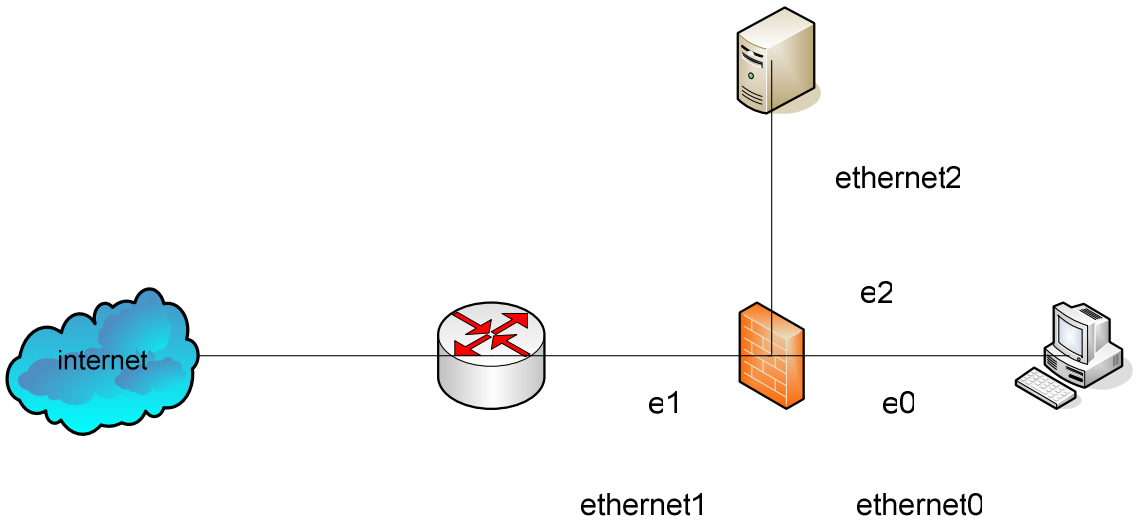


figura 4.2. comando interfase

4.2.3 Comando Nameif

Asigna un nombre a cada interfaz del PIX. El nombre por defecto de las dos interfases del PIX son i*nside* y *outside.*

Sintaxis:

```
Pixfirewall(config)#interfase ethernet0
Pixfirewall(config-if)#nameif outside
```

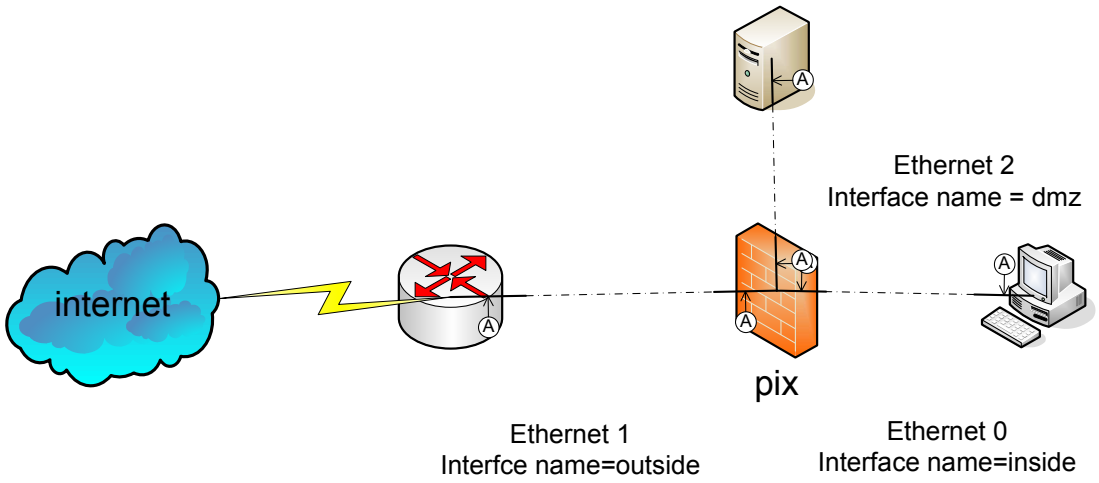


figura 4.3. comando nameif

4.2.4 Comando Ip Address

Cada interfaz del PIX debe ser configurada con una dirección ip. Se usa este comando para dicho propósito. El comando clear ip resetea todas las direcciones ip de las interfases.

sintaxis:

```
Pixfirewall(config)#interfase ethernet0
Pixfirewall(config-if)#nameif outside
Piwfirewall(config-ip)#ip address 192.168.1.1 255.255.255.0
```

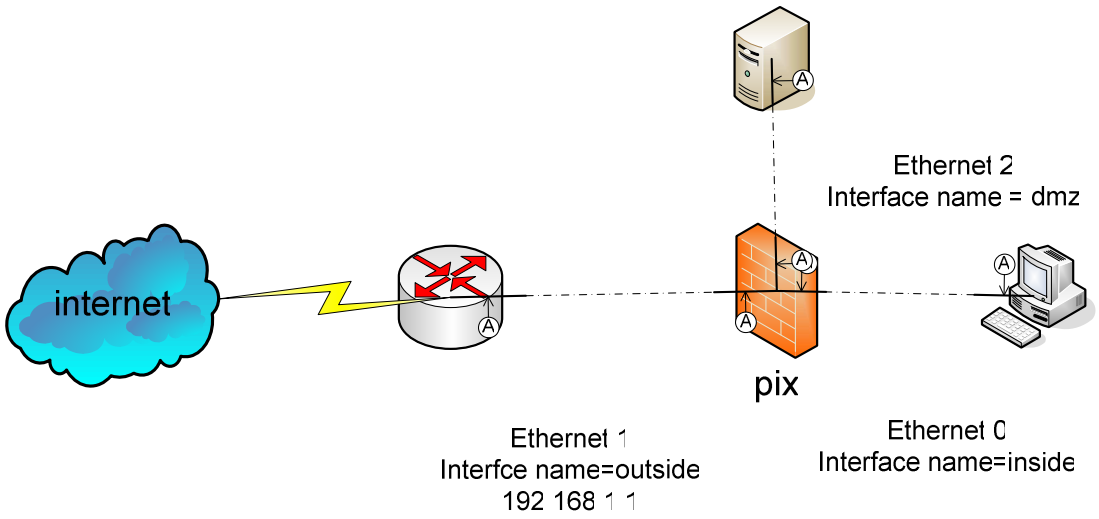


figura 4.4. comando ipaddress

4.2.5 Comando Security Level

Permite especificar el nivel de seguridad de la interfaz, excepto para la interfaz *inside* y *outside*, las cuales tiene asignado el nivel de seguridad 100 y 0 respectivamente.

Cuando una nueva interfaz es asignada, el sistema asigna por defecto el nivel de seguridad 0, por lo que el administrador debe cambiar el nivel de seguridad entre un numero del 1 al 99.

Habitualmente interfases con el mismo nivel de seguridad no pueden comunicarse, si esto es necesario se debe usar el comando *same-security-traffic*.

Si el nivel de seguridad de una interfaz es cambiado, el comando *clear xlate* puede ser usado para limpiar todas las conexiones existentes. Limpiar la tabla de traslaciones desconecta todas las conexiones actuales.

Sintaxis:

```
Pixfirewall(config)#interfase ethernet2
Pixfirewall(config-if)#nameif dmz
Piwfirewall(config-ip)#ip address 192.150.1.1 255.255.255.0
Piwfirewall(config-ip)#security-level 50
```

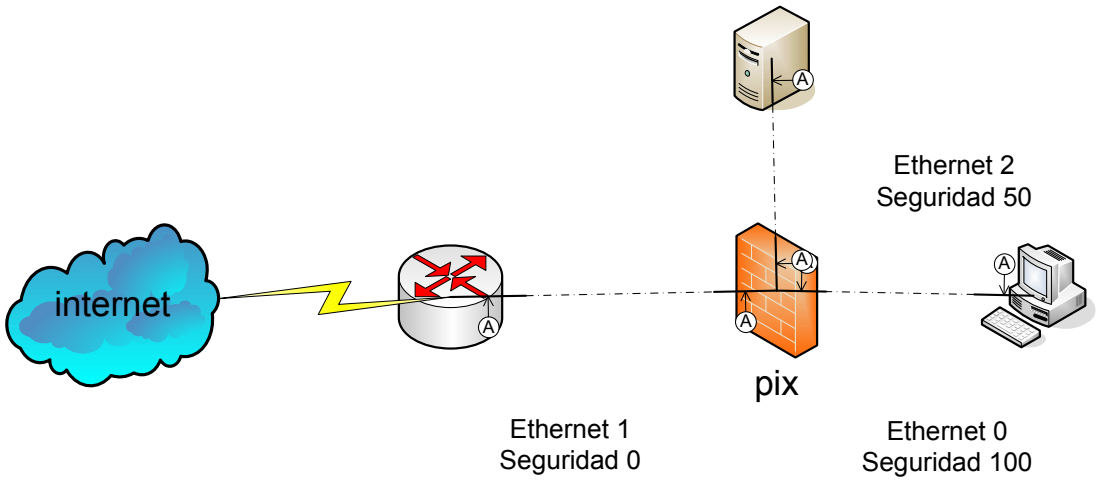


figura 4.5. comando security level

4.2.6 Comando Speed

A través del hardware la velocidad es auto-sensada por defecto, pero es recomendable que la velocidad de la interfase sea especificada.

Para setear la velocidad de una interfaz *fastethernet* o *gigabit ethernet*, use el comando *speed* en modo de interfaz, para restaurar la velocidad por defecto, use la forma no de este comando.

Pixfirewall(config-if)#speed { auto 10 100 1000 nonogotiate}

10	setea la velocidad 10base-T
100	setea la velocidad 100base-T
1000	setea la velocidad 1000bade-T
Auto	autodetesta la velocidad

4.3 NAT “NETWORK ADDRESS TRASLATION”

La conversión de direcciones dinámica se utiliza para convertir un intervalo de direcciones locales a un intervalo de direcciones globales o a una dirección global única.

La conversión de direcciones locales a un grupo direcciones globales se llama Traducción de direcciones de Red (NAT), y la conversión de un grupo de direcciones locales a una dirección única de se llama Traducción de direcciones de Puerto (PAT).

Cuando se utiliza NAT, los *host* locales deberán ser definidos con el comando *nat*, y el *pool* de direcciones deberá ser definido con el comando global.

Un usuario puede especificar hasta 256 *pools* globales de direcciones IP.

La sintaxis de *nat* y *global* es la siguiente:

```
Pixfirewall(config)# nat (inside)1  0.0.0.0  0.0.0.0
Pixfirewall(config)# global (outside)1 192.168.1.10-192.168.1.254 netmask
255.255.255.0
```

Cuando el *host* 10.0.1.10 realiza la primera conexión saliente del PIX, se convertirá en 192.168.1.10.

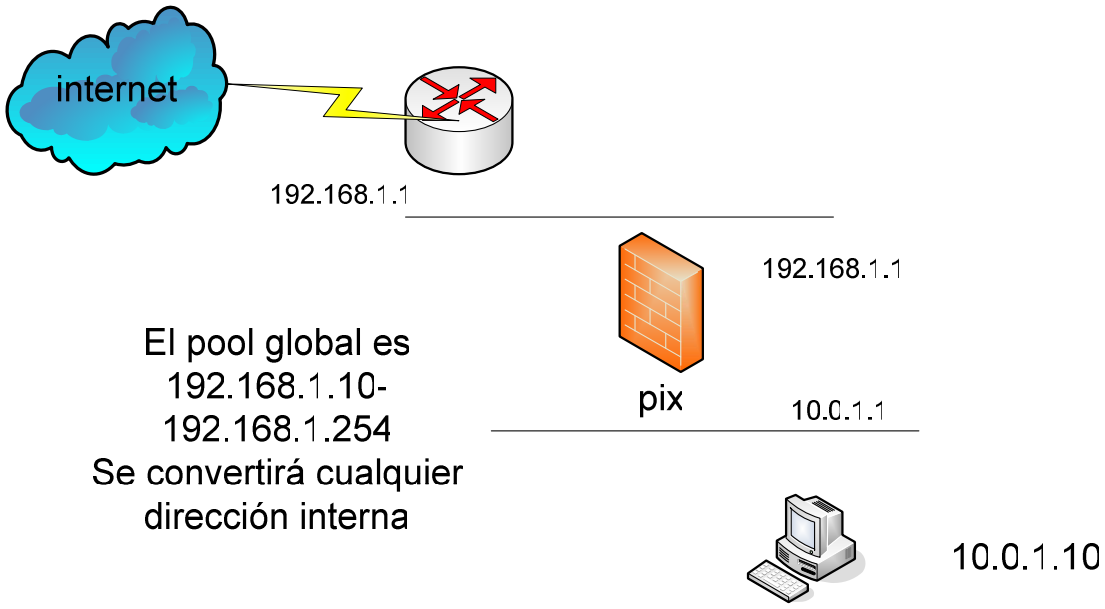


figura 4.6. comando nat y global

En la figura 4.6, el pool de direcciones globales asignado por el comando global va desde 192.168.1.10 a 192.168.1.254, permitiendo que haya hasta 245 direcciones IP individuales, Todas las direcciones locales son convertidas, debido a que se usa 0.0.0.0 en la parte de red y mascara del comando *nat.*

Resulta habitual usar el comando *static* y los comando *nat* y global en una misma configuración, debiendo de tomar muy en cuenta que la dirección IP global del comando *static*, este fuera del rango de direcciones pool.

4.4 PAT"PORT ADDRESS TRASLATION"

Cuando se configura PAT, todas las direcciones locales son convertidas a una dirección IP única global, su configuración es igual a NAT, con la diferencia que en la instrucción global contiene una sola dirección IP.

La sintaxis es la siguiente:

```
Pixfirewall(config)# nat (inside) 1 0.0.0.0  0.0.0.0
Pixfirewall(config)# global (outside) 1 192.168.1.10 netmask 255.255.255.255
```

Al conectarse a Internet, todas las direcciones IP internas son convertidas a una sola dirección IP, 192.168.1.10

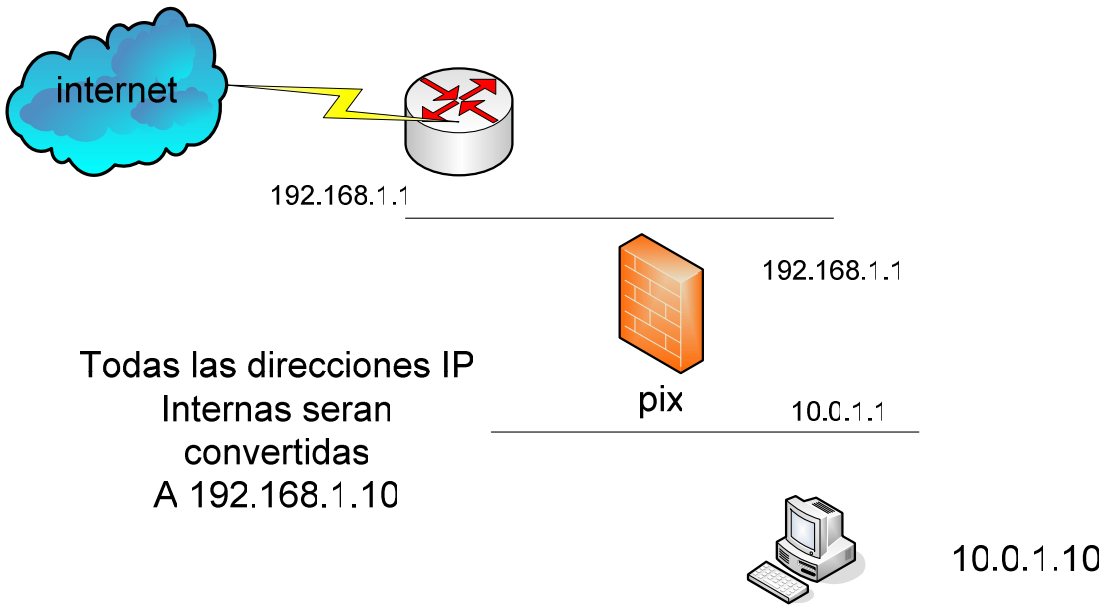


figura 4.7. comando pat y global

Al configurar PAT se debe considerar las siguientes observaciones:

La dirección global configurada con PAT, no puede ser considerada en otro pool de direcciones globales.

PAT permite que múltiples sesiones salientes se origine desde una única dirección IP, y el PIX asigna un número de puerto único a partir de la dirección IP de PAT en cada línea de conversación, siendo esto muy útil cuando el ISP no puede asignar suficientes direcciones IP para conexiones salientes.

PAT no funciona con aplicaciones H323.

Al configurar PAT incrementando un pool de direcciones globales, primero se utilizan las direcciones del pool global y a continuación se toma la conexión saliente de la dirección PAT. Si se libera una dirección del pool global, la conexión siguiente adoptará esa dirección.

PAT funciona con DNS, FTP, HTTP, correo electrónico, TELNET, y *traceroute.*

4.5 CONVERSIÓN ESTÁTICA DE DIRECCIONES

Esta conversión se utiliza cuando hay que convertir un *host* a la misma dirección cada vez que se construye una sesión saliente en el PIX.

Al definir la sintaxis de comandos. La dirección local se define como la dirección asignada a un *host* del interior. La dirección global se define como la dirección a la que se convierte una dirección local cuando se construye una sesión a través del PIX.

Una dirección externa se define como la dirección IP del *host* que se encuentra en el exterior.

En el ejemplo que se ilustra en la Figura 4.8, el paquete de 10.0.0.10 (dirección local) tiene una dirección de origen 192.168.1.101 (dirección global), cuando se construye una sesión a través del PIX.

Mediante el comando static se asigna permanentemente la dirección local a la dirección global.

Sintaxis:

static (nombre_if_interno,nombre_if_externo) ip_global ip_local **netmask** mascar de_red]

Ejemplo:

Pixfirewall(config)# static (inside,outside) 192.168.1.101 10.0.0.10 netmask 255.255.255.255

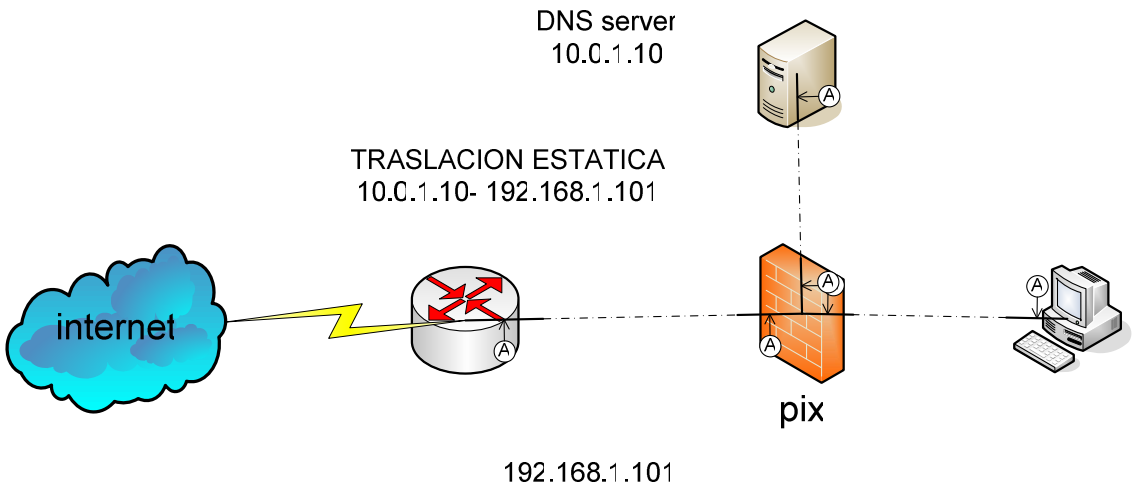


figura 4.8. comando static

4.6 ARMADO DE RUTEO

El comando *route* se utiliza para asignar rutas estáticas a una interfase. Para ingresar una ruta por defecto, ingresa la dirección ip 0.0.0.0 y la máscara 0.0.0.0

En el siguiente ejemplo, se configura una ruta por defecto; el PIX enviara todos los paquetes que no tengan ruta definida por la interfaz 192.168.0.1

Las rutas estáticas con creadas para dar acceso a redes especificas localmente conectadas. En el ejemplo siguiente el PIX envía todos los datos de la red 10.0.1.0

255.255.255.0 hacia fuera de la interfase interna, la misma que tiene como dirección 10.0.0.102

Sintaxis:

route if_name ip_address netmask geteway ip [metric]

if_name.- describe el nombre de la interfaz interna o externa.
ip_address.- describe la direccion ip de la interfaz interna o externa. Use 0.0.0.0 para una ruta por defecto, 0.0.0.0 puede ser abreviado por 0.
netmask.-describe la mascara que será aplicada a la direccion ip.
gateway_ipespecifica el siguiente salto del entutamiento.
metric.- especifica el número de saltos hacia el gateway_ip. No es obligatorio.

Ejemplo:

pixfirewall(config)# route outside 0.0.0.0 0.0.0.0 192.168.0.1 1
pixfirewall(config)# route inside 10.0.1.0 255.255.255.0 10.0.1.102

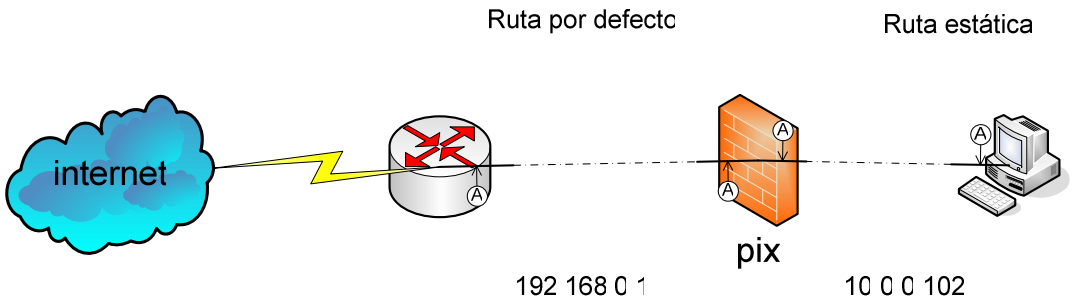


figura 4.9.comando route

4.7 REGLAS DE FILTRADO O LISTAS DE ACCESO

Los comandos *nat* y *global* se usan para definir el acceso desde el interior al exterior.

Para configurar el acceso desde el exterior al interior, se lo hace con el comando *access-list.*

Un ejemplo de cuando usar el comando *access-list* tiene lugar cuando se prueba la conectividad de un PIX con mensajes ICMP. Para permitir que haya una solicitud de eco desde el exterior a través del PIX, es precios configurar un lista de acceso. Además el usuario del exterior deberá poder usar una dirección IP de destino, que se lo puede hacer por medio del comando *static*.

Después de crear una asignación estática entre una dirección IP local y una dirección IP global por medio del comando *static*, la conexión desde el interfaz externa hasta la interfaz interna seguirá estando bloqueada por el ASA. El comando *access-list*, se usa para permitir el flujo de la parte externa hacia la interna.

El comando *access-list* permite o deniega conexiones desde el exterior para acceder a TCP, o UDP y otros servicios de protocolo de los *hosts*, de dentro de la red.

Este comando puede ser general o especifico, por ejemplo es posible permitir que *http* acceda a un *host* específico.

A continuación se describe los parámetros del comando *access-list*, cuya sintaxis es la siguiente:

Sintaxis:

Access-list permit | deny protocolo *ip_global mascara_global* [puerto operador [puerto]]

ip_externa mascara_externa [puerto operador [puerto]]

Parámetro del comando	**Descripción**
permit	permite el acceso si coinciden las condiciones
deny	deniega el acceso si coinciden las condiciones
protocolo	especifica el protocolo de transporte de la conexión. Los Valores posibles son icmp, tcp, udp o un entero que este en el intervalo de 0 a 255.

ip_global una dirección Ip global definida anteriormente por un comando global o un comando static. Puede usar any su ip_global y mascara_global son 0.0.0.0 0.0.0.0. La opción any aplica los parámetros permit o deny a las direcciones globales.

Si ip_global es un host, podrá omitir mascara_global especificando el comando host delante de ip_global. Por ejemplo:

Access-list permit tcp host 209.165.200.3 eq ftp any

En este ejemplo permite a cualquier host externo acceder a la dirección global 209.165.200.3 para FTP

global_mask mascara de red de global_ip. global_mask es un decimal con puntos de 32 bits, como 255.255.255.255.Utilice ceros para indicar las posiciones de bit que se vaya a omitir.Utilice subneteo si es necesario.Si utiliza 0 como ip_global, utilice 0 para la mascara_global.

ip_externa una dirección Ip externa (host o red) que puede acceder a ip_global.Puede especificar 0.0.0.0 o 0 para cualquier host.

mascara_externa mascara de red de ip_externa, es un decimal con puntos de 32 bits, como 255.255.255.255.Utilice ceros para indicar las posiciones de bit que se vaya a omitir.Utilice subneteo si es necesario. Si utiliza 0 para la ip_externa, utilice 0 para la mascara_externa; de otro modo introduzca la mascara_externa para la ip_externa

operador. Un operando de comparación que le permite especificar un puerto o intervalo de puertos.

Utilícelo sin especificar un operador para indicar todos los puertos. Por ejemplo:

Access-list permit tcp any any

Utilice eq y un puerto para permitir o negar el acceso a se puerto.Por ejemplo utilice eq www para permitir o negar el acceso exclusico a internet:

Access-list deny tcp host 191.167.2.2 eq www 209.165.201.1

Utilice It y un Puerto para permitir o denegar el acceso a todos los puertos menos al Puerto que especifique. Por ejemplo utilice It 2025 para permitir o denegar el acceso a los puertos bien conocidos (1 al 1024):

Access-list permit tcp host 192.168.1.1 It 1025 any

Utilice gt y un Puerto para permitir o denegar erl acceso a todos los puertos que sean mayores al Puerto que especifica. Por ejemplo utilice gt 42 para permitir o denegar los puertos 43 a 65535:

Access-list deny tcp 192.168.1.1 gt 42 host 203.36.2.56

En el siguiente ejemplo, primero se utiliza el comando *static* para convertir de forma estática 10.0.1.10 a 192.168.1.101 y el comando *access-list* solo permitirá que http, sea el que acceda al *host* 10.0.1.10 (convertido a 192.168.1.101)

```
Pixfirewall(config)#static (inside,outside) 192.168.1.101 10.0.1.10 netmask
255.255.255.255
Pixfirewall(config)#access-list 1 permit tcp any host 192.168.1.101 eq www
```

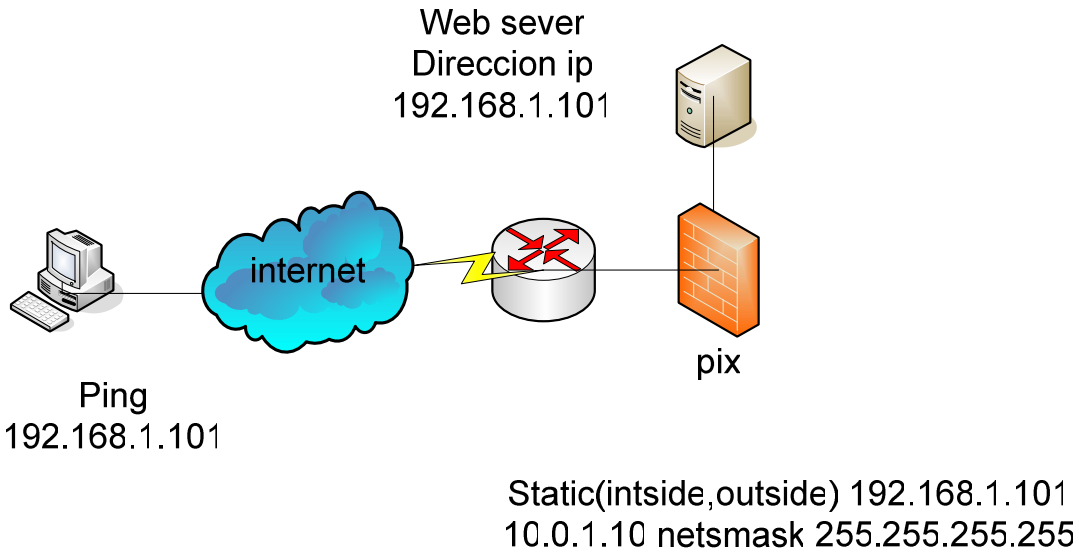


figura 4.10. comando static y acces-list

4.8 EXAMINAR EL ESTADO DEL PIX

El comando show permite al administrador ver la información del funcionamiento del PIX, tenemos algunas opciones de este comando

show memory.- despliega el máximo de memoria física usado, y espacio de memoria libre, dejado por el sistema operativo.

show version.- nos indica la versión del sistema operativo, procesador, memoria flash, numero de serie, identificación de la *bios* y valor de la *key* de activación.

Ejemplo:

```
pixfirewall(config)# show version
Cisco PIX  FIREWALL Version 7.0
Hardware : PIX-515, 64 MB RAM, CPU Pentium 200 MHz
Flash i29b634 @ 0x200 , 8mb
```

show ip address.- es usado par ver la dirección ip con la que a sido asignada la interfase.

show interfase.- revela la información de red de la interfase

show nameif.- no permite visualizar las interfases nombradas y su respectivo nivel de seguridad, primero nos indica las interfases *inside* y *outside*, con su respectivo nivel de seguridad 100 y 0 respectivamente.

Ejemplo:

```
pixfirewall(config)# show nameif
Interfase          Name          Security
Ethernet0          outside       0
Ethernet1          inside        100
Ethernet2          dmz           80
```

show run nat.-este comando nos despliega un *host* o rango de *host* que son transformados de dirección ip a salir a través del PIX. En el siguiente ejemplo todos los *host* de la red 10.0.0.0 serán transformados cuando atraviesen el PIX.

Ejemplo:

```
pixfirewall(config)# show run nat
nat(inside) 1 10.0.0.0          255.255.255.0
```

show run global.- este comando despliega el pool de direcciones con que se configuró al PIX. El pool es configurado en la interfase *outside.*

Ejemplo:

```
pixfirewall(config)# show run global
global (outside) 1 192.168.0.20-192.168.0.254 netmask 255.255.255.0
```

show xlate.- este comando nos indica el *slot* de traslación, es decir la tabla de direcciones internas ,con su respectiva dirección externa.

Ejemplo:

```
pixfirewall(config)# show xlate
1 in use,        1 most used
Global 192.168.0.20  Local 10.0.0.11
```

clock set.-este comando setea el reloj en el PIX, se ingresa la hora, minutos, segundos, opcionalmente día, mes y año.

Cuando el PIX genera mensajes *syslog* sobre eventos de la red hacia un servidor *syslog*, el comando *logging timestamp* es utilizado para agregar a estos mensajes, la fecha y hora del evento.

Se puede ver la hora seteada en el PIX con la ayuda del comando *show clock.*

Sintaxis:

clock set hh:mm:ss {month day ! day month} year

ntp.- El comando *ntp* Server sincroniza al PIX con un timeserver; además se puede configurar en el PIX autenticación antes de sincronizarse con el timeserver. El comando show run ntp se utiliza para obtener la configuración NTP

Sintaxis:

ntp server ip address [key number] source if_name [prefer]

Ejemplo:

```
pixfirewall(config)# show ntp authenticacion-key 1234 md5 cisco123
pixfirewall(config)#ntp trusted-key 1234
pixfirewall(config)#ntp server 10.0.0.12 key 1234 source inside prefer
pixfirewall(config)#ntp authenticate
```

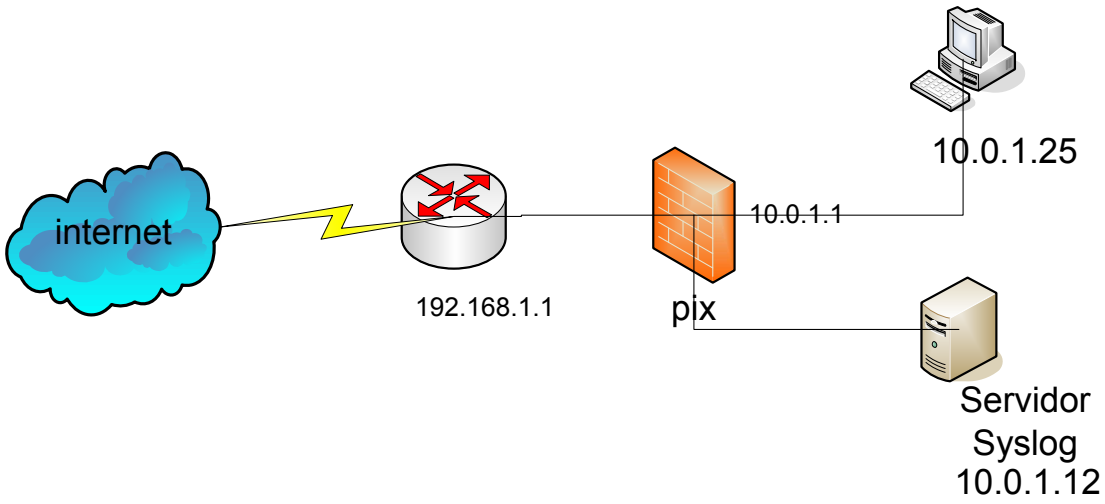


figura 4.11. comando ntp

Comando *syslog*.-el PIX genera mensajes de *syslog* para diferentes eventos del sistema, por ejemplo alertas, agotamientos de recursos entre otros.

Mensajes de *syslog* pueden visualizados a través de la consola o enviados a un servidor *syslo*g, además en el caso de que el servidor *syslog* quede fuera de servicio, el PIX almacena hasta 512 megabytes en su memoria, una vez sobrepasada esta capacidad se sobrescribe desde la primera línea del archivo.

Los mensajes *syslog* pueden ser visualizados de las siguientes formas:

Consola.-al producirse un mensaje *syslog* este es enviado a la consola del PIX
Almacenados.-son guardados en el PIX y se los puede visualizar con el comando show logging.
Monitor.- permite visualizar los mensajes *syslog* a través de sesiones telnet.
Host.-especifica un servidor que recivira los mensajes enviados desde el PIX.
Snmp.-se envía los mensajes *sylog* como SNMP *trap notifications* hacia un servidor snmp.

Los mensajes *syslog* tienen diferentes niveles, estos son:
0-emergencia
1-alerta
2-critica
3-error
4-*warnings*

5-notificación
6-información
7-debugging

En el siguiente ejemplo se configura un servidor syslog de dirección ip 10.0.1.12 Los mensajes enviados al servidor serán de notificación y warnings. Cada mensaje es time stamped e identificado con devide-id

```
pixfirewall(config)# logging host inside 10.0.1.1
pixfirewall(config)#logging trap warnings
pixfirewall(config)#logging timestamp
pixfirewall(config)# logging devie-id pix6
pixfirewall(config)# logging on
```

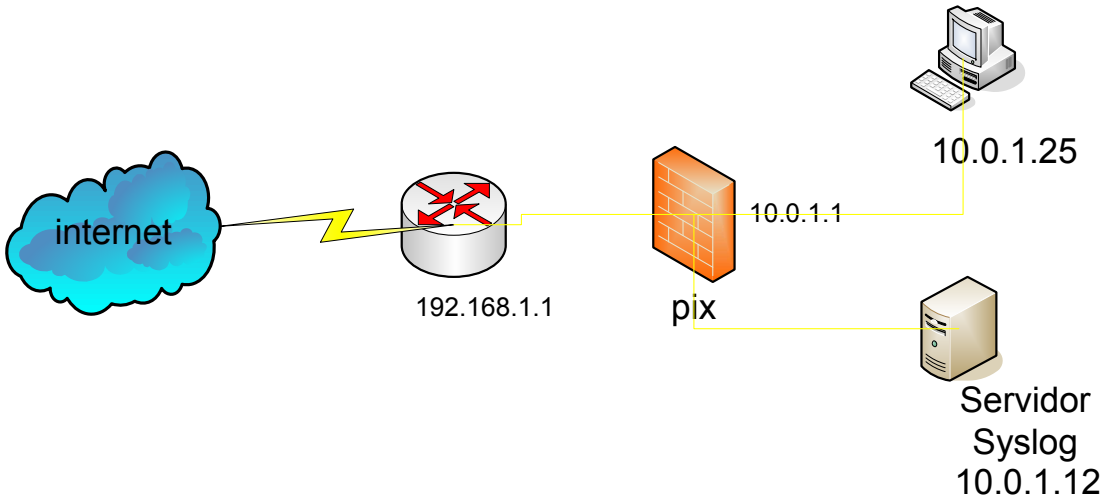


figura 4.12. servidor syslog

Usa el comando *show logging* para ver la configuración y mensajes *syslog* almacenados. Para limpiar los mensajes *syslog* almacenados nos ayuda el comando *clear logging.*

4.9 CONFIGURACIÓN DE MÚLTIPLES INTERFASES

El PIX soporta un máximo de ocho interfases físicas adicionales; a continuación se da el ejemplo de la configuración de tres interfases, y los lineamientos a seguir para el correcto desempeño de NAT:

La interfase *outside* no puede ser renombrada o darle un diferente nivel de seguridad que no sea 100.

Una interfase es siempre *outside* con respecto a otra que tenga un nivel de seguridad superior o más alto.

No puede haber tráfico de paquetes entre dos interfases que tengan el mismo nivel de seguridad.

Usa una ruta por defecto en la interfase *outside*, esto se lo hace con el comando *route*.

Usa el comando *nat* para permitir a los usuarios de la interfase *inside* realizar conexiones salientes.

Para permitir acceso a servidores sobre redes protegidas desde una interfase que tiene un nivel de seguridad bajo, se usa los comandos *static* y *acces-list*.

En la figura 4.11 los *hosts* de la red interna pueden acceder hacia la red externa, la dirección original 10.0.0.0/24 es asignado un pool de direcciones 192.168.0.20-254. Cuando accede un *host* de la parte *inside* hacia la *dmz*, el pool asignado es 172.16.0.20-254. Para acceder al servidor de la *dmz*, desde la parte *outside* se hará con la dirección 192.168.0.11.

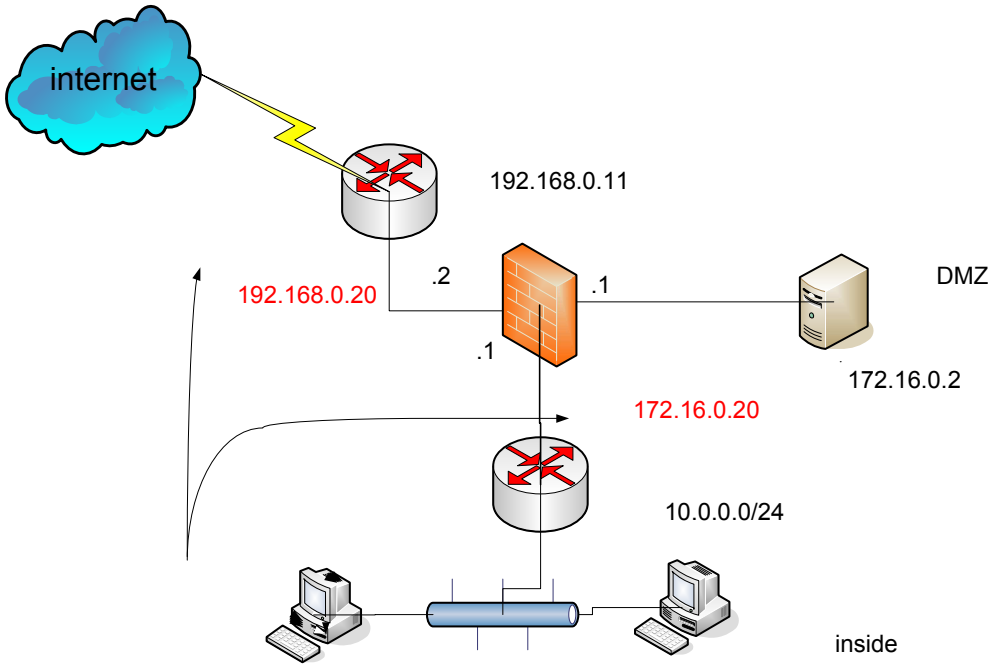


figura 4.13. múltiples interfases

```
pixfirewall(config)# nameif ethernet0 outside sec0
pixfirewall(config)# nameif ethernet1 inside sec100
pixfirewall(config)# nameif ethernet2 dmz sec50
pixfirewall(config)#ip address outside 192.168.0.2 255.255.255.0
pixfirewall(config)# ip address inside 10.0.0.1 255.255.255.0
pixfirewall(config)# ip address dmz 172.16.0.1 255.255.255.0
pixfirewall(config)# nat (inside) 1 10.0.0.0 255.255.255.0
pixfirewall(config)# global (outside)1 192.168.0.20-192.168.0.254 netmask
255.255.255.0
pixfirewall(config)# global (dmz)1 172.16.0.20-172.16.0.254 netmask
255.255.255.0
pixfirewall(config)#static (dmz,outside) 192.168.0.11 172.16.0.2
```

CAPITULO 5

IMPLEMENTACION DE MEJORAS DE POLITICAS DE SEGURIDAD EN LA RED

Las recomendaciones para mejorar la seguridad de la red son: segmentar la red, redundancia a nivel de los *swith,* actualización del servidor DHCP.

A nivel de *firewall* se presenta los conceptos de autenticación, autorización y administración de cuentas (AAA).

Se explica los dos protocolos mayormente utilizados en el proceso AAA, que son *Tacacs+* y *Radius*; las debilidades y fortalezas que se presentan entre ellos.

Hablamos además del *Cisco Secure Access Control Server* (ACS), que es un software que se instala en Windows 2003 Server, que realiza la función AAA., explicaremos el manejo de este software. Además la configuración del PIX para que pueda interactuar con el *Cisco Secure ACS.*

En la parte final de este capítulo hablaremos de la configuración de filtros en el PIX y el beneficio que estos nos brindan para el desempeño de la red.

5.1 TOPOLOGIA LOGICA DE LA RED

La topología de la red se centra en el *Firewall* Cisco PIX, como protección de frontera a los ataques, como seguridad de la red interna además el ISA Server que cuenta con numerosos listas de acceso para que se garantice un buen uso de Internet.

En la DMZ los servidores WEB, FTP y Dns, durante el monitoreo no evidenciaron fallos o interrupción del servicio, por lo que no se recomienda cambio alguna en esta zona de la red.

Durante el periodo de matrículas se recomienda aumentar el ancho de banda asignado al servidor WEB, que se de 4 Mbps a 5Mbps.

En las red interna se evidencia algunas deficiencias, las mismas que deberán ser superadas para mejorar el desempeño de la red, en el desarrollo de este capitulo sugerimos algunas pautas.

5.2 SEGMENTACION DE LA RED

Como concepto de fragmentación de red es, permitir agrupar usuarios en un solo dominio de *broadcast* con independencia de la ubicación física en la red y que tienen un trabajo en común.

El rendimiento de una red se eleva notablemente, al no propagarse *broadcast* de un segmento a otro, y a la vez aumenta los márgenes de seguridad.

Del monitoreo que se realizo en la red de la ESPE, se encontró que todos los usuarios de la red se encuentran en una sola *Vlan*, hecho que brinda poco seguridad y gran trafico de *broadcast.*

El criterio para segmentar la red es conforme a la red organizacional de la ESPE, que es el siguiente:

- ✓ Rectorado
- ✓ Vicerrectorado Académico
- ✓ Vicerrectorado de Investigación y Vinculación a la Colectividad
- ✓ Gerencia Administrativa Financiera

Departamentos:

- ✓ Mecánica
- ✓ Electrónica
- ✓ Biotecnología
- ✓ Civil
- ✓ Educación Física

- ✓ Sistemas
- ✓ Geográfica
- ✓ Ciencia de la Educación

Los departamentos de menor número son Vicerrectorado de la Investigación y el Rectorado.

5.3 DIRECCIONAMIENTO IP DE LA RED

Por medio de monitoreo, se detecto que esporádicamente hay duplicación de direcciones IP en la red, incluso las direcciones de los servidores, lo que ocasionó la caída de los servicios informáticos, por tanto se aconseja la actualización de servidor DHCP.

En el direccionamiento ip, se recomienda implementar las demás vlan que se tiene configurado en el servidor DHCP, el mismo que esta operando en la red interna de la ESPE. Con las siguientes modificaciones:

	Red	mascara	
Administración	10.1.100.0	255.255.252.0	Vlan 1
Usuarios	10.1.1.0	255.255.255.0	Vlan 7
	10.1.2.0	255.255.255.0	Vlan 8
	10.1.3.0	255.255.255.0	Vlan 9
	10.1.4.0	255.255.255.0	Vlan 10
	10.1.5.0	255.255.255.0	Vlan 11
	10.1.6.0	255.255.255.0	Vlan 12
	10.1.7.0	255.255.255.0	Vlan 13
	10.1.8.0	255.255.255.0	Vlan 14
	10.1.9.0	255.255.255.0	Vlan 15
	10.1.10.0	255.255.255.0	Vlan 16
	10.1.11.0	255.255.255.0	Vlan 17
	10.1.12.0	255.255.255.0	Vlan 18
	10.1.13.0	255.255.255.0	Vlan 19
	10.1.14.0	255.255.255.0	Vlan 20
	10.1.15.0	255.255.255.0	Vlan 21

Telefonía IP	10.1.24.0	255.255.252.0	Vlan 50

VLAN 7	Vicerrectorado Académico
VLAN 8	Gerencia Administrativa
VLAN 9	Vicerrectorado de la Investigación
VLAN 10	Rectorado
VLAN 11	Mecánica
VLAN 12	Electrónica
VLAN 13	Biotecnología
VLAN 14	Civil
VLAN 15	Educación Física
VLAN 16	Sistemas
VLAN 17	Geográfica
VLAN 18	Ciencias de la Educación

5.4 CONFIGURACION DE EQUIPOS

5.4.1 Configuración de Switch

En la red de *switch,* se evidencia presencia de lazos o bucles en la red, para evitarlos se recomienda la configuración de *Spanning Tree Protocol*,

El STP (*Spanning Tree Protocol*) es un estándar utilizado en la administración de redes, basado en el algoritmo de Árbol Abarcador, para describir como los *switch* pueden comunicarse para evitar bucles en la red.

El protocolo STP automatiza la administración de la topología de la red con enlaces redundantes, la función principal del protocolo *spanning-tree* es permitir rutas conmutadas/puenteadas duplicadas sin considerar los efectos de latencia de los *loops* en la red.

Al crear redes tolerantes a las fallas, una ruta libre de *loop* debe existir entre todos los nodos de la red. El algoritmo de *spanning tree* se utiliza para calcular una ruta libre de *loops*. Las tramas del *spanning tree,* denominadas unidades de datos del protocolo puente

(BPDU), son enviadas y recibidas por todos los *switches* de la red a intervalos regulares y se utilizan para determinar la topología del *spanning tree*.

El Protocolo *Spanning Tree* que trabaja a nivel de MAC, primeramente construye un árbol de la topología de la red, comenzando desde la raíz (nodo). Uno de los dispositivos STP se convierte en la raíz después de haber ganado la selección, para ello cada dispositivo STP (*router, switch*, u otros) comienza a tratar, desde el momento en que se enciende, de convertirse en la raíz del árbol STP mediante el envío de paquetes de datos específicos denominados *BPDU (Bridge Protocol Data Unit*) a través de todos sus puertos. La dirección del receptor del paquete BPDU es una dirección de un grupo *multicast*, esto permite al paquete BPDU atravesar dispositivos no inteligentes como *hubs* y *switches* no STP.

Después de recibir el paquete *BPDU* desde otro dispositivo, el "puente" (puede ser un conmutador, en este caso se referirán simplemente a puente) compara los parámetros recibidos con los propios y, dependiendo del resultado decide seguir o no intentando ser el nodo raíz. Una vez terminadas las elecciones el dispositivo con el Identificador de Puente con un valor mas bajo será designado raíz. El Identificador de Puente es una combinación entre la dirección *MAC* del Puente y una prioridad del Puente predefinida.

Si se identifica un solo dispositivo STP en la red, éste será la raíz.

La raíz Designada *(Designate Root Bridge*) no tiene ninguna responsabilidad adicional, tan solo es el punto de inicio desde el cual se comenzará a construir el árbol de la topología de la red. Para todos los demás Puentes en una red, STP define el Puerto raíz como el puerto más cercano al Puente raíz. Los demás puentes se diferencian con su Identificador (combinación de la MAC y la prioridad definida para ese puerto).

El Coste de la Ruta raíz (*Root Path Cost)* es también un valor significativo para las elecciones STP, comienza siendo una suma de los costes de las rutas: del puerto raíz del Puente dado y todos los costes de las rutas a los puertos raíz de los demás Puentes en la ruta hacia el Puente raíz.

En adicción al Puente raíz principal STP define una entidad lógica denominada 'Puente Designado. Este cargo también está sujeto a elección. De manera similar, STP define por cada segmento de red el Puerto raíz Designado (que es el que sirve en cada segmento de red) y su correspondiente Coste de Ruta.

Después de que las elecciones han terminado, la red entra en la fase estable. Este estado esta caracterizado por las siguientes condiciones:

Solo hay un dispositivo anunciando ser La raíz, y este informa a todos los demás puentes periódicamente de que él es la raíz del árbol. El Puente raíz envía periódicamente paquetes BPDU a través de todos sus puertos. El intervalo de envío se denomina *'Hello Time'*.

En cada segmento LAN existe un Puerto Designado, y todo el trafico hacia el Puente raíz se realiza a través de el. Comparados con otros Puentes, el es el que tiene el Coste de Ruta menor hacia el Puerto raíz, pero si los valores son iguales, el puerto con el Identificador de Puerto mas bajo es el asignado.

BPDU son recibidos y enviados por la unidad compatible con STP de cada puerto, incluso los puertos que están deshabilitados por el propio STP. Excepcionalmente, las *BPDU* no operan en puertos deshabilitados por el administrador.

Cada Puente reenvía tramas solo entre Puertos raíz y Puertos Designados para los segmentos correspondientes. Todos los demás puertos son bloqueados. Como sigue a esto ultimo, STP administra la topología cambiando el estado de los puertos según la siguiente lista:

- ✓ Bloqueado: El puerto esta bloqueado (se desechan las tramas de usuario), pero se aceptan los *BPDU*.

- ✓ En escucha: Primer escenario antes del reenvío. Las tramas STP (*BPDU*) son aceptadas, pero las tramas de usuario no son procesadas. No se aprenden direcciones, ya que esto podría introducir datos erróneos en las tablas de conmutación en este momento.

- ✓ Aprendiendo: Segundo escenario de preparación para el estado de reenvío. Las *BDPU* son procesadas por completo, pero las tramas de usuario solo se usan para construir las tablas de conmutación y no son reenviadas.

- ✓ Reenviando: Todas las tramas son procesadas.

En el momento de la reconfiguración de la topología de la red, todos los puertos de los Puentes están en uno de estos tres estados, Bloqueados, A la escucha o Aprendiendo, las tramas de usuario no son entregadas y la red trabaja solo para si misma, no para los usuarios.

En el estado estable, todos los Puentes esperan la llegada periódica de paquetes BPDU *Hello* desde el Puente raíz. Si en el periodo de tiempo definido por el parámetros *Max Age* Time no llega ningún paquete BPDU *Hello*, el Puente decide si el Puente raíz esta desconectado o si el enlace se ha roto. En cualquier caso el Puente inicia la reconfiguración de la topología de red. Definiendo los correspondientes parámetros es posible regular como de rápido los Puentes pueden encontrar los cambios de topología y habilitar los enlaces de reserva.

Los estados de protocolo del *spanning-tree* son los siguientes:

- ✓ Bloquear: Ninguna trama enviada, se escuchan BPDU
- ✓ Escuchar: Ninguna trama enviada, escuchar tramas.
- ✓ Aprender: Ninguna trama se envía, aprender direcciones.
- ✓ Enviar: Tramas enviadas, aprender direcciones.
- ✓ Desactivado: Ninguna trama enviada, no se escuchan BPDU

El estado para cada VLAN es establecido inicialmente por la configuración y luego modificado por el proceso de protocolo de *spanning-tree*. Se puede determinar el estado, costo y prioridad de los puertos y las VLAN utilizando el comando show *spanning-tree* Después de que se determina el estado Puerto a VLAN, el Protocolo de *spanning-tree* determina si el puerto envía o bloquea las tramas. Los puertos se pueden configurar para entrar directamente en el modo de envío del protocolo de *spanning-tree* cuando se realiza una conexión, en lugar de seguir la secuencia habitual de bloqueo, aprendizaje y luego envío. La capacidad para pasar rápidamente del modo Bloquear al modo Enviar en lugar de

atravesar los estados de puerto de transición resulta muy útil en situaciones donde se requiere el acceso inmediato a un servidor.

5.5 FIREWALL

La autenticación determina la identidad de un usuario y verifica la información, una vez autenticado el usuario, se le niega o concede ciertos servicios de red, en otras palabras lo que se le permite al usuario realizar, esto es la autorización. Finalmente cuando un usuario ha iniciado una sesión y está accediendo a un servicio, podría conservarse un registro de lo que ese usuario esta haciendo. La administración de cuentas o *accounting* realiza esta acción.

El PIX utiliza la autenticación, autorización y administración de cuentas (AAA), para identificar la identidad del usuario. Lo que puede o no puede realizar y llevar un registro de las acciones hechas.

Los controles de acceso básico del PIX están basados en direcciones IP y puertos, lo que no nos proporciona ningún mecanismo para identificar usuarios individualmente y controlar el flujo de tráfico en base a este usuario.

Al utilizar AAA en el PIX, suele procesarle de la siguiente forma:

- ✓ El cliente solicita el acceso, el PIX como *gateway* entre el cliente y el dispositivo en el que reside el servicio, requiere que el cliente reenvíe el usuario y contraseña.

- ✓ El PIX recibe esta información y la envía al servidor AAA, que permite o deniega. El servidor puede mantener una base de datos de los usuarios y contraseñas.

La existencia de un servidor AAA aparte, reducirá la carga en el CPU del PIX y simplificará la configuración y la administración del PIX.

5.5.1 Tecnologías De Autenticación

5.5.1. *Password* Estáticos

Este es método que menos seguridad nos brinda a la red y consiste en la utilización de usuario y contraseña para dar acceso a un cliente.

Este método es susceptible a varios tipos de ataque como son *playback*, contraseña *cracking* , fuerza bruta.

Cuando se utiliza este tipo de autenticación se recomienda, cada cierto periodo de tiempo cambiar los usuarios y contraseña.

5.5.1. One Time Password

OTP fue liberado por *Bellcore* y definido en el IETF RFC 1760, en este sistema la contraseña es enviado en texto claro a través de la red, pero es utilizada una sola oportunidad.

El esquema de generación de contraseña por una sola vez esta basado en los algoritmos de encriptación MD4 y MD5 desarrollado por Ron Rivest.

Este sistema tiene 3 componentes:

- ✓ Cliente
- ✓ *Host*
- ✓ *Password* Calculador

El cliente es el responsable de proveer el *password* y el servidor responde con un número secuencial y una semilla, como se indica en la siguiente figura:

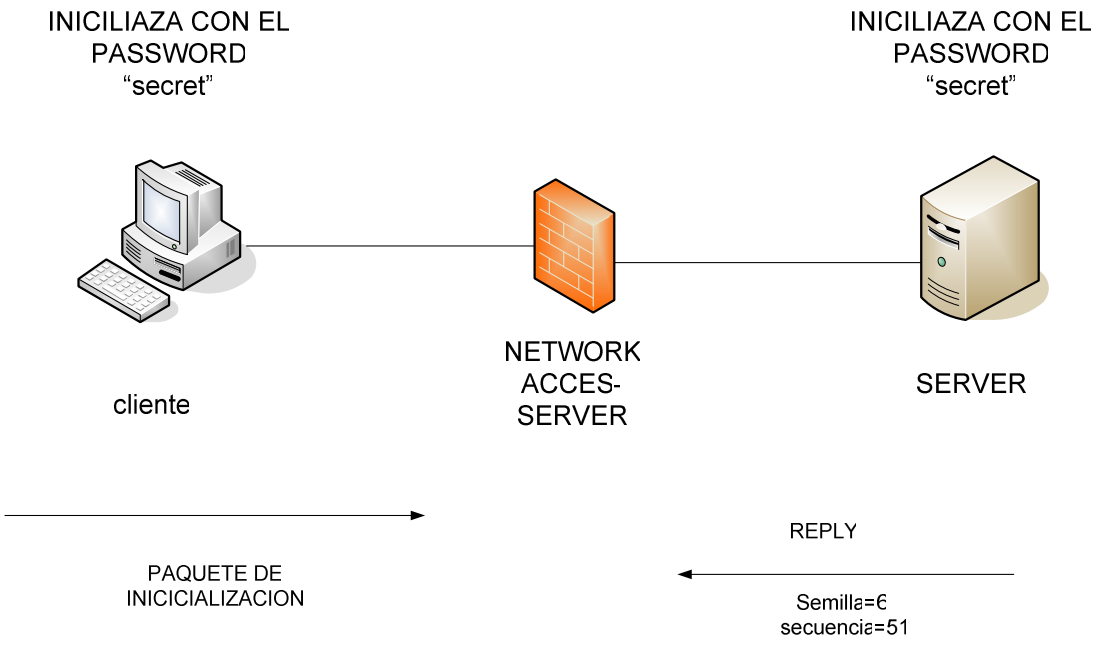


figura. 5.1. one time password fase 1

En el siguiente paso el cliente calcula la contraseña por una sola vez, dicho proceso es de tres pasos:

Paso preparatorio
Paso de generación
Función de salida

En el paso preparatorio, en el cliente entra una frase contraseña secreta, a esta frase se le encadena con la semilla recibida desde el servidor en texto transparente; a continuación en el paso de generación se aplica la función *hash* segura múltiples veces, mientras se produce un bloque de 64 bits para la función de salida, finalmente la función de salida toma la contraseña y con la función *hash* aplicada múltiples veces, se despliega el bloque de 64 bits en forma de ventana leíble y envía la contraseña de uso único donde pueda verificarse, en otras palabras hacia el servidor.

En la figura 5.2 nos detallan estos procesos:

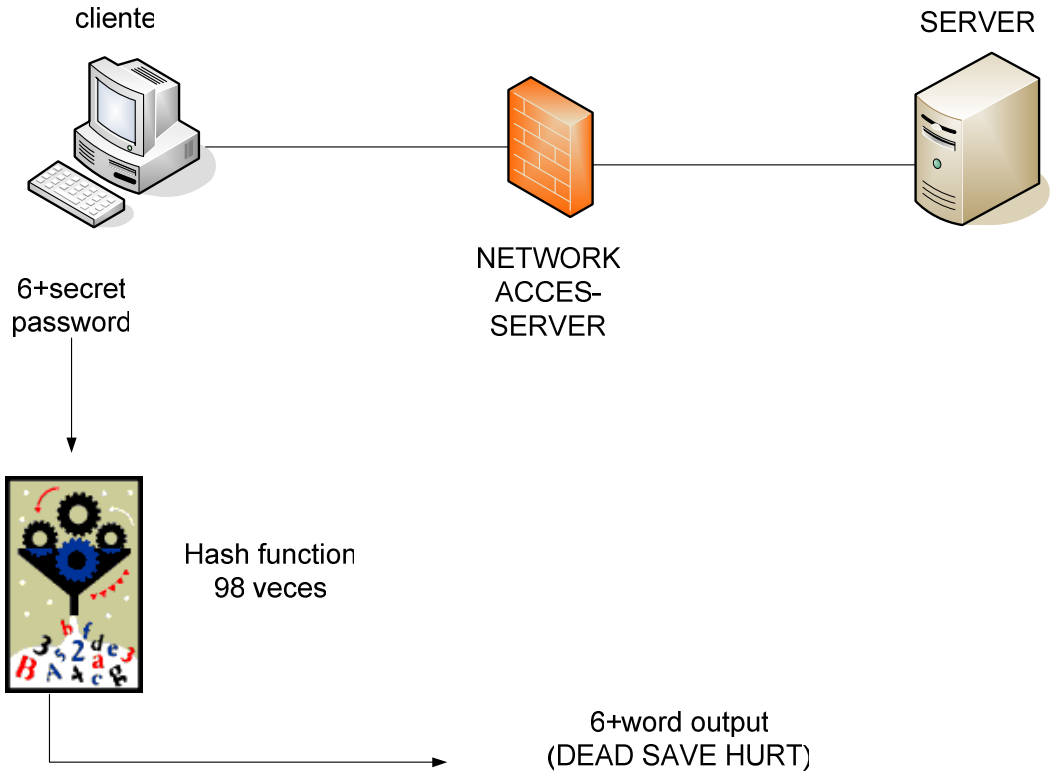


figura. 5.2. one time password fase 2

Después de realizados estos pasos el *host* o servidor tiene que computar la contraseña para uso de solo una vez.

El servidor contiene un archivo, donde se encuentran el *password* único inicial para cada cliente, extraída del último *login* exitoso. Este al recibir el *password*, le aplica la función *hash* segura. Si el resultado empareja la contraseña de uso único anteriormente guardada, la autenticación es exitosa, finalmente esta contraseña de uso único se guarda para usarla el en próximo intento de acceso.

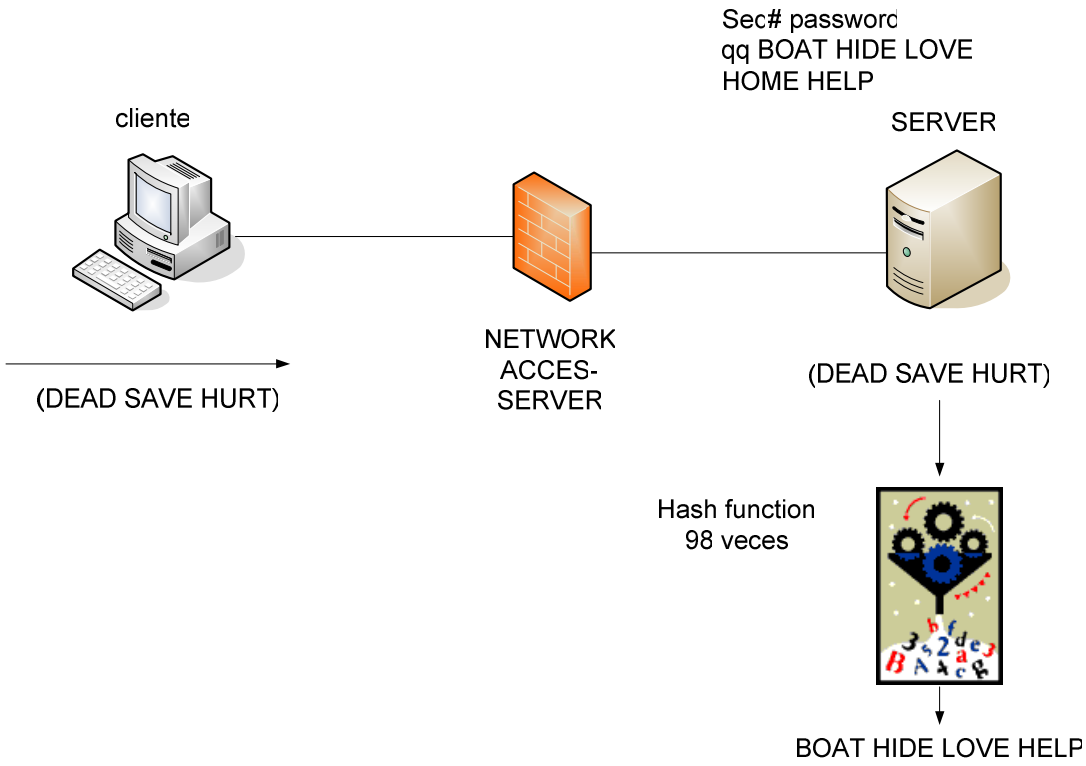


figura. 5.3. one time password fase 3

La función *hash* es ejecutada por el cliente disminuye en 1 en cada generación se asegura una única sucesión de contraseñas generadas, sin embargo en algún punto el usuario debe reinicializar el sistema para evitar que en algún momento no pueda dar *login* otra vez. Cuando la contraseña secreta *S/key* se calcula en el lado del cliente la frase contraseña debe ser de más de 8 caracteres alfanuméricos. El uso de semilla no secreta permite al usuario usar la misma frase contraseña en cualquier máquina usando diferentes semillas y reciclar la frase cambiando las semillas.

Por razones de interoperabilidad se requiere que todos los clientes y *host* y calculadoras usen el mismo diccionario.

5.5.1. Certificados Digitales

Firma Digital

La firma digital es una herramienta tecnología que garantiza la autoría e integridad de los documentos digitales, resultado de aplicar algoritmos matemáticos al documento original.

Cabe indicar que la firma digital no implica confidencialidad, ya que puede ser observado por distintas personas.

Funcionamiento de la firma digital

La firma digital se compone de una llave pública y una llave privada, siendo estas llaves indisociables y ligadas entre sí. Se llaman indisociables ya que en ningún caso puede deducirse una llave de la otra.

La llave pública es conocida por los interlocutores o receptores del mensaje y por una tercera parte llamada autoridad de certificación (CA), mientras que la llave privada solo es conocida por el propietario y nunca debe ser revelada.

La autoridad de certificación es un agente reconocido y autorizado que genera una secuencia de datos, llamado certificado digital, que relaciona la identidad de una persona o entidad jurídica con su llave pública.

Para dar a conocer la llave pública, se envía a los receptores el certificado digital.

El proceso que realiza el emisor es el siguiente:

- ✓ Se calcula el resumen del mensaje o *hash.*
- ✓ Con la llave privada se encripta el *hash,* siendo el resultado de esta operación lo que reconoce como firma digital.
- ✓ Finalmente el emisor envía la firma digital y el documento original.

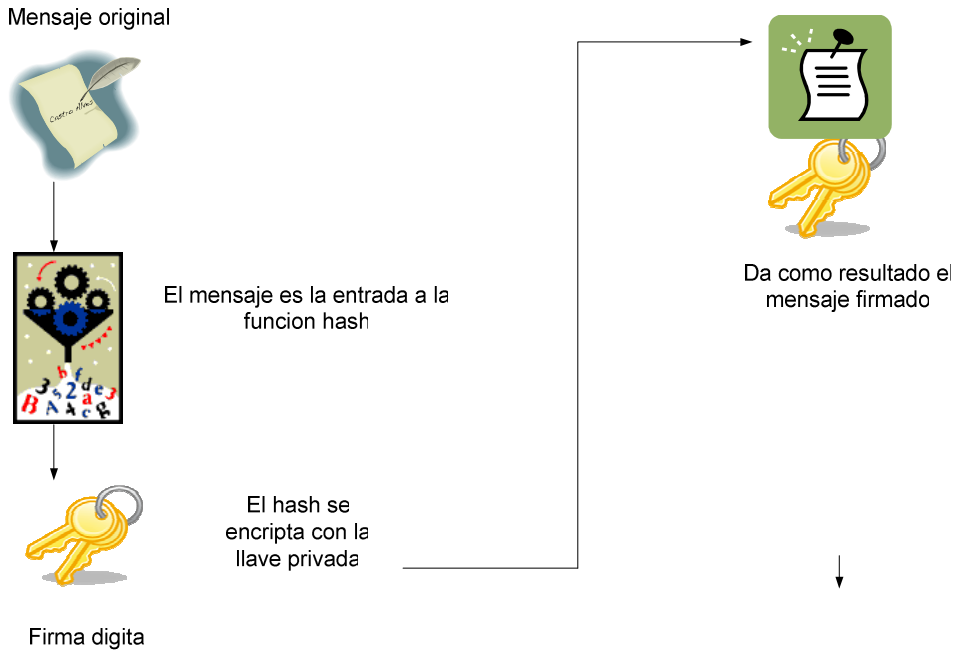


figura. 5.4. generación del hash de un mensaje

El receptor por su parte realiza dos operaciones:

- ✓ Separa el mensaje de la firma digital; el mensaje original es la entrada hacia la función *hash*, dando como resultado el *hash* del mensaje.
- ✓ En sentido paralelo se desencripta la firma digital con la llave publica, obteniéndose el *hash* del documento, a este se lo compara con el *hash* de la primera operación. Si ambos son iguales el receptor esta seguro de la integridad del documento.

Conjuntamente con el certificado digital sabe quien es el autor del documento.

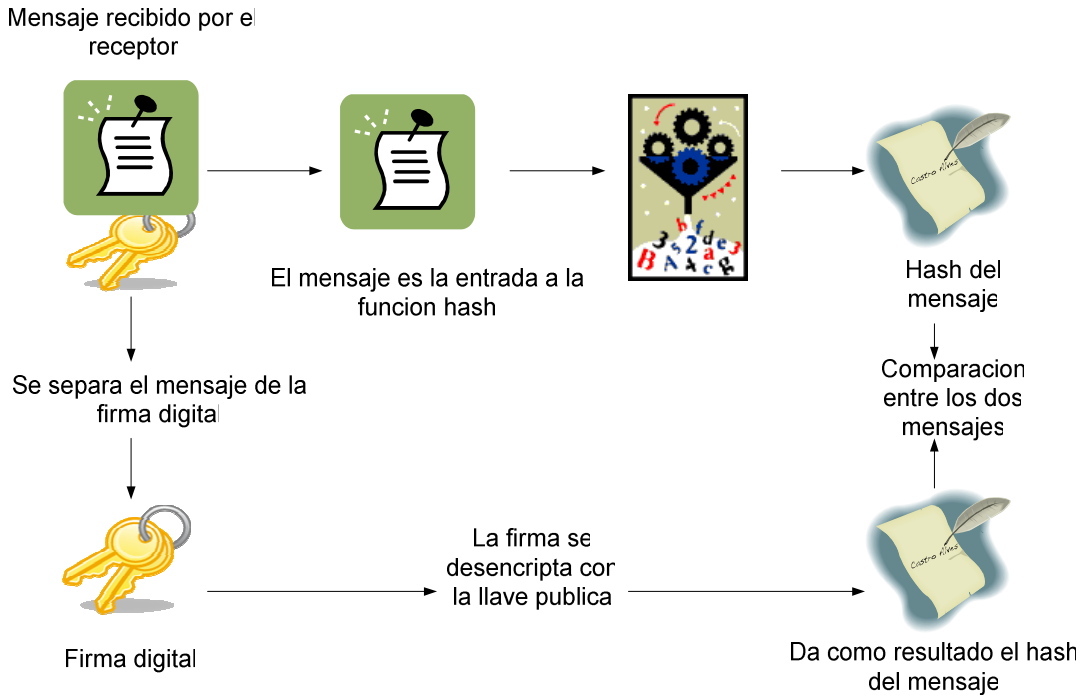


figura. 5.5. desencriptacion del mensaje hash

Dependiendo de los límites financieros del certificado, el estándar ITU-T X.509 define el formato para los certificados digitales, además especifica como gestionar los contenidos de un certificado, creando la llama Infraestructura de Llave Publica (PKI).

5.5.1. Sensores biométricos

La biométrica es la ciencia que mide una característica física única sobre un individuo como mecanismo de identificación.

Existen un gran número de técnicas utilizadas, actualmente las más extendidas son: *Fingerprint scanning*, reconocimiento de voz, reconocimiento del rostro y reconocimiento de firma.

Fingerprint scanning

Es la tecnología mas utilizada, consiste es realizar un escaneo de la yema de los dedos y obtener la huella digital, siendo esta única en cada individuo. Una vez que se obtiene esta huella se la compara con una copia autorizada almacenada en un sistema seguro para realizar la autenticación.

Estos escáner son lo suficientemente pequeños que pueden caber en un ratón, computador portátil o teclado, sin embargo esta tecnología presenta algunas desventajas ya que el escáner no puede determinar si la huella fue obtenida de un usuario legitimo o si fue una copia.

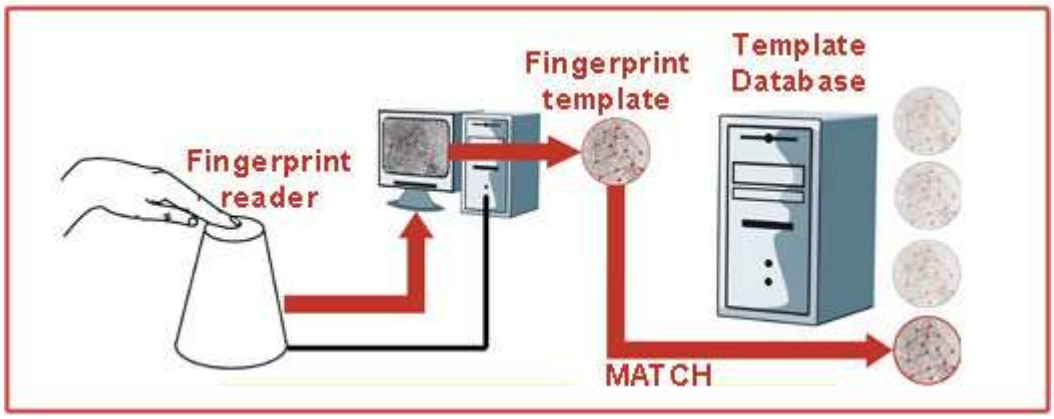


figura. 5.6. técnica de autenticación fingerprint scanning

Reconocimiento de voz

Este tecnología esta basado en la característica vocal única de cada persona, la más común implementación es un micrófono en combinación con un analizador de voz.

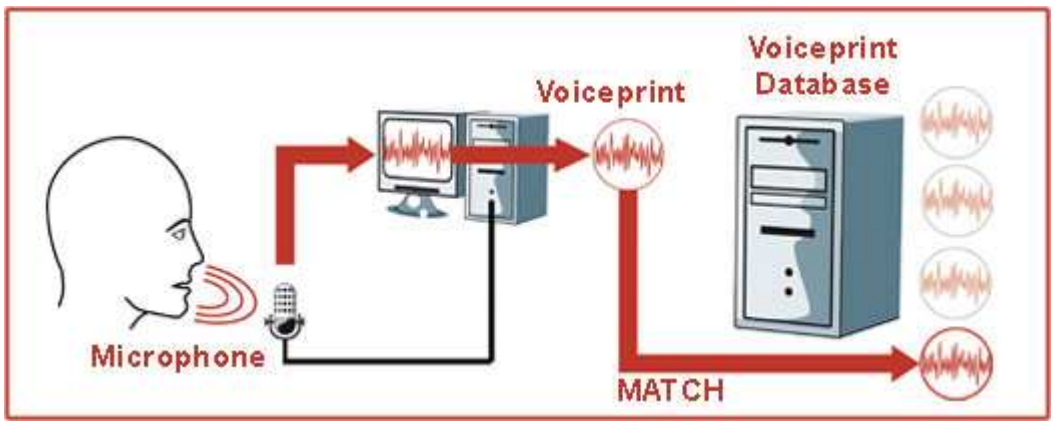


figura. 5.7. técnica de autenticación *reconocimiento de voz*

Reconocimiento del rostro

Esta técnica se basa en el reconocimiento de los rasgos faciales. Una cámara se encarga de tomar una imagen digital del rostro, de la cual se crea una plantilla y se la compara con la base de datos.

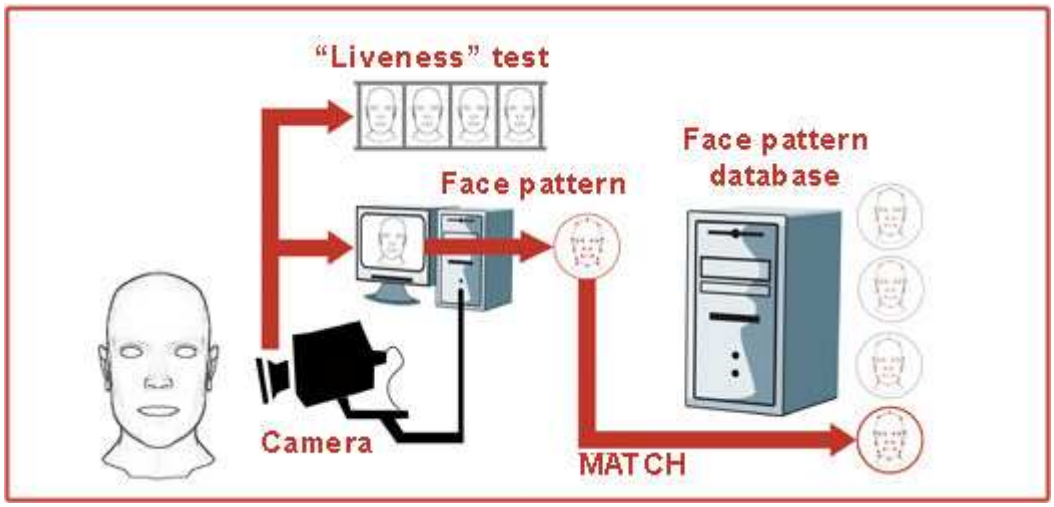


figura. 5.8. técnica de autenticación reconocimiento del rostro

Reconocimiento de la firma

Esta técnica analiza de cómo el usuario realiza su firma, factores como la rapidez, presión, fuerza y apariencia de la firma son comparados con la base de datos del sistema de seguridad.

5.5.2 802.1x

Es un estándar definido por la IEEE, diseñado para proveer control de admisión de red basado en puerto, ya sea por medio cableado o inalámbrico Permite autenticación por medio de información o credenciales únicamente conocida por los clientes.

802.1X se basa en el Protocolo de Autenticación Extensible (EAP), definido en la RFC 3748. EAP define 3 roles en su proceso de autenticación:

Suplicante.- es conocido como el dispositivo o usuario que desea tener acceso a los recursos de red.

Autenticador.- es el dispositivo al que el suplicante se encuentra conectado directamente y por medio de este obtiene el permiso o negación de acceso a la red.

Servidor de autenticación.-es el responsable de autenticar al suplicante, además puede guardar información y hacer un seguimiento de la información de los usuarios, generalmente este servidor es un *Radius* o *Tacacs+*.

El proceso de autenticación de lo describe se realiza de la siguiente manera:

1. El autenticador, después de recibir una petición del suplicante, envía una solicitud de autenticación al servidor.

2. El servidor envía un desafió al suplicante, el mismo que transmite al cliente. El desafió es un método para comprobar la identidad del usuario.

3. Si el suplicante responde al desafió, el servidor de autenticación envía la aprobación al autenticador, quien le permite al usuario ingresar a la red. Si no se puede comprobar la identificación del usuario; el servidor envía una mensaje de negación y el autenticador niega el acceso de red al usuario o suplicante

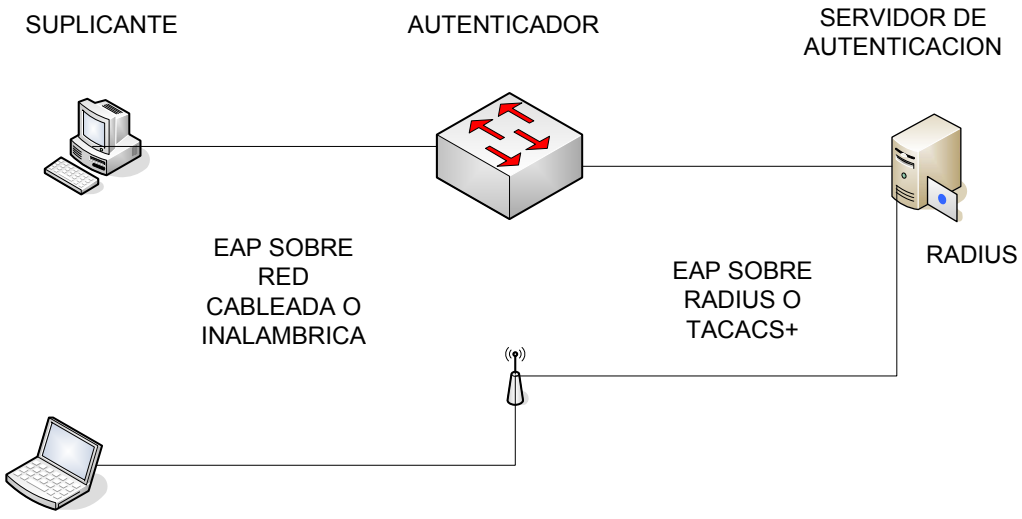


figura. 5.9. 802.1x

Como se observa en le grafico EAP es un protocolo a nivel de la capa de enlace de datos, y se mantiene entre el suplicante y el autenticador, mientras que entre el autenticador y el servidor se habla de EAP sobre *Radius.*

802.1x es un estándar muy ampliamente utilizado en la industria de la telecomunicación, suplicante, autenticadores y servidores de autenticación son disponibles en muchas marcas propietarias y de software libre.

5.5.3 Radius

Radius es el acrónimo en ingles de ***R****emote* ***A****uthentication* ***D****ial-****I****n* ***U****ser* ***S****erver*, desarrollado por *Livingston Enterprise* es un protocolo que se describe en la RFC 2865 y RFC 2866 utilizado para proporcionar servicios de autenticación, autorización y administración de cuentas.

Un cliente *Radius* es responsable de pasar credenciales de usuario e información de parámetros de conexión en forma de un mensaje *radius* a un servidor *radius*, este es el encargado de responder autenticando y autorizando la petición, además los clientes *Radius* también envían mensajes de administración de cuenta a los servidores *Radius.*

Los mensajes *Radius* se envían como mensajes de Protocolo de Usuario (UDP), el puerto UDP 1812 se utiliza para los mensajes de autenticación y el 1813 para los mensajes de administración de cuentas

Los tipos e mensajes *radius* son los siguientes:

Access-Request

Enviado por un cliente *Radius* para solicitar la autenticación y autorización en un intento de conexión.

Access-Accept

Enviado por un servidor *Radius* como respuesta a un mensaje *Access-Request*, en este se indica si es autenticado y autorizado el cliente.

Access-Reject

Enviado por el servidor Radius como respuesta a un mensaje *Acces-Request*, en el se informa de que se ha rechazado el intento de conexión. Se envía este mensaje si el servidor

comprueba que las credenciales no son legítimas o si no se autorizado el intento de conexión.

Access-Challenge

Enviado por un servidor *Radius* como respuesta a un mensaje *Acces-Request,* siendo este mensaje un desafío al cliente *Radius* que exige respuesta.

Accounting-Request

Enviado por un cliente *Radius* para especificar información de administración de cuentas de una conexión que a sido aceptada.

Accounting-Response

Enviado por el servidor Radius como respuesta a un mensaje de *Accounting-Request,* confirmándose la recepción y procesamiento correctos del mensaje *Accounting-Request.*

El servidor *radius* puede utilizar una base de datos local o una base de datos Windows o LDAP para autenticar el *username* y *password.*

Los mensajes entre el cliente y el servidor *Radius* son autenticados utilizando secreto-compartido el cual nunca es enviado a través del trafico de la red, además los usuario y *password* son encriptados para eliminar posibles ataques.

El servidor *radius* soporta una gran variedad de métodos de autenticación entre los cuales tenemos PPP, CHAP, MS-CHAP, EAP, UNIX login.

5.5.4 Tacacs+

Es el acrónimo de ***T****erminal* ***A****ccess* ***C****ontroller* ***A****ccess* ***C****ontrol* ***S****ystem* ; Sistema de Control de Acceso mediante el Control de Acceso desde Terminales. El protocolo de autenticación *Tacacs+* es la versión mejorada de *Tacacs*. Cisco lo ha extendido varias veces. La versión original es un acceso basado en UDP desarrollado por BBN para la red MILNET. El documento RFC 1492 no da detallada información de este protocolo.

Tacacs+ es un protocolo cliente servidor, normalmente es un proceso demonio que corre en UNIX o servidor Microsoft, la característica principal de *Tacasc+* es la separación que hace de la autenticación, autorización y administración de cuentas.

En la autenticación *Tacacs+* permite que el contenido del intercambio de autenticación sea de longitud variable por lo que puede utilizar cualquier mecanismo de autenticación como PPP, CHAP, EAP, *token Chap y kerberos*, la autenticación no es obligatoria.

En el proceso de autenticación existen e tipos de mensajes:

Start, el cliente inicia la autenticación con el servidor.
Continue, que es siempre enviado por el cliente.
Reply, siempre enviado por el servidor.

El proceso de autenticación inicia con el envió del mensaje *Start* por parte del cliente.

El mensaje describe el tipo de autenticación a ser usado por ejemplo CHAP, PAP, etc, además puede contener el nombre de usuario y algún dato de autenticación.

El mensaje *Start* siempre tiene un número de secuencia igual a 1 y solo se envía en el primer mensaje de una sesión de autenticación o como paquete inmediatamente después de un reinicio.

En contestación al mensaje *Start*, el servidor envía un mensaje *Reply*, este mensaje indica si la autenticación continúa o ha finalizado. Si el mensaje indica que continua, el mensaje te4ambien indica que el servidor necesita nueva información, el cliente obtiene la nueva información y responde con un mensaje *Continue*. Este proceso continua hasta que toda la información para la autenticación sea obtenida hasta concluir este proceso.

Cuando la autenticación ha finalizado, el cliente inicia el proceso de autorización el mismo que se realiza con el intercambio de un par de mensajes. *Request* seguido por un Response.

El *Request* de autorización contiene un número fijo de campos que describen y procesan la autenticidad del usuario, y un número no constante de argumentos que describen los servicios para la autorización que se pide.

La administración de cuentas graba lo que el usuario ha hecho, y sirve a dos propósitos; puede utilizarse para el pago de los servicios que utilizó es decir para facturación o como una herramienta de seguridad, para determinar el uso correcto o incorrecto de las normas impuestas por la política de seguridad.

Para realizar la contabilidad *Tacacs+* utiliza 3 clases de registros:
El registro *Start* que indica que un servicio está a punto de iniciar
El registro Stop que indica la finalización de un servicio.
Los registros *Update* que indican que el servicio se está realizando.

Los registros de contabilidad contienen información específica como tiempo de inicio y tiempo de parada y la información de uso del respectivo servicio.

Las transacciones cliente servidor se autentican a través de una contraseña secreta compartida que nunca se envía sobre la red, además se encripta todo el trafico entre los dos.

Se presenta un grafico para resumir este proceso AAA:

1. El usuario inicia una autenticación sobre PPP al Cliente Tacas+
2. El cliente *Tacacs+* le pide al usuario nombre y contraseña.
3. El usuario replica con su contraseña
4. El cliente *Tacacs+* envía un paquete encriptado con la información de usuario al servidor *Tacacs+*.
5. El servidor *Tacacs+* responde con la autenticación o negación.
6. El servidor *Tacacs+* y el cliente intercambian mensaje de autenticación, Si la autorización fue positiva el cliente *Tacacs+* deja entrar al usuario

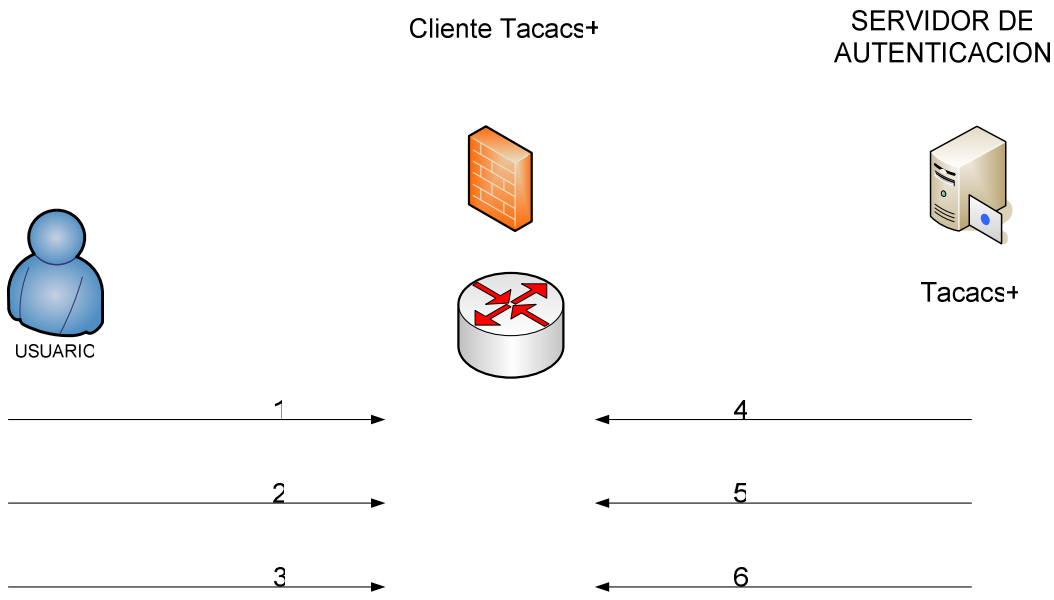


figura. 5.10. protoclo tacacs+

5.5.5 Comparacion De Radius Y Tacacs+.

Protocolo De Transporte.-*Tacacs+* usa TCP, en cambio *Radius* utiliza UDP, simplicando mucho la implementación cliente- servidor, pero hace que *Radius* sea menos robusto.

Desafió/Respuesta.- *Tacacs+* soporta desafió y respuesta bidireccional con el protocolo CHAP, mientras que Radius soporta desafió unidireccional.

Funcionalidad.- *Tacacs+* separa los procesos AAA, permitiendo modularidad para las implementaciones de seguridad. *Radius* combina autenticación y autorización, separando la administración de cuentas.

Integridad de datos.- *Radius* encripta únicamente los usuario y *password*, mientras que *Tacacs+* encripta el paquete entero de datos.

Administrador de Cuentas.-el administrador de cuentas de *radius* puede contener más información que *Tacacs+*, ya que incluye un número limitado de campos de información.

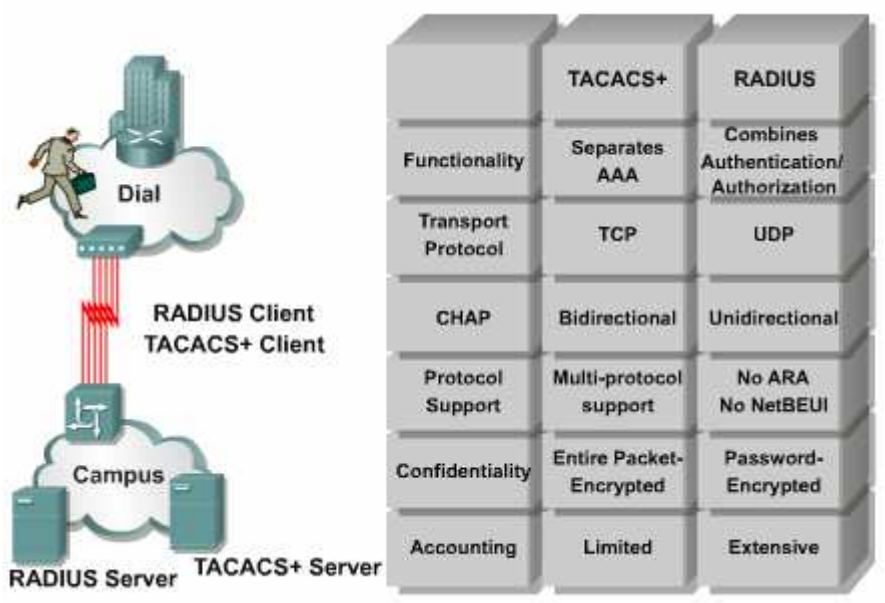


figura. 5.11. comparación entre tacacs+ y radius

5.5.6 Cisco Secure Access Control (Acs)

El *Cisco Secure ACS* Server es un software, que se instala en Windows Server 2000 o 2003, que ayuda al control de acceso a la red, este control lo realiza por medio de la autenticación, autorización y administración de cuentas (AAA).

Este servidor provee AAA a los dispositivos de red que operan como clientes; por ejemplo router, servidores de acceso de red, PIX concentradores VPN; por medio de protocolo Tacacs+ o Radius, Se puede rápidamente administrar clientes, cambiar globalmente los niveles de servicio, individualmente o grupos de usuarios. Sin embargo el uso de una base de usuarios externa es opcional.

Cisco Secure ACS para Windows Server versión 4.0 es fácil en cuanto a su instalación y administración. Las bases de datos con las que puede interactuar son *Windows user database, token Server database o NDS.*

Así mismo ayuda al control de acceso centralizado y administración de cuentas, y un servicio extra que es la capacidad de acceso administrativo a *router y switch.*

Usa *Tacacs+ o Radius* entre el cliente y *Cisco Secure ACS,* dependiendo de la utilidad que va a dar el administrador de la red, en cuanto a los protocolos de autenticación soportados tenemos PAP, CHAP o MS-CHAP.

5.5.6. Autenticación y Base de datos de Usuarios

La autenticación determina la identidad del usuario, antiguamente se utilizaba nombres, usuarios o *password,* en la actualidad se utiliza CHAP o *one-time-password (OTP*), todos estos soportados por el ACS.

El ACS soporta una gran variedad de base de datos externa para la autenticación, entre las cuales tenemos:

- ✓ *Vasco Token Server*
- ✓ *Generic LDAP*
- ✓ *Windows 2000 User Database*
- ✓ *Axent token Server*
- ✓ *ODBC compliant relational databases*
- ✓ *Novell Netware Directory Service (NDS)*
- ✓ *CRYPTOCard Token Server*
- ✓ *RSA SecureId Token Server*

5.5.6. Cisco Secure ACS user Database

Cisco Secure ACS user Database es esencial para el proceso de autorización. Cave indicar que el proceso de autenticación se lo puede hacer por una base de datos externa o interna, mientras que la autorización solo a través de *ACS user database*. Por lo tanto todos los clientes autenticados por una base de datos interna o externa tienen una cuenta en el Cisco *Secure ACS user database.*

Hay cinco maneras de crear usuarios en el *Cisco Secure ACS User Database* de estos RDBMS Syncronization, CSUtil.exe pueden crear cuentas de usuario desde una base externa.

Cisco Secure ACS HTML interfase.- la inteface HTML nos da la facilidad de crear cuenta usuarios, una a la vez.

Unknown User Policy.- habilita al *Cisco Secure ACS database* de agregar usuarios automáticamente cuando un usuario sin una cuenta en la ACS *database* es encontrado en una base de datos externa. La creación de la cuenta de usuario ocurre solo cuando el usuario ha sido autenticado satisfactoriamente por la base de datos externa.

RDBMS Syncronization .-habilita al administrador crear un alto numero de cuentas y así mismo poder configurarlas.

CSUtil.exe .- el CSUtil.exe command-line se utiliza para creer un a cuenta básica, comparado con RDBMS es funcionalmente bastante limitado.

Database replication.- crea cuentas de usuario sobre un *ACS user databse* secundario, teniendo como información una *ACS user databse* primario. Algún cliente único en el ACS secundario es eliminado en la replicación

5.5.6. Arquitectura de Cisco Secure ACS para Windows

Al ser instalado el *Cisco Secure ACS* se agregan algunos servicios a Windows, estos servicios son el núcleo de la funcionalidad de este servidor a continuación los detallamos:

CSAdmin.- provee la interfase HTML para administrar el *Cisco Secure ACS*

CSAuth.-provee los servicios de autenticación.

CDBSync.- provee la sincronización del *Cisco Secure user database* con una aplicación RDBMS externa.

CSlog.- provee los servicios de LOGGING

CSMon.- provee los servicios de monitoreo, grabación y notificación del desempeño del *Cisco Secure ACS* e incluye respuesta automática para algunos eventos.

CSTacacs.- provee comunicación entre el *Tacacs+* AAA cliente y el servicio *CSAuth*

CSRadius.- provee comunicación entre el *Radius* AAA cliente y el servicio *CSAuth*

Cada modulo puede ser iniciado o parado individualmente desde Microsoft Service Control Panel o como un grupo desde *Cisco Secure Acs HTML interfase*.

5.5.6. Autenticación de usuarios Cisco Secure ACS

Vamos a explicar mas detenidamente la autenticación mediante la *ACS User Database*, se puede usar el protocolo *radius o tacacs+*, el servidor de acceso a la red (NAS) hace una petición de autenticación al ACS, el cual verifica el nombre y contraseña; los siguientes servicios y *ACS user database* interactúan así:

- ✓ El servicio *Tacacs+* o *Radius* realiza una solicitud directa al ACS a través del servicio de autenticación, en este momento la solicitud se autentica en contra del *ACS user database*, asociando con la autorización asignada y la información de administración de cuentas es almacenada en el *CSlog*.

- ✓ La base de datos de Windows no autentica al usuario.

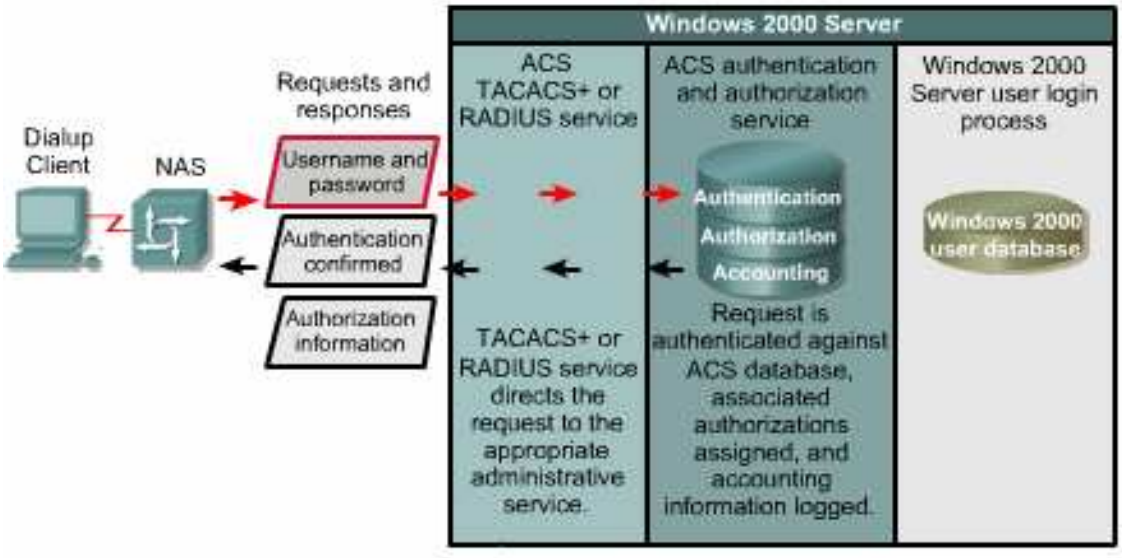


figura. 5.12. autenticación de usuarios acs user database

Al realizar la autenticación por medio de la base de datos de Windows los siguientes servicios y la base de datos interactúan de la siguiente forma:

- ✓ El servicio *Tacacs+ o Radius* dirige la solicitud hacia el servicio de autorización y autenticación, entonces son enviados el usuario y contraseña hacia Base de datos de Windows.

- ✓ Si la petición es aprobada, la base de datos de Windows da el permiso como un usuario local.

- ✓ La respuesta es enviada al *Cisco Secure ACS* y la autorización es asignada al cliente.

- ✓ Confirmación y autorización asignada por el ASC es enviado al cliente o *network access Server* (NAS), y la información de administración de cuentas en guardada.

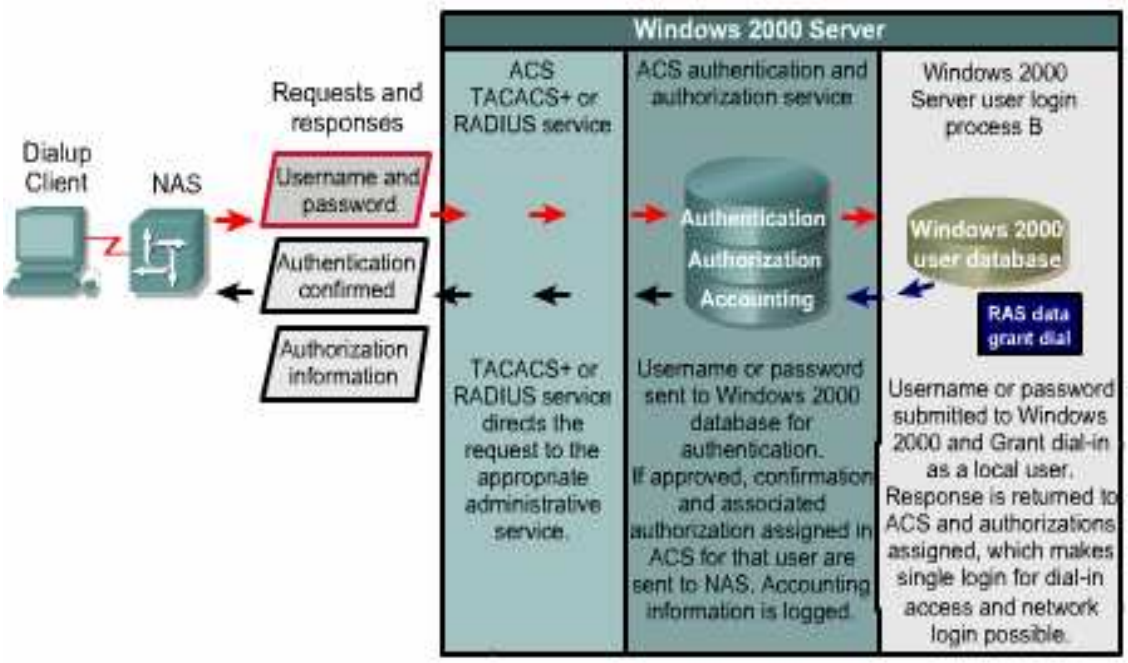


figura. 5.13. autenticación de usuarios con base de datos de windows

5.5.7 Configurar Radius And Tacacs+ En El Cisco Secure Acs

Para la instalación del *Cisco Secure ACS* se requiere información específica acerca de los clientes con los que se conectara y la maquina donde se instalara, estas son algunas de las recomendaciones:

- ✓ Asegurarse que el ASC sea miembro del grupo de servidores de la red, si para el proceso de autenticación se va a utilizar Base de datos de Windows Server es necesario configuración adicional en esta base de datos.

- ✓ Para el primer cliente de AAA, verificar que tipo de protocolo tiene, entre ellos tenemos:

  Tacacs+(Cisco IOS)
  Radius(Cisco Aironet)
  Radius(Cisco BBSM)
  Radius(Cisco IOS/PIX)
  Radius(Cisco VPN 3000)
  Radius(Cisco VPN 5000)
  Radius(IETF)
  Radius(Ascend)
  Radius(Nortel)

- ✓ Recordar el nombre del cliente.
- ✓ Recordar la dirección IP del cliente
- ✓ Recordar la dirección IP de la maquina donde se instalara el ACS
- ✓ Recodar la llave de Tacacs+ o Radius

El proceso de instalación se resume en los siguientes pasos:

1. Preconfigurar el Windows 2000 Server.
2. Verificar conectividad entre el Windows 2000 Server y los *routers* usando ping o *telnet*
3. Instalar el *Cisco Secure ACS* sobre el Windows 2000 Server.
4. Iniciar la configuración del ACS vía *web browser interfase.*
5. Configurar el *router* o pix como cliente AAA.
6. Verificar la correcta instalación y operación.

5.5.7. Administración del *Cisco Secure ACS*

Para una administración fácil del ACS se lo hace por medio del *web browser*. Esta administración esta condensada en botones de control, cada uno realiza una función particular, dependiendo de la configuración que necesitamos los utilizaremos.

Figura. 5.14 cisco secure access control server (acs)

Los botones son los siguientes:

User Setup.-agrega, edita o elimina cuentas de usuarios y enlista los usuarios en la base de datos.

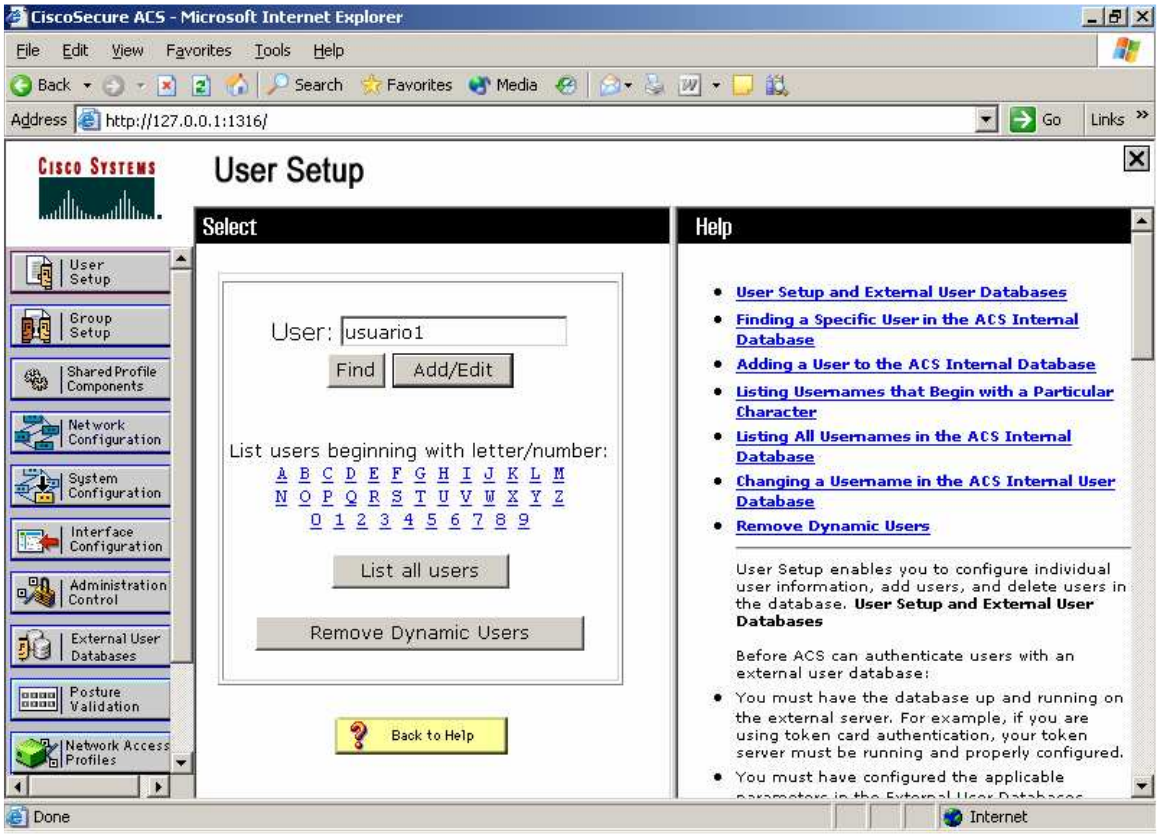


Figura. 5.15 acs user setup

Group Setup.-crea, edita, renombra, y enlista todos los usuarios en grupos.

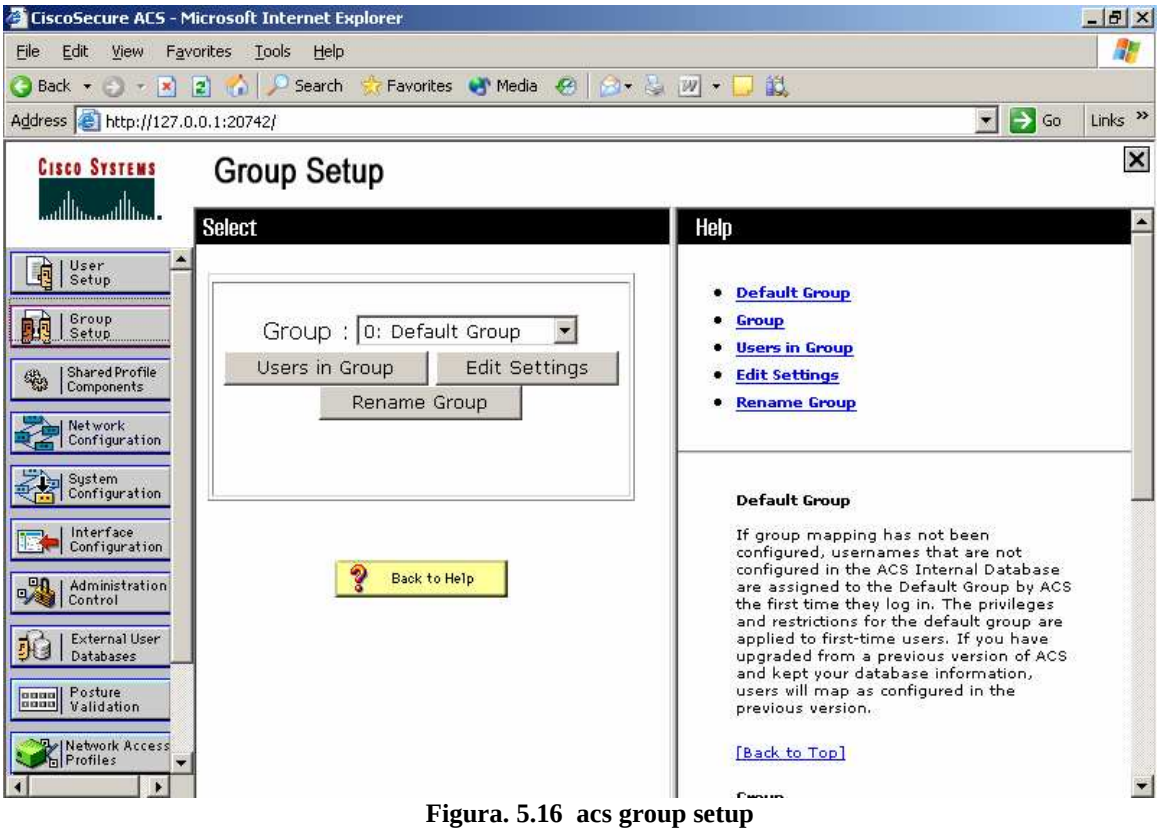


Figura. 5.16 acs group setup

Shared Profile Components.- comparte los atributos de autorización los cuales pueden ser aplicados a uno o muchos usuarios o grupos de usuarios.

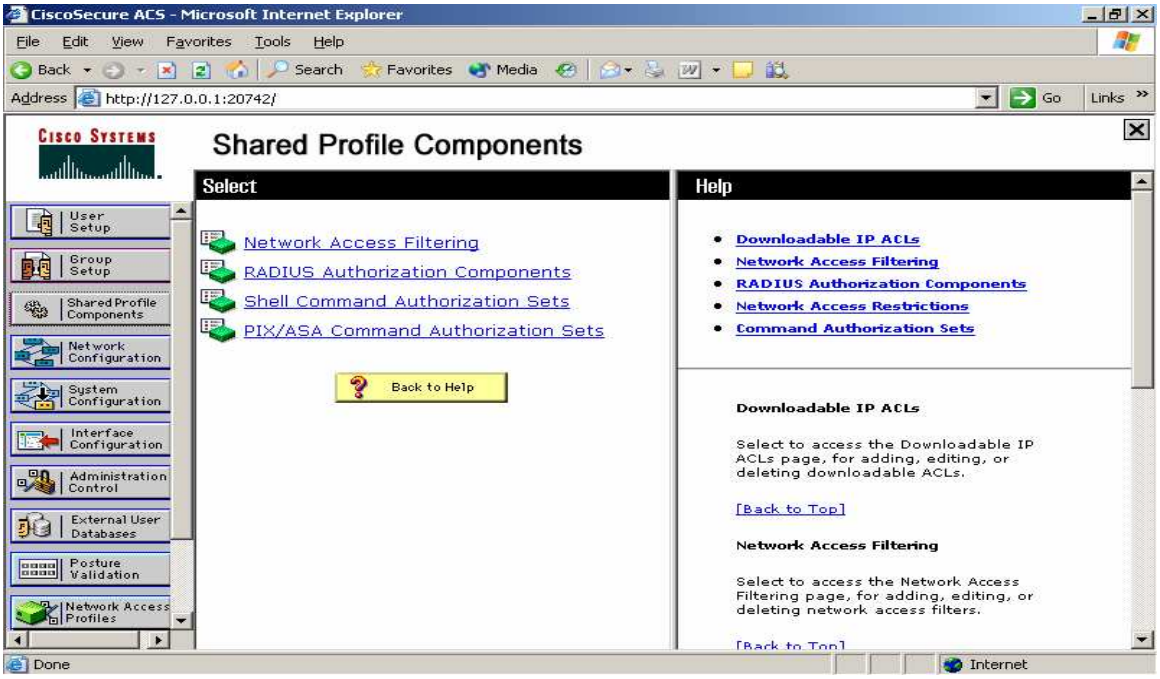


Figura. 5.17 acs user-share profile components

Network Configuration.-configura y edita los clientes AAA (*router, pix, concentradores,switch)*

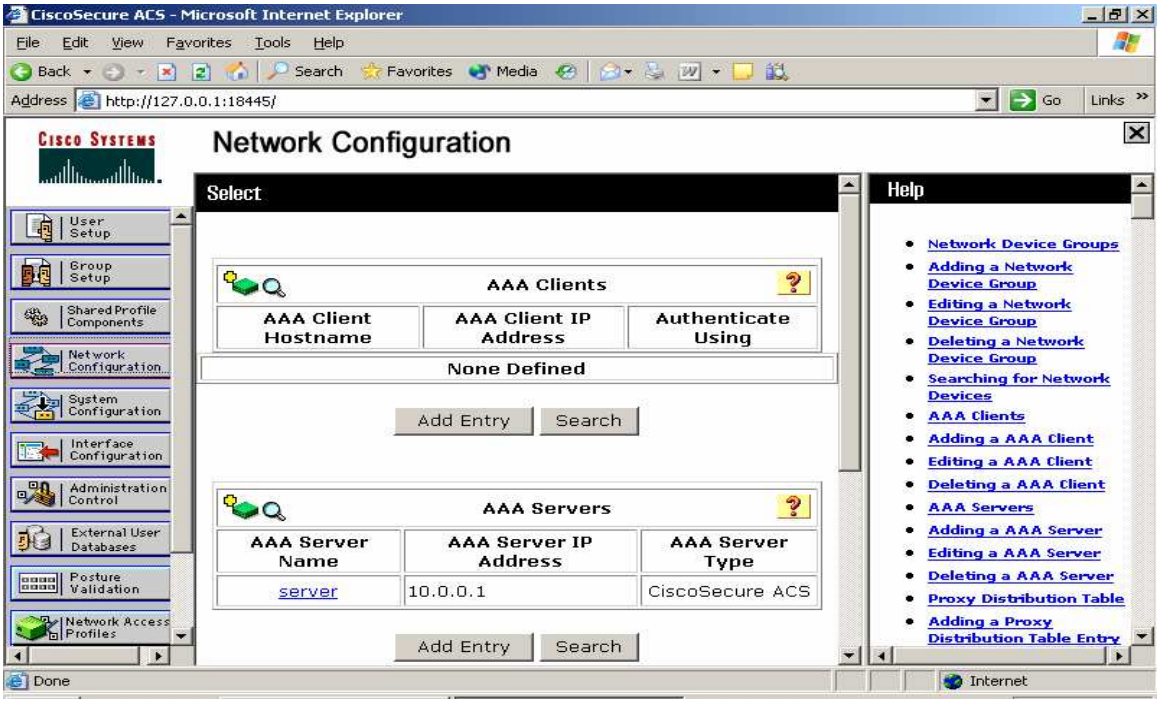


Figura. 5.18 acs user-network configuration

System Configuration.- inicia y para los servicios del ACS, configura la administración de cuentas, la replicación a base de datos externa y controla *RDBMS sincronization.*

Interfase Configuration.-Configura al usuario definiendo los campos que serán guardados en la administración de cuentas, configura las opciones *Radius y Tacacs+* y controla la interfase grafica del administrador.

Administración Control.-permite el control administrativo del ACS desde cualquier computador de la red.

External User Databases.-Configura el servicio *Unknown User Police* para algunos tipos de bases externas en la autenticación.

Reports and Activity.-se aprecia un reporte de las siguientes actividades:

- ✓ *Tacacs+ Accounting Report.*-enlista cuando una sesión empieza y se para, graba este acceso a la red con el usuario y el tiempo de duración de cada sesión
- ✓ *Radius Accounting Report.*- enlista cuando una sesión empieza y se para, graba este acceso a la red con el usuario y el tiempo de duración de cada sesión.
- ✓ *Failed Attemps Report.*-enlista las autenticaciones y autorizaciones falladas y el motivo del fallo.
- ✓ *Logged in Users.*-enlista los usuarios que están actualmente recibiendo los servicios de ACS.
- ✓ *Disabled Accounts.*-enlista los usuarios que estas deshabilitados en ese momento.
- ✓ *Admin Accounting Report.*-enlista los comandos de configuración ingresados sobre el Tacacs+ cliente.

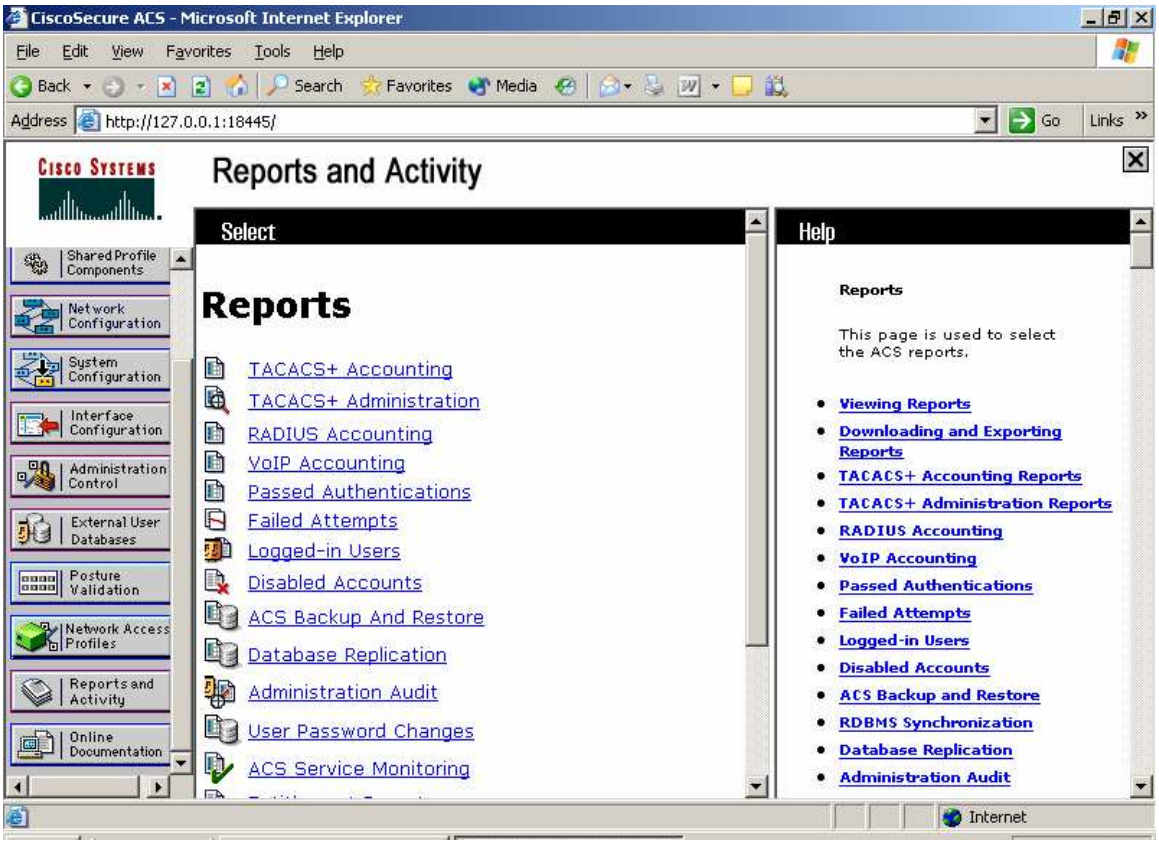


Figura. 5.19 acs user-reports and activity

Online documentación.-provee información detallada acerca de la configuración, operación, y conceptos el ACS.

5.5.7. Solución de Problemas del Cisco Secure ACS.

Para resolver problemas del ACS relacionamos con AAA, empezamos examinando los reportes de *failed attempts* bajo el botón *Reports and Activity*, este reporte indica algunos tipos de fallos.

Fallos de Autenticación

Asumiendo que el ACS y el *router* tienen conectividad, y que la autenticación se la hace por medio de *Windows Database*, se debe chequear los siguientes ítems:

- ✓ Ingresar correctamente el usuario y contraseña
- ✓ Revisar si el usuario y contraseña existen en la base de datos.
- ✓ Tiene el usuario y contraseña intentos exitosos de acceso a al red.
- ✓ Esta el ACS configurado para autenticar en contra de la base de datos de Windows.

- ✓ Tiene el contraseña expirado en la base de datos de Windows.

Fallos de autorización

- ✓ Si el dial-in usuario en autorizado, pero no autenticado, chequear los siguientes:
- ✓ Están siendo los servicios adecuados enlistados en Group Setting.
- ✓ Como el dial-in usuario tiene la dirección IP.
- ✓ Existe un pool de direcciones configurado en el Network Acces Server(NAS).
- ✓ Tiene la opción Permited seleccionada

Failed Attempts 2002-12-06.csv

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port	NAS-IP-Address
12/06/2002	12:59:46	Author failed	aaauser	Default Group	10.1.2.12	..	Service denied	service=auth-proxy cmd*	Ethernet0/0	10.0.2.2
12/06/2002	12:58:31	Author failed	aaauser	Default Group	10.1.2.12	..	Service denied	service=auth-proxy cmd*	Ethernet0/0	10.0.2.2
12/06/2002	12:38:10	Author failed	andy	is-in	async	CS password invalid	..	..	tty0	10.0.2.2

figura 5.20 intentos fallados

5.5.7. Habilitar Tacacs+ O Radius

El primer paso para configurar AAA en el *router o pix* por medio de *Tacacs+*, es especificar el servidor o grupo de servidores ACS que van a dar este servicio y configurar la llave secreta encriptada que es utilizada entre el ACS y el *router o pix.*

El comando *aaa new model* forza al *router* anular todos los tipos de autenticación anteriormente configurados.

```
pixfirewall(config)#aaa new-model
```

El comando Tacacs-server key es usado cuando dos o más servidores Tacacs+ comparten la misma llave, múltiples servidores ACS pueden ser especificados cada uno con su llave usando el comando tacacas-server host, a continuación ejemplos de estos comandos:

Sintaxis:

pixfirewall(config)#aaa-server etiqueta _grupo **protocol** protocolo_autenticacion
pixfirewall(config)#aaa-server etiqueta _grupo **(nombre_if) host** servidor_ip clave **timeout** segundos

etiqueta_grupo.- cadena alfanumerica que es el nombre del grupo del servidor.

Protocolo de autenticación.- el tipo de servidor AAA, tacacs+ o radius.

Nombre_if .- nombre de la interfaz en la que reside el servidor

Servidor_ip.- direccion ip del servidor AAA.

Clave.- una palabra clave alfanúmérica compuesta de hasta 127 caracteres que tiene el mismo valor que la clave del servidor Tacacs+.

segundos.- un temporizador de retransmisión que especifica la duración con la que el PIX reintenta cuatro veces el acceso al servidor AAA antes de elegir el siguiente servidor.

Ejemplo:

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

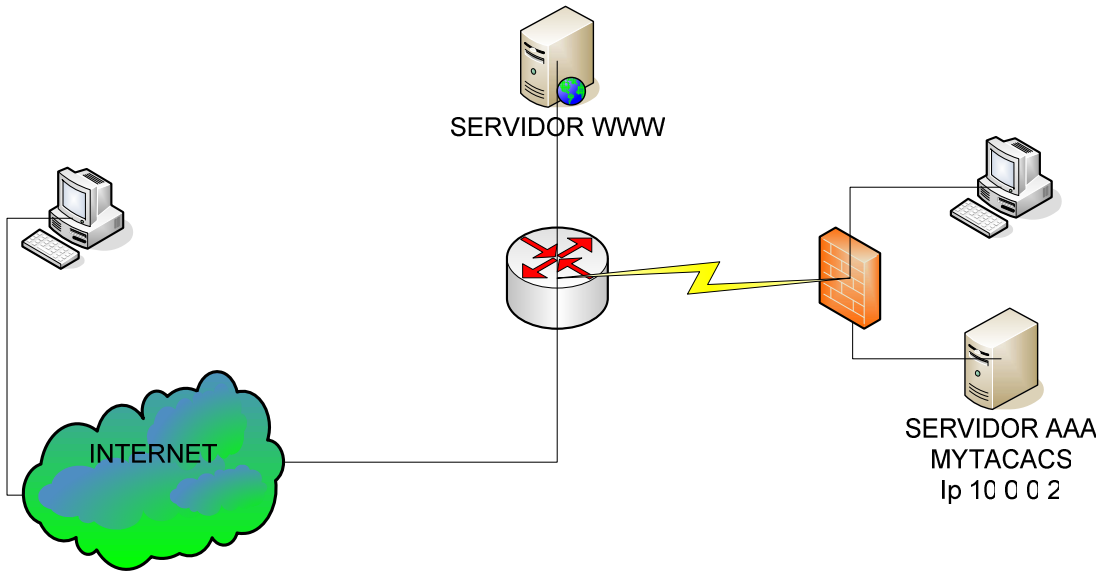


figura. 5.21. habilitar sevidor aaa en el pix

Para la configuración de un servidor radius se utiliza la mima sintaxis, con la diferencia que en vez de la palabra tacacs es radius.

Para verificar el funcionamiento de la configuración de Tacacs+, se utiliza el comando:

- ✓ debug tacacs
- ✓ debug tacacs events
- ✓ debug aaa authentication

debug tacacs.- despliega información asociada con Tacacs, se lo utiliza en modo ***privilegiado.*** A continuación se da ejemplo del este comando, donde el proceso login fue exitoso, indicado por el status pass.

Router# **debug tacacs**

14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15 (AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet

14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15

El proceso de login en este ejemplo fue fallado.

Router# **debug tacacs**

13:53:35: TAC+: Opening TCP/IP connection to 192.168.60.15 using source 192.48.0.79
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 192.168.60.15 (AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 192.168.60.15
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 192.168.60.15 (AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 192.168.60.15
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 192.168.60.15 (AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 192.168.60.15
13:53:38: TAC+ (416942312): received authen response status = FAIL
13:53:40: TAC+: Closing TCP/IP connection to 192.168.60.15

debug aaa authentication.- nos permite obtener un alto nivel de la actividad login en el siguiente ejemplo muestra el resultado de este comando, el proceso de login fue exitoso, el método *Tacacs+*

pixfirewall# **debug aaa authentication**

14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS

El estado de AAA/AUTHEH indica tres posibles estados: pass, *fail* y error.

debug tacacs event.- despliega información al solicitar un *helper process*, se lo utiliza en modo privilegiado.

5.5.8 Configurar AAA En El Pix

5.5.8. Autenticación

Existen dos tipos de autenticación en el PIX:

- ✓ *Access authentication*
- ✓ *Cut-through Proxy authentication*

El *access authentication* es utilizado para requerir autenticación antes del ingreso a la consola del PIX. Los siguientes servicios de autenticación son disponibles: *enable password*, serial, *ssh, http,telnet*.

La opción *enable* permite que haya tres intentos antes de detenerse con un mensaje de acceso denegado, las opciones serial y *telnet*, hacen que se le pregunte continuamente al usuario hasta lograr el inicio de sesión.

Sintaxis:

pixfirewall(config)#aaa authentication [serial | enable | telnet] console etiqueta_grupo **[LOCAL]**

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 rpivilegiado par alas conexiones serie o telnet.

telnet.- oblige 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.

Console.-especifica que el acceso a la consola del PIX solicite autenticación y opcionalmente registra los cambios realizados en la configuración, en un servidor syslog.

etiqueta_grupo.- la etiqueta del grupo se establece con el commando aaa-server.

[LOCAL].- la autenticaron puede ser en contra del la base de datos del PIX.

Ejemplo:

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

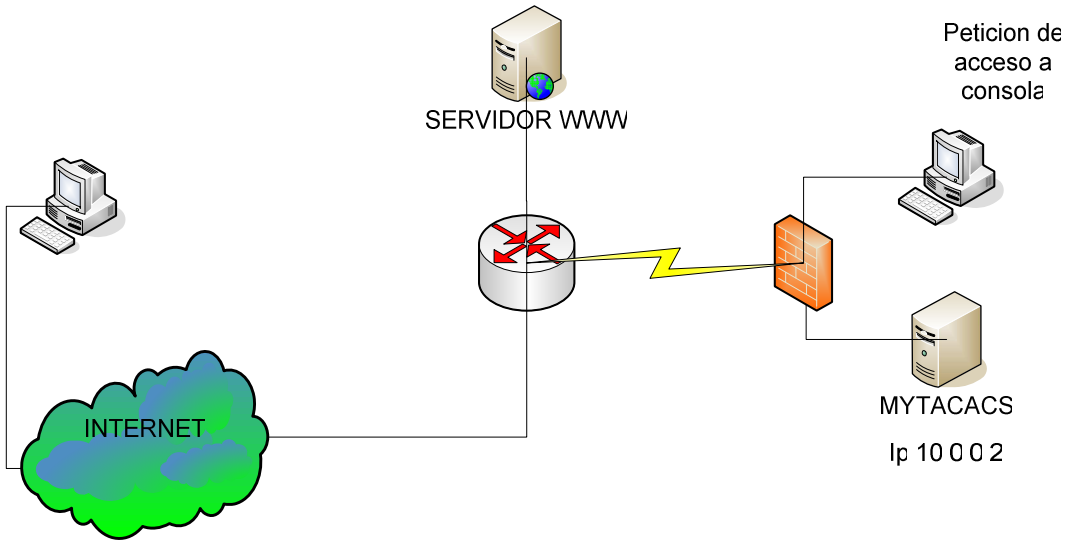


figura. 5.22. configurar autenticación serial

Cut-through Proxy authentication, es un método patentado que sirve para verificar de forma transparente la identidad de los usuarios y permitir o denegar el acceso a cualquier aplicación basada en TCP o UDP. Las sesiones interceptadas son únicamente *Ftp, Https, http o Telnet.*

Llamado también autenticación por método de corte funciona determinando que una sesión requiere la autenticaron basada en usuario, la habilitación de un desafío de nombre de usuario y contraseña, y la autenticación del usuario frente a la base de datos *Tacacs+* o *Radius*. Una vez comprobada el usuario y contraseña, el PIX cambia el flujo de de la sesión y rápidamente todo el tráfico fluye directamente entre el servidor y el cliente, al tiempo que se mantiene la información del estado de la sesión.

Al autenticarse con el servicio *telnet,* el usuario tiene cuatro oportunidades, si falla al cuarto intento el PIX interrumpirá la conexión.

La autenticación mediante *ftp,* permite solo una oportunidad, si falla inmediatamente conexión es interrumpida.

Mediante *http* el usuario genera un *web browser,* si falla la contraseña, tiene la oportunidad de ingresar nuevamente.

Utilizando el servicio *https* para autenticar. El usuario tiene tres oportunidades, si falla al tercer intento el pix interrumpe la conexión

Un ejemplo típico es un usuario de Internet que accede a un servidor *http* de una DMZ, en la siguiente figura se encuentra un usuario de Internet que accede a la URL correspondiente para entrar al servidor *web.*

El requisito AAA del PIX obliga al usuario ingresar un usuario y contraseña, el usuario ingresa estos datos, que pasa al PIX en texto claro, y este envía a su vez la información al servidor AAA, si es autenticado, se le permite al usuario interactuar con el destino. Si el servidor web de destino también requiere autenticación, se pasará el usuario y contraseña.

Sintaxis:

pixfirewall(config)#aaa authentication include | exclude servicio_autenticacion **inbound | outbound** nombre_if ip_local mascara_local ip_externa mascara_externa etiqueta_grupo.

Incluye.- crea un 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.

Servicio_autenticación.- la aplicación con la que el usuario esta accediendo a la red. Se utiliza hay,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, estos deberán usar FTP,http o telnet.

Inbound.- autentica conexiones entrantes, implica que la conexión se origina en la interfaz externa y que se dirige a la interfaz interna.

Outbound.- autentica conexiones salientes, 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.

Ip_local.- la dirección ip del host o red de host a autenticar, está direccion puede ser establecida a 0 para incluir a todos los host y permitir que el servidor de autenticación decida que host se van a autenticar.

Máscara _ local.- máscara de red local, especifique siempre un valor de máscara. Utilice 0 si la dirección ip es 0, tilice 255.255.255.255 para un host.

Ip_externa.-la direccion ip de los host que van a acceder a la dirección ip_local. Utilice 0 para incluir a todos los host.

Ejemplo:

pixfirewall(config)#aaa authentication include http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS
pixfirewall(config)# aaa authentication include ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS
pixfirewall(config) # aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS

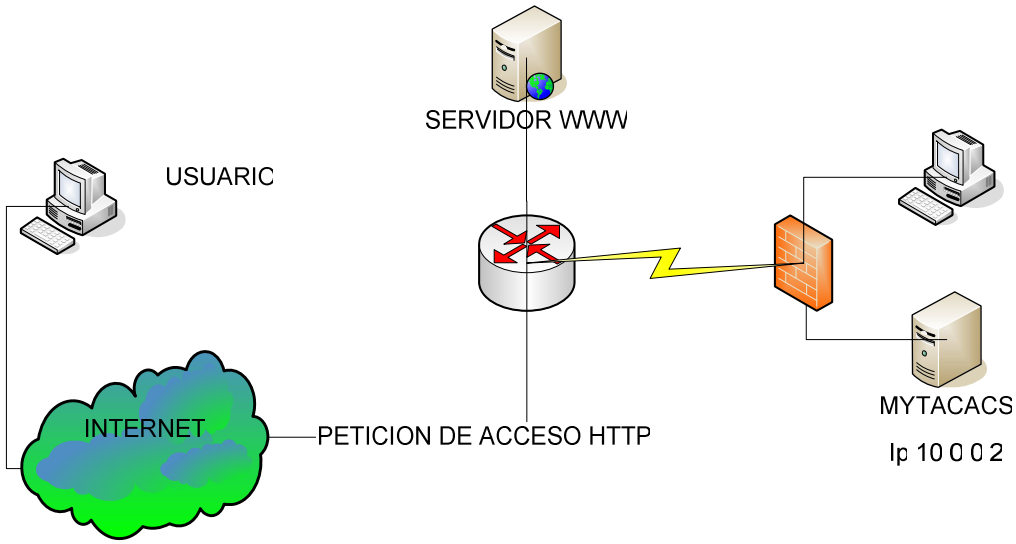


figura. 5.23. configurar autenticación

La autenticación de otros servicios es posible a través del PIX. Por ejemplo si hay usuarios que desean acceder a un servidor de archivos Microsoft en el puerto 139 .Para esto se creo el *telnet* virtual.

El *telnet* virtual nos proporciona una forma de preautenticar a los usuarios que soliciten conexiones atravesando el PIX utilizando servicios o protocolos que no soporten la autenticación.

Cuando un usuario no autenticado hace un *telnet* a la dirección IP virtual, al usuario se le pide un nombre de usuario y contraseña, el servidor AAA es el que lo autentica, luego el usuario ve el mensaje *Authentication Succcessfull* y las credenciales son ubicadas en la cache del PIX y este restablece la sesión *telnet.*

Si un usuario desea finalizar la sesión para borrar la entrada de la memoria *cache*, deberá hacer un nuevo *telnet* a la dirección virtual. Se le pedirá nuevamente usuario y contraseña, el PIX eliminara de la *cache* las credenciales asociadas y se le aparecerá al usuario un mensaje *Logout Successful*.

Ejemplo:

```
pixfirewall(config)#aaa authentication  include tcp/139 inbound  0.0.0.0  0.0.0.0
0.0.0.0 0.0.0.0 MYTACACS
pixfirewall(config)# virtual telnet 172.16.0.5
pixfirewall(config) # static(inside,outside) 172.16.0.5 10.0.0.10
pixfirewall(config) # virtual telnet 172.16.0.5
pixfirewall(config) # accees-list permit tcp host 172.16.0.5 eq 139 any
```

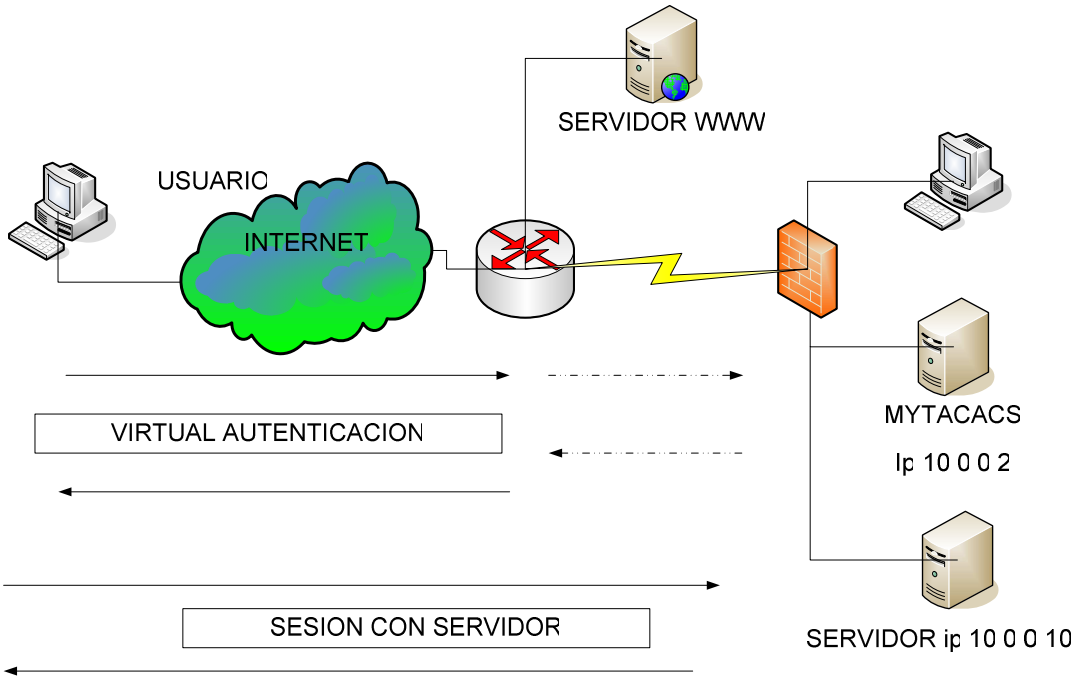


figura. 5.24. configurar autenticación para telnet virtual

Tiempos de Espera de autenticación

Se usa el comando *timeout uauth* para especificar el tiempo que debe esperar la memoria *cache* posterior a la inactividad de las conexiones de usuario, este tiempo debe ser mínimo de dos minutos, se utiliza el comando *clear uauth* para eliminar todas las caches de los usuarios, teniendo que volver a autenticarse en una nueva conexión.

Sintaxis:

time uauth [hh:mm:ss] [absolute| inactivity]

[hh:mm:ss].- plazo de expiración de la *cache* de autenticación y autorización que tiene el usuario para reautenticar la siguiente conexión, establezca 0 para desactivar la *cache*. No establezca a 0 si utiliza ftp pasivo.
Absolute.-ejecuta continuamente el temporizador *uauth,* pero una vez que este se termine, espera hasta el inicio de una nueva conexión.
Inactivity.- inicia el temporizador *uauth* cuando una conexión pasa al estado de inactividad.

En otras palabras los *cualificadores* i*nactivity* y *absolute* obligan a los usuarios a reautenticarse transcurrido un periodo de inactividad o una duración absoluta.

El temporizador de inactividad y absoluto pueden funcionar al mismo tiempo. El temporizador absoluto deberá ser configurado para un tiempo mas prologado que el Temporizador de inactividad. Si el temporizador absoluto es menor que el temporizador de inactividad, este último no se producirá.

Cambiar la petición de autenticación

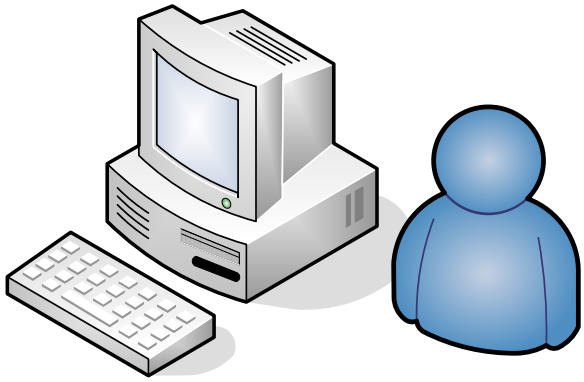
Utilice el comando auth-prompt para crear un texto de desafío para el acceso *http, Ftp* o *Telnet* a través del PIX, este texto se muestra en la parte superior a las peticiones de nombre de usuario y contraseña. Es posible también cambiar el texto de rechazo y aceptación de la autenticación.
Sintaxis:

auth-prompt [accept | reject | prompt] cadena

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 aceptación.
prompt.- la cadena de petición de desafío AAA sigue a esta palabra clave.
Cadena.- una cedena de hasta 235 caracteres alfanuméricos.

Ejemplo:

pixfirewall(config)#auth-prompt prompt Por favor ingresa tu usuario y contraseña
pixfirewall(config)#auth-prompt reject Usuario o contraseña incorrecta intenta nuevamente.
pixfirewall(config)#auth-prompt accept Autenticación exitosa



Por Favor ingresa tu usuario y contraseña
USERNAME:Estudiante
PASSWORD:
Usuario o contraseña incorrecto intenta nuevamente
USERNAME:Estudiante
PASSWORD:
Autenticacion exitosa

figura. 5.25. configurar banner de autenticación

5.5.8. Autorización

Si todos los usuarios autenticados son permitidos utilizar los servicios: *Ftp, http, Https* y *telnet* no es necesario la autorización. Si por alguna razón se permite solo un segmento de usuarios a algún servicio, entonces es necesaria la autorización. El PIX soporta dos métodos para la autorización.

- ✓ Autorización clásica
- ✓ Listas de Acceso descargables por usuario

En la autorización clásica, las listas de acceso son configuradas en el servidor *Tacacs+* o *Radius* y consultadas bajo demanda.

A continuación damos la sintaxis de los comandos y ejemplo de configuración clásica de autorización

Sintaxis:

pixfirewall(config)#aaa authorization match acl_name if_name server_tag

acl_name.- nombre de la lista de acceso que permite o niega el servicio ftp,http,telnet,https.
if_name.-corresponde en nombre de la interfaz dado por el comando nameif.
server_tag.-nombre del grupo de servidores creados con e comando aaa-server.

Ejemplo:

Este grupo de comando autoriza el tráfico telnet, ftp y www desde la intefaz outside, o en otras palabras entrante a la red interna.

```
pixfirewall(config)#access-list 101 permit tcp any any eq telnet
pixfirewall(config)# access-list 101 permit tcp any any eq ftp
pixfirewall(config)# access-list 101 permit tcp any any eq www
pixfirewall(config)# aaa authorization match 101 outside MYTACACS
```

Las listas de Acceso descargables que consiste en almacenar todas las listas de acceso sobre el servidor AAA y que estas sean descargadas en el PIX, la lista de acceso es enlazada al usuario o grupo de usuarios en el AAA Server, durante el proceso de autenticación, después que el usuario y contraseña son validados, el servidor AAA retorna al PIX la lista de acceso, esta lista de acceso retornada es modificada basado en la dirección IP del usuario autenticado, esta funcionalidad solo es soportado por *Radius.*

Para descargar las listas de acceso durante la autenticación, siga el siguiente procedimiento en el ACS

- ✓ Selecciona *downloadable acls desde Shared Profile Component* (SPC)
- ✓ Dar un click en add ACL definition, ingresa el nombre, descripción y definición de la ACL
- ✓ A continuación un ejemplo de la definición de una ACL antes de que sea cargada en el PIX

```
+-----------------------------------------+
| Shared profile Components               |
|                                         |
|   Downloadable PIX ACLs                 |
|                                         |
| Name:              acs_ten_acl          |
| Description:  10 PIX access-list commands|
|                                         |
|                                         |
|      ACL Definitions                    |
|                                         |
| permit tcp any host 10.0.0.254          |
| permit udp any host 10.0.0.254          |
| permit icmp any host 10.0.0.254         |
| permit tcp any host 10.0.0.253          |
| permit udp any host 10.0.0.253          |
| permit icmp any host 10.0.0.253         |
| permit tcp any host 10.0.0.252          |
| permit udp any host 10.0.0.252          |
| permit icmp any host 10.0.0.252         |
| permit ip any any                       |
+-----------------------------------------+
```

Configure el usuario o grupo de usuarios por medio de *User Setup o Group Setup* e incluye las ACL al usuario o grupo.

Una vez que la configuración este realizada correctamente, a la petición de autenticación de un usuario provocará que las ACL sean enviadas al PIX. El PIX determinará si la ACL nombrada existe o no, si la ACL ya esta en el PIX esta no será descargada nuevamente.

Si la descarga de las ACL fue exitosa, las ACL sobre el PIX tendrán el siguiente nombre

#ACSACL#-*acl_name*-12345678

Donde acl_name, es el nombre de la lista de acceso definido en el SPC y 123456789 es el identificador único de la ACL. Si la lista de acceso no esta configurada en el ACS la descarga falla y se registrará un mensaje syslog.

Después que la ACL a sido descargada en el PIX , esta tendrá la siguiente forma:

access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-PIX-acs_ten_acl-3b5385f7 permit ip any any

Finalmente tenemos que habilitar la ACL, siguiendo los siguientes pasos: Click en Interfase Configuration en el menú principal del ACS y Click en Advanced Options, y selecciona una o ambas opciones:

User-Level Downloadable ACL

Group-Level Downloadable ACL

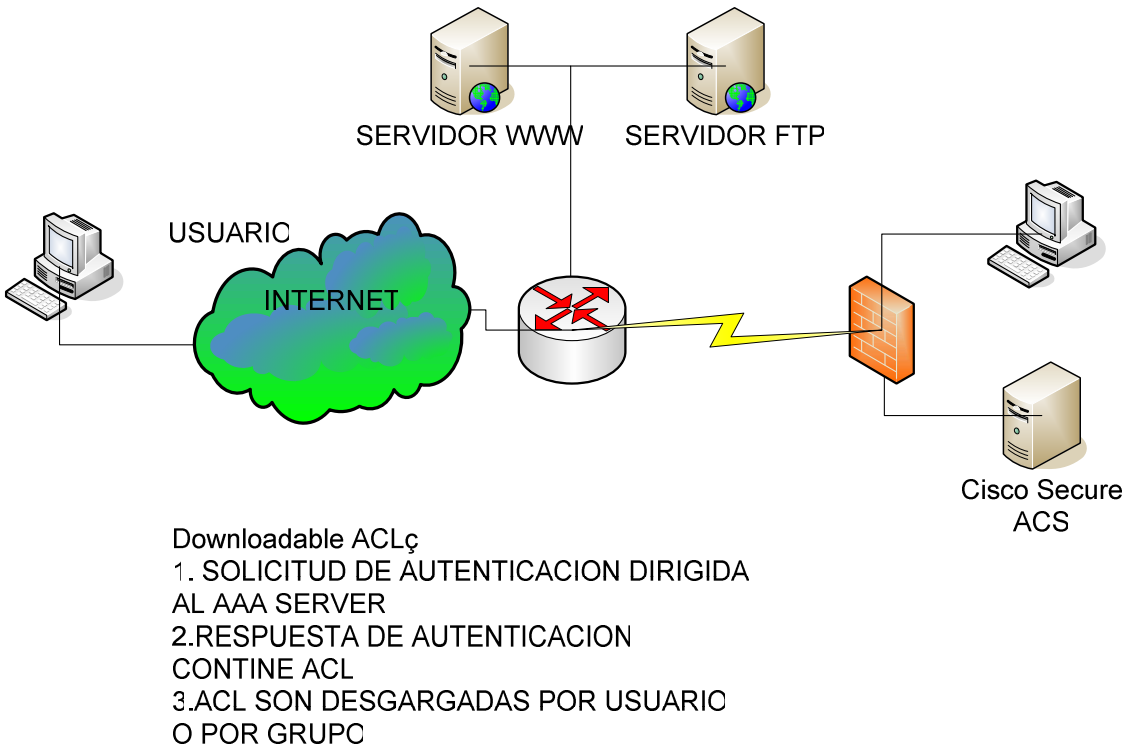


figura 5.26 download acl

5.5.8. Administración De Cuentas

Para habilitar, deshabilitar o ver la administración de cuentas sobre el servidor designado por el comando aaa-server, se usa el comando *aaa accounting*, este comando se aplica hacia todos y puede ser limitado para uno o pocos servicios; este comando permite guardar una grabación de los servicios que han sido accesados de la red, la misma que es guardada sobre el servidor aaa designado o grupo de servidores.

Para habilitar la grabación, el administrador tiene que identificar el tráfico que se grabar o registrar a través de listas de acceso y referirse hacia el comando *aaa accounting* match. En el ejemplo siguiente la lista de acceso identifica el trafico *www* y *ftp* desde cualquier host hacia el servidor *www* con dirección ip 192.168.4.1 y se configura luego el comando *aaa accounting* match pata que realice el registro de estos dos tipos de trafico, de este forma cualquier usuario que acceda al servidor *www* por ftp o *www* la grabación o registro será generado y enviado hacia el servidor aaa.

El trafico que no es especificado por la sentencia *include* no es registrado, en el ejemplo serán registrados en el servidor aaa todas las conexiones salientes, es decir trafico desde la interfaz interna a la externa.

Sintaxis:

aaa accounting include | exclude name_if local_ip local_mask ip_forgein mask_forgein server_tag
aaa accounting include | exclude service if_name server_tag
aaa accounting match acl_name if_name server_tag

include.- crea una nueva regla con el servicio especificado a incluir.

exclude.-crea una excepción a una regal declarada con anterioridad excluyendo el servicio especifico de contabilidad del host especifico.

name_if.- nombre de la interfaz desde la cual los usuarios requieren administración de cuentas.

local_ip.-direccion ip del host o de la red que se va a obtener el registro de servicios

mask_ip.-mascar de red local_ip. Utilce 0 si la dirección es 0.

ip_forgein.-direcion ip de los host que va a acceder a la direction local_ip

mask_forgein.-mascar de la red ip_forgein.

Service.- este servicio se facilita a todos los servicios, el administrador puede limitar a uno o varios servicios, los valores posibles son any, ftp,http,telnet o protocolo/ puerto, any se utiliza para todos los servicios.

server_tag.-representa el nombre que se le dio al servidor aaa con el commando aaa new-model

Ejemplo:

pixfirewall(config)#access-list 101 permit tcp any host 192.168.4.1 eq ftp
pixfirewall(config)# access-list 101 permit tcp any host 192.168.4.1 eq www
pixfirewall(config)# aaa accounting match 101 outside MYTACACS
pixfirewall(config)# aaa accounting include any inside 0.0.0.0. 0.0.0.0 0.0.0.0 0.0.0.0 MYTACACS
pixfirewall(config)# aaa accounting exclude any inside 10.0.0.34. 2555.255.255.255 0.0.0.0 0.0.0.0 MYTACACS

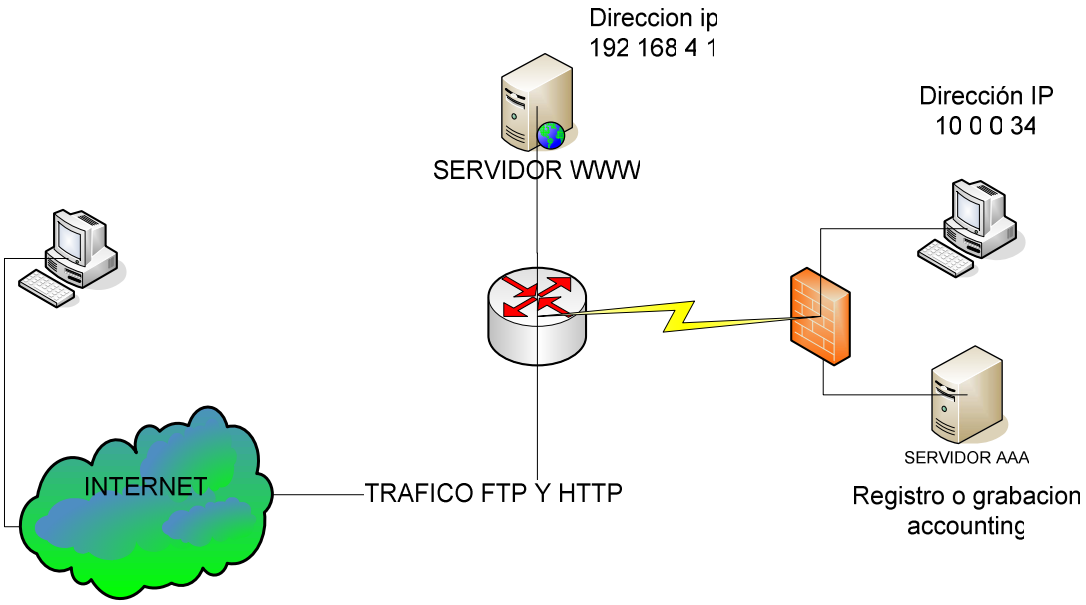


figura 5.27 configurar autorización

El registro de administración también es posible realizarlo, en el ejemplo siguiente se crea un usuario de administración en la base de datos del PIX, que se autentique por *telnet* y se crea un registro de este usuario.

Sintaxis:

aaa accounting [serial | telent | ssh | enable] console server

Ejemplo:

pixfirewall(config)#username administrador1 password cisco **pixfirewall(config)#aaa authentication telnet console LOCAL** **pixfirewall(config)# aaa accounting telnet console MYTACACS**

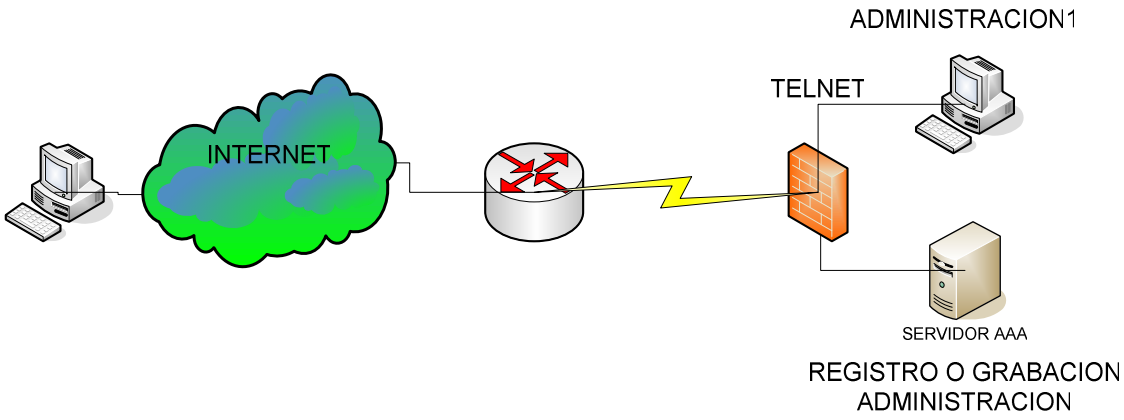


figura 5.28 configurar autorización de acceso a consola

5.5.8. Verificación De Configuración De aaa

El comando *show uauth* despliega todos los usuarios correctamente autenticados y la dirección IP con la que están accediendo a la red, en el ejemplo el usuario autenticado es *aaauser* con la dirección ip 192.168.1.10

Sintaxis:

show uauth

Ejemplo:

pixfirewall# show uauth

	Current	Most Seen
Authenticated Users	1	1
Authe In Progress	0	1

Para desplegar la estadística de el servidor o grupo de servidores aaa, en ele ejemplo el grupo de servidores de llama MYTACACS, utilizan el protocolo Tacacs+ y su direccion IP es la 10.0.0.2

Sintaxis:

show aaa-server

Ejemplo:

```
pixfirewall# show aaa-server

Server Group:          MYTACACS
Server Protocol:       tacacas+
Server Address:        10.0.0.2
Server Port:           49
Server Status:         ACTIVE, last transaction at 17:54:12  Mon Dec 29 2007
Number of authentication:          2
 Number of autorization:           1
```

Para poder verificar el comando auth-prompt configurado con anterioridad se emite el comando show auth-prompt

Sintaxis:

```
show aaa-prompt
```

Ejemplo:

```
pixfirewall# show aaa prompt

auth-prompt prompt Por favor ingresa tu usuario y contraseña
auth-prompt accept Autenticación exitosa
auth-prompt reject Usuario o contraseña incorrecta intenta nuevamente.
```

5.5.9 CONFIGURAR FILTROS En El PIX

5.5.9. INTRODUCCION OBJECT-GROUPS

Una lista de acceso le permite al PIX designar un cliente el acceso a un determinado servidor para un servicio específico, cuando hay un cliente, un *host*, o un servicio, con pocas líneas de listas de acceso es suficiente. Sin embargo cuando el número de clientes, servidores o servicios se incrementa, el número de líneas para las listas de acceso se incrementa exponencialmente.

Para simplificar la tarea de creación de nuevas listas de acceso, el administrador puede agrupar los llamados *object-group*, como son *host*, servicios, servidores, esto reduce

el numero de listas de acceso requerido para implementar complejas políticas de seguridad. Por ejemplo una política de seguridad podría requerir 3300 líneas mientras que con la utilización de *object-group* bastaría con unas 50 líneas.

Los *Object group* pueden ser:

Network.-usado para agrupar host, servidores o redes.

Protocol.- usado para agrupar protocolos, pueden ser icmp, tcp ,udp, tipo un entero entre 1 y 254 representado un protocolo IP.

Service.-usado para agrupar servicios TCP o UDP.

Icmp.-utilizado para agrupar mensajes ICMP

Para configurar object-group se sigue los siguientes pasos:

- ✓ Usar el comando object-group para ingresar y el subcomando respectivo dependiendo del grupo que se va a formar.
- ✓ Definir los miembros del object-group.
- ✓ Use el subcomando description para describir el grupo (opcional).
- ✓ Use el comando exit o quit para retormar al modo de configuración.
- ✓ Use show object-group para verificar los object-group que has sido configurados (opcional).
- ✓ Use show access-list para desplegar en pantalla las listas de acceso (opcional).

5.5.9. Configurar Object-Group

El comando utiliza es *object-group*, seguido de el grupo que se va a formar

Sintaxis:

object-group [network | protocol | service | icmp-type] name_group
port-object eq service
network-object host_ip | net_ip
protocol-object tcp | udp | tcp-udp
icmp-object icmp-type

Ejemplo:
Para el ejemplo vamos a tomar en cuenta la configuración del conjunto de listas de acceso de la facultad de electrónica.

access-list electro_acl permit tcp 192.188.58.208 255.255.255.248 any eq domain

access-list electro_acl permit udp 192.188.58.208 255.255.255.248 any eq domain

access-list electro_acl permit tcp 192.188.58.208 255.255.255.248 any eq pop3
access-list electro_acl permit tcp 192.188.58.208 255.255.255.248 any eq imap4
access-list electro_acl permit tcp 192.188.58.208 255.255.255.248 any eq ssh
access-list electro_acl permit tcp 192.188.58.208 255.255.255.248 any eq telnet
access-list electro_acl permit tcp 192.188.58.208 255.255.255.248 any eq smtp
access-list electro_acl permit tcp 192.188.58.208 255.255.255.248 any eq ftp
access-list electro_acl permit tcp 192.188.58.208 255.255.255.248 any eq https
access-list electro_acl permit tcp 192.188.58.208 255.255.255.248 any eq www
access-list electro_acl permit icmp any any
access-list electro_acl permit tcp 192.188.58.0 255.255.255.0 host 192.188.58.41 eq 1731
access-list electro_acl permit tcp 192.188.58.0 255.255.255.0 host 192.188.58.41 eq h323
access-list electro_acl permit tcp 192.188.58.0 255.255.255.0 host 192.188.58.41 eq 1503
access-list electro_acl permit tcp 192.188.58.0 255.255.255.0 host 192.188.58.41 eq ldap
access-list electro_acl permit tcp 192.188.58.0 255.255.255.0 host 192.188.58.41 eq 522

Primero formaremos el grupo de servicios

pixfirewall(config)#Object-group service electronica_servicios_externo
pixfirewall(config-service)#port-object eq domain
pixfirewall(config-service)#port-object eq pop3
pixfirewall(config-service)#port-object eq imap4
pixfirewall(config-service)#port-object eq ssh
pixfirewall(config-service)#port-object eq telnet
pixfirewall(config-service)#port-object eq smtp
pixfirewall(config-service)#port-object eq ftp
pixfirewall(config-service)#port-object eq https
pixfirewall(config-service)#port-object eq www
pixfirewall(config)#Object-group service electronica_servicios_interno
pixfirewall(config-service)#port-object eq 1731
pixfirewall(config-service)#port-object eq h323
pixfirewall(config-service)#port-object eq 1503
pixfirewall(config-service)#port-object eq Idap
pixfirewall(config-service)#port-object eq 522

A continuación crearemos el grupo de network:

```
pixfirewall(config)#Object-group  network electronica_redes_interna
pixfirewall(config-network)#network-object 192.188.58.208 netmask
255.255.255.248
pixfirewall(config-network)# network -object  192.188.58.0 netmask
255.255.255.0
pixfirewall(config)#Object-group  network electronica_host_externo
pixfirewall(config-service)#network-object host  192.188.58.41
```

El grupo de protocolo:

```
pixfirewall(config)#Object-group  protocol proto_grupo1
pixfirewall(config-service)#protocol-object tcp
pixfirewall(config-service)# protocol-object udp
```

Finalmente creamos la nueva lista de acceso:

```
pixfirewall(config)#access-list electro_acl permit object-group proto_grupo1
object-group electronica redes interna any object-group
electronica_servicios_externo

pixfirewall(config)# access-list electro_acl permit object-group proto_grupo1
interna object-group electronica redes interna object-group electronica
_host_externo object-group electronica_servicios_interno
```

5.5.9. Verificación De Object-Group

Los comandos utilizados para este propósito son:

Sintaxis:

show running-config object-group—muestra la listas de acceso configuradas.

show access-list <*acl*> —muestra las listas de acceso línea por línea, indica también las listas de acceso definidas para cada object-group.

clear object-group [*grp_type*]—cuando ingresamos sin ningún parámetro **clear object-group** remueve todos los object-group definidos, si escribimos el tipo remueve todos los object-group del recpectivo tipo.

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- ✓ El tráfico de Internet en la red de la ESPE, inicia a las 7:00 hasta las 21:30

- ✓ Durante este tiempo, la hora de mayor tráfico oscila a las 11:30 hasta las 14:00, teniendo valores pico de 15Mbps hasta 22Mbps.

- ✓ En el horario de la tarde comprendido desde las 14:00 a 21:30, el tráfico de Internet tiene un promedio de 7Mbps a 6Mbps.

- ✓ Durante los días sábado y domingo el tráfico baja hasta un promedio de 1Mbps a 2Mbps.

6.2 RECOMENDACIONES

- ✓ Fragmentación de la red en Vlan, teniendo en cuenta el Orgánico Estructural de la ESPE.

- ✓ Actualizar el servidor DCHP, a fin de evitar la duplicación de direcciones ip.

- ✓ Bloquear el trafico ICMP desde la red externa a la red interna, en el Cisco PIX.

- ✓ Configurar el protocolo Spanning Tree, a fin de evitar la caída de los switch, debido a formación de lazos o bucles.

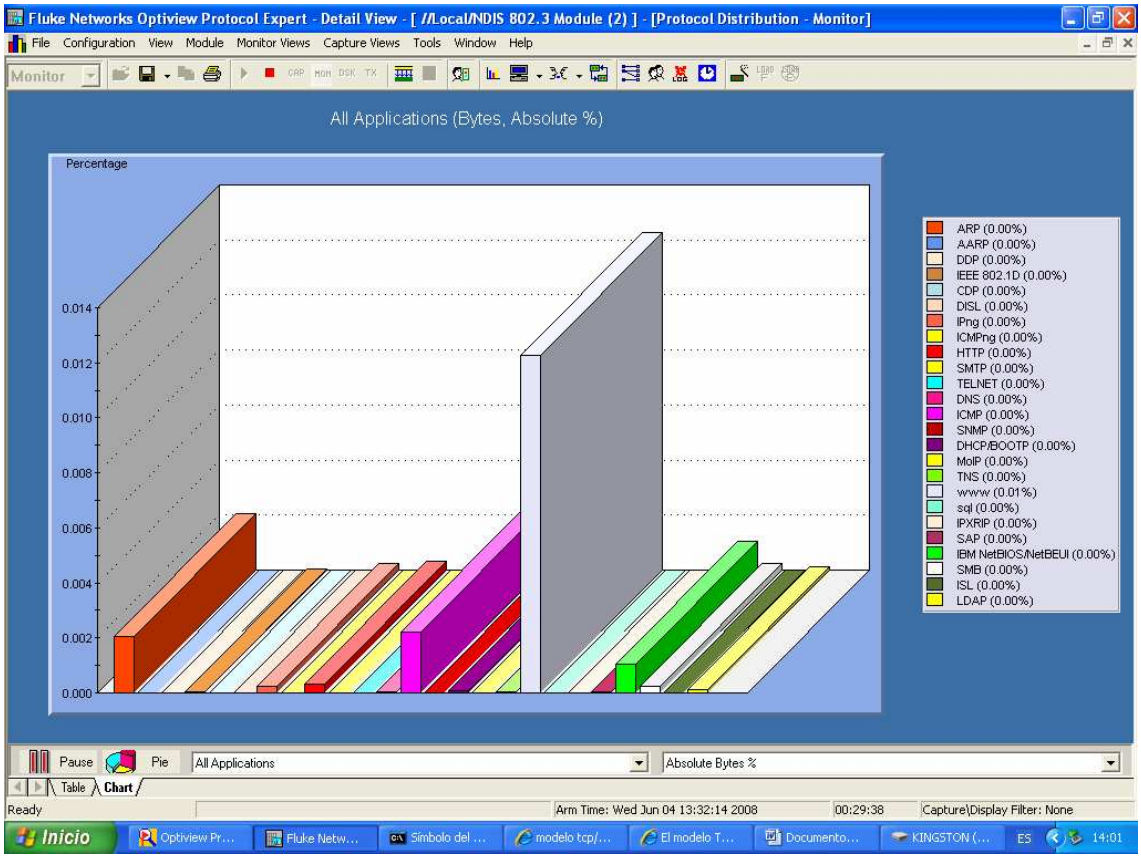
- ✓ Actualizar periódicamente las páginas prohibidas y pornografía en el ISA Server.

- ✓ Implementar un servidor AAA, para el control de acceso a la red, o el control de los administradores de Firewall.

- ✓ Para mejorar la configuración de las listas de acceso en el PIX, se recomienda crear los Object-Group, para una rápido y eficaz administración.

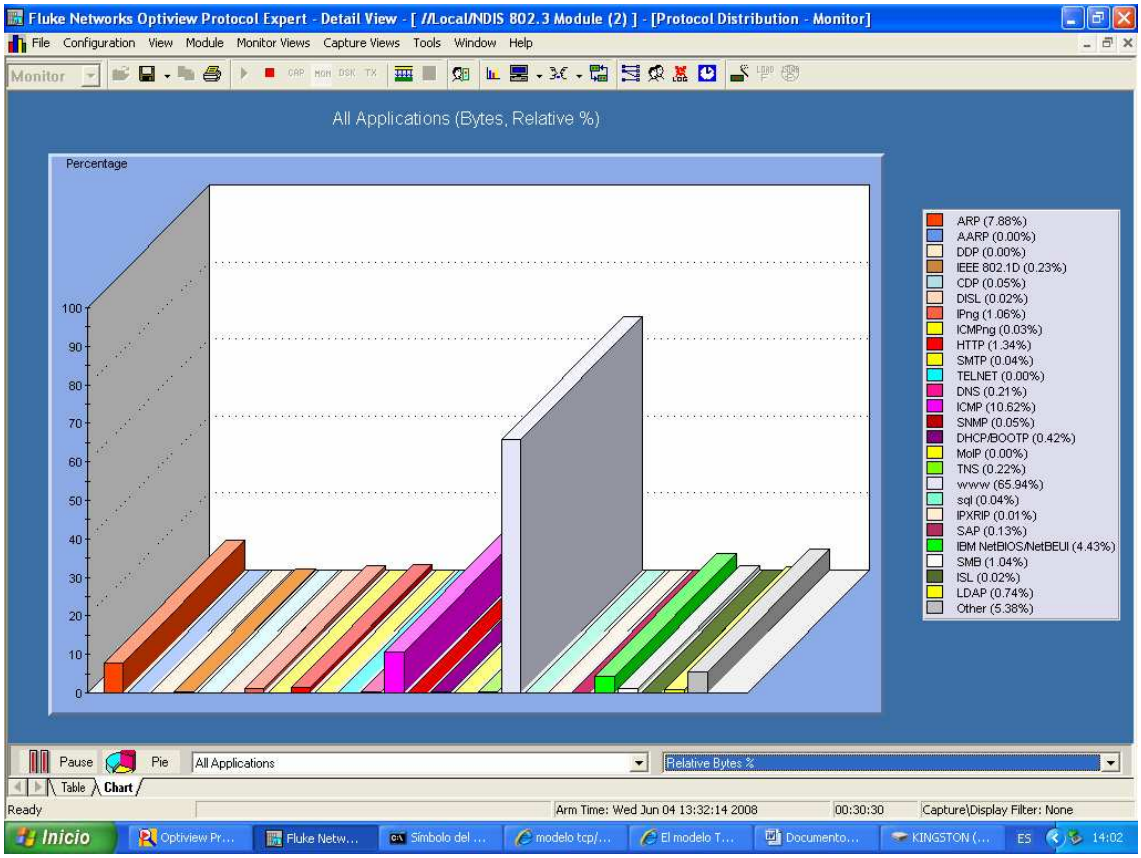
- ✓ Creación de grupos de administradores para el Cisco Pix, y un servidor AAA para el llevar la autenticación, autorización y administración de cuentas del personal a cargo del Firewall.

A1
14:00 PM
GRAFICO ABSOLUTO



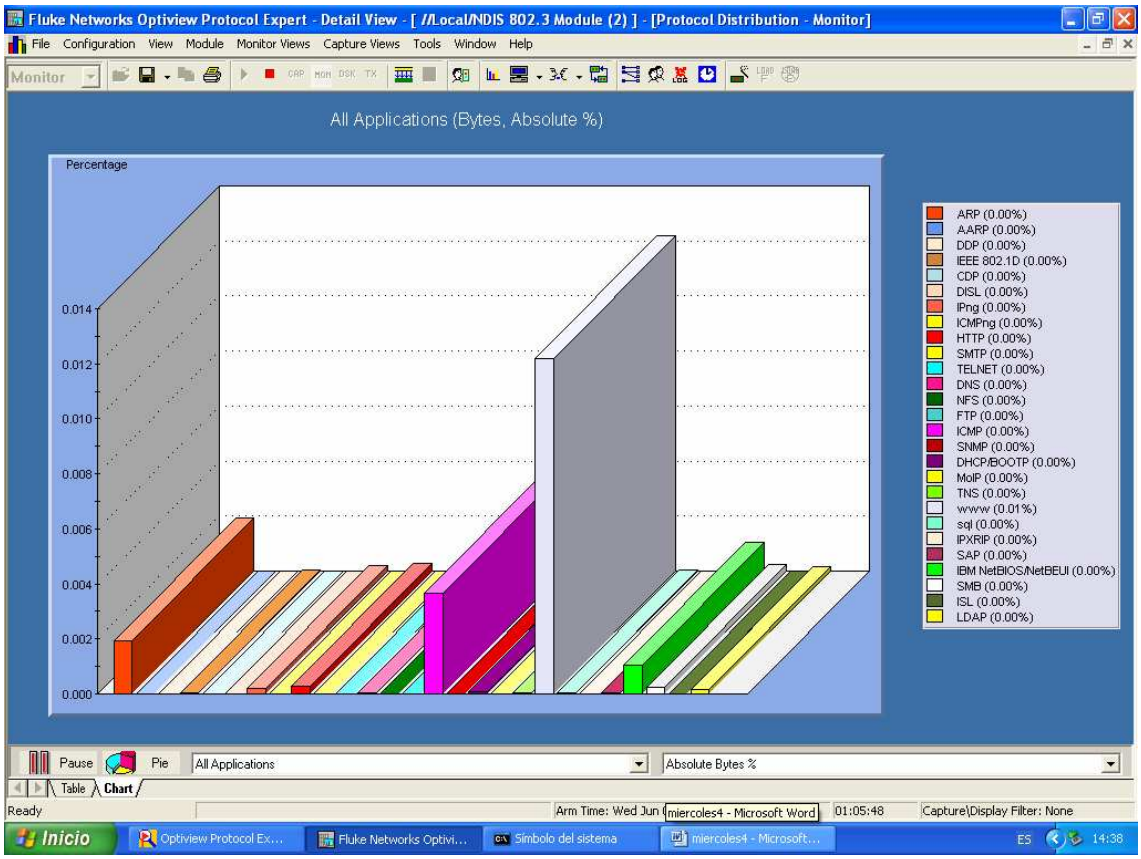
ARP	2	Mbps
IPv6	200	Kbps
http	300	Kbps
ICMP	2.1	Mbps
DHCP	50	Kbps
WWW	15.5	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	250	Kbps

A2
GRAFICO RELATIVO



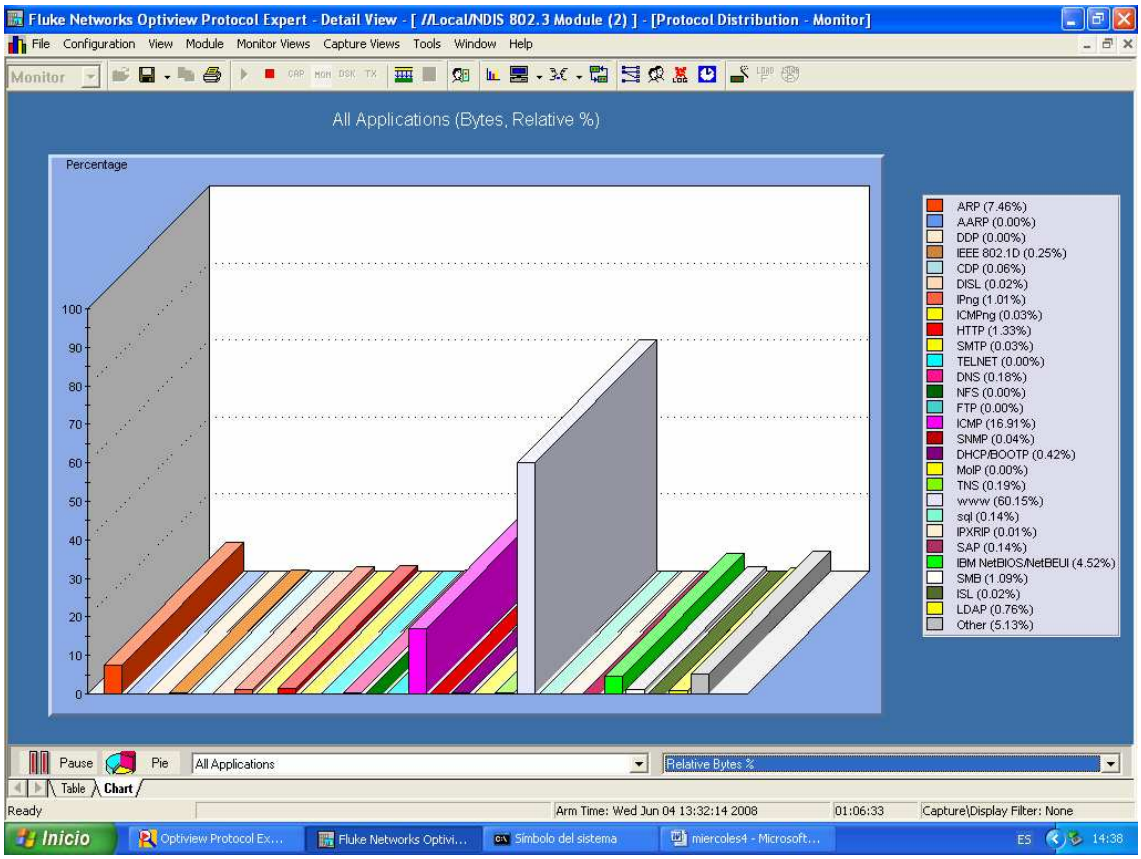
ARP	7.56%
802.1D	0.22%
IPv6	0.97%
http	1.29%
ICMP	10.03%
DHCP	0.37%
WWW	67.58%
NETBIOS	4.18%
SMB	0.94%
LDAP	0.83%
Otros	5.07%

A3
14:30 PM
GRAFICO ABSOLUTO



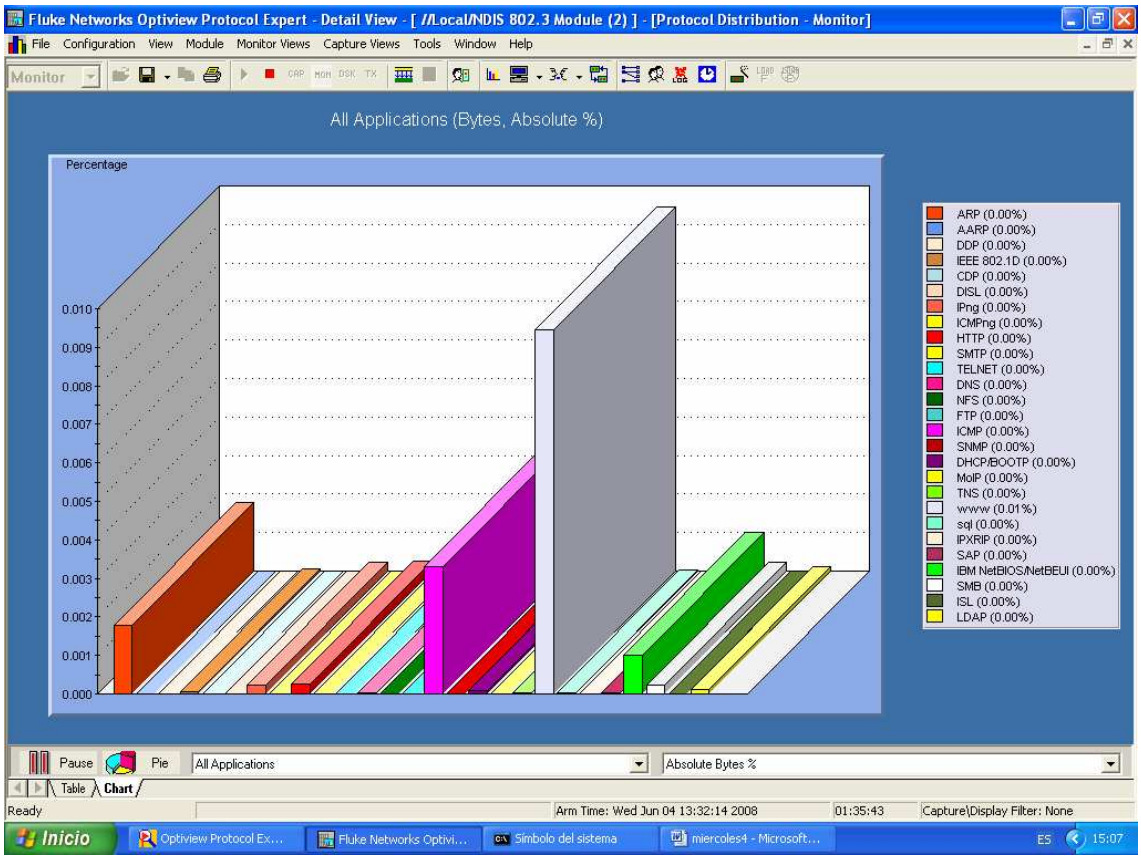
ARP	1.9	Mbps
IPv6	250	Kbps
http	350	Kbps
ICMP	3.3	Mbps
DHCP	100	Kbps
WWW	11.7	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	200	Kbps

A4
GRAFICO RELATIVO



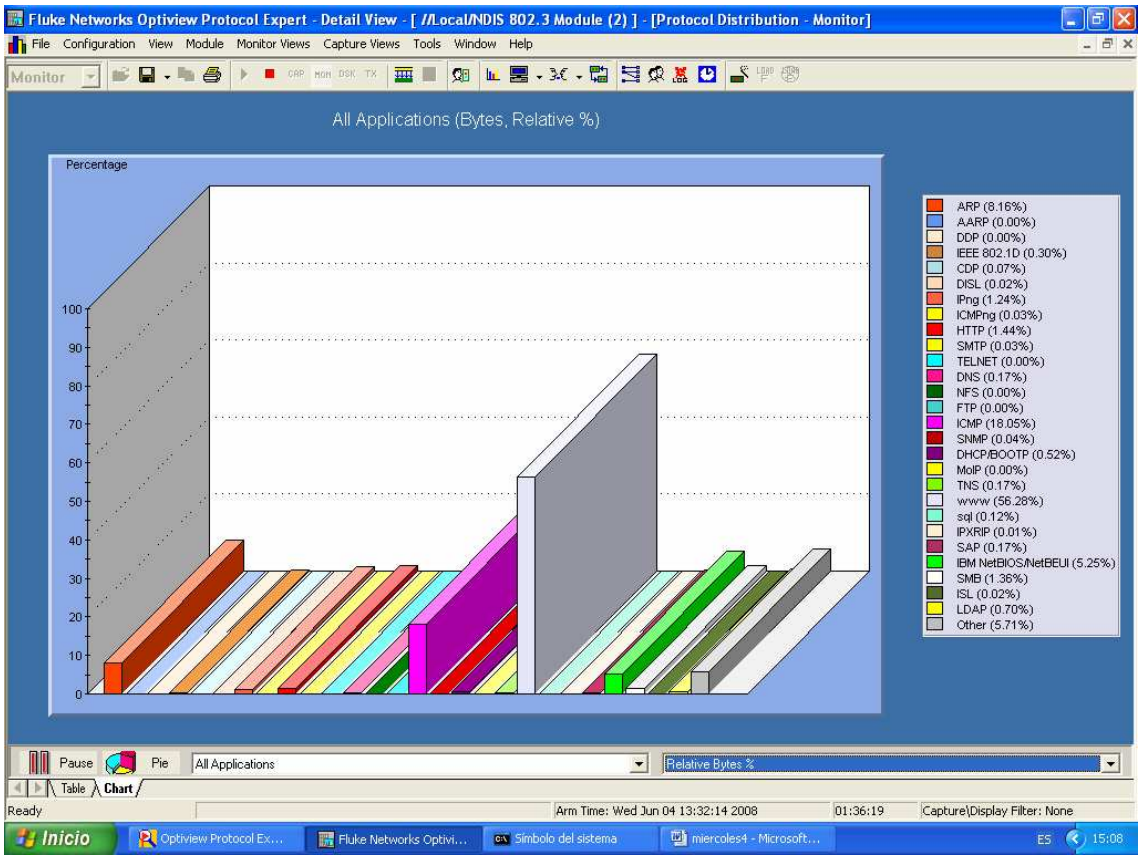
ARP	7.60%
802.1D	0.22%
IPv6	1.07%
http	1.36%
ICMP	16.76%
DHCP	0.45%
WWW	59.51%
NETBIOS	4.75%
SMB	1.16%
LDAP	0.75%
Otros	5.37%

A5
15:00 PM
GRAFICO ABSOLUTO



ARP	1.8	Mbps
802.1D	100	Kbps
IPv6	300	Kbps
http	400	Kbps
ICMP	3.3	Mbps
DHCP	100	Kbps
WWW	9	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

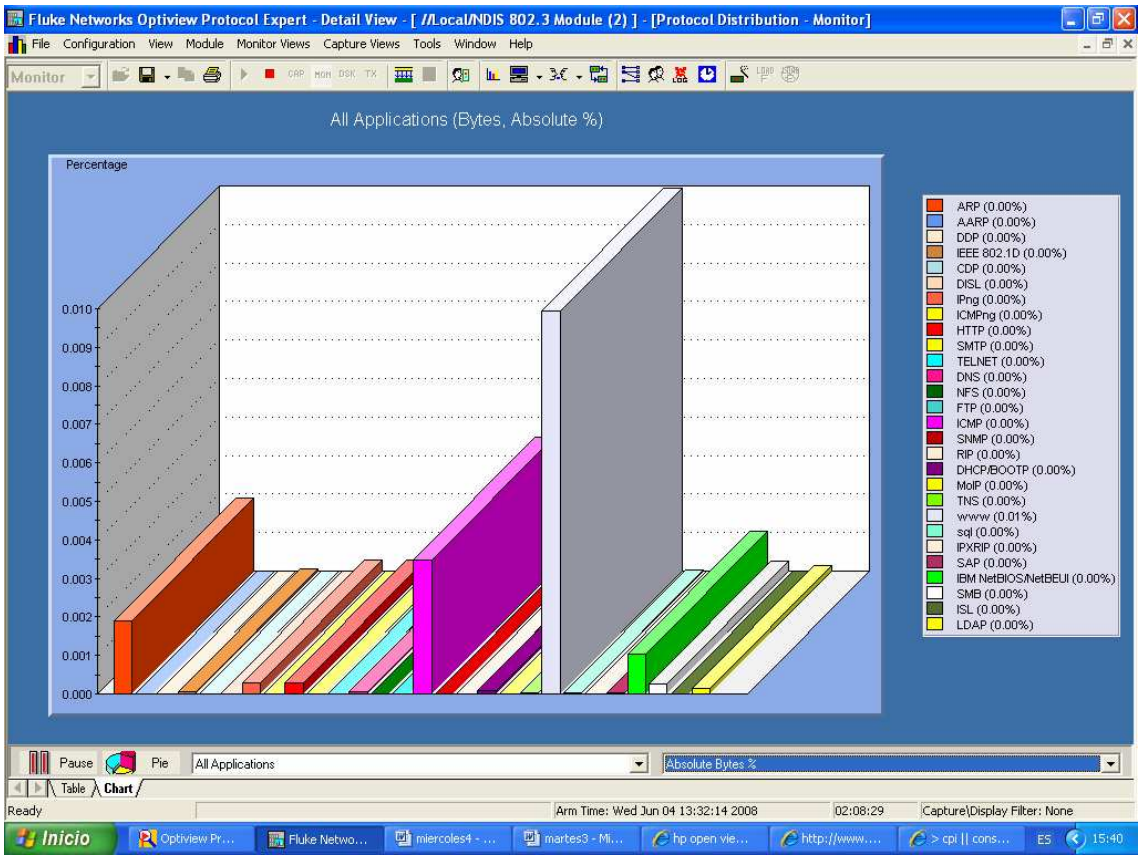
A6
GRAFICO RELATIVO



ARP	8.13%
802.1D	0.31%
IPv6	1.33%
http	1.44%
ICMP	19.29%
DHCP	0.52%
WWW	55.03%
NETBIOS	5.26%
SMB	1.40%
LDAP	0.69%
Otros	5.67%

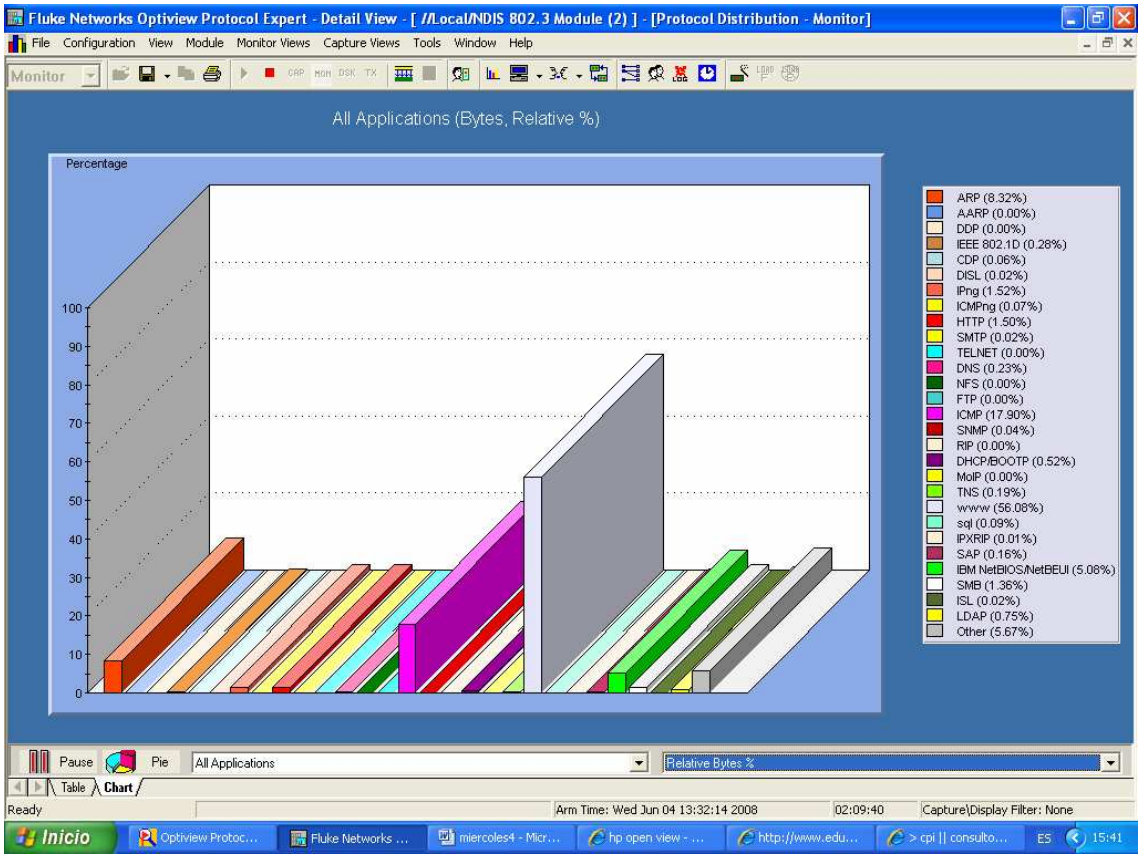
A7
15:30

GRAFICO ABSOLUTO



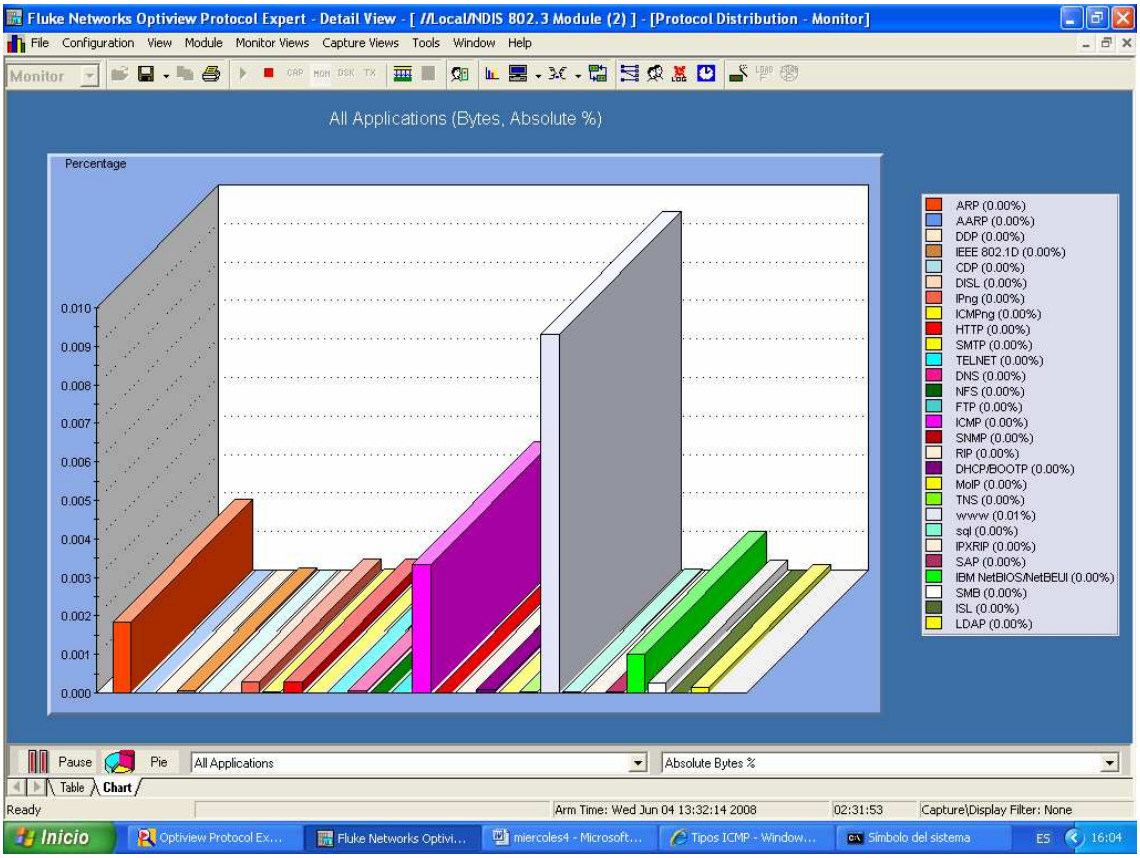
ARP	1.8	Mbps
802.1D	100	Kbps
IPv6	300	Kbps
http	400	Kbps
ICMP	3.3	Mbps
DHCP	100	Kbps
WWW	10	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A8
GRAFICO RELATIVO



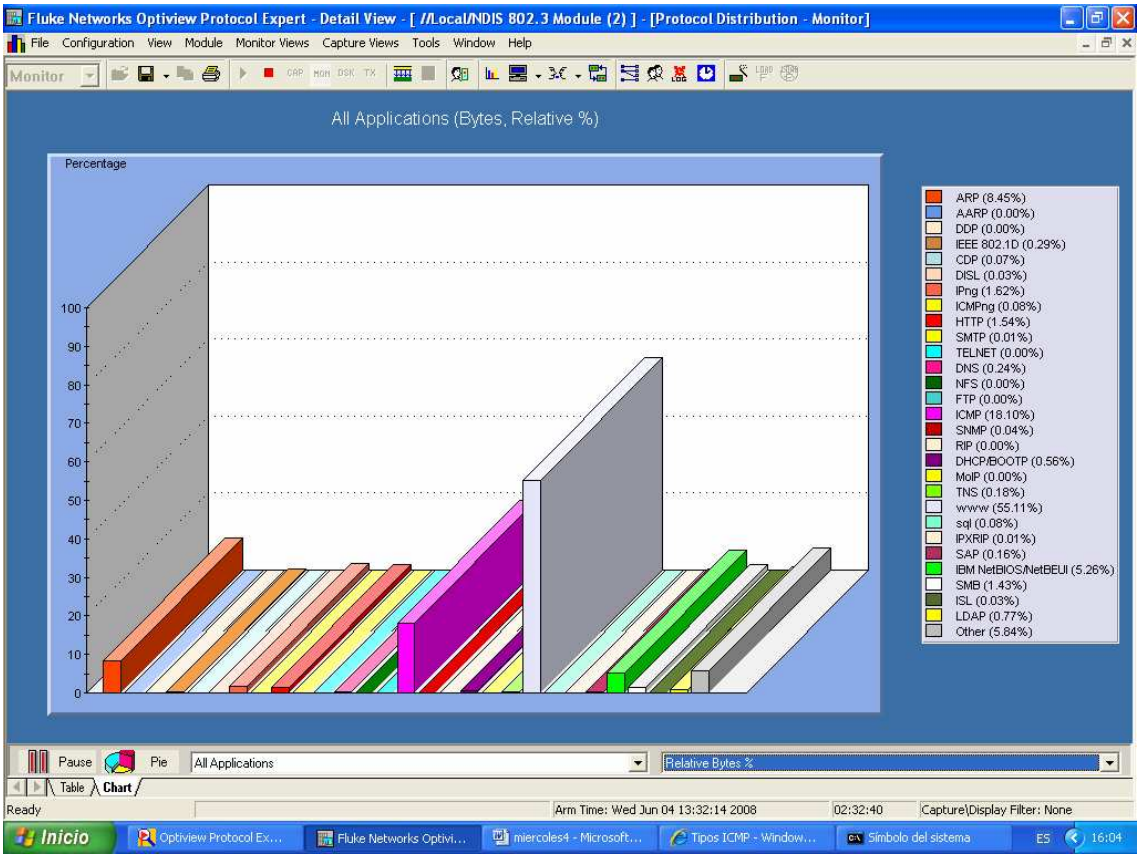
ARP	8.35%
802.1D	0.28%
IPv6	1.33%
http	1.44%
ICMP	17.90%
DHCP	0.52%
WWW	55.83%
NETBIOS	5.15%
SMB	1.38%
LDAP	0.75%
Otros	5.71%

A9
16:00
GRAFICO ABSOLUTO



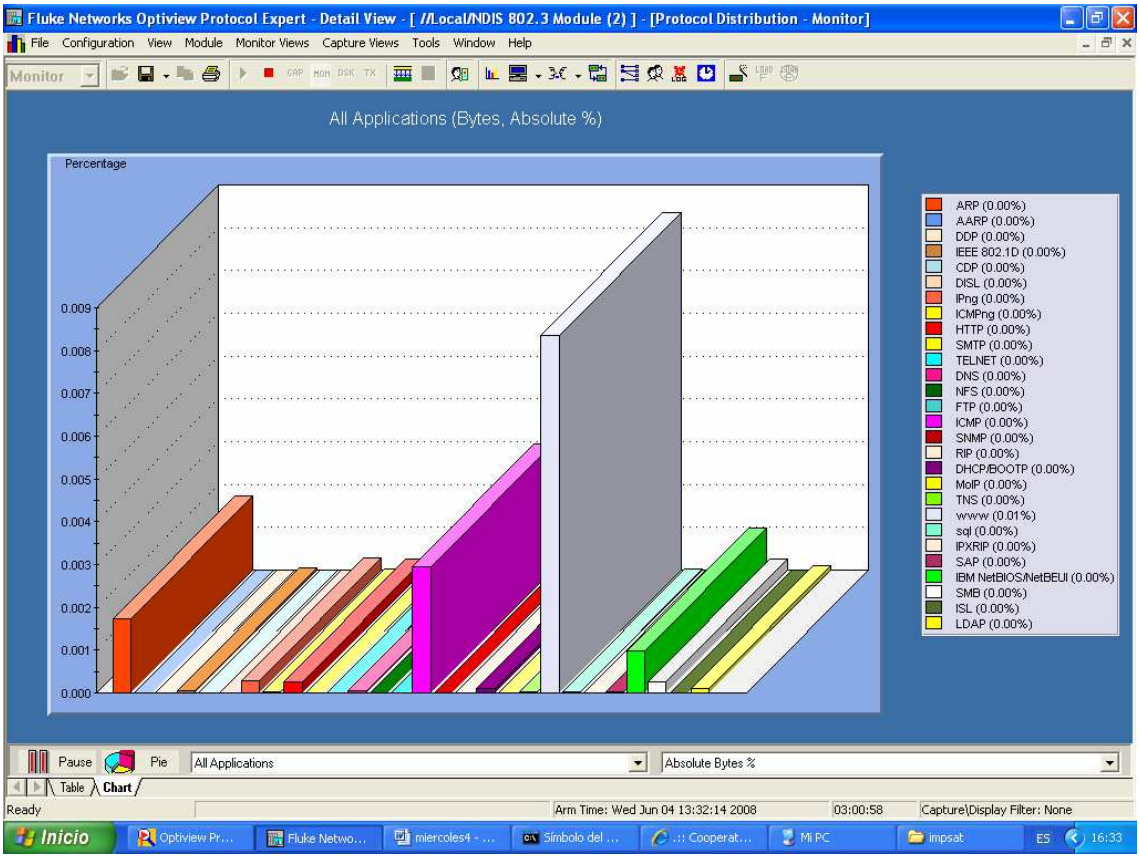
ARP	1.8	Mbps
802.1D	100	Kbps
IPv6	300	Kbps
http	400	Kbps
ICMP	3.3	Mbps
DHCP	100	Kbps
WWW	9.3	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A10
GRAFICO RELATIVO



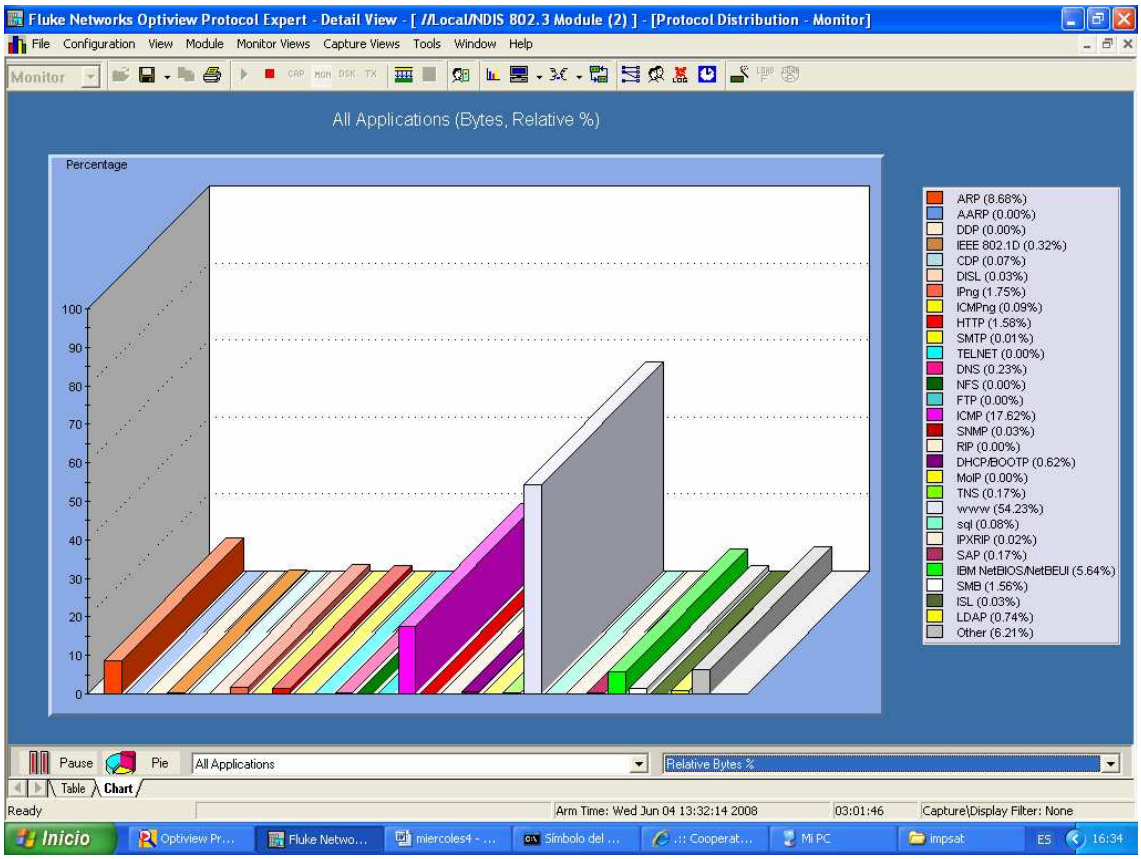
ARP	8.48%
802.1D	0.30%
IPv6	1.62%
http	1.60%
ICMP	18.05%
DHCP	0.57%
WWW	54.96%
NETBIOS	5.15%
SMB	5.32%
LDAP	1.45%
Otros	5.91%

A11
16:30 PM
GRAFICO ABSOLUTO



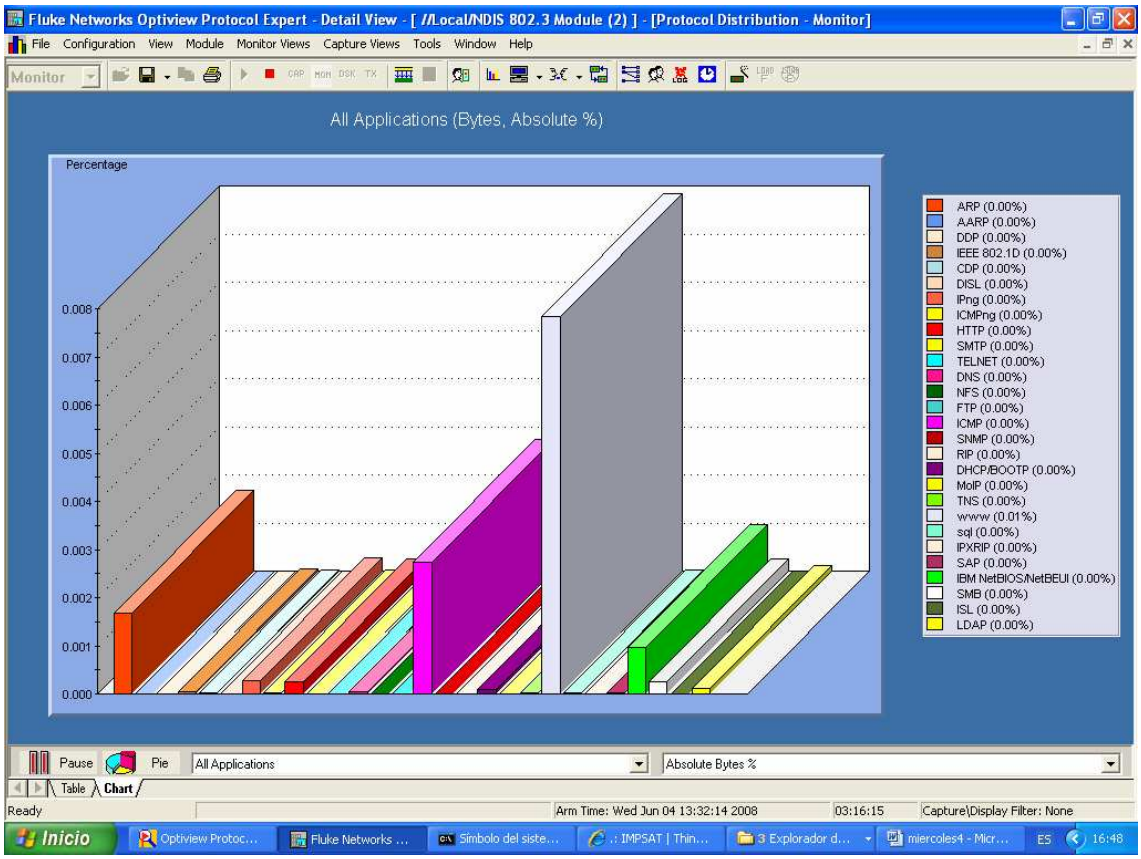
ARP	1.7	Mbps
802.1D	100	Kbps
IPv6	350	Kbps
http	300	Kbps
ICMP	2.8	Mbps
DHCP	100	Kbps
WWW	8.3	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A12
GRAFICO RELATIVO



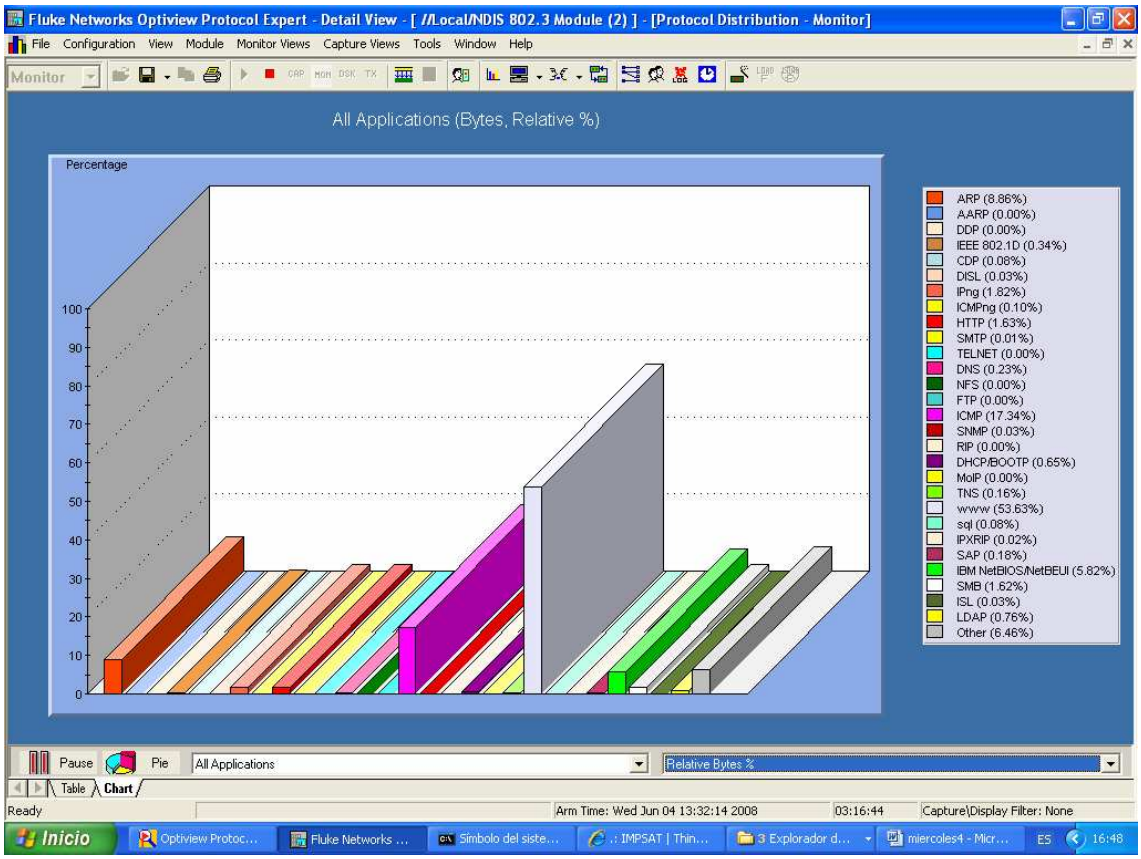
ARP	8.71%
802.1D	0.33%
IPv6	1.76%
http	1.60%
ICMP	17.57%
DHCP	0.63%
WWW	54.06%
NETBIOS	5.71%
SMB	1.59%
LDAP	0.74%
Otros	6.30%

A13
17:00 PM
GRAFICO ABSOLUTO



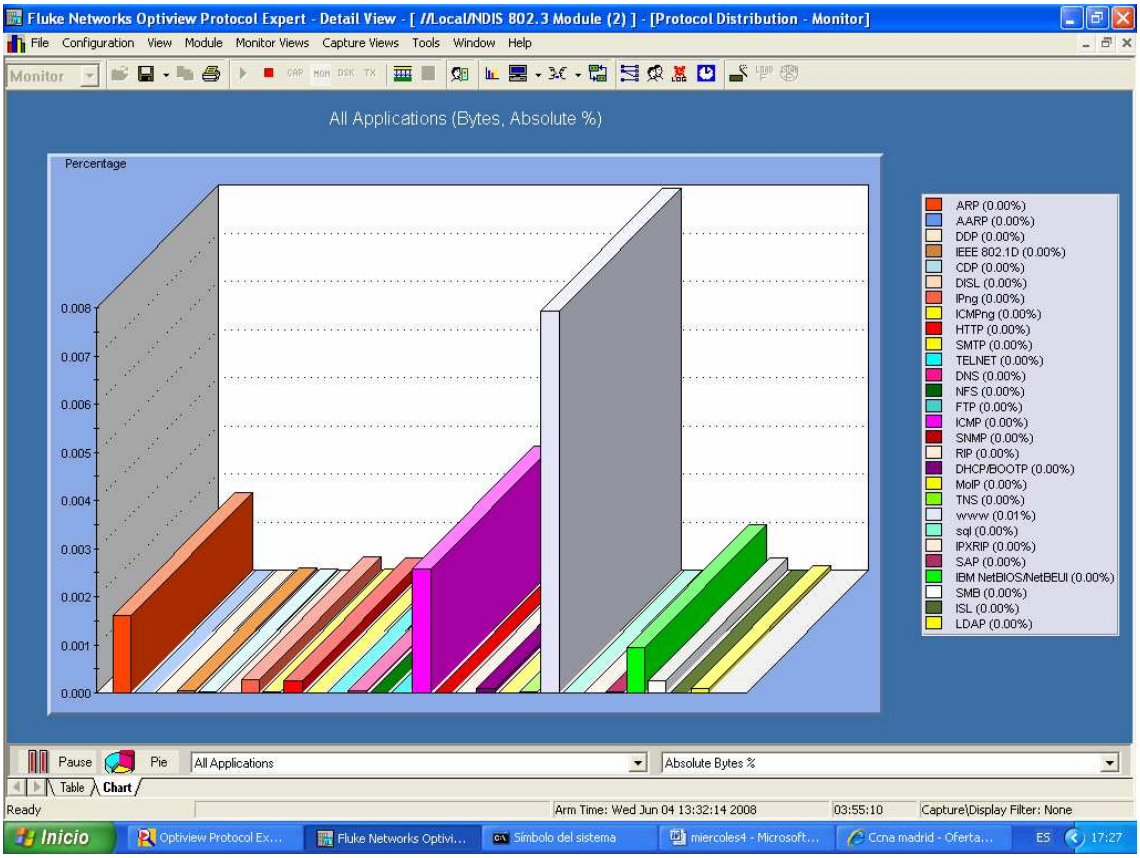
ARP	1.7	Mbps
802.1D	50	Kbps
IPv6	350	Kbps
http	300	Kbps
DNS	50	Kbps
ICMP	2.8	Mbps
DHCP	100	Kbps
WWW	7.8	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A14
GRAFICO RELATIVO



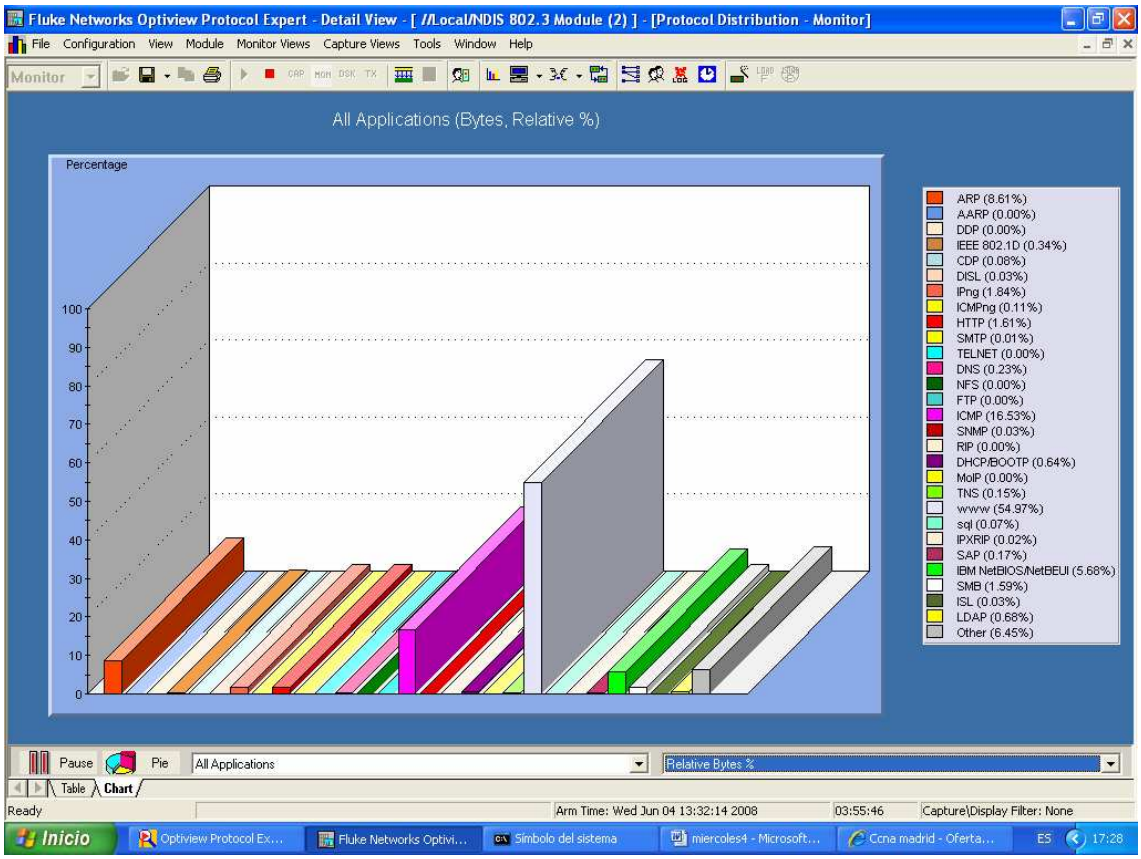
ARP	8.91%
802.1D	0.35%
IPv6	1.85%
http	1.64%
ICMP	17.27%
DHCP	0.66%
WWW	53.37%
NETBIOS	5.90%
SMB	1.65%
LDAP	0.75%
Otros	6.57%

A15
17:30 PM
GRAFICO ABSOLUTO



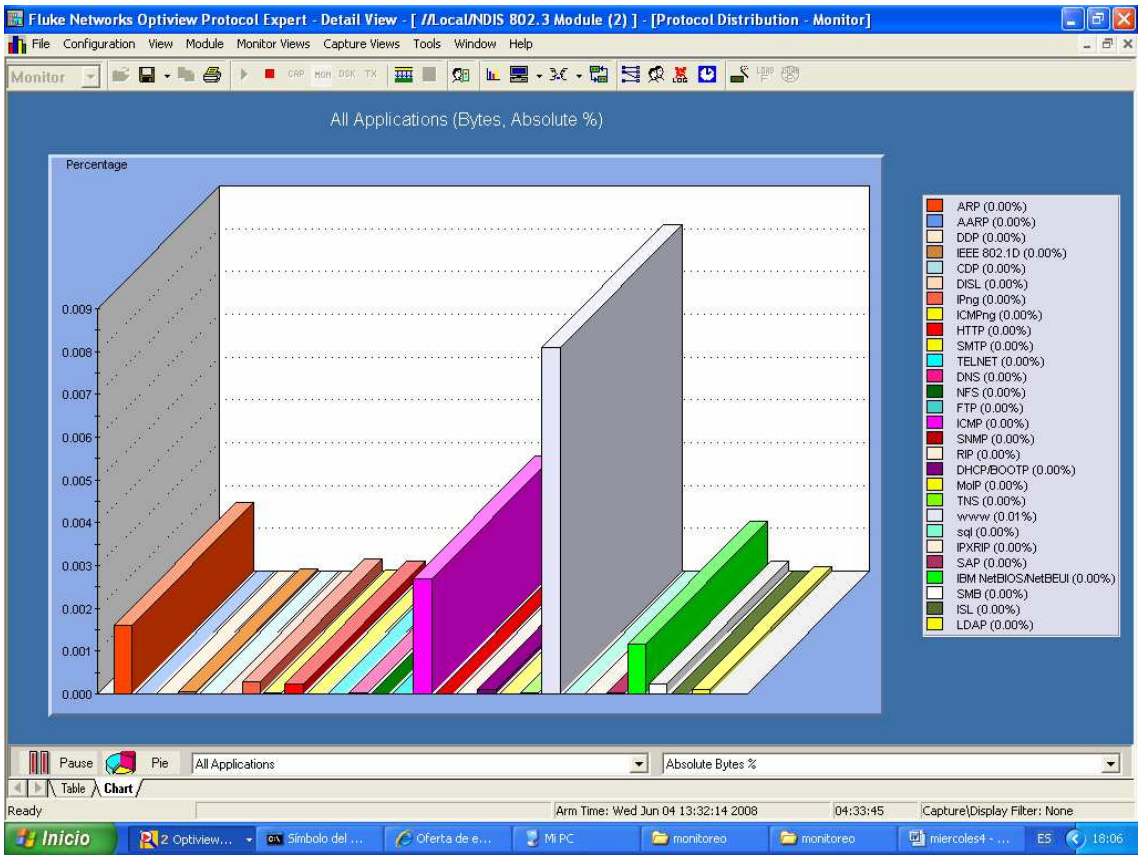
ARP	1.6	Mbps
802.1D	50	Kbps
IPv6	350	Kbps
http	300	Kbps
DNS	50	Kbps
ICMP	2.8	Mbps
DHCP	100	Kbps
WWW	8	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A16
GRAFICO RELATIVO



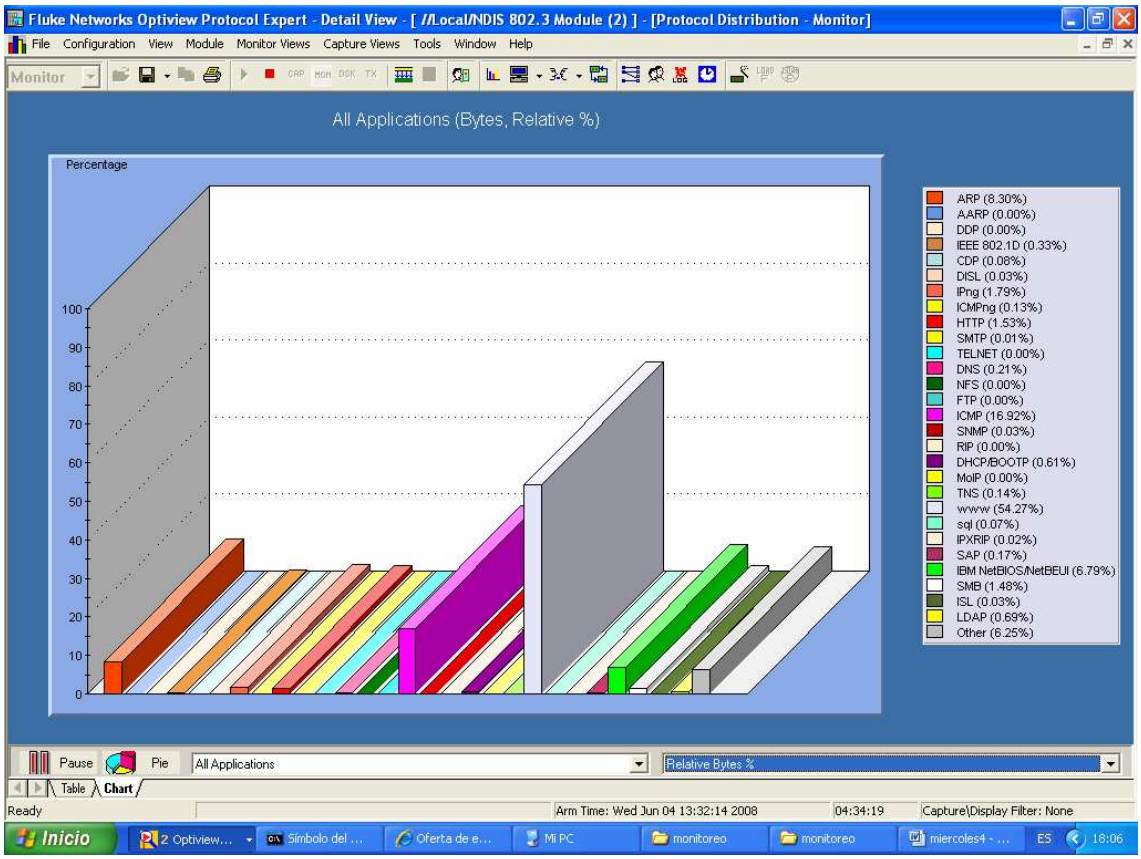
ARP	8.52%
802.1D	0.34%
IPv6	1.84%
http	1.59%
ICMP	16.59%
DHCP	0.66%
WWW	55.16%
NETBIOS	5.61%
SMB	1.57%
LDAP	0.68%
Otros	6.42%

A17
18:00 PM
GRAFICO ABSOLUTO



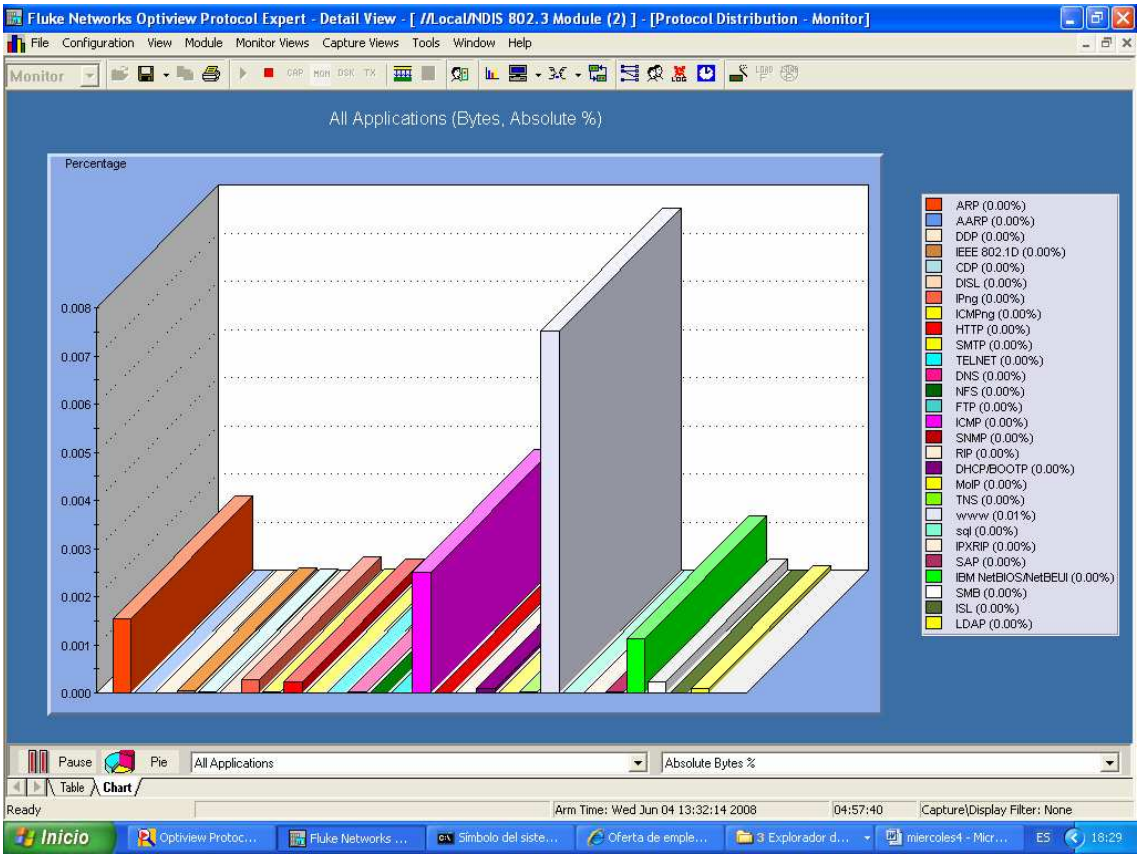
ARP	1.6	Mbps
802.1D	50	Kbps
IPv6	350	Kbps
http	300	Kbps
DNS	0	Kbps
ICMP	2.8	Mbps
DHCP	100	Kbps
WWW	8.1	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A18
GRAFICO RELATIVO



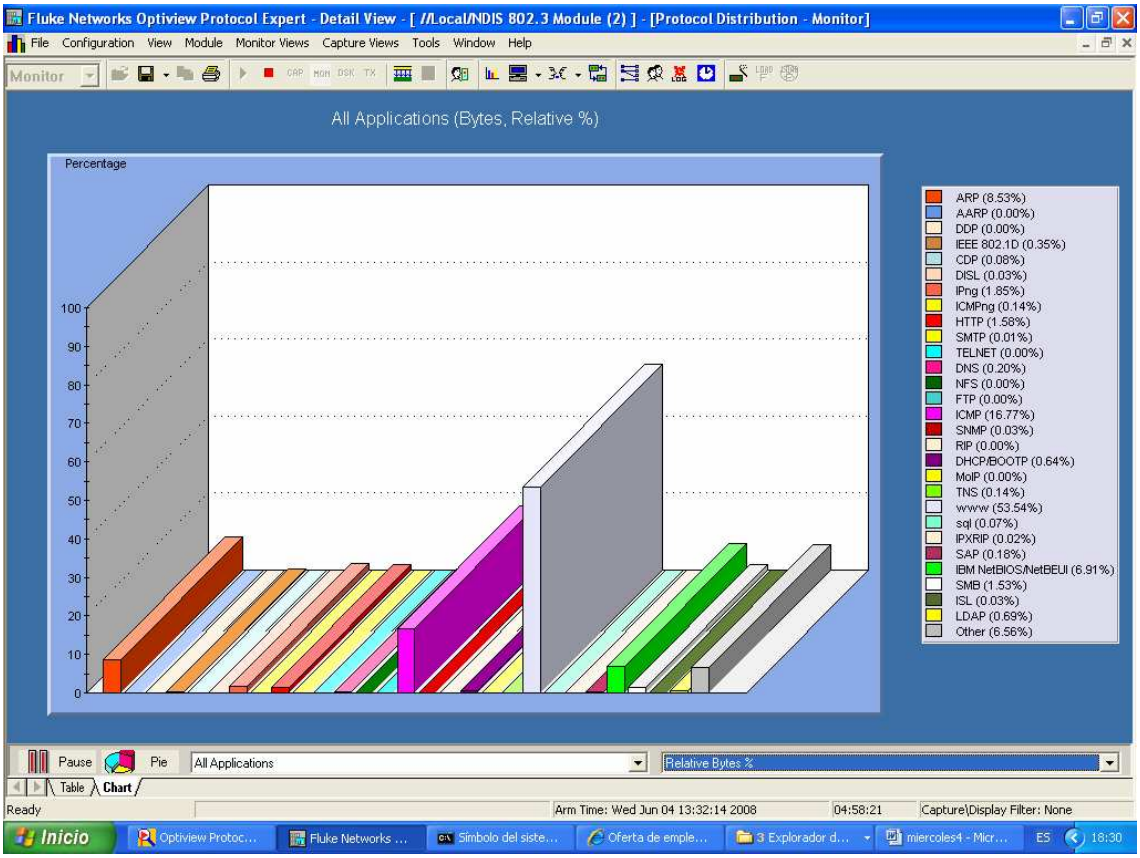
ARP	8.33%
802.1D	0.34%
IPv6	1.80%
http	1.54%
ICMP	16.89%
DHCP	0.62%
WWW	54.13%
NETBIOS	5.83%
SMB	1.49%
LDAP	0.69%
Otros	6.32%

A19
18:30 PM
GRAFICO ABSOLUTO



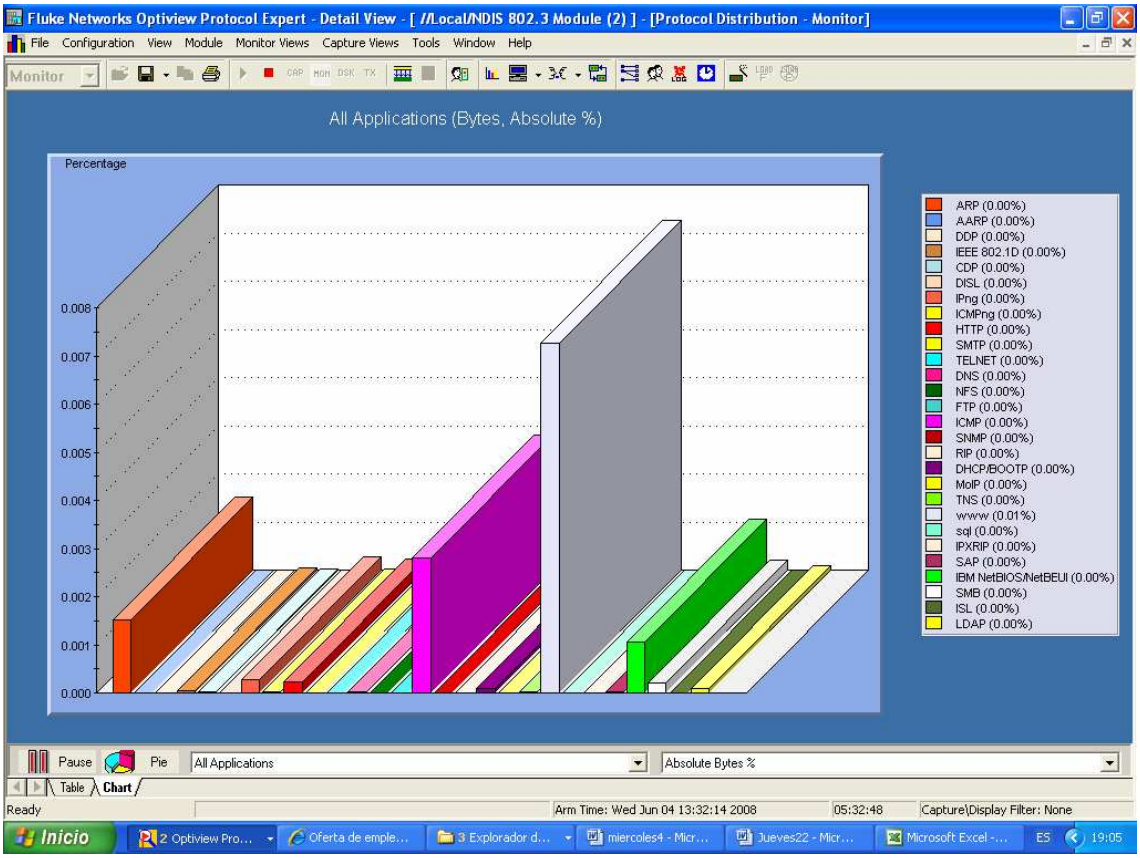
ARP	1.75	Mbps
802.1D	50	Kbps
IPv6	350	Kbps
http	300	Kbps
DNS	0	Kbps
ICMP	2.5	Mbps
DHCP	100	Kbps
WWW	7.7	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A20
GRAFICO RELATIVO



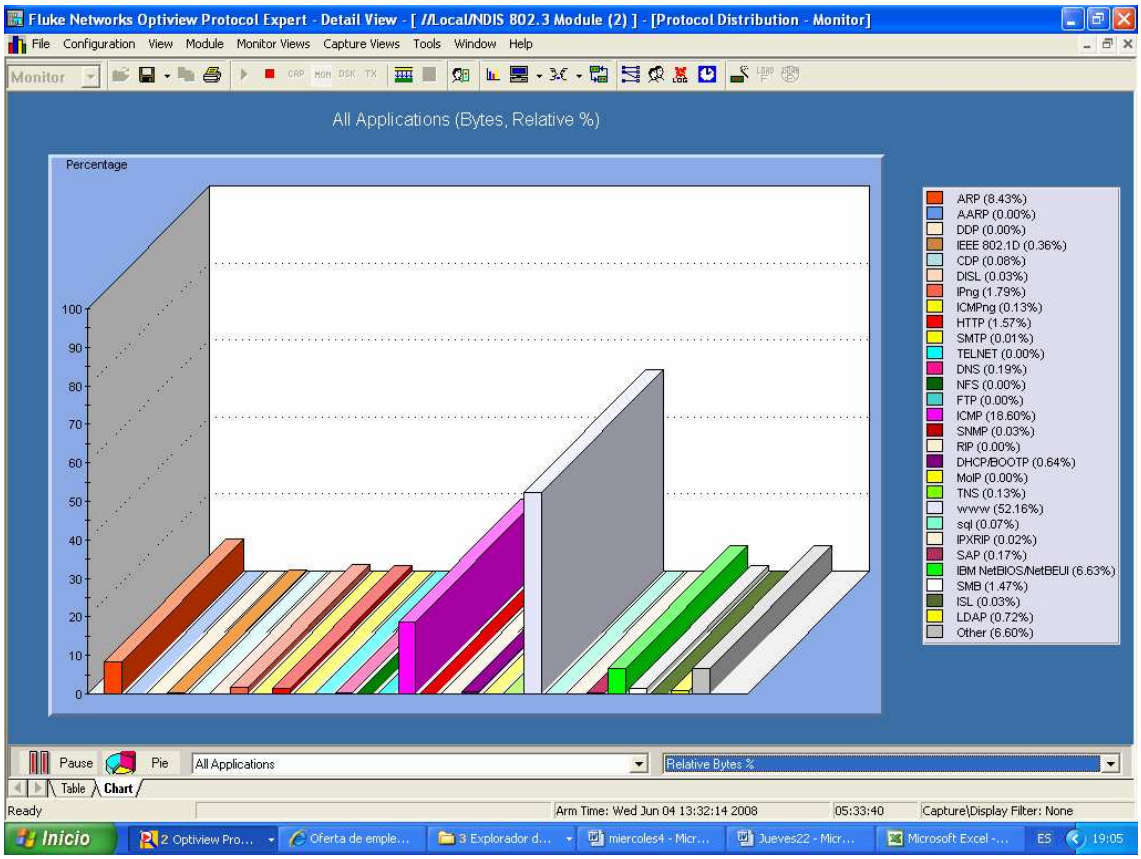
ARP	8.49%
802.1D	0.35%
IPv6	1.48%
http	1.58%
ICMP	16.86%
DHCP	0.64%
WWW	53.50%
NETBIOS	6.89%
SMB	1.52%
LDAP	0.69%
Otros	6.59%

A21
19:00
GRAFICO ABSOLUTO



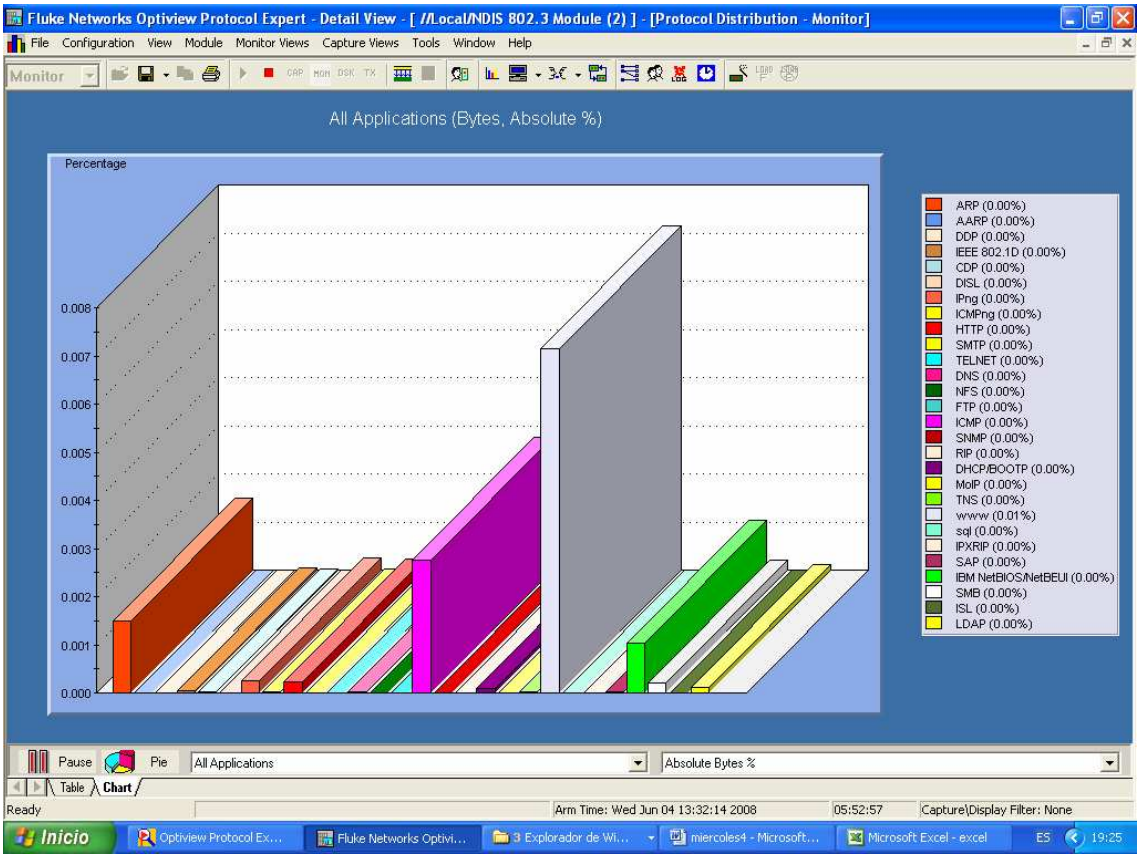
ARP	1.5	Mbps
802.1D	50	Kbps
IPv6	350	Kbps
http	300	Kbps
ICMP	2.8	Mbps
DHCP	100	Kbps
WWW	7.3	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A22
GRAFICO RELATIVO



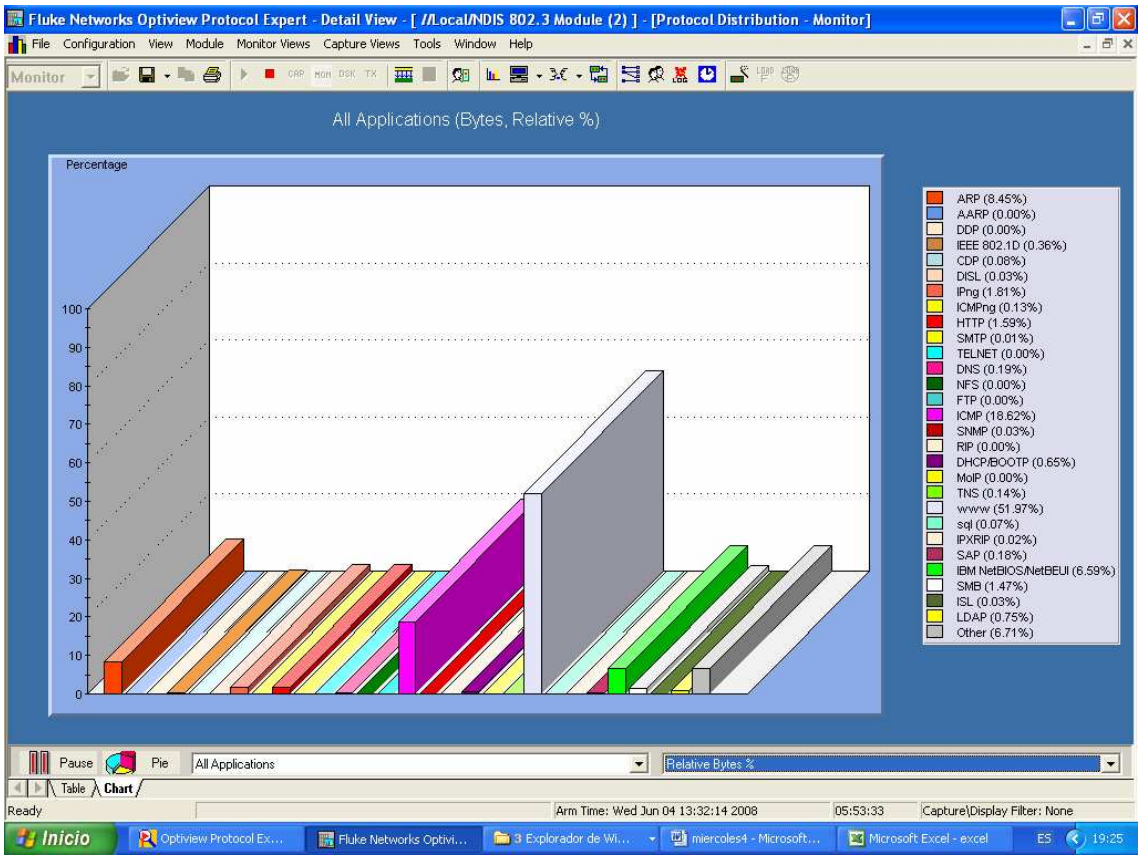
ARP	8.44%
802.1D	0.36%
IPv6	1.78%
http	1.58%
ICMP	18.61%
DHCP	0.64%
WWW	52.17%
NETBIOS	6.59%
SMB	1.46%
LDAP	0.74%
Otros	6.59%

A23
19:30 PM
GRAFICO ABSOLUTO



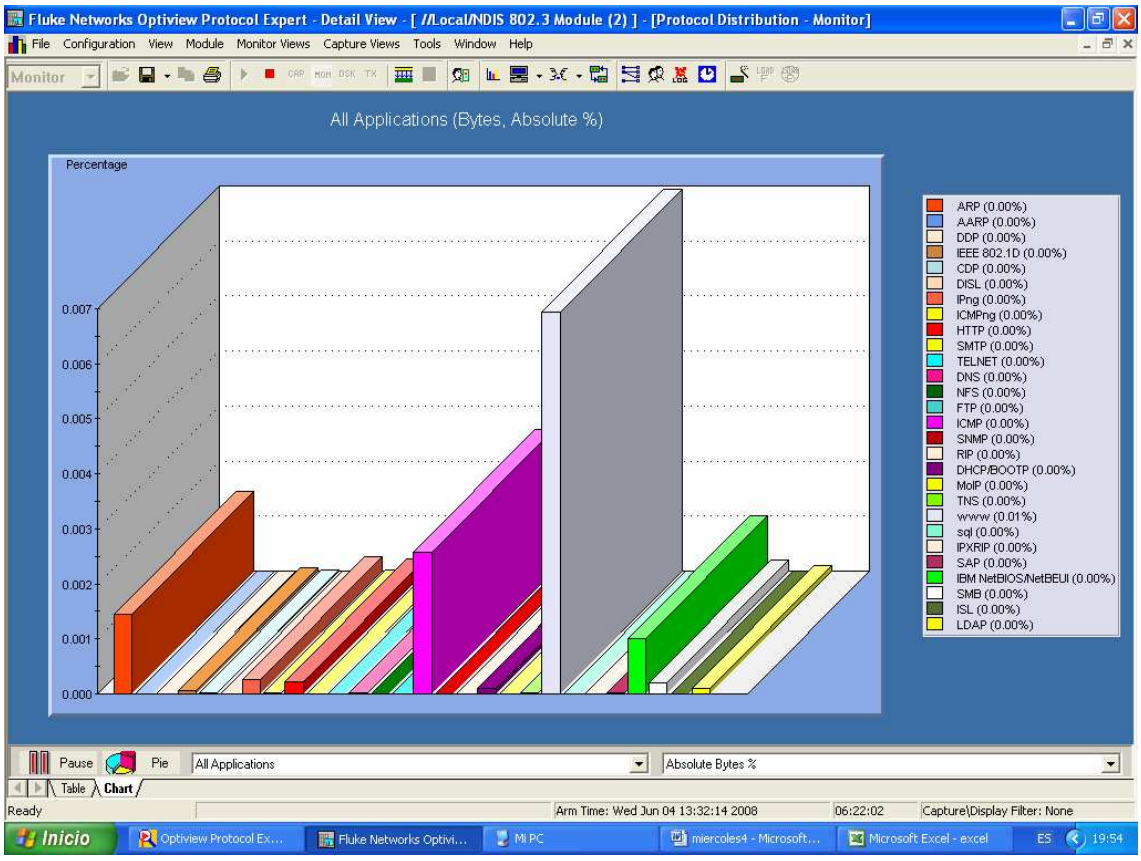
ARP	1.5	Mbps
802.1D	50	Kbps
IPv6	350	Kbps
http	300	Kbps
ICMP	2.8	Mbps
DHCP	100	Kbps
WWW	7.3	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A24
GRAFICO RELATIVO



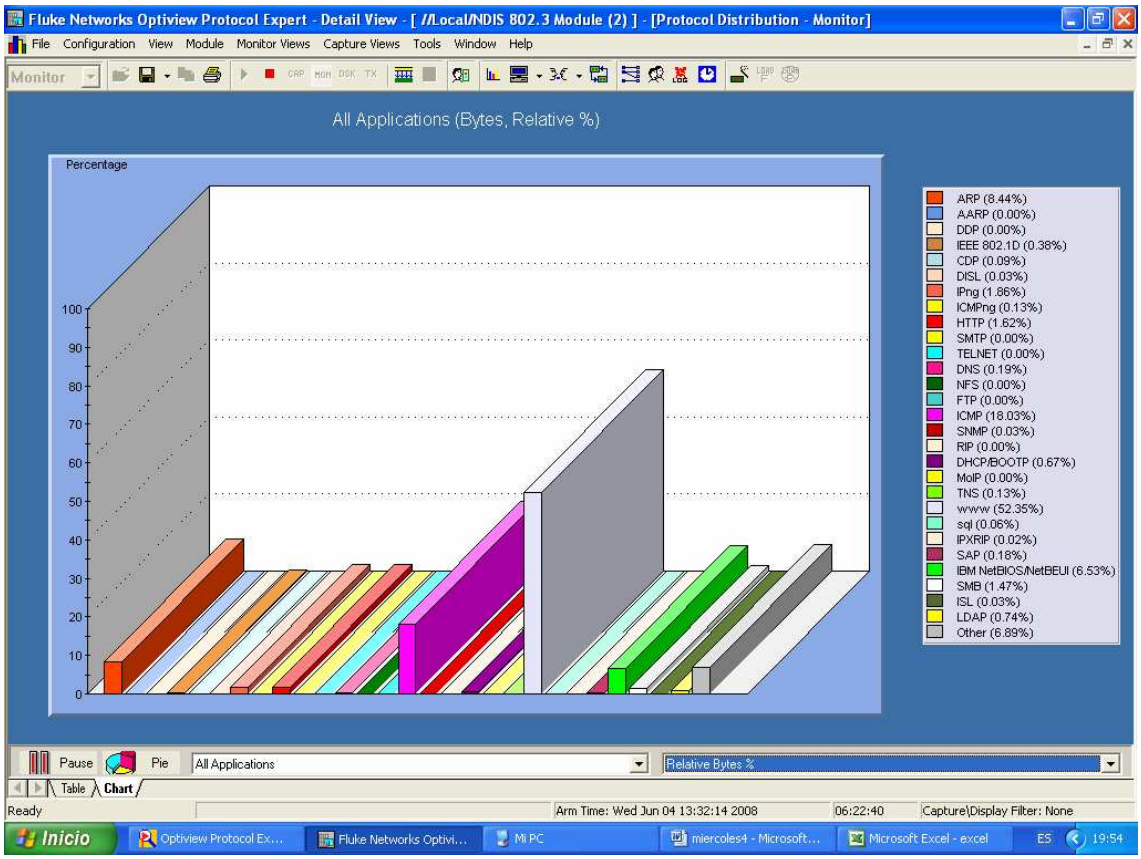
ARP	8.46%
802.1D	0.36%
IPv6	1.81%
http	1.60%
ICMP	18.60%
DHCP	0.65%
WWW	51.92%
NETBIOS	6.60%
SMB	1.47%
LDAP	0.75%
Otros	6.74%

A25
20:00
GRAFICO ABSOLUTO



ARP	1.5	Mbps
802.1D	50	Kbps
IPv6	350	Kbps
http	300	Kbps
ICMP	2.8	Mbps
DHCP	100	Kbps
WWW	7.3	Mbps
NETBIOS	1	Mbps
SMB	250	Kbps
LDAP	100	Kbps

A26
GRAFICO RELATIVO



ARP	8.45%
802.1D	0.38%
IPv6	1.88%
http	1.62%
ICMP	18.01%
DHCP	0.68%
WWW	52.29%
NETBIOS	6.54%
SMB	1.47%
LDAP	0.74%
Otros	6.92%

A27
PROMEDIO DE TRÁFICO

ABSOLUTO

Trafico ARP	1.7	Mbps
Trafico 802.1d	100	Kbps
Tráfico IPv6	319	Kbps
Trafico http	295	Kbps
ICMP	2.8	Mbps
Dhcp	100	Kbps
Trafico www	8.3	Mbps
Netbios	1.0	Mbps
Smb	250	Kbps
Ldap	100	Kbps
Otros	900	Kbps

RELATIVO

Trafico ARP	10.71%
Trafico 802.1d	0.63%
Tráfico IPv6	2.01%
Trafico http	1.85%
Icmp	17.65%
Dhcp	0.63%
Trafico www	52.31%
Netbios	6.30%
Smb	1.57%
LDAP	0.66%
Otros	5.67%

Chapman David, Fox Andy, *Firewalls PIX de Cisco Secure*,Pearson education,Madrid 2002

Maiwald Eric, Fundamentos de seguridad de redes,Mac Graw Hill,Mexico,2005

Chapman David, Fox Andy, *Firewalls PIX de Cisco Secure*,Pearson education,Madrid 2002

Maiwald Eric, Fundamentos de seguridad de redes,Mac Graw Hill,Mexico,2005

http://www.flukenetworks.com/fnet/es-es/products/OptiView+Protocol+Expert/Specifications.htm?categorycode=LANH

http://www.cisco.com

http://es.kioskea.net

http://www.biometco.com

http://www.microsoft.com/spain/isaserver/default.mspx

http://www.isaserver.org/

http://freeradius.org/

http://www.diphuelva.es/contenido_basico.asp?idContenido=782