Capítulo 1

Marco Teórico

En este capítulo de describen, en forma muy resumida, las técnicas, protocolos y herramientas relacionados directa o indirectamente con la seguridad de las LAN y WAN, así como su uso más eficiente. La información aquí descrita es un resumen del material contenido en el CD "Seguridad en Informática y Comunicaciones" del profesor Vincenzo Mendillo, año 2001. Entre los principales aspectos que se estudian, están:

- Seguridad en las Redes
- Criptografía
- Redes Virtuales Privadas (VPN)
- DHCP
- Firewall/Proxy
- NAT

Estos puntos serán aplicados en el diseño y desarrollo de la WAN Segura de INE.

1.1 Servicio DHCP

El DHCP (Dynamic Host Configuration Protocol) es un protocolo que simplifica la tarea de administrar grandes redes. El equipo Equipo Firebox suministra este servicio para distribuir los parámetros más importantes de la configuración IP a las estaciones de trabajo correspondientes a la red interna ("trusted").

El Protocolo de Configuración Dinámica de Host (DHCP) proporciona un espacio de trabajo para pasar información de configuración a los hosts sobre una red TCP/IP. DHCP se basa en el protocolo BOOTP, añadiendo la capacidad de localización automática de direcciones de red reutilizables y

opciones de configuración adicionales. DHCP consiste en dos componentes:

- Un protocolo que transporta los parámetros de configuración específicos de host de un servidor DHCP a un host.
- Un mecanismo para la localización de direcciones de red a hosts.

IP requiere la configuración de varios parámetros del software de implementación del protocolo. Como IP se puede usar en muchos tipos distintos de hardware de red, los valores para esos parámetros no se pueden adivinar o asumir que son correctos por defecto. El uso de un esquema de localización de direcciones distribuidas basada en un mecanismo sondeo/defensa, para descubrir direcciones de red que ya están en uso, no puede garantizar direcciones únicas de red porque los hosts no pueden ser capaces de ocultar sus direcciones de red.

DHCP soporta tres mecanismos para asignar direcciones IP:

- Asignación automática. DHCP asigna una dirección IP permanente al host.
- Asignación dinámica. DHCP asigna una dirección IP para un periodo de tiempo limitado. Tal mecanismo se llama *lease*. Este es el único mecanismo que permite la reutilización automática de direcciones que el host ya no necesita .
- Asignación manual. El administrador de red asigna la dirección del host.

El formato de un mensaje DHCP es:

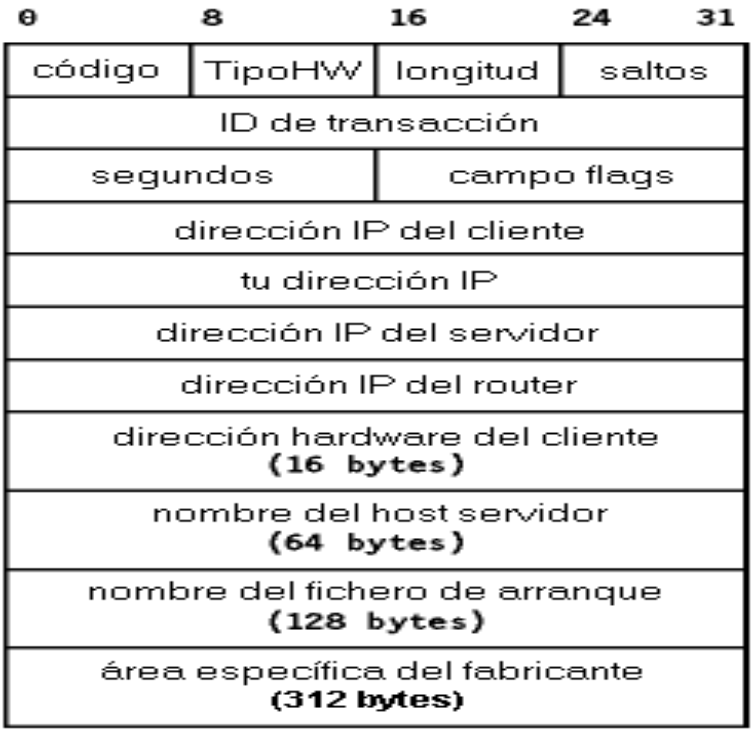


Tabla N°1 Formato del mensaje DHCP

1.2 Servicio NAT

Dentro de las técnicas empleadas en enrutamiento, una de las más útiles es el NAT (Netwok Address Traslation), definida inicialmente en la RFC1631. Entre otras aplicaciones, resulta una alternativa muy eficaz para posibilitar el acceso a Internet desde los equipos internos de una red privada en comparación a los servidores Proxy y Sockets.

En su configuración más simple, NAT trabaja en un *router o en servidor NAT* que une dos redes, cada de las cuales puede usar su propio esquema de direcciones IP, bien sean privadas o públicas. Una de las redes se designa como interior (*incide)* y la otras como exterior (*outside)*. Típicamente la primera es una red privada y la segunda una que da acceso directo Internet. Cuando se requiere enviar paquetes de una red a la otra,

las direcciones deben ser traducidas antes. NAT puede realizar la tarea de traducción en ambos sentidos.

Dos tipos de traducción son posibles y aplicables a la vez: estática y dinámica. Las traducciones estáticas son fijadas por el administrador de la red, y definen explicitamente una asignación de una dirección IP interna a una externa. Con la traducción dinámica el *router* tiene asignada una lista de direcciones en su interfaz, y para cada nueva dirección IP a traducir se asigna dinámicamente otra dirección IP de la lista siguiendo estrategias como *round-robin*. Por ejemplo, la asignación estática puede resultar útil cuando en la red interna hay un servidor DNS que requiere comunicarse con un servidor DNS externo, o cuando un equipo externo desea acceder a un servidor web interno.

En muchos casos se dispone de un número grande de direcciones IP privadas internas que deben ser traducidas a un pequeño número de direcciones externas públicas (una sola en el caso límite). Esto es posible gracias a una característica llamada *overload*, también conocida como PAT (*Port Address Translation*), y que es un subconjunto de la funcionalidad de NAT. Esta se basa en utilizar distintos números de puerto cliente de TCP/UDP con la misma dirección externa para distinguir entre varias traducciones.

El número de traducciones que puede mantener el NAT depende principalmente de memoria física del *router*, ya que para cada traducción se requiere mantener información en una entrada de la tabla de traducciones, la cual contiene las traducciones en curso, además de las recientemente realizadas a modo de caché.

Como primera ventaja del uso de NAT se tiene que los equipos de una red privada, con direccionamiento privado, pueden acceder a un esquema de direccionamiento público de forma transparente. Como es posible asignar muchas direcciones privadas a un pequeño lote de

direcciones públicas se obtiene una reducción de costos, además de reducir la necesidad de las ya escasas direcciones IP públicas legales. Además, con el uso de NAT y direcciones privadas válidas (la 10.0.0.0 de clase A, las 172.16.0.0 a 172.31.0.0 de clase B, y las 192.168.0.0 a 192.168.255.0 de clase C dadas por el *Internet Assigned Numbers Authority* o IANA) el diseño de la red se simplifica mucho. Otras ventajas destacables son la flexibilidad de administración que NAT aporta, ya que permite opciones como el manejo de varias listas de direcciones, el balanceo de carga, y la seguridad añadida que implica el uso de direcciones privadas "invisibles" al lado público.

Los principales inconvenientes de NAT derivan de la propia traducción. NAT requiere analizar las cabeceras de los paquetes IP de red o de niveles superiores, e incluso los datos, para traducir (cambiar) las direcciones IP y los números de puerto de los sockets. Ese proceso también implica recalcular las sumas de chequeo de errores. Por ello NAT repercute en el rendimiento de los *routers,* además de dificultar el seguimiento o traza de los paquetes. En este sentido puede delegarse esta función a equipo s especiales como el equipo Firebox. También hay que tener en cuenta que la traducción no siempre es sencilla o posible, y de hecho no todos los protocolos de aplicación sobre TCP/IP admiten NAT. Cambiar las direcciones IP en una cabecera de un paquete es fácil, pero hay aplicaciones (como por ejemplo FTP), que envían información sobre el direccionamiento IP dentro de los datos de algún paquete de comando, e incluso codifican dicha información con valores ASCII en vez de numéricos. Aun así, NAT puede soportar protocolos como ICMP, FTP o SMTP. Esto también implica que NAT puede funcionar correctamente cuando se utilizan mecanismos de seguridad con encriptación de datos.

A continuación se describe un ejemplo del uso típico de NAT. Considérese la siguiente estructura de red, donde se interconecta una red privada o intranet (lado interno o *inside*) con Intenet (lado externo o *outside*)

mediante un *router* con NAT (y PAT) habilitado. En la red privada se usan direcciones IP privadas de la red 10.0.0.0, mientras que en el lado externo el *router* tiene asignadas dos direcciones IP públicas legales (asignadas por la IANA) de clase B: 171.69.89.1 y 171.69.89.2.

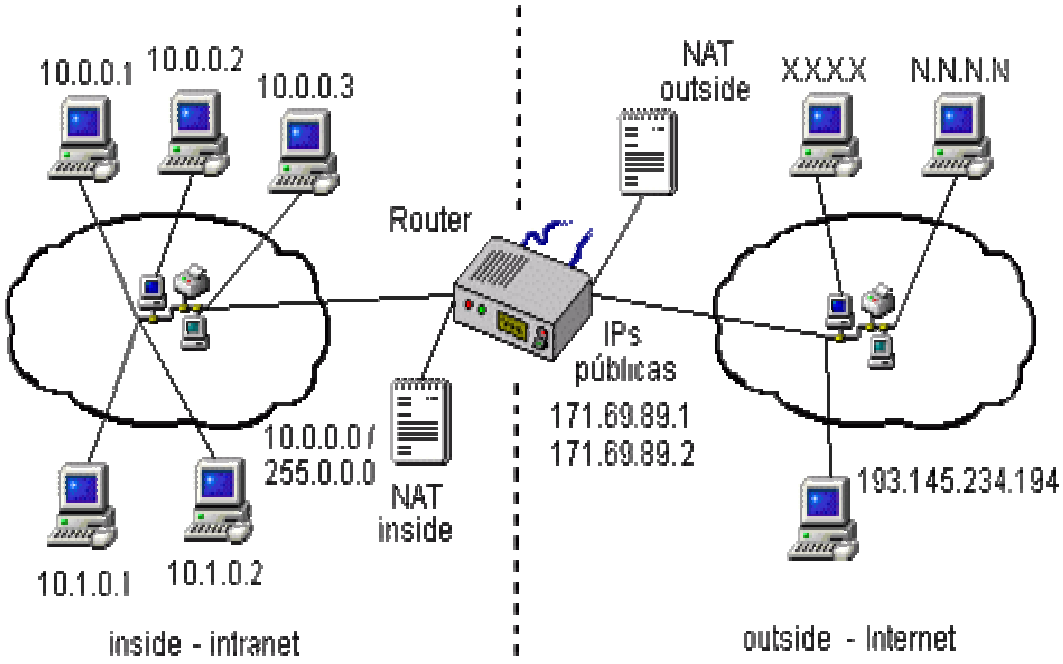


Figura N° 1 Uso del NAT

Interesa que el router traduzca cualquier dirección 10.-.-.- interna a una dirección externa válida, esto es, aplicar traducción NAT de salida a las direcciones fuente privadas para acceder a los servicios de Internet. Esto se realiza en la interfaz con la red privada (*inside* NAT). Puesto que sólo hay dos IP públicas, se requiere una traducción *overload* o con PAT. Con *inside* NAT, equipo s como el 10.0.0.1, el 10.0.0.2 y el 10.0.0.3 pueden comunicarse con servidores en el exterior mediante traducciones dinámicas, como por ejemplo:

Paquete original en el interior (local)	**paquete traduccido al exterior (global)**
origen: IP 10.0.0.1, puerto 1000 destino: IP 193.145.234.194, puerto 80	origen: IP 171.69.89.1, puerto 1000 destino: IP 193.145.234.194, puerto 80
origen: IP 10.0.0.2, puerto 2000 destino: IP 193.145.234.194, puerto 80	origen: IP 171.69.89.2, puerto 2000 destino: IP 193.145.234.194, puerto 80
origen: IP 10.0.0.3, puerto 1000 destino: IP 193.145.234.194, puerto 21	origen: IP 171.69.89.1, puerto 1001 destino: IP 193.145.234.194, puerto 21

Tabla N° 2 Traducciones dinámicas

Hay que notar que NAT trata de mantener el número de puerto cliente si es posible. El *router* mantiene las traducciones en una tabla a modo de caché para que las direcciones destino de los paquetes de vuelta procedentes de los servidores sean traducidas a direcciones privadas siguiendo el proceso inverso. En este caso no interesa considerar traducciones diferentes para las direcciones públicas, lo que se realizaría en el *outside* NAT. Esto es, el direccionamiento interior nunca se verá en el exterior, pero interesa que las direcciones externas si se vean como tales en la red interior.

Si se desease además disponer de servidores dentro de la red privada, por ejemplo un servidor web en el equipo con IP 10.1.0.1 y un servidor FTP en el equipo con IP 10.1.0.2, asociados a la dirección pública 171.69.89.1 y que sean accesibles desde equipo s externos cualquiera con IP X.X.X.X o N.N.N.N, también habría que configurar el *inside NAT* en el interfaz con la red privada para realizar estas traducciones estáticas:

Paquete original en el exterior (global)	paquete traduccido al interior (local)
origen: IP X.X.X.X, puerto Y destino: IP 171.69.89.1, puerto 80	origen: IP X.X.X.X, puerto Y destino: IP 10.1.0.1, puerto 80
origen: IP N.N.N.N, puerto M destino: IP 171.69.89.1, puerto 21	origen: IP N.N.N.N, puerto M destino: IP 10.1.0.2, puerto 21

Tabla N° 3 Traducciones Estáticas

De este modo incluso resulta posible configurar varios servidores para una misma aplicación, por ejemplo web, que, que desde el punto de vista del lado exterior sean accesibles a través de distintos puertos.

En resumen puede afirmarse que el servicio NAT permite básicamente dos funciones:

- Asignar muchas direcciones no válidas a una pocas direcciones válidas, las cuales son escasas en Ipv4
- Ocultar las verdaderas direcciones de origen de los "hosts" para prevenir ataques externos

1.3 Servicio Firewall / Proxy

Firewall

Generalmente se combina con un filtro de paquetes (función que puede recaer en un enrutador) a fin de optimizar la protección. Los filtros de paquetes se utilizan como el primer nivel de defensa contra una red no confiable y constituyen una manera eficaz y general para controlar el tráfico entre redes. Esta solución tiene la ventaja de no realizar ningún cambio en

las aplicaciones del cliente y del host, pues opera en las capas IP y TCP, las cuales son independientes de los niveles de aplicación. Por falta de información de contexto, ciertos protocolos como UDP y RPC no pueden filtrarse con efectividad. Así que sólo la información de las capas de transporte y de red (modelo OSI), como las direcciones IP, los números de puerto y las banderas TCP están disponibles para las decisiones de filtración. En la mayoría de los enrutadores comerciales el número de reglas puede ser limitado; además, mientras mayor sea este número, habrá una alta penalización en el desempeño, a causa del proceso adicional necesario para las reglas complementarias.

El objetivo principal de una barrera de protección es proteger una red de otras. En general, la red que se protege es propiedad del usuario (o es su responsabilidad) y la red contra la que se protege es externa, en la que no puede confiarse y desde la cual puede violarse la seguridad. Proteger la red es prevenir que los usuarios no autorizados tengan acceso a datos delicados y permitir que los usuarios legítimos tengan libre acceso a los recursos de la red.

El firewall o host de bastión es un elemento de la barrera de protección, determinante para la seguridad en la red. Es el host principal para la seguridad en la red de una organización y, por su función, debe estar en una buena fortaleza. Esto significa que al host de bastión lo monitorean con detenimiento los administradores de la red. La seguridad del sistema y del software del host de bastión debe revisarse con regularidad. Asimismo, es preciso observar los registros de acceso en busca de cualquier brecha potencial de seguridad y de un intento de asalto al host de bastión.

Como los hosts de bastión actúan como un punto de interfaz para una red externa no confiable, casi siempre están sujetos a invasiones. La distribución más simple de un host de bastión es el primer y único punto de

entrada para el tráfico de una red externa (Figura N° 2)

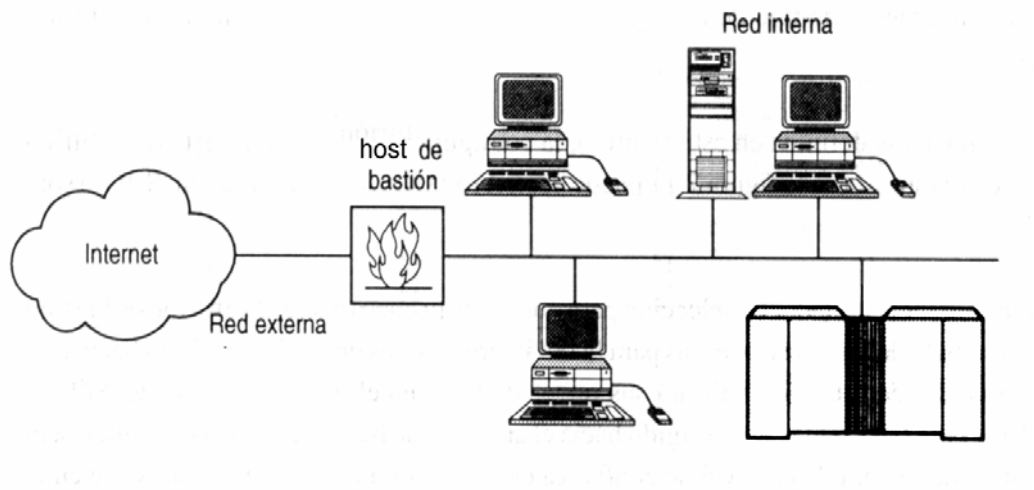


Figura N° 2 Distribución más simple de un host de bastión

En vista de que el host de bastión es determinante para la seguridad de la red interna, por lo regular se coloca otra primera línea de defensa entre la red externa no confiable y la red interna. Esta línea casi siempre la proporciona un filtro de paquetes. En la figura 2 se muestra el uso de un host de bastión con un filtro de paquetes como la primera línea de defensa. En este ejemplo, sólo la interfaz de red del host de bastión está configurada y conectada a la red interna. Uno de los puertos del filtro de paquetes está conectado a la red interna, mientras el otro puerto está conectado a Internet. Este tipo de configuración se conoce como *compuerta de host seleccionado*.

Se debe configurar el filtro de paquetes para que envíe primero hacia el host de bastión todo el tráfico recibido de las redes externas para la red interna. Antes de enviar el tráfico hacia este host, el filtro de paquetes aplicará sus reglas de filtro en el tráfico del paquete. Sólo el tráfico de red que pase tales reglas será dirigido hacia el host de bastión; el resto del tráfico será rechazado. Esta arquitectura da un nivel de confianza en la seguridad de la red que no existe en la arquitectura de la figura N° 2. Un

intruso necesita penetrar primero en el filtro de paquetes y, si lo logra, debe enfrentarse con el host de bastión.

El host de bastión utiliza funciones a nivel de aplicación para determinar si las solicitudes hacia y desde la red externa se aceptarán o negarán. Si la solicitud pasa el escrutinio del host de bastión, se enviará a la red interna para el tráfico de entrada. Para el tráfico de salida (tráfico hacia , la red externa), las solicitudes se enviarán al filtro
de paquetes.

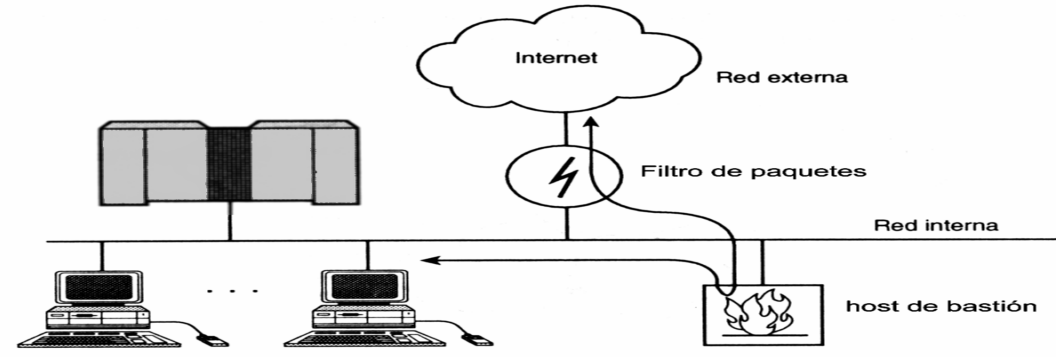


Figura N° 3 Un host de bastión con una sola interfaz de red y un filtro de paquetes

Algunas organizaciones prefieren que su proveedor de acceso a Internet (ISP) proporcione las reglas de los filtros de paquetes para el tráfico en red enviado a la red de dicha organización (véase la figura N° 3).

Las tablas de enrutamiento de los filtros de paquetes deben configurarse para enviar el tráfico externo al host de bastión. Dichas tablas necesitan estar protegidas contra las invasiones y los cambios no autorizados. Si la entrada de las tablas se cambia para que el tráfico no se envíe al host de bastión, sino en forma directa a la red conectada localmente, el host de bastión se ignorará.

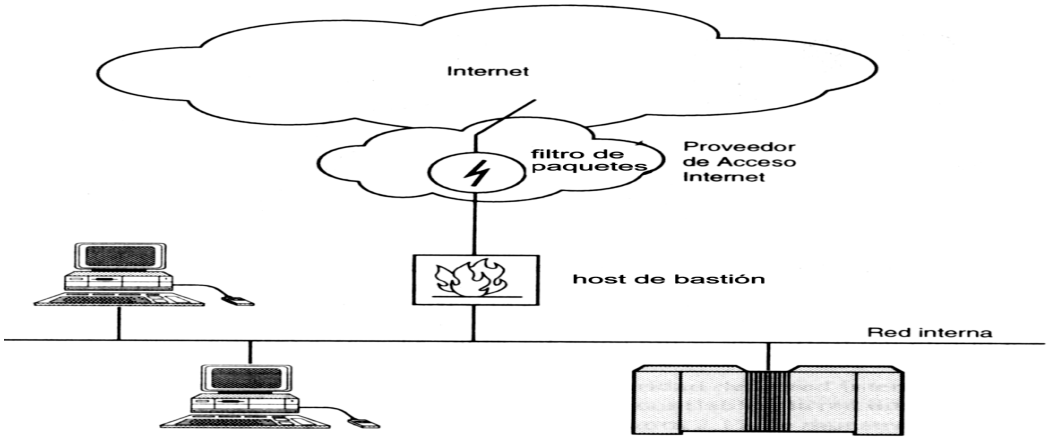


Figura N° 4 El filtro de paquetes como primera línea de defensa

En la figura N° 4, la tabla de enrutamiento del filtro de paquetes señala al host de bastión. El número de la red interna es 199.245.180.0 y la dirección IP del host de bastión es 199.245. 180.10. El filtro de paquetes tiene la siguiente entrada en su tabla de enrutamiento:

Destino : 199.245. 180.0

Enviar a: 199.245.180.10

Todo el tráfico de la red 199.245.180.0 se envía a la dirección IP 199.245.180.10 del host de bastión.

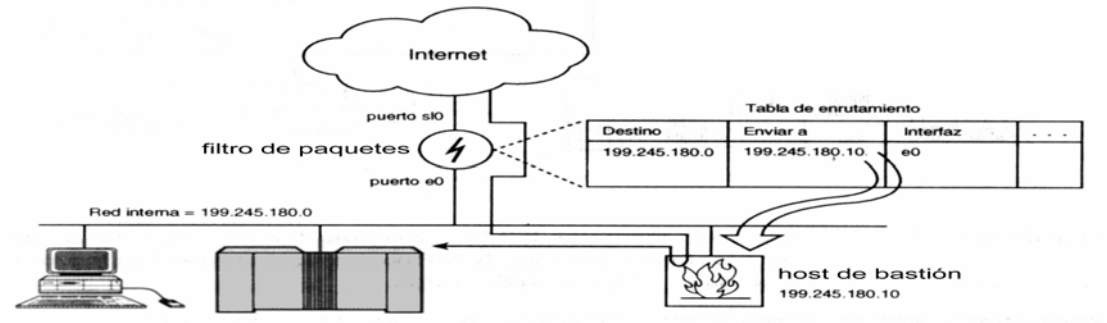


Figura N° 5 Configuración normal de la tabla de enrutamiento del filtro de paquetes

En la figura N° 5 las tablas de enrutamiento del filtro de paquetes se han subvertido y la entrada para la red de destino 199.245.180.0 se ha eliminado. El tráfico externo recibido por el filtro de paquetes para la red 199.245.180.0 no se envía al host de bastión, sino que se manda en forma directa por la interfaz local en la red interna. El host de bastión se ignora y el filtro de paquetes es la única línea de defensa. Lo más probable es que si el filtro se ha subvertido, ocurra lo mismo con otras funciones del enrutador y la zona de riesgo abarque la red interna.

El plan de cortafuegos más básico es bloquear todo el tráfico, luego permitir servicios específicos caso por caso. Este plan es restrictivo pero seguro. Sin embargo, puede ser tan restrictivo que los usuarios se lo salten. Además cuanto más restrictivo, más difícil será administrar las conexiones que se permitan. En enrutadores de filtrado se necesitará implementar conjuntos de reglas complicadas, una tarea difícil. La mayoría de los cortafuegos que se describen más adelante simplifican este proceso usando interfazs gráficas y un conjunto de reglas más eficaces (en la mayoría de casos ni siquiera se emplea el filtrado de paquetes). El plan de seguridad debe ser resumido previamente para que los administradores y los usuarios sepan qué tipos de actividades están permitidas en la red. Tal plan debería incluir el acceso interno y externo, el acceso de usuarios remotos, la protección frente a virus, necesidades de encriptación, uso de programas y varias otras consideraciones que se describen a continuación:

- El tráfico de red hacia y desde redes externas como Internet debe pasar por un cortafuegos. El tráfico debe ser filtrado para permitir sólo el paso de los paquetes autorizados.

- Nunca utilizar un cortafuegos para el almacenamiento de archivos de propósito general o para ejecutar programas, excepto los que necesite el cortafuegos.
- No ejecutar ningún servicio en el cortafuegos excepto los imprescindibles para suministrar servicios al cortafuegos. Asúmase que el cortafuegos puede perderse en un ataque.
- No permitir que ninguna contraseña ni direcciones internas pasen el cortafuegos.
- Si se necesita suministrar servicios al público, deben ponerse en la parte exterior del cortafuegos e implementar las configuraciones internas que protejan al servidor de ataques de denegación de servicio.
- Aceptar el hecho de que se podría necesitar restaurar completamente los sistemas públicos de copias de seguridad en caso de un ataque. Se puede implementar un esquema de duplicación que copie información automáticamente a un servidor público a través de un canal seguro.

Proxies

Las pasarelas trabajan en el nivel más alto del stack del protocolo para suministrar más oportunidades para monitorear el acceso entre redes. Una pasarela es como un agente que lleva mensajes de clientes internos a servicios externos. El servicio cambia la dirección IP de los paquetes de clientes para ocultar el cliente interno en relación a Internet, luego actúa como un agente proxy para el cliente en Internet.

El uso de proxy reduce la amenaza de hackers que visualicen el tráfico de la red para conseguir información sobre las computadoras en redes internas. Proxy oculta las direcciones de todas las computadoras internas. Tradicionalmente, el uso de proxy ha reducido el rendimiento y la

transparencia en el acceso a otras redes. Sin embargo, los productos de cortafuegos actuales resuelven algunos de estos problemas.

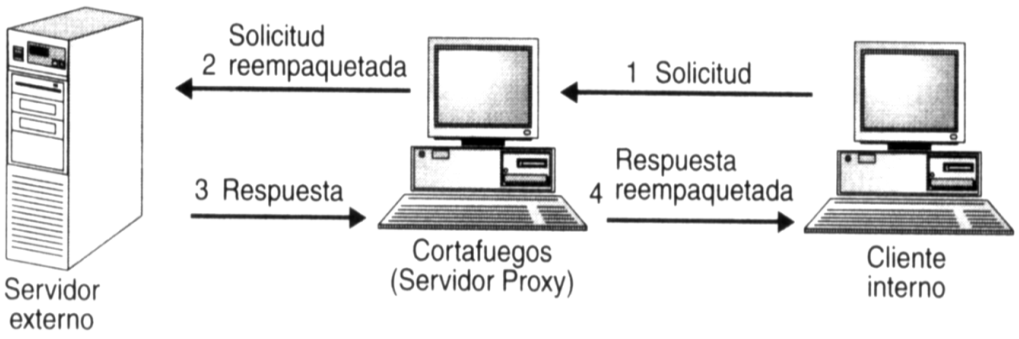


Figura N° 6. Los servidores proxy ocultan las direcciones internas

Tipos de Servidor Proxy:

Pasarela a Nivel de Circuito*.* Este tipo de servidor proxy suministra un conexión de red controlada entre sistemas internos y externos (es decir, no hay “colchón de aire”). Existe un “circuito” virtual entre el cliente interno y el servidor proxy. Las consultas de Internet pasan por este circuito al servidor proxy, que se encarga de enviar estas peticiones a Internet después de cambiar la dirección IP. Los usuarios externos sólo ven la dirección IP del servidor proxy. Las respuestas son recibidas por el servidor proxy y enviadas por el circuito al cliente. Mientras que se permite pasar el tráfico, los sistemas externos nunca ven a los sistemas internos. Este tipo de conexión se utiliza con frecuencia para conectar usuarios internos “de confianza” a Internet.

Pasarela a Nivel de Aplicación.

Un servidor proxy a nivel de aplicación suministra las propiedades proxy básicas y también análisis extensivo de paquetes. Cuando llegan paquetes desde fuera a la pasarela son examinados y evaluados para determinar si la política de seguridad permite al paquete entrar en la red interna. No sólo evalúa el servidor las direcciones IP, sino también mira los datos de los paquetes para evitar que los hackers oculten información en dichos paquetes. Una pasarela a nivel de aplicación típica puede proporcionar servicios proxy para aplicaciones y protocolos como Telnet, FTP, HTTP (servicios Web) y SMTP (correo electrónico). Debe instalarse un proxy separado para cada servicio a nivel de aplicación (algunos fabricantes consiguen seguridad simplemente no proporcionando proxy para algunos servicios, por lo que se debe ser cuidadoso en la evaluación).Los servidores proxy de nivel de aplicación hoy en día suministran el mayor nivel de protección. En la Figura 4, los servicios proxy se ejecutan en el nivel de aplicación del stack del protocolo de red para cada tipo de servicio diferente (FTP, HTTP, etc.).

Un servidor proxy es un componente de un cortafuegos que controla cómo los usuarios internos acceden al mundo exterior (Internet) y cómo los usuarios de Internet acceden a la red interna. En algunos casos, proxy bloquea todo el exterior y sólo permite a los usuarios internos acceder a Internet. Los únicos paquetes permitidos de entrada son las respuestas a las peticiones de los usuarios internos. En otros casos, tanto el tráfico entrante como saliente está permitido bajo estrictos controles. Existe entonces un “colchón de aire” virtual en el cortafuegos entre las redes internas y externas y que los proxy salvan ese espacio trabajando como agentes para los usuarios internos y externos.

Con los proxies, los planes de seguridad pueden ser mucho más poderosos y flexibles porque toda la información de los paquetes puede ser utilizada por los administradores para escribir las reglas que determinan cómo son tratados los paquetes por la pasarela. Es fácil auditar casi todo lo que ocurre en la pasarela. También se puede quitar los nombres de las computadoras para ocultar sistemas internos, y se puede evaluar los contenidos de paquetes para ver su adecuación y por seguridad.

La adecuación es una opción interesante. Se podría configurar un filtrado que descarte cualquier mensajes de correo electrónico que contenga insultos.

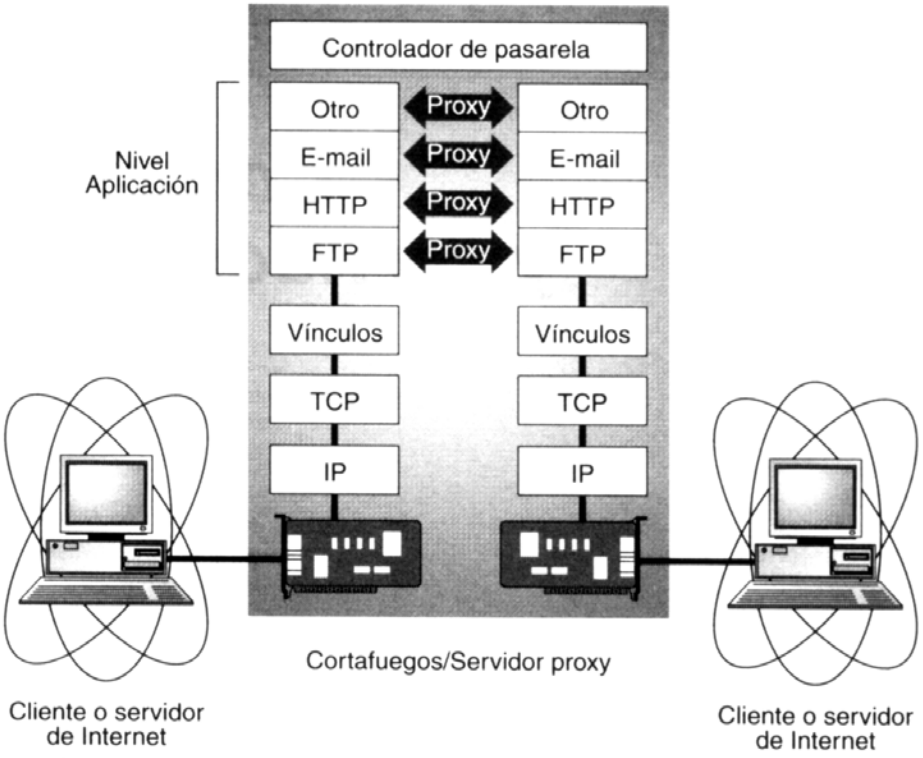


Figura N° 7 Un cortafuegos/servidor proxy

Técnicas de Inspección Personalizada

Uno de los problemas con proxy es que tienen que evaluar mucha información en muchos paquetes. Además se necesita instalar un proxy por separado para cada aplicación que se quiera soportar. Esto afecta al rendimiento y aumenta los gastos. Aparece una nueva clase de productos de cortafuegos que utilizan técnicas de inspección personalizada. En vez de examinar los contenidos de cada paquete, los patrones de bits de los paquetes se comparan con los paquetes que ya son conocidos y de confianza.

Por ejemplo, si un usuario accede a algún servicio externo, el servidor recuerda cosas de su consulta original como el número de puerto y la dirección de fuente y de destino. Este “recuerdo” se llama *salvado de estado*. Cuando el sistema externo responde a una consulta, el servidor de cortafuegos compara los paquetes recibidos con el estado saltado para determinar si se les permite entrar. A este proceso se le denomina *stateful inspection* en inglés.

Mientras que la inspección personalizada suministra velocidad y transparencia, una de las mayores desventajas es que los paquetes internos viajan a la red externa exponiendo las direcciones IP internas a hackers potenciales. Algunos fabricantes de cortafuegos utilizan inspección personalizada junto con proxy como seguridad adicional.

Como solución, las pasarelas (*gateway*s) a nivel de aplicación suministran proxy que controlan el acceso por el cortafuegos de un modo único. Proxy comprende completamente los protocolos de las aplicaciones que son permitidas para interoperar a través de la pasarela y administran completamente el tráfico tanto entrante como saliente en un nivel que no es posible mediante los enrutadores de filtrado.

Otra propiedad importante de servidores a nivel de aplicación es la identificación. Puede permitir que sólo los usuarios específicos pasen por el cortafuegos según sus credenciales. Hacer esto es útil para usuarios móviles de confianza o gente de organizaciones afiliadas que necesiten acceder a sistemas específicos en sus redes.

Además los cortafuegos pueden ocultar las direcciones de red interna a Internet por razones de seguridad o para que se pueda implementar cualquier esquema necesario de direcciones IP sin tener que registrarlo en las autoridades de Internet. Esta propiedad está creciendo en importancia debido a que las direcciones IP registradas están comenzando a ser escasas.

Los servicios proxy pueden suministrar funciones adicionales de interés a los administradores de redes:

- El rastreo de todas los sitios a las que accedan los usuarios en Internet y el registro de ellas puede ayudar a reducir actividades en Internet. Enviar estos registros a los usuarios periódicamente les avisará que están siendo vigilados.
- El filtrado de hosts específicos y los URL pueden ser utilizados para restringir los sitios a las que los usuarios internos puedan acceder.
- La cache de páginas Web accedidas con más frecuencia puede reducir las peticiones y respuestas a Internet.

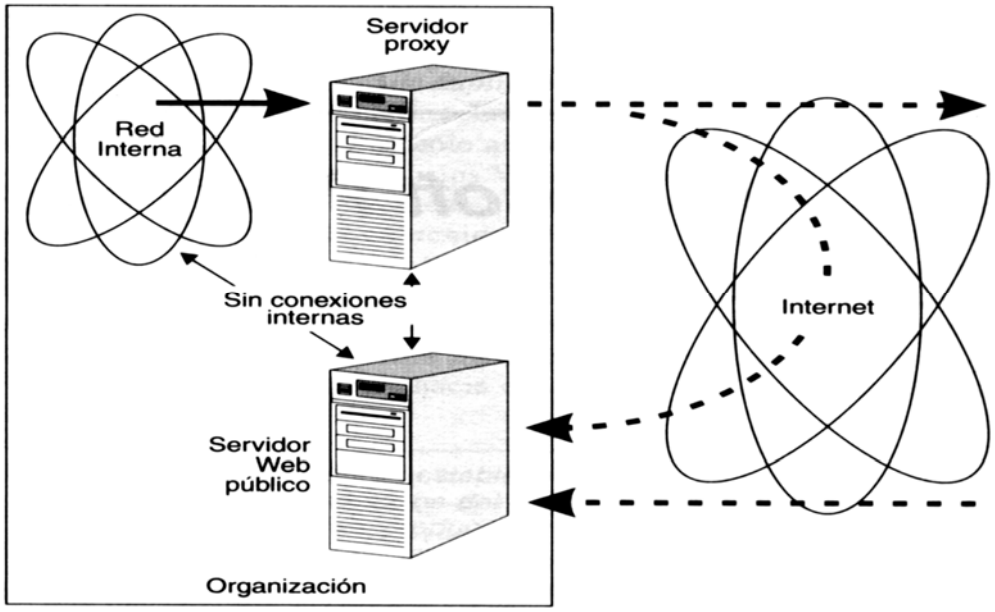


Figura N° 8 Acceso al Web desde adentro

Proxy Server suministra una solución para conectar redes no TCP/IP a Internet. Algunas de sus propiedades se describen a continuación:

Cuando un cliente de red interna necesita hacer una petición a un servidor Internet, Proxy Server empieza a trabajar. Como se muestra en la Figura 14, los exploradores de los clientes redirigen sus peticiones a Proxy Server mediante protocolos propios. Luego, Proxy Server transmite estas peticiones a Internet por TCP/IP. Este mecanismo ofrece propiedades de seguridad avanzadas como control de planes por usuario e integración con la seguridad Windows NT. El cliente puede ejecutar Windows NT Workstation, Windows 95, Windows para trabajo en grupo o Windows versión 3.1.

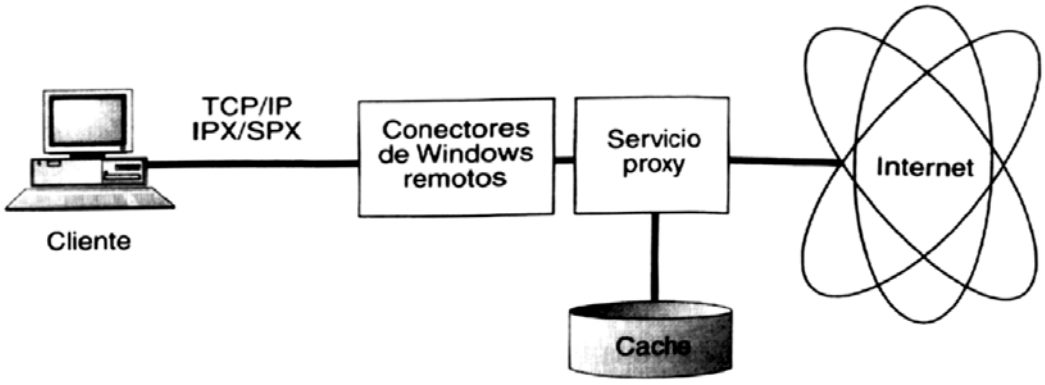


Figura N° 9 La arquitectura Proxy Server

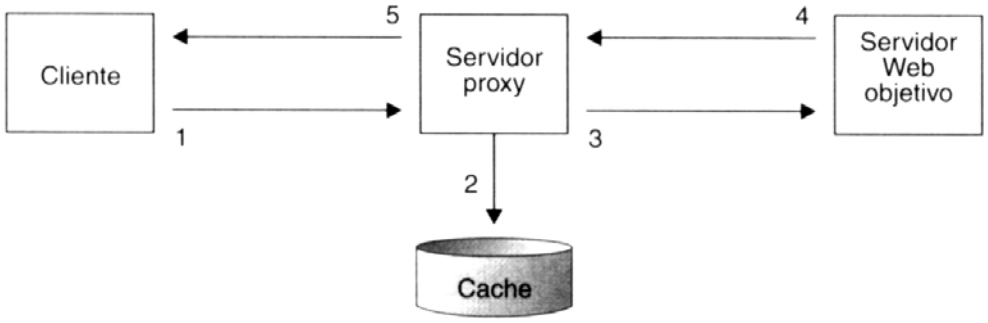


Figura N° 10 Cumplimiento de peticiones proxy

Cuando un servidor proxy está entre un cliente y un servidor objetivo, como se muestra en la Figura N° 10, el protocolo de consulta y respuesta HTTP cambia ligeramente. A continuación se las caracteristicas de la aplicación:

- El cliente Web hace una petición a un servidor Web específico en Internet como siempre.
- Proxy comprueba la bondad de la relación entre el cliente y el servidor objetivo. El servidor Web recibe la petición y comprueba si el cliente está autorizado para este tipo de acceso.

- Proxy comprueba si el usuario puede hacer la petición al dominio especificado.
- Proxy comprueba su cache para ver si el documento pedido está en ella. Si lo está, lo devuelve al cliente.
- Si el documento no está en la cache, Proxy Server lo pide al servidor Web objetivo.
- El servidor Web objetivo devuelve el documento a Proxy Server.
- Proxy devuelve el documento al cliente.

Microsoft Proxy Server es un servicio proxy a nivel de aplicación que tiene conocimiento de los protocolos usados por las aplicaciones. Debido a esto, puede suministrar servicios de alto nivel como la identificación, el filtrado, uso de cache y conversión de protocolos.

1.4 Ataques Comunes

Una razón para bloquear direcciones IP es para evitar ataques de falsificación (*spoofing*). Un paquete falsificado proviene de una fuente no conocida o no autorizada y contiene una dirección de fuente falsificada. La dirección falsificada hace que el paquete aparente ser de una computadora en su propia red interna. El enrutador enviará este paquete al sistema de destino sin problema a menos que estén configuradas las opciones de seguridad adecuadas. Un enrutador de filtrado puede ser programado para desechar paquetes falsificados.

¿Cómo se sabe que un paquete está falsificado? Muy fácil: si el paquete llega desde el exterior con la dirección de fuente de una computadora interna, el paquete es falso.

También existen otras técnicas, algunas de las cuales semencionarán brevemente.

IP Spoofing

En el ataque IP Spoofing (figura N° 11), el intruso utiliza la confianza “trusted” que un servidor le tiene a otro. Esta confianza significa que al servidor que confía sólo le basta conocer la dirección IP del otro, sin que tenga necesidad de otro tipo de identificación, para ser accedido desde aquel. En primer lugar, el intruso C debe seguir la secuencia de los paquetes que intercambian A y B, ya que él en algún momento se hará pasar por B y no desea que A se entere al detectar cambios en la secuencia de paquetes. Luego, el intruso C aplicará un ataque de negación de servicio a B para evitar que responda a futuras solicitudes de A. Finalmente C enviará a A paquetes con dirección de origen falsificada (“B”) y A no se percatará del cambio ya que se mantiene la secuencia de paquetes original. En este intercambio de información, el intruso C puede, por ejemplo, crearse una cuenta de usuario en A para entrar luego “legalmente” o borrar todos los archivos de los discos.

El IP spoofing requiere mucha maestría ya que es un ataque a ciegas. Es decir, a pesar de que el intruso envía paquetes a A, este host responde a B , ya que el enrutamiento no ha sido cambiado. C debe “imaginarse” las respuesta de entrega A para enviar paquetes que concuerden con las mismas. Esto, además de la obtención del sincronismo entre A y B mediante las banderas ACK y SYN, lo hacen un ataque difícil de llevar a cabo.

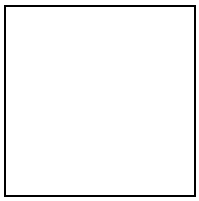


Fig. N° 11 IP Spoofing

Puertos y filtrado de puertos

Además del filtrado basado en direcciones IP, los enrutadores con filtrado pueden ver información disponible en el nivel de transporte del stack del protocolo y tomar decisiones de envío basadas en ella. El nivel de transporte es responsable de enviar paquetes de modo confiable entre sistemas y para administrar múltiples sesiones a través de la misma conexión de red. Cada sesión tiene su propio canal. Por ejemplo, si se utiliza FTP para pedir un archivo desde un servidor, la peticiones se envían por un canal y el archivo se transmite por otro. El punto final del canal se llama *puerto*. FTP normalmente utiliza los puertos 20 y 21.

La idea básica es bloquear un puerto si no se quiere que alguien lo utilice de modo inapropiado. Por ejemplo, si no ejecuta servicios FTP, se puede configurar el enrutador con filtrado para que bloquee los puertos 20 y 21. Mirando esto de modo diferente, si se quiere suministrar sólo servicios WWW en un servidor conectado directamente con Internet, se puede bloquear los demás puertos excepto el 80, que es el puerto HTTP.

Junto al filtrado de puertos, un enrutador con filtrado también mira las banderas TCP en la cabecera del paquete. Cada paquete tiene una bandera que define su propósito en la “conversación” que está teniendo lugar por el canal entre el cliente y el servidor. Éstas son las banderas más importantes (figura N° 12) :

- ACK. Si está activada esta bandera, el paquete forma parte de una conversación que está teniendo lugar. Un paquete que no tiene esta bandera es parte de una petición de establecimiento de conexión.

- FIN. Un paquete con esta bandera activada, es una petición de cerrar la conexión.

- RST. Un paquete con esta bandera activada hace que el canal se reinicie debido a algún error.

- SYN. Un paquete con esta bandera activada indica una petición de abrir una conexión.

Las banderas se utilizan junto al filtrado de puertos para suministrar una base de reglas mayor. Por ejemplo, se puede configurar una regla que diga algo como "*permita que nuestros usuarios internos inicien una sesión con un host externo y sólo acepte las respuestas del host externo*". Esta regla evita que los hosts externos inicien sus propias sesiones. Las banderas ACK y SYN son las claves para hacerlo: El primer paquete para iniciar la conversación no tendrá configurada la bandera ACK sino la bandera SYN y los paquetes subsecuentes relacionados con esta conversación tendrán configurada la bandera ACK.

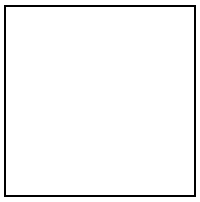


Figura 12. Uso de los flags

Syn Flood (Inundación de "Syn")

El protocolo TCP de Internet, sobre el que se basa la mayoría de los servicios, implica una conexión entre dos máquinas. El establecimiento de la conexión se realiza mediante una "conexión en tres pasos" (three way handshaking). El ataque consiste en no llegar a efectuar el último paso con lo que la conexión permanece en estado "semiabierto". Luego de crear

varias conexiones en ese estado, la máquina de destino colapsará ya que utilizará sus recursos (CPU y memoria) para mantener esas conexiones.

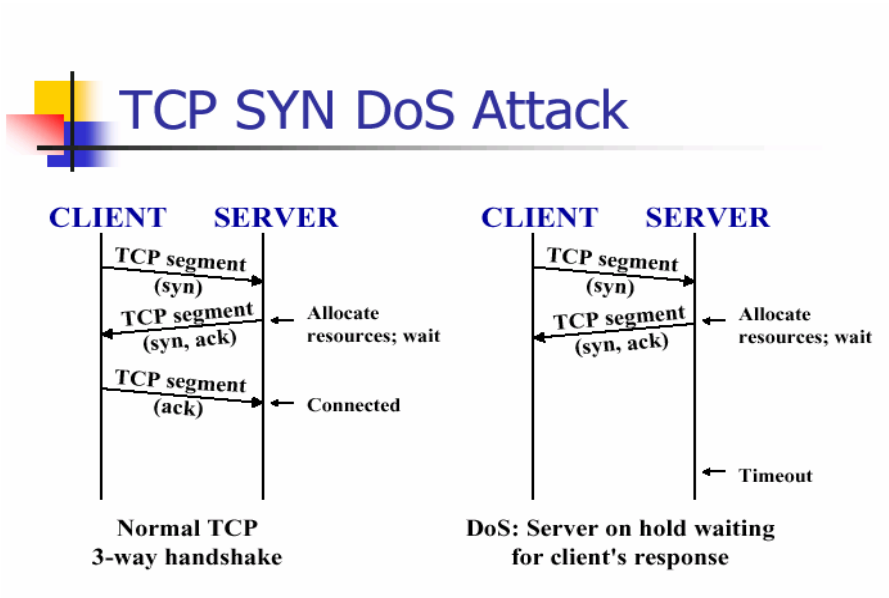


Figura N° 13 Ataque TCP SYN

Negación de servicio (DoS)

Un ataque de negación de servicio simplemente consiste en entorpecer a los usuarios a acceder a los servicios de manera que este quede total o parcialmente inoperativo. Este tipo de ataque aprovecha una debilidad del sistema para afectar a los servicios instalados. No afecta a los datos de los servidores ni compromete la confidencialidad de los datos.

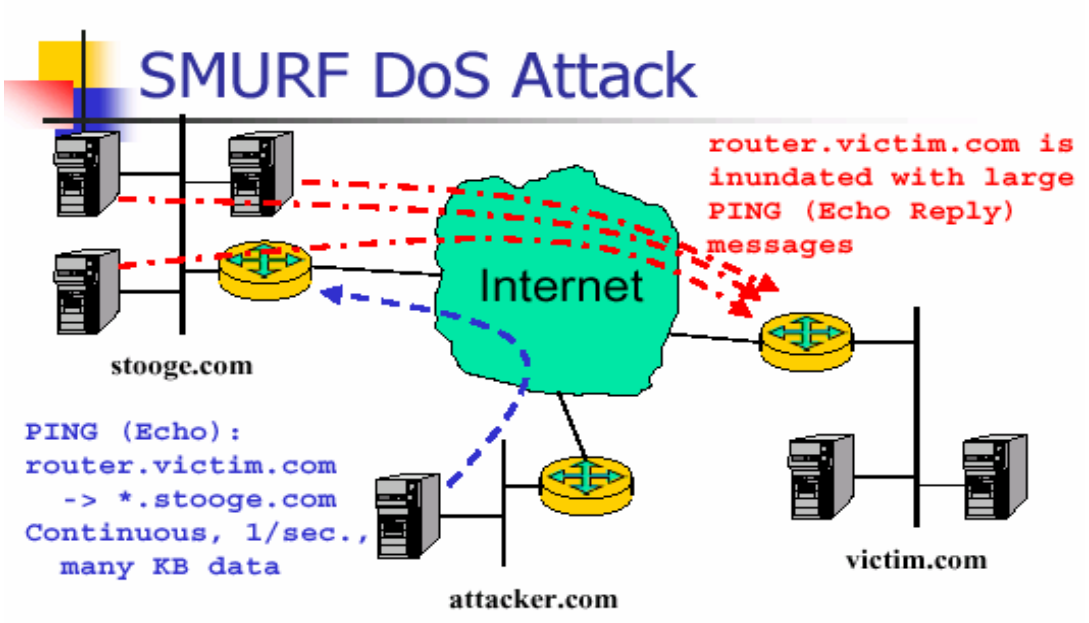
Los ataques de negación de servicio existen desde hace años y aunque son una constante en Internet desde sus comienzos (el más célebre fue el gusano de Morris), generalmente se han desarrollado a pequeña escala. No obstante, en la segunda mitad de 1.999 este tipo de ataque evolucionó de tal forma que el origen del ataque se producía desde diferentes nodos y de forma coordinada y a gran escala. El origen puede ser prácticamente imposible de determinar.

Es difícil defenderse de estos ataques. En un ataque de negación de servicio tradicional, la víctima puede averiguar de dónde viene

el ataque y cerrar la conexión con el atacante. Pero en un ataque distribuido no hay una única fuente. Se deberían cerrar todas las conexiones (puertos), excepto aquellas en las que confía, pero esto es inútil si se trata de un servidor de Internet. La solución más práctica es la adopción de medidas preventivas:

- Mantener las máquinas actualizadas y seguras. Ello implica tener personal especializado en cuestiones de seguridad (o subcontratarlo).
- No permitir el tráfico "broadcast" desde desde fuera de la red.
- Filtrar el tráfico “IP spoof".
- No tener proxies abiertos a todo Internet.
- Auditorias de seguridad y sistemas de detección.

En la variante SMURF, el atacante configura varias máquinas para realizar un ataque DoS sobre un objetivo común mediante la generación de paquetes ICMP (PING). El objetivo tratará de responder estos mensajes por lo que agotará sus recursos y dejará de prestar su propio servicio.



F

Figura N° 14 Ataque SMURF

Sondas de Pruebas

En ocasiones, los intrusos envían paquetes de prueba para detectar cuáles direcciones IP están activas y cuáles puertos responden (con la bandera ACK) a la solicitud de servicios. Con esto localizan puntos débiles en la red para introducirse y atacar. Existen varios programas comerciales para monitoreo como Super Scan, Port Scan, LANGuard, etc, y otros especializados en la captura de datos como Iris, Ethereal, Sniffer, etc, que le permiten a un intrusos saber cuales direcciones IP y puertos se encuentran funcionando en una red.

1.5 Criptografía

Las Redes Virtuales Privadas basan gran parte de su seguridad en los sistemas criptográficos modernos por lo que se explicarán brevemente algunos conceptos de esta área de las matemáticas.

La criptografía deriva del griego criptos (oculto) y grafos (escritura), por lo que literalmente significa escribir en forma oculta, oscura o aparentemente incoherente. En la actualidad se define la criptografía como: la ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave o el método para averiguar su significado oculto.... en pocas palabras, la criptografía es la ciencia de las comunicaciones secretas.

En un sistema criptográfico un mensaje es encriptado o cifrado para volverlo ininteligible y luego es desencriptado o descifrado para devolverlo a su forma original.

El uso de la palabra “cifrado” se debe a que a menudo el mensaje en convertido a cifras, esto es números, para que hacerlo ininteligible.

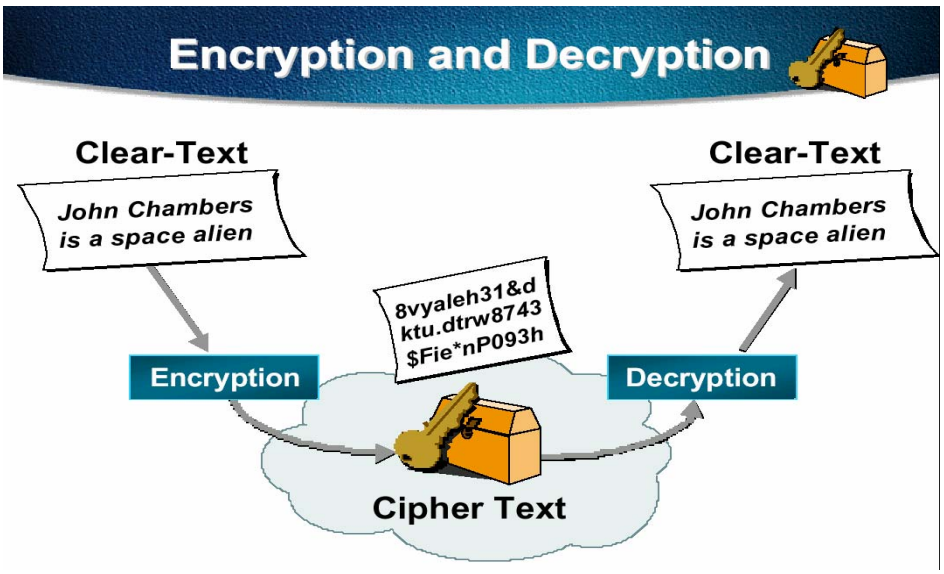


Figura N° 15 Proceso de Cifrado

Si se desea que un mensaje sea confidencial (es decir secreto), el remitente lo debe cifra antes de enviarlo al destinatario, y este último debe conocer el procedimiento o la clave de descifrado para recuperar el mensaje original. Si un intruso intercepta ese mensaje cifrado, verá solamente caracteres o números sin significado alguno para él.

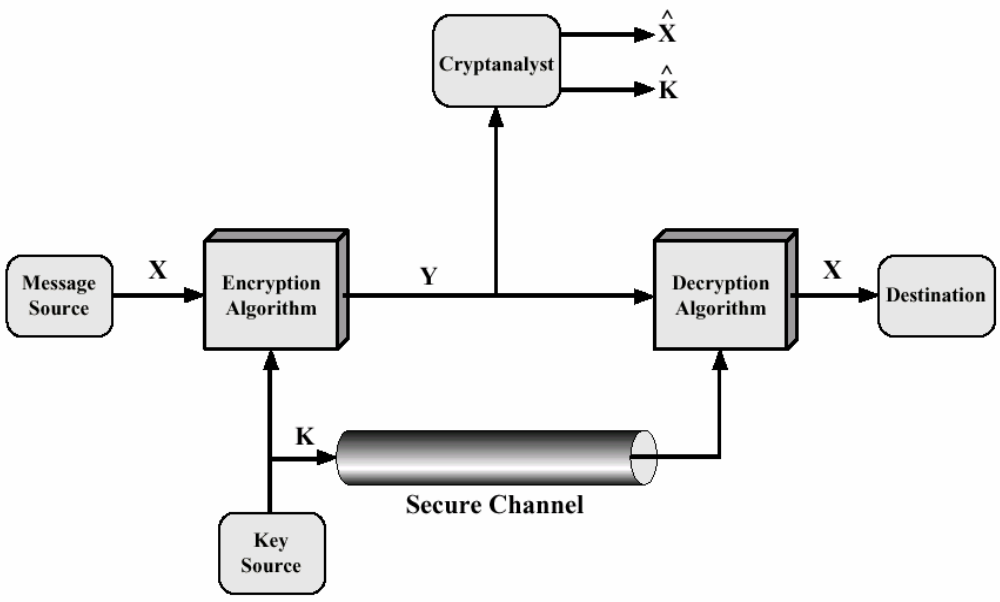


Figura N° 16 Algoritmos y transmisión de claves

Al mensaje no cifrado se le llama texto en claro (*plaintext* en inglés) para distinguirlo del texto encriptado *o* cifrado (*ciphertext* en inglés), también conocido como criptograma. Al proceso de cifrado, llamado cifrar, también se le llama encriptar y al proceso de descifrado se le llama descifrar o desencriptar.

Un criptosistema es un sistema diseñado para cifrar y descifrar información. La clave (*key*) es una pieza fundamental en la criptografía. En un sistema simétrico existe una sola clave que se utiliza para cifrar y descifrar el mensaje. En un sistema asimétrico existen 2 claves: una para cifrar y otra para descifrar el mensaje.

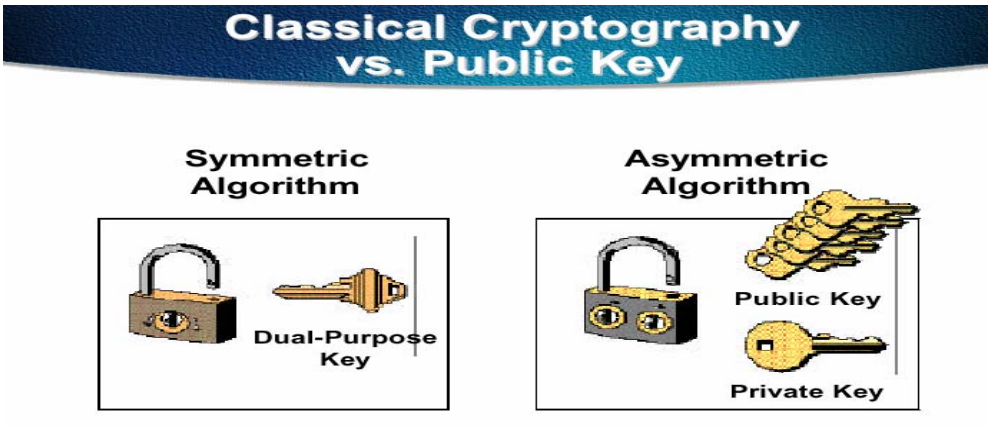


Figura N° 17 Criptografía simétrica y asimétrica

Los criptógrafos, tradicionalmente, han utilizado algoritmos muy sencillos y han confiado en claves largas para su seguridad. En la actualidad, se puede hacer un algoritmo de cifrado tan complicado e intrincado que, incluso si el criptoanalista consigue grandes cantidades de texto cifrado de su propia elección, no tiene ninguna posibilidad de obtener de él nada con sentido. De manera que se pueden utilizar las mismas ideas básicas de la criptografía tradicional, es decir, los conceptos de transposición y substitución, pero con un énfasis diferente.

Las transposiciones y substituciones pueden instrumentarse en hardware con circuitos electrónicos relativamente muy sencillos o en software mediante algoritmos y tablas.

El DES (*Data Encryption Standard*) es un cifrador basado en estos elementos y fue desarrollado en 1974 por IBM como respuesta a una invitación pública del NBS (*National Bureau of Standards*) dirigida a promover estándares criptográficos, tanto para uso del gobierno como de entidades privadas. Los detalles del algoritmo fueron publicados en 1977.La necesidad de que el proceso de cifrado y descifrado fuera
rápido llevó a diseñarlo para poder ser fabricado en hardware, pero posteriormente y con la llegada de computadoras cada vez más rápidas, el sistema se fue aplicado también en forma de software. El cifrado del texto en claro se realiza en bloques de 64 bits, produciendo así 64 bits de texto cifrado. El algoritmo utiliza una clave K de 56 bits. Internamente se realizan 16 iteraciones, y en cada iteración se utiliza una clave K_i que en una variante de la clave original.

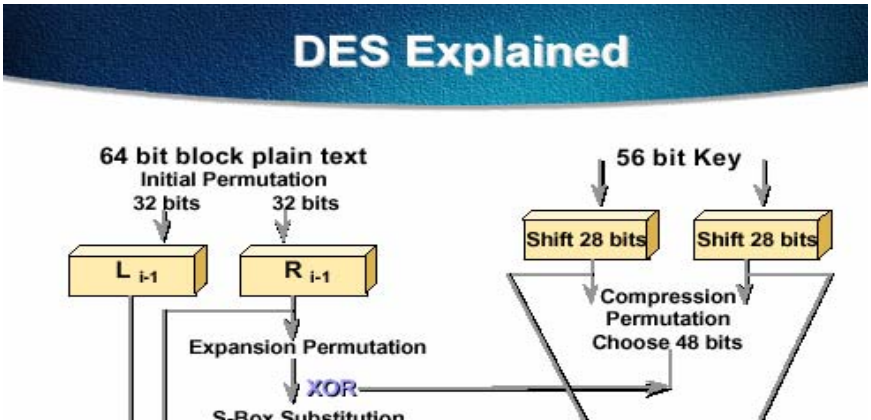


Figura N° 18 Sistema DES

El DES, así como muchos otros sistemas criptográficos convencionales, utiliza la misma clave secreta tanto para cifrar la información como para descifrarla. Por tal razón es llamado criptosistema simétrico. Entre otros sistemas simétricos que tratan de desplazar al DES están: el triple DES ó 3DES, IDEA, SAFER, CAST, Blowfish, Skipjack, RC2, RC4, RC5, AES.

Sin embargo, el problema de la distribución de claves es uno de los principales obstáculos de la criptografia simétrica. La criptografía asimétrica o de clave pública solventa estas deficiencias. Una de las aplicaciones más interesantes de la la criptografía de clave pública es en la firma digital.

La firma digital suministra un modo de verificar que el documento fue originado por la persona que lo envió y que el documento no ha sido alterado en el camino (autenticidad). Además impide que el remitente pueda negar el haber enviado ese mensaje (firma digital). La autenticidad es necesario, por ejemplo, en sistemas financieros. Cuando un cliente le ordene a un banco la compra de una mercancía, el banco necesita tener la seguridad de que la orden es genuina y no fue dañada o

alterada en el camino. La firma digital se necesita con objeto de proteger al banco contra un posible daño. Supóngase que el banco compra la mercancía, e inmediatamente después de esto, el precio de la mercancía cae abruptamente. Un cliente deshonesto podría aducir que él jamás emitió la orden para comprar dicha mercancía. Cuando el banco presente el mensaje ante un juez, el cliente podría negar haber enviado dicha orden. El juez mediante la firma digital puede comprobar que más nadie pudo haber enviado esa orden.

Función Hash

Una función hash se usa para crear un extracto o digesto del mensaje (message digest) que puede ser usado para generar la firma digital. Se procesa un mensaje para producir un condensado del mensaje, luego se encripta el extracto del mensaje con la clave privada y se envía anexo al mensaje. Cuando el receptor recibe el mensaje, procesa el mensaje con la misma función hash, descifra el extracto y lo compara con el que el que él obtuvo. Si son iguales, el mensaje se considera válido y no alterado. Además no puede ser repudiado.

Así, el proceso de firma de un mensaje se compone de dos pasos: el primero es la ejecución del proceso hash sobre el mensaje a firmar H(M), que genera una huella digital. La huella digital hash resultante se encripta con la clave privada produciendo la firma digital E[H(M)] y se envía al destinatario junto con el mensaje.

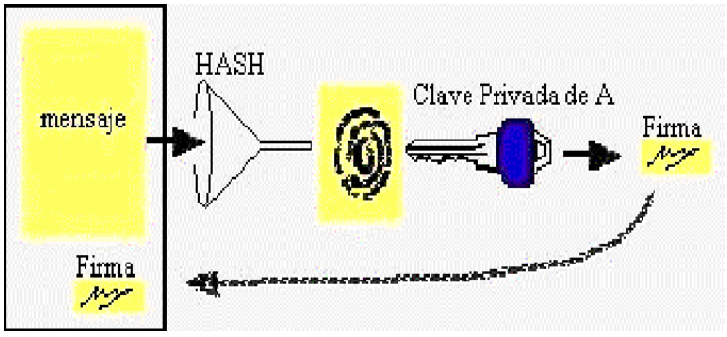


Figura N° 19 Firma Digital: resumen encriptado de un mensaje

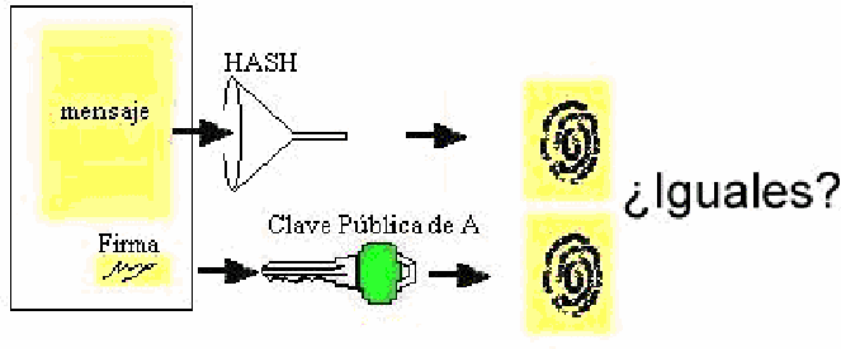


Figura N° 20 Prueba de la autenticidad de un mensaje

Propiedades de las funciones Hash:

- No existen colisiones: No es posible encontrar dos mensajes diferentes M y M´ que produzcan la misma huella digital. Es decir Hash(M) < > Hash(M') siempre que M < > M‘. Con esto se impide adulteraciones del mensaje en tránsito.
- Irreversible: A partir de una huella digital es imposible encontrar un mensaje que genere esta misma huella. Con esto se impide adjuntar una firma de un mensaje a otro mensaje.

La función hash es entonces una función de una sola vía, pero con la condición adicional de que aunque se conozca P, debe ser virtualmente imposible generar otro mensaje adulterado P' que produzca el mismo resultado. Además debe ser de conocimiento público, ya que también el

destinatario la aplica al mensaje. Los mensajes puede ser de diferentes tamaños, pero la función H es usualmente de longitud fija (típicamente 128 bits o 160 bits).

1.6 Redes Virtuales Privadas (VPN)

Luego de describir los conceptos relacionados con la criptografía se explicará la técnica y utilidad de las redes virtuales privadas. Para ilustrar la situación se considerará inicialmente un enlace digital dedicado.

El costo de un enlace dedicado alquilado se incrementa con la distancia, como se ilustra en la figura N° 21 (a). Sin embargo, Internet puede usarse para suministrar la parte de larga distancia de la conexión y reducir substancialmente el costo de los enlaces WAN, como se muestra en la figura N° 21 (b).

Nótese que la configuración mediante VPN todavía usa una línea de 64 kb/s para llegar al proveedor local de servicios Internet al otro lado del enlace, pero la distancia es mucho menor. Los costos pueden disminuir de miles de dólares a cientos de dólares cada mes.

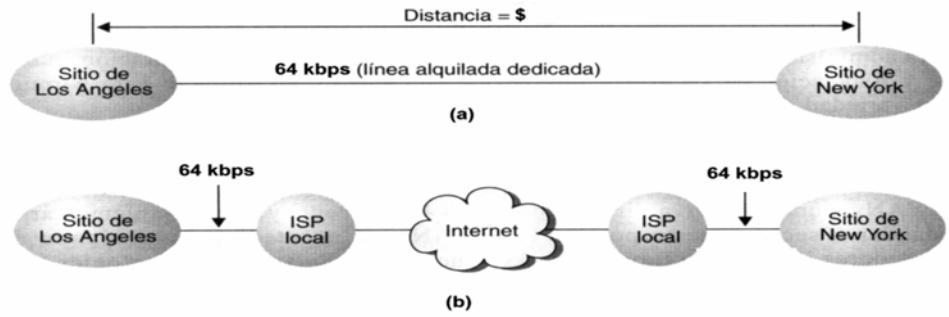


Figura N° 21 Comparación entre línea dedicada y VPN

La figura N° 22 ilustra el viejo método de implementar el acceso remoto para teletrabajadores y usuarios móviles. Se configura un RAS

(*Remote Access Server*) y un banco de módem para recibir llamadas. Se necesitan bastantes líneas telefónicas de entrada para cada módem, además de pagar los costos de todas las líneas si los usuarios remotos llaman desde sitios distantes.

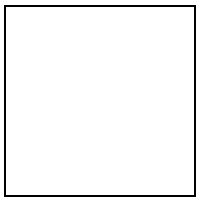


Figura N° 22 Una conexión RAS convencional

La figura N° 23 muestra cómo cambian las cosas al llevar los servicios de acceso remoto al ISP. Ahora se tiene una línea para acceder al ISP y los usuarios remotos usan Internet para acceder a la red corporativa.

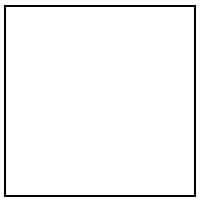


Figura N° 23 Una conexión por Internet

caso típico sería el de un usuario que trabaja en la oficina conectado a la red local (LAN). Cuando llega a casa, puede conectarse a la LAN mediante el RAS (algo caro si no se encuentra ubicado en la misma área metropolitana que su empresa). Con una VPN, el usuario puede conectarse a Internet desde casa, navegar, leer el correo, chatear, y abrir una sesión de cliente VPN con el cual conectarse a la LAN de su empresa y usar todos los recursos de ésta para trabajar.

Básicamente, la tecnología VPN conforma un canal de comunicaciones encriptado seguro a través de Internet para oficinas remotas, usuarios móviles y socios comerciales. En lugar de alquilar una línea dedicada (circuito) entre dos sitios, es a menudo mucho mejor crear un circuito virtual a través de una red pública. Todo aquel que use la red comparte los costos, en oposición a las líneas alquiladas dedicadas para las cuales la organización paga todos los costos aunque pudiera no utilizarla el 100% del tiempo.

Un aspecto importante de las VPN por medio de Internet es que ellas enriquecen las comunicaciones, facilitando flexibilidad de comunicación entre clientes, proveedores, socios de negocio y otros, lo cual permite a los usuarios establecer comunicación con cualquier socio de negocio, no sólo algunos.

Pero Internet no está diseñada para ofrecer la calidad de servicio ni la seguridad que se requiere en muchas aplicaciones. Estos aspectos y otros son los que se deben considerar cada vez que vayan a enviar datos importantes de una corporación vía una red en la cual nadie tiene prácticamente el control. En todo caso, si se transmite información sensible al retardo o urgente, VPN sobre Internet no ser la mejor solución porque puede encontrar problemas de rendimiento debido a los retardos.

Los requisitos para VPN basadas en Internet se puede agrupar en cuatro áreas principales: compatibilidad, interoperabilidad, disponibilidad y, evidentemente, seguridad.

Compatibilidad

Para que una VPN pueda utilizar Internet, debe ser compatible con el protocolo de Internet (IP). Sin embargo, la mayoría de redes privadas emplean direcciones IP privadas o no-oficiales, provocando que únicamente

unas pocas puedan ser empleadas en la interacción con Internet. La razón por la que sucede esto es simple: la obtención de un bloque de direcciones IP oficiales suficientemente grande como para facilitar un *subnetting* resulta imposible. Las subredes simplifican la administración de direcciones así como la gestión de los routers y conmutadores pero malgastan direcciones muy preciadas.

Actualmente existen tres técnicas básicas con las que poder obtener la compatibilidad deseada entre las redes privadas e Internet: la conversión a direcciones Internet mediante NAT (*Network Address Traslation*), la instalación de pasarelas (*gateways*) IP, y el empleo de encapsulamiento (*tunneling*).

Seguridad

Debe considerarse seriamente la seguridad cuando se usa Internet. Las comunicaciones ya no van a estar confinadas a circuitos privados, sino que van a viajar a través de Internet, que es considerada una red “demasiado pública” para realizar comunicaciones privadas. Aunque puede parecer poco probable que alguien monitoreando una línea consiga capturar información y hacer uso de ella, la posibilidad existe. Sin embargo y aplicando las correspondientes medidas de protección y seguridad, Internet puede convertirse en una red altamente privada y segura. Para eso la encriptación es muy importante. Cuando la información está encriptada, se requiere una clave para desencriptarla. Los usuarios en cada extremo deben tener las claves adecuadas para encriptar y desencriptar los datos. Si se está configurando una conexión con una sucursal es fácil administrar este intercambio de claves. Sin embargo, si un usuario remoto accede a la red corporativa, se necesita un modo de verificar quién es y un modo de

intercambiar las claves para la encriptación. Las claves públicas y las firmas digitales son los que más de utilizan para este propósito.

Disponibilidad

La disponibilidad viene motivada principalmente por dos variables: una accesibilidad plena e independiente del momento y del lugar, y un rendimiento óptimo que garantice la calidad de servicio ofrecida al usuario final.

La calidad de servicio (*QoS – Quality of Service*) hace referencia a la capacidad que dispone una red para asegurar un cierto nivel de funcionamiento extremo a extremo. La QoS puede venir dada como una cierta cantidadde ancho de banda o un retardo que no debe sobrepasarse o bien como una combinación de ambas. Actualmente, la entrega de datos en Internet es realizada de acuerdo al mejor esfuerzo (*best effort*) lo cual no garantiza la calidad de servicio demandada. No obstante y en un breve espacio de pocos años, Internet será capaz de suplir esta carencia ofreciendo un soporte para la QoS a través de un conjunto de protocolos emergentes entre los que cabe destacar DiffServ (*Differential Services*), RSVP (*Resource ReSerVation Protocol*) y RTP (*Real Time Protocol*). Por ahora, los proveedores deberán seguir proporcionando la QoS de las VPNs haciendo uso del tráfico CIR (*Committed Information Rate*) en Frame Relay u otras técnicas.

Interoperavilidad

Las implementaciones de los tres primeros requisitos han provocado la aparición de un cuarto: la interoperabilidad. Los estándares sobre tunneling, autenticación, encriptación y modo de operación ya mencionados anteriormente son de reciente aparición o bien se encuentran en proceso de

desarrollo. Por esta razón, previamente a la adquisición de una tecnología VPN, se debe prestar una cuidadosa atención a la interoperabilidad extremo-a-extremo. Esta responsabilidad puede residir tanto en el usuario final como en el proveedor de red, dependiendo de la implementación deseada. Una manera de asegurar una correcta interoperabilidad radica en la elección de una solución completa ofrecida por un mismo fabricante.

Una vez vista la relevancia que presentan estas cuatro áreas para las VPN, se procederá a realizar una breve descripción de los principales protocolos disponibles, los cuales permiten alcanzar en general unos resultados satisfactorios, principalmente en las áreas de seguridad y compatibilidad.

IPSec

IPSec representa un conjunto de mecanismos de seguridad de alta calidad basado en claves criptográficas. Proporciona un canal seguro para los datos a través de la red, ofreciendo para ello un control de acceso, así como una integridad en los datos transmitidos además de mecanismos de autenticación y confidencialidad. IPSec opera sobre la capa 3 de red.

Los servicios IPSec son llevados a cabo mediante el uso de dos protocolos de seguridad: *Authentication Header (AH)* y *Encapsulating Security Protocol (ESP)*, así como mediante un conjunto de protocolos necesarios para la gestión de llaves criptográficas, llamado IKE (*Internet Key Exchange*).

El protocolo AH proporciona únicamente mecanismos de autenticación. Los datos AH son insertados entre la cabecera IP y los datos referentes al paquete de nivel superior (TCP, UDP, ICMP), tal como se muestra en la figura N° 24.

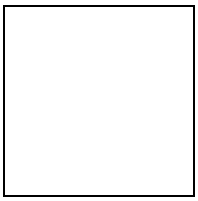


Figura N° 24 Un datagrama IPSec y el header AH

En la figura N° 25 se ilustra la estructura del campo AH, cuyos campos son los siguientes:

- *Next Header* (8 bits): Identifica el tipo de datagrama llevado (ej. TCP).
- *Payload Length* (8 bits): Longitud del header en múltiplo de 32 bits. El valor normal El valor normal es 4 y no 6, ya que por convención se resta 2.
- *Reserved* (16 bits): Este camplo es para uso futuro.
- *Security Parameters Index* (32 bits): Este campo identifica a una SA (security association).
- *Sequence Number* (32 bits): Es un contador que se incrementa monotónicamente.
- *Authentication Data* (variable): Contiene el *Integrity Check Value* (ICV), o MAC, para ese datagrama.

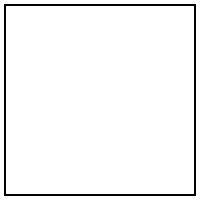


Figura N° 25 Detalles del header AH

El protocolo ESP, en cambio, proporciona mecanismos de autenticación y además de encriptación. ESP hace uso de una amplia

variedad de algoritmos de encriptación entre los cuales cabe destacar DES, 3DES, CAST128 y *Blowfish*. Tanto AH como ESP, dispone de dos modos de uso: modo transporte y modo túnel. En el modo transporte AH o ESP es insertado entre la cabecera IP y los datos de niveles superiores (TCP, UDP, ICMP). En el modo túnel en cambio, se añade una nueva cabecera IP que puede contener direcciones distintas, tales como las direcciones de los gateways de seguridad. La cabecera IP interna transporta las direcciones fuente y destino. En cuanto al proceso de inserción, es totalmente idéntico al realizado en el modo transporte. A continuación se muestran los datagramas correspondientes y la estructura del header ESP.

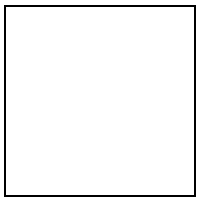


Figura N° 26 Estructura de los datagramas

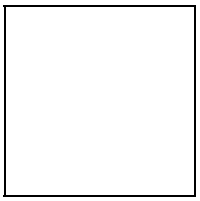


Figura N° 27 Detalles del header ESP

El protocolo de autenticación empleado con IPSec se encuentra especificado de acuerdo a la *Security Association (SA)* e incluye códigos de autenticación de mensajes (MAC) basados en algoritmos de encriptación simétrica como DES y funciones hash tales como MD5 y SHA-1.

La SA utilizada para llevar a cabo la autenticación representa una conexión unidireccional para la cual se definen todos los servicios de

seguridad que deben ser aplicados al tráfico de red. Las SAs pueden ser creadas tanto automáticamente como manualmente, empleando para ello el protocolo IKE (*Internet Key Exchange*), que es una variante de ISAKMP/Oakley (*Internet Security Association and Key Management Protocol/Oakley Key Determination Protocol*). Este protocolo presenta tres características principales:

- Asegura que la comunicación IPSec y el intercambio de claves se lleve a cabo entre partes autenticadas.
- Negocia los protocolos, algoritmos, y claves que serán utilizados en la comunicación IPSec.
- Proporciona un método seguro para actualizar y renegociar asociaciones una vez que éstas han expirado.

IKE dispone de dos fases. En la primera, los hosts crean una asociación bidireccional estableciendo con ello un canal seguro entre ellos. Ya en la segunda fase, este canal será empleado para realizar la negociación de las asociaciones IPSec.

IPSec utiliza el identificador de protocolo 51 en el paquete IP para AH y el identificador 50 para ESP. IPSec IKE (*Internet key exchange*) utiliza el puerto UDP 500.

Como ejemplo, en una sesión Telnet con IPSec en modo transporte y protocolo ESP, el encabezado IP contiene el valor 51 en su campo *Next Header* y en el campo ESP, el campo *Next Header* contiene el valor 6 (TCP), mientras que en el encabezado TCP, Telnet queda identificado por el puerto 23. Si en cambio se usa el modo tunel, entonces el campo *Next Header* en ESP contiene el valor 4 (*IP-in-IP*), lo que significa que todo el paquete IP original es la carga útil.

PPTP - Point-to-Point Tunneling Protocol

PPTP es un protocolo de red creado por Microsoft que permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet. En el escenario típico de PPTP, el cliente establecerá una conexión *dial-up* con el servidor de acceso a red (NAS) del proveedor del servicio, empleando para ello el protocolo PPP. Una vez conectado, el cliente establecerá una segunda conexión con el servidor PPTP (necesariamente Windows NT/2000) el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada.

PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y desencriptados de acuerdo al protocolo de red transmitido. Por el momento, PPTP únicamente soporta los protocolos de red IP, IPX, y NetBEUI. El protocolo PPTP especifica además una serie de mensajes de control con el fin de establecer, mantener y destruir el túnel PPTP. Estos mensajes son transmitidos en paquetes de control en el interior de segmentos TCP. De este modo, los paquetes de control almacenan la cabecera IP, la cabecera TCP, el mensaje de control PPTP y los *trailers* apropiados.

La autenticación PPTP está basada en el sistema de acceso de Windows NT/2000, en el cual todos los clientes deben proporcionar un par login/password. La autenticación remota de clientes PPTP es realizada empleando los mismos métodos de autenticación utilizados por cualquier otro tipo de servidor de acceso remoto (RAS). En el caso de Microsoft, la autenticación utilizada para el acceso a los RAS soporta los protocolos

CHAP, MS-CHAP, y PAP. Los accesos a los recursos NTFS o a cualquier otro tipo, precisa de los permisos adecuados, para lo cual resulta recomendable utilizar el sistema de archivos NTFS para los recursos de archivos a los que deben acceder los clientes PPTP. En cuanto a la encriptación de datos, PPTP utiliza el proceso de encriptación de secreto compartido en el cual sólo los extremos de la conexión comparten la clave. Dicha clave es generada empleando el estándar RSA RC-4 a partir del password del usuario. La longitud de dicha clave puede ser 128 bits o 40 bits.

L2F - Layer 2 Forwarding

El protocolo L2F, desarrollado por Cisco Systems, tiene como objetivo proporcionar un mecanismo de tunneling para el transporte de tramas a nivel de enlace (HDLC, PPP, SLIP, etc). El proceso de tunneling involucra tres protocolos diferentes: Protocolo pasajero, protocolo encapsulador, y protocolo portador. El protocolo pasajero representa el protocolo de nivel superior que debe encapsularse (PPP, SLIP, etc). A continuación, el protocolo encapsulador indica el protocolo que será empleado para la creación, mantenimiento y destrucción del túnel de comunicación. En este caso, el protocolo encapsulador será L2F. Por último, el protocolo portador será el encargado de realizar el transporte de todo el conjunto. Por lo general, este protocolo suele ser IP dadas sus capacidades de enrutamiento, su acople a los diferentes medios y su estandarización dentro del ámbito de Internet.

Entre las principales ventajas que ofrece el protocolo L2F, cabe destacar el soporte multiprotocolo, la multiplexación de múltiples sesiones remotas (minimizando el número de túneles abiertos en un momento dado), y la gestión dinámica de los túneles, en la cual los recursos de los

servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario. Además, por cada túnel L2F establecido, el proceso de seguridad genera una clave aleatoria como medida de prevención ante posibles ataques basados en falsificación de la fuente (*spoofing*). A su vez, en el interior de los túneles, cada una de las sesiones multiplexadas mantiene un número de secuencia para evitar problemas debidos a la duplicidad de paquetes.

L2TP - Layer 2 Tunneling Protocol

Creado como combinación de los protocolos L2F y PPTP, permite la creación de túneles a través de una gran variedad de redes (IP, SONET, ATM) para el transporte de tráfico PPP. Dado que el protocolo pasajero es PPP, L2TP hereda el mecanismo de autenticación de éste, al igual que los protocolos empleados para el control de la encriptación (ECP) y la compresión (CCP), además de incluir un soporte propio de autenticación que podrá ser empleado en ambos extremos del túnel.

Los túneles L2TP pueden llevarse a cabo tanto en redes públicas IP como no-IP. Esto provoca que tanto los paquetes de control como los paquetes de datos sean vulnerables frente a posibles ataques como *snooping,* denegaciones de servicio, modificaciones, o incluso interceptación de los procesos de negociación de la encriptación (ECP) y de la compresión (CCP) con el fin de provocar la supresión de los mecanismos de confidencialidad o en su caso, obtener el acceso a los passwords de los usuarios. Para evitar todas estas posibles situaciones, el protocolo de seguridad deberá proporcionar autenticación así como mecanismos para asegurar la integridad y la protección de los paquetes de control, además de la confidencialidad de todos los paquetes. Para poder alcanzar este nivel, es necesario implementar IPSec-ESP. No obstante, esta utilización de IPSec requiere un soporte para la todos los algoritmos de cifrado.

Firewalls / VPN

La mayoría de las organizaciones hoy día protegen sus instalaciones mediante firewalls y filtros de paquetes. Estos dispositivos deben configurarse para que permitan pasar el tráfico VPN. En la figura N° 73 se muestra la configuración típica, donde el servidor VPN está colocado detrás del firewall, en la zona desmilitarizada (DMZ) o en la propia red interna. En la práctica muchos firewalls incorporan un servidor VPN (Figura N° 28), pero desde el punto de vista lógico se puede considerar que corresponde a la figura N° 29.

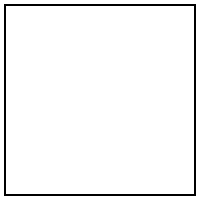


Figura N° 28 Firewall y VPN

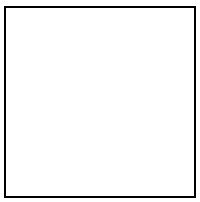


Figura N° 29 VPN + firewall

Las reglas del firewall deben permitir el tráfico PPTP, L2TP e IPSec en base a los puertos utilizados. PPTP usa el puerto TCP 1723 y además usa GRE (*generic route encapsulation*) para el mantenimiento del tunel. GRE tiene el identificador de protocolo 47 en el paquete IP. L2TP usa el puerto UDP 1701 para L2TP.

Capítulo 2

Solución Planteada para la WAN Segura

2.1 Situación Actual de la Plataforma INE-Red Platino

El Instituto Nacional de Estadística (INE), mediante el diseño y puesta en producción de modernos sistemas de bases de datos en ambiente Web, mejora considerablemente la fase de procesamiento de la información estadística. Sin embargo, existen serios inconvenientes en las fases de recolección y divulgación de información, motivado principalmente a la carencia de una plataforma tecnológica que soporte tales servicios.

El sistema actual basado en la mensajería tradicional, la comunicación telefónica y el uso de los servicios gratuitos de correo electrónico suministrados por los portales de Internet, presenta las siguientes deficiencias:

- Retraso constante en el envío y recepción de datos
- Limitaciones en el volumen de datos transmitidos por sesión
- Reducida cobertura geográfica
- Carencia de confidencialidad en el tratamiento de la información
- Dificultad en el establecimiento del origen genuino de los datos
- Peligro de adulteración o modificación de los contenidos
- Falta de elementos de seguridad adicionales, como disponibilidad y no repudiación de los datos

Otro aspecto capital es la disposición de la información para el ente o persona que la requiera en medios de fácil y amigable acceso. Gran parte de la información estadística se suministra actualmente en CD-ROM, los cuales son distribuidos en la sede principal de INE ubicada en Maripérez, adoleciendo de operatividad para la mayor parte de los usuarios. También puede obtenerse información a través del sitio Web de INE, pero la misma es escasa. La incorporación de los nuevos contenidos, como se indicó, es una

tarea que se realiza en estos momentos, pero se precisa de la plataforma de acceso a los mismos.

El presente proyecto tiene como propósito general la implantación de la nueva red de transporte de datos para solucionar los problemas planteados.

2.2 Desarrollo de la Solución para la WAN de INE

La implantación de la WAN Segura de INE se realizará según las siguientes fases:

I. Estudio del flujo de datos
II. Diseño de la topología, arquitectura y plan de direccionamiento IP de la WAN de INE
III. Diseño de las políticas y técnicas de seguridad como túneles VPN, disposición de firewalls, accesos restringidos, etc.
IV. Diseño y desarrollo de las LANs seguras de los nodos regionales en las capitales de estado. Para este proyecto sólo se implantarán tres nodos a nivel de prueba, correspondientes a: Maracay, Valencia y Maracaibo. En el futuro, se prevee extenderlo a todas las capitales de estado
V. Reorganización de la LAN Platino. Esta fase implica la introducción en la red de elementos de seguridad, control de tráfico y limitación de tráfico de las instituciones independientes de INE pero conectadas a Red Platino, ubicada en Torre Este, Piso 6, Parque Central
VI. Reorganización de la LAN INE. Esta fase incluye la segmentación de la red LAN ubicada en el Edificio Fundación La Salle, Av. Boyacá. También la incorporación de elementos de

seguridad y reubicación de servidores de aplicaciones, Web y bases de datos.

VII. Implantación de un sistema de contingencia en caso de fallas en la red principal.

VIII. Supervisión y monitoreo de la WAN.

En este capítulo se aplican las técnicas, métodos y normas descritas en los diversos nodos que compondrán la red. Los detalles de configuración y cableado de equipos se tratan en capítulo posteriores.

2.3 Fase I: Estudio del flujo de datos

Los datos estadísticos se producen a lo largo de todo el país. Los nodos regionales tienen la responsabilidad de recoger la información en forma casi inmediata de su origen (aduanas, hospitales, centros de producción, etc). Dos portales web denominados www.sistine.gov.ve y www.sen.gov.ve, ubicados físicamente en la sede de INE, sirven de interfaz para los servidores de aplicación y de base de datos (DBMS) para la actualización y consulta de la información. Desde su origen hasta su utilización, el flujo de información sigue los siguientes pasos con los correspondientes requerimientos:

- Recolección de Datos: En los nodos regionales, denominadas “Coordinaciones del INE”, se recogen los datos directamente en las capitales de estado. Esto requiere el diseño y establecimiento de LANs en cada ciudad. Para el caso de recolección de información fuera de la capital, se utilizarán accesos remotos “túnelizados” mediante “VPN” para la conexión hacia la capital de estado. De este modo los encuestadores y el personal operativo podrán transmitir la información desde cualquier punto. El establecimiento del nodo

regional exige la existencia de un firewall para la protección de la LAN, así como las funciones complementarias de NAT saliente y DHCP para la mejor administración de las direcciones IP y de un Proxy para ahorrar ancho de banda. Un aspecto fundamental es la creación del túnel VPN entre el nodo regional y Red Platino en Caracas. El túnel será utilizado sólo para transmitir los datos estadísticos corporativos. Otros tipos de tráfico, como el de Internet, no utilizará el túnel y será enviado directamente a Red Platino para su tratamiento.

- Envío de Datos: Para la transmisión de información serán utilizados túneles VPN sobre red ATM/Frame Relay de CANTV. Los routers regionales poseerán circuitos virtuales hacia Red Platino, que actuará como puente hacia la LAN de INE. Los routers principales de Red Platino permitirán el paso de los túneles hacia INE para la información estadística. Sin embargo, el tráfico no corporativo será tratado directamente por los routers de Red Platino. Dentro de este tipo de tráfico se encuentra el que pueda estar dirigido a cualquiera de las instituciones conectadas a Red Platino (más de 90) o dirigido a los servidores públicos de Web, Correo o FTP de Red Platino. La conexión entre Red Platino e INE se realiza mediante un enlace dedicado de 256 Kb/s. La creación de los nodos regionales requiere de la adecuación de la Red Platino actual.

- Utilización de los Datos: El tráfico de datos llega, como se indicó, a dos portales principales. De aquí, tras una fase de autenticación, se logra el acceso a los servidores de aplicación y de base de datos. La información es luego analizada y procesada por expertos para finalmente producir las tablas que podrán ser consultadas en

www.ine.gov.ve, convertidas en libros, folletos u otras formas impresas o ser expendidas, como se prevee en un futuro próximo, a través de comercio electrónico. En la (Figura N° 30) se muestra el esquema general de la WAN.

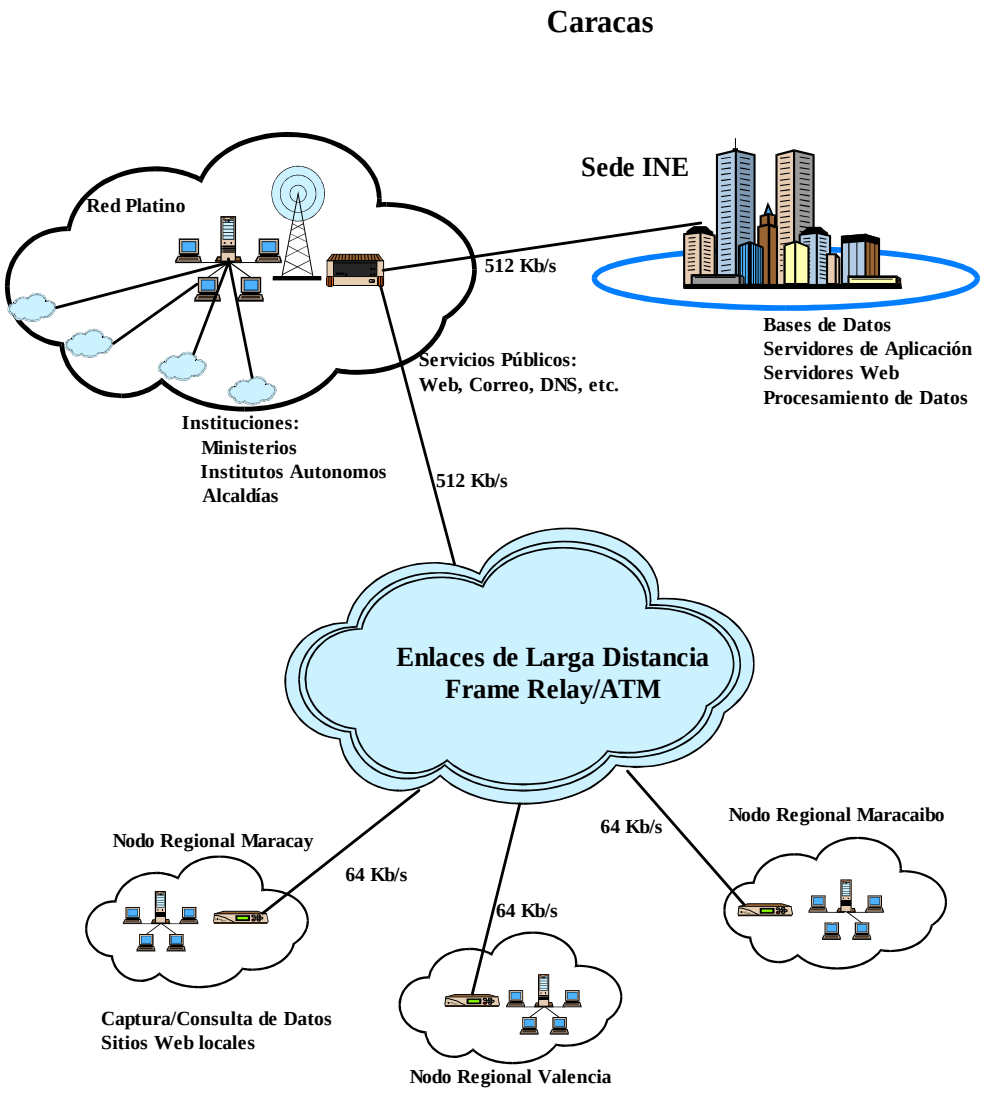


Figura N° 30 Diagrama General de la WAN

2.4 Fase II: Topología, Arquitectura y Planes de Enrutamiento y Direccionamiento IP

La idea fundamental de la WAN segura de INE es conectar los nodos regionales a Red Platino y, de ahí, acceder a la Red INE. Esta estructura obedece a que en Red Platino están concentradas las comunicaciones de aproximadamente cien instituciones gubernamentales además de servicios públicos y el acceso Internet.

El enrutamiento de las comunicaciones entre los nodos regionales y Red Platino se realizará mediante enlaces Frame Relay, mientras que entre Red Platino e INE será a través de enlaces dedicados con las siguientes características:

- Enlace entre cada nodo regional (Maracay, Valencia, Maracaibo) y Red Platino:

  Tipo: Frame Relay
  Proveedor del servicio: CANTV
  Velocidad de línea: 128 Kb/s
  C.I.R (Commited Information Rate): 64 Kb/s
  Puertos DLCI: Serán asignados por el proveedor durante el mes de Julio del 2003

- Enlace entre Red Platino y Red INE (*):

  Tipo: Enlace Dedicado (TDI)
  Proveedor del servicio: CANTV
  Velocidad: 256 Kb/s
  Encapsulamiento: HDLC

Adicionalmente al enlace dedicado, Red Platino-INE utilizarán un enlace inalámbrico Ethernet 802.11 a 10 Mb/s como medio de contingencia.

Se estima que las velocidades elegidas son aplicables por cuanto la mayor parte del flujo de datos es código ASCII, existiendo muy pocas

imágenes u otro tipo de información. Luego, con un monitoreo constante se evaluarán los enlaces para posibles mejoras.

En cuanto al direccionamiento IP, actualmente Red Platino posee cuatro bloques de direcciones IP, suministradas por las empresas proveedoras de servicio Internet CANTV Servicios y Global One. Estos son:

200.44.63.0/24, 245 direcciones, CANTV
200.44.64.0/24, 256 direcciones, CANTV
209.88.103.0/24, 256 direcciones, Global One
161.196.215.64/26, 64 direcciones, CANTV

El uso de las mismas es como sigue:

- Bloques 200.44.64.0/24 y 209.88.103.0/24: Se emplean para realizar traducciones de direcciones privadas a públicas (NAT). Internamente, en Red Platino, INE y las instituciones se utilizan las direcciones 172.20.0.0/16 y 172.197.0.0/24, las cuales, al requerirse conexiones hacia el exterior de la red, son convertidas por los enrutadores en algunas de las indicadas en los bloques. Se realiza el servicio NAT de dos formas: dinámico (para las estaciones de trabajo que desean acceder el exterior de la red) y estático (para aquellos servidores que requieren ser accedidos en forma pública desde el exterior y, por tanto, deben ser “vistos” mediante direcciones válidas).

- Bloque 161.196.215.64/26: Las direcciones de este bloque están asignadas a los servicios propios de red Platino a ser accedidos por las instituciones, como Web, correo, DNS, entre otros. Por ejemplo, el servidor de correo posee la 161.196.215.67, el de Web/DNS la 161.196.215.65, etc. Los servidores de respaldo también están dentro de este grupo.

- Bloque 200.44.63.0/24: Este bloque no se encuentra en uso actualmente. De él se tomarán las direcciones válidas requeridas en INE y en los nodos regionales, según se detalla más adelante.

Para cubrir la necesidad de direcciones IP en todo el sistema se requiere el uso de direcciones privadas (no válidas) para las estaciones de trabajo en general y de direcciones públicas (válidas) para aquellos servicios o máquinas que deben ser accedidos públicamente. Se plantea el siguiente esquema:

- Uso de direcciones privadas del bloque 192.168.0.0/16 para las redes internas de Platino, INE y los nodos regionales. Se usará el formato:
- 192.168.X.0, donde X indica la ubicación física del bloque de direcciones
- Uso de direcciones públicas del bloque 200.44.63.0/24 en las redes INE y nodos regionales (red Platino no requiere) para aquellos servicios o servidores (VPN, Web, etc) que requieran ser accedidos desde el exterior. Se usará el formato 200.44.63.Y, donde Y indica la ubicación física del bloque de direcciones.

Asignación de Direcciones IP

Las direcciones IP que se utilizarán serán tomadas de los bloques 161.196.215.64/26 y 200.44.63.0/24 suministradas por la empresa CANTV. A partir de estas direcciones se tomarán grupos de IP para su asignación a los servidores y para proporcionar mediante servicios NAT y PAT acceso a las estaciones de trabajo hacia otras redes.

En la Tabla N° 4 se indican los “subnetting” realizados a dichos bloques.

Red	Direcciones públicas	Direcciones privadas
INE	200.44.63.0/26 (64 direcciones)	192.168.0.0/24 192.168.1.0/24 192.168.2.0/24 (3 x 256 direcciones)
Platino	161.196.215.64/26 (64 direcciones)	192.168.3.0/24 (256 direcciones)
Nodo Maracay	200.44.63.64/29 (8 direcciones)	192.168.10.0/24 (256 direcciones)
Nodo Valencia	200.44.63.72/29 (8 direcciones)	192.168.11.0/24 (256 direcciones)
Nodo Maracaibo	200.44.63.80/29 (8 direcciones)	192.168.12.0/24 (256 direcciones)

Tabla N° 4 Direcciones IP Red Platino

Más adelante serán presentados diagramas con la ubicación física de las direcciones en las redes.

Nodo Regional

En la figura N° 33 se muestra el esquema de direccionamiento de los equipos en el nodo regional. Sólo los equipos marcados con (*) corresponden a los incluidos en el presente proyecto. Bloque 192.168.X.0/24:

- Se usarán las primeras 4 direcciones para los enlaces Red Platino – Nodo Regional, es decir: 192.168.X.0/30
- Se usarán las siguientes 128 direcciones para la red interna del nodo o red protegida, es decir: 192.168.X.4/25

Bloque 200.44.63.Y/29:

- De estas 8 direcciones, 2 se usarán en los puertos enrutador – VPN (Interfaz externa) y las 4 restantes en los servidores del nodo (la primera y la última no se asignan)

Red Platino

En la figura N° 34 se muestra el esquema de direccionamiento de los equipos en el nodo regional. Sólo los equipo s marcados con (*) corresponden a los incluidos en el presente proyecto.

La Red Platino mantendrá el esquema de direcciones válidas existente para los servicios (161.196.215.64/27), e incorporará las direcciones privadas 192.168.3.0/24 para su red interna.

Las direcciones válidas son necesarias en las interfaces externas del equipo de seguridad para el establecimiento de las VPN. De esta forma, las interfaces Ethernet de los enrutadores de INE y los nodos regionales, así como la interfaz externa de equipo VPN/Cortafuegos/NAT/Proxy, requiere este tipo de direcciones.

Las zonas públicas de las redes (desmilitarizadas o DMZ) también usan direcciones válidas. Las redes internas, tal como se observa en las mismas figuras, se organizan con el esquema de direcciones privadas.

Es importante destacar que se aprovechará el nuevo plan de direccionamiento IP para eliminar el uso de los bloques de direcciones que actualmente posee el INE como 172.197.45.0/24 y 172.197.46.0/24, las cuales son válidas y no están autorizadas para esta red. El uso de estos bloques genera conflictos con los servicios de Internet que las empleen.

Red INE

En la figura N° 37 se muestra el esquema de direccionamiento de los equipos en el nodo regional. Sólo los equipos marcados con (*) corresponden a los incluidos en el presente proyecto. Bloques 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24:

- Se utilizarán en su red interna o protegida.

Bloque 200.44.63.0/26:

- De este grupo de 64 direcciones, 2 se asignarán a los interfazs enrutador - VPN (Interfaz Externa) y 60 a los servidores o servicios públicos de INE (Bases de datos, Web, etc.)

2.5 Fase III: Diseño de las Políticas y Técnicas de Seguridad

Las políticas y técnicas de seguridad tienen como objetivo la implantación de las siguientes características en la WAN de INE:

- Integridad: los datos estadísticos no deben ser modificados en su ruta desde los nodos regionales o Red Platino hasta el INE
- Autenticidad: los datos deben provenir del nodo regional o encuestador/operario autorizado para tal fin
- Disponibilidad: deben existir sistemas de contingencia para acceder la los servidores de INE
- Confidencialidad: aunque ésta no es del todo indispensable por tratarse de datos estadísticos, sí es importante cuando para las comunicaciones entre los gerente de las coordinaciones con la junta directiva de INE o cuando, en un futuro próximo, se realice comercio electrónico para la venta de estadísticas.

Para el establecimiento de la seguridad en las comunicaciones se aplicarán las siguientes técnicas:

- Creación de túneles VPN entre los nodos regionales e INE y entre la Red Platino e INE (Figura N° 31). Los túneles serán extensivos a los usuarios remotos que, por motivos geográficos, están alejados de los nodos regionales y deban comunicarse con ellos para el envío de estadísticas al INE (encuestadores, etc.). Lo túneles serán usados sólo para este tipo de tráfico. Las comunicaciones hacia otras instituciones de Caracas o Internet no serán “tunelizadas” aunque utilicen los mismos medios físicos.

- Uso de Firewall / Proxy de capa 7 en todas las redes para el filtrado de tráfico en todos los nodos

- Uso general de direcciones privadas y NAT para el enmascaramiento de las direcciones reales de origen

- Uso de elementos de control de tráfico (como el SQUID e IPTABLES) para aumentar la disponibilidad en nodos congestionados como Red Platino

Figura N° 31 Túneles VPN en la WAN de INE

2.6 Fase IV: Diseño y Desarrollo de los Nodos Regionales

En la Figura N° 32 se presenta el diagrama explicativo de un nodo regional típico.

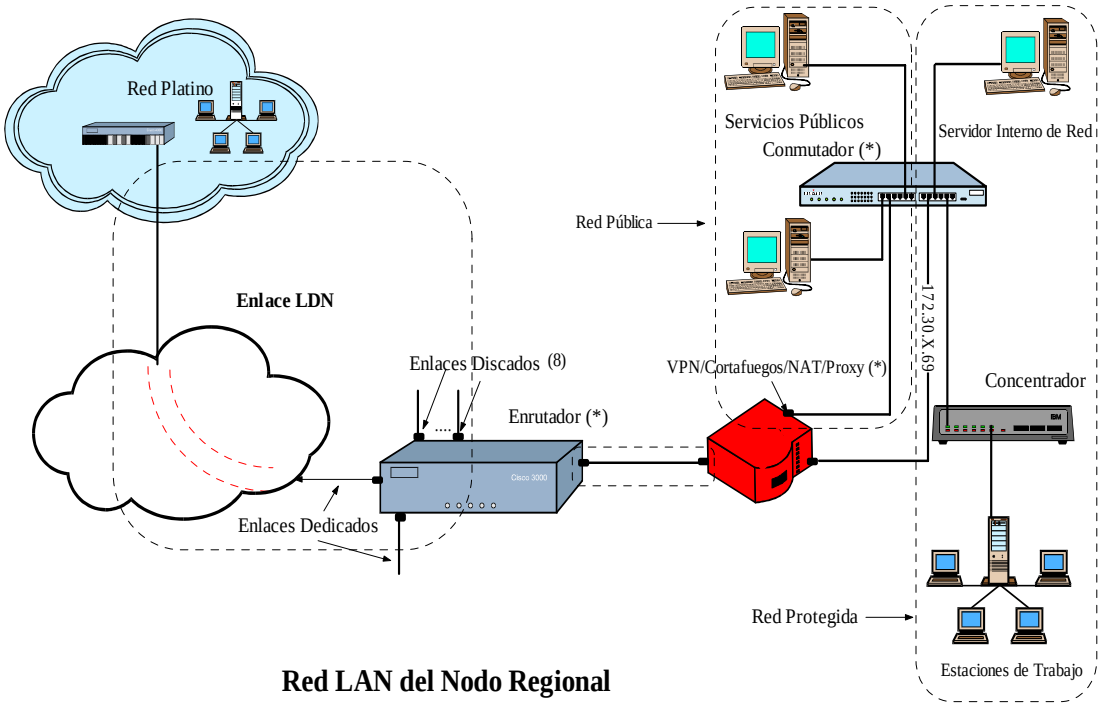


Figura N° 32 Nodo Regional

Los nodos regionales se soportan sobre LAN seguras basadas en el equipo Firebox. A continuación se detallan sus características principales:

- Implantación de un firewall con las tres zonas de seguridad: Externa, DMZ e Interna.
- Establecimiento del túnel VPN entre el nodo regional y Red Platino para el envío de los datos estadísticos

Segmentación de la red

Cada red de los nodos regionales se segmentará en sus porciones Interna, DMZ y Externa. Inicialmente, la zona DMZ no poseerá servidores; solo se instalará un servidor de red y de base de datos local en la red Interna. El equipo Firebox operará en modo enrutado con dirección de red 200.44.63.Y/29, donde "Y" indica el nodo (Los modos "drop-in" y enrutado se explicarán en el siguiente capítulo):

Nodo Maracay: 200.44.63.64/29
Nodo Valencia: 200.44.63.72/29
Nodo Maracaibo: 200.44.63.80/29

Se considera que 8 direcciones válidas por nodo son suficientes para incorporar nuevos servicios regionales. Además, el equipo Firebox requiere direcciones válidas en su interfaz externa. La red interna tendrá direcciones 192.168.X.4/25.

En los nodos se instalarán switches marca Allied Telesyn de 24 puertos, segmentados a 8 puertos por VLAN para el fin propuesto.

Autenticación

Esta característica será usada para reconocer a aquellos usuarios remotos PPTP que, encontrándose en la misma región pero distantes del nodo regional, deban accederlo para transmitir sus datos (encuestas del censo, por ej.). Cada usuario autorizado debe poseer una cuenta en el

equipo Firebox. Esta es en realidad la opción que se usará, aunque el equipo Firebox permite que las cuentas estén depositadas en otros servidores como RADIUS, Windows NT/2000, etc. (ver Capítulo 4). Se establecerán ocho cuentas iniciales por cada nodo regional ya que el router Cisco 4500 estará equipado con ocho enlaces asíncronos para conexiones "dial-up". Se configurará el protocolo de autenticación CHAP por ser más seguro. En el siguiente apartado se indica cómo serán usadas estas cuentas en el establecimiento de túneles VPN para usuarios remotos.

Túneles VPN

Los túneles hacia Red Platino e INE se originan en la interfaz externa del Equipo Firebox. Los túneles VPN entre redes son denominados "Branch Office Virtual Private Network" en la terminología de WatchGuard. Existen opciones para formar túneles entre dos redes usando un Equipo Firebox en cada extremo a través de una red insegura, o entre un Equipo Firebox y un equipo compatible IPSec. En el caso de los nodos regionales se utilizará la segunda opción, por ser la más estudiada públicamente (se debe tener cuidado con tecnologías propietarias desconocidas), formándose túneles IPSec entre cada nodo y la LAN de INE a través de la nube Frame Relay y el enrutador de red Platino, que actuará como puente. Cada nodo regional sólo utilizará el túnel para el envío de datos estadísticos a los servidores de aplicaciones www.sistine.gov.ve y www.sen.gov.ve, ubicados en INE. El tráfico dirigido hacia Internet o hacia otras instituciones gubernamentales, conectadas a Red Platino, no usará el túnel aunque sí el mismo medio físico. La configuración de túneles se realiza en dos partes: primero se crea el túnel con sus características propias y luego, se determina el tipo de tráfico que lo utilizará.

En los nodos regionales, la creación de los túneles tendrán las siguientes características:

Remote Gateway: Es la interfaz remota del túnel. En este caso constituye la interfaz externa del equipo Firebox de INE: 200.44.63.3

Tipo de Negociación de Claves: ISAKMP manual

Clave Compartida: Es un requerimiento de la negociación ISAKMP. Debe ser igual en ambos extremos del túnel

Gateway: Nombre del extremo remoto ("INE")

Túnel: Nombre del túnel a crearse. Se colocará "estadística" por el tipo de datos que fluirá por él

Método: Se usará ESP ("Encapsulating Security Protocol") en modo túnel porque se requiere que los datagramas estén autenticados y encriptados. Se añadirán la nueva cabecera IP, las direcciones IP de las interfaces externas de los equipos Firebox de cada nodo regional y de INE:

Nodo Maracay: 200.44.63.66/29
Nodo Valencia: 200.44.63.74/29
Nodo Maracaibo: 200.44.63.82/29

Esta misma configuración de parámetros se aplica al tráfico saliente y entrante

Valor de SPI: Es el *Security Parameters Index* (32 bits). Este campo viaja dentro del datagrama e identifica a una SA (security association). El Equipo Firebox acepta valores entre 257 y 1023

Cifrado: Para cifrar los datagramas, el equipo Firebox acepta los algoritmos: DES-CBC (56-bits) y 3DES-CBC (168-bits). Se escoge el 3DES por su mayor robustez. El tiempo de cifrado/descifrado no es relevante en este caso por tratarse, en su mayoría, de datos en ASCII

Autenticación: Para comprobar la integridad y autenticidad de los datagramas, el Equipo Firebox utiliza los algoritmos para "hash" MD5-HMAC (128-bits) y el SHA1-HMAC (160-bits). Se toma el segundo por su mayor seguridad.

Clave: Para la autenticación debe agregarse una “passphrase”

Cada Equipo Firebox de los nodos regionales se configura del mismo modo. El Equipo Firebox de INE debe posseer las mismas políticas para los túneles.

Luego de la creación de los túneles se debe establecer el tipo de tráfico que fluirá a través de ellos. Para esto deben crearse las políticas o normas (IPSec Policy) en el equipo Firebox. Como se indicó, sólo el tráfico hacia los servidores www.sistine.gov.ve y www.sen.gov.ve será “tunelizado”, para lo cual se asigna:

Túnel: nombre del túnel que se usará (el establecido anteriormente)
Local: red local que utilizará el túnel. Son las redes internas de los nodos regionales con formato de dirección: 192.168.X.4/25
Remote: Se establecen los servidores remotos indicados y que corresponden a:
200.44.63.4 y 200.44.63.5
Disposition: Se coloca “Secure”. IPSec encriptará todo el tráfico que coincida con esta regla. Si se coloca “Bypass”, no se le aplicará IPSec al tráfico que coincide con la regla.
Dst Port: Son los puertos de destino del tráfico. Se usarán 80 y 443 porque las aplicaciones están realizadas en ambiente Web Seguro
Protocol: TCP
Src Port: Se fija “0” para abarcar todos los puertos de origen

Para el resto del tráfico que se origina en el nodo regional y se dirige a las instituciones conectadas a red Platino e Internet, no se aplicará el túnel, por lo que se usará:

Tunel: nombre del túnel
Local: 192.168.X.4/25
Remote: 0.0.0.0/0
Disposition: “Bypass”
Dst Port: “0” indica todos
Protocol: TCP
Src Port: “0”

Los usuarios remotos que operan en regiones cercanas al nodo regional, lo accederán mediante enlace telefónico, estableciéndose un túnel PPTP para ellos. El equipo Firebox soporta hasta 50 sesiones PPTP simultáneas, lo cual es más que suficiente. El equipo Firebox incluye dos grupos para los usuarios remotos: pptp_users e ipsec_users. Los usuarios remotos via “dial-up” deben pertenecer al grupo pptp_users. Se deben agregar individualmente los usuarios para este tipo de acceso. Luego, deben habilitarse cada uno de los servicios del equipo Firebox (http, SMTP, FTP, etc), para su acceso por parte de los usuarios remotos. Por ejemplo, en el servicio http:

Incoming: Enabled and Allowed
From: pptp_users
To: Any

Outgoing: Allowed
From: Any
To: pptp_users

Luego de configurar el equipo Firebox, debe instalarse el software correspondiente en cada una de las máquinas remotas que originarán el túnel PPTP. En el caso de usar sistema operativo Windows, debe instalarse el paquete Microsoft VPN Adapter en cada PC remota.

Firewall / Proxy (Nodos Regionales)

En el equipo Firebox de los nodos regionales se activarán las siguientes funciones correspondientes al servicio Firewall / Proxy:

Bloqueo de Sitios y Puertos: Habilitación para detectar y bloquear automáticamente patrones de “syn flood”, smurf, sondas de pruebas para puertos y direcciones abiertos y falsificación de direcciones “IP”, todo esto desde la red Externa hacia la redes DMZ e Interna. Se activará la opción de auditoría (logging) para guardar los orígenes de dichos ataques. El Equipo

Firebox automáticamente bloquea los datagramas que provengan desde la red externa con direcciones no válidas (10, 172 y 192) ya que pueden tratarse de direcciones falsificadas. Se bloqueará manualmente el acceso al puerto 23 de todas las máquinas.

Control de Tráfico Web: Se activará la función WebBlocker, la cual es una característica que trabaja conjuntamente con el proxy HTTP para proveer filtrado sobre sitios Web. El WebBlocker se soporta sobre una base de datos remota de URL´s mantenida por la empresa SurfControl. Esta base de datos contiene más de 65.000 direcciones y 40.000 directorios y es copiada sobre el equipo Firebox a intervalos regulares. El PC utilizado como Procesador de Eventos está configurado para bajar la más reciente versión de la base de datos. Inicialmente, se activará la conexión automática a la base datos de WebBlocker (Auto-download) para el filtrado de los temas específicos sexo, drogas y violencia. Posteriormente, según el comportamiento del tráfico y de los usuarios, podrían aplicarse filtros a programas ejecutables o configuraciones provenientes de los servidores Web, como applets de Java, controles ActiveX, cookies, etc., activándose en determinados horarios (horas operacionales y no operacionales), eliminar en los paquetes http la información de cliente dirigida al servidor o restingir los tipos de contenido como audio, texto y video pueden filtrarse. Todo esto es posible porque son reconocibles los formatos MIME.

Configuración de Servicios

Los nodos regionales originalmente no poseerán servicios propios, por lo cual se bloquearán todos los accesos a servicios como DNS, SMTP, POP3, etc.

DHCP

Se configurará este servicio para la distribución de las direcciones IP 192.168.X.10 hasta 192.168.X.131, dentro de la red 192.168.X.4/25. Las primeras 5 direcciones serán estáticas y se reservarán para el servidor de red interno y otros.

NAT Dinámico Saliente

Se activará este servicio para asignar a cualquier dirección de origen 192.168.X.4/25, a la nueva dirección 200.44.63.Y, que corresponde a la interfaz externa del equipo Firebox. Cada nodo tendrá las siguientes direcciones para la interfaz interna del router y la externa del Equipo Firebox para el NAT:

Nodo Maracay

Router:200.44.63.65 Equipo Firebox: 200.44.63.66

Nodo Valencia

Router:200.44.63.73 Equipo Firebox: 200.44.63.74

Nodo Maracaibo

Router:200.44.63.81 Equipo Firebox: 200.44.63.82

NAT Estático Entrante

No se activará por no existir servicios públicos inicialmente

Acceso a Red Platino mediante la interfaz Frame Relay

Las interfaces externas de los routers de los nodos regionales se configurarán con las siguientes direcciones IP (ver diagrama del nodo):

Nodo Maracay: 192.168.10.2/30
Nodo Valencia: 192.168.11.2/30
Nodo Maracaibo: 192.168.12.2/30

La encapsulación es Frame Relay.

Las interfaces internas serán:

Nodo Maracay: 200.44.63.65/29
Nodo Valencia: 200.44.63.73/29
Nodo Maracaibo: 200.44.63.81/29

La encapsulación es Ethernet

2.7 Fase V: Adecuación de la Red Platino

La adecuación del nodo Red Platino requiere la realización de las tareas que se indican a continuación. La mayor parte se encuentran reflejadas en la figura N° 33. A continuación se explicarán cada una de ellas:

Segmentación del Smart Switch Cabletron 6000

Para comprender la situación de Red Platino, es preciso identificar que esta red es utilizada por INE (de hecho, Platino depende de ese instituto) pero también sirve de plataforma para las instituciones públicas de Caracas, por lo que confluyen los siguientes tipos de tráfico, clasificados por instituciones:

1.- Tráfico entre Red Platino y los nodos regionales
2.- Tráfico entre Red Platino e INE
3.- Trafico entre Red Platino e instituciones (fibra, radio y dedicado)
4.- Tráfico desde las dos oficinas de INE: Censo y Comercio Exterior, ubicadas en Parque Central hacia Red Platino para alcanzar a INE

Para organizar el tráfico y mejorar la seguridad de Red Platino deben crearse tres VLAN's. Cada VLAN estará formada por ocho puertos. En la VLAN Interna se ubicarán las máquinas y servidor de red internos del nodo Platino (Piso 6, Parque Central), con las nuevas direcciones

192.168.245.0/24. A la VLAN Interna también llegan conexiones vía fibra óptica desde oficinas de INE ubicadas en los pisos 19 y 38 de Parque Central con el fin de realizar cargas de datos estadísticos sobre los servidores de INE de la sede principal. En la VLAN DMZ estarán los servicios Web, Correo, FTP y TUTOS (manejador de proyectos basado en Web) manteniendo las direcciones IP actuales 161.l196.215.64/26. En la VLAN Externa confluirán todas las instituciones (ministerios e institutos autónomos) conectadas a través de fibras ópticas, radio enlaces y enlaces dedicados ("clear channel"). Todas ellas tienen direcciones IP 172.20.X.X/16.. En este segmento externo se produce un gran volumen de tráfico "broadcasting" que debe ser limitado mediante elementos de control de tráfico como se describe en "Mejoramiento de la disponibilidad".

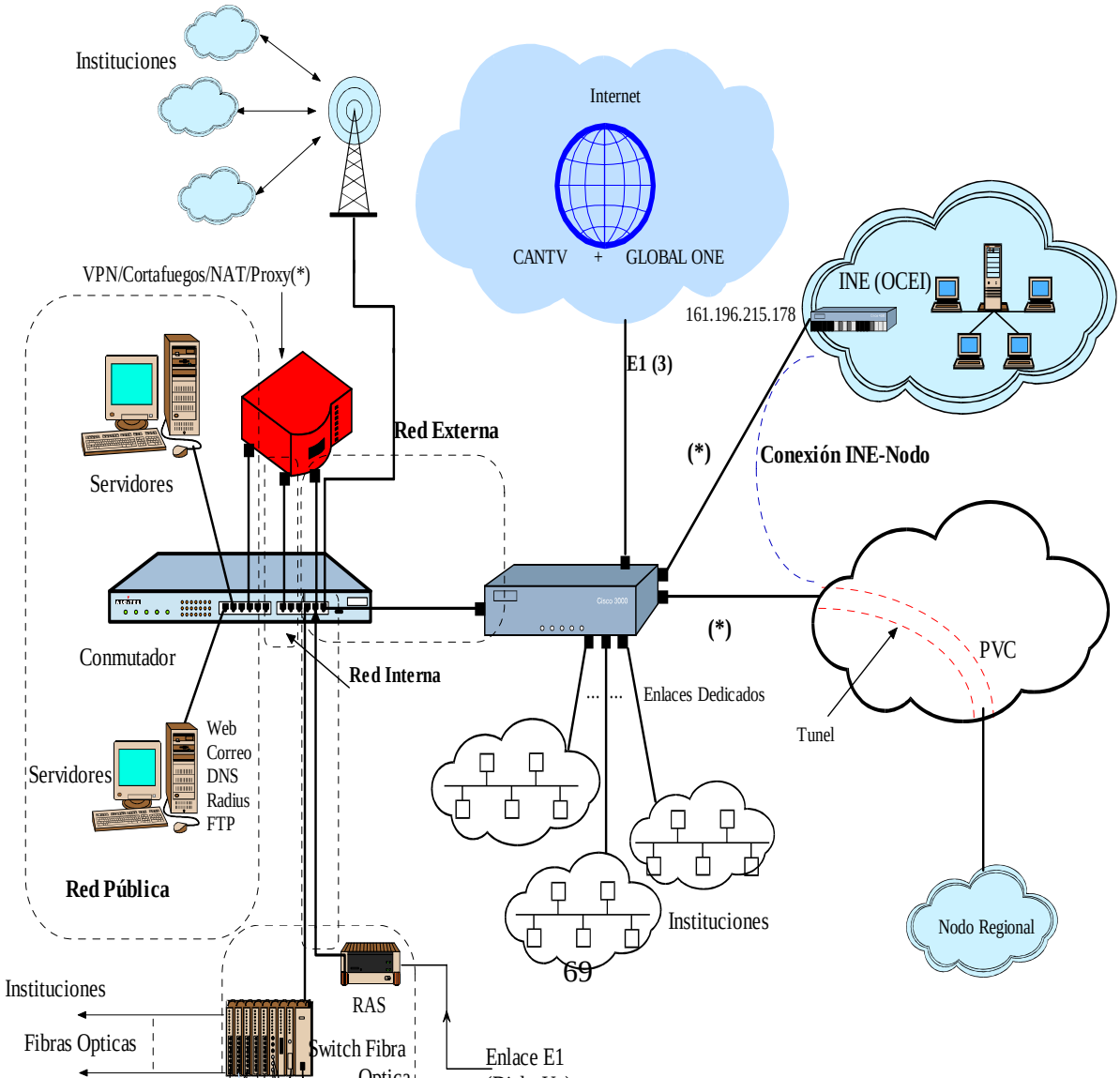


Figura N° 33 Red Platino

En vista del número de redes ya establecidas, el equipo Firebox se configurará en modo “drop-in” con las tres interfaces ubicadas en la red 161.196.215.64/26 y con direcciones IP 161.196.215.94. Las redes 172.20.0.0/16,192.168.0.3/24, 192.168.0.4/24192.168.0.5/24 se añadirán como redes secundarias a las interfaces externa e interna respectivamente. En el modo “drop-in” los servidores con direcciones 161.196.215.65 (web), 161.196.215.67 (Correo), etc. ubicados en la DMZ podrán “ver” directamente la interfaz del router 161.196.215.98 y viceversa mediante el “proxy ARP”, sin necesidad de configurar enrutamiento en el Equipo Firebox.

Cambio de direccionamiento IP a la red interna

Para normalizar y uniformizar el esquema de direccionamiento de las redes internas de Platino, INE y los nodos regionales, se adoptará el bloque 192.168.3.0/24. Esto diferenciará a Red Platino del resto de las instituciones que seguirán utilizando el bloque 172.20.X.X/16, donde el penúltimo número identifica la institución particular.

Configuración del Firewall / Proxy

Bloqueo de Sitios y Puertos: Similar a los nodos regionales

Control de Tráfico Web: Similar a los nodos regionales

Configuración de Servicios: Red Platino posee los servicios públicos en su zona DMZ con direcciones válidas 161.196.215.64/26. El servidor Web (donde se encuentran ubicados la mayoría de los sitios Web de las instituciones públicas) funciona con la técnica de "virtual hosting" por lo que requiere una sola dirección válida (161.196.215.65) para todos los sitios. A esta dirección se le habilitará tráfico entrante solo a los puertos 80 (Web), 443 (Web Seguro), 20 y 21, estos dos últimos para las sesiones de FTP de los clientes que deban cambiar el contenido de su sitio Web. El servicio FTP de este servidor sólo será permitido a direcciones IP de origen específicas. El resto de los puertos de este servidor será bloqueado. El servidor FTP 161.196.215.66, tendrá habilitado los puertos 20 y 21 y el comando "GET" únicamente. El punto más importante, en cuanto a los servicios, es el servidor de correo (161.196.215.67). Para evitar la utilización del servidor de correo como "open-relay" por parte de terceros para llegar al destino (ver capítulo 4) se configura el SMTP proxy para que reciba sólo correos dirigidos a los dominios platino.gov.ve e ine.gov.ve y rechace otros dominios que no sean recipientes locales. En este caso el Equipo Firebox analiza el "header" del mensaje de correo. También se filtrarán contenidos del tipo .bat y .exe para evitar la entrada de virus al servidor. Podrían filtrarse contenidos de imagen, audio, html, etc. Pero esto dependerá de evaluaciones futuras.

Arreglo del túnel VPN

Las oficinas de INE ubicadas en Parque Central, torre oeste, utilizarán la Red Platino para alcanzar la sede principal de INE. Las redes de ambas oficinas llegan mediante fibra óptica a la red Interna del Switch Cabletron ubicado en Red Platino. Ambas redes (192.168.4.0/24 y

192.168.5.0/24) deben utilizar un túnel VPN para alcanzar a INE. La Red Platino sólo manejara este túnel para los datos estadísticos. El resto de las instituciones no usará cifrado/autenticación de datagramas.

El túnel será creado en forma similar al de los nodos regionales, con la siguiente diferencia de configuración:

Local: 192.168.4.0/24 , 192.168.5.0/24
Remote: 200.44.63.4 y 200.44.63.5
Disposition: Secure

Debe asignarse “Bypass” para el resto del tráfico que provenga de estas oficinas y se dirija a Internet o a otras instituciones.

La Red Platino será utilizada como medio de contingencia para que los usuarios de los nodos regionales puedan alcanzar a INE aún cuando fallen sus redes o los enlaces Frame Relay. Para esto se dispondrá de enlaces remotos “tunelizados”

Tres cuentas tipo PPTP para usuarios remotos: Ingresarán a Red Platino a través del RAS (30 canales PCM) con el numero master: 5099711

Tres cuentas IPSec para usuarios remotos: Ingresarán desde otras redes (por ej. ADSL) conectándose a la dirección 161.196.215.94 (interfaz externa del Equipo Firebox)

Conexión de los servidores públicos a la red DMZ y su reconfiguración

Deben conectarse físicamente todos los servidores públicos al segmento DMZ de la red y asignarle su nueva configuración de red. El Galway de los servidores puede no cambiarse, ya que el equipo Firebox está operando en modo “drop-in” y los servidores podrán “ver” al router aunque se encuentre en el segmento externo.

Configuración del router

La interfaz Frame Relay del router debe poseer tres sub-interfaces, cada una de ellas hacia un nodo regional.

Nodo Maracay: 192.168.10.1/30
Nodo Valencia: 192.168.11.1/30
Nodo Maracaibo: 192.168.12.1/30

La encapsulación es Frame Relay. Las interfaces interna será 161.196.215.98 con encapsulación Ethernet.

Utilidad del DHCP

No se usará debido a que es necesario conocer las direcciones IP de cada máquina de la interfaz interna para aplicar filtros de servicios.

Características del NAT Dinámico Saliente

Todas las máquinas de las redes interna y DMZ utilizarán la dirección 161.196.215.94 (interfaz externa de equipo Firebox) como dirección de origen hacia el exterior.

Características del NAT Estático Entrante

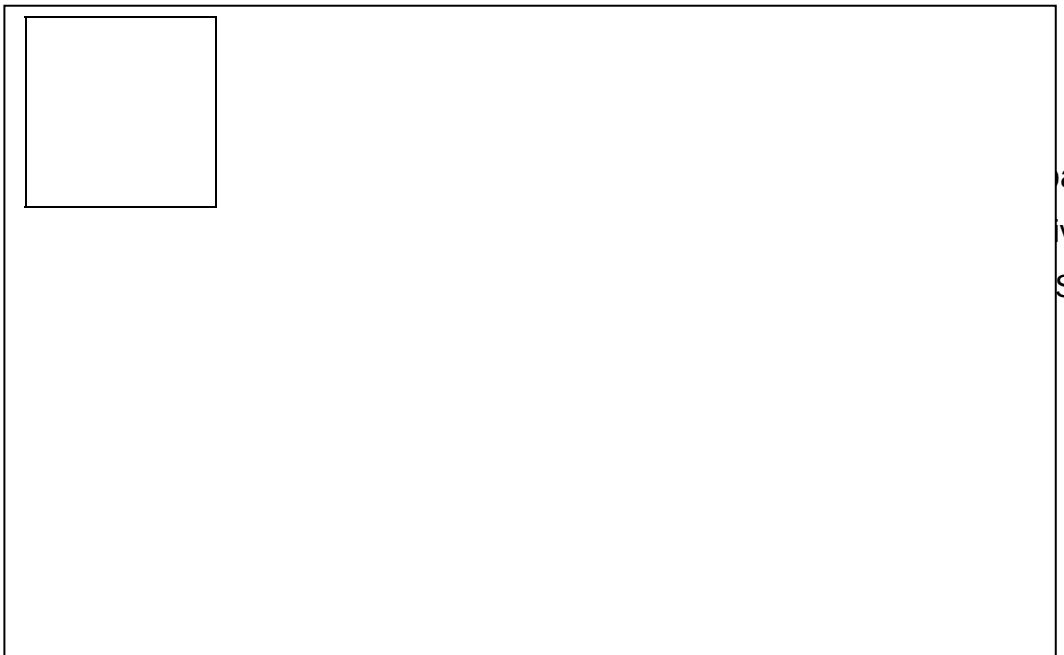
Los servicios poseen direcciones válidas por lo que no es requerido

Optimización del segmento externo del Switch

Este es un punto fundamental. La mayor parte de la Red Platino en el Área Metropolitana de Caracas está conformada por una gran LAN de fibra óptica y enlaces inalámbricos. Independientemente de los enlaces dedicados tipo “clear channel” que comunican instituciones a través de enrutadores, un gran número de instituciones están conectadas directamente a los “switches” de Red Platino mediante fibra óptica (16

instituciones en ambas torres de Parque Central) y a través de enlaces inalámbricos (40 instituciones de Caracas). Estas últimas generan una gran volumen de tráfico tipo “broadcasting” y de tipo indeseado (video, audio, sitios prohibidos, etc.) sobre los switches de Red Platino lo cual afecta el desempeño de las aplicaciones y flujo datos que se intercambian entre los nodos regionales, Red Platino y Red INE. En este sentido, se debe aplicar control de tráfico desde/hacia otras instituciones. Para este fin se impone la incorporación de un tipo de dispositivo entre las LAN´s de las instituciones conectadas vía fibra óptica o radio con la Red Platino. Este dispositivo debe ser colocado físicamente en cada una de las instituciones que acceden a Red Platino y, en lo posible, debe generar poco o ningún gasto económico adicional.

Se recurrió a una solución estable y comprobada de software libre (GNU) sobre plataforma Linux, consistente el las herramientas “IPTABLES” que es un enrutador y filtro de paquetes y el “SQUID”, un proxy cache. Estas soluciones operan sobre un PC convencional (Pentium II o III), equipado con dos interfaces de red, lo cual es fácil de obtener en cualquier institución. Se consideran estos productos muy convenientes por no requerir de mayor inversión por parte de los entes involucrados (y todo el proceso administrativo que ello acarrea) y por estar soportados por la robusta plataforma Linux-Debian.



as
vo
Se

El uso de la herramienta “Calamaris” permite monitorear el comportamiento del caché. Como muestra, se presenta la información sobre los métodos y objetos HTTP más utilizados.

Method	request	%	Byte	%	sec	kB/sec
GET	366220	98.74	1047287K	96.90	0	3.78
POST	3105	0.84	32639146	2.95	2	3.52
PROPFIND	1216	0.33	1390031	0.13	0	2.33
HEAD	314	0.08	143450	0.01	0	1.68
CONNECT	44	0.01	129565	0.01	3	0.92
PROPPATCH	3	0.00	3404	0.00	0	2.22
BMOVE	2	0.00	3592	0.00	0	2.26
MOVE	1	0.00	1395	0.00	1	0.88
NONE	1	0.00	2494	0.00	0	81.18
Sum	370906	100.00	1080796K	100.00	0	3.77

Tabla N° 5 Incoming requests by method

Extensions	request	%	Byte	%	hit-%
Gif	174978	47.18	149453K	13.83	86.32
Jpg	70932	19.12	236701K	21.90	76.05
Js	12223	3.30	9738952	0.88	81.33

Swf	10386	2.80	15455256	1.40	98.21
Html	9295	2.51	25102005	2.27	63.95
Css	3226	0.87	3540266	0.32	63.08
Asp	1998	0.54	6550365	0.59	0.00
Htm	1887	0.51	17948391	1.62	26.44
Zip	1063	0.29	2622741	0.24	5.55
Php	1019	0.27	5594712	0.51	0.00
JPG	1015	0.27	7851331	0.71	26.40
Other: 118 extensions	2799	0.75	197639K	18.29	32.90
Sum	370906	100.00	1080796K	100.00	65.62

Tabla N° 6 Requested extensions

2.8 Fase VI: Adecuación de la Red INE

La recolección de estadísticas y su consulta por parte de los empleados del INE, se lleva a cabo en varios servidores de bases de datos. El acceso se realiza sobre los servidores www.sistine.gov.ve y www.sen.gov.ve, los cuales actúan como portales web. El usuario común tiene acceso a los datos procesados en www.ine.gov.ve.

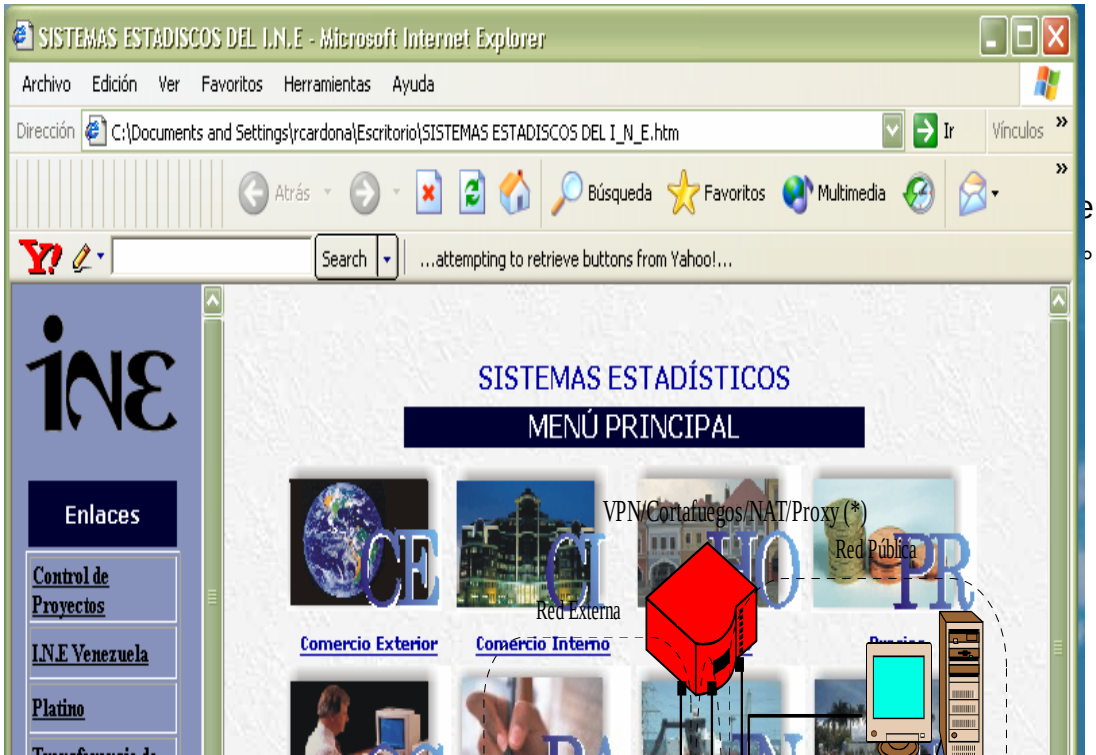


Figura N° 36 Red INE

Arreglo de túneles VPN

Se deben configurar cuatro túneles con las características descritas en la sección “Nodo Regional”. Cada túnel tendrá como dirección de origen (Local) los tres bloques IP de las direcciones de INE:192.168.0.0/24, 192.168.0.1/24 y 192.168.0.0/24. Los destinos serán:

- Remote Gateway:

- 161.196.215.94: (oficinas de INE ubicadas en Parque Central)
- 200.44.63.66/29: nodo Maracay
- 200.44.63.74/29: nodo Valencia
- 200.44.63.82/29: nodo Maracaibo

Los paquetes que utilizarán los túneles sólo serán los provenientes de www.sistine.gov.ve y www.sen.gov.ve. El tráfico desde www.ine.gov.ve (consultas de Web desde el exterior) es de uso común por lo que se le debe aplicar la propiedad “Bypass” al túnel.

Utilidad del DHCP

No se usará debido a que es necesario conocer las direcciones IP de cada máquina de la interfaz interna para aplicar filtros de servicios. Máquinas específicas tendrán restringido el acceso a Internet.

Características del NAT Dinámico Saliente

Todas las máquinas de las redes interna y DMZ utilizarán la dirección 200.44.63.3 (interfaz externa de Equipo Firebox) como dirección de origen hacia el exterior.

Características del NAT Estático Entrante

A diferencia de los nodos anteriores, en este se usará el NAT estático entrante. Los servidores poseen direcciones de los bloques 192.168.X.X, por lo que deben ser accesibles desde el exterior mediante la asignación de direcciones válidas 200.44.63.X.

Configuración del Firewall / Proxy

El arreglo de los Firewall y Proxies, debe respetar las siguientes

reglas:

- Bloqueo de Sitios y Puertos: Similar a los nodos regionales
- Control de Tráfico Web: Similar a los nodos regionales
- Configuración de Servicios: Se bloqueará todo tráfico al puerto 23 y se permitirá tráfico al puerto 80 de www.ine.gov.ve , además de 80 y 443 a los servidores www.sen.gov.ve y www.sistine.gov.ve. Adicionalmente, se permitirá acceso a estos servidores sólo desde las direcciones IP de los nodos regionales y desde red Platino (interfaces externas de los equipos Firebox).

2.9 Fase VII: Sistema de Contingencia

En caso de fallas de conexión del sistema de comunicación Frame Relay, se accederá las bases de datos, desde los nodos regionales, con dos modalidades de acceso remoto “tunelizado” (en terminología WatchGuard: Remote User VPN o RUVPN). Usuario Remoto PPTP: usa protocolo PPTP en conexiones telefónicas o “dial-up”. Soporta hasta 50 conexiones simultáneas con cualquier nivel de cifrado. El acceso se hará al RAS ubicado en red Platino a través del número 5099711 (1 master y 30 esclavos) el cual, a su vez, se encuentra conectado a la interfaz externa del Equipo Firebox (Figura N° 37)

Usuario Móvil VPN: Se aplica a usuarios remotos que poseen acceso a Internet diferente a la línea telefónica, como sistema ADSL u otras redes. El cifrado debe ser medio o alto. Estos usuarios entrarían a Red Platino a través de las conexiones Internet, conectándose con la interfaz externa del equipo Firebox 161.196.215.94.

Ambos tipos de usuarios deben disponer de un software especial en sus estaciones para la creación de los túneles. Es importante destacar que los equipos de comunicación como routers o RAS servers se conectan en el segmento externo de la red. En este caso, cuando un usuario accede en forma remota en el modo PPTP (módem) o IPSec (Internet), el equipo Firebox, mediante un servicio llamado “Any” crea un túnel internamente en el equipo Firebox, desde la interfaz externa hasta la interna. Luego de la autenticación, el usuario se encuentra conectado en forma “lógica” en el lado interno de la red, aunque físicamente se encuentre en el lado externo. De este modo, se comporta como un usuario interno más.

Figura N° 37 Conexión de Usuarios Remotos

2.10 Fase VIII: Supervisión y Monitoreo de la WAN

Independientemente de los sistemas propios que poseen los routers y switches para el monitoreo de enlaces y tráfico, en la WAN de INE serán utilizados intensivamente los siguientes sistemas:

- Sistemas de Auditoría y Monitoreo de los Equipo Firebox (a nivel local)

En cada uno de cinco Equipo Firebox se dispone de las siguientes herramientas, cuyo uso se presenta en el capítulo 3 :

HostWatch: monitorea las conexiones actuales individualmente desde las redes Interna y DMZ hacia la Externa y viceversa
Bandwidth Meter: presenta gráficamente el ancho de banda utilizado por servicio en el tiempo.

Service Watch: cantidad de conexiones por servicio en el tiempo.

Status Report: Provee un conjunto de estadísticas de la actividad del Equipo Firebox, como tiempo de actividad del Equipo Firebox, conteo de paquetes permitidos, negados y rechazados, configuración de redes, conexiones activas TCP, FTP, etc,; bloqueo de sitios y puertos, promedio de carga, procesos activos del Equipo Firebox, tabla ARP, etc.

Generador de Reportes: produce informes de estadísticas por protocolo, conexiones actuales por tipo de servicio.

Auditoría y Notificación: registra toda la actividad a través del Equipo Firebox y puede notificarla a otro computador o a un “pager”.

Se recomienda revisar estas funciones periódicamente.

- Sistema supervisorio SPECTRUM (nivel general)

La incorporación del sistema SPECTRUM no es parte de este proyecto, pero se puede utilizar para obtener una imagen general del comportamiento la red INE. En la figura N° 38 se muestra la ubicación del SPECTRUM con respecto al resto de los elementos.

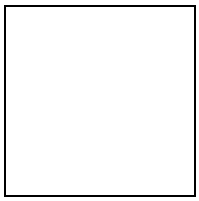


Figura N° 38 Supervisión de la WAN

- Herramientas comerciales y gratuitas de monitoreo y captura de datos

Herramientas como el Snifer, Ethereal, Iris, Net Inspector, Little Brother, Whats Up y otros, se han utilizado desde hace mucho tiempo en las redes Platino e INE y seguirán utilizándose en los nodos regionales. En forma concreta, ellos han permitido detectar:

- Apropiación y utilización indebida de direcciones IP en las instituciones.
- Exceso de tráfico proveniente de máquinas infectadas con virus como el Nimda.
- Intento de ataques a los puertos 23 de los servidores.

Capítulo 3

Ingeniería Básica de Detalle

En este capítulo se abarcará la configuración de software y hardware de los equipos y paquetes más importantes en la realización de la WAN segura, a saber:

- Equipo Firebox
- Servicios IPTABLES y SQUID sobre sistema operativo Linux
- Conmutadores
- Enrutadores
- Servidores
- Estructura Física de la Red
- Diagramas de Piso y Cableado

Conviene aclarar que las configuraciones de equipo s que se presentan contemplan todos los servicios relacionados con este proyecto, sin embargo, a los fines de síntesis, se presentarán ejemplos concretos y no todos los casos posibles con sus valores particulares. Tomando como guía el capítulo anterior, se podrán reproducir todas las situaciones particulares de configuración.

En este capítulo también se estudiará la planta física de los nodos regionales de Maracay, Valencia y Maracaibo, las cuales fueron inspeccionadas para la realización de este proyecto y la implantación de las LAN respectivas.

3.1 Configuración del Equipo Firebox

El equipo equipo Firebox (Fig. N° 39), de la empresa Watchguard, es un dispositivo integral que reúne varias funciones comunes requeridas en la mayoría de las redes. Este equipo realiza funciones de:

- DHCP
- NAT
- Firewall/Proxy
- Autenticación/Control de Acceso
- Red Virtual Privada (VPN)
- Monitoreo/Supervisión

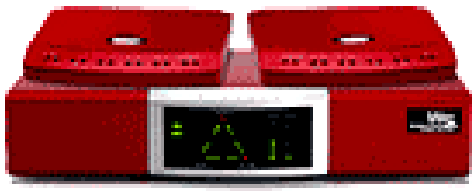


Figura N° 39 Equipo de Seguridad "Equipo Firebox"

Todo esto simplifica enormemente el diseño e implantación de las LANs, al encargarse de realizar la administración de direcciones y la aplicación de seguridad, requiriéndose equipos únicamente para las áreas de conectividad (switches, routers, etc) y de servicios (Web, SMTP, FTP,

etc.). La ubicación del equipo Firebox con respecto a Internet y a la LAN se muestra en la figura N° 40.

El equipo Firebox posee tres interfaces de red y cada una de ellas está conectada a un segmento de la LAN, diferenciándose tres áreas:

Externa: Permite el acceso a los equipos de conectividad, como el enrutador. Es la conexión con el mundo exterior (Internet) que representa típicamente el reto de seguridad.

Interna ("Trusted"): Es el segmento de red protegida desde el exterior.

Opcional (DMZ ó Pública): Es un segmento protegido pero más accesible desde el exterior y desde la zona interna. Típicamente contiene los servidores como Web ó FTP.

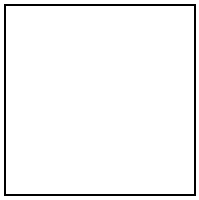


Figura N° 40 El Equipo Firebox y su entorno

En la zona interna se encuentran dos equipos, que también pueden funcionar en un solo PC, que realizan la gestión del equipo Firebox:

Estación de Gestión (Management Station): Es el computador sobre el que se instala y ejecuta el programa de administración del Equipo Firebox ("Watchguard LiveSecurity Control Center")

Procesador de Eventos (Event Processor): Es el computador que recibe y almacena los mensajes de "log" y envía señales de alerta y notificaciones. Como se indicó, un solo computador puede controlar ambas funciones.

En el presente proyecto se utilizará un solo PC para las funciones indicadas.

Para operar el equipo, en primer lugar debe realizarse su configuración de red a fin de que reconozca sus tres interfaces y su entorno

de red. Posteriormente se configurarán los servicios requeridos según las necesidades particulares (Firewall, Proxy, DHCP, etc.). Este orden se aplicará en el presente trabajo. En las siguientes secciones se abordará la programación del equipo en todas sus facetas. En cada una de las secciones, previamente a la descripción de la configuración y uso del equipo se dedicarán algunos párrafos al estudio del servicio en particular de que se trate. Finalmente, se estudiará el equipo en diversos entornos prácticos para reconocer su versatilidad y aplicabilidad al proyecto.

Configuración de Red

El Equipo Firebox posee tres interfaces tipo Ethernet: Trusted, Optional y External. Comúnmente, en los sistemas tipo Firewall, éstas se asocian o se conectan a segmentos de red con los nombres de: Interna, DMZ (ó Pública) y Externa.

En la red interna se conectan las estaciones y servidores que deban estar más protegidos (red privada, servidores de red, bases de datos, datos confidenciales, etc.). En la red pública se ubican servidores que requieren ser accesibles desde el exterior, para el público en general o Internet, como es el caso de los servicios de Web, Correo, etc. En la red externa se conectan equipo s de comunicación como enrutadores, RAS, o similares, e inclusive, otras redes sin requerimientos mayores de protección por parte del Equipo Firebox. A nivel de red, el Equipo Firebox puede operar en dos modos: Enrutado (routed) y Enmascarado (“drop-in”).

Independientemente del modo de operación, deben establecerse la puerta de enlace (“default gateway”) y el servidor de DNS o WINS.

Modo Enrutado

En este modo, cada interfaz del equipo Firebox debe pertenecer a

una red diferente (Fig. Nº 41). Esta configuración debe asignar redes separadas a, por lo menos, dos de las tres interfaz, generalmente la interna y la externa. En redes complejas se crean tres redes, cada una asociada a una interfaz. En el ejemplo se aprecian las redes 192.168.245.0/24, 161.196.215.64/27 y 161.196.215.96/27 asociadas a las tres interfaz con direcciones 192.168.245.1, 161.196.215.65 y 161.196.215.97, respectivamente. Estas últimas actuarán como “gateway” para las estaciones en las redes interna y opcional y para el “router” en la red externa. El “switch” segmentado en tres porciones proporciona LANs virtuales (VLAN) requeridas para el correcto funcionamiento del equipo Firebox. De esta forma, el tráfico no puede pasar de un segmento a otro del “switch” a menos que lo haga a través de equipo Firebox para que se le apliquen la políticas de seguridad.

La interfaz externa debe pertenecer a una red con direcciones IP válidas, ya que el equipo Firebox supone que este punto está conectado a Internet. La red interna posee direcciones no válidas como protección para ingresos desde la zona externa, mientras que la red DMZ posee direcciones válidas para ser accesible públicamente.

Una vez definidas las interfaces, pueden añadírsele redes secundarias a cada una de ellas para extender su entorno. Estas nuevas redes también estarán protegidas por las reglas establecidas para la interfaz en particular.

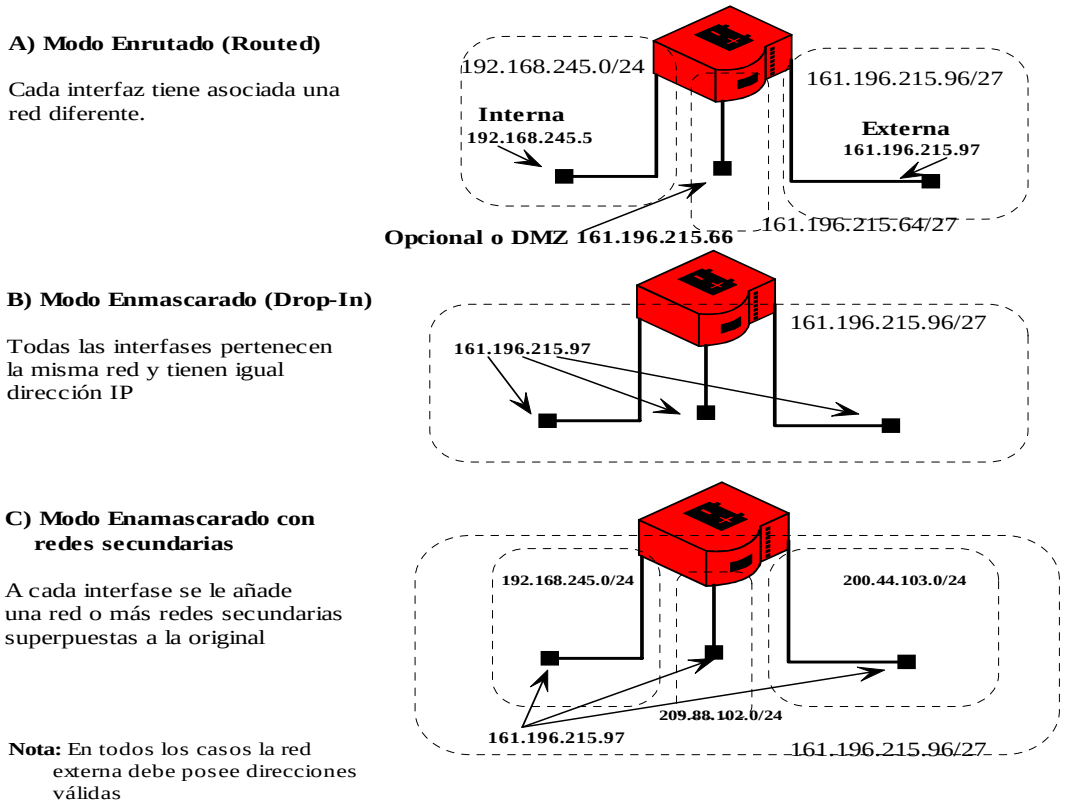


Figura N° 41 Modos de Operación del Equipo Firebox

Para que alguna máquina o recurso en particular ubicado en la red interna (generalmente con direcciones no válidas) pueda ser accedido desde la externa (direcciones válidas), puede establecerse un NAT estático, tal como se verá en la sección correspondiente.

- **Modo Enmascarado**

En el modo enmascarado ó “drop-in” las tres interfaces del equipo Firebox tienen la misma dirección IP y pertenecen a la misma red (Fig. Nº 42). Este modo es útil en el caso que se encuentren redes y direccionamientos ya establecidos al momento de la incorporación del equipo Firebox. En este modo, así como en el enrutado, pueden añadirse redes secundarias, tal como se aprecia en la misma figura.

Para la configuración de la red en este modo, deben separarse los diferentes elementos que componen la red de acuerdo al nivel de protección requerido (estaciones de trabajo, servidores públicos, equipo s de comunicación). El “switch” proporciona la segmentación ó división requerida mediante los “dominios de broadcasting” o VLAN, como también se les denomina. No es necesario modificar el direccionamiento IP de máquinas ni de su puerta de enlace. Al equipo Firebox se le asigna una dirección IP no utilizada.

En este modo, la comunicación entre máquinas o dispositivos ubicados en diferentes zonas del “switch” se logra mediante una técnica denominada “proxy-ARP”: el equipo Firebox reenvía las consultas de ARP, realizadas por una máquina, al resto de sus interfaces cuando esta máquina no obtiene una respuesta en el segmento en el cuál está conectada. El equipo Firebox actúa como un intermediario entre la máquina y la respuesta al mensaje ARP que requiere para establecer una comunicación. Por supuesto, también deben verificarse las permisologías correspondientes para lograr finalmente el acceso al recurso deseado.

Las principales características de este modo, son:

- La red no se subdivide en pequeñas subredes (“subnetting”). Todas las interfaces de red del equipo Firebox tienen la misma dirección.

El equipo Firebox se comporta como si estuviese “sumergido” dentro de una misma red IP.

- El equipo Firebox realiza el proxy-ARP: responde las solicitudes de las máquinas que no pueden oir directamente las respuestas a sus mensajes de difusión.
- El equipo Firebox se coloca en la red sin cambiar la configuración de puerta de enlace (default gateway) de las máquina en la zona interna: si el “default garteway” era un enrutador, el equipo Firebox responde en lugar del enrutador auque éste no pueda oir las solicitudes de ARP de la zona interna, simplemente porque el equipo Firebox las repite (“proxy” significa “intermediario”).
- Las máquinas ubicadas en la zona interna deben tener borradas sus tablas de ARP.
- Desde el punto de vista del “router”, las direcciones MAC de las máquinas de la red interna son reemplazadas por la interfaz “trusted”.
- Se pueden añadir redes secundarias detrás del equipo Firebox. Estas redes IP están solapadas sobre la red primaria y se definen dentro de la configuración de las interfaces

Suponiendo que, antes de instalarse el equipo Firebox, existiese una red 161.196.215.0/24 conectada al “switch” y que las estaciones tuviesen como gateway al enrutador 161.196.215.1, por ejemplo, no existe necesidad de modificar esta configuración de las estaciones al incorporar al Equipo Firebox en modo enmascarado. Se agrupan las estaciones, servidores y equipos en cada uno de los tres segmentos del switch, según su función e independientemente de su dirección lógica. El equipo Firebox, a través de la técnica “proxy-arp” se encargará de obtener la dirección MAC de destino y conectará a los equipos pertenecientes a segmentos diferentes. Cabe destacar que, en este modo, es necesario informar al equipo Firebox sobre

cuales equipos se encuentran en cada una de las tres interfaces.

A la red primaria anterior (161.196.215.0/24) pueden añadírsele redes secundarias. Cada una de estas debe asociarse a una interfaz y, por supuesto, a la interfaz de la nueva red, debe agregársele una nueva dirección. En el caso anterior, si debe incorporarse una red 192.168.245.0/24 en la red interna, se debe añadir, por ejemplo, la dirección 192.168.245.1 a la interfaz interna, la cuál será el gateway de las máquinas en esa red.

Cada interfaz puede tener una o más redes secundarias.

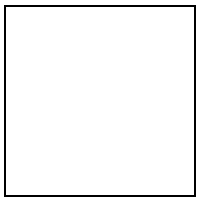
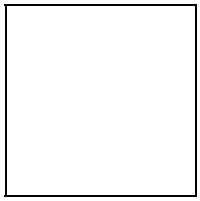
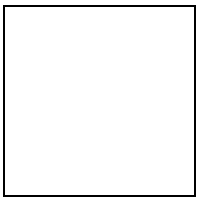


Figura N° 42 Modo Enmascarado (“drop-in”)

Para realizar la configuración de red, se debe entrar en la opción Policy Manager/Network/Configuration. Posteriormente se configuran las interfaces (Figura N° 43). Si se le asigna la misma dirección a las tres interfaces se activa automáticamente el modo “drop in”. Si se le asignan direcciones IP de redes diferentes trabajará en modo enrutado. Nótese la caja de texto en la que se pueden añadir redes secundarias en cualquiera de los dos modos.



Si se opera en modo “drop in” se deben indicar las estaciones ubicadas en cada interfaz (figura N° 44).



- **Otros Parámetros**

Como se indicó, además de configurar el modo de operación del equipo Firebox, en esta fase también se debe determinar el resto de las características de red :

- Puerta de Enlace: Generalmente es el enrutador ubicado en la red externa.
- Servidores DNS ó WINS: Se le debe indicar la dirección del servidor para la resolución de nombres.
- Servicio DHCP: El equipo Firebox puede ser un servidor DHCP para la red interna, asignando automáticamente los parámetros IP a un conjunto de máquinas. En este caso se establece el grupo (“pool”) de direcciones a repartir cuando las máquinas las soliciten. Este servicio se describirá en la próxima sección.

Configuración del Servicio DHCP en el Equipo Firebox

El equipo Firebox, actuando como servidor DHCP, asigna las direcciones IP de un “poll” a los solicitantes. También suministra los valores IP de “gateway” y DNS . El administrador debe definir el “lease time” o tiempo de arrendamiento. Este es el tiempo que el servidor DHCP “prestará” la dirección al cliente. Cuando se encuentre cerca el momento de expiración de la dirección, el cliente deberá solicitar una renovación del “lease”. Los “hosts” de la red interna realizan sus solicitudes iniciales o de renovación al equipo Firebox, quien le

suministrará los parámetros requeridos. Por ejemplo, si el equipo Firebox se encuentra configurado en modo enrutado, el servidor DHCP asignará el siguiente bloque de configuración a cada estación solicitante:

Dirección IP: 192.168.245. 50 hasta 192.168.245.100
Máscara: 255.255.255.0
Gateway: 192.168.245.1 (Interfaz interna)
DNS: 161.196.215.70 (Servidor DNS asignado al Equipo Firebox)

En caso de que se encuentre en modo enmascarado con una sola red primaria, la asignación que haría será:

Dirección IP: 161.196.215.80 hasta 161.196.215.100
Máscara: 255.255.255.0
Gateway: 161.196.215.1 (Enrutador, gateway del Equipo Firebox)
DNS: 161.196.215.70 (Servidor DNS asignado al Equipo Firebox)

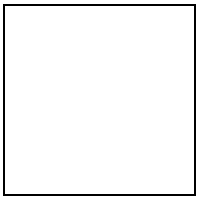


Figura N° 45 Servicio DHCP

Para configurar este servicio, debe seleccionarse Network/Configuration/DHCP Server

Configuración del Servicio NAT en el Equipo Firebox

En el equipo Equipo Firebox, el servicio NAT se aplica del siguiente modo:

NAT dinámico saliente:

También conocido como enmascaramiento o traducción “puerto-dirección”, el NAT dinámico esconde las direcciones de los “hosts” internos, de otros “hosts”. Los equipos en el exterior perciben como si todos los

paquetes provienen del Equipo Firebox mismo. Esta característica protege la confidencialidad y la arquitectura de la red. También permite conservar las escasas direcciones IPv4 válidas. El equipo Firebox permite implementar dos formas de NAT dinámico saliente.

NAT simple:

Las direcciones IP de las redes interna y/o opcional se asignan a una sola dirección IP de origen en el tráfico saliente. Para realizar la asignación de *varias a una,* se utilizan los puertos (PAT). De esta forma se diferencian entre sí las direcciones IP no válidas que originan el tráfico hacia el exterior. Normalmente la dirección contra la cual se hace el NAT es la de la interfaz externa. De este modo se logra "enmascarar" la red interna.

Por ejemplo, si la red interna posee direcciones del bloque 192.168.245.0/24 y la interfaz externa es 161.196.215.97, entonces todos los paquetes en las conexiones desde la red interna hacia la exterior tendrán como dirección de origen 161.196.215.97 y puertos superiores al 1023, es decir, se enmascara el origen real 192.168.245.X. Es importante señalar esto: una dirección de origen del tipo 192.168.245.X puede corresponder a *varios* puertos en la dirección 161.196.215.97, dependiendo de la cantidad de paquetes que se envían o reciben; se hace esta aclaratoria porque en ocasiones se llega a suponer que corresponde a *un solo* puerto, lo cual es falso. En este sentido las dirección 192.168.245.8 puede corresponder a las siguientes asignaciones: 161.196.215.97:2541, 161.196.215.97:2601, 161.196.215.97:3115 y 161.196.215.97:1700. Como se sabe, en el caso de una "sesión" http, en realidad el cliente realiza varias sesiones con el servidor para "bajar" todos los elementos de una página, lo que involucra varios paquetes correspondientes a las asignaciones indicadas. Al compartir una dirección válida con un grupo de usuarios,

asignándole a estos direcciones no válidas, se logra un mejor aprovechamiento de las escasas direcciones válidas y disminuye la carga de los enrutadores, usados como NAT, ya que estos procesarán un menor número de direcciones (las entregadas por el equipo Firebox) y no las direcciones individuales de cada usuario.

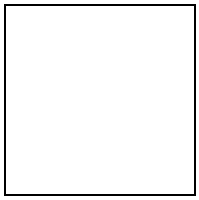
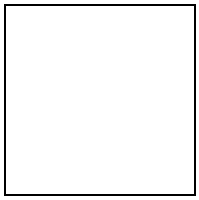


Figura N° 46 Tipos de NAT en el Equipo Firebox

Para configurar en NAT Simple debe seleccionarse en Policy Manager: Setup/NAT.

En este punto se habilita “Enable Dynamic NAT” y luego se añade:
From: Trusted
To: External

Por supuesto, también es aplicable desde Opcional a Externa.



NAT basado en servicio:

Usando esta técnica, se puede establecer un NAT saliente dinámico basado en una política “servicio-por-servicio”. El NAT basado en servicio es usado más frecuentemente para hacer excepciones a un NAT simple y global.

Por ejemplo, se usa el NAT basado en servicios en una red con NAT simple habilitado desde la red Interna a la Opcional, con un servidor Web en

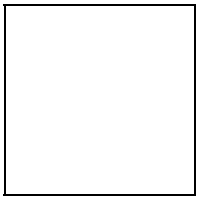
la red opcional al cual no se le deba enmascarar la dirección de la red interna. En este caso se añade un icono de servicio permitiendo el acceso Web desde la red interna hacia la red opcional y se deshabilita el NAT simple. En esta configuración, todos los accesos Web desde la red interna se realizan con la dirección IP verdadera (no enmascarada) y todo el resto del tráfico de la interna a la opcional es enmascarado. Esta opción es de poco uso, por lo que no se tratará en mayor detalle.

NAT estático entrante

El NAT estático opera sobre la base de "puerto-a-host". Los paquetes entrantes destinados para una dirección externa específica y un puerto particular, en la interfaz externa, son "re-mapeados" a una nueva dirección y a un nuevo puerto detrás del equipo Firebox (redes Interna y Opcional). Para en NAT estático, cada servicio debe configurarse separadamente.
Por ejemplo, si tenemos configurada una red opcional con direcciones no válidas (10.0.0.0/24) y deseamos hacer público el servidor http que se encuentra en esa red, digamos 10.0.0.2, se deberá asignar un NAT estático de la interfaz externa 161.196.215.94:80 a la dirección 10.0.0.2:80. Nótese el uso de los puertos que en este caso es el mismo para ambas direcciones pero no siempre es así. El cliente que solicite la página Web hará una conexión desde el exterior a la dirección 161.196.215.94:80 y el equipo Firebox se encargará de la conversión. Si luego se desea incorporar un servidor de correo (SMTP) con dirección 10.0.0.3, el equipo Firebox deberá asignar ("mapear") la dirección 161.196.215.94:25 a la 10.0.0.3:25 que corresponde al servicio. Nótese lo siguiente: los servidores están instalados en máquinas diferentes, sin embargo desde el exterior son "vistos" con una sola dirección, y para hacer la conversión el equipo Firebox requiere del valor del puerto. En esto consiste el mapeo "puerto-a-host".Este servicio es sólo para el uso en las conexiones desde el exterior. Para accesos internos

entre las redes interna y opcional o dentro de una de ellas, debe usarse la dirección no válida para llegar al servicio.Para usar este servicio, primero se debe asignar una dirección externa. Para esto se selecciona Network/Configuration/External/Aliases. Se añade una o varias direcciones válidas. Finalmente se aplica “Ok”. Es importante destacar que puede emplearse como dirección externa la misma que la interfaz externa. Por supuesto, las nuevas direcciones deben pertenecer a la red externa.

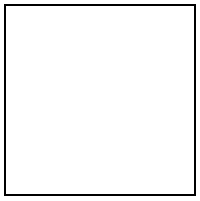
En segundo lugar, debe establecerse el servicio (HTTP, SMTP, FTP, etc.) al que se le asignará la dirección del punto anterior. Como se indicó, el servicio reside en un host con dirección no válida. Para esto se debe seleccionar el servicio correspondiente y luego:
Propierties/Incoming/Enabled and Allowed (El NAT se establece en tráfico entrante). Luego se escoge: NAT/External IP Ardes. Si se desea “mapear” el puerto externo a otro puerto interno (diferentes, por supuesto) se aplicará en este punto “Set Internal Port To Different Port Than Service” , pero esta opción raramente se usa.



Se recomienda asignar a los servidores ubicados en las interfaz Interna y DMZ direcciones privadas. El equipo Firebox se encargará, mediante una tabla definida internamente, de asignar esas direcciones privadas a direcciones públicas a fin de que los servicios puedan ser accedidos desde el exterior (si se requiere). Esto protege los programas y servicios instalados en estos servidores.

Finalmente se muestra un ejemplo de la configuración de NAT´s estáticos configurados en el INE (Instituto Nacional de Estadística). En el

INE existen varios servidores de aplicación basados en plataforma Web. Para ser accedidos desde el exterior los servidores 172.197.45.X (direcciones no autorizadas), requieren direcciones del tipo 200.44.63.X.



Configuración de Firewall / Proxy

En el Equipo Firebox se pueden realizar las siguientes tareas:

- Bloqueo de Sitios y Puertos
- Control del Tráfico Web
- Configuración de Servicios
- Proxy SMTP, FTP y http

Bloqueo de Sitios y Puertos

Muchos tipos de ataques a la seguridad de las redes son descubiertos fácilmente por el patrón encontrado en el encabezado de los paquetes. Ataques como prueba de puertos abiertos, pruebas de direcciones disponibles y falsificación ó “spoofing”, syn flood, smurf, exhiben características que un firewall debe reconocer.

El equipo Firebox permite el bloqueo de puertos y sitios manual y dinámico, y usa las opciones de “default packet-handling” para bloquear temporal y automáticamente a los hosts que originan sondas y ataques. Las opciones de auditoria o “logging” pueden servir para identificar sitios

sospechosos que tienen comportamiento fuera de lo común. Entonces se procede al bloqueo manual o automático. Adicionalmente, se pueden bloquear puertos con vulnerabilidades conocidas desactivando su uso no autorizado.

Manejo de paquetes por defecto

El equipo Firebox examina el origen de los paquetes, su dirección y puerto de destino. También revisa patrones en paquetes sucesivos que indican intentos no autorizados en la red. El equipo Firebox puede reconocer y bloquear ataques de “IP spoofing”, “syn flood” y sondas de prueba para puertos y direcciones. También se pueden registrar en archivos “.log” los mismos.

Bloqueo permanente de sitios

Cualquier dirección del tipo 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16 es bloqueada por defecto ya que no deberían ingresar desde la red externa paquetes con estas direcciones como origen o destino. Pueden tratarse de direcciones falsificadas (“spoofed”) o sospechosas. Además pueden bloquearse otras direcciones, redes, nombres de hosts y nombres de usuarios (“username”).

Bloqueo permanente de puertos

Se pueden bloquear puertos para cortar el acceso a ciertos servicios de red que son puntos de entrada vulnerables en una LAN. Esta característica tiene prioridad entre todas las propiedades de un servicio. El bloqueo de puertos es útil en varias situaciones.

Constituye una verificación independiente para proteger la mayoría de los servicios sensibles. Si una parte de las políticas de seguridad no ha sido bien configurada, el bloqueo de puertos provee una defensa adicional para la mayoría de los servicios vulnerables. Las sondas de prueba hacia servicios particularmente sensibles pueden ser auditadas ("logged") independientemente.

Algunos puertos TCP/IP superiores a 1024 son vulnerables a ser atacados si el intruso genera una conexión de desde un servicio "bien-conocido" inferior a 1024, ya que puede ser interpretada como la conexión en sentido contrario o la respuesta de un servidor.

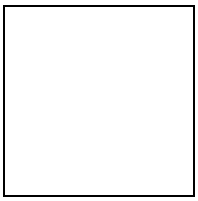
El bloqueo de puertos se realiza en la opción Setup/Blocked Ports/Add, como se muestra a continuación.

Control del Tráfico Web

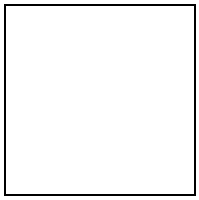
El WebBlocker es una característica que trabaja conjuntamente con el proxy http para proveer filtrado sobre sitios Web. Se aplica al tráfico saliente desde la red interna. El WebBlocker se soporta sobre una base de datos remota de URL ´s mantenida por la empresa SurfControl. Esta base de datos contiene más de 65.000 direcciones y 40.000 directorios y es copiada sobre el equipo Firebox a intervalos regulares. El PC utilizado como Procesador de Eventos está configurado para bajar la más reciente versión de la base de datos.

El equipo Firebox puede filtrar programas ejecutables o configuraciones provenientes de los servidores Web, como: applets de Java, controles

Activex, cookies, etc. También se puede eliminar en los paquetes http la información de cliente dirigida al servidor.



Los tipos de contenido como audio, texto y video pueden filtrarse (figura N° 50). Es conveniente activar la conexión automática a la base datos del WebBlocker (Auto-Download).Se le puede activar en determinados horarios (horas operacionales y no operacionales).



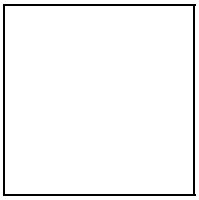
También se dispone de filtrado por temas específicos (sexo, drogas, violencia, etc.)

Configuración de servicios Proxies

Mediante esta función se puede filtrar el tráfico saliente y entrante en cada uno de los servicios. Se encuentran disponibles todos los servicios comunes como: telnet, DNS, SMTP, SNMP, http, POP3, IMAP, etc. El usuario también puede crear nuevos servicios o modificar uno existente (por ejemplo, cambiar el puerto de escucha). El Equipo Firebox, por defecto, bloquea todo tipo de tráfico a menos que, explícitamente se permita.

En la pantalla “Arena de Servicios” del Policy Manager (figura N° 52), se puede apreciar un icono para cada servicio configurado. Un servicio representa un tipo particular de conexión a la cual se le aplicará un “filtro de

paquetes” o un “proxy”. Los proxies realizan una revisión a nivel de las capas altas. En este sentido pueden apreciar iconos como: FTP, SMTP, proxied http, SMTP proxy, etc.

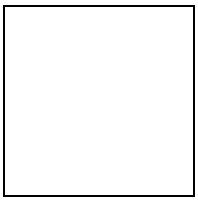


Es importante destacar que el equipo Firebox aplica las normas de seguridad “por servicio”, a diferencia de otros tipos de Firewall donde primero se establecen las direcciones de origen y destino del tráfico para luego configurar los servicios permitidos o negados. Los símbolos (flechas) cercanos al icono indica si el servicio esta configurado para el tráfico saliente, entrante o ambos. La ausencia de símbolos indica servicio inactivo. Los círculos rojo y verde indican tráfico bloqueado y permitido. Se incluyen varios servicios “bien-conocidos”, sin embargo pueden agregarse nuevos servicios creados por los usuarios.

A manera de ilustración, se muestra la configuración para permitir el tráfico FTP entrante desde cualquier sitio o red en el exterior (Any) hacia los servidores 161.196.215.65 y 161.196.215.94 únicamente. También se detectarán y registrarán (logging) los accesos negados que se realicen a otros servidores con direcciones diferentes. La notificación, como se verá luego, puede realizarse con varios métodos, como: correo, “pager”, etc.

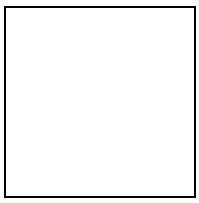
En la siguiente figura se observa como se permite el acceso mediante http desde (Incoming) cualquier sitio externo a un grupo de servidores web

172.197.45.X, posteriormente a la realización de un NAT estático (200.44.63.X).



También puede permitirse que un conjunto de máquinas naveguen, es decir, utilicen el protocolo http en sentido saliente (outgoing). En el caso que sigue, las máquinas indicadas pueden conectarse al exterior mediante http. Para el Equipo Firebox, como se indicó, cualquier usuario no especificado en esta lista, será bloqueado.

Un servicio muy importante es el SMB (Server Message Block), núcleo del NetBIOS. Activando este servicio se permite que fluya el protocolo NetBIOS a través del equipo Firebox, para las redes Windows. Es útil en el caso que se desee compartir en ambiente Windows un recurso (por ejemplo, una impresora) que se encuentre en una red o interfaz diferente. El servicio SMB activa los puertos 137 (UDP), 138 (UDP) y 139 (TCP) a través de los cuales se comunica NetBIOS.



El equipo Firebox suministra la función proxy para varios servicios como: SMTP, http, H.323, FTP, DNS, etc. El proxy permite una mayor granularidad en el filtrado. Se estudiará en detalle el SMTP proxy y luego se referirán las características más importantes de otros proxies.

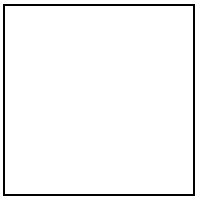
Proxy SMTP

El proxy SMTP limita algunos aspectos peligrosos del servicio de correo. El proxy revisa el tipo de contenido y los encabezados (“headers”) de los mensajes de correo y los compara contra una lista de patrones de información peligrosos, definidos por el usuario. Los correos con anexos sospechosos son bloqueados y se envían mensajes informando sobre esta situación. La lista de patrones deshabilitados puede ser modificada en Content Types dentro de la caja de diálogo SMTP Proxy. El proxy también deshabilita comandos no estandarizados en los mensajes de correo como Debug, y puede limitar el tamaño de los mensajes y de los recipientes. Si los mensajes exceden estos límites, el equipo Frebox los rechazará.

El Policy Manager usa cajas de diálogos separadas para las reglas de entrada y de salida. Debido a que los mensajes de entrada representan un mayor riesgo para la red, el SMTP entrante posee más controles y propiedades configurables.

Para configurar el Proxy SMTP para correo entrante se selecciona SMTP Proxy/Propierties/Incoming. Aparecen las características generales de: máximo tamaño del mensaje, número de correos recibidos, caracteres permitidos en el mensaje y tiempo máximo de espera de mensajes SMTP.

Para seleccionar los tipos de contenido permitidos se escoje “Content Types” dentro del cuadro anterior (figura N° 55):



El protocolo MIME especifica los tipos de contenido como: texto, imagen, audio, etc. Además, se pueden especificar tipos de archivo como: .bat, .exe, .html, etc. Se puede bloquear o permitir el correo desde/hacia orígenes y destino particulares. Por ejemplo, se puede impedir que al dominio platino.gov.ve lleguen correos desde el domino yahoo.com y otros.

En “Address Patterns” se establecen estos filtros. La característica anterior puede ser utilizada para evitar el “open relay”. El “open relay” o correo masivo consiste en el uso, por parte de hackers o empresas inescrupulosas, de servidores de correo de terceros para el envío de información masiva como propaganda, mensajes anónimos, etc. En este caso, el servidor de correo de la empresa en lugar de enviar su correo directamente (utilizando sus recursos de memoria, CPU, etc.), utiliza un servidor de correo de un tercero el cual hace las veces de “relay”.

A este servidor (“victima”) se le envía un grupo grande de mensajes para que este se encargue de retransmitirlos a sus destinos finales, gastando recursos propios. Se observa en este caso que los correos recibidos por el servidor “relay” tienen dominios de origen y destino diferentes al suyo. Para evitar esto, el equipo Firebox que protege al servidor de correo ubicado en la interfaz opcional, sólo recibirá correos cuyo destino sea el dominio en el que se encuentre el servidor. El servidor de correo de un tercer dominio (platino.gov.ve) se puede usar para llegar desde abusadores.com a destino.com.

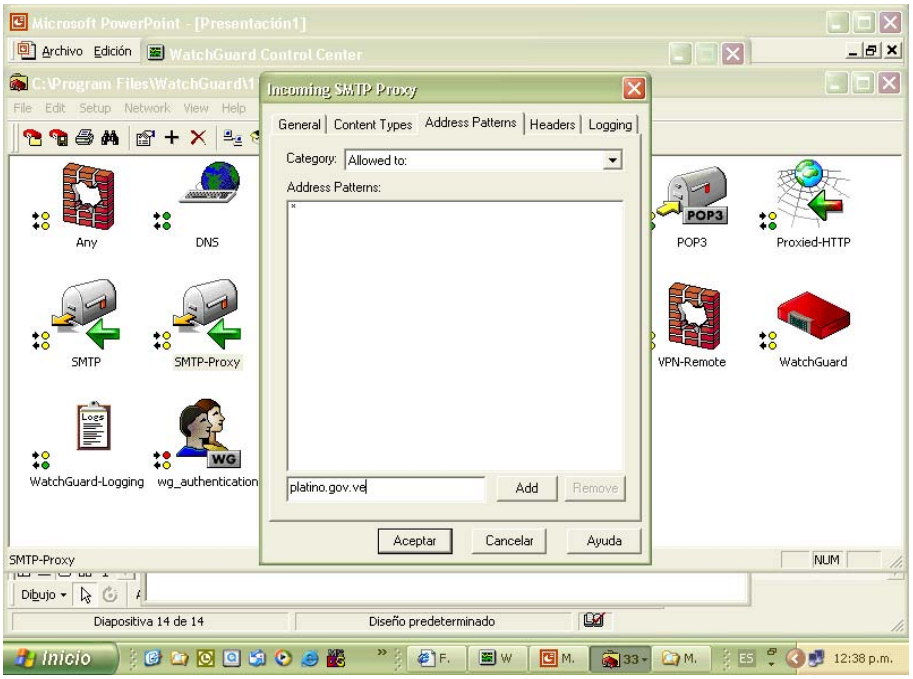


Figura N° 56 SMTP Proxy: Evitando el “Open Relay”

Eventualmente, el servidor de correo de platino.gov.ve será detectado como generador de “relay”. Organismos internacionales como mail-abuse.org se dedican a detectar estas anormalidades e ingresan a los servidores de origen y de “relay” en una lista negra (“blackhole”) que les impedirá enviar y recibir correo hasta que se solvente la irregularidad. Estas instituciones ofrecen software gratuito (“parches”) para añadirlos a los servidores para que eviten este tipo de uso. Sitios como www.samspade.org o www.trucsontechnologies.com permiten hacer pruebas sobre nuestro servidor o verificar si está en la lista negra.

Para evitar el mail relay se debe instalar un software en el servidor de correo. Sin embargo, el equipo Firebox también defiende contra este tipo de ataques. Para realizar esto, debe colocarse el dominio que recibirá el correo, por ej., platino.gov.ve, dentro de la lista “Allowed To” dentro de “Address Patterns” (figura N° 56)

El filtrado que ejecuta el SMTP Proxy puede llegar al punto de discriminar información dentro del “header” de correo, como los campos: “subject”, “from”, “to”, “cc”, etc.

Proxy FTP

Con este servicio puede filtrarse a nivel de capa 7 el tráfico FTP, pudiendo discriminarse sitios de origen y destino permitidos o bloqueados, comandos ftp permitidos o bloqueados como: get, put, dir, etc. Es de gran utilidad si se posee un servidor de FTP para sólo lectura y se debe evitar que se escriban archivos en él, acción que se ejecuta generalmente con el comando “put”.

Proxy HTTP

Este servicio realiza un filtrado basado en contenido en las conexiones salientes. Este filtrado puede incluir el bloqueo o remoción de contenido “inseguro” como applets de Java o controles ActiveX, así como realizar verificaciones generales en el intercambio HTTP.

Proxy DNS

Protege contra el procesamiento de registros “nxt”, contra el “tsig” y otros ataques de DNS como “zone transfer requests”.

Proxy H.323

Este protocolo se utiliza en aplicaciones de videoconferencia como NetMeeting e Internet Phone. Monitorea el puerto 1720 y los comandos enviados y recibidos durante la videoconferencia.

Configuración del Servicio de Autenticación en el Equipo Firebox

Los alias son abreviaciones utilizadas para identificar grupos de hosts, redes o usuarios con un nombre. El uso del alias simplifica la autenticación del usuario y la configuración del servicio.

La autenticación de usuario provee el control de acceso para las conexiones salientes. La autenticación “mapea” dinámicamente un “username” a una dirección IP de una estación de trabajo, permitiendo el seguimiento de las conexiones de los usuarios basándose en el nombre antes que la estática dirección IP.

Los alias de los hosts permiten recordar fácilmente las direcciones IP de los hosts, gamas de hosts, grupos, nombres de usuarios y direcciones de red. Ellos funcionan en forma similar a las listas de distribución de correo electrónico, combinando direcciones y nombres en grupos fácilmente reconocibles. Con el uso del alias se puede configurar la autenticación y la aplicación de reglas para el filtrado de servicios (control de acceso). Si embargo, con ellos no puede configurarse la red propiamente dicha.

El Equipo Firebox automáticamente tiene cuatro alias de hosts:

- equipo Firebox: identifica las direcciones pertenecientes a las tres interfaces
- trusted: identifica las direcciones pertenecientes a la interfaz interna
- optional: identifica las direcciones pertenecientes a la interfaz opcional (pública)
- external: identifica las direcciones pertenecientes a la interfaz externa

Como se aprecia en la figura N° 57 al alias “prueba” se le puede asignar cualquiera o una mezcla de los siguientes elementos:

- Direcciones IP
- Direcciones de Red
- Rango de Hosts
- Nombres de Hosts
- Nombres de Grupos
- Otros Alias

En la opción SetUp/Authentication/Aliases se aplican estas opciones.

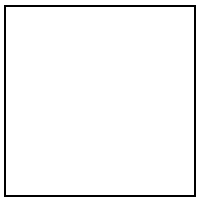


Figura N° 57 Creación de un Alias

El establecimiento de los alias es opcional. El paso siguiente es configurar el mecanismo de autenticación.

La autenticación permite el seguimiento de las conexiones basado en los nombres antes que en las direcciones. Con la autenticación no importa cuál dirección es utilizada o desde que estación una persona desea trabajar; el “username” define los permisos del usuario y sigue al usuario de estación en estación.

Para obtener acceso a los servicios de Internet como http o FTP, el usuario provee sus datos de autenticación mediante el username y el password. También se permite modificar la duración de la autenticación.El equipo Firebox soporta cinco métodos de autenticación, identificados por el tipo de servidor utilizado:

- Equipo Firebox
- Windows NT/2000
- RADIUS
- CRYPTOCard
- Securid

En la figura N° 58 se muestra el proceso de autenticación. El cliente realiza la misma secuencia de tareas para autentificarse contra cualquiera de estos métodos. En el primer caso, el equipo Firebox contiene internamente los usernames, passwords y grupos. En los otros cuatros métodos, se requiere que estos datos estén almacenados en el servidor autenticador.

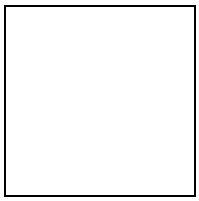
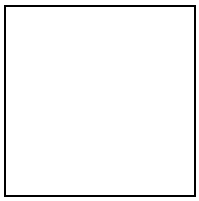


Figura N° 58 Proceso de Autenticación

El tipo de sistema a utilizar se escoge con: SetUp/Autentication (figura N° 59). Si se desea trabajar únicamente con el Equipo Firebox, se escoge “Equipo Firebox” y luego, en “Equipo Firebox Users” se añaden el usuario y el grupo al que pertenece. En esta misma opción se pueden crear nuevos grupos.



Por otra parte, si la base de datos de los usuarios se encuentra en un servidor RADIUS (de otro tipo), debe indicársele la dirección IP del servidor y el puerto que atenderá la autenticación el la opción RADIUS Server, por ejemplo.

Si el usuario es remoto (vía “dial-up”) , se requiere un servidor de acceso remoto (RAS) para llegar hasta el equipo Firebox. Al RAS debe configurársele la dirección IP del equipo Firebox para que éste pueda proceder a la autenticación (figura N° 60)

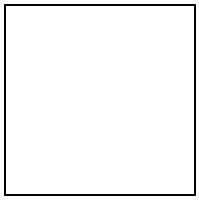


Figura N° 60 Autenticación para un usuario remoto

Sin embargo, para los usuarios remotos que serán autentificados por el equipo Firebox, se prefiere trabajar mediante túneles VPN para garantizar la seguridad de los datos enviados y no únicamente en el momento de la autenticación. Para esto el equipo Firebox dispone, por defecto, de dos grupos de usuarios: ipsec_users y pptp_users. Esto será tratado en la sección de VPN.

Finalmente, se muestra la pantalla que aparecerá en el cliente para su autenticación. Para ellos debe introducirse el siguiente URL: http://direcciónIPdelequipofirebox:4:100/java.html.

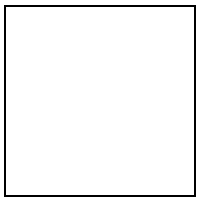


Figura N° 61 Pantalla inicial para la autenticación

Configuración de VPN en el Equipo Firebox

Una red virtual privada (VPN) permite la conexión segura entre dos redes (o entre un host y una red) a través de una tercera red insegura. El Equipo Firebox dispone de dos métodos para realizar túneles seguros:

- VPN´s para sucursales
- VPN´s para usuarios remotos

A su vez, cada una de ellas tiene diversas modalidades.

- VPN´s para sucursales

Esta configuración permite realizar túneles entre dos LAN mediante conexiones equipo Firebox-a-equipo Firebox ó equipo Firebox-a-dispositivo IPSec (figura N° 62). Nótese que el túnel se establece entre las interfaz externas de ambos equipos Firebox.

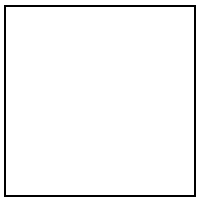


Figura N° 62 Red VPN entre sucursales

Existen tres métodos para realizar estas VPN´s:

- DVCP VPN (Protocolo Dinámico para Configuración de VPN´s)
- IPSec VPN (Internet Proptocol Security)
- WatchGuard VPN

Características del protocolo dinámico del DVCP / VPN

Es un protocolo propietario de WatchGuard en el cual un servidor DVCP (un equipo Firebox) contiene la configuración VPN de diferentes clientes como otros equipo Firebox, clientes SOHO, etc. El servidor DVCP mantiene la conexión entre dos clientes, almacenando todas las políticas de seguridad, como: rango de direcciones de las redes, propiedades del túnel (cifrado, timeouts y autenticación). Este método no será aplicado en el presente proyecto, por lo cual no se describirá.

Características del protocolo IPSec VPN

Como se explicó, IPSec es un protocolo que encripta y/o autentifica el tráfico a nivel IP entre cualquier combinación de de hosts y gateways de seguridad. El término “autenticación” se refiere al tráfico en sí y no a un usuario en particular, es decir, el destino se debe garantizar que el origen del tráfico proviene realmente del origen genuino del túnel y no de “otro” túnel. Para configurar el túnel deben procederse, en primer lugar, a establecer el gateway remoto, según los siguientes pasos:

- Remote Gateway: es el extremo remoto del túnel. Puede especificarse con la dirección IP, el nombre del dominio, etc.
- Key Negotiation Type: Es el modo de negociación de seguridad de ambos equipo s. Puede ser del tipo isakmp (dinámico) o manual.
- Shared key: Palabra clave compartida. Debe ser igual en ambos extremos.

Esta información debe repetirse para todos los gateway con los que se desea establecer túneles. En las figuras siguientes se observa la creación de dos gateways, uno con negociación tipo manual y el otro de tipo dinámico. Nótese los parámetros adicionales para el segundo. Una vez establecidos los posibles gateways, se crean los túneles. Si la seguridad se asignará manualmente, deben crearse los túneles del siguiente modo:

- Nombre del Túnel : Colocar el nombre de la conexión VPN
- Gateway Remoto: Debe escogerse el gateway del extremo remoto. Este fue creado en el procedimiento anterior. El gateway deberá tener una negociación de seguridad del tipo “Manual”
- Tipo de túnel: Puede ser ESP o AH
- Tipo de Tráfico: Normalmente se aplica el mismo tipo de túnel para el tráfico entrante y saliente

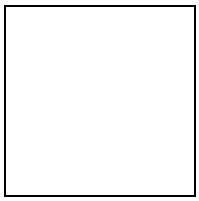


Figura N° 63 Configuración del gateway IPSec (manual)

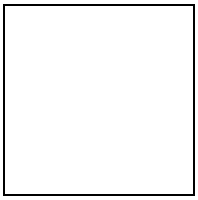


Figura N° 64 Configuración del gateway IPSec (dinámica)

Es importante destacar que se pueden crear varios túneles con el mismo gateway. Luego en el manejo de los servicios se establecerá cuál tipo de tráfico fluirá en cada túnel. El anterior procedimiento debe repetirse para crear nuevos túneles sobre otros gateways.

En el ejemplo que se muestra, al túnel “datos” se le asoció el gateway “pueba”. El tipo de encriptación puede ser DES-CBC ó 3DES-CBC y la autenticación son MD5-HMAC ó SHA1-HMAC. Nótese que existen claves diferentes para encriptar y para autentificar. El SPI (Security Parameter Index) se utiliza para mayor seguridad y debe fijarse un valor entre 257 y 1.023.

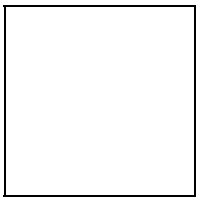


Figura N° 65 Configuración de Túneles (manual)

Por otra parte, si la seguridad se asignará dinámicamente, debe seguirse el siguiente procedimiento. Este método usa la negociación tipo “ISAKMP” la cual genera automáticamente las claves para cada nueva sesión. Entre las características del túnel están :

- Nombre del Túnel : Colocar el nombre de la conexión VPN
- Gateway Remoto: Debe escogerse el gateway del extremo remoto. Este fue creado en el primer procedimiento anterior. El gateway deberá tener una negociación de seguridad del tipo “Dynamic”
- Tipo de túnel: ESP ó AH
- Expiración de la Clave: Cada cantidad de bytes o cada cantidad de tiempo, lo que ocurra antes.

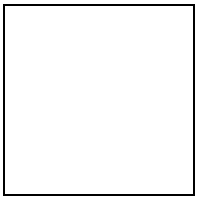


Figura N° 66 Configuración de Túneles (automática)

Creación de políticas en el IPSec

Una vez creados los túneles, debe determinarse el tipo de tráfico y servicios que fluirán a través de ellos. Para esto deben establecerse:

- Local: Direcciones IP de los Host o de las redes que están detrás de Equipo Firebox local
- Remote: Direcciones IP de los Host o de las redes que están detrás de Equipo Firebox remoto
- Diposition:

    - Secure: IPSec encriptará todo el tráfico que coincida con la regla particular en las políticas del túnel

    - Block: IPSec no permitirá el tráfico que coincida con la regla particular en las políticas del túnel

- Dst Port: Puerto de destino del tráfico al que se aplicará la política para el túnel

- Protocol: Limita los protocolos que usarán la política

- Src Port: Puerto de origen del tráfico al que se aplicará la política para el túnel

El equipo Firebox aplica las políticas según el orden de la lista, es decir, de arriba abajo. Inicialmente las políticas son listadas en ewl orden de creación. El usuario deberá reordenarlas desde las más específicas hacia las más generales. El orden sugerido es:

- Host a Host
- Host a Red
- Red a Host
- Red a Red

WatchGuard VPN

Este método permite implantar VPN entre dos Equipo Firebox. El encriptado WatchGuard usa el puerto UDP 4104. y usa cifrado de 40 y de 128 bits. También se puede disponer del DES – 128 bits y de 3DES. Este método permite hacer VPN punto a punto o configuración múltiple, de un Equipo Firebox a varios.

Los parámetros a configurar son prácticamente iguales a los anteriores, salvo algunas diferencias menores. Los principales son:

- Remote Equipo Firebox IP: extremo remoto del túnel
- Local Equipo Firebox IP: extremo local del túnel

- Encryption: Para escoger el número de bits usados para encriptar

VPN para Usuarios Remotos

Las VPNs para usuarios remotos (RUVPN) permiten establecer conexiones seguras entre un host remoto y una red protegida a través de una red insegura. RUVPN permite la conexión de usuarios viajeros, de trabajadores desde sus hogares y otros tipos de accesos a distancia.

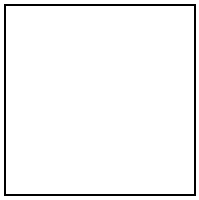


Figura N° 67 Túneles para usuarios remotos y móviles

Existen dos tipos de RUVPN:

- Usuario Remoto PPTP: usa protocolo PPTP en conexiones telefónicas o “dial-up”. Permite hasta 50 conexiones simultáneas con cualquier nivel de cifrado.

- Usuario Móvil VPN: Se aplica a usuarios remotos que poseen acceso a Internet diferente a la línea telefónica, como sistema ADSL u otro. El cifrado debe ser medio o alto.

Es importante destacar que los equipo s de comunicación como routers o RAS servers se conectan en el segmento externo de la red. En este caso, cuando un usuario accede en forma remota en el modo PPTP (módem) o IPSec (Internet), el equipo Firebox, mediante un servicio llamado “Any” crea un túnel internamente en el equipo Firebox, desde la interfaz externa hasta la interna. Luego de la autenticación, el usuario se encuentra conectado en

forma “lógica” en el lado interno de la red aunque físicamente se encuentre en el lado externo. De este modo, se comporta como un usuario más interno.

Para ambos tipos de usuario RUVPN se requiere configuración en el equipo Firebox y en el host remoto. Se describirá inicialmente la configuración en el equipo Firebox. Para ello se requiere la siguiente información:

- El bloque de direcciones IP para asignar a los usuarios durante las sesiones.
- Direcciones de servidores DNS o WINS
- Los usernames y password de los usuarios
- Para los usuarios móviles, se debe tener la licencia respectiva y capacidad para cifrado medio o alto en el Equipo Firebox

El equipo Firebox incluye automáticamente dos grupos de usuarios para este servicio: pptp_users y ipsec_users. Cuando el usuario se autentifica ante el equipo Firebox, éste automáticamente añade la dirección IP remota al grupo. Luego, el equipo Firebox utilizará el grupo para la configuración de servicios para el tráfico saliente y entrante a los usuarios RUVPN.

El proceso para añadir usuarios es similar para los casos de PPTP e IPSec. Para ello debe escogerse la opción SetUp/Autentication/Equipo Firebox Users/Add (figura N° 68).

Una vez creados los usuarios, se le deben asignar los servicios permitidos. Estos se puede hacer de dos formas:

- Modificándose las propiedades del servicio específico (por ejemplo http), agregando:
  Incoming
  - Enabled and Allowed
  - From: pptp_users o ipsec_users
  - To: Any

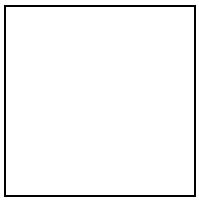


Figura N° 68 Usuarios en los grupos ipsec_users y pptp_users

Outgoing:

- Outgoing allowed
- From: Any
- To: pptp_users o ipsec_users

Activando el servicio “Any” y, dentro de él, se establecen las propiedades:

Incoming

- Enabled and allowed
- From: pptp_users o ipsec_users
- To: seleccionado

Outgoing

- Enabled and allowed
- From: seleccionado
- To: pptp_users o ipsec_users

Configuración del servicio usuario PPTP

Los usuarios PPTP se conectan en la red interna. Generalmente conviene asignarle direcciones IP de una red secundaria conectada a la interfaz interna.

Para generar el servicio PPTP se debe agregar el ícono wg_pptp en la pantalla “Arena de Servicios”. Esto se hace con Network/Remote User/PPTP. Habilitando el checkbox correspondiente, aparece este ícono. Posteriormente debe asignarse el poll de direcciones que se asignarán a los usuarios a medida que se conecten (Network/Remote User/PPTP/Add/Chose Type).

Configuración del servicio usuario móvil VPN

El acceso se hace desde un host remoto a través de Internet (ADSL u otro servicio) y no mediante línea telefónica. A diferencia del anterior, el administrador puede obtener mayor control sobre la configuración del cliente a través de un archivo de configuración de usuario final. Para configurarlo se requiere:

- Licencia de WatchGuard
- Agregar los nombres de los usuarios en el grupo ipsec_users
- Crear los archivos de configuración de usuario final
- Configurar las propiedades de los servicios usando ipsec_users
- Distribuir la configuración de usuario final junto con el software cliente RUVPN y la documentación

En primer lugar se debe instalar la licencia (license key) aplicable a un grupo de usuarios (Network/Remote User/Mobile User Licenses/Add).

Luego se debe crear la configuración para usuario móvil VPN y su archivo de configuración respectivo. Este archivo tiene extensión .exp y contiene la clave compartida del usuario (“shared key”), la identificación del usuario, direcciones IP y parámetros para crear un túnel seguro entre el host remoto y el Equipo Firebox. Para realizar la configuración, se debe entrar Network/Remote User/Mobile User VPN/Add (figura N° 69).

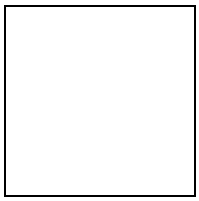


Figura N° 69 Creación de un usuario móvil

Luego, usando la guía (wizard) se establecen:

- Username
- Clave compartida (shared key): esta no es la misma que Equipo Firebox Users usa para la autenticación, anque se le puede asignar el mismo valor
- Dirección IP virtual para el usuario
- Método del túnel: ESP ó AH
- Método de autenticación: MD5-HMAC (algoritmo de 128 bits) o SHA1-HMAC (algoritmo de 160 bits)
- Método de cifrado: DES-CBC (56 bits) y 3DES-CBC (168 bits)

Para activar el servicio, debe guardarse la configuración en el Equipo Firebox. Durante este proceso, también puede guardarse en un disco la configuración de usuario final en un archivo .exp.

Para ambos servicios debe instalarse el software cliente en los hosts remotos. Adicionalmente, para los usuarios móviles VPN debe instalarse el archivo de configuración generado en el paso anterior.

Finalmente, todos los tipos de VPN descritas pueden observarse, una vez configuradas, en la pantalla principal del sistema.

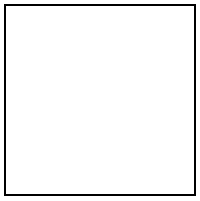


Figura N° 70 Túneles VPN configurados

Monitoreo / Supervisión

Estas funciones son importantes para determinar la calidad del servicio, posibles “cuellos de botella” en la red, requerimientos de equipo s y eventuales ataques. Se describirán brevemente los mecanismos para llevar a cabo estas tareas. Todas las opciones que se describen se obtienen de la barra superior del menú principal.

HostWatch

Esta aplicación monitorea todas las conexiones del equipo Firebox en tiempo real. En forma gráfica se indican las conexiones entrantes y salientes con las direcciones IP de las máquinas o nombres de usuarios o servidores en el origen y el destino. Mediante los colores rojo, azul, verde y negro se identifican las conexiones “negadas”, “por proxy”, “por NAT” y “ninguna de las anteriores” respectivamente. Si se desean ver en el HostWatch los intentos negados de telnet entrantes, debe configurarse el Equipo Firebox para realizar el “log” respectivo. Apréciense las direcciones no válidas internas y las válidas externas, así como la indicación a color del tráfico. Abajo se ofrecen detalles a nivel de texto.

Bandwidth Meter

Este servicio muestra el uso del ancho de banda en cada una de las interfaces del WatchGuard. Se indica el tráfico saliente y entrante de la interfaz externa.

Service Watch

Esta aplicación muestra el número de conexiones por servicio en el tiempo. En gráficos x-y, los servicios se encuentran el el eje x diferenciados por colores. Aquí se observan la cantidad de conexiones tipo HTTP y SMTP a través de la interfaz externa (abajo a la izquierda).

StatusReport

Provee un conjunto de estadísticas de la actividad del Equipo Firebox, como: tiempo de actividad del Equipo Firebox, conteo de paquetes permitidos, negados y rechazados, configuración de redes, conexiones

activas TCP, FTP, etc,; bloqueo de sitios y puertos, promedio de carga, procesos activos del Equipo Firebox, tabla ARP, etc. En la siguiente figura se indican algunos aspectos del StatusReport. Al final se observa el número de paquetes permitidos y rechazados. También se indica el estado de la configuración de las tres interfaces Ethernet (Eth0, Eth1, Eth2) y las reglas aplicadas al tráfico. Finalmente, se muestran los procesos que se ejecutan en el Equipo Firebox, a nivel de su sistema operativo Linux.

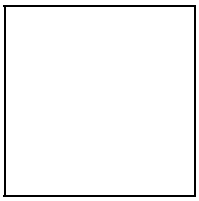


Figura N° 71 Status Report

Generación de Reportes

Los reportes se utilizan para realizar resúmenes del comportamiento del tráfico, basándose en varios criterios. La siguiente pantalla despliega las horas de inicio y fin de los reportes el número de paquetes entrantes y salientes capturados. En la figura siguiente se aprecian las estadísticas del número de conexiones en el tiempo, número y porcentaje de conexiones por servicio (http, POP3, etc.) y número de sesiones entre hosts, respectivamente.

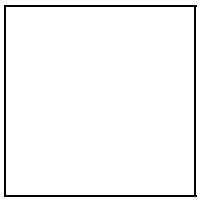


Figura N° 72 Conexiones por Tipo de Servicio

Existen gran número de reportes clasificados de diversas formas, pero sólo se han mostrado algunos de los más representativos.

Auditoría (logging) y Notificación

Estas tareas son cruciales para ahacer seguimiento a las políticas de seguridad. La auditoría (logging, término más común) se refiere al registro de un evento por parte del equipo Firebox en un archivo log. La notificación ocurre cuando el equipo Firebox envía un correo, dispara una ventana en el Event Processor o disca un número telefónico para notificar al administrador la ocurrencia de un evento. Esto permite monitorear la seguridad de la red, identificar los ataques y los atacantes y tomar las acciones necesarias.

Cuando los logging y notificaciones se envían a una máquina diferente (Event Processor) la información es cifrada en 3-DES. El cifrado no se realiza al almacenarse la información en la misma máquina. Existen numerosas opciones para el logging y la notificación. Prácticamente cada tipo de tráfico o de acción del Equipo Firebox se puede registrar. Sólo se mencionarán algunos aspectos.

En primer lugar se debe establecer la dirección IP de la estación que recibirá los logs y las notificaciones.Luego, cada servicio debe configurarse si se desea que genere logs. En el caso anterior, se le puede establecer al servicio FTP que se registren los accesos denegados o permitidos para el tráfico saliente o entrante. Lo mismo aplica para todos los servicios.

LogViewer

Las entradas logs son guardadas en el Procesador de Eventos. Por defecto, los archivos logs son almacenados en el subdirectorio \logs. La utilidad LogViewer provee una vista dinámica de este archivo de datos. Pueden aplicarse filtros para buscar logs o campos especificos.

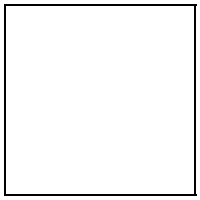


Figura N° 73 Visualización de los logs

En esta sección sólo se han mostrado algunas de las vistas más importantes del equipo Firebox que contribuyen a llevar a cabo parte de las funciones de gestión de red. En realidad, este es uno de los puntos más fuertes del equipo .

3.2 Servicios IPTABLES y SQUID sobre Sistema Operativo Linux

La mayor parte de la Red Platino en el Área Metropolitana de Caracas está conformada por una gran LAN de fibra óptica y enlaces inalámbricos. Independientemente de los enlaces dedicados tipo “clear channel” que comunican instituciones a través de enrutadores, un gran número de instituciones están conectadas directamente a los “switches” de Red Platino mediante fibra óptica (16 instituciones en ambas torres de Parque Central) y a través de enlaces inalámbricos (40 instituciones de Caracas). Estas últimas generan una gran volumen de tráfico tipo “broadcasting” y de tipo indeseado (video, audio, sitios prohibidos, etc.) que afecta el desempeño de las aplicaciones y datos que se intercambian entre los nodos regionales, Red Platino y Red INE. En otras palabras, se debe aplicar control de tráfico desde/hacia otras instituciones. Para este fin se impone la incorporación de un tipo de dispositivo entre las LAN´s de las instituciones conectadas vía fibra óptica o radio con Red Platino. Este dispositivo debe ser colocado físicamente en cada una de las instituciones que acceden a Red Platino y, en lo posible debe generar poco o ningún gasto económico adicional.

En este sentido se recurrió a una solución estable y comprobada de software libre (GNU) sobre plataforma Linux, consistente el las herramientas “IPTABLES” que es un enrutador y filtro de paquetes y el “SQUID” , un proxy cache. Estas soluciones operan sobre un PC convencional (Pentium II

o III), equipado con dos interfaz de red, lo cual es fácil de obtener en cualquier institución. Se consideran estos productos muy convenientes por no requerir de mayor inversión por parte de los entes involucrados (y todo el proceso administrativo que ello acarrea) y por estar soportados por la robusta plataforma Linux Debian.

A continuación se explica, a modo de ejemplo, la configuración típica del servidor “enrutador-filtro-proxy” implantada en la institución INAM (instituto Nacional del Menor) la cual se encuentra conectada a Red Platino mediante fibra óptica. Una solución similar a la que se describe se aplicó en MPD (Ministerio de Planificación y Desarrollo) y progresivamente se incorporarán el resto mediante este sistema.

Configuración de IPTABLES

Como se indicó, Red Platino asigna a las instituciones subredes del bloque 172.20.0.0/16. Generalmente, las instituciones usan estas subredes o pueden poseer un esquema de direccionamiento interno diferente. En el caso que se describe, INAM usa un bloque 172.16.0.0/16. El servidor de comunicaciones se inserta entre la red interna INAM y Red Platino, como se indica en la (figura N° 74).

Figura N° 74 SQUID e IPTABLES

IPTABLES actúa como un enrutador, filtro de paquetes a nivel de las capas 3 y 4, y servidor de NAT. A continuación se muestra un extracto del archivo de configuración (“router”) de este servicio, ubicado en /etc/init.d. Se explicará en detalle cada línea de configuración:

Colocación en “1” de la bandera ip_forward para activar a IPTABLES en modo enrutamiento. En este modo se puede redirigir el tráfico entre las interfaz del PC:

- echo 1 > /proc/sys/net/ipv4/ip_forward

Creación del NAT dinámico saliente. Las direcciones de origen (“-s”) 172.16.0.0/16 son convertidas a direcciones de origen 172.20.204.63, la cual es una de las direcciones de la interfaz externa del PC. Este proceso se hace en la fase del “POSTROUTING” del IPTABLES:

- iptables -t nat -A POSTROUTING -s 172.16.0.0/16 -j SNAT --to-source 172.20.204.63

Se hace un NAT estático entrante para el servidor de correo del INAM. La dirección 172.20.204.4 fue asignada por parte de Red Platino para este servidor de correo (paralelamente a esto, Red Platino también tiene un pool de direcciones para NAT estáticos con respecto a Internet). Es preciso convertir 172.20.204.4 a 172.16.43.201, en las conexiones provenientes de Red Platino hacia INAM, por lo que el NAT se aplica a direcciones de destino:

- iptables -t nat -A PREROUTING -d 172.20.204.4 -j DNAT --to-destination 172.16.43.201

Se añade la dirección 172.20.204.4 a la interfaz externa eth0 para que pueda ser accedida desde Red Platino:

- ip addr add 172.20.204.4 dev eth0

Se aplican filtros para permitir únicamente tráfico entrante (INPUT) hacia los servicios de correo (puertos 25 y 110, en el servidor 172.20.204.4):

- iptables -t filter -A INPUT -p tcp -i eth0 -d 172.20.204.4 --dport 25 -j ACCEPT
- iptables -t filter -A INPUT -p tcp -i eth0 -d 172.20.204.4 --dport 110 -j ACCEPT

Se aplican filtros para permitir únicamente tráfico saliente (OUTPUT) hacia los servicios de FTP (puertos 20 y 21) ubicados en el servidor de Red Platino, a los fines de actualizar su sitio Web:

- iptables -t filter -A OUTPUT -p tcp -i eth0 -d 172.20.204.4 --dport 21 -j ACCEPT
- iptables -t filter -A OUTPUT-p tcp -i eth0 -d 172.20.204.4 --dport 20 -j ACCEPT
- iptables -t filter -A OUTPUT -p tcp -i eth0 -d 172.20.204.4 --dport 20 -j ACCEPT

Se prohíbe (DROP) cualquier otro tipo de tráfico entrante

- iptables -t filter -A INPUT -i eth0 -d 172.20.204.4 -j DROP

Se redirige (REDIRECT) el tráfico cuyo destino (“dport”) sea el puerto 80 (Web) hacia el puerto 3128 en el cual el SQUID está esperando peticiones para procesarlas:

- iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 3128

El SQUID, como se describirá, aplicará restricciones a los contenidos Web. Sólo el tráfico con destino al puerto 80 se redirigirá al SQUID, el resto será enrutado según la configuración de IPTABLES.

Con la inserción de este punto de control en la red de la institución se logra:

- Eliminar el tráfico broadcasting que llegaba a Red Platino, el cual queda restringido a la LAN interna del cliente.

- Filtrar el tráfico indeseado, reduciendo el ancho de banda utilizado en los switches y routers de Red Platino. Como complemento, se protege a los servidores ubicados en la institución.

Configuración de SQUID

A continuación se muestran las partes más importantes del archivo de configuración “squid.conf”, que se encuentra en /etc/ en el cual se programa el comportamiento de este servicio. La mayor parte de los

comentarios se encuentran dentro de este archivo, sin embargo, se resaltarán los aspectos más importantes.

En esta porción se establece el puerto de escucha 3128 como el receptor de mensajes por parte del SQUID. El tráfico es redireccionado por IPTABLES a este puerto 3128. También están definidos por defecto los protocolos icp y htcp para comunicación con otros proxy cachés vecinos (esta característica no se usa en el presente proyecto):

```
proxy:~# cd /etc
proxy:/etc# more squid.conf

#       IP address with port.
#
#       The default port number is 3128.
```

Con la opción *no_cache* se obliga a no guardar ciertos objetos en la memoria temporal. Esta característica tiene utilidad cuando se trata de programas ejecutables o respuestas de programas a datos previamente introducidos (por ejemplo, la repuesta a un formulario bancario):

```
#  TAG: no_cache
#       A list of ACL elements which, if matched, cause the reply to
#       immediately removed from the cache.  In other words, use this
#       to force certain objects to never be cached.
#
#       You must use the word 'DENY' to indicate the ACL names which
should
#       NOT be cached.
#
#We recommend you to use the following two lines.
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
```

Las opciones que siguen se refieren al tamaño del caché y porcentajes de utilización del área de “swap” del disco duro. Se toman las opciones por defecto:

```
#       Data for these objects are stored in 4 KB blocks.  This
```

```
#       parameter specifies the ideal upper limit on the total size of
#       4 KB blocks allocated.  In-Transit objects take the highest
#       priority.
#
#Default:
# cache_mem 8 MB

#  TAG: cache_swap_low  (percent, 0-100)
#  TAG: cache_swap_high (percent, 0-100)
#
#       The low- and high-water marks for cache object replacement.
#       Replacement begins when the swap (disk) usage is above the
#       low-water mark and attempts to maintain utilization near the
#       low-water mark.  As swap utilization gets close to high-water
#       mark object eviction becomes more aggressive.  If utilization is
#       close to the low-water mark less replacement is done each time.
#
#       Defaults are 90% and 95%. If you have a large cache, 5% could be
#       hundreds of MB. If this is the case you may wish to set these
#       numbers closer together.
#
#Default:
# cache_swap_low 90
# cache_swap_high 95
```

Relacionados con el punto anterior, están los tamaños máximos y mínimos de los objetos a ser almacenados temporalmente:

```
#  TAG: maximum_object_size     (bytes)
#       Objects larger than this size will NOT be saved on disk.  The
#       value is specified in kilobytes, and the default is 4MB
#Default:
 maximum_object_size 4096 KB


#  TAG: minimum_object_size     (bytes)
#       Objects smaller than this size will NOT be saved on disk.  The
#       value is specified in kilobytes, and the default is 0 KB, which
#       means there is no minimum.
#
#Default:
# minimum_object_size 0 KB
```

En el siguiente archivo se guardan las solicitudes realizadas por los clientes e información sobre su permiso o rechazo.

```
#  TAG: cache_access_log
#       Logs the client request activity.  Contains an entry for
#       every HTTP and ICP queries received.
#
#Default:
 cache_access_log /var/log/squid/access.log
```

La auditoria de la actividad del SQUID queda registrada en el archivo “cache.log”, cuya ruta se configura a continuación.

```
#  TAG: cache_log
#       Cache logging file. This is where general information about
#       your cache's behavior goes. You can increase the amount of data
#       logged to this file with the "debug_options" tag below.
#
#Default:
# cache_log /var/log/squid/cache.log
```

Cabe señalar que, en ocasiones, se utiliza una aplicación llamada “calamaris” para la presentación de la información de “cache.log” en una forma más elegante.

La etiqueta *acl* permite la definición de las listas de acceso (Access list): Las listas de acceso son creadas por etiquetas de la forma:

acl aclname acltype

El aclname es el nombre que el usuario le desea dar a la lista. Generalmente se colocan nombres descriptivos como “pornografía” o “violencia” según la restricción que se esté aplicando. El acltype se refiere al tipo de objeto que se le aplicará la lista de acceso. Entre los tipos más comunes están:

- src: dirección-IP/máscara de origen
- acl: dirección-IP/máscara de destino

- srcdomain: dominio de origen
- dstdomain: dominio destino
- srcdom_regex: nombre de la máquina cliente
- dstdom_regex: nombre del servidor
- time: establece días y horas dentro de la semana
- url_regex: indica un URL particular
- port: se aplica a los puertos
- myport: se aplica al puerto propio
- proto: establece el protocolo como HTTP, FTP, etc.
- method: indica el método dentro de un servicio particular, como: GET, POST, etc

Según lo indicado, se crean las listas de acceso utilizando direcciones IP de origen, URL's de destino y puertos de destino, como se indica en el siguiente fragmento:

```
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl porno url_regex  .*http://www.sexplexx.com*
.*http://www.adulteras.com*
acl porno url_regex  .*http://www.sexyven.net* .*http://a-rated-sex.com*
.*http:
//www.all-sexxx.com*
acl porno url_regex  .*http://ranking.sexranks.com*  .*http://www.sex-
movies-qua
lyty.co*
acl porno url_regex  .*http://http://www.culo.com*
.*http://www.chicas.com* .*h
ttp://www.pussy.com*
acl porno url_regex  .*http://www.anpland.com*
.*http://www.megapage.org/html*
 .*http://www.sexylegsplaygirl.com*
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
```

```
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl Safe_ports port 901         # SWAT
acl purge method PURGE
acl CONNECT method CONNECT
```

La etiqueta http_access permite o niega el acceso basado en las listas de acceso anteriores. El formato es:

http_access allow|deny [!]aclname ...

donde " !aclname " significa "no pertenece" a la lista de acceso. Si no aparecen líneas http_access, la opción por defecto es negar la solicitud. A continuación se muestran la configuración para restringir o permitir el tráfico tipo http:

```
#Default:
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Only allow purge requests from localhost
http_access allow purge localhost
http_access deny purge
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM
YOUR CLIENTS
#
http_access allow localhost
# And finally deny all other access to this proxy
http_access deny porno
http_access allow all
```

```
#  TAG: icp_access
#       Allowing or Denying access to the ICP port based on defined
#       access lists
#
#       icp_access  allow|deny [!]aclname ...
#
#       See http_access for details
#
#Default:
# icp_access deny all
#
#Allow ICP queries from eveyone
icp_access allow all
```

3.3 Configuración de los Conmutadores

Una parte fundamental en la configuración de las redes en la topología vista, consiste en la segmentación o creación de VLAN´s virtuales en los nodos regionales, Red Platino e INE. Con ellas se logra el establecimiento de las zonas interna, pública o DMZ y externa. En el siguiente apartado se comenta la creación de estos tres segmentos en el switch marca Allied, Modelo Rapier 24, utilizado en este proyecto.

Presentación del estado inicial del switch (show VLAN). Se aprecia que en el switch existe una VLAN por defecto (VLAN 1) que contiene los 24 puertos y la cual no puede ser borrada:

```
Manager Switch_Platino> sh vlan

 VLAN Information
Manager Switch_Platino>
--------------------------------------------------------------------------------
 Name ..... default
Identifier ..... 1
Status ..... static
Untagged ports ..... 1-24
Tagged ports ..... None
Spanning Tree ..... default
```

Trunk ports ..... None
Mirror port ..... None

Creación de la VLAN2. Se crea una VLAN 2 con el nombre de “interna” :

Manager Switch_Platino> create vlan=interna vid=2

Info (189003): Operation successful.

Añadido de puertos a la VLAN. A la VLAN 2 se le asignan 8 puertos (1-8):

Manager Switch_Platino> add vlan=2 port=1-8

Info (189003): Operation successful.

Presentación del estado actual de las VLAN´s. Se observa que se han restado 8 puertos a la VLAN 1 y se han añadido a la VLAN 2
Manager Switch_Platino> sh vlan

VLAN Information

Name ..... default
Identifier 1
Status ..... static
Untagged ports 9-24
Tagged ports ..... None
Spanning Tree ..... default
Trunk ports ..... None
Mirror port ..... None
Attachments:

Module	Protocol	Format	Discrim	MAC address
GARP	Spanning tree	802.2	42	-

Name ..... interna
Identifier 2
Status ..... static
Untagged ports 1-8
Tagged ports ..... None

Spanning Tree ..... default
Trunk ports ..... None
Attachments:

Module	Protocol	Format	Discrim	MAC address
GARP	Spanning tree	802.2	42	-

Utilizando los comando “cre ” y “add ” se crean las VLAN 3 y VLAN 4 con los puertos 9-16 y 17-24 respectivamente. Finalmente, el switch que con cuatro VLAN´s, pero la primera no tiene puertos asignados y sólo las restantes 2, 3 y 4 serán utilizadas en la práctica para conectar los servidores, Equipo Firebox, router, etc.

3.4 Configuración de los enrutadores

Para utilizar la nube ATM/FR, los routers de los nodos regionales y de Red Platino deben configurarse de acuerdo a las Centrales FR de CANTV que prestarán el servicio de transporte. Se utilizarán direcciones en la gama 10.0.0.X para asignarlas a los puertos WAN. Los DLCI utilizados fueron asignados experimentalmente por CANTV con carácter de prueba.

Enrutador Principal

El enrutador principal, ubicado en Red Platino, es un Cisco 4500. El mismo provee las conexiones hacia los nodos regionales y hacia la sede de INE. Adicionalmente posee las rutas hacia otras instituciones servidas por Red Platino y hacia el proveedor de servicio CANTV. En esta discusión de omitirán los últimos dos aspectos y nos centraremos en las conexiones desde/hacia los nodos e INE.

A continuación se describirá la configuración del enrutador Cisco 4500:

Creación de la interfaz Serial0 con encapsulación tipo Frame Relay
interfaz Serial0:
no ip address encapsulation frame-relay
no fair-queue
frame-relay traffic-shaping
hold-queue 1024 out

Creación de las subinterfaz dentro de la interfaz Serial0. Cada subinterfaz corresponde a un enlace virtual Frame Relay hacia un nodo regional y debe tener asignado una dirección IP y un DLCI :

interfaz Serial0.1 point-to-point
 description (Enlace Maracay)
 ip address 10.0.0.1 255.255.255.252
 frame-relay class frs1
 frame-relay interfaz-dlci 103
!
interfaz Serial0.2 point-to-point
 description (Enlace Valencia)
 ip address 10.0.0.5 255.255.255.252
 frame-relay class frs1
 frame-relay interfaz-dlci 104
!

interfaz Serial0.3 point-to-point
 description (Enlace Maracaibo)
 ip address 10.0.0.9 255.255.255.252
 frame-relay class frs1
 frame-relay interfaz-dlci 170

Tabla de enrutamiento. Se encamina el tráfico con dirección de destino 200.44.63.X hacia los tres nodos regionales:

ip route 200.44.63. 255.255.255 10.0.0.2
ip route 200.44.63. 255.255.255 10.0.0.6
ip route 200.44.63. 255.255.255. 10.0.0.10

Enrutador de un Nodo Regional

A continuación se muestra la configuración del nodo regional Maracay. Se define en primer lugar la interfaz serial:

```
interfaz Serial0   ;
 description ( Enlace Red Platino)
 ip address 10.0.0.2 255.255.255.252
 no ip directed-broadcast
 encapsulation frame-relay
 no ip route-cache
 no ip mroute-cache
 no fair-queue
 frame-relay class frs1
 frame-relay interfaz-dlci
 hold-queue 1024 out
```

Se establece la tabla de enrutamiento. En este caso, todo el tráfico saliente (Internet+INE+Otras Instituciones) será dirigido a Red Platino:

- ip route 0.0.0.0 0.0.0.0 10.0.0.1

El resto de los nodos regionales se configuran de modo similar.

3.5 Configuración de los Servidores

En los servidores ubicados en Red Platino e INE se hizo necesario modificar su esquema de direccionamiento para adaptarlo al nuevo plan propuesto. A continuación se muestra la nueva configuración de red del servidor de Web apolo.platino.gov.ve, sobre plataforma LINUX. El resto de los servidores posee configuraciones similares pero, por carácter de confidencialidad, no pueden publicarse.

Entrada al sistema:

```
login as: root
root@161.196.215.65's password:
Last login: Fri Jan  3 09:35:57 2003 from ip-172-20.245.38.platino.inet on
pts/0
```

```
Linux  2.4.18-bf2.4 #1 Son Apr 14 09:53:28 CEST 2002

Most of the programs included with the Debian GNU/Linux system are
freely redistributable; the exact distribution terms for each program
are described in the individual files in /usr/share/doc/*/copyright

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jan  3 09:35:57 2003 from ip-172-20.245.38.platino.inet
```

Modificando el archivo “interfaz” ubicado en la ruta /etc/network, se coloca la nueva configuración:

```
apolo:/etc/network# more interfaz
# /etc/network/interfaz -- configuration file for ifup(8), ifdown(8)

# The loopback interfaz
auto lo
iface lo inet loopback

# The first network card - this entry was created during the Debian
installation
# (network, broadcast and gateway are optional)
auto eth0
iface eth0 inet static
      address 161.196.215.65
      netmask 255.255.255.192
      network 161.196.215.64
      broadcast 161.196.215.127
      gateway 161.196.215.98
```

Los servidores DNS se definen en /etc/resolv.conf:

```
firewall:/etc# more resolv.conf
search inam-msds.gov.ve
nameserver 161.196.215.65
nameserver 161.196.215.71
```

Para mostrar la configuración se aplica #ifconfig -a

```
firewall:/etc# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:50:04:68:C7:EE
```

```
          inet addr:172.20.204.63  Bcast:172.20.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10226974 errors:840 dropped:0 overruns:0 frame:865
          TX packets:3526771 errors:0 dropped:0 overruns:0 carrier:0
          collisions:3922 txqueuelen:100
          RX bytes:995792880 (949.6 MiB)  TX bytes:478535455 (456.3 MiB)
          Interrupt:11 Base address:0xcc00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1393 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1393 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:332753 (324.9 KiB)  TX bytes:332753 (324.9 KiB)
```

3.6 Estructura Física de la Red

La red de cada nodo regional estará construida bajo cableado estructurado, UTP nivel 5, norma 568B, con 24 puntos de red ubicados en los sitios indicados en los diagramas de piso de la siguiente sección. El cableado terminará en el distribuidor (“patch pannel”) de la sala de control. El distribuidor de cable y los equipo s de conectividad (concentrador, conmutador, enrutador y equipo de seguridad) estarán instalados en un bastidor dentro de la sala de control.

Para implementar el sistema se requieren los siguientes equipo y obras:

En cada nodo regional:

- Cableado estructurado para 24 puntos
- Conmutador (“switch”)
- Enrutador (“router”)
- Sistema de Protección VPN/Cotafuegos/NAT/Proxy
- Administrador de Ancho de Banda
- Bastidor (“rack”)
- Enlace de larga distancia

En Red Platino:

- Interfaz WAN en el enrutador hacia los nodos
- Enlace de larga distancia de 512 Kb/s hacia los nodos
- Ampliación del enlace Platino – INE a 512 Kb/s
- Sistema de Protección VPN/Cortafuegos/NAT/Proxy

En Red INE:

- Ampliación del enlace Platino – INE a 512 Kb/s
- Sistema de Protección VPN/Cortafuegos/NAT/Proxy

Diagramas de Piso y Cableado

Se presentan los planos de planta, con las ubicaciones previstas para los puntos de red y la sala de control. Los puntos de red, marcados como puestos de trabajo, deben disponer de una toma hembra para red ("wall plate"). El cableado estructurado estará orientado hacia el bastidor ubicado en la sala de control.

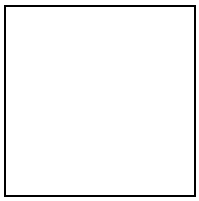


Figura N° 75 Diagrama de Planta Nodo Regional Maracay

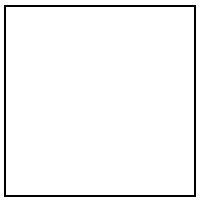


Figura N° 76 (a) Diagrama de Planta Nodo Regional Valencia

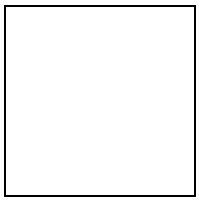


Figura N° 76 (b) Diagrama de Planta Nodo Regional Valencia (Cont.)

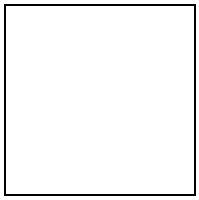


Figura N° 77 Diagrama de Planta Nodo Regional Maracaibo

Asignación de Puertos en los Conmutadores

En los siguientes diagramas se muestra la asignación de puertos en los switches de los nodos

Puerto	Equipo Conectado
1	Hub Interno 1
2	Hub Interno 2
3	Hub Interno 3
4	Hub Interno 4
5	Servidor Base de Datos Industria
6	Servidor Base de Datos Comercio
7	Servidor Base de Datos Encuestas
8	Servidos Base de Datos Censo
9	Servidor Base de Datos Hogar
10	Servidor de Respaldo 1
11	Servidor de Respaldo 2
12	Interfaz Interna del Equipo Firebox
13	Servidor Web www.ine.gov.ve
14	Servidor Web www.sistine.gov.ve
15	Interfaz DMZ del “Equipo Firebox”
16	Libre
17	Libre
18	Libre

19	Puerto Ethernet Router Cisco
20	Puerto Ethernet Modem de Antena
21	Interfaz Externa del “Equipo Firebox”
22	Libre
23	Libre
24	Libre

Tabla N° 7 Conmutador Nodo INE

VLAN 1: Sin puertos (por defecto)

VLAN2: Interna (puertos del 1 al 12)

VLAN3: DMZ (puertos del 13 al 18)

VLAN4: Externa (puertos del 19 al 24)

Puerto	**Equipo Conectado**
1	Hub Interno
2	Servidor de Red
3	Servidor de Base de Datos
4	Interfaz interna del “Equipo Firebox”
5	
6	
7	
8	
9	
10	
11	
12	
13	Servidor de Web
14	Interfaz DMZ del “Equipo Firebox”
15	
16	
17	
18	
19	Puerto Ethernet del “Equipo Firebox”
20	Puerto Ethernet del Router/RAS
21	Interfaz Externa del “Equipo Firebox”
22	

23	
24	

Tabla N° 8 Conmutador Nodo Regional

VLAN 1: Sin puertos (por defecto)

VLAN2: Interna (puertos del 1 al 12)

VLAN3: DMZ (puertos del 13 al 18)

VLAN4: Externa (puertos del 19 al 24)

Puerto	**Equipo Conectado**
1	Hub Interno 1
2	Hub Interno 2
3	Interfaz Interna del “Equipo Firebox”
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	Servidor Web/DNS Platino
14	Servidor Correo Platino
15	Servidor de Autenticación RADIUS
16	Servidor de Respaldo 1
17	Servidor de Respaldo 2
18	Interfaz DMZ del “Equipo Firebox”
19	Interfaz Eth0 del Router Cisco

20	Interfaz Eth1 del Router Cisco
21	Interfaz Ethernet del Router Cabletron
22	Interfaz Externa del “Equipo Firebox”
23	Puerto de Antena “Spike”
24	RAS

Tabla N° 9 Conmutador Nodo Platino

VLAN 1: Sin puertos (por defecto)

VLAN2: Interna (puertos del 1 al 12)

VLAN3: DMZ (puertos del 13 al 18)

VLAN4: Externa (puertos del 19 al 24

Conclusiones

Una vez instalados los nodos regionales se realizaron diversas pruebas produciendo los siguientes resultados:

1.- El tiempo de acceso desde los nodos a los servidores de INE se encuentra alrededor de 100 mseg, lo cual resulta satisfactorio

2.- Se detectaron problemas de conexión dentro de una misma aplicación debidos a errores de programación de aplicaciones específicas

3.- Se probó la efectiva encriptación de los datagramas mediante el uso de paquetes de captura de datos como el Sniffer e Iris, instalados en las VLAN externas de las diferentes redes

4.- Se cambiaron y aplicaron diferentes restricciones de tráfico en el equipo Firebox, comprobándose su efectividad

5.- Se protege el servidor de correo de Red Platino contra el “Open-Relay”. Desde la instalación del Equipo Firebox, no ha sido incluido este servidor en la “lista negra” de algunas organizaciones de protección, como mail-abuse.org.

6.- Se ha agilizado la actualización de datos. Inclusive, muchos de ellos se cargan en “tiempo real”, favoreciendo la toma de decisiones en varios niveles gubernamentales

Recomendaciones

Actualmente Red Platino se encuentra adscrita al INE. Sin embargo, existen conversaciones para anexarla a los Ministerios de Planificación y Desarrollo y de Ciencia y Tecnología. Esta situación de incertidumbre ha causado la paralización del flujo presupuestario a Red Platino. Los nodos regionales, después de una primera etapa de instalación y pruebas, fueron suspendidos en su operación por carencias económicas en la cancelación de las tarifas de Frame Relay y telefónicas. En este sentido, la primera recomendación está dirigida al INE y a las altas autoridades de los ministerios indicados para que se resuelva el caso de la adscripción de Red Platino para que vuelva a su normal funcionamiento.

Una vez resuelta esta situación, en la operación normal de la WAN se recomienda:

- Monitorear constantemente el flujo de datos en los cinco equipos Equipo Firebox , en el SPECTRUM y los routers para detectar

    - Interrupciones en los enlaces e interfaz de los equipos
    - Cuellos de botella en los enlaces Frame Relay y en los Equipo Firebox
    - Intentos de violar las normas de seguridad
    - Asignación indebida de direcciones IP

- Revisión constante del funcionamiento de las aplicaciones ASP y Tarantella, ya que pueden causar retrasos importantes en el servicio
- Búsqueda de recursos económicos para la completación del resto de los nodos regionales

Referencias

Mendillo, Vincenzo, CDROM N°1 Seguridad en Redes y Criptografía, UCV, 2002

Mendillo, Vincenzo, CDROM N° 2 Seguridad en Redes y Criptografía, UCV, 2002

Bibliografía

Mendillo, Vincenzo, CDROM N°1 Seguridad en Redes y Criptografía, UCV, 2002

Mendillo, Vincenzo, CDROM N° 2 Seguridad en Redes y Criptografía, UCV, 2002

Feid, Sydney, TCP/IP, Prentice Hall, Mexico, 1.998

WatchGuard, User Guide,2002

Switch Allied Telesyn, CDROM Allied Telesyn