Seguridad y Alta Disponibilidad

UD 4: Instalación y configuración de cortafuegos

INDICE:

Threat Management).SEGURIDAD Y ALTA DISP

•Cortafuegos:

- Concepto. Utilización de cortafuegos.

Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. Es un mecanismo para restringir acceso entre la Internet y la red corporativa interna. Típicamente se instala un firewall en un punto estratégico donde una red (o redes) se conectan a la Internet.

Un buen Firewall para Internet puede ayudarle a impedir que extraños accedan a su PC desde Internet. Los Firewalls pueden ser de dos tipos, de software o de hardware, y proporcionan una frontera de protección que ayuda a mantener fuera a los invasores no deseados de Internet.

La existencia de un firewall en un sitio Internet reduce considerablemente las probabilidades de ataques externos a los sistemas corporativos y redes internas, además puede servir para evitar que los propios usuarios internos comprometan la seguridad de la red al enviar información peligrosa (como passwords no encriptados o datos sensitivos para la organización) hacia el mundo externo.

Si el Firewall "observa" alguna actividad sospechosa: que alguien de fuera esté intentando acceder a nuestro Pc o que algún programa espía trate de enviar información sin consentimiento, el Firewall nos advertirá con una alarma en el sistema.

Para entender el funcionamiento de este sistema, debes saber que el ordenador dispone de varias puertas de salida y entrada cuando se conecta a Internet. Éstas se llaman puertos y cada servicio que utilizas se sirve de un puerto diferente: Los navegadores de internet necesitan el puerto 80, los programas FTP el 21, etc... En general tenemos todos los puertos abiertos.

- Historia de los cortafuegos.

El término "firewall / fireblock" significaba originalmente una pared para confinar un incendio o riesgo potencial de incendio en un edificio. Más adelante se usa para referirse a las estructuras similares, como la hoja de metal que separa el compartimiento del motor de un vehículo o una aeronave de la cabina. La tecnología de los cortafuegos surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad.

Los predecesores de los cortafuegos para la seguridad de la red fueron los routers utilizados a finales de 1980, que mantenían a las redes separadas unas de otras. La visión de Internet como una comunidad relativamente pequeña de usuarios con máquinas compatibles, que valoraba la predisposición para el intercambio y la colaboración, terminó con una serie de importantes violaciones de seguridad de Internet que se produjo a finales de los 80:Clifford Stoll, que descubrió la forma de manipular el sistema de espionaje alemán.Bill Cheswick, cuando en 1992 instaló una cárcel simple electrónica para observar a un atacante.

En 1988, un empleado del Centro de Investigación Ames de la NASA, en California, envió una nota por correo electrónico a sus colegas que decía:

"Estamos bajo el ataque de un virus de Internet! Ha llegado a Berkeley, UC San Diego,

Lawrence Livermore, Stanford y la NASA Ames."El Gusano Morris, que se extendió a través de múltiples vulnerabilidades en las máquinas de la época. Aunque no era malicioso, el gusano Morris fue el primer ataque a gran escala sobre la seguridad en Internet; la red no esperaba ni estaba preparada para hacer frente a su ataque.

Primera generación – cortafuegos de red: filtrado de paquetesEl primer documento publicado para la tecnología firewall data de 1988, cuando el equipo de ingenieros Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes.

Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet. En AT&T Bell, Bill Cheswick y Steve Bellovin, continuaban sus investigaciones en el filtrado de paquetes y desarrollaron un modelo de trabajo para su propia empresa, con base en su arquitectura original de la primera generación.

El filtrado de paquetes actúa mediante la inspección de los paquetes (que representan la unidad básica de transferencia de datos entre ordenadores en Internet). Si un paquete coincide con el conjunto de reglas del filtro, el paquete se reducirá (descarte silencioso) o será rechazado (desprendiéndose de él y enviando una respuesta de error al emisor). Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico. En su lugar, se filtra cada paquete basándose únicamente en la información contenida en el paquete en sí (por lo general utiliza una combinación del emisor del paquete y la dirección de destino, su protocolo, y, en el tráfico TCP y UDP, el número de puerto). Los protocolos TCP y UDP comprenden la mayor parte de comunicación a través de Internet, utilizando por convención puertos bien conocidos para determinados tipos de tráfico, por lo que un filtro de paquetes puede distinguir entre ambos tipos de tráfico (ya sean navegación web, impresión remota, envío y recepción de correo electrónico, transferencia de archivos…); a menos que las máquinas a cada lado del filtro de paquetes son a la vez utilizando los mismos puertos no estándar.

El filtrado de paquetes llevado a cabo por un cortafuegos actúa en las tres primeras capas del modelo de referencia OSI, lo que significa que todo el trabajo lo realiza entre la red y las capas físicas. Cuando el emisor origina un paquete y es filtrado por el

cortafuegos, éste último comprueba las reglas de filtrado de paquetes que lleva configuradas, aceptando o rechazando el paquete en consecuencia. Cuando el paquete pasa a través de cortafuegos, éste filtra el paquete mediante un protocolo y un número de puerto base (GSS). Por ejemplo, si existe una norma en el cortafuegos para bloquear el acceso telnet, bloqueará el protocolo IP para el número de puerto 23.

Segunda generación – cortafuegos de estado

Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, Dave Presetto, Janardan Sharma, y Nigam Kshitij, desarrollaron la tercera generación de servidores de seguridad. Esta tercera generación cortafuegos tiene en cuenta además la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por los cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

Tercera generación - cortafuegos de aplicación Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un cortafuegos de aplicación es mucho más seguro y fiable cuando se compara con un cortafuegos de filtrado de paquetes, ya que repercute en las siete capas del modelo de referencia OSI. En esencia es similar a un cortafuegos de filtrado de paquetes, con la diferencia de que también podemos filtrar el contenido del paquete. El mejor ejemplo de cortafuegos de aplicación es ISA (Internet Security and Acceleration).

Un cortafuegos de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP (GSS). Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear esa palabra en particular. No obstante, los cortafuegos de aplicación resultan más lentos que los de estado.

AcontecimientosposterioresEn 1992, Bob Braden y DeSchon Annette, de la Universidad del Sur de California (USC), dan forma al concepto de cortafuegos. Su producto, conocido como "Visas ", fue el primer sistema con una interfaz gráfica con colores e iconos, fácilmente implementable y compatible con sistemas operativos como Windows de Microsoft o MacOS de Apple. En 1994, una compañía israelí llamada Check Point Software Technologies lo patentó como software denominándolo FireWall-1. La funcionalidad existente de inspección profunda de paquetes en los actuales cortafuegos puede ser compartida por los sistemas de prevención de intrusiones (IPS). Actualmente, el Grupo de Trabajo de Comunicación Middlebox de la Internet Engineering Task Force (IETF) está trabajando en la estandarización de protocolos para la gestión de cortafuegos.Otro de los ejes de desarrollo consiste en integrar la identidad de los usuarios dentro del conjunto de reglas del cortafuegos. Algunos cortafuegos proporcionan características tales como unir a las identidades de usuario con las direcciones IP o MAC. Otros, como los cortafuegos NuFW, proporcionan características de identificación real solicitando la firma del usuario para cada conexión.

- Funciones principales de un cortafuegos: Filtrado de paquetes de datos, filtrado por aplicación, Reglas de filtrado y registros de sucesos de un cortafuegos.

Una de las funciones más importantes de un firewall es el filtrado o control de acceso de toda la información que sea recibida en los distintos puntos de acceso a la red interna o a los sistemas finales, que son administrados por aquél. El filtrado de datos permite controlar la transferencia segura de datos basado principalmente en: la dirección de donde provienen los datos, la dirección de destino de los datos y los protocolos de transporte y aplicación utilizados.

Esta función puede ser implementada en diferentes niveles de la arquitectura de red, con lo cual se logran diferentes niveles de granularidad, es decir, qué tan minucioso es

el control de seguridad efectuado. Sobre la base del nivel donde se efectúe el filtrado,

la función se implementará en diferentes dispositivos

1. Los niveles mencionados son tres: filtrado de paquetes, control de acceso de conexiones y filtrado de datos de aplicación.

Filtrado de paquetes con NAT

Es posible efectuar el filtrado de paquetes junto con la Traducción de Direcciones de Red sin causar dificultades a ninguna de las dos funciones. La función de filtrado de paquetes se diseña ignorando por completo cualquier traducción de direcciones que se lleve a cabo ya que ésta última se realiza entre la entrada / salida de datos en el borde

de la red y el filtrado de paquetes. Las direcciones captadas por el filtro serán las

direcciones origen y destino reales.

Control de Acceso de Conexiones

Este mecanismo controla y retransmite conexiones TCP manteniendo registro del estado de todos los paquetes que agrupan tal conexión, de forma que solo aquellos hosts externos confiables puedan establecer conexiones con aquellos dispositivos habilitados a ofrecer un servicio a tales usuarios. De la misma forma es posible restringir las conexiones originadas en la red interna con destino a ciertos sitios de la red externa. Esta función es realizada por un proceso proxy instalado en un Gateway que interconecta la red interna con la red pública. Estos dispositivos son llamados gateways a nivel de circuitos. (ver Figura 8)

Una alternativa a mantener el contexto de cada paquete es utilizar tablas dinámicas basadas en las banderas SYN/ACK del encabezado de los paquetes TCP. En esta forma,

la tabla de reglas se genera a medida que un host interno solicita una conexión con un sitio externo por lo que el gateway asume la política de reenviar solo aquellos paquetes entrantes que pertenezcan a conexiones iniciadas desde el interior y rechazar aquellas iniciadas en el exterior (similar a la estrategia lograda con NAT dinámico). Mediante el uso del proxy, los sistemas internos no podrán establecer conexiones directas con el exterior sino por intermedio del proxy; quien solicite una conexión, se conectará a un puerto TCP del gateway, luego el proxy determinará si la conexión es permitida o no, basado en un conjunto de reglas

de acceso que utilizan información del encabezado del paquete TCP, luego (si la conexión fue aceptada) el gateway crea

una conexión al dispositivo interno final. En este caso, el gateway retransmitirá todos los paquetes involucrados en la conexión.

Estos gateways pueden implementar algunos mecanismos de control de acceso tales como autenticación e intercambio de mensajes de protocolo entre cliente y proxy para establecer ciertos parámetros del circuito.

El control de acceso de conexiones no es del todo transparente ya que los usuarios deben ser configurados para dirigir todas sus solicitudes al dispositivo que implemente esta función.

La ventaja del mecanismo de filtrado a nivel de circuitos es que provee servicios para un amplio rango de protocolos aunque requiere software especial en el cliente, lo que

lleva al problema de que la seguridad basada en hosts no es escalable (con una arquitectura de seguridad perimetral). A medida que crece la red, la administración de la seguridad de los clientes se hace más compleja por lo que demora más tiempo llevarla a cabo y propensa al error; esto si no se efectúa un control central e implementado de forma distribuida.

Filtrado de Datos de Aplicación

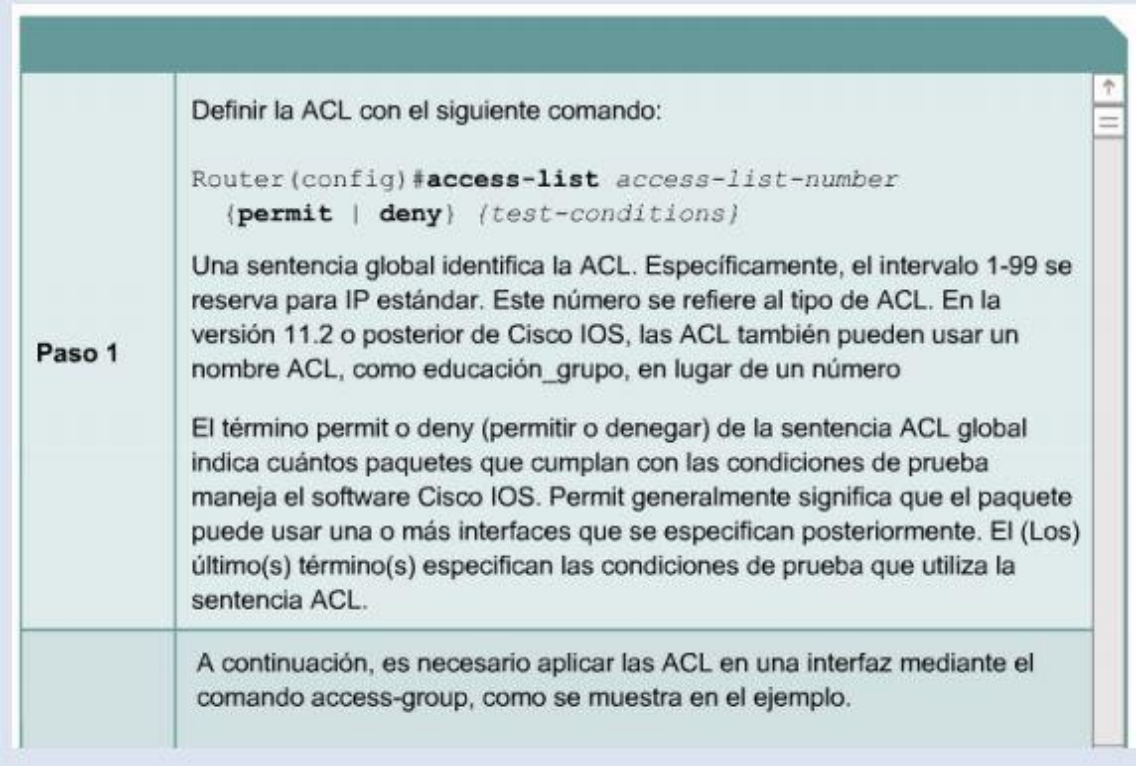
Este mecanismo interpreta los datos encapsulados en los paquetes correspondientes a protocolos de aplicación particulares para determinar si deben o no deben ser procesados por la aplicación correspondiente, ya que pueden contener datos que afecten el buen funcionamiento de las mismas. La función de seguridad ofrecida por este mecanismo es mucho más segura que las anteriores (ver Figura 9).Son implementados por servicios proxies instalados en gateways, llamados gateways a nivel de aplicación. Proveen una barrera de seguridad entre los usuarios internos y la red pública. Los usuarios de la red interna se conectan al filtro de datos de aplicación, quien funciona como intermediario entre diferentes servicios de la red externa y el usuario interno.

Son implementaciones de propósito especial que intentan ofrecer servicios de seguridad a las aplicaciones que procesen tales datos. Son específicos de la aplicación, es decir que se necesita un proceso proxy para cada aplicación. Esto presenta una desventaja de implementación. Aunque solo algunos programas o protocolos de aplicación necesitan ser analizados (por Ej. FTP y protocolos de correo electrónico, ICMP) ya que otros no presentan peligros de seguridad. El correo electrónico puede ser dirigido a través de estos dispositivos, sin importar que tecnología se utilice en el resto del firewall. También hay que tener en cuenta que el tipo de filtrado usado depende de las necesidades locales. Un sitio con muchos usuarios de PC debería analizar los archivos que reciba por posibles virus. Además presentan otra ventaja, que en algunos ambientes es bastante crítica: el registro de todo el tráfico de entrada y salida es simple implementar.

- Listas de control de acceso (ACL).

Una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en RDSI.



Paso 1	Definir la ACL con el siguiente comando: `Router(config)#access-list access-list-number {permit | deny} {test-conditions}` Una sentencia global identifica la ACL. Específicamente, el intervalo 1-99 se reserva para IP estándar. Este número se refiere al tipo de ACL. En la versión 11.2 o posterior de Cisco IOS, las ACL también pueden usar un nombre ACL, como educación_grupo, en lugar de un número El término permit o deny (permitir o denegar) de la sentencia ACL global indica cuántos paquetes que cumplan con las condiciones de prueba maneja el software Cisco IOS. Permit generalmente significa que el paquete puede usar una o más interfaces que se especifican posteriormente. El (Los) último(s) término(s) especifican las condiciones de prueba que utiliza la sentencia ACL.
	A continuación, es necesario aplicar las ACL en una interfaz mediante el comando access-group, como se muestra en el ejemplo.

En redes informáticas. En redes informáticas, ACL se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en un terminal u otro

dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio. Tanto servidores individuales como enrutadorespueden tener ACL de redes. Las listas de control de acceso pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a un cortafuegos.

Existen dos tipos de listas de control de acceso:

Listas estándar, donde solo tenemos que especificar una dirección de origen; listas extendidas, en cuya síntaxis aparece el protocolo y una dirección de origen y de destino.

Las redes empresariales necesitan seguridad para asegurarse de que solo los usuarios autorizados accedan a los recursos de red.

Las herramientas de filtrado, como las listas de control acceso, son un componente importante de la seguridad de red empresarial.

Las ACL permiten y rechazan tipos específicos de informacion entrante y trafico saliente.Los ingenieros y los técnicos de red planifican, configuran y verifican las ACL en los routers y otros dispositivos de red.

En este capítulo describiremos los siguientes puntos:

Describir el filtrado de tráfico.

Explicaremos como las listas de control de acceso (ACL) pueden filtrar el tráfico en las interfaces de Reuter.

Para los que tienen dudas sobre el filtrado de trafico aqui les doy una idea:

Filtrado de Tráfico:

La seguridad dentro de una red empresarial es sumamente importante. Es esencial impedir el acceso de usuarios no autorizados y proteger la red de diversos ataques, como los ataques DoS. Los usuarios no autorizados pueden modificar, destruir o robar datos confidenciales de los servidores. Los ataques DoS impiden el acceso de los usuarios válidos. Estas dos situaciones hacen perder tiempo y dinero a las empresas.

Mediante el filtrado de tráfico, los administradores controlan el tráfico de varios.segmentos de la red. El filtrado es el proceso de analizar los contenidos de un paquete para determinar si debe ser permitido o bloqueado.El filtrado de paquetes puede ser simple o complejo, denegando o permitiendo el

tráfico basado en:

Dirección IP de origen

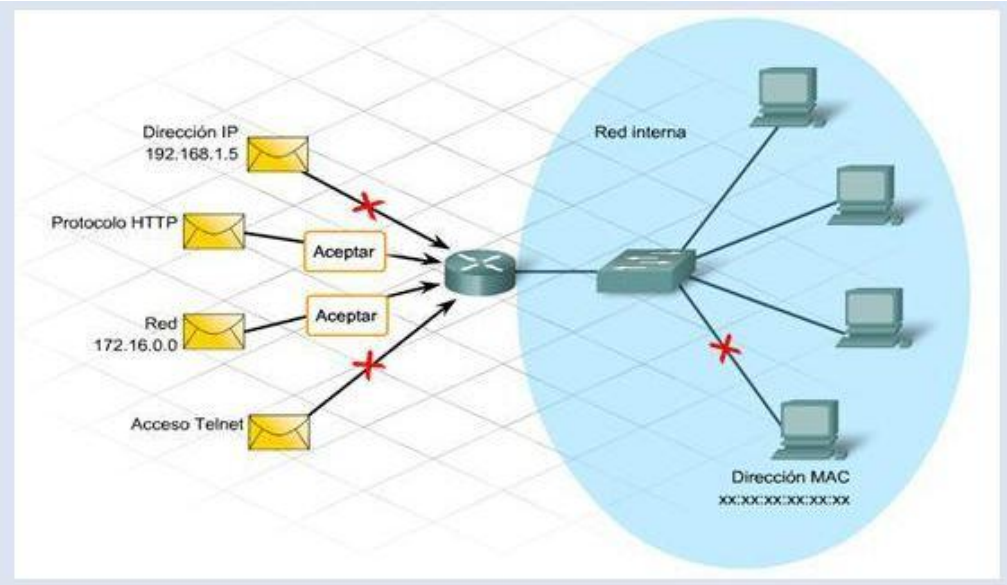
Dirección IP de destino

Direcciones MAC

Protocolos

Tipo de aplicación

El filtrado de paquetes se puede comparar con el filtrado de correo basura. Muchas aplicaciones de correo electrónico permiten a los usuarios ajustar la configuración para que los correos electrónicos enviados desde una dirección de origen particular se eliminen automáticamente. El filtrado de paquetes se puede utilizar de la misma forma mediante la configuración de un router para identificar el tráfico no deseado.El filtrado de tráfico mejora el rendimiento de la red. Al denegar el tráfico no deseado o restringido cerca de su origen, éste no viajará a través de la red ni consumirá recursos valiosos.



Los dispositivos más utilizados para proporcionar filtrado de tráfico son:

Firewalls incorporados en routers integrados

Aplicaciones de seguridad dedicadas a Servidores

Algunos dispositivos sólo filtran el tráfico que se origina en la red interna. Los dispositivos de seguridad más sofisticados reconocen y filtran los tipos de ataques conocidos de fuentes externas.

Los routers empresariales reconocen el tráfico perjudicial e impiden que ingrese y dañe la red. Casi todos los routers filtran tráfico de acuerdo con las direcciones IP de origen y de destino de los paquetes. También filtran aplicaciones específicas y protocolos tales como IP, TCP, HTTP, FTP y Telnet.

Listas de Control de Acceso:

Uno de los métodos más comunes de filtrado de tráfico es el uso de listas de control de acceso (ACL). Las ACL pueden utilizarse para administrar y filtrar el tráfico que ingresa a una red, así como también el tráfico que sale de ella.

El tamaño de una ACL varía desde una sentencia que permite o deniega el tráfico de un origen, hasta cientos de sentencias que permiten o deniegan paquetes de varios orígenes. El uso principal de las ACL es identificar los tipos de paquetes que se deben

aceptar o denegar.

Las ACL identifican el tráfico para varios usos, por ejemplo:

Especificar hosts internos para NAT

Identificar o clasificar el tráfico para funciones avanzadas tales como QoS y colas

Restringir el contenido de las actualizaciones de enrutamiento

imitar el resultado de la depuración

Controlar el acceso de terminales virtuales a los routers

El uso de las ACL puede provocar los siguientes problemas potenciales:La carga adicional sobre el router para verificar todos los paquetes se traduce en menos tiempo para el envío de paquetes.

Las ACL con diseños defectuosos colocan una carga aún mayor sobre el router y podrían interrumpir el uso de la red.Las ACL colocadas de forma incorrecta bloquean el tráfico que debe ser permitido y permiten el tráfico que debe ser bloqueado.

Tipos y Uso de ACL:

Al crear listas de control de acceso, el administrador de red tiene varias opciones. La complejidad de las pautas de diseño determina el tipo de ACL necesaria.

Hay tres clases de ACL:

1.- ACL estándar:

La ACL estándar es la más simple de las tres clases. Al crear una ACL IP estándar, las ACL filtran según la dirección IP de origen de un paquete. Las ACL estándar permiten o deniegan el acceso de acuerdo con la totalidad del protocolo, como IP. De esta manera, si un dispositivo host es denegado por una ACL estándar, se deniegan todos los servicios provenientes de ese host. Este tipo de ACL sirve para permitir el acceso de todos los servicios de un usuario específico, o LAN, a través de un router y, a la vez, denegar el acceso de otras direcciones IP. Las ACL estándar están identificadas por el número que se les ha asignado. Para las listas de acceso que permiten o deniegan el tráfico IP, el número de identificación puede variar entre 1 y 99 y entre 1300 y 1999.

2.- ACL extendidas:

Las ACL extendidas filtran no sólo según la dirección IP de origen, sino también según la dirección IP de destino, el protocolo y los números de puertos. Las ACL extendidas se utilizan más que las ACL estándar porque son más específicas y ofrecen un mayor control. El rango de números de las ACL extendidas va de 100 a 199 y de 2000 a 2699.

3.- ACL nombradas:

Las ACL nombradas (NACL, Named ACL) son ACL estándar o extendidas a las que se hace referencia mediante un nombre descriptivo en lugar de un número. Cuando se configuran ACL nombradas, el IOS del router utiliza un modo de subcomando de NACL.

Las listas de control de acceso consisten de una o más sentencias. Cada sentencia puede permitir o denegar el tráfico según parámetros específicos. El tráfico se compara con cada sentencia de la ACL en forma secuencial hasta encontrar una coincidencia o hasta que no haya más sentencias.

La última sentencia de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico. Esta función impide la entrada accidental de tráfico no deseado.Después de crear una lista de control de acceso, aplíquela a una interfaz para que entre en vigencia. La ACL se aplica al tráfico entrante o saliente a través de la interfaz.

Si un paquete coincide con una sentencia de permiso, se le permite entrar o salir del router. Si coincide con una sentencia de denegación, no puede seguir avanzando. Una ACL que no tiene al menos una sentencia de permiso bloquea todo el tráfico. Esto se debe a que al final de todas las ACL hay una denegación implícita. Por lo tanto, una ACL rechazará todo el tráfico que no está específicamente permitido.El administrador aplica una ACL entrante o saliente a una interfaz de router. La

dirección se considera entrante o saliente desde la perspectiva del router. El tráfico que ingresa a un interfaz será entrante y el tráfico que sale de ella será saliente.

Cuando un paquete llega a una interfaz, el router controla los siguientes parámetros:

¿Hay una ACL asociada con la interfaz?

¿La ACL es entrante o saliente?

¿El tráfico coincide con los criterios para permitir o para denegar?

Una ACL aplicada en dirección saliente a una interfaz no tiene efectos sobre el tráfico

entrante en esa misma interfaz.Cada interfaz de un router puede tener una ACL por dirección para cada protocolo de red. Respecto del protocolo IP, una interfaz puede tener una ACL entrante y una ACL saliente al mismo tiempo.

Las ACL aplicadas a una interfaz agregan latencia al tráfico. Incluso una ACL larga puede afectar el rendimiento del router.

- Ventajas y Limitaciones de los cortafuegos.

Ventajas de un cortafuegos

Bloquea el acceso a personas y/o aplicaciones no autorizadas a redes privadas.

Limitaciones de un cortafuegos

Las limitaciones se desprenden de la misma definición del cortafuego: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuegos (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

Un cortafuego no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él. El cortafuego no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuegos no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y

sustraerlas del edificio. El cortafuegos no puede proteger contra los ataques de ingeniería social.El cortafuegos no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.

El cortafuego no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet.

POLITICAS DE CORTAFUEGOS

Hay dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

-**Política restrictiva:** Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar la empresas y organismos gubernamentales.

-**Política permisiva:** Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a internet.La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

TIPOS DE CONTAFUEGOS

Existen dos criterios para clasificar su ubicación:

• **Cortafuegos personales:** Restringen la comunicación no autorizada con un equipo. Surgen de la necesidad de proteger los equipos particulares conectados a Internet.

• **Cortafuegos de subredes:** Aplican unas políticas de seguridad a un grupo de sistemas desde un único punto. Para ello se agrupan en zonas de seguridad, de forma que se apliquen unas normas para cada zona. En cada zona habrá un cortafuegos.

SEGÚN SU TECNOLOGÍA

• Cortafuegos que actúan a nivel de paquetes de datos: Trabaja a través de red de la pila de protocolos OSI, y para determinar que paquetes debe dejar pasar, mira IP's tanto de origen como de destino y los puertos.

• **Cortafuegos que actúan a nivel de circuitos**: Actúan a nivel de sesión, y aparte de mirar las IP's y los puertos, también mira la información de la sesión y los números de secuencia de los paquetes enviados.

• **Cortafuegos que actúan como pasarelas de aplicación: Actúan** en el nivel de aplicación de OSI, analizan todos los paquetes de datos de un determinado servicio. Consumen muchos recursos y necesitan un software específico.

• **Cortafuegos transparentes:** Actúan a nivel de enlace, determinando que paquetes pasan en función del resultado de evaluar una serie de reglas. Son indetectables porque no usan una dirección IP.

ARQUITECTURA DE CORTAFUEGOS

Las principales arquitecturas de cortafuegos son:Computador Múlti-puerto (ó "multi-homed host"):Se trata de un computador que tiene más de un interface de red, cada interface se **conecta asegmentos de red física y lógicamente separados. Un computador de doble puerto** (un computador con dos interfaces) es el ejemplo más común de computador multi-puerto. Uncortafuegos de doble puerto es un cortafuegos con dos tarjetas de red (ó NICs, NetworkInterface Cards), cada interface conectado a una red diferente. El encaminamiento del cortafuegos seinhabilitará para un cortafuegos de doble puerto para que los paquetes IP de una red no se encaminen directamente de una red a la otra

Computador Pantalla (ó "screened host"):

Un cortafuegos con esta arquitectura utiliza un computador denominado "bastión" para que todos los computadores de fuera se conecten, en vez de permitir conexión directa a otros computadores internos menos seguros. Para realizar esto, un router de filtrado de paquetes se configura para que todas las conexiones a la red interna desde la red externa se dirijan hacia el computador "bastión". Si se debe utilizar un cortafuegos de filtrado de paquetes, entonces un computador "bastión" debería establecerse para que todas las conexiones desde la red externa vayan a través del computador "bastión" para impedir que la conexión Internet directa entre la red de la organización y el mundo exterior.

Subred Pantalla (ó "screened subnet"):

Esta arquitectura es esencialmente similar a la arquitectura del "computador pantalla", pero añade una capa extra de seguridad creando una red en la que reside el computador "bastión"(denominada "red perimetral") que se encuentra separada de la red interna. Una "subred pantalla" se crea añadiendo una red perimetral que separe la red interna de la externa. Estoasegura que si existe un ataque con éxito en el computador bastión, el atacante está restringido a la red perimetral por el "router pantalla" que se conecta entre la red interna y la red perimetral.

PRUEBAS DE FUNCIONAMIENTO

Un Firewall funciona, en principio, denegando cualquier tráfico que se produzca cerrando todos los puertos de nuestro PC. En el momento que un determinado servicio o programa intente acceder al ordenador nos lo hará saber. Podremos en ese momento aceptar o denegar dicho tráfico, pudiendo asimismo hacer (para no tener que repetir la operación cada vez) "permanente" la respuesta hasta que no cambiemos nuestra política de aceptación.

También puedes optar por configurar el Firewall de manera que reciba sin problemas cierto tipo de datos (FTP, chat o correo, por ejemplo) y que filtre el resto de posibilidades. Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet.

Windows XP cuenta con un Firewall, aunque muy sencillo. Sólo te permite filtrar la información que entra en tu ordenador, no la que sale.

De esta forma, no te servirá de nada si tienes instalado un programa Adware que recoge datos de tu equipo y se conecta al exterior para enviarlos. Conviene que te instales un Firewall más completo y que te permita configurar políticas de seguridad.

2.Cortafuegos software

y hardware

Cortafuegos software integrados en los sistemas Operativos. El Sistema Operativo

El Sistema Operativo que usamos, la mayoría Windows, no solo es la forma grafica con la que vemos el escritorio.

El Sistema operativo es el primer guardian de las operaciones que producen en el nucleo del procesador. Por este motivo, es importante mantenerlo siempre actualizado y evitar añadirle parches y agregados que no pertenezcan al origen del mismo.

Lo mejor es dejar activadas las actualizaciones automáticas e instalarlas cuando el sistema lo pida, siempre reiniciando si asi se requiere.Dentro del sistema operativo viene integrado un Firewall o Cortafuegos.

El Firewall

El Firewall (Cortafuegos), es el centinela de todos los procesos que se ejecutan en el ordenador, y de todas las solicitudes de

coneccion hacia y desde el exterior que hacen los programas. Su Sistema Operativo, si es Windows, traeráun Firewall integrado. Si no es un usuario avanzado, debería dejar la configuracion del mismo en automático, para que sus cortafuegos decida por usted.

Pero el Firewall solo es capaz de dar y quitar permisos a los programas, pero no puede diferenciar entre un programa bueno y uno malo. Para eso estan los Antivirus.

- Cortafuegos software libres y propietarios.

El Software Libre y la seguridad informática

¿Qué es el Software Libre?

Para entender la situación de este tipo de software con respecto a su uso en seguridad informática es imprescindible describir, en primer lugar, a qué se refiere este documento cuando hace referencia a "software libre".

El concepto de software libre es, en primera instancia, fácil de presentar, aún no existiendo una única descripción reconocida por todos de lo que es realmente este tipo de software. En general se entiende como software libre aquel programa o conjunto de ellos de los que el usuario puede disponer del código fuente, sin restricciones, y el cual puede modificar y redistribuir también sin restricciones. Estas libertades garantizadas al usuario del software (o a aquel que lo recibe) no son contrarias a los derechos legítimos del autor del programa, es decir, éste no tiene por qué perder sus derechos sobre el mismo. No se incluye, por tanto, en esta definición software en el "domino público" (aquél para en el que el autor ha cedido todos sus derechos).

Una descripción más completa de lo que podría considerarse software libre, es la dada por las directrices de software Libre de Debian, que constituyen la base de la definición de Open Source (Open Source Definition, www.opensource.org), aunque existen entre ellas ciertas diferencias. Entre las licencias más utilizadas para este tipo de software cabe destacar la licencia GNU GPL y la licencia BSD.

Ventajas del Software Libre en el mundo de la seguridad

Si se analiza la descripción realizada previamente de la definición de software libre se

derivan una serie de ventajas principales de este tipo de software sobre el software propietario, algunas de las cuales son muy adecuadas para el mundo de la seguridad. A saber:

-Al disponer del código fuente de los programas en su totalidad, éste puede ser analizado por terceras personas ajenas a sus autores en busca de fallos de diseño o de implementación. Es decir, cualquiera con los conocimientos necesarios puede realizar una auditoría del código del program.

-La posibilidad de realizar modificaciones libremente al código fuente y distribuirlas permite que cualquiera pueda ofrecer mejoras sobre éste. Estas mejoras podrán ser nuevas funcionalidades que se incorporen al mismo o parches que corrijan problemas detectados anteriormente.

-Las características del software libre hacen que no sea lógico cargar costes sobre el software en sí (dado que se ha de distribuir sin cargo), lo que permiteque este tipo de software pueda ser utilizado por organizaciones y personas con menos recursos económicos. Esto se presenta como una ventaja cuando se compara con los precios de lo que cuesta el software de

seguridad propietario hoy en día (licencias de cortafuegos, vpns, sistemas de detección de intrusos, etc.). El software libre pone en manos de cualquiera el tipo de tecnología que,

hoy por hoy, sólo podían tener grandes corporaciones.

-De igual forma, la posibilidad de modificar libremente el software permite a las organizaciones que lo adapten a sus propias necesidades, pudiendo eliminar funcionalidades que no le sean de interés. En el mundo de la seguridad existe la

máxima de "lo más sencillo es más seguro" por ello poder eliminar funciones innecesarias de las herramientas las puede convertir de forma inmediata en más seguras (porque no podrán ser utilizadas estas funcionalidades para subvertirlas).

Frente al análisis de fallos que puede sobrevenir en la realización del software (presentado anteriormente), el software libre protege a sus usuarios con una serie de mecanismos determinados. Entre estos:

La posibilidad de una auditoría de código en las herramientas software reduce los riesgos de seguridad debido a la aparición de fallos desconocidos, a la introducción de funcionalidades no deseadas en el código o la incorrecta implementación de algoritmos públicos. Aunque no se pueda asegurar que el código esté carente de errores, si es posible garantizar que tantas posibilidades tiene de encontrar un fallo de programación en éste (que lleve implícito un riesgo de seguridad) un atacante externo como la organización lo utilice. Si bien no se puede asegurar que los mejores cerebros del mundo realicen la auditoría de código del software que una compañía utiliza, dicha compañía si tiene la posibilidad, en función de sus necesidades respecto a la seguridad, de realizar

ella misma dicha auditoría de código o pagar a alguien para que la realice.

La posibilidad de corregir los programas y distribuir dichas correcciones permite que los programas evolucionen de una forma más abierta. En el mundo de la seguridad, un fallo en el sistema significa exponer a éste a una "ventana de vulnerabilidad" que tiene lugar desde la detección del fallo (por parte de sus usuarios legítimos o de terceras partes, hostiles incluso) a la aplicación de la medida correctiva, que pueda ser la instalación del parche adecuado que arregle el problema, pasando por la generación de dicho parche. El hecho deque la generación de dicho parche pueda realizarse por un número de personas (confiables) elevado, y no por un sólo fabricante, debe, en teoría, reducir este tiempo de exposición a dicha vulnerabilidad.

Desventajas del software propietario

En primer lugar, es necesario aclarar que en este documento se entenderá como software propietario aquél que se distribuye en forma de binarios, sin código fuente, por parte de una compañía que licencia dicho software para un uso concreto, con un coste determinado. No se van a realizar comparativas con la nebulosa intermedia de distintos tipos de software cuyas licencias se sitúan entre ambos extremos, por ejemplo: software que se distribuye el código

fuente pero no se puede modificar, software que se distribuye con limitaciones para su uso comercial, etc.

Con respecto a la seguridad, las mismas garantías que ofrece el software libre en el mundo de la seguridad son problemas que se le pueden achacar al software propietario. Se puede hablar de las siguientes desventajas del software propietario para el usuario final:

-Posibilidad de que existan funcionalidades no deseadas en dicho software.

-Dependiendo de la programación realizada, algunas funcionalidades podrán ser activadas o desactivadas por el usuario, pero pueden existir también funcionalidades que no se puedan desactivar o que, incluso, no se encuentren

documentadas. Llevándolo al extremo se podría hablar de "puertas traseras" abiertas por el fabricante del software que, después de todo, es un agente comercial y, por tanto, tiene sus propios intereses que pueden ser contrarios a los de la compañía que instala un software de seguridad específico.

- Desconocimiento del código por parte del usuario. Esto puede llevar a que el fabricante pueda llegar a tener una falsa sensación de seguridad por oscuridad, es decir, las vulnerabilidades de su producto no tienen por qué ser conocidas porque nadie tiene acceso a las "tripas" del mismo. De igual forma, esto puede llevar a que el fabricante no tenga interés en desarrollar el código de una forma adecuada porque, al fin y al cabo, el usuario no va a ver dicho código ni evaluar la calidad de su implementación.

-Necesidad de confiar totalmente en el fabricante. Esto es así por cuanto éste ha Implementado los algoritmos de seguridad y el usuario no puede garantizar por sí mismo que su implementación ha sido correcta y que, por ejemplo, las propiedades matemáticas necesarias para que estos algoritmos funcionen correctamente se cumplan en todas las condiciones.

-Dependencia de una tercera entidad, ya que es el fabricante del producto el único que puede ofrecer nuevas versiones de éste en caso de fallo o incluir nuevas funcionalidades que puedan ser necesarias. Esto es una desventaja debido a que el usuario no puede transferir esta dependencia a otra entidad, en caso de que el fabricante original haya traicionado su confianza (demasiados errores en la implementación, demasiado tiempo en la generación de parches

para arreglar problemas graves, etc..)

Cabe hacer notar que, algunos fabricantes de software, observando las ventajas del modelo Open Source ofrecen, con restricciones o sin ellas, copias del código fuente a terceras entidades interesadas. Tal es el caso, por ejemplo, de fabricantes de sistemas operativos como Sun Microsystems y Microsoft y de fabricantes de productos de seguridad como PGP (hasta febrero de 2001 con su suite de aplicaciones basadas en cifrado asimétrico) y NAI (con su cortafuegos Gauntlet).

Desventajas del software libre

Sin embargo, el uso de software libre no está exento de desventajas. Así se podrían enumerar las siguientes:

-la posibilidad de una generación más fácil de troyanos, dado que el código fuente también puede ser modificado con intenciones maliciosas. Si el troyano logra confundirse con la versión original puede haber problemas graves. La fuente del programa, en realidad, será el método de distribución de software, que, de no ser seguro, permitirá que un tercer agente lo manipule. La distribución de software se asegura añadiendo posibilidad de firmado de hashes de la información distribuida

-el método de generación de software libre suele seguir, en la mayoría de los casos, el modelo bazar, es decir, muchas personas trabajan sobre partes concretas e integrando sus cambios o personas desde el exterior contribuyen mejoras al proyecto global. Esto puede dar lugar a que se realice una mala gestión del código fuente del software por no seguir métodos formales de seguimiento, la consecuencia final es que falten piezas clave (que nadie ha contribuido) como es el caso de la documentación.

-Al no tener un respaldo directo, la evolución futura de los componentes software no está asegurada o se hace demasiado despacio.

En mayor o menor medida, algunas de estas desventajas están comenzado a soluciones. El caso la difusión de troyanos se limita mediante el uso de técnicas de firma digital para garantizar la inviolabilidad del código o binarios transmitidos. Es frecuente que algunos autores de software libre al distribuir el código indique también información (sumas MD5 firmadas) que permitan garantizar la integridad del código descargado.

-Distribuciones libres para implementar cortafuegos en máquinas dedicadas.

Existen equipos diseñados específicamente para trabajar como cortafuegos. La ventaja fundamental de estos aparatos es que todos sus componentes han sido diseñados con los mismos requisitos de seguridad, al contrario de lo que ocurre con otras soluciones.

Algunos cortafuegos dedicados (o "cajas negras") disponen de circuitos que realizan algunas funciones que de otra forma se harían por software, acelerando enormemente las prestaciones. El cifrado en las redes privadas virtuales es lo que más se beneficia de esto; un router solamente puede hacerlo a velocidades moderadas, mientras algunos

cortafuegos dedicados son capes de cifrar un flujo de datos a velocidades de hasta 100

Mbps.

En Linux:

-ClearOS: La distro que combina facilidad de uso con funcionalidad.

-IPCop: Distribución versátil y rápida. Altamente configurable.

-eBox Platform: Algo más que un simple software cortafuegos .

-Monowall: La más liviana de las propuestas de la entrada.

-PfSense: Si desea un servidor de seguridad integral y nada más, no busques

más.

-Smoothwall Express: Probablemente la distribución firewall con la mayor

reputación.

-Smoothwall Advanced: Y su versión de pago, con asistencia técnica y más

opciones.

La ventaja fundamental de algunos de ellos, de cualquier manera, es la sencillez de configuración. Muchos problemas de seguridad se deben a errores provocados por equipos complicados o tediosos de configurar. Cuanto más sencillo resulte, más improbable es cometer errores.

Algunos modelos recientes, además, pueden incorporar un antivirus dentro de la misma unidad, ofreciendo una primera l'nea de defensa cuyo funcionamiento no se ve afectada por los propios virus; algunos de ellos desactivan el software antivirus de los equipos afectados.

- Cortafuegos hardware. Gestión Unificada de Amenazas

"Firewall UTM" (Unified Threat Management).

Listado de firewalls hardware o cortafuegos hardware

-AlphaShield

o AlphaShield Home Edition

o AlphaShield Professional Edition

o Clavister

o Clavister Security Gateway 50 series

o Clavister Security Gateway 3100 series

o Clavister Security Gateway 4200 series

o Clavister Security Gateway 4400 series

Las organizaciones de todos los tamaños están encarando retos relacionados a la seguridad de la información. Las regulaciones gubernamentales, el alto costo de la pérdida de imagen pública cuando se da un ataque, y la creciente complejidad de los nuevos ciber-ataques, son sólo algunos de estos retos.

Las organizaciones actuales confían en entornos informáticos seguros y de alta disponibilidad para realizar para desarrollar sus negocios. Los firewalls y los UTM

(Unified Threat Management) son componentes claves de una red segura y deben ser gestionados adecuadamente para asegurarse de que protegen sus activos de información crítica.

Los firewalls y UTMs deben ser configurados para permitir el tráfico "bueno" y para mantener el tráfico "malo" afuera. Los firewalls y UTMs deben ser actualizadas continuamente para apoyar a los requerimientos empresariales cambiantes, tales como:

-Nueva VPN de usuarios

-Cambios en la condición de empleado

-Nuevos socios

-Nuevas aplicaciones

La administración de Firewalls y UTMs es intensiva en recursos y requiere un alto nivel de conocimientos. Debido a la complejidad asociada a estas tareas, la mayoría de las violaciones son causadas por la incorrecta configuración de reglas y políticas de firewall. Ximark UTM/Firewall Administrado es un servicio de administración de dispositivos de seguridad de perímetro, conocidos también como “Administradores de Amenazas

Unificadas” que protegen a las organizaciones con herramientas integrales como: antispam, anti-virus, sistema de prevención de intrusos (IPS), filtro de contenido web, control de “peer-to-peer” (P2P) y control de chat, entre otros.

El registro de eventos, la administración de la configuración y los reportes centralizados son fundamentales de acuerdo a las mejores prácticas de seguridad modernas. Con Ximark UTM/Firewall Administrado las organizaciones pequeñas y medianas pueden cumplir con estas prácticas. Con nuestro modelo de seguridad “OnDemand” las empresas de todos los tamaños pueden beneficiarse de una solución centralizada de administración y monitoreo de sus dispositivos de seguridad perimetral de varios fabricantes líderes. No hay requerimientos adicionales de hardware, software o facilidades, lo cual provee un costo competitivo.

Funcionalidades del Servicio

-Monitoreo

-Administración de registros (logs). Revise registros en tiempo real o

históricamente. Para diagnóstico o análisis de seguridad.

-Monitoreo de la disponibilidad del dispositivo. Sea notificado cuando el

dispositivo presenta problemas de desempeño o conectividad.

-Reportes

-Servicio “On-demand”. Acceda al servicio desde cualquier ubicación vía

Internet vía un browser.

-Reportes pre-configurados. Vea reportes de actividades como los hosts más activos, servicios más usados, sitios más visitados y otra información útil para diagnóstico y control.

-Administración

-Administración de la configuración. La ejecución de cambios programados se incluyen dentro Ximark UTM/Firewall Administrado.

-Mantenimiento. Las tareas de mantenimiento como actualización de firmware y otras.

-Actualización de servicios de protección. Los servicios de protección UTM como anti-spam, anti-virus, IPS y filtrado de contenido web se actualizan.

-Mesa de Servicio

-Mesa de servicio vía Web. Puede abrir casos 24x7x365 días al año vía web y por teléfono. Como un sólo punto de contacto para todas sus necesidades de soporte, nuestros ingenieros que atienden vía nuestra plataforma web, tienen experiencia en soportar redes y ayudar a diagnosticar problemas y proveer soluciones. La mesa de servicio permite que Ximark responda tan rápido como sea posible o de acuerdo a los acuerdos de niveles de servicio (SLA) establecidos con el cliente.

Para ellos es posible manejar escalamientos y alertas a los gerentes del área de soporte. La mesa de servicio es basado en Web y en tecnologías de última generación. El sistema posee una base de datos conocimiento, calendario, manejo de SLAs, y otras funcionalidades que permiten brindar un servicio de soporte avanzado.

-Niveles de Servicio

-Ximark UTM/Firewall Administrado ofrece niveles de acuerdo de servicio (SLA) para garantizar la disponibilidad y confiabilidad.

Funcionalidades de Dispositivos UTM

Ximark UTM/Firewall Administrado ofrece la administración y el monitoreo de dispositivos UTM de fábricas líderes de la industria. Estas plataformas proveen funcionalidades de protección unificada contra las principales amenazas que encaran los negocios hoy día. Las características de seguridad son comunes a los fabricantes que Ximark UTM/Firewall Administrado soporta son enunciados a continuación.

-Firewall. Es posible con controlar y bloquear el tráfico de entrada y salida a la red interna o a la zona desmilitarizada (DMZ). El tráfico a controlar se puede definir por servicio (SMTP, HTTP, etc.) y por horarios.

-Red Privada Virtual (VPN). Una VPN es un túnel seguro que se crea entre dos o más UTMs o entre usuarios que se mueven fuera de la empresa. Esta capacidad viene incluida dentro de las funcionalidades del UTM.

 Filtrado de contenido web. Se controla el acceso a sitios que puedan con contenido no deseado como sitios que contengan pornografía o contenido malicioso. Estos sitios se controlan por categorías que definen grupos de sitios según su contenido. Asimismo se establecen acceso a sitios personalizados, en caso de que no hayan sido clasificados en las categorías.

-Prevención contra intrusos (IPS). El IPS provee la capacidad de bloquear ataques contra vulnerabilidades conocidas de aplicaciones, sistemas operativos y hardware.

-Anti-Virus y AntiSpyware. Protección anti-virus que inspecciona el tráfico que entra y sale de la red de los protocolos más comunes como SMTP, POP3, HTTP,

FTP y otros.

-Anti-Spam. Distingue comunicaciones por correo electrónico legítimas de

aquellas que son spam, bloqueando este último en tiempo real.

Beneficios Claves

-Con Ximark UTM/Firewall Administrado los clientes obtienes los siguientes beneficios:

-Minimiza el riesgo del impacto que podrían tener las violaciones de seguridad.-Les permite cumplir con regulaciones y certificaciones de la industria.

-Reduce la sobre-carga de administración logrando un mejor uso del recurso humano interno.

-Provee administración consolidada y “todo-en-uno” de la seguridad de la red.