Unidad 5

El proxy

Seguridad y alta disponibilidad

5

Índice

Introducción

Un proxy es un programa que actúa como intermediario en la comunicación entre un cliente y un servidor, que pueden o no tener la capacidad de comunicarse directamente. El proxy funciona a nivel de aplicación, a diferencia de los cortafuegos, que operan a nivel de red y transporte.

Un proxy de reenvío, también conocido como forward proxy, se encuentra en la red de origen y actúa como intermediario para los clientes de dicha red. Por otro lado, el proxy inverso, o reverse proxy, reside en la red de destino y hace de intermediario para el servidor o servidores de nuestra red de destino.

El proxy anónimo oculta la dirección IP del cliente del servidor de destino, haciendo que el servidor crea que se encuentra en comunicación directa con el proxy. Este tipo de proxy es utilizado frecuentemente para evadir restricciones y censura entre países.

Un proxy puede ser usado para proteger la privacidad del usuario o para mantener un perfil social separado de su vida privada, en línea con el Reglamento General de Protección de Datos (RGPD).

Los clientes deben configurarse para enviar sus solicitudes a través de un proxy, lo cual puede almacenarse en un archivo PAC (Proxy Auto-Config) para la configuración automática del cliente. Cuando se crea una configuración en el cliente para que el tráfico saliente sea redirigido automáticamente al proxy, se denomina proxy transparente.

Los proxies inversos pueden utilizarse para acelerar la carga de páginas web (proxy caché) o para equilibrar la carga de trabajo entre dos o más servidores. En este caso, el proxy se denomina frontend, mientras que los servidores en la parte posterior se llaman backends.

Al finalizar esta unidad

- Comprenderemos la importancia de los cortafuegos como medida fundamental de seguridad.
- Examinaremos los componentes y el funcionamiento de los cortafuegos en Linux.
- Estudiaremos la base de numerosas reglas de los cortafuegos.
- Analizaremos las diferencias entre el funcionamiento de los cortafuegos en Linux y Windows.
- Aprenderemos a diferenciar las características de los cortafuegos genéricos y los cortafuegos de aplicaciones web.

5.1. Introducción

Un proxy actúa como un servidor intermediario entre su computadora (cliente) y la página de destino que desea visitar. El proxy es responsable de recibir sus solicitudes de acceso y dirigirlas a la página de destino, permitiéndole acceder a ella sin revelar que lo está haciendo.

Dado que la conexión no es directa, su dirección IP no se registra en el destino; en su lugar, se registra la dirección IP del proxy a través del cual estableció la conexión. Este tipo de servicios a menudo se utilizan para ocultar el país de origen de su conexión, lo que puede ser útil para acceder a servicios bloqueados por geolocalización, siendo una alternativa a las VPN.

5.1.1. Proxy directo y proxy inverso

- **Proxy directo** (forward proxy): Un forward proxy es un proxy configurado para gestionar solicitudes de un grupo de clientes bajo el control de un administrador local, hacia un grupo desconocido o aleatorio de recursos fuera de su control. La palabra "forward" generalmente se omite y se menciona solo como un proxy. Un buen ejemplo es un dispositivo proxy web que acepta solicitudes de tráfico web de clientes en la red local y las reenvía a servidores en Internet. El propósito de un proxy de reenvío es administrar el tráfico desde el sistema de un cliente hacia el exterior.
- **Proxy inverso** (reverse proxy): Un reverse proxy se coloca frente a otro servidor que va a suplantar sin el conocimiento del cliente. Un cliente es cualquier hardware o software que puede enviar solicitudes a un servidor. El proxy inverso transmite todas las solicitudes de los clientes a los servidores y también entrega todas las respuestas y servicios procedentes de los servidores de vuelta a los clientes. Desde el punto de vista del cliente, parece que todo procede del mismo lugar.

IMPORTANTE

Es esencial comprender las diferencias entre un proxy directo (forward proxy) y un proxy inverso (reverse proxy), así como las implicaciones de seguridad asociadas con cada uno.

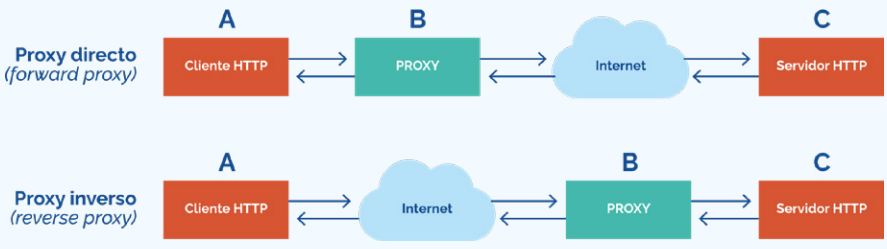

Imagen 1. Diferencias entre proxy directo e inverso

De manera general, podemos decir que los objetivos principales de un proxy directo son los siguientes:

- Controlar el acceso a recursos externos, permitiendo el acceso a algunos y denegando a otros.
- Optimizar el acceso a Internet, distribuyendo de manera equilibrada el tráfico entre todos los clientes locales.
- Registrar las actividades realizadas por los clientes para prevenir posibles acciones futuras no deseadas.
- Proteger a los clientes mediante el uso de protocolos actualizados y seguros.

En el caso de los proxies inversos, que se utilizan principalmente para acceder a diferentes servidores en la misma red, se pueden lograr los siguientes objetivos:

1. **Seguridad:** el proxy actúa como una capa de seguridad adicional frente a los servidores protegidos.
2. **Cifrado:** la comunicación entre el cliente y el proxy está cifrada, mientras que la comunicación interna no necesariamente requiere esa capa de seguridad.
3. **Aceleración:** al igual que en los proxies directos, los proxies inversos pueden almacenar en caché contenido estático para agilizar su entrega.
4. **Balanceo de carga:** se puede distribuir equitativamente el trabajo entre diferentes servidores, logrando así un mejor rendimiento.

IMPORTANTE

Comprender las diferencias en los objetivos y aplicaciones de los proxies directos e inversos es fundamental para su correcta implementación y uso en entornos de red.

5.1.2. El proxy anónimo

Los proxies anónimos son servidores que brindan anonimato al usuario. Sin embargo, no todos los proxies anónimos son intencionalmente anónimos. Algunas razones por las cuales podemos comunicarnos usando un proxy anónimo son las siguientes:

Configuración incorrecta del servidor proxy

Si no se limitan las fuentes correctamente al configurar un servidor proxy, cualquier persona podría utilizarlo como un proxy anónimo. Esto puede ocurrir debido a errores de configuración y no a la intención del administrador del servidor.

Intencionalmente puesto a disposición de cualquier persona

Algunos servidores proxy son lanzados deliberadamente para que todos los usen. Sin embargo, esto puede conllevar riesgos legales y de seguridad, como la posibilidad de ser arrestado o de escuchas electrónicas en las conexiones.

Algunos servidores proxy son lanzados deliberadamente para que todos los usen. Sin embargo, esto puede conllevar riesgos legales y de seguridad, como la posibilidad de ser arrestado o de escuchas electrónicas en las conexiones.

5.1.3. Conflicto con la privacidad de los usuarios

El análisis y registro de las comunicaciones de los usuarios realizado por un proxy pueden entrar en conflicto con la privacidad del usuario bajo el Reglamento General de Protección de Datos (RGPD). Aunque no se requiere ninguna ley para entender esto, el análisis de las comunicaciones puede utilizarse para investigar la privacidad del usuario o para construir perfiles sociales.

Por lo tanto, el uso de un proxy como medida de control o de seguridad solo debe aplicarse si es la mejor manera de lograr lo que se requiere y siempre después de que el usuario haya sido debidamente informado de la existencia de este programa y de sus consecuencias.

IMPORTANTE

Al utilizar proxies, es fundamental considerar los aspectos relacionados con la privacidad y la seguridad, así como cumplir con las regulaciones aplicables, como el RGPD.

5.2. Configuración del cliente

Aunque se pueden obtener beneficios adicionales, como la aceleración de caché, el propósito del proxy de reenvío desde una perspectiva de seguridad informática es controlar las solicitudes del usuario. La implementación de políticas de privacidad podría incluir las siguientes acciones:

- Evitar el acceso a sitios web peligrosos.
- Evitar el acceso a webmails diferentes al corporativo.
- Evitar el acceso a servidores con una IP contenida en una lista negra.
- Limitar el acceso a determinadas páginas web según el usuario.
- Limitar el acceso a determinadas páginas web según el momento del día.
- Limitar el acceso a determinadas páginas web en función del usuario y del momento del día.

Es fundamental que el cliente se configure de manera específica para realizar las conexiones a través del proxy. Esta configuración se realizará en el sistema operativo, de modo que todas las aplicaciones puedan establecer comunicación a través del proxy y obtener la configuración automática.

Mozilla Firefox es un ejemplo de una aplicación que tiene su propio sistema de configuración de proxy. Por lo tanto, se puede configurar el navegador de manera diferente a las demás aplicaciones instaladas en el sistema.

IMPORTANTE

Asegurarse de que el cliente esté correctamente configurado para trabajar con el proxy es esencial para garantizar que las políticas de seguridad y privacidad se apliquen de manera efectiva.

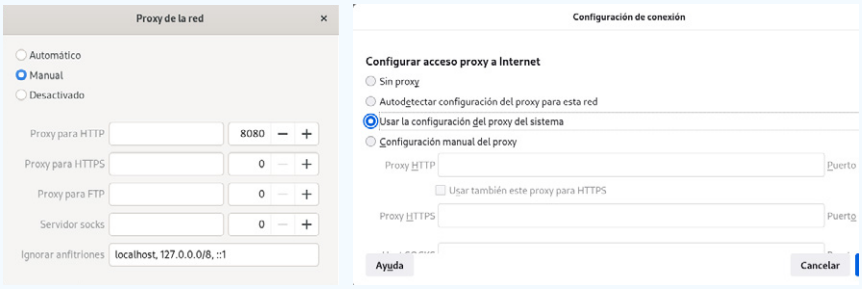

Imagen 2. Configuración del proxy en el sistema operativo y configuración del proxy en un navegador Firefox

5.2.1. Configuración manual

Como podemos observar, para habilitar las conexiones a través de un proxy, es fundamental especificar la dirección IP del servidor y el puerto utilizado. Es posible utilizar distintos servidores de proxy para cada uno de los protocolos aplicados o bien usar los mismos servidores para todos ellos.

SOCKS es un protocolo de Internet que permite que las aplicaciones cliente-servidor utilicen de forma transparente los servicios de firewall de la red. SOCKS significa "SOCKeTS".

Alternativamente, los clientes de firewall que necesitan acceso a servidores externos pueden conectarse a un servidor proxy SOCKS. Este servidor proxy controla qué clientes pueden acceder al servidor externo y enviar solicitudes al servidor. SOCKS también se puede usar a la inversa, lo que permite que los clientes fuera del firewall ("clientes externos") se comuniquen con los servidores dentro del firewall.

5.2.2. Configuración automática

Hay varios métodos disponibles para configurar Windows para usar un servidor proxy para conectarse a Internet. El método que sea mejor para su equipo depende del tipo de aplicación que esté utilizando.

Debe usar WPAD (Web Proxy Auto-Discovery Protocol) para configurar Windows para usar un servidor proxy de Internet. La configuración se realiza a través de DNS o DHCP. No requiere ninguna configuración en la estación de trabajo del cliente. Los usuarios pueden traer computadoras y dispositivos desde su hogar u otros lugares y detectar automáticamente la configuración del servidor proxy de Internet.

Con el protocolo WPAD, se deben seguir los siguientes pasos:

- Si se conoce la ubicación del archivo PAC de una ejecución previa, se utilizará el mismo archivo.
- Se consultará el servidor DHCP, que puede proporcionar una respuesta con la URL para completar el archivo PAC:
- Se consultará el servidor DNS para determinar qué equipo se denomina "wpad". Si existe, se intentará solicitar al equipo el archivo "wpad.dat", cuyo nombre de archivo debe ser PROXY.PAC.
- En Windows, si se produce un error en todo lo mencionado anteriormente, se desarrollarán otras estrategias similares a DNS, denominadas LLMNR (Link-Local Multicast Name Resolution) o NBT-NS (NetBIOS Name Service).

Un archivo PAC (Proxy Auto-Config) es un archivo de configuración utilizado por los navegadores web para determinar automáticamente la configuración del proxy apropiada para acceder a un sitio web o recurso en Internet. Estos archivos contienen un script, generalmente escrito en JavaScript, que especifica las reglas para seleccionar un servidor proxy específico en función de la URL solicitada, permitiendo así a los navegadores gestionar de manera eficiente y automática la navegación a través de redes con servidores proxy.

5.2.3. Proxy transparente

Los servidores proxy transparentes mejoran la calidad de la navegación por Internet, proporcionando contenido con mayor ancho de banda y reduciendo la latencia de transmisión. Sin un proxy, los usuarios accederían a Internet de manera menos eficiente, experimentando conexiones más lentas o interrupciones en función de la ubicación geográfica del dispositivo.

En otras palabras, si alguien ya ha descargado un archivo o visitado un sitio web que deseamos ver, la infraestructura del proxy transparente entregará ese contenido mucho más rápido que si tuviéramos que volver a conectarnos y obtener el archivo desde su ubicación original.

La diferencia entre un proxy normal y un proxy transparente radica principalmente en su configuración. Aunque ambos tipos de proxy pueden desempeñar roles similares y, en muchos casos, ser la misma máquina, no es necesario configurar la red para capturar el tráfico HTTP con un proxy transparente. Como parte de la arquitectura de la red, todo el tráfico dirigido al puerto 80 (o cualquier otro puerto configurado para HTTP) debe pasar automáticamente por este proxy transparente. De esta manera, los usuarios no necesitan realizar ajustes manuales en sus dispositivos para beneficiarse de las ventajas que ofrece un proxy transparente.

5.3. Un proxy para Windows: WinGate

WinGate es un servidor proxy que permite compartir una única conexión a Internet en tu hogar con todos los ordenadores conectados a la misma red. Esta herramienta permite gestionar y controlar la red de forma más segura, ya que puede analizar virus o denegar el acceso a determinadas páginas. Además, controla el ancho de banda consumido o bloqueado por accesos externos, no solo de nuestro ordenador, sino de todos los dispositivos conectados al software.

La herramienta cuenta con protocolos seguros que permiten conectarse de forma remota como si estuvieras conectado directamente a un router en casa u oficina. Esta es la mejor manera de proteger tu red de terceros. Para activar WinGate, solo tendrás que configurar un nombre y una contraseña para que cualquiera pueda acceder a ellos siempre que lo haga con las credenciales correctas.

5.3.1. Configuración inicial

IMPORTANTE

Lo primero que debes hacer es definir la(s) interfaz(es) de red interna y qué interfaz(es) de red se utilizarán para la conexión externa. El proxy funcionará con conexiones abiertas desde la interfaz interna hacia el exterior. Esto se realiza en Panel de control > Conexión en red.

A continuación, debemos activar los servicios que WinGate ofrecerá en Panel de control > Servicios.

Por defecto, algunos servicios están disponibles y son necesarios para el funcionamiento normal de WinGate, como el Servicio de entrega SMTP, que la aplicación utiliza para enviar alertas a la administración. Aunque se puede detener y desinstalar, el WWW Proxy Server viene instalado previamente y se inicia, lógicamente, por defecto. Es importante entrar en sus propiedades para ajustar su comportamiento.

Para que WinGate actúe como servidor de SOCKS, proxy FTP/POP3/SMTP, etc., será fundamental instalar los nuevos servicios y configurarlos correctamente. WinGate busca ser una solución completa para empresas, pudiendo funcionar también como servidor de DNS y DHCP en la red interna del servicio.

Ejemplo

Imagina que deseas limitar el acceso a ciertas páginas web para mejorar la productividad de los empleados. Con WinGate, podrás establecer reglas específicas que bloqueen el acceso a sitios como redes sociales o plataformas de video durante las horas de trabajo. De este modo, se garantiza un entorno laboral más enfocado y seguro.

5.3.2. Reglas de acceso

Para finalizar, debemos establecer las reglas de acceso al proxy. WinGate utiliza un sistema para organizar los dominios en grupos, permitiendo así una estructuración adecuada en distintas categorías.

Es necesario definir dos tipos de reglas: por un lado, las que asignan un dominio a una determinada categoría y, por otro lado, las que aceptan o rechazan ciertas conexiones en función de las categorías. Podemos editar y modificar las categorías disponibles, así como organizarlas de manera jerárquica.

Para configurar las primeras reglas, debemos ir a Web Access Control > Classifiers > Manual Classifier.

Para configurar las segundas reglas, debemos ir a Web Access Control > Access Rules, donde podremos especificar la acción de la regla.

Ejemplo

Imagina que quieres permitir el acceso a sitios web educativos y de investigación, pero restringir el acceso a plataformas de entretenimiento y redes sociales durante las horas de trabajo. Primero, crea categorías como "Educación", "Investigación", "Entretenimiento" y "Redes sociales". Luego, asigna los dominios correspondientes a cada categoría utilizando los Classifiers. Finalmente, establece reglas de acceso que permitan la conexión a las categorías "Educación" e "Investigación", mientras bloqueas el acceso a "Entretenimiento" y "Redes sociales". De esta manera, podrás mantener un ambiente de trabajo productivo y enfocado.

5.3.3. Reglas de cortafuegos

Dentro del Control Panel > Extended Networking, podemos habilitar o deshabilitar una función específica del cortafuegos de WinGate, que generalmente estará siempre activada.

Las reglas que se incluyen por defecto permiten la apertura de los puertos necesarios para que funcione correctamente, como TCP 80 para proxy HTTP transparente, TCP 8080 para proxy HTTP normal, entre otros. Las reglas se pueden gestionar en función del origen de la conexión o en función del destino de la misma. Podremos aceptar, rechazar o redirigir los paquetes a un puerto o a una dirección IP específica.

Es fundamental prestar atención a la acción predeterminada, la cual determina si acepta o rechaza las conexiones que no tienen una regla establecida correspondiente a las políticas en iptables.

IMPORTANTE

Al configurar las reglas del cortafuegos, asegúrese de que no bloquee el tráfico necesario para el correcto funcionamiento de WinGate y las aplicaciones en su red.

Siempre revise y ajuste las reglas del cortafuegos según las necesidades de su red y la política de seguridad de su organización.

5.4. Un proxy para Linux: Squid

De manera predeterminada, Squid actuará como un proxy transparente y un proxy de almacenamiento en caché, lo que nos permite administrar el acceso de los clientes y crear ACL (listas de control de acceso) para hosts, grupos y redes. Con Squid, podemos permitir o denegar la navegación y también bloquear el acceso a ciertos sitios web específicamente.

Los servidores proxy transparentes, como Squid, también pueden actuar como filtros de contenido, ya que son un servidor intermediario (proxy). Filtraremos este contenido a través de los diversos comandos que utiliza Squid.

Squid es un proxy HTTP para Linux que ofrece distintas formas de funcionamiento:

- **Forward proxy:** es la forma básica en la que se basan el resto de las modalidades.
- **Interception proxy:** funciona como un proxy transparente, interceptando y redirigiendo el tráfico sin necesidad de configuración en el cliente.
- **Reserve proxy:** es lo opuesto al Forward proxy. Gestiona las conexiones externas entrantes que atraviesan el proxy para llegar a la zona web interna, protegiendo y balanceando la carga de los servidores internos.
- **Offline proxy:** se usa para gestionar y almacenar completamente todo, reduciendo el uso de la red y ofreciendo un acceso más rápido a los recursos almacenados en caché.

IMPORTANTE

Squid es una herramienta potente y altamente configurable, pero requiere un conocimiento adecuado de su configuración y administración para aprovechar al máximo sus características.

Asegúrese de revisar y ajustar las configuraciones de Squid según las necesidades de su red y la política de seguridad de su organización.

Utilice ejemplos y casos de uso específicos para ilustrar cómo configurar y utilizar Squid de manera efectiva en diferentes situaciones.

5.4.1. Instalación

Squid está disponible en los repositorios de las principales distribuciones de Linux.

La configuración de Squid se encuentra en el archivo **/etc/squid/squid.conf.** Cualquier modificación en este archivo requerirá un reinicio del servicio para que los cambios surtan efecto.

5.4.2. Reglas de acceso

Squid utiliza listas de control de acceso (ACL) para identificar sitios web, direcciones IP, palabras clave, puertos, usuarios y más. Las reglas de acceso (http_access) permiten o deniegan el uso de una o más de estas ACL. Veamos un ejemplo para bloquear el acceso a cualquier URL en Google (la primera línea define la ACL y la segunda línea establece la regla que utiliza la ACL recién definida):

```
acl WebDeGoogle dstdomain .google.es
http_access deny WebDeGoogle
```

Los tipos de ACL (como dstdomain en el ejemplo anterior) son variados y todos se explican en los comentarios del archivo /etc/squid/squid.conf. Es una buena práctica crear uno o más archivos de definición de ACL separados e incluirlos en la configuración global mediante la directiva include:

```
acl social_network dstdomain "/etc/squid/
social_networks.txt"
```

Squid evalúa las reglas de acceso de arriba hacia abajo; cuando encuentra una regla aplicable, no sigue evaluando el resto. Por lo tanto, si todas nuestras reglas se encuentran en la categoría de denegación, la última línea debe ser:

```
http_access allow all
```

Es importante destacar también que Webmin cuenta con un módulo para la gestión del servidor Squid mediante una interfaz gráfica, facilitando la administración y configuración del proxy.

IMPORTANTE

- Al configurar las reglas de acceso, asegúrese de que no haya conflictos ni brechas de seguridad involuntarias.
- Siempre es buena idea hacer copias de seguridad de los archivos de configuración antes de realizar cambios importantes y probar los cambios en un entorno controlado antes de aplicarlos en un entorno de producción.
- La administración y supervisión de Squid es fundamental para mantener la seguridad y el rendimiento de la red. Monitoree el uso del proxy y ajuste las reglas y configuraciones según sea necesario.

5.5. Proxies inversos

En las redes informáticas, un proxy inverso es un tipo de servidor proxy que obtiene recursos en nombre del cliente de uno o más servidores. Estos recursos se devuelven al cliente como si provinieran del propio servidor proxy. A diferencia de un proxy de reenvío, que permite a sus clientes conectarse a cualquier servidor, un proxy inverso permite a los clientes conectados a él acceder a un conjunto específico de servidores. La conexión al servidor se realiza a través del proxy inverso en lugar de directamente por el cliente.

Los servidores web populares a menudo utilizan la función de proxy inverso, lo que ayuda a proteger la infraestructura de la aplicación de las vulnerabilidades de seguridad de HTTP.

Desde el punto de vista de la seguridad informática, el interés de los proxies inversos radica en su capacidad para equilibrar la carga entre dos o más servidores redundantes. Para cada solicitud recibida, el proxy (front-end) elige el servidor (back-end) al que reenviar la solicitud para ser procesada. Todos estos conceptos se tratarán en profundidad en las siguientes secciones, así como ejemplos de este tipo de software.

IMPORTANTE

Los proxies inversos pueden mejorar la seguridad y el rendimiento de una infraestructura de servidores al distribuir la carga y proteger los servidores internos de los ataques directos.

Es crucial configurar correctamente los proxies inversos para garantizar la máxima seguridad y eficiencia en la red.

Los proxies inversos pueden ser útiles para implementar medidas adicionales de seguridad, como la terminación de SSL/TLS, lo que reduce la carga de cifrado en los servidores de back-end.

La monitorización y el mantenimiento de los proxies inversos son fundamentales para garantizar su correcto funcionamiento y prevenir posibles problemas en la red.

www.universae.com