

SERVIDOR PROXY CON FIREWALL

Administración de Servicios en Red

Integrates:

Campos Gómez Fernanda Ivette

Hernández López César Erick

Ruiz Pérez Alejandro

EQUIPO 5

ÍNDICE

[**INTRODUCCIÓN**](#_8aikxmplerxz) **3**

[**FIREWALL**](#_8aikxmplerxz) **3**

[TIPO [1]](#_8aikxmplerxz) 3

[POLÍTICAS](#_8aikxmplerxz) 4

[**PROXY**](#_8aikxmplerxz) **5**

[CARACTERÍSTICAS](#_wpcvxco33ws6) 5

[TIPOS](#_8aikxmplerxz) 6

[Servidores proxy directos e inversos](#_d2wqqcqm4465) 6

[Proxies transparentes](#_vnnog2bn7sdw) 7

[Proxies anónimos](#_wrlhy07wysuh) 7

[Proxies altamente anónimos](#_17monm1o00x4) 7

[Proxies Socks 4 y 5](#_9w8274tqu7m3) 7

[Proxy de DNS](#_g1b34b35rkys) 7

[**SQUID**](#_uezsu8ibjdfa) **7**

[SQUIDGUARD](#_gyhvx1hxy7at) 8

[**SHOREWALL**](#_akl9kvz0wg3r) **8**

[**OBSERVIUM**](#_6vkpir5nsbkh) **8**

[**REFERENCIAS**](#_8aikxmplerxz) **9**

# INTRODUCCIÓN

El presente manual explica de forma breve los conceptos de firewall y proxy, tipos que existen y usos de estos. Se incluyen algunas herramientas para la implementación tanto de un servidor proxy y un firewall. Además, se agrega información sobre Observium, un monitor de red, donde podemos ver el tráfico de nuestra red, los paquetes que recibe nuestra interfaz de red, así como los errores que se generan en ésta.

# FIREWALL

Un firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad.Un firewall puede ser hardware, software o ambos. [1]

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. [2]

## TIPO [1]

* Proxy Firewall: un firewall proxy sirve como puerta de enlace de una red a otra para una aplicación específica. Los servidores proxy pueden proporcionar una funcionalidad adicional, como el almacenamiento en caché de contenido y la seguridad, impidiendo las conexiones directas desde fuera de la red. Sin embargo, esto también puede afectar las capacidades de rendimiento y las aplicaciones que pueden admitir.
* Firewall de inspección de estado: Ahora pensado como un firewall "tradicional", un firewall de inspección de estado permite o bloquea el tráfico según el estado, el puerto y el protocolo. Supervisa toda la actividad desde la apertura de una conexión hasta que se cierra. Las decisiones de filtrado se toman en base tanto a las reglas definidas por el administrador como al contexto, que se refiere al uso de información de conexiones anteriores y paquetes que pertenecen a la misma conexión.
* Firewall de gestión de amenazas unificadas (UTM): Un dispositivo UTM generalmente combina, de forma flexible, las funciones de un firewall de inspección con estado con prevención de intrusiones y antivirus. También puede incluir servicios adicionales y, a menudo, la gestión de la nube. Los UTM se centran en la simplicidad y la facilidad de uso.
* Firewall de última generación (Next-Generation firewall: NGFW): Los firewalls han evolucionado más allá del simple filtrado de paquetes y la inspección de estado. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear amenazas modernas, como malware avanzado y ataques de capa de aplicación.

Según la definición de Gartner, Inc., un firewall de próxima generación debe incluir:

* + Capacidades de cortafuegos estándar como inspección de estado
  + Prevención integral de intrusiones.
  + Conocimiento y control de aplicaciones para ver y bloquear aplicaciones de riesgo.
  + Actualizar rutas para incluir futuros feeds de información
  + Técnicas para hacer frente a las amenazas de seguridad en evolución

Si bien estas capacidades se están convirtiendo cada vez más en el estándar para la mayoría de las empresas, los NGFW pueden hacer más.

* NGFW centrada en la amenaza: Estos firewalls incluyen todas las capacidades de un NGFW tradicional y también proporcionan detección y remediación avanzada de amenazas. Con un NGFW enfocado en la amenaza usted puede:
  + Sepa qué activos están en mayor riesgo con un conocimiento completo del contexto
  + Reaccione rápidamente a los ataques con la automatización de seguridad inteligente que establece políticas y fortalece sus defensas dinámicamente
  + Detectar mejor la actividad evasiva o sospechosa con la red y la correlación de eventos de punto final
  + Disminuye considerablemente el tiempo desde la detección hasta la limpieza con seguridad retrospectiva que monitorea continuamente las actividades y comportamientos sospechosos incluso después de la inspección inicial
  + Facilite la administración y reduzca la complejidad con políticas unificadas que protegen todo el continuo de ataques

## POLÍTICAS

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 las 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. [3]

# PROXY

Es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina ***A*** solicita un recurso a ***C***, lo hará mediante una petición a ***B***, que a su vez trasladará la petición a ***C***; de esta forma ***C*** no sabrá que la petición procedió originalmente de ***A***. Esta situación estratégica de punto intermedio le permite ofrecer diversas funcionalidades: control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, caché web, etc. [4]

Hay dos tipos de proxys atendiendo a quién es el que quiere implementar la política del proxy:

* **proxy local**: En este caso el que quiere implementar la política es el mismo que hace la petición. Por eso se le llama local. Suelen estar en la misma máquina que el cliente que hace las peticiones. Son muy usados para que el cliente pueda controlar el tráfico y pueda establecer reglas de filtrado que por ejemplo pueden asegurar que no se revela información privada (Proxys de filtrado para mejora de la privacidad).
* **proxy de red** o **proxy externo**: El que quiere implementar la política del proxy es una entidad externa. Por eso se le llama externo. Se suelen usar para implementar cacheos, bloquear contenidos, control del tráfico, compartir IP, etc.

## CARACTERÍSTICAS

* **Control**: solamente el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos únicamente al servidor proxy.
* **Ahorro**: solamente *uno* de los usuarios (el proxy) ha de estar preparado para hacer el trabajo real. Con estar preparado significa que es el único que necesita los recursos necesarios para hacer esa funcionalidad. Ejemplos de recursos necesarios para hacer la función pueden ser la capacidad y lógica de la dirección de red externa (IP).
* **Velocidad**: si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
* **Filtrado**: el proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
* **Modificación**: como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
* **Anonimato**: si todos los usuarios se identifican como uno solo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.
* **Abuso**: al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
* **Carga**: un proxy tiene que hacer el trabajo de *muchos* usuarios.
* **Intromisión**: es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.
* **Incoherencia**: si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en caché sigue siendo la misma que la existente en el servidor remoto.
* **Irregularidad**: el hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

## TIPOS

### Servidores proxy directos e inversos

Los proxies directos (*forward proxy servers*) envían las solicitudes de un cliente a un servidor web. Los usuarios acceden a proxies directos navegando directamente a una dirección de proxy web o estableciendo sus configuraciones de internet. Los proxies directos permiten eludir los firewalls y aumentar la privacidad y la seguridad de un usuario, pero a veces pueden usarse para descargar materiales ilegales, como los materiales protegidos por derechos de autor o pornografía infantil.

Los proxies inversos (*reverse proxies*) manejan de forma transparente todas las solicitudes de recursos en los servidores de destino sin requerir ninguna acción por parte del solicitante.

Se utilizan proxies inversos:

* Para habilitar el acceso indirecto cuando un sitio web no permite conexiones directas como medida de seguridad.
* Para permitir el equilibrio de carga entre los separadores.
* Para transmitir contenido interno a los usuarios de internet.
* Para deshabilitar el acceso a un sitio, por ejemplo cuando un ISP o un gobierno desea bloquear un sitio web.

Los sitios pueden bloquearse por razones más o menos legítimas. Pueden utilizarse proxies inversos para impedir el acceso a contenido inmoral, ilegal o protegido por derechos de autor. A veces estas razones son justificables, pero a veces la justificación es dudosa. Los proxies inversos a veces impiden el acceso a sitios de noticias donde los usuarios pueden ver la información filtrada. También pueden impedir que los usuarios accedan a sitios donde puedan revelar información sobre acciones del gobierno o de la industria. El bloqueo del acceso a dichos sitios web puede violar los derechos de libertad de expresión. [5]

### Proxies transparentes

Se encuentran típicamente cerca de la salida de una red corporativa. Estos proxies centralizan el tráfico de red. En las redes corporativas, un servidor proxy está asociado con –o forma parte de– un servidor gateway que separa la red de las redes externas (normalmente internet) y un firewall que protege la red de la intrusión externa y permite que los datos sean escaneados para propósitos de seguridad antes de la entrega a un cliente en la red. Estos proxies ayudan a monitorear y administrar el tráfico de red, ya que los ordenadores de una red corporativa suelen ser dispositivos seguros que no necesitan anonimato para tareas típicamente mundanas. [5]

### Proxies anónimos

Ocultan la dirección IP del cliente, permitiéndoles acceder a los materiales que están bloqueados por firewalls o evitar las prohibiciones de direcciones IP. Pueden ser utilizados para mayor privacidad y/o protección contra ataques. [5]

### **Proxies altamente anónimos**

Ocultan incluso el hecho de que están siendo utilizados por los clientes y presentan una dirección IP pública no proxy. Así que no sólo ocultan la dirección IP del cliente que los usa, sino que también permiten el acceso a sitios que pueden bloquear servidores proxy. Ejemplos de proxies altamente anónimos incluyen I2P y [TOR](https://whatis.techtarget.com/definition/TOR-third-generation-onion-routing). [5}

### Proxies Socks 4 y 5

Proporcionan servicio de proxy para datos UDP y operaciones de búsqueda de DNS, además del tráfico web. Algunos servidores proxy ofrecen ambos protocolos Socks. [5]

### Proxy de DNS

Envían solicitudes de servicio de [nombres de dominio (DNS)](https://searchdatacenter.techtarget.com/es/consejo/DNS-en-la-nube-Construccion-de-una-arquitectura-DNS-segura) desde LANs a servidores DNS de internet durante el almacenamiento en caché para una velocidad mejorada. [5]

# SQUID

Squid es un proxy HTTP / 1.0. Squid ofrece un rico entorno de control de acceso, autorización y registro para desarrollar aplicaciones web de proxy y contenido. Squid ofrece un amplio conjunto de opciones de optimización de tráfico, la mayoría de las cuales están habilitadas de forma predeterminada para una instalación más sencilla y un alto rendimiento. [6]



## SQUIDGUARD

SquidGuard es un redireccionador de URL que se usa para usar listas negras con el software Squid. Hay dos grandes ventajas para el SquidGuard: es rápido y es gratis. SquidGuard se publica bajo licencia pública de GNU. [4]



# SHOREWALL

Shorewall (Shoreline Firewall) es una robusta y extensible herramienta de alto nivel para la configuración de muros cortafuego. Shorewall solo necesita se le proporcionen algunos datos en algunos archivos de texto simple y éste creará las reglas de cortafuegos correspondientes a través de iptables. Shorewall puede permitir utilizar un sistema como muro cortafuegos dedicado, sistema de múltiples funciones como puerta de enlace, dispositivo de encaminamiento y servidor. [8]

# OBSERVIUM

Observium es una plataforma de supervisión de red de auto-descubrimiento de bajo mantenimiento que soporta una amplia gama de tipos de dispositivo.

Para obtener información de un dispositivo se usa o clientes nativos o se usa SNMP. El SNMP tiene que estar prendido en cada servidor, switch o dispositivo que desea graficar en Observium. [7]

# REFERENCIAS

[1] https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

[2] Ingham, Kenneth; Forrest, Stephanie (2002). [«A History and Survey of Network Firewalls»](http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf)

[3] <https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)>

[4] <https://es.wikipedia.org/wiki/Servidor_proxy#Aplicaciones_Web_Proxy>

[5] <https://searchdatacenter.techtarget.com/es/definicion/Servidor-Proxy>

[6] <http://www.squid-cache.org/Intro/>

[7] <http://www.uprm.edu/cms/index.php?a=file&fid=11526>

[8] <http://www.shorewall.net/>