INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES PROXY

MARÍA ÁNGELES PEÑASCO SÁNCHEZ- TEMA 5- SAD

Servidores proxy:

- Tipos de «proxy».

- Características.

- Funcionamiento.

- Instalación de servidores «proxy».

- Instalación y configuración de clientes «proxy».

- Configuración del almacenamiento en la caché de un «proxy».

- Configuración de filtros.

- Métodos de autenticación en un «proxy».

- «proxys» inversos.

- «proxys» encadenados.

- Pruebas de funcionamiento. Herramientas gráficas.

Servidores proxy:

Tipos de «proxy»

Proxy de web / Proxy cache de web

Se trata de un proxy para una aplicación específica; el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una caché para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

Funcionamiento

1. El cliente realiza una petición (p. ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
2. Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargo en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones.

El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

Los proxies web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como proxies Web. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

Un cliente de un ISP manda una petición a Google la cual llega en un inicio al servidor Proxy que tiene este ISP, no va directamente a la dirección IP del dominio de Google. Esta página concreta suele ser muy solicitada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su Proxy por un cierto tiempo y crea una respuesta en mucho

menor tiempo. Cuando el usuario crea una búsqueda en Google el servidor Proxy ya no es utilizado; el ISP envía su petición y el cliente recibe su respuesta ahora sí desde Google.

Otras funciones

Como método extra y de ayuda en las descargas mediante aplicaciones P2P; el cual es usado en Lphant y algunos Mods del Emule.

Ventajas

- Ahorro de Tráfico: las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.
- Velocidad en Tiempo de respuesta: el servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.
- Demanda a Usuarios: puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.
- Filtrado de contenidos: el servidor proxy puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.
- Modificación de contenidos: basándose en la misma función del filtrado, y llamado Privoxy, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

Desventajas

- Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché.

Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona habitualmente para un proxy.

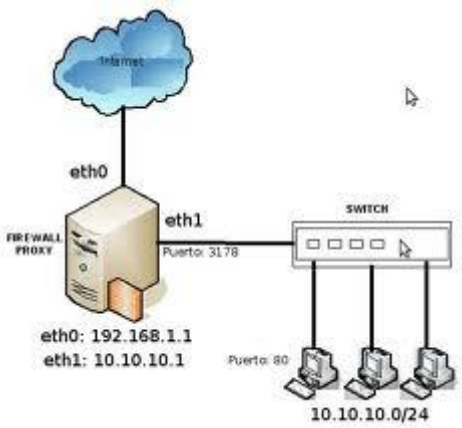
- El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.

- Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.

Proxies transparentes

Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración. Una ventaja de tal es que se puede usar para redes de empresa.

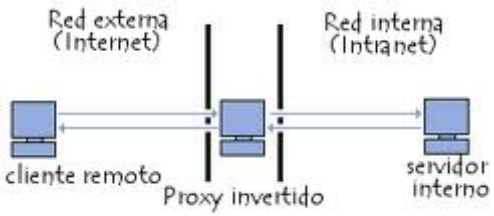
Un proxy transparente combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de internet (ISP).



Reverse Proxy / Proxy inverso

Un reverse proxy es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. Hay varias razones para instalar un "reverse proxy":

- Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.
- Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).
- Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).
- Caché de contenido estático: Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido gráfico.



Proxy NAT (Network Address Translation) / Enmascaramiento

Otro mecanismo para hacer de intermediario en una red es el NAT.

La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy.

La función de NAT reside en los Cortafuegos y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero encaminador.

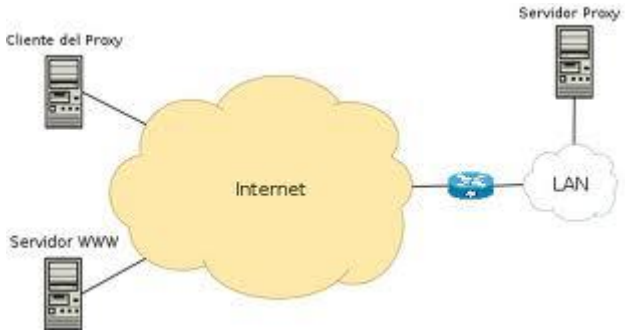
Proxy abierto

Este tipo de proxy es el que acepta peticiones desde cualquier ordenador, esté o no conectado a su red.

En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam. Un proxy se usa, normalmente, para almacenar y redirigir servicios como el DNS o la navegación Web, mediante el cacheo de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al

aplicarle una configuración "abierta" a todo internet, se convierte en una herramienta para su uso indebido.

Debido a lo anterior, muchos servidores, como los de IRC, o correo electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras ("BlackList").

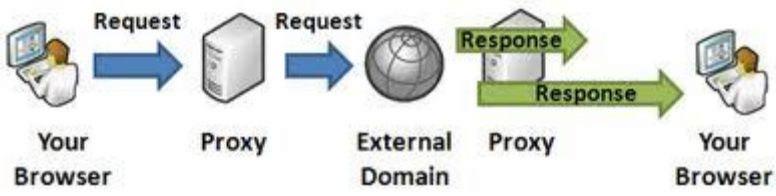


Cross-Domain Proxy

Típicamente usado por Tecnologías web asíncronas (flash, ajax, comet, etc) que tienen restricciones para establecer una comunicación entre elementos localizados en distintos dominios.

En el caso de Ajax, por seguridad sólo se permite acceder al mismo dominio origen de la página web que realiza la petición. Si se necesita acceder a otros servicios localizados en otros dominios, se instala un Cross-Domain proxy[2] en el dominio origen que recibe las peticiones ajax y las reenvía a los dominios externos.

En el caso de flash, también han solucionado creando la revisión de archivos XML de Cross-Domain, que permiten o no el acceso a ese dominio o subdominio.



Características

- El uso más común es el de servidor proxy, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.
    - De ellos, el más famoso es el servidor proxy web (comúnmente conocido solamente como «proxy»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.
    - También existen proxies para otros protocolos, como el proxy de FTP.
    - El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.
- Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.
- Un componente hardware también puede actuar como intermediario para otros.

Como se ve, proxy tiene un significado muy general, aunque siempre es sinónimo de intermediario.

Ventajas

En general (no sólo en informática), los proxies hacen posible:

- Control: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- Ahorro. Por tanto, sólo uno de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- 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 sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Desventajas

En general (no sólo en informática), el uso de un intermediario puede provocar:

- 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 ha de 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 cache 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).

Funcionamiento

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (p.ej.: una página web) en una caché que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de proxy se agrupan diversas técnicas.

Instalación de servidores «proxy»

La instalación de un Servidor Proxy en su Red Local es súper sencilla. En este apartado damos por supuesto que usted sabe:

- Cómo instalar y configurar el protocolo TCP/IP en la máquina en la que se instalará el Servidor Proxy (sea un Windows NT o un Windows 95)

- Cómo instalar y configurar el protocolo TCP/IP en los Puestos de Trabajo de su Red Local (sean estos Puestos de Trabajo ordenadores Windows 3.11, Windows 95, Macintosh, UNIX, o cualquier otro sistema operativo)

- Cómo instalar el Módem o la Tarjeta RDSI que utilizará para conectarse a internet

- Cómo instalar el Acceso Remoto a Redes (RAS) de Windows NT o el Acceso Telefónico a Redes de Windows 95

Si usted carece de estos conocimientos, en la documentación de Windows NT y de Windows 95 encontrará gran cantidad de información útil.

Asignación de Direcciones IP a los Puestos de Trabajo de su Red Local

Antes de instalar el Servidor Proxy, Usted deberá haber instalado y configurado el protocolo TCP/IP en su Red Local. No es necesario que instale este protocolo en todos los ordenadores de su Red Local, sino solamente en aquellos en los que querrá utilizar servicios de internet, y también en aquel en el que vaya a querer instalar el Servidor Proxy.

Cuando instale el protocolo TCP/IP, asigne a los Puestos de Trabajo de su Red Local direcciones de la subred de Clase B 192.168.X.X. Este rango de direcciones IP está reservado para su uso en intranets, y le proporciona un espacio seguro de direcciones. Debe asignar una dirección IP diferente a cada conexión de su Red Local (a partir de ahora nos referiremos a su Red Local como su ``intranet'').

Por ejemplo, puede comenzar por 192.168.0.1, 192.168.0.2, 192.168.0.3, etc...

Le recomendamos que reserve la dirección 192.168.0.1 para el ordenador en el que vaya a instalar el Servidor Proxy, ya que esta dirección le resultará más fácil de recordar.

Comprobación de la Instalación del Protocolo TCP/IP

Para comprobar que la instalación del protocolo TCP/IP ha sido correcta, haga un PING a cada una de las direcciones IP que haya definido en su intranet. Si no obtiene respuesta de alguna de ellas repase la configuración y solucione el error antes de continuar. Para realizar un PING desde una máquina con sistema operativo Windows, abra una ventana MS-DOS y teclee:

C:> ping 192.168.x.x

Donde 192.168.x.x es la dirección IP de la máquina que está interrogando.

Instalación y configuración de clientes «proxy»

Los clientes proxy web son aplicaciones que realizan solicitudes de descarga HTTP, HTTPS o FTP a través de HTTP al puerto TCP en el que Forefront TMG escucha las solicitudes web salientes de la red del cliente.

Una aplicación cliente proxy web debe ser:

- Compatible con CERN: es decir, entiende el método correcto para realizar una solicitud de proxy web.
- Proporciona un medio para que los clientes especifiquen un nombre (o dirección IP) y un puerto para utilizar con las solicitudes de proxy web.

Los clientes proxy web presentan las características siguientes:

- Una aplicación que se ejecuta en un equipo cliente de una red interna puede ser un cliente proxy web si realiza solicitudes, como se ha descrito anteriormente. Normalmente, los clientes son aplicaciones de explorador web conformes con HTTP 1.1. El explorador especifica Forefront TMG como proxy o utiliza la detección automática para recibir la configuración proxy desde otro servidor.
- Los clientes utilizan la detección automática para detectar el servidor Forefront TMG que se va a utilizar para las solicitudes proxy web.
- Los protocolos están limitados a solicitudes HTTP, HTTPS y FTP sobre HTTP.
- Los clientes se pueden autenticar en Forefront TMG mediante autenticación básica, implícita o WDigest, o integrada.
- Forefront TMG resuelve las solicitudes en nombre de los clientes proxy web.

Configuración de los clientes proxy web y los clientes del explorador para utilizar Forefront TMG como proxy web

Configure los clientes proxy web como sigue:

- Habilite una red interna o perimetral para escuchar para las solicitudes de los clientes proxy web. Forefront TMG escucha las solicitudes web salientes de los clientes que se encuentran en la red interna predeterminada en el puerto 8080.

Configure los clientes del explorador para que utilicen Forefront TMG como proxy web de la forma siguiente:

- Especifique manualmente un proxy estático en la configuración del explorador.
- También puede utilizar un método de detección automática para que los clientes utilicen un script de configuración o el protocolo WPAD para descubrir el servidor proxy que deben utilizar. Para obtener más información, vea Configuración de la detección automática.

Para clientes con el software de cliente de Forefront TMG instalado, puede configurar las opciones del explorador web del cliente en Administración de Forefront TMG. Estas opciones se insertan en los clientes después de la instalación, a petición o periódicamente.

Los clientes proxy web se pueden configurar para que tengan acceso directo a los recursos ubicados en su propia red y para omitir el proxy para direcciones y nombres de dominio determinados. Para obtener más información, vea Omisión de Forefront TMG para las solicitudes de cliente proxy web.

Configuración del almacenamiento en la caché de un «proxy»

Proxy Caché

Su método de funcionamiento es similar al de un proxy HTTP o HTTPs. Su función es precargar el contenido web solicitado por el usuario para acelerar la respuesta Web en futuras peticiones de la misma información de la misma máquina u otras.

Características

La palabra proxy se usa en situaciones en donde tiene sentido un unos algunos intermediario.

- El uso más común es el de servidor proxy, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.
    - De ellos, el más famoso es el servidor proxy web (comúnmente conocido solamente como «proxy»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.
    - También existen proxies para otros protocolos, como el proxy de FTP.
    - El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.

- Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.
- Un componente hardware también puede actuar como intermediario para otros.

Como se ve, proxy tiene un significado muy general, aunque siempre es sinónimo de intermediario.

Ventajas

En general (no sólo en informática), los proxies hacen posible:

- Control: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- Ahorro. Por tanto, sólo uno de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- 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 lo usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

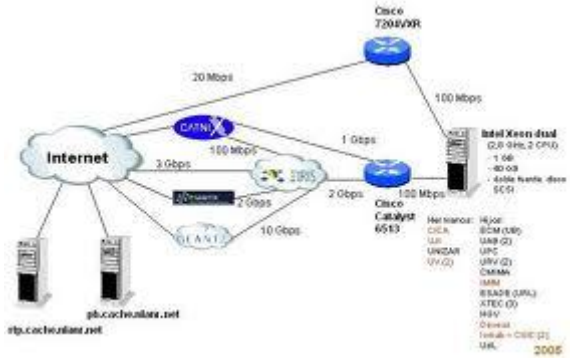
Desventajas

En general (no sólo en informática), el uso de un intermediario puede provocar:

- 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 ha de 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 cache 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).

Funcionamiento

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (p.ej.: una página web) en una caché que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de proxy se agrupan diversas técnicas.



Configuración de filtros

El cliente de Terminal Server intenta utilizar el puerto TCP 3389 como un puerto de destino cuando intenta conectarse a Terminal Server. Configurar Proxy Server para permitir que a un cliente en Internet para conectar con el servidor en el puerto TCP 3389 desde un puerto de origen aleatorio:

1. Abra el Administrador de servicios de Internet.
2. Haga clic con el botón secundario en Proxy Web y, a continuación, haga clic en Propiedades.
3. Haga clic en seguridad.
4. En la ficha Filtros de paquetes, haga clic en Agregar.
5. Haga clic en Filtro personalizado y, a continuación, cambie los valores que coincida con la siguiente tabla:
6. Setting Value
7. ----------
8. Protocol ID TCP
9. Direction Both
10. Local Port Fixed Port: 3389
11. Remote Port Any

12. Haga clic en Aceptar y, a continuación, comprobar que el filtro se ha agregado a la lista de excepciones.
13. Si el filtro se agrega correctamente a la lista, cierre la interfaz de proxy Web.

Para obtener información adicional acerca de puertos y servicios de Microsoft, haga clic en el número de artículo siguiente para verlo en Microsoft Knowledge Base: 150543 (http://support.microsoft.com/kb/150543/EN-US/) WinNT, Terminal Server y Exchange Services Use TCP/IP Ports

Métodos de autenticación en un «proxy»

Auto: el modo default es seleccionado basándonos en la petición que haga el cliente. Auto puede seleccionar cualquier de las opciones, proxy, origin, origin-ip, o origin-cookie-redirect dependiendo en el tipo de conexión (explicita o transparente) y la configuración de la cookie de autenticación en modo transparente.

Si usted tiene muchas peticiones de autenticación en el back-end (LDAP, RADIUS o el cliente BCAAA) puede configurar el ProxySG (y posiblemente el cliente) para que utilicen conexiones persistentes, esto reduce dramáticamente la carga en el back-end y el performance general de su red local.

Proxy-IP: El proxy utiliza un desafío en forma explícita y la IP del cliente como credenciales sustitutas. Proxy-IP específica un forward proxy inseguro. En algunos casos el desafío del proxy no funciona por lo que “origin” desafíos deben de ser generados.

Origin: El proxy actúa como una OCS y genera desafíos OCS. La conexión autenticada sirve como credenciales sustitutas.

Origin-IP: el proxy actúa como una OCS y genera desafíos OCS. La dirección del cliente es usada como credenciales sustitutas. Origin-IP es usado para soportar autenticación por IWA cuando el cliente no puede manejar credenciales por cookies.

Origin-Cookie: El ProxySG actual como un servidor de origen y genera desafíos de servidor de origen. Una cookie es generada como credenciales sustitutas. Origin-Cookie es usado en forward proxies para soportar autenticación pass-through de manera más segura que Origen-IP si en cliente entiende cookies. Solamente los protocolos HTTP y HTTPS soportan cookies; todos los demás protocolos son degradados a utilizar automáticamente Origin-IP.

Este modo también puede ser utilizado en proxy reverso en situaciones que se está personificando (cuando el proxy usa credenciales para conectar a otra computadora y accede a contenido que el usuario está autorizado a ver) no es posible y el server origen requiere autenticación.

Origin-cookie-redirect: El cliente es redirigido a una URL Virtual para ser autenticado, y las cookies son usadas como credenciales sustitutas. El Proxy SG no soporta Origin-Redirect con el método de CONNECT. Para forward proxy, solamente modos origin-*-redirect son soportados para autenticación por Kerberos/IWA. (Cualquier otro modo utiliza NTLM)

Es de notar cuando se autentica por cookies la petición de la redirección para hacerle un “Strip” a la cookie de autenticación desde la URL es logueada HTTP/307 (o 302) TCP_DENIED.

SG2: Este modo es seleccionado automáticamente, basando en la petición, y usa las reglas definidas del SGOS 2.x.

From-IP: una forma es presentada para recolectar las credenciales del usuario. La forma es presentada cada vez que el caché de las credenciales del usuario expiren.

From-Cookie: Una forma es presentada para colectar las credenciales del usuario. Las cookies son situadas en el dominio OCS solamente y el usuario es presentado con una nueva forma para cada dominio. Este modo es más utilizado en escenarios de proxy reverso donde hay un número limitado de dominios.

From-Cookie-Redirect: Una forma es presentada para colectar las credenciales del usuario. El usuario es re direccionado a la URL Virtual antes de ser presentada la forma. La cookie de autenticación es situada en ambos, la URL Virtual y el dominio OSC. El usuario es desafiado solamente cuando el cache de las credenciales expira.

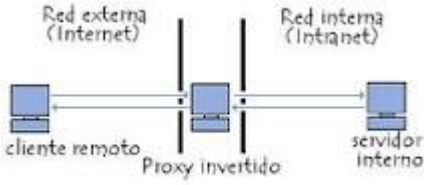
From-IP-Redirect: Este es similar a From-IP con la excepción que el usuario es re direccionado a la URL Virtual de autenticación antes que la forma sea presentada.

Es de notar que los modos que utilizan credenciales sustitutas por IP son inseguras: después que un usuario ha sido autenticado desde su dirección IP todos los requerimientos siguientes desde esa IP son tratados como si fueran de dicho usuario. Si el cliente está detrás de un NAT o en un sistema multiusuario, esto puede representar un serio problema de seguridad.

«Proxys» inversos

Sólo autenticación básica funcionará en una configuración donde un equipo único proxy funciona como un equipo proxy de reenvío y un equipo proxy inverso y autenticación de proxy se desea. Además, el servidor de publicación debe configurarse para recibir los encabezados de autenticación. Desgraciadamente, este doble uso del equipo como un proxy y un equipo proxy inverso entra en conflicto con la recomendación de Microsoft para no utilizar la autenticación con proxy inverso, como habilitar la autenticación para el proxy también permite para el proxy inverso.

Conviene señalar que un equipo que funciona como un proxy inverso y un proxy de reenvío puede configurarse para utilizar NTLM y autenticación básica correctamente. En el caso de proxy de reenvío, Internet Explorer favorecerá NTLM a través de Basic. En el caso de proxy inverso, Internet Explorer actuará del mismo modo y, cuando el servidor de publicación produce el error "Acceso denegado", Internet Explorer usará la autenticación básica y que se realizará correctamente. Tenga en cuenta que aunque esto funciona, también implica una sobrecarga considerable y por lo tanto, no ser adecuado si la ruta de acceso proxy inverso se utiliza con frecuencia.



«Proxys» encadenados

Un proxy encadenado puede configurarse para realizar la autenticación en su asociado de proxy indirecto. En este caso, el proxy indirecto actúa como un explorador cliente. Puesto que hay un proxy indirecto entre el cliente y el proxy que precede en la cadena, todas las limitaciones para autenticar con un servidor proxy (descrito anteriormente) se aplican.

La diferencia entre este caso el caso de proxy única es que el administrador puede decidir habilitar específicas las credenciales de proxy a proxy, incluidas mediante NTLM entre los servidores proxy. Esto funciona porque la autenticación de proxy a proxy es salto por salto.

Siempre se autenticarán los clientes de explorador de Web con el primer servidor proxy que se conectan con. No se pasan credenciales desde el explorador Web cliente a servidores proxy que precede en la cadena.

Pruebas de funcionamiento. Herramientas gráficas

Cuando un servidor proxy se inserta en el sistema, entre el explorador Web y el servidor de publicación de Web, la autenticación NTLM entre el explorador del cliente y el servidor de publicación de WEB dejarán de funcionar. De hecho cualquier método de autenticación depender implícita estado de extremo a extremo (por ejemplo, NTLM) dejará de trabajo.

La especificación de HTTP 1.1 indica que todo el estado es salto por salto. Estado de extremo a extremo puede realizarse mediante una cookie o algunos otro token distinto de HTTP. El síntoma más evidente de este error es los exploradores de cliente recibe un mensaje de error de autenticación, como "Acceso denegado".

Ya que los encabezados HTTP para la autenticación de proxy son diferentes de los de autenticación del servidor Web, es posible habilitar la autenticación básica en el proxy y también realice la autenticación básica entre un explorador cliente y un servidor de publicación de Web mientras se conecta a través de un equipo con Microsoft Proxy Server. Microsoft Internet Explorer admite esta configuración.

En resumen, autenticación básica no requiere un estado de extremo a extremo implícito y, por lo tanto, puede utilizarse a través de un servidor proxy. Autenticación desafío/respuesta de Windows NT requiere estado implícito de extremo a extremo y no funcionará a través de un servidor proxy.