Comprender el diseño de firewall de políticas basado en zonas

Contenido

Introducción

Este documento describe el modelo de configuración para el conjunto de funciones de Cisco IOS® Firewall, Zone-based Policy Firewall (ZFW).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Este nuevo modelo de configuración ofrece políticas intuitivas para routers de varias interfaces, mayor granularidad de la aplicación de políticas de firewall y una política predeterminada de deny-all que prohíbe el tráfico entre zonas de seguridad del firewall hasta que se aplica una política

explícita para permitir el tráfico deseado.

La nueva interfaz de inspección de políticas basadas en zonas permite utilizar casi todas las funciones clásicas de Cisco IOS Firewall implementadas antes de Cisco IOS Software Release 12.4(6)T:

- Inspección de paquetes con estado
- Cisco IOS Firewall con reconocimiento de VRF
- Filtrado de URL
- Mitigación de Negación de Servicio (DoS)

En Cisco IOS Software Release 12.4(9)T, ZFW también permite utilizar los límites de rendimiento y conexión/sesión por clase, además del control y la inspección de aplicaciones:

- HTTP
- Protocolo de oficina de correo (POP3), protocolo de acceso a correo por Internet (IMAP), protocolo simple de transferencia de correo/protocolo simple de transferencia de correo mejorado (SMTP/ESMTP)
- Remote Procedure Call (RPC) de Sun
- Aplicaciones de mensajería instantánea (IM):Microsoft MessengerYahoo! MensajeríaAOL Instant Messenger
- Uso compartido de archivos Peer-to-Peer (P2P):BittorrentKaZaAGnutellaeDonkey

En Cisco IOS Software Release 12.4(11)T, se agregaron estadísticas para facilitar el tuning de la protección contra DoS.

En ZFW de Cisco IOS Software Release 12.4(15)T, aún no son soportadas algunas funciones y capacidades de Cisco IOS Classic Firewall:

- Proxy de Autenticación
- Conmutación por falla de firewall activo
- MIB de firewall unificado
- Inspección activa de IPv6
- Soporte de TCP fuera de pedido

En general, ZFW mejora el rendimiento de Cisco IOS para la mayoría de las actividades de inspección de firewall. Ni Cisco IOS ZFW ni Classic Firewall incluyen soporte de inspección stateful para el tráfico multicast.

Descripción General de Zone-Based Policy

La stateful inspection de Cisco IOS Classic Firewall (antes conocida como Context-Based Access Control, Control de Acceso Basado en Contexto o CBAC) utilizaba un modelo de configuración basado en interfaces, en el cual se aplicaba una política de stateful inspection a una interfaz. Todo el tráfico que pasa a través de esa interfaz recibió la misma política de inspección. Este modelo de configuración limitaba la granularity (especificidad) de las políticas de firewall y causaba confusión en la aplicación adecuada de las políticas de firewall, especialmente en situaciones donde las políticas de firewall se deben aplicar entre varias interfaces.

Zone-Based Policy Firewall (también conocido como Zone-Policy Firewall o ZFW) cambia la configuración de firewall del modelo anterior, basado en interfaces, a un modelo basado en zonas, más flexible y fácil de comprender. Las interfaces se asignan a zonas y la política de

inspección se aplica al tráfico que se mueve entre las zonas. Las políticas entre zonas ofrecen considerable flexibilidad y granularity (especificidad), de modo que se pueden aplicar distintas políticas de inspección a varios grupos de hosts conectados a la misma interfaz del router.

Las políticas de firewall se configuran con Cisco Policy Language (CPL), que emplea una estructura jerárquica para definir la inspección de los protocolos de red y los grupos de hosts a los que se puede aplicar la inspección.

Modelo de Configuración de Zone-Based Policy

En comparación con Cisco IOS Classic Firewall, ZFW cambia completamente la forma de configurar la inspección de Cisco IOS Firewall.

El primer cambio importante a la configuración del firewall es la introducción de la configuración basada en zonas. Cisco IOS Firewall es la primera función de defensa contra amenazas de Cisco IOS Software que implementa un modelo de configuración por zonas. Otras funciones pueden adoptar el modelo de zona con el tiempo. Durante un período de tiempo, se mantendrá el modelo de configuración basado en interfaces con stateful inspection (o CBAC) de Cisco IOS Classic Firewall que utiliza el conjunto de comandos ip inspect. Sin embargo, muy pocas o ninguna de las nuevas funciones son configurables con la Interfaz de Línea de Comandos (CLI) clásica. ZFW no utiliza la stateful inspection ni los comandos CBAC. Los dos modelos de configuración se pueden utilizar simultáneamente en los routers, pero no combinados en las interfaces. Una interfaz no se puede configurar como un miembro de zona de seguridad y al mismo tiempo se puede configurar para ip inspect .

Las zonas establecen las fronteras de seguridad de la red. Una zona define un límite donde el tráfico se somete a las restricciones de las políticas al pasar a otra región de la red. La política predeterminada de ZFW entre zonas es denegar todo. Si no se configura ninguna política explícitamente, se bloquea todo el tráfico que se mueve entre zonas. Se trata de una desviación significativa del modelo de inspección con estado, en el que se permitía implícitamente el tráfico hasta que se bloqueaba explícitamente con una lista de control de acceso (ACL).

El segundo cambio importante es la introducción de un nuevo lenguaje de políticas de configuración conocido como CPL. Los usuarios familiarizados con la CLI (MQC) de calidad de servicio modular (QoS) del software Cisco IOS pueden reconocer que el formato es similar al uso de QoS de los mapas de clase para especificar qué tráfico se ve afectado por la acción aplicada en un mapa de política.

Reglas Para La Aplicación De Firewall De Políticas Basadas En Zonas

Las pertenencias a la interfaz de red del router en las zonas están sujetas a varias reglas que rigen el comportamiento de la interfaz, al igual que el tráfico que se mueve entre las interfaces de miembro de zona:

- Se debe configurar una zona antes de poder asignar interfaces a esa zona.
- Una interfaz puede ser asignada solo a una zona de seguridad.
- Todo el tráfico hacia y desde una interfaz determinada se bloquea implícitamente cuando se asigna la interfaz a una zona, excepto el tráfico hacia y desde otras interfaces de la misma zona y el tráfico hacia cualquier interfaz del router.

- Implícitamente, se permite que el tráfico fluya de forma predeterminada entre las interfaces que son miembros de la misma zona.
- Para permitir el tráfico hacia y desde una interfaz de miembro de zona, se debe configurar una política que permita o inspeccione el tráfico entre esa zona y cualquier otra zona.
- La zona automática es la única excepción a la directiva predeterminada de denegación de todo. Se permite todo el tráfico hacia cualquier interfaz del router hasta que se deniega explícitamente el tráfico.
- El tráfico no puede fluir entre una interfaz miembro de una zona y otra interfaz que no es miembro de una zona. Las acciones Pass, Inspect y Drop sólo se pueden aplicar entre dos zonas.
- Las interfaces que no se han asignado a una función de zona como puertos de router clásicos y todavía pueden utilizar la configuración clásica de inspección de estado/CBAC.
- Si es necesario que una interfaz en el cuadro no forme parte de la política de zona/firewall. Todavía puede ser necesario poner esa interfaz en una zona y configurar una política de pasar todo (una especie de política ficticia) entre esa zona y cualquier otra zona a la que se desee flujo de tráfico.
- Del comportamiento anterior se desprende que, si el tráfico va a fluir entre todas las interfaces de un router, todas las interfaces deben ser parte del modelo de zonificación (cada interfaz debe ser miembro de una zona u otra).
- La única excepción al comportamiento anterior, el enfoque de denegación predeterminado, es el tráfico entrante y saliente del router, que está permitido de forma predeterminada. Se puede configurar una política explícita para restringir dicho tráfico.

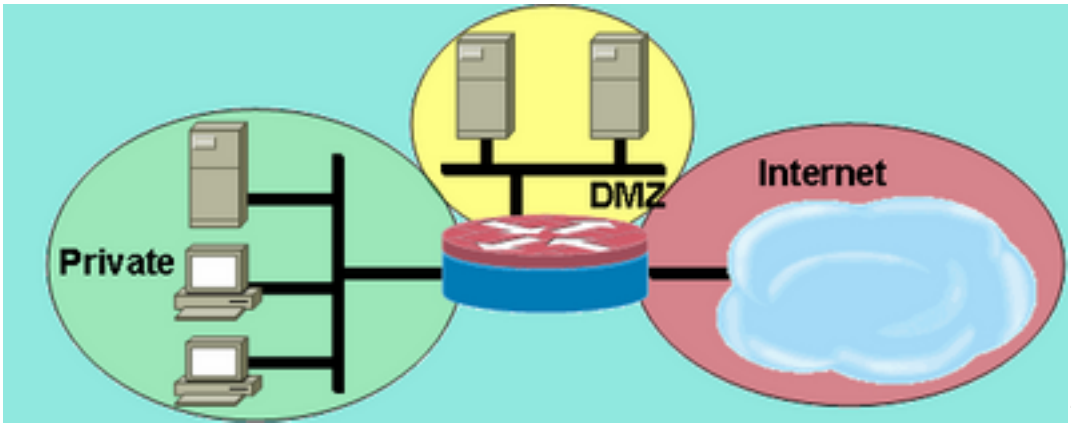
Diseño de políticas de seguridad de red basadas en zonas

Se debe configurar una zona de seguridad para cada región de seguridad relativa dentro de la red, de modo que todas las interfaces asignadas a la misma zona estén protegidas con un nivel de seguridad similar. Por ejemplo, considere un router de acceso con tres interfaces:

- Una interfaz conectada a la Internet pública.
- Una interfaz conectada a una red de área local (LAN) privada que no debe ser accesible desde la Internet pública.
- Una interfaz conectada a una zona desmilitarizada (DMZ) de servicio de Internet, en la que un Webserver, un servidor de Sistema de Nombres de Dominio (DNS) y un servidor de correo electrónico deben ser accesibles desde la Internet pública.

Cada interfaz de esta red está asignada a su propia zona, aunque puede desear permitir un acceso variado desde la Internet pública a hosts específicos de la DMZ y políticas de uso de aplicaciones variadas para hosts de la LAN protegida. (Consulte la figura 1.)

Figura 1: Topología Básica de Zonas de Seguridad



Topología Básica de Zonas de Seguridad

En este ejemplo, cada zona tiene una sola interfaz. Si se agrega una interfaz adicional a la zona privada, los hosts conectados a la nueva interfaz en la zona pueden pasar tráfico a todos los hosts de la interfaz actual en la misma zona. Además, el tráfico del host a los hosts en otras zonas se ve afectado de manera similar por las políticas actuales.

Normalmente, la red de ejemplo tiene tres políticas principales:

- Conectividad de la zona privada a Internet
- Conectividad de la zona privada a los hosts de la DMZ
- Conectividad de la zona de Internet a los hosts de la DMZ

Dado que la DMZ se expone a la red pública de Internet, los hosts de la DMZ pueden estar sujetos a actividades no deseadas de individuos malintencionados que pueden dañar uno o más hosts de la DMZ. Si no se proporciona una política de acceso para que los hosts de la DMZ alcancen los hosts de zonas privadas o de la zona de Internet, los individuos que comprometan los hosts de la DMZ no pueden utilizarlos para realizar otro ataque contra los hosts privados o de Internet. ZFW impone una postura de seguridad prohibitiva predeterminada. Por lo tanto, a menos que a los hosts de la DMZ se les proporcione acceso específicamente a otras redes, las demás redes están protegidas contra todas las conexiones de los hosts de la DMZ. De manera similar, a los hosts de Internet no se les proporciona acceso a los hosts de zonas privadas, de modo que los hosts de zonas privadas están protegidos contra el acceso no deseado por parte de los hosts de Internet.

Uso de VPN IPSec con firewall de políticas basadas en zonas

Recientes mejoras a VPN IPSec simplifican la configuración de políticas de firewall para la conectividad VPN. La interfaz de túnel virtual (VTI) IPSec y GRE+IPSec permiten el confinamiento de las conexiones VPN de sitio a sitio y de cliente a una zona de seguridad específica mediante la ubicación de las interfaces de túnel en una zona de seguridad especificada. Si se debe limitar la conectividad según una política específica, se pueden aislar las conexiones en una DMZ de la VPN. O bien, si se confía implícitamente en la conectividad VPN, se puede colocar la conectividad VPN en la misma zona de seguridad confiable de la red inside.

Si no se aplica una VTI IPSec, la política de firewall de conectividad VPN requiere un examen riguroso para mantener la seguridad. La directiva de zona debe permitir específicamente el acceso mediante una dirección IP a los hosts de sitio remoto o a los clientes VPN si los hosts seguros se encuentran en una zona distinta de la conexión cifrada del cliente VPN al router. Si la política de acceso no está configurada correctamente, los hosts que deben protegerse pueden quedar expuestos a hosts potencialmente hostiles no deseados. Consulte Uso de VPN con Zone-Based Policy Firewall para obtener un análisis más detallado de conceptos y configuraciones.

Configuración de Cisco Policy Language (CPL)

Para configurar ZFW, se puede utilizar el siguiente procedimiento. La secuencia de pasos no es importante, pero algunos eventos se deben completar en orden. Por ejemplo, se debe configurar un class-map antes de asignarlo a un policy-map. De manera similar, no se puede asignar un policy-map a un zone-pair hasta que se configura la política. Si se intenta configurar una sección que depende de otra parte de la configuración que aún no se configuró, el router responde con un mensaje de error.

1. Defina las zonas.
2. Defina los zone-pairs.
3. Defina los class-maps que describen el tráfico al que se debe aplicar una política cuando éste cruza un zone-pair.
4. Defina los policy-maps para aplicar la acción a su tráfico de class-maps.
5. Aplique los policy-maps a los zone-pairs.
6. Asigne las interfaces a las zonas.

Configuración de mapas de clase de firewall de políticas basadas en zonas

Los class-maps definen el tráfico que el firewall selecciona para aplicar las políticas. Los class-maps de capa 4 ordenan el tráfico según los criterios enumerados a continuación. Estos criterios se especifican con el comando match en un class-map:

- Access-group: Una ACL estándar, extendida o con nombre puede filtrar el tráfico según la dirección IP de origen y de destino y el puerto de origen y de destino.
- Protocolo: protocolos de capa 4 (TCP, UDP e ICMP) y servicios de aplicación como HTTP, SMTP, DNS, etc. Se puede especificar cualquier servicio conocido o definido por el usuario conocido por mapeo de aplicaciones de puerto.
- Class-map: Se puede anidar un class-map subordinado que proporciona criterios de match adicionales dentro de otro class-map.
- Not: el criterio not especifica que cualquier tráfico que no coincida con un servicio (protocolo), grupo de acceso o mapa de clase subordinado especificado se selecciona para el mapa de clase.

Combinar criterios de "coincidencia": "Match-Any" en comparación con "Match-All"

Con los class-maps, se pueden aplicar operadores de match-any o de match-all a fin de determinar cómo aplicar los criterios de match. Si se especifica match-any, el tráfico debe cumplir solamente con uno de los criterios de coincidencia en el class-map. Si se especifica match-all, el tráfico debe coincidir con todos los criterios de class-map para pertenecer a esa clase en particular.

Los criterios de coincidencia se deben aplicar en orden de más específicos a menos específicos si el tráfico cumple múltiples criterios. Por ejemplo, considere el siguiente class-map:

```
class-map type inspect match-any my-test-cmap
 match protocol http
 match protocol tcp
```

El tráfico HTTP debe encontrar primero el match protocol http para asegurarse de que el tráfico es procesado por las capacidades de servicio específicas de la inspección HTTP. Si las líneas de coincidencia se invierten, de modo que el tráfico encuentra la sentencia TCP del protocolo de coincidencia antes de compararla con el protocolo http, el tráfico se clasifica simplemente como tráfico TCP y se inspecciona en función de las capacidades del componente Inspección TCP del firewall. Esto es un problema para ciertos servicios, tales como FTP, TFTP y varios servicios de señalización multimedia y de voz, tales como H.323, SIP, Skinny, RTSP y otros. Estos servicios requieren capacidades de inspección adicionales para reconocer las actividades más complejas de tales servicios.

Aplicación de una ACL como criterios de coincidencia

Los class-maps pueden aplicar una ACL como uno de los criterios de match para la aplicación de políticas. Si un mapa de clase sólo coincide con el criterio es una ACL y el mapa de clase está asociado con un mapa de política que aplica la acción de inspección, el router aplica la inspección básica de TCP o UDP para todo el tráfico permitido por la ACL, excepto para el que ZFW proporciona inspección con reconocimiento de aplicación. Esto incluye (entre otros) FTP, SIP, Skinny (SCCP), H.323, Sun RPC y TFTP. Si la inspección de aplicaciones específica está disponible y la ACL permite el canal primario o de control, se permite cualquier canal secundario o de medios asociado con el canal primario o de control, independientemente de que la ACL permita o no el tráfico.

Si un class-map sólo aplica la ACL 101 como criterio de match, aparece una ACL 101 de la siguiente manera:

```
access-list 101 permit ip any any
```

Todo el tráfico se permite en la dirección de la política de servicio aplicada a un par de zonas determinado, y el tráfico de retorno que corresponde a esto se permite en la dirección opuesta. Por lo tanto, la ACL debe aplicar la restricción para limitar el tráfico a las especificaciones deseadas. Observe que la lista de PAM incluye servicios de aplicación como HTTP, NetBIOS, H.323 y DNS. Sin embargo, a pesar de que PAM conoce el uso específico de aplicaciones de un puerto determinado, el firewall solo aplica la capacidad específica de aplicaciones suficiente para dar cabida a los requisitos bien conocidos del tráfico de aplicaciones. Por lo tanto, el tráfico de aplicaciones simples como Telnet, SSH y otras aplicaciones de canal único se inspeccionan como TCP, y sus estadísticas se combinan en el resultado del comando show. Si desea obtener visibilidad específica de la aplicación de la actividad de red, debe configurar la inspección de los servicios por nombre de aplicación (configurar el protocolo de coincidencia HTTP, el protocolo de coincidencia telnet, etc.).

Compare las estadísticas disponibles en la salida del comando show policy-map type inspect zone-pair de esta configuración con la política de firewall más explícita que se muestra más adelante en la página. Esta configuración se utiliza para inspeccionar el tráfico de un Cisco IP Phone y de varias estaciones de trabajo que utilizan diversos tráficos, incluidos http, ftp, netbios, ssh y dns:

```
class-map type inspect match-all all-private
 match access-group 101
!
policy-map type inspect priv-pub-pmap
 class type inspect all-private
  inspect
 class class-default
```

```
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

Si bien esta configuración es fácil de definir y admite todo el tráfico que se origina en la zona privada (siempre que el tráfico use los puertos de destino estándar y reconocidos por PAM), proporciona una visibilidad limitada de la actividad de servicios y no ofrece la oportunidad de aplicar límites de sesión y ancho de banda de ZFW para tipos de tráfico específicos. Esta salida del comando show policy-map type inspect zone-pair priv-pub se deriva de la configuración simple anterior que utiliza solo una definición permit ip [subnet] any ACL entre los zone-pairs. Como se ve, la mayor parte del tráfico de las estaciones de trabajo se cuenta en las estadísticas TCP o UDP básicas:

```
stg-871-L#show policy-map type insp zone-pair priv-pub
Zone-pair: priv-pub

  Service-policy inspect : priv-pub-pmap

    Class-map: all-private (match-all)
      Match: access-group 101
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [413:51589]
        udp packets: [74:28]
        icmp packets: [0:8]
        ftp packets: [23:0]
        tftp packets: [3:0]
        tftp-data packets: [6:28]
        skinny packets: [238:0]

        Session creations since subsystem startup or last reset 39
        Current session counts (estab/half-open/terminating) [3:0:0]
        Maxever session counts (estab/half-open/terminating) [3:4:1]
        Last session created 00:00:20
        Last statistic reset never
        Last session creation rate 2
        Maxever session creation rate 7
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

Por el contrario, una configuración similar que agrega clases específicas de la aplicación proporciona más estadísticas y control granulares de la aplicación, y aún acomoda la misma amplitud de servicios que se mostró en el primer ejemplo cuando se define el mapa de clase de última oportunidad que coincide sólo con la ACL como la última oportunidad en el mapa de política:

```
class-map type inspect match-all all-private
 match access-group 101
class-map type inspect match-all private-ftp
 match protocol ftp
 match access-group 101
class-map type inspect match-any netbios
 match protocol msrpc
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
class-map type inspect match-all private-netbios
 match class-map netbios
 match access-group 101
class-map type inspect match-all private-ssh
 match protocol ssh
 match access-group 101
class-map type inspect match-all private-http
 match protocol http
 match access-group 101
!
policy-map type inspect priv-pub-pmap
 class type inspect private-http
  inspect
 class type inspect private-ftp
  inspect
 class type inspect private-ssh
  inspect
 class type inspect private-netbios
  inspect
 class type inspect all-private
  inspect
 class class-default!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

La configuración más específica proporciona esta salida substancialmente detallada para el comando show policy-map type inspect zone-pair priv-pub:

```
stg-871-L#sh policy-map type insp zone-pair priv-pub
 Zone-pair: priv-pub

   Service-policy inspect : priv-pub-pmap

     Class-map: private-http (match-all)
       Match: protocol http
       Match: access-group 101
       Inspect
         Packet inspection statistics [process switch:fast switch]
         tcp packets: [0:2193]
```

```
    Session creations since subsystem startup or last reset 731
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [0:3:0]
    Last session created 00:29:25
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 4
    Last half-open session total 0

Class-map: private-ftp (match-all)
  Match: protocol ftp
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [86:167400]
    ftp packets: [43:0]

    Session creations since subsystem startup or last reset 7
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [2:1:1]
    Last session created 00:42:49
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 4
    Last half-open session total 0

Class-map: private-ssh (match-all)
  Match: protocol ssh
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [0:62]

    Session creations since subsystem startup or last reset 4
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [1:1:1]
    Last session created 00:34:18
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 2
    Last half-open session total 0

Class-map: private-netbios (match-all)
  Match: access-group 101
  Match: class-map match-any netbios
    Match: protocol msrpc
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol netbios-dgm
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol netbios-ns
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol netbios-ssn
      2 packets, 56 bytes
      30 second rate 0 bps
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [0:236]

    Session creations since subsystem startup or last reset 2
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [1:1:1]
    Last session created 00:31:32
    Last statistic reset never
```

```
    Last session creation rate 0
    Maxever session creation rate 1
    Last half-open session total 0

Class-map: all-private (match-all)
  Match: access-group 101
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [51725:158156]
    udp packets: [8800:70]
    tftp packets: [8:0]
    tftp-data packets: [15:70]
    skinny packets: [33791:0]

    Session creations since subsystem startup or last reset 2759
    Current session counts (estab/half-open/terminating) [2:0:0]
    Maxever session counts (estab/half-open/terminating) [2:6:1]
    Last session created 00:22:21
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 12
    Last half-open session total 0

Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    4 packets, 112 bytes
```

Otra ventaja añadida cuando se utiliza una configuración más granular de mapa de clase y mapa de política, como se mencionó anteriormente, es la oportunidad de aplicar límites específicos de clase en los valores de sesión y velocidad; y ajustar específicamente los parámetros de inspección mediante la aplicación de un mapa de parámetros para ajustar cada comportamiento de inspección de clase.

Configurar Policy Firewall Policy-Maps basados en zonas

El policy-map aplica acciones de política de firewall a uno o más class-maps para definir la política de servicio que se aplica a un par de zonas de seguridad. Cuando se crea un policy-map de tipos de inspecciones, al final de la clase se aplica una clase predeterminada denominada clase class-default. La acción de política predeterminada de clase predeterminada es drop pero se puede cambiar para pasar. Se puede agregar la opción Log con la acción Drop. No se puede aplicar la acción Inspect en la clase class-default.

Acciones de Zone-Based Policy Firewall

ZFW proporciona tres acciones para el tráfico que viaja de una zona a otra:

- Drop — Esta es la acción predeterminada para todo el tráfico, según la aplica la clase class-default que termina cada policy-map de tipo inspeccionar. También se pueden configurar otros class-maps en un mismo policy-map para descartar el tráfico no deseado. El tráfico manejado por la acción de descartar es descartado silenciosamente (es decir, no se envía ninguna notificación de la descarta al host final relevante) por el ZFW, a diferencia de un comportamiento ACL cuando envía un mensaje "host inalcanzable" ICMP al host que envió el tráfico denegado. Actualmente, no existe la opción de cambiar el comportamiento de descarte silencioso. Se puede agregar la opción log con la opción drop para enviar una notificación syslog de que el firewall descartó tráfico.

- Pass: Esta acción permite al router reenviar el tráfico de una zona a otra. La acción Pass no realiza un seguimiento del estado de las conexiones o sesiones dentro del tráfico. Pass sólo permite el tráfico en una dirección. Se debe aplicar una política paralela para permitir que el tráfico de retorno pase en la dirección opuesta. La acción Pass es útil para protocolos como IPSec ESP, IPSec AH, ISAKMP y otros protocolos intrínsicamente seguros y de comportamiento predecible. Sin embargo, en ZFW el tráfico de la mayoría de las aplicaciones se procesa mejor con la acción Inspect.
- Inspect: La acción Inspect ofrece un control de tráfico basado en estado. Por ejemplo, si se inspecciona el tráfico de la zona privada a la zona de Internet en la red del ejemplo anterior, el router mantiene la información de conexión o sesión para el tráfico TCP y User Datagram Protocol (UDP). Por lo tanto, el router permite el tráfico de retorno enviado desde los hosts de la zona de Internet en respuesta a peticiones de conexión de la zona privada. Además, la inspección puede proporcionar inspección y control de aplicaciones para determinados protocolos de servicio que pueden transportar tráfico de aplicaciones vulnerable o delicado. Se puede aplicar una Audit-trial con un parameter-map para registrar el inicio, el fin y la duración de la conexión o sesión, el volumen de datos transferidos y las direcciones de origen y destino.

Las acciones se asocian con los class-maps en policy-maps:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

Los mapas de parámetro ofrecen opciones para modificar los parámetros de conexión para una política de inspección de mapa de clase determinada.

Configurar Zone-Policy Firewall Parameter-Maps

Los mapas de parámetro especifican el comportamiento de inspección para ZFW, para parámetros como protección DoS, temporizadores de sesión TCP/UDP y configuración de registro de trazas de auditoría. Los parameter-maps también se aplican con class-maps y policy-maps de capa 7 para definir el comportamiento de aplicaciones específicas, por ejemplo, objetos HTTP, requisitos de autenticación POP3 e IMAP y otra información de aplicaciones específicas.

Los parameter-maps de inspección de ZFW están configurados como type inspect, al igual que otros objetos de políticas y clases de ZFW:

```
stg-871-L(config)#parameter-map type inspect z1-z2-pmap stg-871-L(config-profile)#?
parameter-map commands:
  alert           Turn on/off alert
  audit-trail     Turn on/off audit trail
  dns-timeout     Specify timeout for DNS
  exit            Exit from parameter-map
  icmp            Config timeout values for icmp
  max-incomplete  Specify maximum number of incomplete connections before
                  clamping
  no              Negate or set default values of a command
  one-minute      Specify one-minute-sample watermarks for clamping
  sessions        Maximum number of inspect sessions
  tcp             Config timeout values for tcp connections
  udp             Config timeout values for udp flows
```

Los tipos específicos de parameter-maps especifican los parámetros aplicados por las políticas de inspección de aplicaciones de capa 7. Los mapas de parámetro de tipo Regex definen una expresión regular para su uso con la inspección de aplicación HTTP que filtra el tráfico con una expresión regular:

```
parameter-map type regex [parameter-map-name]
```

Los mapas de parámetro de tipo de información de protocolo definen los nombres de servidor para su uso con la inspección de aplicación de IM:

```
parameter-map type protocol-info [parameter-map-name]
```

Los detalles completos sobre la configuración de la inspección de aplicaciones HTTP e IM se proporcionan en las respectivas secciones de inspección de aplicaciones de este documento.

Aplicar registro para políticas de firewall de políticas basadas en zonas

ZFW ofrece opciones de logging para el tráfico que se descarta o inspecciona de forma predeterminada o las acciones de políticas de firewall configuradas. El logging de la audit-trial está disponible para el tráfico que inspecciona el ZFW. La pista de auditoría se aplica cuando se define una pista de auditoría en un mapa de parámetros y el mapa de parámetros con la acción inspeccionar se aplica en un mapa de políticas:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [parameter-map-name (optional)]
```

Drop logging está disponible para el tráfico que descarta el ZFW. Cuando agrega un registro con la acción de descartar en un policy-map, configura el registro de descarte:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

Editar mapa de clase y mapa de política de firewall de política de zona

Actualmente, ZFW no tiene un editor con el cual se puedan modificar las diversas estructuras de ZFW, como los policy-maps, class-maps y parameter-maps. Para reorganizar las sentencias de coincidencia en un class-map o la aplicación de una acción a varios class-maps contenidos dentro de un policy-map, se deben completar los siguientes pasos:

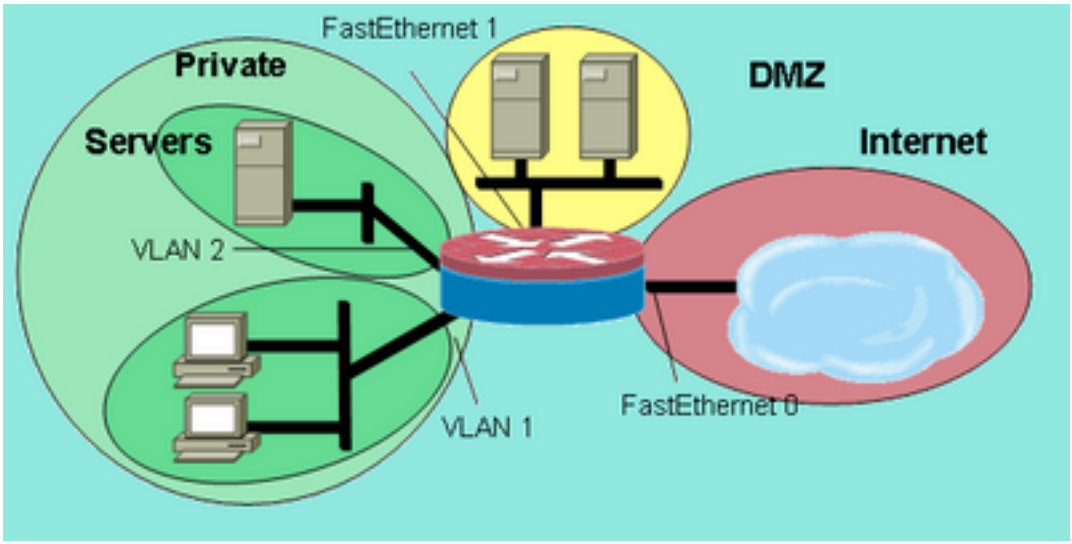
1. Copie la estructura actual en un editor de texto como el Bloc de notas de Microsoft Windows, o en un editor como vi en plataformas Linux/Unix.
2. Elimine la estructura actual de la configuración del router.
3. Modifique la estructura en el editor de texto.
4. Vuelva a copiar la estructura en la CLI del router.

Ejemplos de Configuración

En este ejemplo de configuración, se utiliza un router Cisco 1811 Integrated Services. En el Apéndice A, se encuentra disponible una configuración básica con conectividad IP, configuración VLAN y bridging transparente entre dos segmentos LAN de Ethernet privada. El router está separado en cinco zonas:

- La Internet pública está conectada a FastEthernet 0 (zona de Internet).
- Dos servidores de Internet están conectados a FastEthernet 1 (zona DMZ).
- El switch Ethernet está configurado con dos VLANs:Las estaciones de trabajo están conectadas a la VLAN1 (zona de clientes).Los servidores están conectados a la VLAN2 (zona de servidores).La zona de clientes y la de servidores están en la misma subred. Se aplica un firewall transparente entre las zonas, por lo que las políticas entre zonas en esas dos interfaces sólo pueden afectar al tráfico entre las zonas cliente y servidor.
- Las interfaces VLAN1 y VLAN2 se comunican con otras redes a través de la bridge virtual interface (BVI1). Esta interfaz se asigna a la zona privada. (Consulte la Figura 2).

Figura 2: Detalle de Topología de Zonas

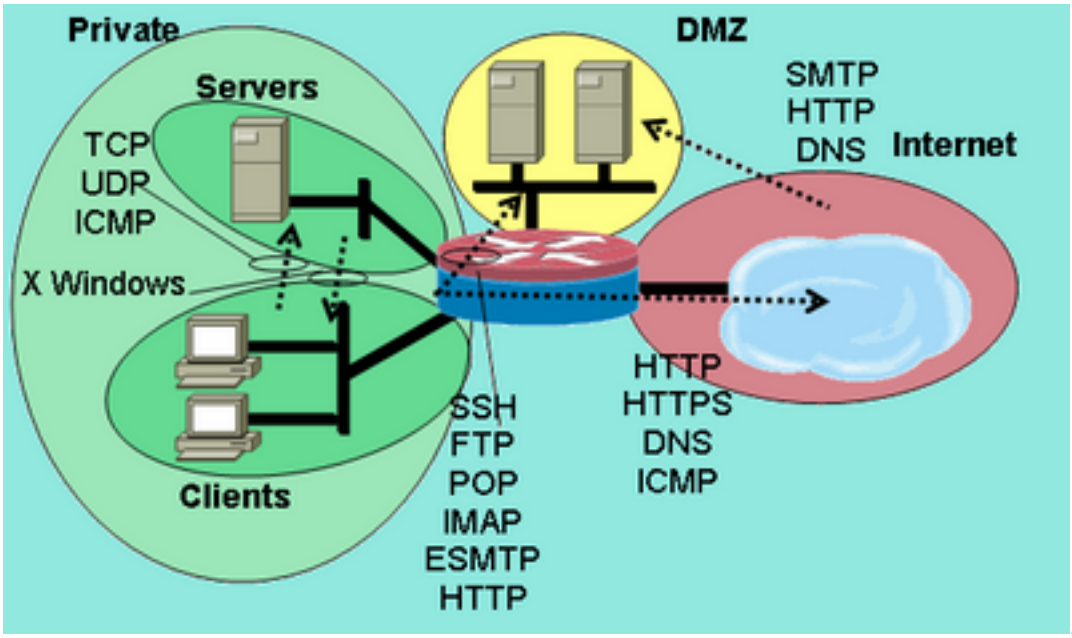


Detalle de Topología de Zonas

Estas políticas se aplican, con las zonas de red definidas anteriormente:

- Los hosts de la zona de Internet pueden alcanzar los servicios DNS, SMTP y SSH en un servidor de la DMZ. El otro servidor ofrece servicios SMTP, HTTP y HTTPS. La política de firewall restringe el acceso a los servicios específicos disponibles en cada host.
- Los hosts de la DMZ no se pueden conectar con los hosts de ninguna otra zona.
- Los hosts de la zona de clientes se pueden conectar con hosts de la zona de servidores en todos los servicios TCP, UDP e ICMP.
- Los hosts de la zona de servidores no se pueden conectar con hosts de la zona de clientes, excepto un servidor de aplicación basado en UNIX que puede abrir sesiones de clientes X Windows con servidores X Windows en equipos de escritorio de la zona de clientes, en los puertos 6900 a 6910.
- Todos los hosts de la zona privada (combinación de clientes y servidores) pueden acceder a los hosts de la DMZ en los servicios SSH, FTP, POP, IMAP, ESMTP y HTTP, y en la zona de Internet en los servicios HTTP, HTTPS y DNS y en ICMP. Además, la inspección de la aplicación se aplica en las conexiones HTTP de la zona privada a la zona de Internet para garantizar que las aplicaciones de IM y P2P admitidas no se transmiten en el puerto 80. (Consulte la figura 3.)

Figura 3: Permisos de Servicios del Zone-Pair para Aplicar en el Ejemplo de Configuración



Permisos de Servicios del Zone-Pair para Aplicar en el Ejemplo de Configuración

Estas políticas de firewall se configuran por orden de complejidad:

1. Inspección de clientes-servidores TCP/UDP/ICMP
2. Inspección de SSH/FTP/POP/IMAP/ESMTP/HTTP de Zona Privada-DMZ
3. Inspección restringida por direcciones de hosts de SMTP/HTTP/DNS de Internet-DMZ
4. Inspección X Windows de servidores-clientes con un servicio de Port-Application Mapping (PAM) especificado
5. HTTP/HTTPS/DNS/ICMP con inspección de aplicación HTTP de zona privada-Internet

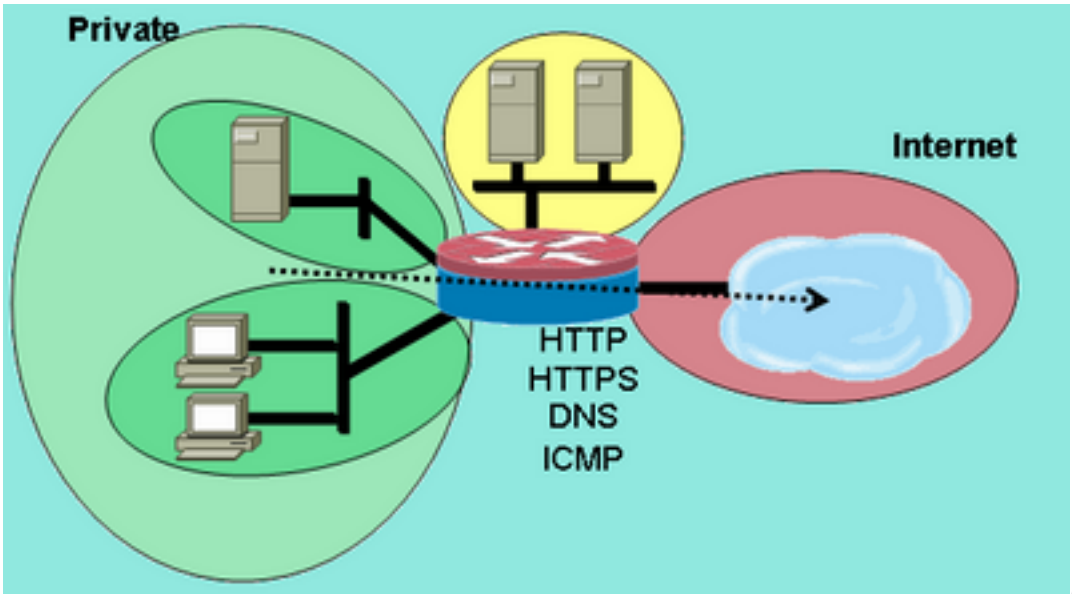
Dado que aplica partes de la configuración a diferentes segmentos de red en momentos diferentes, es importante recordar que un segmento de red pierde conectividad con otros segmentos cuando se coloca en una zona. Por ejemplo, cuando se configura la zona privada, los hosts de la zona privada pierden la conectividad con la DMZ y las zonas de Internet hasta que se definen sus respectivas políticas.

Firewall de routing con inspección activa

Configuración de la Política de Zona Privada-Internet

La figura 4 ilustra la configuración de la política de Internet privada.

Figura 4: Inspección de Servicios de la Zona Privada a la Zona de Internet



Inspección de Servicios de la Zona Privada a la Zona de Internet

La política de zona privada-Internet aplica la inspección de capa 7 a HTTP, HTTPS, DNS y la inspección de capa 4 a ICMP, de la zona privada a la zona de Internet. Esto permite conexiones desde la zona privada a la zona de Internet y permite el tráfico de retorno. La inspección de capa 7 conlleva las ventajas de un control más estricto de las aplicaciones, una mayor seguridad y compatibilidad con las aplicaciones que requieren reparación. Sin embargo, la inspección de la capa 7, como se ha mencionado, requiere una mejor comprensión de la actividad de la red, ya que los protocolos de la capa 7 que no están configurados para la inspección no están permitidos entre zonas.

1. Defina mapas de clase que describan el tráfico que desea permitir entre zonas, basándose en las políticas descritas anteriormente:
```
configure terminal
 class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```
2. Configure un policy-map para inspeccionar el tráfico en los class-maps que definió:
```
configure terminal
 policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
```
3. Configure las zonas privada y de Internet y asigne las interfaces del router a sus respectivas zonas:
```
configure terminal
 zone security private
 zone security internet
 int bvi1
  zone-member security private
 int fastethernet 0
  zone-member security internet
```

Configure el zone-pair y aplique el policy-map correspondiente.

> **Nota:** Solo necesita configurar el par de zonas de Internet privadas en este momento para inspeccionar las conexiones originadas en la zona privada que viaja a la zona de Internet, que se muestra a continuación:

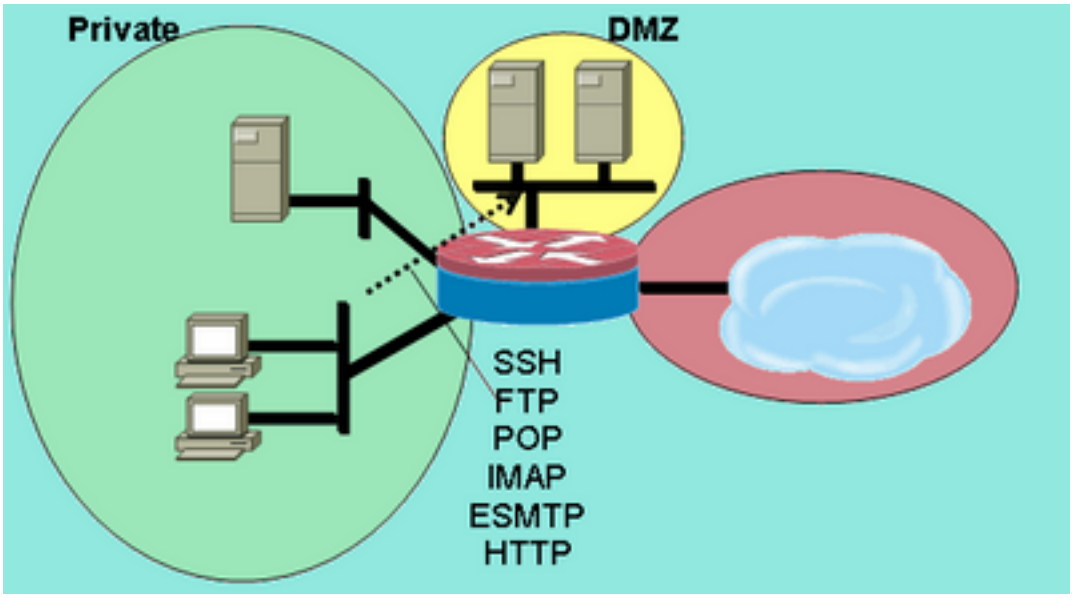
```
configure terminal
 zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```

Con esto se completa la configuración de la política de inspección de capa 7 en el zone-pair privada-Internet para permitir las conexiones HTTP, HTTPS, DNS e ICMP de la zona privada a la zona internet, y para aplicar la inspección de aplicaciones al tráfico HTTP a fin de garantizar que no se permita pasar el tráfico no deseado en TCP 80, el puerto de servicio de HTTP.

Configuración de la Política de Zona Privada-DMZ

La figura 5 muestra la configuración de la política de DMZ privada.

Figura 5: Inspección de Servicios de la Zona Privada a la Zona DMZ



Inspección de Servicios de la Zona Privada a la Zona DMZ

La política de zona privada-DMZ agrega complejidad porque requiere una mejor comprensión del tráfico de red entre zonas. Esta política aplica la inspección de capa 7 de la zona privada a la DMZ. Esto permite conexiones desde la zona privada a la DMZ y permite el tráfico de retorno. La inspección de capa 7 conlleva las ventajas de un control más estricto de las aplicaciones, una mayor seguridad y compatibilidad con las aplicaciones que requieren reparación. Sin embargo, la inspección de la capa 7, como se ha mencionado, requiere una mejor comprensión de la actividad de la red, ya que los protocolos de la capa 7 que no están configurados para la inspección no están permitidos entre zonas.

1. Defina mapas de clase que describan el tráfico que desea permitir entre zonas, basándose en las políticas descritas anteriormente:
   ```
   configure terminal
    class-map type inspect match-any L7-inspect-class
     match protocol ssh
     match protocol ftp
     match protocol pop
     match protocol imap
     match protocol esmtp
     match protocol http
   ```
2. Configure los policy-maps para inspeccionar el tráfico en los class-maps que definió:
   ```
   configure terminal
    policy-map type inspect private-dmz-policy
   ```

```
 class type inspect L7-inspect-class
  inspect
```

3. Configure las zonas privada y DMZ y asigne las interfaces del router a sus respectivas zonas:

```
configure terminal
 zone security private
 zone security dmz
 int bvi1
  zone-member security private
 int fastethernet 1
  zone-member security dmz
```

4. Configure el zone-pair y aplique el policy-map correspondiente.

   Nota: Solo necesita configurar el par de zonas DMZ privado en este momento para inspeccionar las conexiones originadas en la zona privada que viaja a la DMZ, que se muestra a continuación:

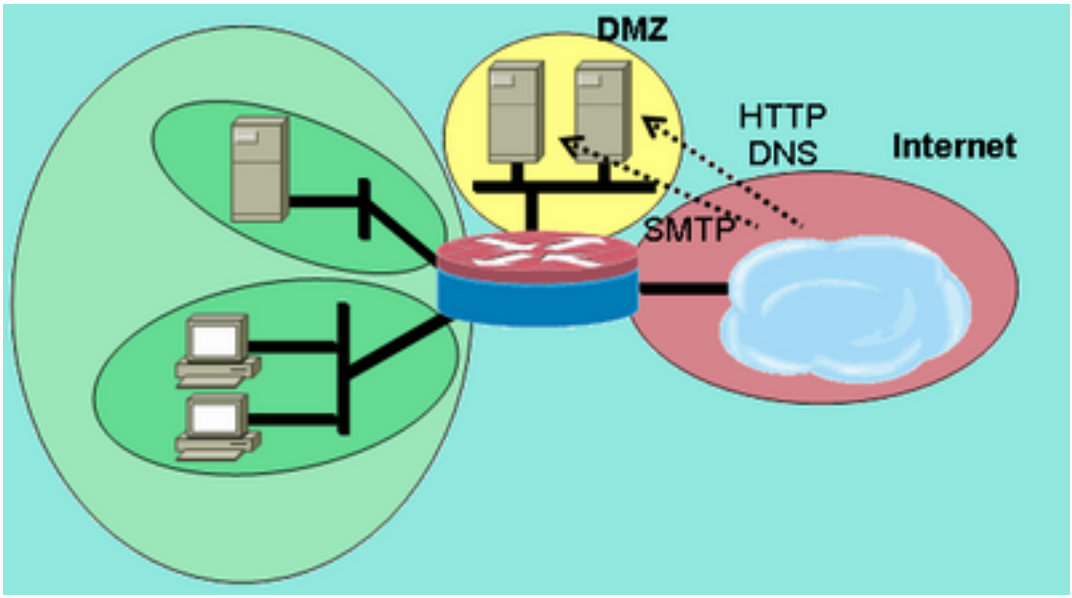
```
configure terminal
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```

Con esto se completa la configuración de la política de inspección de capa 7 de la DMZ a la zona privada para permitir todas las conexiones TCP, UDP e ICMP de la zona de clientes a la zona de servidores. La directiva no aplica correcciones para canales subordinados, pero proporciona un ejemplo de directiva simple para alojar la mayoría de las conexiones de aplicación.

Configuración de la Política de Internet-DMZ

La figura 6 muestra la configuración de la política DMZ de Internet.

Figura 6: Inspección de Servicios de la Zona de Internet a la Zona DMZ



Inspección de Servicios de la Zona de Internet a la Zona DMZ

Esta política aplica la inspección de capa 7 de la zona de Internet a la DMZ. Esto permite conexiones desde la zona de Internet a la DMZ y permite el tráfico de retorno desde los hosts DMZ a los hosts de Internet que originaron la conexión. La política de Internet-DMZ combina la inspección de capa 7 con los grupos de direcciones definidos por las ACL para restringir el acceso a servicios específicos en hosts específicos, grupos de hosts o subredes. Para ello, anide

un mapa de clase que especifique servicios dentro de otro mapa de clase que haga referencia a una ACL para especificar direcciones IP.

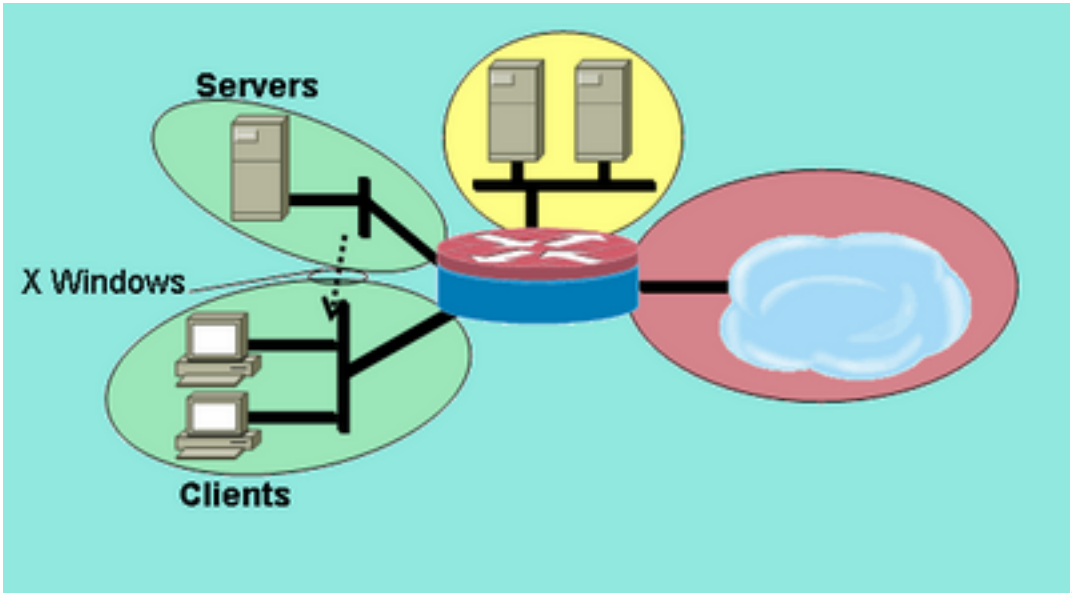
1. Defina mapas de clase y ACL que describan el tráfico que desea permitir entre las zonas, según las políticas descritas anteriormente.Se deben utilizar varios mapas de clase para los servicios, ya que se aplican diferentes políticas de acceso para el acceso a dos servidores diferentes. Los hosts de Internet tienen permitidas las conexiones DNS y HTTP a 172.16.2.2, y las conexiones SMTP a 172.16.2.3. Observe la diferencia en los class-maps. Los class-maps que especifican servicios utilizan la palabra clave match-any para permitir cualquiera de los servicios enumerados. Los class-maps que asocian las ACL con los class-maps de servicios utilizan la palabra clave match-all para requerir que se cumplan ambas condiciones en el class-map a fin de permitir el tráfico:
```
configure terminal
 access-list 110 permit ip any host 172.16.2.2
 access-list 111 permit ip any host 172.16.2.3
 class-map type inspect match-any dns-http-class
  match protocol dns
  match protocol http
 class-map type inspect match-any smtp-class
  match protocol smtp
 class-map type inspect match-all dns-http-acl-class
  match access-group 110
  match class-map dns-http-class
 class-map type inspect match-all smtp-acl-class
  match access-group 111
  match class-map smtp-class
```
2. Configure los policy-maps para inspeccionar el tráfico en los class-maps que definió:
```
configure terminal
 policy-map type inspect internet-dmz-policy
  class type inspect dns-http-acl-class
   inspect
  class type inspect smtp-acl-class
   inspect
```
3. Configure las zonas Internet y DMZ y asigne las interfaces del router a sus respectivas zonas. Omita la configuración de la DMZ si la configuró en la sección anterior:
```
configure terminal
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```
4. Configure el zone-pair y aplique el policy-map correspondiente.**Nota:** Sólo necesita configurar el par de zonas DMZ de Internet en este momento para inspeccionar las conexiones originadas en la zona de Internet que se desplaza a la zona DMZ, que se muestra a continuación:
```
configure terminal
 zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
```
Con esto se completa la configuración de la política de inspección de capa 7 de direcciones específicas en el zone-pair Internet-DMZ.

Firewall transparente con inspección activa

Configuración de la Política de Servidores-Clientes

La siguiente figura ilustra la configuración de la política de cliente-servidor.

Figura 7: Inspección de Servicios de la Zona de Servidores a la Zona de Clientes



Inspección de Servicios de la Zona de Servidores a la Zona de Clientes

La política de servidores-clientes aplica la inspección con un servicio definido por el usuario. La inspección de capa 7 se aplica de la zona de servidores a la zona de clientes. Esto permite conexiones X Windows a un rango de puertos específico desde la zona de servidores a la zona de clientes y permite el tráfico de retorno. X Windows no es un protocolo nativo compatible con PAM, por lo que se debe definir un servicio configurado por el usuario en PAM para que ZFW pueda reconocer e inspeccionar el tráfico apropiado.

Dos o más interfaces de router se configuran en un grupo de puentes IEEE para proporcionar Integrated Routing and Bridging (IRB) para proporcionar puentes entre las interfaces en el grupo de puentes y enrutar a otras subredes a través de la Interfaz virtual de puente (BVI). La política de firewall transparente aplica la inspección de firewall para el tráfico que "cruza el puente", pero no para el tráfico que sale del grupo de puentes a través de BVI. La política de inspección sólo se aplica al tráfico que cruza el bridge-group. Por lo tanto, en este escenario, la inspección sólo se aplica al tráfico que se mueve entre las zonas de clientes y servidores, que están anidadas dentro de la zona privada. La política aplicada entre la zona privada y las zonas pública y DMZ sólo interviene cuando el tráfico sale del bridge-group a través de la BVI. Cuando el tráfico sale a través de BVI desde las zonas de clientes o servidores, no se invoca la política de firewall transparente.

1. Configuración de PAM con una Entrada Definida por el Usuario para X WindowsLos clientes X de Windows (donde se alojan las aplicaciones) abren conexiones para mostrar información a los clientes (donde trabaja el usuario) en un intervalo que comienza en el puerto 6900.Cada conexión adicional utiliza puertos sucesivos, de modo que si un cliente muestra 10 sesiones diferentes en un host, el servidor utiliza los puertos 6900 a 6909. Por lo tanto, si inspecciona el rango de puertos de 6900 a 6909, las conexiones abiertas a los puertos más allá de 6909 fallan:
```
configure terminal
 ip port-map user-Xwindows port tcp from 6900 to 6910
```
2. Consulte los documentos de PAM para obtener respuestas a las preguntas adicionales sobre PAM o controle la documentación detallada sobre la inspección de protocolos para obtener información sobre los detalles de interoperabilidad entre PAM y la stateful inspection

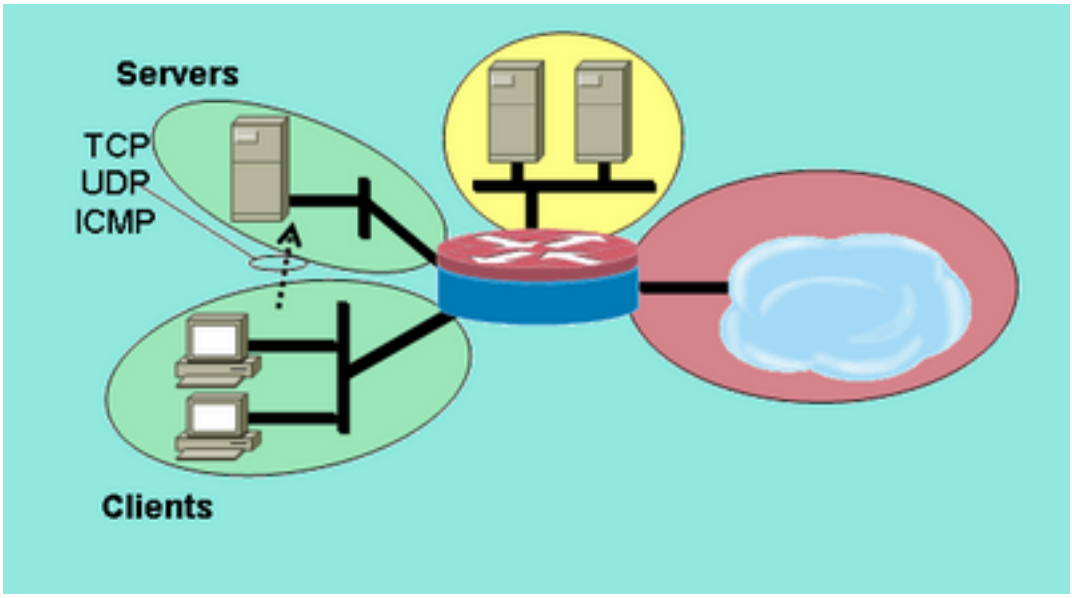
de Cisco IOS Firewall.

3. Defina mapas de clase que describan el tráfico que desea permitir entre zonas, basándose en las políticas descritas anteriormente:
```
configure terminal
 class-map type inspect match-any Xwindows-class
  match protocol user-Xwindows
```
4. Configure los policy-maps para inspeccionar el tráfico en los class-maps que definió:
```
configure terminal
 policy-map type inspect servers-clients-policy
  class type inspect Xwindows-class
   inspect
```
5. Configure la zona de clientes y la de servidores y asigne las interfaces del router a sus respectivas zonas.Si configuró esas zonas y asignó las interfaces en la sección Configuración de la Política de Clientes-Servidores, puede pasar a la definición del zone-pair. Para que la información esté completa, se proporciona la configuración de bridging IRB:
```
configure terminal
bridge irb
bridge 1 protocol ieee
bridge 1 route ip
zone security clients
zone security servers
 int vlan 1
 bridge-group 1
 zone-member security clients
int vlan 2
 bridge-group 1
 zone-member security servers
```
6. Configure el zone-pair y aplique el policy-map correspondiente.**Nota:** Solo necesita configurar el par de zona servidores-clientes actualmente para inspeccionar las conexiones originadas en la zona de servidores que viajan a la zona de clientes, que se muestra a continuación:
```
configure terminal
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```
Con esto se completa la configuración de la política de inspección definida por el usuario en el zone-pair servidores-clientes para permitir las conexiones X Windows de la zona de servidores a la zona de clientes.

Configuración de la Política de Clientes-Servidores

En la figura 8, se muestra la configuración de la política de clientes-servidores.

Figura 8: Inspección de Servicios de la Zona de Clientes a la Zona de Servidores



Inspección de Servicios de la Zona de Clientes a la Zona de Servidores

La política de clientes-servidores es menos compleja que las otras. La inspección de capa 4 se aplica de la zona de clientes a la zona de servidores. Esto permite conexiones desde la zona de clientes a la zona de servidores y permite el tráfico de retorno. La inspección de capa 4 ofrece la ventaja de la simplicidad de la configuración del firewall, ya que sólo se requieren algunas reglas para permitir el tráfico de la mayoría de las aplicaciones. Sin embargo, la inspección de capa 4 también tiene dos importantes desventajas:

- Las aplicaciones como FTP o los servicios multimedia negocian con frecuencia un canal subordinado adicional del servidor al cliente. Esta funcionalidad se acomoda generalmente en una corrección de servicio que monitorea el diálogo del canal de control y permite el canal subordinado. Esta capacidad no está disponible en la inspección de capa 4.
- La inspección de capa 4 permite casi todo el tráfico de la capa de aplicaciones. Si se debe controlar el uso de la red de modo que sólo algunas aplicaciones puedan atravesar el firewall, se debe configurar una ACL para el tráfico saliente a fin de limitar los servicios permitidos a través del firewall.

Ambas interfaces de router están configuradas en un grupo de puentes IEEE, por lo que esta política de firewall aplica una inspección de firewall transparente. Esta política se aplica en dos interfaces de un bridge group IP IEEE. La política de inspección sólo se aplica al tráfico que cruza el grupo de puentes. Esto explica por qué la zona de clientes y la de servidores se anidan dentro de la zona privada.

1. Defina mapas de clase que describan el tráfico que desea permitir entre zonas, basándose en las políticas descritas anteriormente:
```
configure terminal
 class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
```
2. Configure los policy-maps para inspeccionar el tráfico en los class-maps que definió:
```
configure terminal
 policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
```
3. Configure la zona de clientes y la de servidores y asigne las interfaces del router a las zonas respectivas:
```
configure terminal
```

```
zone security clients
zone security servers
interface vlan 1
 zone-member security clients
interface vlan 2
 zone-member security servers
```

4. Configure el zone-pair y aplique el policy-map correspondiente.**Nota:** Solo necesita configurar el par de zonas clientes-servidores en este momento para inspeccionar las conexiones originadas en la zona de clientes que viajan a la zona de servidores, que se muestra a continuación:

```
configure terminal
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```

Con esto se completa la configuración de la política de inspección de capa 4 del zone-pair clientes-servidores para permitir todas las conexiones TCP, UDP e ICMP de la zona de clientes a la zona de servidores. La directiva no aplica correcciones para los canales subordinados, pero proporciona un ejemplo de directiva simple para alojar la mayoría de las conexiones de aplicación.

Política de velocidad para firewall de políticas basadas en zonas

Las redes de datos a menudo se benefician de la capacidad de limitar la velocidad de transmisión de tipos específicos de tráfico de red y de limitar el impacto del tráfico de menor prioridad a un tráfico más esencial para la empresa. El software Cisco IOS ofrece esta capacidad con regulación del tráfico , que limita la velocidad nominal del tráfico y la ráfaga. Cisco IOS Software permite utilizar la regulación de tráfico desde Cisco IOS Release 12.1(5)T.

La versión 12.4(9)T del software del IOS de Cisco aumenta el ZFW con la limitación de velocidad cuando se agrega la capacidad para supervisar el tráfico que corresponde a las definiciones de un mapa de clase específico cuando atraviesa el firewall de una zona de seguridad a otra. Esto ofrece la comodidad de un punto de configuración para describir el tráfico específico, aplicar la política de firewall y controlar el consumo de ancho de banda del tráfico. ZFW se diferencia de los servicios basados en interfaz en que sólo proporciona las acciones de transmisión para la conformidad de políticas y de eliminación para la violación de políticas. ZFW no puede marcar el tráfico para DSCP.

ZFW solo puede especificar el uso de ancho de banda en bytes/segundo, paquete/segundo y no se ofrece el porcentaje de ancho de banda. ZFW se puede aplicar con o sin interfaz. Por lo tanto, si se requieren capacidades adicionales, estas funciones se pueden aplicar mediante una interfaz. Si se utiliza basado en interfaz junto con firewall, asegúrese de que las políticas no entren en conflicto.

Configurar política ZFW

La regulación de ZFW limita el tráfico en un mapa de clase de policy-map a un valor de velocidad definido por el usuario entre 8.000 y 2.000.000.000 de bits por segundo, con un valor de ráfaga configurable en el rango de 1.000 a 512.000.000 de bytes.

En ZFW, la regulación se configura mediante una línea adicional de configuración en el policy-map, la cual se aplica después de la acción de la política:

```
policy-map type inspect private-allowed-policy
```

```
 class type inspect http-class
  inspect
  police rate [bps rate value <8000-2000000000>] burst [value in bytes <1000-512000000>]
```

Control de la sesión

La política ZFW también introdujo el control de sesión para limitar el recuento de sesiones para el tráfico en un policy-map que se aplica que coincide con un class-map. Esto se suma a la capacidad actual para aplicar la política de protección DoS por mapa de clase. Efectivamente, esto permite un control granular sobre el número de sesiones que se aplican que coincide con cualquier mapa de clase determinado que cruza un par de zonas. Si se utiliza el mismo class-map en varios policy-maps o zone-pair, se pueden aplicar diferentes límites de sesiones en las distintas aplicaciones de los class-maps.

El control de sesión se aplica cuando se configura un mapa de parámetro que contiene el volumen de sesión deseado, luego el mapa de parámetro se agrega a la acción de inspección aplicada a un mapa de clase en un mapa de política:

```
parameter-map type inspect my-parameters
 sessions maximum [1-2147483647]

policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters
```

Los mapas de parámetro sólo se pueden aplicar a la acción de inspección y no están disponibles en las acciones de pasar o colocar.

Las actividades de control y regulación de sesión de ZFW son visibles con este comando:

```
show policy-map type inspect zone-pair
```

Inspección de Aplicaciones

La inspección de aplicaciones introduce una capacidad adicional al ZFW. Las políticas de inspección de aplicaciones se aplican en la capa 7 del modelo de Interconexión de Sistema Abierto (OSI), donde las aplicaciones de usuario envían y reciben mensajes que permiten a las aplicaciones ofrecer capacidades útiles. Algunas aplicaciones pueden ofrecer capacidades no deseadas o vulnerables, por lo que los mensajes asociados a estas capacidades deben filtrarse para limitar las actividades en los servicios de la aplicación.

El ZFW de Cisco IOS Software ofrece control e inspección de aplicaciones en los siguientes servicios de aplicaciones:

- HTTP
- SMTP
- POP3
- IMAP
- Sun RPC
- Tráfico de Aplicaciones P2P
- Aplicaciones IM

La capacidad de Control e Inspección de Aplicaciones (AIC) varía según el servicio. La inspección

HTTP ofrece un filtrado granular de varios tipos de actividad de aplicaciones y proporciona funciones para limitar el tamaño de la transferencia, las longitudes de las direcciones web y la actividad del navegador para garantizar el cumplimiento de los estándares de comportamiento de las aplicaciones y limitar los tipos de contenido que se transfieren a través del servicio. El AIC para SMTP puede limitar la extensión del contenido y hacer cumplir las normas del protocolo. La inspección POP3 e IMAP puede ayudar a garantizar que los usuarios utilicen mecanismos de autenticación seguros para evitar que se comprometan las credenciales de los usuarios.

La inspección de aplicaciones se configura como un conjunto adicional de mapas de clase y mapas de políticas específicos de la aplicación, que se aplican a los mapas de clase y los mapas de políticas de inspección actuales cuando se define la política de servicio de aplicaciones en el mapa de políticas de inspección.

Inspección de Aplicaciones HTTP

La inspección de aplicaciones se puede aplicar en el tráfico HTTP para controlar el uso no deseado del puerto de servicio HTTP para otras aplicaciones como MI, intercambio de archivos P2P y aplicaciones de tunelización que pueden redirigir otras aplicaciones con firewall a través de TCP 80.

Configure un class-map de inspección de aplicaciones para describir el tráfico que infringe el tráfico HTTP permitido:

```
! configure the actions that are not permitted
class-map type inspect http match-any http-aic-cmap
 match request port-misuse any
 match req-resp protocol-violation
! define actions to be applied to unwanted traffic
policy-map type inspect http http-aic-pmap
 class type insp http http-aic-cmap
  reset
  log
! define class-map for stateful http inspection
class-map type inspect match-any http-cmap
 match protocol http
! define class-map for stateful inspection for other traffic
class-map type inspect match-any other-traffic-cmap
 match protocol smtp
 match protocol dns
 match protocol ftp
! define policy-map, associate class-maps and actions
policy-map type inspect priv-pub-pmap
 class type inspect http-cmap
  inspect
  service-policy http http-aic-pmap
 class type inspect other-traffic-cmap
  inspect
```

Mejoras de la Inspección de Aplicaciones HTTP

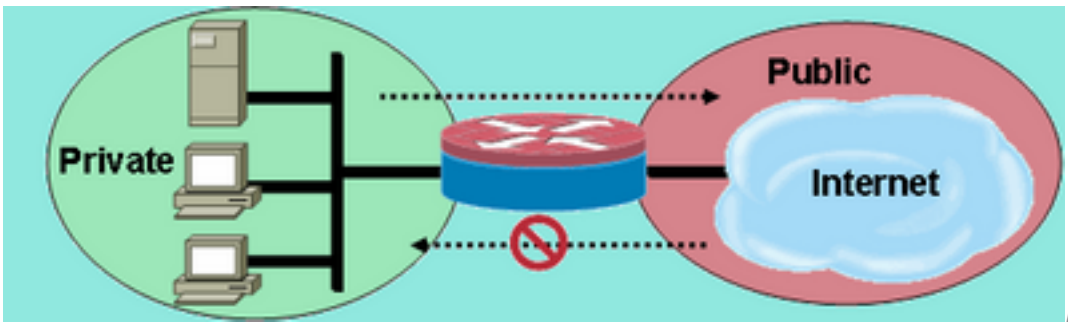
La versión 12.4(9)T del software del IOS de Cisco introduce mejoras en las capacidades de inspección HTTP de ZFW. En Cisco IOS Firewall, se introdujo la inspección de la aplicación HTTP en Cisco IOS Software Release 12.3(14)T. La versión 12.4(9)T del software del IOS de Cisco aumenta las capacidades actuales al agregar:

- Capacidad de permitir, denegar y supervisar peticiones y respuestas según los nombres de

encabezado y valores de encabezado. Esto es útil para bloquear peticiones y respuestas que tengan campos de encabezado vulnerables.
- Capacidad para limitar los tamaños de los diferentes elementos de los encabezados de solicitud y respuesta HTTP, como la longitud máxima de URL, la longitud máxima de encabezado, el número máximo de encabezados, la longitud máxima de línea de encabezado, etc. Resulta útil para evitar desbordamientos de búfer.
- Capacidad de bloquear peticiones y respuestas que tienen varios encabezados del mismo tipo; por ejemplo, una petición con dos encabezados de extensión de contenido.
- Capacidad de bloquear peticiones y respuestas con encabezados que contienen caracteres que no sean ASCII. Esto es útil para evitar diversos ataques que utilizan caracteres binarios y otros caracteres que no son ASCII a fin de enviar gusanos y otros contenidos maliciosos a los servidores web.
- Capacidad de agrupar métodos HTTP en categorías especificadas por el usuario y flexibilidad para bloquear, permitir y supervisar cada método del grupo que se ofrece. El HTTP RFC permite un grupo restringido de métodos HTTP. Algunos de los métodos estándar no se consideran seguros, ya que pueden utilizarse para aprovechar las vulnerabilidades de un servidor web. Muchos de los métodos no estándares no tienen un buen registro de seguridad.
- Método para bloquear Identificadores Uniformes de Recursos (URI) específicos según una regular expression configurada por el usuario. Esta función permite al usuario bloquear URI y consultas personalizadas.
- Capacidad de simular tipos de encabezado (spoofing) (especialmente el tipo de encabezado de servidores) con cadenas de caracteres (strings) personalizadas por el usuario. Esto es útil cuando un atacante analiza las respuestas de un servidor web, obtiene toda la información posible y luego ejecuta un ataque que aprovecha las debilidades de ese servidor web determinado.
- Capacidad de bloquear una conexión HTTP, o enviar una alerta sobre ella, si uno o más valores de los parámetros HTTP coinciden con los valores ingresados por el usuario como regular expression. Entre los posibles contextos de valores HTTP se incluyen el encabezado, el cuerpo, el nombre de usuario, la contraseña, el agente de usuario, la línea de petición, la línea de estado y las variables decodificadas de la Interfaz de Gateway Común (CGI).

Los ejemplos de configuración para las mejoras en la inspección de aplicaciones HTTP suponen una red sencilla, como se muestra en la figura 9.

Figura 9: Inspección de aplicaciones Suponga una red sencilla



Inspección de aplicaciones Suponga una red sencilla

El firewall agrupa el tráfico en dos clases:

- Tráfico HTTP
- Todo el resto del tráfico de canal único TCP, UDP e ICMP

El HTTP se separa para permitir la inspección específica del tráfico web. Esto permite configurar la regulación en la primera sección de este documento y la inspección de aplicaciones HTTP en la segunda sección. Puede configurar mapas de clase y mapas de políticas específicos para el tráfico P2P y MI en la tercera sección de este documento. Se permite la conectividad de la zona privada a la zona pública. No se proporciona conectividad de la zona pública a la zona privada.

Consulte el Apéndice C para obtener una configuración completa que implemente la política inicial.

Configurar mejoras en la inspección de aplicaciones HTTP

La inspección de aplicaciones HTTP (al igual que otras políticas de inspección de aplicaciones) requiere una configuración más compleja que la configuración básica de capa 4. Se debe configurar la política y la clasificación de tráfico de capa 7 para reconocer el tráfico específico que se desea controlar y para aplicar la acción requerida al tráfico deseado y no deseado.

La inspección de aplicaciones HTTP (al igual que otros tipos de inspección de aplicaciones) sólo se puede aplicar al tráfico HTTP. Por lo tanto, se deben definir los class-maps y los policy-maps de capa 7 para el tráfico HTTP específico, luego definir un class-map de capa 4 específicamente para HTTP y aplicar la política de capa 7 a la inspección HTTP en un policy-map de capa 4, de la siguiente forma:

```
!configure the layer-7 traffic characteristics:
class-map type inspect http match-any http-l7-cmap
 match  req-resp protocol-violation
 match  request body length gt 4096
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect http http-l7-pmap
 class type inspect http http-l7-cmap
  reset
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all http-l4-cmap
 match protocol http
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect http-l4-cmap
  inspect
  service-policy http http-l7-pmap
```

Todas estas funciones del tráfico de la inspección de aplicaciones HTTP se definen en un class-map de capa 7:

- El comando de inspección de encabezado proporciona la capacidad de permitir/denegar/supervisar solicitudes o respuestas cuyo encabezado coincida con la expresión regular configurada. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:
  `APPFW-6-HTTP_HDR_REGEX_MATCHED`
  Uso de Comandos:

```
match {request|response|req-resp} header regex <parameter-map-name>
```

Ejemplo de Caso de Uso

- Configure una política http appfw para bloquear las peticiones o respuestas cuyos encabezados contengan caracteres que no son ASCII.

```
parameter-map type regex non_ascii_regex
   pattern “[^\x00-\x80]”
class-map type inspect http non_ascii_cm
   match req-resp header regex non_ascii_regex
policy-map type inspect http non_ascii_pm
   class type inspect http non_ascii_cm
      reset
```

Header length inspection: Este comando controla la extensión del encabezado de una petición o respuesta y aplica la acción si la extensión excede el umbral configurado. Se permite la acción o el restablecimiento. Si se agrega la acción Log, se genera un mensaje syslog:

```
APPFW-4- HTTP_HEADER_LENGTH
```

Uso de Comandos:

```
match {request|response|req-resp} header length gt <bytes>
```

Ejemplo de Caso de Uso

Configure una política de aplicación http para bloquear solicitudes y respuestas que tengan una longitud de encabezado mayor que 4096 bytes.

```
class-map type inspect http hdr_len_cm
   match req-resp header length gt 4096

policy-map type inspect http hdr_len_pm
   class type inspect http hdr_len_cm
      reset
```

Header count inspection: Este comando verifica la cantidad de líneas de encabezado (campos) de una petición o respuesta y aplica una acción cuando el conteo excede el umbral configurado. Se permite la acción o el restablecimiento. Si se agrega la acción Log, se genera un mensaje syslog:

```
APPFW-6- HTTP_HEADER_COUNT
```

Uso de Comandos:

```
match {request|response|req-resp} header count gt <number>
```

Ejemplo de Caso de Uso

Configure una política http appfw para bloquear una petición que tenga más de 16 campos de encabezado.

```
class-map type inspect http hdr_cnt_cm
   match request header count gt 16
```

```
policy-map type inspect http hdr_cnt_pm
   class type inspect http hdr_cnt_cm
      reset
```

Header field inspection: Este comando proporciona la capacidad de permitir, denegar y supervisar peticiones y respuestas que contengan un valor y un campo de encabezado HTTP específico. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:

```
APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED
```

Uso de Comandos:

```
match {request|response|req-resp} header <header-name>
```

Ejemplo de Caso de Uso

Configure una política de inspección de aplicaciones http para bloquear el spyware y el adware:

```
parameter-map type regex ref_regex
   pattern “\.delfinproject\.com”
   pattern “\.looksmart\.com”

parameter-map type regex host_regex
   pattern “secure\.keenvalue\.com”
   pattern “\.looksmart\.com”

parameter-map type regex usragnt_regex
   pattern “Peer Points Manager”

class-map type inspect http spy_adwr_cm
   match request header refer regex ref_regex
   match request header host regex host_regex
   match request header user-agent regex usragnt_regex

policy-map type inspect http spy_adwr_pm
   class type inspect http spy_adwr_cm
      reset
```

Header field length inspection: Este comando proporciona la capacidad de limitar la extensión de una línea de campo de encabezado. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:

```
APPFW-6- HTTP_HDR_FIELD_LENGTH
```

Uso de Comandos:

```
match {request|response|req-resp} header <header-name> length gt <bytes>
```

Ejemplo de Caso de Uso

Configure una política http appfw para bloquear una petición cuya cookie y extensión del campo agente de usuario excedan 256 y 128, respectivamente.

```
class-map type inspect http hdrline_len_cm
   match request header cookie length gt 256
```

```
   match request header user-agnet length gt 128

policy-map type inspect http hdrline_len_pm
   class type inspect http hdrline_len_cm
      reset
```

Inspection of header field repetition: Este comando controla si una petición o respuesta tiene campos de encabezado repetidos. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se activa la acción Registrar, se genera un mensaje syslog:

```
APPFW-6- HTTP_REPEATED_HDR_FIELDS
```

Uso de Comandos:

```
match {request|response|req-resp} header <header-name>
```

Ejemplo de Caso de Uso

Configure una política http appfw para bloquear una petición o respuesta que tenga varias líneas de encabezado de extensión de contenido. Esta es una de las funciones más útiles utilizadas para prevenir el contrabando de sesiones .

```
class-map type inspect http multi_occrns_cm
   match req-resp header content-length count gt 1

policy-map type inspect http multi_occrns_pm
   class type inspect http multi_occrns_cm
      reset
```

- Method inspection: El HTTP RFC permite un grupo restringido de métodos HTTP. Sin embargo, incluso algunos de los métodos estándares no se consideran seguros, ya que se pueden utilizar para aprovechar las vulnerabilidades de un servidor web. Muchos de los métodos no estándares se utilizan frecuentemente para actividades maliciosas. Esto crea la necesidad de agrupar los métodos en diversas categorías y de que el usuario elija la acción para cada categoría. Este comando proporciona al usuario una forma flexible de agrupar los métodos en varias categorías, como métodos seguros, métodos no seguros, métodos webdav, métodos RFC y métodos extendidos. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:

```
APPFW-6-HTTP_METHOD
```

Uso de Comandos:

```
match request method <method>
```

Ejemplo de Caso de Uso

Configure una política http appfw que agrupe los métodos HTTP en tres categorías: seguros, no seguros y webdav. Estos se muestran en la tabla siguiente. Configure acciones de modo que:

- Se permitan todos los métodos seguros sin log.
- Se permitan todos los métodos no seguros con log.
- Se bloqueen todos los métodos webdav con log.

Seguridad	No Seguros	WebDAV
GET, HEAD, OPTION	POST, PUT, CONNECT, TRACE	BCOPY, BELIMINAR, BMOVE

```
http policy:

class-map type inspect http safe_methods_cm
   match request method get
   match request method head
   match request method option

class-map type inspect http unsafe_methods_cm
   match request method post
   match request method put
   match request method connect
   match request method trace

class-map type inspect http webdav_methods_cm
   match request method bcopy
   match request method bdelete
   match request method bmove

policy-map type inspect http methods_pm
   class type inspect http safe_methods_cm
      allow
   class type inspect http unsafe_methods_cm
      allow log
      class type inspect http webdav_methods_cm
      reset log
```

URI inspection: Este comando proporciona la capacidad de permitir, denegar y supervisar peticiones cuyos URI coincidan con la inspección normal configurada. Esto permite al usuario bloquear las consultas y los URLs personalizados. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:

```
APPFW-6- HTTP_URI_REGEX_MATCHED
```

Uso de Comandos:

```
match request uri regex <parameter-map-name>
```

Ejemplo de Caso de Uso

Configure una política http appfw para bloquear una petición cuyo URI coincida con alguna de las siguientes regular expressions:

- .* cmd. exe
- .*sex
- .*gambling

```
parameter-map type regex uri_regex_cm
   pattern “.*cmd.exe”
   pattern “.*sex”
   pattern “.*gambling”

class-map type inspect http uri_check_cm
   match request uri regex uri_regex_cm
```

```
policy-map type inspect http uri_check_pm
   class type inspect http uri_check_cm
      reset
```

- Inspección de longitud de URI: este comando verifica la longitud del URI que se envía en una solicitud y aplica la acción configurada cuando la longitud supera el umbral configurado. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:
  `APPFW-6- HTTP_URI_LENGTH`
  Uso de Comandos:
  `match request uri length gt <bytes>`
  Ejemplo de Caso de Uso

Configure una política http appfw para emitir una alarma cuando la extensión del URI de una petición exceda los 3076 bytes.

```
class-map type inspect http uri_len_cm
   match request uri length gt 3076

policy-map type inspect http uri_len_pm
   class type inspect http uri_len_cm
      log
```

Argument inspection: Este comando proporciona la capacidad de permitir, denegar o supervisar peticiones cuyos argumentos (parámetros) coincidan con la inspección normal configurada. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:

```
APPFW-6- HTTP_ARG_REGEX_MATCHED
```

Uso de Comandos:

```
match request arg regex <parameter-map-name>
```

Configure una política http appfw para bloquear una petición cuyos argumentos coincidan con alguna de las siguientes regular expression:

- .*codered
- .*attack

```
parameter-map type regex arg_regex_cm
   pattern “.*codered”
   pattern “.*attack”

class-map type inspect http arg_check_cm
   match request arg regex arg_regex_cm

policy-map type inspect http arg_check_pm
   class type inspect http arg_check_cm
      reset
```

- Inspección de longitud de argumentos: este comando verifica la longitud de los argumentos que se envían en una solicitud y aplica la acción configurada cuando la longitud supera el umbral configurado. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:

APPFW-6- HTTP_ARG_LENGTH

Uso de Comandos:

```
match request arg length gt <bytes>
```

Ejemplo de Caso de Uso

Configure una política http appfw para emitir una alarma cuando la extensión del argumento de una petición exceda los 512 bytes.

```
class-map type inspect http arg_len_cm
   match request arg length gt 512

policy-map type inspect http arg_len_pm
   class type inspect http arg_len_cm
      log
```

- Body inspection: Esta CLI permite al usuario especificar una lista de regular expressions con las cuales debe coincidir el cuerpo de la petición o respuesta. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:

  APPFW-6- HTTP_BODY_REGEX_MATCHED

  Uso de Comandos:

  ```
  match {request|response|reg-resp} body regex <parameter-map-name>
  ```

  Ejemplo de Caso de Uso

Configure una aplicación http para bloquear una respuesta cuyo cuerpo contenga el patrón `.*[Aa][Tt][Tt][Aa][Cc][Kk]`

```
parameter-map type regex body_regex
   pattern “.*[Aa][Tt][Tt][Aa][Cc][Kk]”

class-map type inspect http body_match_cm
   match response body regex body_regex

policy-map type inspect http body_match_pm
   class type inspect http body_match_cm
      reset
```

Inspección de longitud del cuerpo (contenido): este comando verifica el tamaño del mensaje que se envía mediante solicitud o respuesta. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:

```
APPFW-4- HTTP_CONTENT_LENGTH
```

Uso de Comandos:

```
match {request|response|req-resp} body length lt <bytes> gt <bytes>
```

Ejemplo de Caso de Uso

Configure una política http appfw para bloquear una sesión http que tenga un mensaje de más de 10K bytes en una petición o respuesta.

```
class-map type inspect http cont_len_cm
   match req-resp header content-length gt 10240

policy-map type inspect http cont_len_pm
```

```
   class type inspect http cont_len_cm
      reset
```

Status line inspection: Este comando permite al usuario especificar una lista de regular expressions con las cuales debe coincidir la línea de estado de una respuesta. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:

```
APPFW-6-HTTP_STLINE_REGEX_MATCHED
```

Uso de Comandos:

```
match response status-line regex <class-map-name>
```

Ejemplo de Caso de Uso

Configure una política http appfw para registrar una alarma cuando se intenta acceder a una página prohibida. Una página prohibida suele contener un código de estado 403 y la línea de estado es similar a `HTTP/1.0 403 page forbidden\r\n`.

```
parameter-map type regex status_line_regex
   pattern “[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403”

class-map type inspect http status_line_cm
   match response status-line regex status_line_regex

policy-map type inspect http status_line_pm
   class type inspect http status_line_cm
      log
```

- Content-type inspection: Este comando verifica si el tipo de contenido del encabezado del mensaje está en la lista de tipos de contenido soportados. También verifica que el tipo de contenido del encabezado coincida con el contenido de la parte del cuerpo de la entidad o de los datos del mensaje. Si se configura la palabra clave mismatch, el comando verifica el tipo de contenido del mensaje de respuesta con el valor de campo aceptado del mensaje de petición. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Registrar, se genera el mensaje syslog correspondiente:

  ```
  APPFW-4- HTTP_CONT_TYPE_VIOLATION
  APPFW-4- HTTP_CONT_TYPE_MISMATCH
  APPFW-4- HTTP_CONT_TYPE_UNKNOWN
  ```

  Uso de Comandos:

  ```
  match {request|response|req-resp} header content-type [mismatch|unknown|violation]
  ```

  Ejemplo de Caso de UsoConfigure una política de aplicación http para bloquear una sesión http que transporta solicitudes y respuestas que tienen un tipo de contenido desconocido.

  ```
  class-map type inspect http cont_type_cm
     match req-resp header content-type unknown

  policy-map type inspect http cont_type_pm
     class type inspect http cont_type_cm
        reset
  ```

Inspección de uso incorrecto del puerto: este comando se utiliza para evitar que el puerto http (80) se use incorrectamente para otras aplicaciones como IM, P2P, Tunelización , etc. Se puede aplicar la acción Permitir o restablecer a una solicitud o respuesta que coincida con los criterios del mapa de clase. Si se agrega la acción Registrar, se genera el mensaje syslog correspondiente:

```
APPFW-4- HTTP_PORT_MISUSE_TYPE_IM
APPFW-4-HTTP_PORT_MISUSE_TYPE_P2P
APPFW-4-HTTP_PORT_MISUSE_TYPE_TUNNEL
```

Uso de Comandos:

```
match request port-misuse {im|p2p|tunneling|any}
```

Ejemplo de Caso de Uso

Configure una política de aplicación http para bloquear una sesión http que se utiliza indebidamente para la aplicación IM.

```
class-map type inspect http port_misuse_cm
   match request port-misuse im

policy-map type inspect http port_misuse_pm
   class type inspect http port_misuse_cm
      reset
```

- Strict-http inspection: Este comando activa un control estricto de cumplimiento de protocolos de las peticiones y respuestas HTTP. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:
  ```
  APPFW-4- HTTP_PROTOCOL_VIOLATION
  ```
  Uso de Comandos:
  ```
  match req-resp protocol-violation
  ```
  Ejemplo de Caso de UsoConfigure una política de aplicación http para bloquear solicitudes o respuestas que violen RFC 2616:
  ```
  class-map type inspect http proto-viol_cm
     match req-resp protocol-violation

  policy-map type inspect http proto-viol_pm
     class type inspect http proto-viol_cm
        reset
  ```
- Inspección de transferencia y codificación: este comando proporciona la capacidad de permitir, denegar o supervisar solicitudes/respuestas cuyo tipo de codificación de transferencia coincida con el tipo configurado. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se agrega la acción Log, se genera un mensaje syslog:
  ```
  APPFW-6- HTTP_TRANSFER_ENCODING
  ```
  Uso de Comandos:
  ```
  match {request|response|req-resp} header transfer-encoding
  {regex <parameter-map-name> |gzip|deflate|chunked|identity|all}
  ```
  Ejemplo de Caso de UsoConfigure una política http appfw para bloquear una petición o respuesta que tenga una codificación de tipo compresión.
  ```
  class-map type inspect http trans_encoding_cm
     match req-resp header transfer-encoding type compress

  policy-map type inspect http trans_encoding_pm
     class type inspect http trans_encoding_cm
        reset
  ```
- Java Applet inspection: Este comando controla si una respuesta tiene un subprograma de Java y aplica la acción configurada al detectar el subprograma. La acción Allow o Reset se puede aplicar a una solicitud o respuesta que coincida con los criterios del class-map. Si se

agrega la acción Log, se genera un mensaje syslog:

```
APPFW-4- HTTP_JAVA_APPLET
```

Uso de Comandos:

```
match response body java-applet
```

Ejemplo de Caso de UsoConfigure una política http appfw para bloquear los applets de Java.

```
class-map type inspect http java_applet_cm
   match response body java-applet

policy-map type inspect http java_applet_pm
   class type inspect http java_applet_cm
      reset
```

Soporte de ZFW para el control de aplicaciones Instant-Messaging y Peer-to-Peer

Cisco IOS Software Release 12.4(9)T introdujo el soporte de ZFW con las aplicaciones IM y P2P.

Cisco IOS Software permitió por primera vez utilizar el control de aplicaciones IM en Cisco IOS Software Release 12.4(4)T. La versión inicial de ZFW no permitía utilizar las aplicaciones IM en la interfaz de ZFW. Si se deseaba utilizar el control de aplicaciones IM, los usuarios no podían migrar a la interfaz de configuración de ZFW. La versión 12.4(9)T del software del IOS de Cisco introduce el soporte ZFW para la inspección de IM, que soporta Yahoo! Messenger (YM), MSN Messenger (MSN) y AOL Instant Messenger (AIM). Cisco IOS Software Release 12.4(9)T es la primera versión de Cisco IOS Software que ofrece compatibilidad nativa con Cisco IOS Firewall para aplicaciones P2P de intercambio de archivos.

La inspección de IM y P2P ofrece políticas de capa 4 y de capa 7 para el tráfico de aplicaciones. Esto significa que ZFW puede proporcionar una inspección stateful básica para permitir o denegar el tráfico, así como un control granular de capa 7 sobre actividades específicas en los diversos protocolos, de modo que se permiten ciertas actividades de aplicación mientras que otras se deniegan.

Control e Inspección de Aplicaciones P2P

SDM 2.2 introdujo el control de aplicaciones P2P en la sección de configuración de firewall. SDM aplicó una política de QoS y reconocimiento de aplicaciones basadas en red (NBAR) para detectar y controlar la actividad de las aplicaciones P2P a una velocidad de línea de cero y para bloquear todo el tráfico P2P. Esto planteó el problema de que los usuarios de CLI, que esperaban compatibilidad P2P en la CLI del firewall de Cisco IOS, no podían configurar el bloqueo P2P en la CLI a menos que conocieran la configuración de NBAR/QoS necesaria. La versión 12.4(9)T del software del IOS de Cisco introduce el control P2P nativo en la CLI de ZFW para aprovechar NBAR con el fin de detectar la actividad de las aplicaciones P2P. Esta versión de software permite utilizar varios protocolos de aplicaciones P2P:

- BitTorrent
- eDonkey
- FastTrack
- Gnutella
- KaZaA/KaZaA2
- WinMX

Las aplicaciones P2P son especialmente difíciles de detectar debido al comportamiento de "cambio de puertos" (port-hopping) y otros trucos utilizados para evitar la detección, además de los problemas introducidos por los frecuentes cambios y actualizaciones de las aplicaciones P2P

que modifican los comportamientos de los protocolos. ZFW combina la inspección nativa con estado del firewall con las capacidades de reconocimiento de tráfico de NBAR para realizar el control de aplicaciones P2P en la interfaz de configuración del CPL de ZFW. El NBAR ofrece dos excelentes beneficios:

- Reconocimiento opcional de aplicaciones basado en la heurística para reconocer aplicaciones a pesar del comportamiento complejo y difícil de detectar.
- Infraestructura ampliable que ofrece un mecanismo de actualización para estar al día de las actualizaciones y modificaciones de protocolos

Configurar inspección P2P

Como se mencionó anteriormente, el control y la inspección de P2P ofrecen stateful inspection de capa 4 y control de aplicaciones de capa 7. La inspección de capa 4 se configura de manera similar a otros servicios de aplicación, si la inspección de los puertos de servicio de aplicación nativa es adecuada:

```
class-map type inspect match-any my-p2p-class
match protocol [bittorrent | edonkey | fasttrack | gnutella | kazaa | kazaa2 | winmx ]
[signature (optional)]
!
policy-map type inspect private-allowed-policy
 class type inspect my-p2p-class
  [drop | inspect | pass]
```

Tenga presente la opción signature en match-protocol adicional en service-name. Cuando se agrega la opción de firma al final de la instrucción match protocol, se aplica heurística NBAR al tráfico para buscar indicadores en el tráfico que indiquen actividad de aplicación P2P específica. Esto incluye los cambios de puertos y otros cambios del comportamiento de las aplicaciones para evitar la detección de tráfico. Este nivel de inspección de tráfico demanda una mayor utilización del CPU y reduce la capacidad de rendimiento de la red. Si no se aplica la opción de firma, el análisis heurístico basado en NBAR no se aplica para detectar el comportamiento de salto de puertos y el uso de la CPU no se ve afectado en la misma medida.

La inspección de servicios nativa tiene la desventaja de no poder mantener el control sobre las aplicaciones P2P en el caso de que la aplicación "cambie" a un puerto de origen y de destino no estándar, o si la aplicación se actualiza para comenzar su acción en un número de puerto no reconocido:

Aplicación	Puertos Nativos (reconocidos por la lista de PAM 12.4(15)T)
bittorrent	TCP 6881-6889
edonkey	TCP 4662
fasttrack	TCP 1214
gnutella	TCP 6346-6349 TCP 6355,5634 UDP 6346-6348
kazaa2	Dependiente de PAM
winmx	TCP 6699

Si desea permitir (inspeccionar) el tráfico P2P, puede que necesite proporcionar una configuración adicional. Algunas aplicaciones pueden utilizar varias redes P2P o implementar comportamientos específicos que se pueden tener en cuenta en la configuración del firewall para que la aplicación funcione:

- Los clientes BitTorrent generalmente se comunican con "rastreadores" (servidores de

directorio de peer) a través de http que se ejecuta en algún puerto no estándar. Esto es típicamente TCP 6969, pero puede necesitar verificar el puerto de seguimiento específico del torrent. Si desea permitir BitTorrent, el mejor método para acomodar el puerto adicional es configurar HTTP como uno de los protocolos de coincidencia y agregar TCP 6969 a HTTP con el comando ip port-map:

```
ip port-map http port tcp 6969
```

Debe definir http y bittorrent como los criterios de coincidencia aplicados en el mapa de clase.

- Aparentemente, eDonkey inicia conexiones que se detectan como eDonkey y Gnutella.
- La inspección de KaZaA depende completamente de la detección de NBAR signatures.

La inspección de la capa 7 (aplicaciones) aumenta la inspección de la capa 4 con la capacidad de reconocer y aplicar acciones específicas de servicios, como bloquear selectivamente o permitir funciones de búsqueda de archivos, transferencia de archivos y chat de texto. Las capacidades de servicios específicos varían según el servicio.

La inspección de aplicaciones P2P es similar a la inspección de aplicaciones HTTP:

```
!configure the layer-7 traffic characteristics:
class-map type inspect [p2p protocol] match-any p2p-l7-cmap
 match action
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect [p2p protocol] p2p-l7-pmap
 class type inspect p2p p2p-l7-cmap
  [ reset | allow ]
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all p2p-l4-cmap
 match protocol [p2p protocol]
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect p2p-l4-cmap
  [ inspect | drop | pass ]
  service-policy p2p p2p-l7-pmap
```

La inspección de aplicaciones P2P ofrece capacidades de aplicaciones específicas para un subgrupo de las aplicaciones que la inspección de capa 4 permite utilizar:

- edonkey
- fasttrack
- gnutella
- kazaa2

Cada una de estas aplicaciones ofrece opciones de criterios de coincidencia específicos de la aplicación:

edonkey

```
router(config)#class-map type inspect edonkey match-any edonkey-l7-cmap
router(config-cmap)#match ?
  file-transfer     Match file transfer stream
```

```
  flow              Flow based QoS parameters
  search-file-name  Match file name
  text-chat         Match text-chat
```

fasttrack

```
router(config)#class-map type inspect fasttrack match-any ftrak-l7-cmap
router(config-cmap)#match ?
  file-transfer  File transfer stream
  flow           Flow based QoS parameters
```

gnutella

```
router(config)#class-map type inspect gnutella match-any gtella-l7-cmap
router(config-cmap)#
```

kazaa2

```
router(config)#class-map type inspect kazaa2 match-any kazaa2-l7-cmap
router(config-cmap)#match ?
  file-transfer  Match file transfer stream
  flow           Flow based QoS parameters
```

Las nuevas definiciones de protocolo P2P o las actualizaciones de los protocolos P2P actuales se pueden cargar con la funcionalidad de actualización dinámica pdlm de NBAR. El siguiente es el comando de configuración para cargar el PDLM nuevo:

```
ip nbar pdlm <file-location>
```

El nuevo protocolo está disponible en los comandos match protocol para la inspección de tipo de clase. Si el protocolo P2P nuevo tiene servicios (subprotocolos), los nuevos tipos de class-maps de inspección de capa 7 y los criterios de coincidencia de capa 7 estarán disponibles.

Control e Inspección de Aplicaciones IM

Cisco IOS Software Release 12.4(4)T introdujo el control y la inspección de aplicaciones IM. La versión 12.4(6)T no permitía utilizar IM con ZFW, de modo que los usuarios no podían aplicar el control de IM y ZFW en la misma política de firewall, ya que ZFW y las funciones de firewall heredadas no pueden coexistir en una interfaz determinada.

Cisco IOS Software Release 12.4(9)T permite utilizar la stateful inspection y el control de aplicaciones para los siguientes servicios de IM:

- AOL Instant Messenger
- MSN Messenger
- Yahoo! Mensajería

La inspección de IM varía ligeramente con respecto a la mayoría de los servicios, ya que la inspección de IM controla el acceso a un grupo específico de hosts para cada servicio dado. Por lo general, los servicios de IM dependen de un grupo de servidores de directorios relativamente permanente, al cual los clientes se deben poder contactar para acceder al servicio de IM. Las aplicaciones de IM suelen ser muy difíciles de controlar desde el punto de vista de un servicio o un protocolo. La forma más efectiva de controlar estas aplicaciones es limitar el acceso a los servidores de IM fijos.

Configurar inspección de IM

La inspección y el control de IM ofrecen inspección stateful de capa 4

y control de aplicaciones de capa 7.

La inspección de capa 4 se configura de manera similar a otros servicios de aplicaciones:

```
class-map type inspect match-any my-im-class
match protocol [aol | msnmsgr | ymsgr ]
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  [drop | inspect | pass
```

Las aplicaciones de IM pueden contactarse con los servidores en varios puertos para mantener su funcionalidad. Para permitir un servicio de mensajería instantánea determinado con la acción de inspección, no puede necesitar una lista de servidores para definir el acceso permitido a los servidores del servicio de mensajería instantánea. Sin embargo, cuando configura un mapa de clase que especifica un servicio de mensajería instantánea determinado, como AOL Instant Messenger, y aplica la acción de descartar en el mapa de política asociado puede hacer que el cliente de mensajería instantánea intente localizar un puerto diferente donde se permita la conectividad a Internet. Si no se desea permitir la conectividad a un servicio determinado, o si se desea restringir la capacidad del servicio de IM a la conversación de texto, se debe definir una lista de servidores para que el ZFW pueda identificar el tráfico asociado con la aplicación de IM:

```
!configure the server-list parameter-map:
parameter-map type protocol-info <name>
  server name <name>
  server ip a.b.c.d
  server ip range a.b.c.d a.b.c.d
```

Por ejemplo, la lista de servidores de IM de Yahoo se define de la siguiente forma:

```
parameter-map type protocol-info ymsgr-pmap
  server name scs.msg.yahoo.com
  server name scsd.msg.yahoo.com
  server ip 10.0.77.88
  server ip range 172.16.0.77 172.16.0.99
```

Debe aplicar la lista de servidores a la definición de protocolo:

```
class-map type inspect match-any ym-l4-cmap
 match protocol ymsgr ymsgr-pmap
```

Debe configurar los comandos ip domain lookup e ip name-server ip.ad.re.ss para activar la resolución de nombres.

Los nombres de los servidores de IM son bastante dinámicos. Debe comprobar periódicamente que las listas de servidores de MI configuradas están completas y son correctas.

La inspección de la capa 7 (aplicaciones) aumenta la inspección de la capa 4 con la capacidad de reconocer y aplicar acciones específicas de servicios, como bloquear o permitir de forma selectiva funciones de chat de texto y denegar otras capacidades de servicios.

Actualmente, la inspección de aplicaciones de IM ofrece la capacidad de diferenciar entre la actividad de conversación de texto y todos los demás servicios de la aplicación. Para restringir la actividad de IM a la conversación de texto, configure una política de capa 7:

```
class-map type inspect ymsgr match-any ymsgr-text-cmap
  match service text-chat

class-map type inspect ymsgr match-any ymsgr-default-cmap
  match service any

policy-map type inspect im ymsgr-l7-pmap
  class type inspect im ymsgr-text-cmap
    allow
    [log]
  class type inspect im ymsgr-text-cmap
    reset
    [log]
```

Aplique la política de capa 7 a la política de Yahoo! Messenger configurada anteriormente:

```
class-map type inspect match-any my-im-class
match protocol ymsgr
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  inspect
  service-policy im ymsgr-l7-pmap
```

Filtros de URL

ZFW ofrece capacidades de filtrado de direcciones URL para limitar el acceso al contenido web según lo especificado en una lista blanca o negra definida en el router, o reenviar nombres de dominio a un servidor de filtrado de direcciones URL para verificar el acceso a dominios específicos. El filtrado de direcciones URL de ZFW en Cisco IOS Software Releases 12.4(6)T a 12.4(15)T se aplica como una acción de política adicional, similar a la inspección de aplicaciones.

Para el filtrado URL basado en el servidor, se debe definir un parameter-map que describa la configuración del servidor urlfilter:

```
parameter-map type urlfilter websense-parmap
 server vendor [n2h2 | websense] 10.1.1.1
```

Si se prefieren listas blancas o negras estáticas, se puede definir una lista de dominios o subdominios que se permitan o denieguen específicamente, mientras que la acción inversa se aplica al tráfico que no coincide con la lista:

```
parameter-map type urlfilter websense-parmap
 exclusive-domain deny .disallowed.com
 exclusive-domain permit .cisco.com
```

Si se define una lista negra de URL con opciones de denegación en las definiciones de dominio exclusivo, se permiten todos los demás dominios. Si se define alguna definición de "permit", todos los dominios permitidos deben especificarse explícitamente, de manera similar a la función de las listas de control de acceso IP.

Configure un mapa de clase que coincida con el tráfico HTTP:

```
class-map type inspect match-any http-cmap
 match protocol http
```

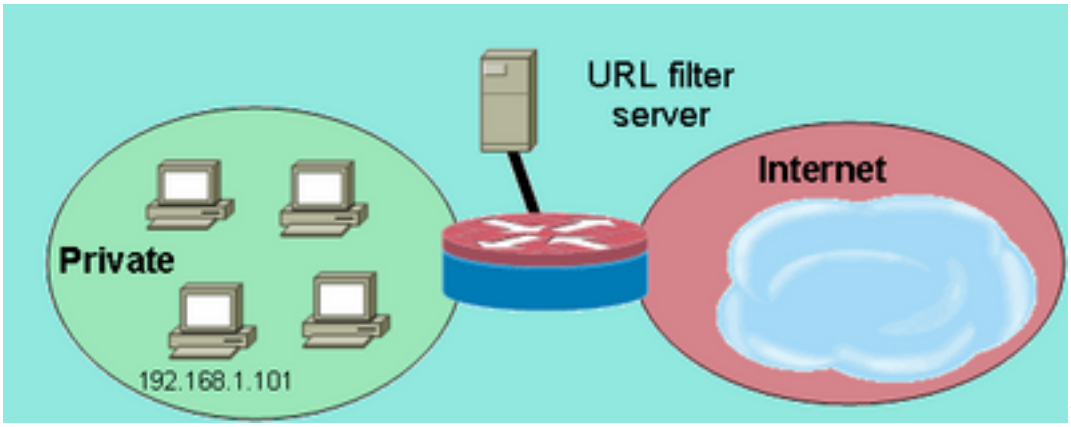
Defina un policy-map que asocie el class-map con las acciones inspect y urlfilter:

```
policy-map type inspect http-filter-pmap
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
```

Esto configura el requisito mínimo para comunicarse con un servidor de filtrado de direcciones URL. Existen varias opciones para definir un comportamiento adicional de filtrado de direcciones URL.

Algunas implementaciones de red desean aplicar el filtrado de URL para algunos hosts o subredes y omitir el filtrado de URL para otros hosts. Por ejemplo, en la figura 9, un servidor de filtrado de direcciones URL debe controlar el tráfico HTTP de todos los hosts de la zona privada, a excepción del host específico 192.168.1.101.

Figura 10: Topología de Ejemplo de Filtrado de Direcciones URL



Topología de Ejemplo de Filtrado de Direcciones URL

Esto se puede lograr si define dos mapas de clase diferentes:

- Un mapa de clase que sólo coincide con el tráfico HTTP para el grupo más grande de hosts, que reciben filtrado de URL.
- Un mapa de clase para el grupo más pequeño de hosts, que no reciben filtrado de URL. El segundo mapa de clase coincide con el tráfico HTTP, así como con una lista de hosts que están exentos de la política de filtrado de URL.

Ambos mapas de clase se configuran en un mapa de política, pero sólo uno recibe la acción urlfilter:

```
class-map type inspect match-any http-cmap
 match protocol http
class-map type inspect match-all http-no-urlf-cmap
 match protocol http
 match access-group 101
!
policy-map type inspect http-filter-pmap
 class type inspect http-no-urlf-cmap
  inspect
 class type inspect http-cmap
```

```
  inspect
  urlfilter websense-parmap
!
access-list 101 permit ip 192.168.1.101 any
```

Control del acceso al router

La mayoría de los ingenieros de seguridad de la red se sienten incómodos si exponen las interfaces de gestión del router (por ejemplo, SSH, Telnet, HTTP, HTTPS, SNMP, etc.) a la Internet pública y, en determinadas circunstancias, también se necesita control para el acceso LAN al router. Cisco IOS Software ofrece varias opciones para limitar el acceso a las distintas interfaces, las cuales incluyen la familia de características Network Foundation Protections (NFP), diversos mecanismos de control de acceso para las interfaces de administración y la self-zone de ZFW. Debe revisar otras funciones, como el control de acceso VTY, la protección del plano de administración y el control de acceso SNMP para determinar qué combinación de funciones de control del router funciona mejor para su aplicación específica.

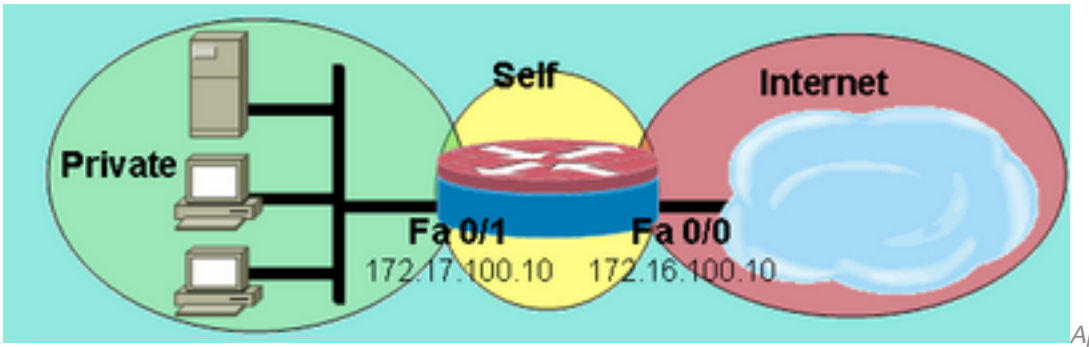
Por lo general, la familia de funciones de NFP es la mejor opción para el control del tráfico destinado al router. Consulte Descripción General de la Seguridad del Plano de Control en Cisco IOS Software para obtener información que describe la protección del router con las funciones NFP.

Si decide aplicar ZFW para controlar el tráfico hacia y desde las direcciones IP en el propio router, debe comprender que la política y las capacidades predeterminadas del firewall difieren de las disponibles para el tráfico de tránsito. El tráfico de tránsito se define como el tráfico de red cuyas direcciones IP de origen y destino no coinciden con ninguna dirección IP aplicada a ninguna de las interfaces del router, y el tráfico no hace que el router envíe, por ejemplo, mensajes de control de red tales como vencimiento ICMP TTL o mensajes de red/host inalcanzable.

ZFW aplica una política de denegación de todo predeterminada al tráfico que se mueve entre zonas, excepto, como se menciona en las reglas generales, que el tráfico en cualquier zona que fluye directamente a las direcciones de las interfaces del router está permitido implícitamente. Esto garantiza que se mantenga la conectividad a las interfaces de administración del router cuando se aplica una configuración de firewall por zonas al router. Si la misma política de deny-all afectara la conectividad directa al router, se debería aplicar una configuración de política de administración completa antes de configurar las zonas en el router. Es probable que esto afecte la conectividad de administración si la política no se implementa apropiadamente o no se aplica en el orden correcto.

Cuando se configura una interfaz para ser miembro de una zona, los hosts conectados con la interfaz se incluyen en la zona. Sin embargo, el tráfico que fluye hacia y desde las direcciones IP de las interfaces del router no está controlado por las políticas de zona (con la excepción de las circunstancias descritas en la nota de la figura 10). En su lugar, todas las interfaces IP del router se convierten automáticamente en parte de la zona automática cuando se configura ZFW. Para controlar el tráfico IP que se desplaza a las interfaces del router desde las distintas zonas de un router, deben aplicarse políticas para bloquear o permitir/inspeccionar el tráfico entre la zona y la zona autónoma del router, y viceversa (consulte la figura 11).

Figura 11: Aplicación de políticas entre zonas de red y zona automática del router



Aplicación de políticas entre zonas de red y zona automática del router

Aunque el router ofrece una política predeterminada de permitir entre todas las zonas y la zona automática, si se configura una política desde cualquier zona a la zona automática y no se configura ninguna política desde sí mismo a las zonas conectadas por interfaz configurables por el usuario del router, todo el tráfico originado por el router encuentra la política de zona conectada a zona automática cuando devuelve el router y se bloquea. Por lo tanto, se debe inspeccionar el tráfico originado en el router para permitir su retorno a la zona automática.

> **Nota:** Cisco IOS Software siempre utiliza la dirección IP asociada con la interfaz "más cercana" a los hosts de destino para el tráfico como syslog, tftp, Telnet y otros servicios de planos de control, y somete este tráfico a la política de firewall de la self zone. Sin embargo, si un servicio define una interfaz específica como la interfaz de origen con comandos que incluyen, entre otros, logging source-interface [número de tipo] , ip tftp source-interface [número de tipo] e ip telnet source-interface [número de tipo] , el tráfico se somete a la zona automática.

> **Nota**: algunos servicios (especialmente los servicios de voz sobre IP de los routers) utilizan interfaces efímeras o no configurables que no se pueden asignar a zonas de seguridad. Estos servicios no pueden funcionar correctamente si su tráfico no se puede asociar a una zona de seguridad configurada.

Limitaciones de la Política de Self Zone

La política de self zone tiene una funcionalidad limitada en comparación con las políticas disponibles para los zone-pairs de tráfico en tránsito:

- Al igual que ocurría con la stateful inspection clásica, el tráfico generado por el router está limitado a TCP, UDP, ICMP y la inspección de protocolos complejos para H.323.
- La inspección de aplicaciones no está disponible para las políticas de self zone.
- La limitación de sesión y velocidad no se puede configurar en las políticas de self zone.

Configuración de la Política de Self Zone

En la mayoría de las circunstancias, se recomiendan las siguientes políticas de acceso para los servicios de administración de routers:

- Niegue toda la conectividad Telnet, ya que el protocolo de texto sin encriptar de Telnet expone fácilmente las credenciales de usuario y otros datos confidenciales.
- Permita las conexiones de Secure Shell (SSH) de cualquier usuario en cualquier zona. SSH encripta las credenciales de usuario y los datos de sesión, lo cual brinda protección contra

usuarios maliciosos que utilicen herramientas de captura de paquetes para indagar la actividad del usuario y comprometer las credenciales de usuario u otros datos confidenciales, como la configuración del router. La versión 2 de SSH proporciona una mayor protección y aborda vulnerabilidades específicas inherentes a la versión 1 de SSH.
- Permita la conectividad HTTP al router desde las zonas privadas si la zona privada es de confianza. De lo contrario, si la zona privada alberga la posibilidad de que los usuarios malintencionados pongan en peligro la información, HTTP no utiliza cifrado para proteger el tráfico de gestión y puede revelar información confidencial como las credenciales o la configuración del usuario.
- Permita la conectividad HTTPS desde cualquier zona. Al igual que SSH, HTTPS encripta los datos de sesión y las credenciales de usuario.
- Restrinja el acceso SNMP a una subred o un host específicos. SNMP se puede utilizar para modificar la configuración del router y revelar información sobre la configuración. SNMP se debe configurar con control de acceso en las diversas comunidades.
- Bloquee las solicitudes ICMP de la Internet pública a la dirección de la zona privada (se supone que la dirección de la zona privada es enrutable). Una o más direcciones públicas se pueden exponer para el tráfico ICMP para la resolución de problemas de red, si es necesario. Se pueden utilizar varios ataques de ICMP para saturar los recursos de router o reconocer la topología y la arquitectura de la red.

Un router puede aplicar este tipo de política con la incorporación de dos zone-pairs para cada zona que se debe controlar. Cada par de zonas para el tráfico entrante o saliente desde la zona automática del router debe corresponderse con la política respectiva en la dirección opuesta, a menos que el tráfico no se origine en la dirección opuesta. Se puede aplicar un policy-map para los zone-pairs entrantes y salientes, en el cual se describa todo el tráfico, o se pueden aplicar policy-maps específicos para cada zone-pair. La configuración de pares de zonas específicos por policy-map proporciona granularidad para ver la actividad que coincide con cada policy-map.

Una red de ejemplo con una estación de administración SNMP en 172.17.100.11 y un servidor TFTP en 172.17.100.17, este resultado proporciona un ejemplo de la política de acceso de la interfaz de administración completa:

```
class-map type inspect match-any self_service-cmap
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol h323
!
class-map type inspect match-all to-self-cmap
 match class-map self_service-cmap
 match access-group 120
!
class-map type inspect match-all from-self-cmap
 match class-map self_service-cmap
!
class-map type inspect match-all tftp-in-cmap
 match access-group 121
!
class-map type inspect match-all tftp-out-cmap
 match access-group 122
!
policy-map type inspect to-self-pmap
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
```

```
  pass
!
policy-map type inspect from-self-pmap
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
zone security private
zone security internet
zone-pair security priv-self source private destination self
 service-policy type inspect to-self-pmap
zone-pair security net-self source internet destination self
 service-policy type inspect to-self-pmap
zone-pair security self-priv source self destination private
 service-policy type inspect from-self-pmap
zone-pair security self-net source self destination internet
 service-policy type inspect from-self-pmap

!
interface FastEthernet 0/0
 ip address 172.16.100.10
 zone-member security internet
!
interface FastEthernet 0/1
 ip address 172.17.100.10
 zone-member security private
!
access-list 120 permit icmp 172.17.100.0 0.0.0.255 any
access-list 120 permit icmp any host 172.17.100.10 echo
access-list 120 deny icmp any any
access-list 120 permit tcp 172.17.100.0 0.0.0.255 host 172.17.100.10 eq www
access-list 120 permit tcp any any eq 443
access-list 120 permit tcp any any eq 22
access-list 120 permit udp any host 172.17.100.10 eq snmp
access-list 121 permit udp host 172.17.100.17 host 172.17.100.10
access-list 122 permit udp host 172.17.100.10 host 172.17.100.17
```

Lamentablemente, la política de self zone no ofrece la capacidad de inspeccionar las transferencias TFTP. Por lo tanto, el firewall debe pasar todo el tráfico desde y hacia el servidor TFTP si el TFTP debe pasar a través del firewall.

Si el router finaliza las conexiones VPN IPSec, también debe definir una política para pasar IPSec ESP, IPSec AH, ISAKMP y NAT-T IPSec (UDP 4500). Esto depende de qué servicios utilice y cuáles son necesarios. Esta siguiente política se puede aplicar además de la política anterior. Observe el cambio en los policy-maps donde se ha insertado un class-map para el tráfico VPN con una acción pass. Por lo general, el tráfico encriptado es confiable, a menos que la política de seguridad establezca que se debe permitir el tráfico encriptado desde y hacia puntos finales especificados.

```
class-map type inspect match-all crypto-cmap
 match access-group 123
!
policy-map type inspect to-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
  pass
!
```

```
policy-map type inspect from-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
access-list 123 permit esp any any
access-list 123 permit udp any any eq 4500
access-list 123 permit ah any any
access-list 123 permit udp any any eq 500
```

Zone-Based Firewall y Wide-Area Application Services

Consulte Release Note for Cisco Wide Area Application Services (Software Version 4.0.13) - New Features for Software Version 4.0.13 para obtener una nota sobre la aplicación que proporciona ejemplos de configuración e instrucciones de uso

Supervisión del firewall de políticas basadas en zonas con comandos show y debug

ZFW introduce nuevos comandos para ver la configuración de políticas y supervisar la actividad del firewall.

Para mostrar la descripción de la zona y las interfaces contenidas en una zona especificada:

```
show zone security [<zone-name>]
```

Cuando no se incluye el nombre de la zona, el comando muestra la información de todas las zonas configuradas.

```
Router#show zone security z1
zone z1
  Description: this is test zone1
  Member Interfaces:
    Ethernet0/0
```

Para mostrar la zona de origen, la zona de destino y la política adjunta al zone-pair:

```
show zone-pair security [source <source-zone-name>] [destination <destination-zone-name>]
```

Cuando no se especifica el origen ni el destino, se muestran todos los zone-pairs con origen, destino y política asociada. Cuando sólo se menciona la zona de origen o destino, se muestran todos los zone-pairs que contienen esta zona como origen o destino.

```
Router#show zone-pair security
zone-pair name zp
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

Para mostrar un policy-map especificado:

```
show policy-map type inspect [<policy-map-name> [class <class-map-name]]
```

Cuando no se especifica el nombre de un policy-map, muestra todos los policy-maps de tipo inspect (junto con policy-maps de Capa 7 que contienen un subtipo).

```
Router#show policy-map type inspect p1
 Policy Map type inspect p1
   Class c1
    Inspect
```

Muestra las estadísticas de policy-map de tipo Inspeccionar en tiempo de ejecución actualmente en un par de zonas especificado.

```
show policy-map type inspect zone-pair [zone-pair-name] [sessions]
```

Cuando no se menciona no zone-pair name, se muestran los policy-maps de todos los zone-pairs.

La opción sessions muestra las sesiones de inspección creadas por la aplicación del policy-map en el zone-pair especificado.

```
Router#show policy-map type inspect zone-pair zp
 Zone-pair: zp

  Service-policy : p1

    Class-map: c1 (match-all)
      Match: protocol tcp
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0

    Class-map: c2 (match-all)
      Match: protocol udp
      Pass
        0 packets, 0 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

La palabra clave urlfilter muestra las estadísticas relacionadas con el filtro URL que corresponden al policy-map especificado (o de los policy-maps de todos los destinos cuando no se especifica un nombre de zone-pair):

```
show policy-map type inspect zone-pair [zone-pair-name] [urlfilter [cache]]
```

Cuando se especifica la palabra clave cache junto con urlfilter, se muestra la memoria caché de urlfilter (de las direcciones IP).

Resumen del comando show policy-map para los policy-maps Inspect:

```
show policy-map type inspect inspect { <policy name> [class <class name>] |
                  zone-pair [<zone-pair name>] [sessions | urlfilter cache] }
```

Ajuste de la protección de denegación de servicio del firewall de políticas basadas en zonas

ZFW ofrece protección contra DoS para alertar a los ingenieros de red sobre cambios importantes en la actividad de la red y para mitigar la actividad no deseada a fin de reducir el impacto de los cambios en la actividad de la red. ZFW mantiene un contador separado para cada class-map del policy-map. Por lo tanto, si se utiliza un mapa de clase para dos mapas de políticas de pares de zonas diferentes, se aplican dos conjuntos diferentes de contadores de protección DoS.

ZFW proporciona mitigación de ataques de DoS de forma predeterminada en versiones anteriores a Cisco IOS Software Release 12.4(11)T. El comportamiento de protección contra DoS predeterminado cambió en Cisco IOS Software Release 12.4(11)T.

Consulte Definición de Estrategias para Protegerse contra los Ataques de Negación de Servicio (DoS) TCP SYN para obtener más información sobre los ataques de DoS TCP SYN.

Apéndices

Apéndice A: Configuración Básica

```
ip subnet-zero
ip cef
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
```

```
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 bridge-group 1
!
interface Vlan2
 no ip address
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 ip route-cache flow
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
bridge 1 protocol ieee
bridge 1 route ip
!
end
```

Apéndice B: Configuración Final (Completa)

```
ip subnet-zero
ip cef
!
ip port-map user-Xwindows port tcp from 6900 to 6910
!
class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
class-map type inspect match-any dns-http-class
 match protocol dns
 match protocol http
class-map type inspect match-any smtp-class
 match protocol smtp
class-map type inspect match-all dns-http-acl-class
 match access-group 110
 match class-map dns-http-class
class-map type inspect match-all smtp-acl-class
 match access-group 111
 match class-map smtp-class
class-map type inspect match-any Xwindows-class
 match protocol user-Xwindows
class-map type inspect match-any internet-traffic-class
 match protocol http
 match protocol https
 match protocol dns
 match protocol icmp
class-map type inspect http match-any bad-http-class
 match  port-misuse all
```

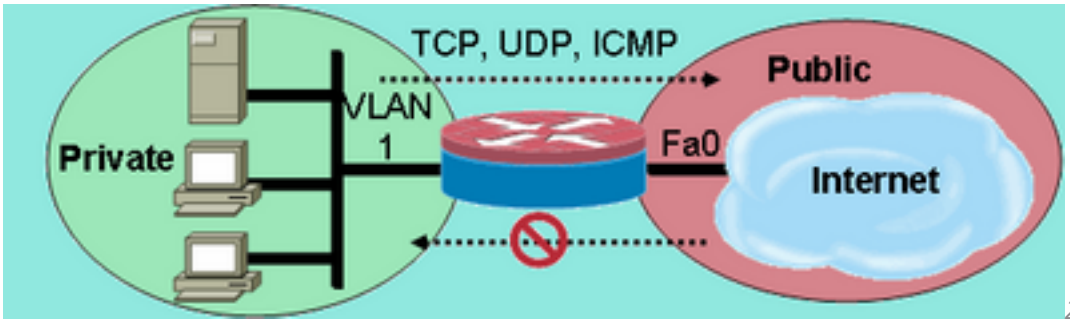
```
 match  strict-http
!
policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
policy-map type inspect internet-dmz-policy
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
policy-map type inspect servers-clients-policy
 class type inspect Xwindows-class
  inspect
policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
  class type inspect bad-http-class
   drop
!
zone security clients
zone security servers
zone security private
zone security internet
zone security dmz
zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 zone-member internet
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 zone-member dmz
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
```

```
 switchport access vlan 1
!
interface Vlan1
 no ip address
 zone-member clients
 bridge-group 1
!
interface Vlan2
 no ip address
 zone-member servers
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 zone-member private
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
access-list 110 permit ip any host 172.16.2.2
access-list 111 permit ip any host 172.16.2.3
!
bridge 1 protocol ieee
bridge 1 route ip
!
End
```

Apéndice C: Configuración Básica de Zone-Policy Firewall para Dos Zonas

En este ejemplo se proporciona una configuración sencilla como base para probar las características de las mejoras del ZFW del software Cisco IOS. Esta configuración es un modelo de configuración para dos zonas, configuradas en un router 1811. La zona privada se aplica a los puertos de switch fijos del router, de modo que todos los hosts de los puertos de switch están conectados a la VLAN 1. La zona pública se aplica en FastEthernet 0 (consulte la figura 12).

Figura 12: Zona pública aplicada en FastEthernet 0



Zona pública aplicada en FastEthernet 0

```
class-map type inspect match-any private-allowed-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all http-class
 match protocol http
!
policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters
 class type inspect private-allowed-class
  inspect
```

```
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect private-allowed-policy
!
interface fastethernet 0
 zone-member security public
!
interface VLAN 1
 zone-member security private
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).