Diseño del Firewall de la directiva y guía Zona-basados de la aplicación

Contenido

Introducción

El Software Release 12.4(6)T de Cisco IOS® introducido Zona-basó el Firewall de la directiva (ZFW), un nuevo modelo de la configuración para el conjunto de funciones del Cisco IOS Firewall. Este nuevo modelo de la configuración ofrece las directivas intuitivas para el Routers de la

interfaz múltiple, el granularity creciente de la aplicación de las políticas del firewall, y un valor por defecto negar-toda directiva que prohíba el tráfico entre las zonas de Seguridad del Firewall hasta que una directiva explícita se aplique para permitir el tráfico deseable.

Casi todas las características de firewall del Cisco IOS clásico implementadas antes de que el Cisco IOS Software Release 12.4(6)T se soporte en la nueva interfaz zona-basada del examen de la directiva:

- Inspección de paquetes stateful
- Firewall Cisco IOS que reconoce VRF
- Filtrado de URL
- Mitigación del servicio negado (DOS)

Cisco IOS Software Release 12.4(9)T soporte agregado Inspección de la aplicación ZFW para los límites de la sesión/de la conexión y de la producción de las por class, así como y control:

- HTTP
- El protocolo Post Office Protocol (POP3), el Internet Mail Access Protocol (IMAP), protocolo simple mail transfer/aumentó el protocolo simple mail transfer (SMTP/ESMTP)
- Llamada a procedimiento remoto (RPC) de Sun
- Aplicaciones de la Mensajería inmediata (IM):Mensajero de MicrosoftYahoo! MensajeroAOL Instant Messenger
- Capacidad de compartir archivos entre iguales (P2P):BittorrentKaZaAGnutellaeDonkey

Estadísticas agregadas Cisco IOS Software Release 12.4(11)T para ajustar más fácil del protección DoS.

Algunas características de firewall y capacidades clásicas del Cisco IOS todavía no se soportan en un ZFW en el Cisco IOS Software Release 12.4(15)T:

- Proxy de Autenticación
- Conmutación por falla del escudo de protección con estado
- Firewall unificado MIB
- Inspección con estado del IPv6
- Soporte fuera de servicio TCP

ZFW mejora generalmente el funcionamiento del Cisco IOS para la mayoría de las actividades del examen del Firewall.

Ni el Cisco IOS ZFW o el Firewall clásico incluye el soporte de la inspección con estado para el tráfico Multicast.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

Convenciones

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

Descripción Zona-basada de la directiva

La inspección con estado clásica del Firewall del Cisco IOS (conocida antes como el Context-Based Access Control, o CBAC) empleó un modelo basado en la interfaz de la configuración, en el cual una directiva de la inspección con estado fue aplicada a una interfaz. Todo el tráfico que pasaba a través de esa interfaz recibió la misma directiva del examen. Este modelo de la configuración limitó el granularity de las políticas del firewall y causó la confusión de la aplicación apropiada de las políticas del firewall, determinado en los escenarios cuando las políticas del firewall deben ser aplicadas entre las interfaces múltiples.

El Firewall Zona-basado de la directiva (también conocido como el Firewall de la Zona-directiva, o ZFW) cambia la configuración de escudo de protección del más viejo modelo basado en la interfaz a un modelo zona-basado más flexible, más facilmente comprensible. Las interfaces se asignan a las zonas, y la directiva del examen se aplica para traficar la mudanza entre las zonas. las directivas de la Inter-zona ofrecen la considerable flexibilidad y el granularity, así que diversas directivas del examen se pueden aplicar a los grupos del host múltiple conectados con la interfaz del mismo router.

Las políticas del firewall se configuran con el lenguaje de la directiva del Cisco® (COMPLETO), que emplea una estructura jerárquica para definir el examen para los Network Protocol y los grupos de host a los cuales el examen sea aplicado.

Modelo Zona-basado de la configuración de la política

ZFW cambia totalmente la manera que usted configura un examen del Firewall Cisco IOS, con respecto al Firewall de la obra clásica del Cisco IOS.

El primer cambio importante a la configuración de escudo de protección es la introducción de configuración zona-basada. El Firewall Cisco IOS es la primera característica de la defensa de la amenaza del Cisco IOS Software para implementar un modelo de la configuración de la zona. Las otras funciones pudieron adoptar el modelo de la zona en un cierto plazo. El modelo basado en la interfaz clásico de la configuración de la inspección con estado del Firewall del Cisco IOS (o CBAC) que emplea el conjunto del **comando ip inspect** se mantiene por un período de tiempo. Sin embargo, pocas o incluso ningúas nuevas funciones son configurables con el comando line interface(cli) clásico. ZFW no utiliza la inspección con estado o los comandos CBAC. Los dos modelos de la configuración se pueden utilizar en paralelo en el Routers, pero no combinar en las interfaces. Una interfaz no se puede configurar como miembro de la zona de Seguridad así como siendo configurado para el **IP examine** simultáneamente.

Las zonas establecen las fronteras de la Seguridad de su red. Una zona define un límite donde el tráfico se sujeta a las restricciones de la directiva como él cruza a otra región de su red. La política predeterminada ZFW entre las zonas es niega todos. Si no se configura ninguna directiva explícitamente, todo el tráfico que se mueve entre las zonas se bloquea. Esto es una salida significativa del modelo de la inspección con estado donde el tráfico fue permitido implícito hasta bloqueado explícitamente con un Access Control List (ACL).

El segundo cambio importante es la introducción de un nuevo lenguaje de la directiva de configuración conocido como CPL. Users que el familiar con la calidad de servicio modular del Cisco IOS Software (QoS) CLI (MQC) pudo reconocer que el formato es similar al uso de QoS de las correspondencias de la clase de especificar qué tráfico será afectado por la acción aplicada en una correspondencia de políticas.

Reglas para aplicar el Firewall Zona-basado de la directiva

La calidad de miembro de las interfaces de red del router en las zonas está conforme a varias reglas que gobiernen el comportamiento de la interfaz, al igual que el tráfico que se mueve entre las interfaces de miembro de la zona:

- Una zona debe ser configurada antes de que las interfaces se puedan asignar a la zona.
- Una interfaz se puede asignar a solamente una zona de Seguridad.
- Todo el tráfico a y desde una interfaz dada se bloquea implícito cuando la interfaz se asigna a una zona, a menos que tráfico a y desde otras interfaces en la misma zona, y tráfico a cualquier interfaz en el router.
- El tráfico se permite implícito fluir por abandono entre las interfaces que son miembros de la misma zona.
- Para permitir el tráfico a y desde una interfaz de miembro de la zona, una directiva permitiendo o examinando el tráfico se debe configurar entre esa zona y cualquier otra zona.
- La zona del uno mismo es la única excepción al valor por defecto niega toda la directiva. Todo el tráfico a cualquier interfaz del router se permite hasta que el tráfico se niegue explícitamente.
- El tráfico no puede fluir entre una interfaz de miembro de la zona y ninguna interfaz que no sea un miembro de la zona. El paso, examina, y las acciones de descarte pueden solamente ser aplicadas entre dos zonas.
- Interfaces que no se han asignado a una función de la zona como puertos de router clásicos y pudieron todavía utilizar la configuración stateful clásica inspection/CBAC.
- Si se requiere que una interfaz en el cuadro no ser parte del Establecimiento de zonas/las políticas del firewall. Puede ser que todavía sea necesario poner que interfaz en una zona y configura un paso toda la directiva (clase de una directiva simulada) entre esa zona y cualquier otra zona a las cuales se desee el flujo de tráfico.
- De preceder sigue que, si el tráfico es fluir entre todas las interfaces en un router, todas las interfaces deben ser parte del modelo del Establecimiento de zonas (cada interfaz debe ser un miembro de una zona o de otra).
- La única excepción a preceder niega por abandono el acercamiento es el tráfico a y desde el router, que será permitido por abandono. Una directiva explícita se puede configurar para restringir tal tráfico.

Diseño de la Seguridad Zona-basada de la red de políticas

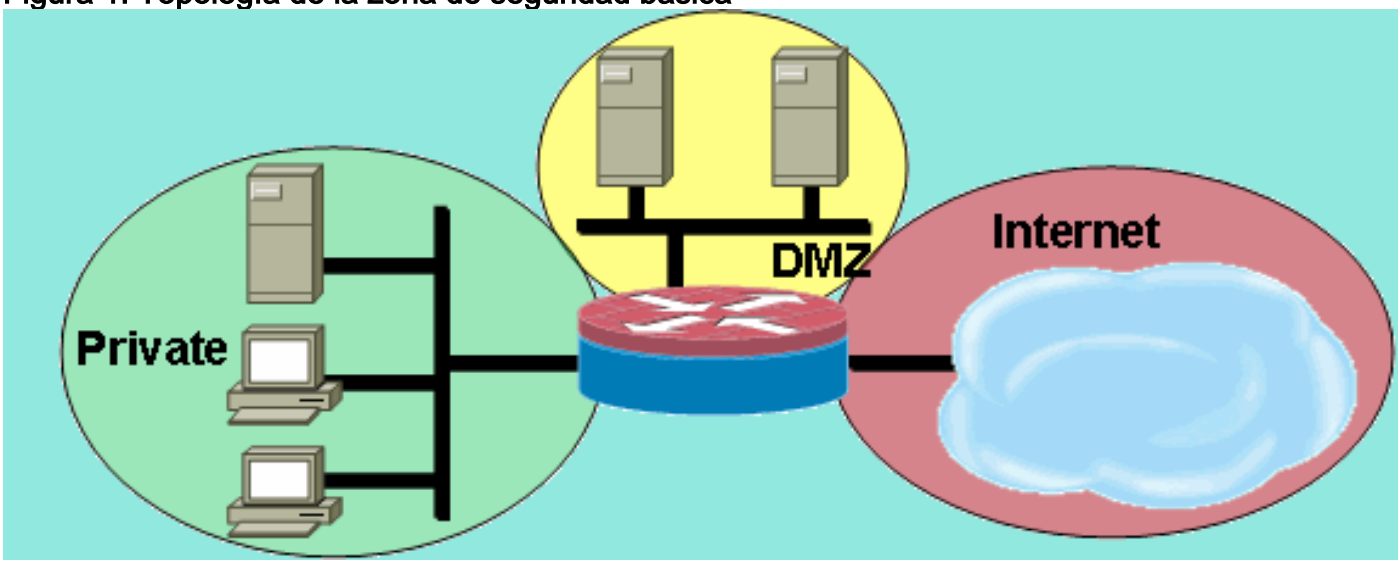
Una zona de Seguridad se debe configurar para cada región de Seguridad relativa dentro de la red, de modo que todas las interfaces que se asignan a la misma zona sean protegidas con un nivel de seguridad similar. Por ejemplo, considere un router de acceso con tres interfaces:

- Una interfaz conectada con el Internet pública
- Una interfaz conectada con un LAN privado que no debe ser accesible del Internet pública

- Una interfaz conectada con una zona desmilitarizada del servicio de Internet (DMZ), donde un servidor del servidor Web, del Domain Name System (DNS), y el servidor del email deben ser accesibles al Internet pública

Cada interfaz en esta red será asignada a su propia zona, aunque usted puede ser que quiera permitir el acceso variado del Internet pública a los host específicos en el DMZ y a las directivas variadas del uso de la aplicación para los host en el LAN protegido. (Véase el cuadro 1.)

Figura 1: Topología de la zona de seguridad básica



En este ejemplo, cada zona lleva a cabo solamente una interfaz. Si una interfaz adicional se agrega a la zona privada, los host conectados con la nueva interfaz en la zona pueden pasar el tráfico a todos los host en la interfaz existente en la misma zona. Además, el tráfico de los host a los host en otras zonas es afectado semejantemente por las políticas existentes.

Típicamente, la red de muestra tendrá tres directivas principales:

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

Porque el DMZ se expone al Internet pública, los host DMZ se pudieron sujetar a la actividad indeseada de los individuos malévolos que pudieron tener éxito en el compromiso de uno o más host DMZ. Si no se proporciona ninguna política de acceso para que los host DMZ alcancen los host privados de los host de la zona o de la zona de Internet, después los individuos que comprometieron los host DMZ no pueden utilizar los host DMZ para realizar los otros ataques contra el soldado o los host de Internet. ZFW impone una postura de seguridad predeterminada prohibitiva. Por lo tanto, a menos que los host DMZ sean específicamente acceso proporcionado a otras redes, otras redes se salvaguardan contra cualquier conexión de los host DMZ. Semejantemente, no se proporciona ningún acceso para que los host de Internet accedan los host privados de la zona, así que los host privados de la zona son seguros del acceso indeseado por los host de Internet.

Usando el IPSec VPN con el Firewall Zona-basado de la directiva

Las mejoras recientes al IPSec VPN simplifican la configuración de las políticas del firewall para la conectividad VPN. La interfaz del túnel virtual del IPSec (VTI) y GRE+IPSec permiten el confinamiento del sitio a localizar y de las conexiones cliente VPN a una zona de Seguridad específica poniendo las interfaces del túnel en una zona de Seguridad especificada. Las

conexiones se pueden aislar en un VPN DMZ si la Conectividad se debe limitar por una directiva específica. O, si la conectividad VPN se confía en implícito, la conectividad VPN se puede poner en la misma zona de Seguridad que la red interna de confianza.

Si un IPSec NON-VTI es aplicado, las políticas del firewall de la conectividad VPN requieren el examen riguroso mantener la Seguridad. La directiva de la zona debe permitir específicamente el acceso por una dirección IP para los host de los sitios remotos o los clientes VPN si asegure los host están en una diversa zona que la conexión encriptada del cliente VPN al router. Si la política de acceso no se configura correctamente, los host que deben ser protegidos pueden terminar para arriba expuesto a los host indeseados, potencialmente hostiles. Refiérase con el VPN con el Firewall Zona-basado de la directiva para la discusión adicional del concepto y de la configuración.

Configuración (COMPLETA) del lenguaje de la directiva de Cisco

Este procedimiento se puede utilizar para configurar un ZFW. La secuencia de pasos no es importante, pero algunos eventos se deben completar en la orden. Por ejemplo, usted debe configurar un clase-mapa antes de que usted asigne un clase-mapa a un directiva-mapa. Semejantemente, usted no puede asignar un directiva-mapa a un zona-par hasta que usted haya configurado la directiva. Si usted intenta configurar una sección que confíe en otra porción de la configuración que usted no ha configurado, el router responde con un mensaje de error.

1. Defina las zonas.
2. Defina los zona-pares.
3. Defina class-maps que describa el tráfico que debe tener directiva aplicada como él cruza un zona-par.
4. Defina las correspondencias de políticas para aplicar la acción al tráfico de sus clase-correspondencias.
5. Aplique las correspondencias de políticas a los zona-pares.
6. Asigne las interfaces a las zonas.

Configurando el Firewall Zona-basado de la directiva class-maps

Class-maps defina el tráfico que el Firewall selecciona para la aplicación de la directiva. Clase class-maps de la capa 4 que el tráfico basado en estos criterios enumeró aquí. Estos criterios se especifican usando el **comando match** en un clase-mapa:

- Acceso-grupo — Un estándar, un extendido, o ACL mencionado pueden filtrar tráfico basado en el IP Address de origen y de destino y el puerto de origen y de destino.
- Protocolo — Los protocolos de la capa 4 (TCP, UDP, y ICMP) y servicios de aplicación tales como HTTP, S TP, DNS, etc. Cualquier servicio bien conocido o definido por el usario sabido a la asignación de la aplicación del puerto puede ser especificado.
- Clase-mapa — Un clase-mapa subordinado que proporciona los criterios de concordancia adicionales se puede jerarquizar dentro de otro clase-mapa.
- No — *No el* criterio especifica que cualquier clase-mapa del tráfico que no hace juego un servicio especificado (protocolo), del acceso-grupo o del subordinado será seleccionado para el clase-mapa.

Combinar los criterios de la “coincidencia”: “Match-any” contra “corresponda con todos”

Class-maps puede aplicar el match-any o a los operadores corresponda con todos para determinar cómo aplicar los criterios de concordancia. Si se especifica el match-any, el tráfico debe cumplir solamente uno de los criterios de concordancia en el clase-mapa. Si es corresponda con todos se especifica, tráfico debe hacer juego los criterios de todas las clase-correspondencias para pertenecer a esa clase determinada.

Los criterios de concordancia se deben aplicar en la orden de más específico a menos específico, si el tráfico cumple los criterios múltiples. Por ejemplo, considere este clase-mapa:

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

El tráfico HTTP debe encontrar el HTTP del protocolo de la coincidencia primero para aseegurarse el tráfico es dirigido por las capacidades del servicio específico del examen HTTP. Si se invierten las Líneas de coincidencia, así que el tráfico encuentra la declaración tcp del protocolo de la coincidencia antes de que la compare para hacer juego el HTTP del protocolo, el tráfico se clasifica simplemente como tráfico TCP, y se examina según las capacidades del componente del examen TCP del Firewall. Éste es servicios de un problema con certeza tales como FTP, TFTP, y varios servicios de las multimedias y de la señalización de voz tales como H.323, SORBO, flaco, RTSP, y otros. Estos servicios requieren las capacidades adicionales del examen reconocer las actividades más complejas de estos servicios.

Aplicación de un ACL como criterios de concordancia

Class-maps puede aplicar un ACL como uno de los criterios de concordancia para la aplicación de la directiva. Si un único criterio de la coincidencia de las clase-correspondencias es un ACL y el clase-mapa se asocia a un directiva-mapa que aplica la acción de la inspección, el router aplica el examen básico TCP o UDP para todo el tráfico permitido por el ACL, salvo que ZFW proporciona el examen que reconoce la aplicación. Esto incluye (pero no limitado a) el FTP, el SORBO, flaco (SCCP), H.323, Sun RPC, y TFTP. Si el examen específico a la aplicación está disponible y el ACL permite el primario o el canal de control, cualquier canal secundario o de los media asociado al primario/al control se permite, sin importar si el ACL permita el tráfico.

Si un clase-mapa aplica solamente el ACL 101 como los criterios de concordancia, un ACL 101 aparece como esto:

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

Todo el tráfico se permite en dirección de la servicio-directiva aplicada a un zona-par dado, y el tráfico de retorno correspondiente se permite en la dirección opuesta. Por lo tanto, el ACL debe aplicar la restricción para limitar el tráfico a los tipos deseados específico. Observe que la lista PAM incluye los servicios de aplicación tales como HTTP, NetBios, H.323, y DNS. Sin embargo, a pesar del conocimiento PAM del uso de la aplicación específica de un puerto dado, el Firewall aplica solamente la suficiente capacidad específica a la aplicación para acomodar los requisitos bien conocidos del tráfico de aplicación. Así, el tráfico de aplicación simple tal como telnet, SSH, y otras aplicaciones monocanal se examinan como TCP, y sus estadísticas se combinan juntas en la **salida del comando show**. Si la visibilidad específica a la aplicación en la actividad de la red se desea, usted necesita configurar el examen para los servicios por el nombre de la aplicación (HTTP del protocolo de la coincidencia de la configuración, telnet del protocolo de la coincidencia, etc.).

Compare las estadísticas disponibles en el **tipo del directiva-mapa de la demostración examinan la** salida de comando de los zona-**pares de** esta configuración con las políticas del firewall más explícitas mostradas plumón adicional la página. Esta configuración se utiliza para examinar el

tráfico de un Cisco IP Phone, así como varios puestos de trabajo que utilicen una variedad de tráfico, que incluye el 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
```

Mientras que esta configuración es fácil de definir y acomoda todo el tráfico que origine en los puertos destino PAM-reconocidos privados de la zona (mientras el tráfico observa el estándar,), proporciona la visibilidad limitada en la actividad de servicio, y no ofrece la oportunidad de aplicar el ancho de banda y los límites de sesión ZFW para los tipos de tráfico específicos. Este **tipo del directiva-mapa de la demostración examina la** salida de comando del priv-**pub de los zona-pares** es el resultado de la Configuración simple anterior que utiliza solamente un [subnet] del IP del permiso cualquier ACL entre los zona-pares. Como usted puede ver, la mayor parte del tráfico del puesto de trabajo se cuenta en las estadísticas básicas TCP o UDP:

```
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 las clases específicas a la aplicación proporciona estadísticas y un control más granulares de la aplicación, y todavía acomoda la misma anchura de los servicios que fue mostrada en el primer ejemplo definiendo el clase-mapa de la última oportunidad que correspondía con solamente el ACL como la última oportunidad en el directiva-mapa:

```
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 del más específico proporciona esta salida granular sustancial para el **tipo del directiva-mapa de la demostración examina el** comando del priv-**pub de los zona-pares**:

```
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 agregada de usar una configuración más granular del class-map y policy-map, según lo mencionado anterior, es la posibilidad de aplicar los límites clase-específicos en la sesión y los valores de velocidad y específicamente de ajustar los parámetros de inspección aplicando un parámetro-mapa para ajustar el comportamiento del examen de cada clase.

Configurar las correspondencias de políticas Zona-basadas del Firewall de la directiva

El directiva-mapa aplica las acciones de las políticas del firewall a uno o más class-maps para definir la servicio-directiva que será aplicada a un zona-par de la Seguridad. Cuando se crea un directiva-mapa del examinar-tipo, una clase predeterminada nombrada class class-default es aplicada en el extremo de la clase. La acción de la política predeterminada de los clase-valores por defecto de la clase es descenso, pero se puede cambiar para pasar. La opción del registro se puede agregar con la acción de descarte. Inspect no se puede aplicar en el class class-default.

Acciones Zona-basadas del Firewall de la directiva

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

- **Descenso** — Ésta es la acción predeterminada para todo el tráfico, según lo aplicado por el “class class-default” que termine cada directiva-mapa del examinar-tipo. Otro class-maps dentro de un directiva-mapa se puede también configurar para caer el tráfico no deseado. Trafique que es manejado por la acción de descarte es caído “silenciosamente” (es decir, no se envía ninguna notificación del descenso al host extremo relevante) por el ZFW, en comparación con el comportamiento ACL de enviar un ICMP “imposible acceder al host” mensaje al host que envió el tráfico denegado. Actualmente, no hay una opción para cambiar el comportamiento del “descenso silencioso”. La opción del registro se puede agregar con el descenso para la notificación de Syslog que el tráfico fue caído por el Firewall.
- **Paso** — Esta acción permite que el router remita el tráfico a partir de una zona a otra. La acción del paso no sigue el estado de las conexiones o de las sesiones dentro del tráfico. El paso permite solamente el tráfico en una dirección. Una directiva correspondiente se debe aplicar para permitir que el tráfico de retorno pase en la dirección opuesta. La acción del paso es útil para los protocolos tales como IPSec ESP, IPSec AH, ISAKMP, y otros protocolos intrínsecamente seguros con el comportamiento fiable. Sin embargo, la mayoría del tráfico de aplicación se maneja mejor en el ZFW con la acción de la inspección.
- **Examine** — La acción de la inspección ofrece el control de tráfico basado en el estado. Por ejemplo, si el tráfico de la zona privada a la zona de Internet en la red de muestra anterior se examina, el router mantiene la conexión o la información de la sesión para el tráfico TCP y del User Datagram Protocol (UDP). Por lo tanto, el router permite el tráfico de retorno enviado de los host de la Internet-zona en respuesta a los pedidos de conexión privados de la zona. También, examine puede proporcionar los Protocolos de servicio de la Inspección de la aplicación y del control con certeza que pudieron llevar el tráfico vulnerable o de la aplicación

sensible. El rastro de auditoría se puede aplicar con un parámetro-mapa para registrar la conexión/el comienzo de la sesión, la parada, la duración, el volumen de los datos transferido, y a las direcciones de origen y de destino.

Las acciones se asocian a class-maps en las correspondencias de políticas:

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

las Parámetro-correspondencias ofrecen las opciones para modificar los parámetros de la conexión para una directiva del examen de las clase-correspondencias dadas.

Configurar las Parámetro-correspondencias del Firewall de la Zona-directiva

las Parámetro-correspondencias especifican el comportamiento del examen para ZFW, para los parámetros tales como protección DoS, temporizadores de sesión TCP connection/UDP, y configuraciones del registro del rastro de auditoría. las Parámetro-correspondencias también se aplican con la clase y las correspondencias de políticas de la capa 7 para definir el comportamiento específico a la aplicación, tal como objetos HTTP, los Requisitos de autenticación POP3 y IMAP, y la otra información específica a la aplicación.

Las parámetro-correspondencias del examen para ZFW se configuran como el **tipo examina**, similar a la otra clase y a los directiva-objetos 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 parámetro-correspondencias especifican los parámetros aplicados por las directivas de la Inspección de la aplicación de la capa 7. las parámetro-correspondencias del Regex-tipo definen una expresión normal para el uso con la Inspección de la aplicación HTTP que los filtros trafican usando una expresión normal:

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

las parámetro-correspondencias del Protocolo-Info-tipo definen los nombres de servidor para el uso con el examen inmediato de la aplicación de mensajería:

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

Proporcionan los detalles de la configuración completos para el HTTP e IM Inspección de la aplicación en las secciones del examen de la aplicación respectiva de este documento.

El ajuste del protección DoS se cubre en una sección posterior de este documento.

Configurar la Inspección de la aplicación se cubre en una sección posterior de este documento.

Aplicación del registro para las políticas del firewall Zona-basadas de la directiva

ZFW ofrece las opciones de registro para el tráfico que se cae o se examina por abandono o las acciones configuradas de las políticas del firewall. El registro del rastro de auditoría está disponible para el tráfico que el ZFW examina. El rastro de auditoría es aplicado definiendo el

rastro de auditoría en un parámetro-mapa y aplicando el parámetro-mapa con la acción de la inspección en un directiva-mapa:

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

El registro del descenso está disponible para el tráfico ese los descensos ZFW. El registro del descenso es configurado agregando el registro con la acción de descarte en un directiva-mapa:

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

Editando el Firewall de la Zona-directiva class-maps y correspondencias de políticas

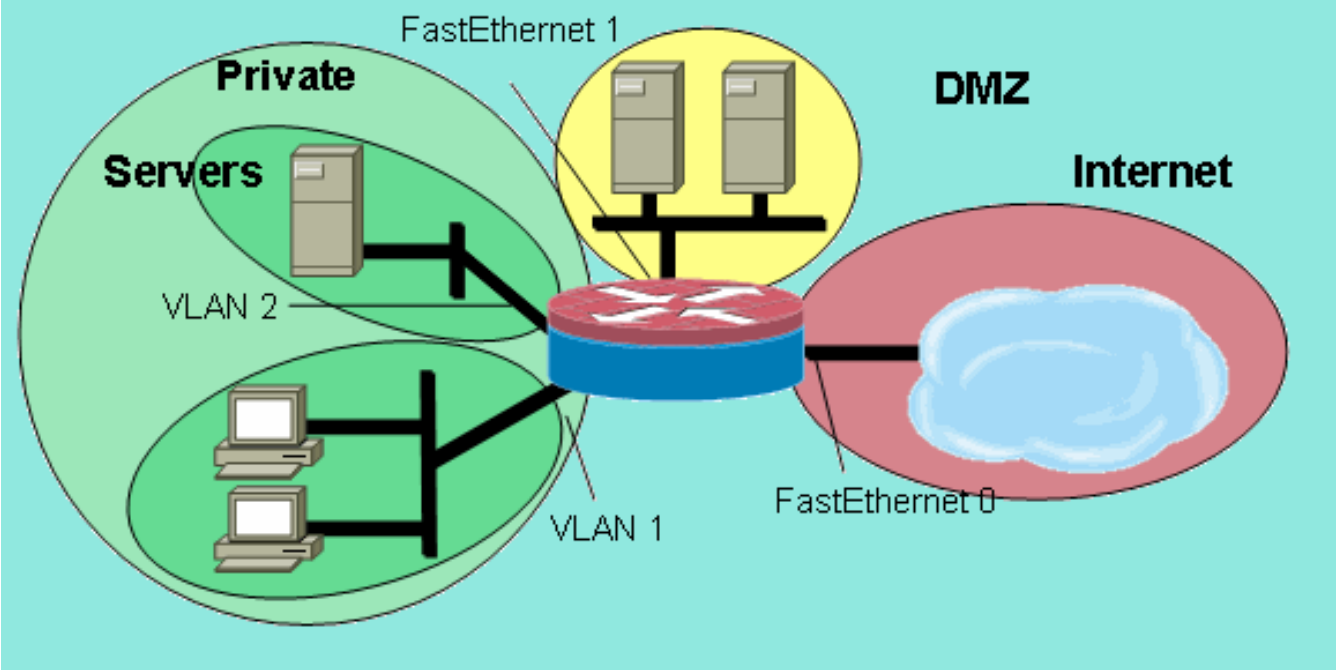
ZFW no incorpora actualmente un editor que pueda modificar las diversas estructuras ZFW tales como correspondencias de políticas, class-maps, y parámetro-correspondencias. Para cambiar las declaraciones de coincidencia en una aplicación del clase-mapa o de la acción a diverso class-maps contenido dentro de un directiva-mapa, usted necesita completar estos pasos:

1. Copie la estructura existente a un editor de textos tal como libreta de Microsoft Windows, o un editor por ejemplo VI en las Plataformas de Linux/de Unix.
2. Quite la estructura existente de la configuración del router.
3. Edite la estructura en su editor de textos.
4. Copie la estructura de nuevo al CLI del router.

Ejemplos de Configuración

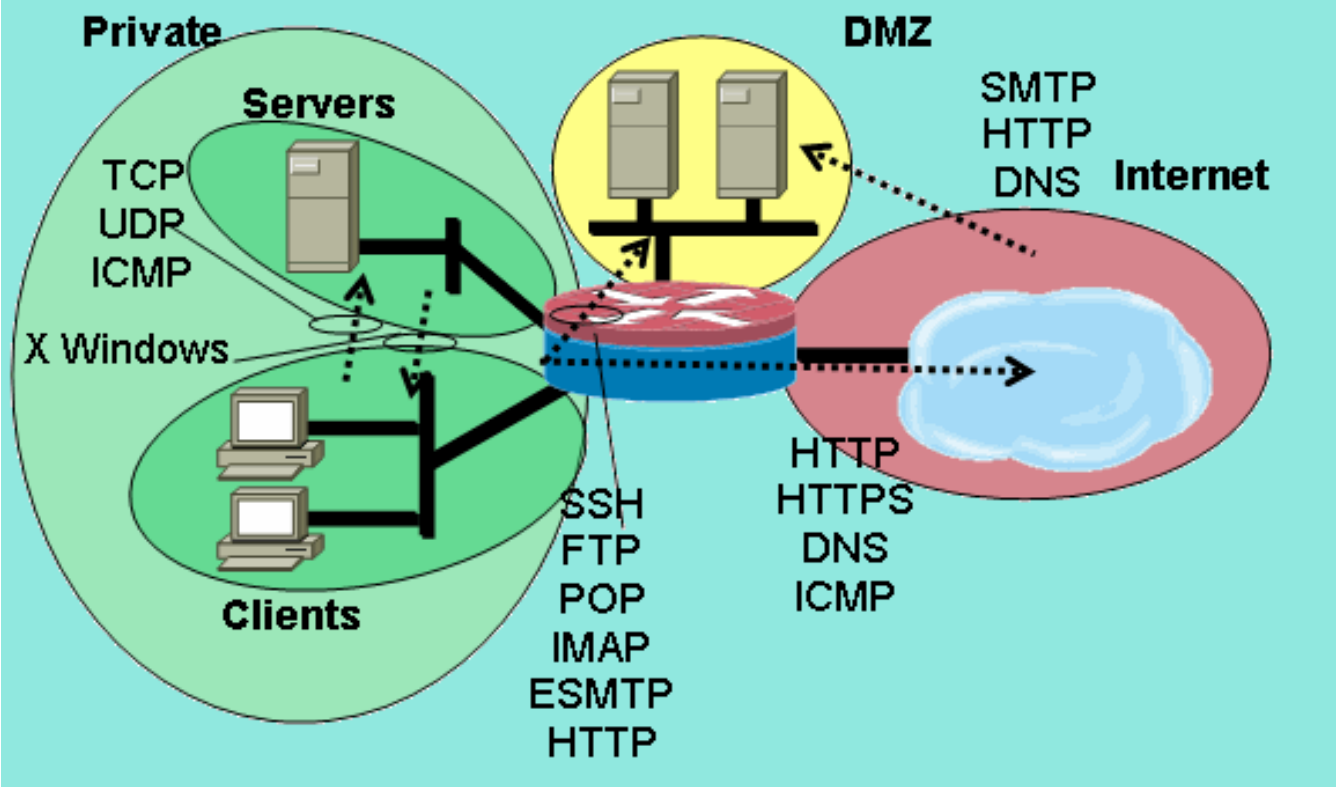
Este ejemplo de configuración emplea a un Router de servicios integrados Cisco 1811. Una configuración básica con la conectividad del IP, la configuración de VLAN, y Puente transparente entre dos segmentos privados del LAN Ethernet está disponible en el Apéndice A. Separan al router en cinco zonas:

- El Internet pública está conectado con el FastEthernet 0 (la zona de Internet)
- Dos servidores de Internet están conectados con el FastEthernet 1 (la zona DMZ)
- El switch de Ethernet se configura con dos VLA N:Los puestos de trabajo están conectados con el VLAN1 (zona del cliente).Los servidores están conectados con VLAN2 (zona del servidor).Las zonas del cliente y servidor están en la misma subred. Un Firewall transparente será aplicado entre las zonas, así que las directivas de la inter-zona en esas dos interfaces afectarán solamente al tráfico entre las zonas del cliente y servidor.
- El VLAN1 y las interfaces VLAN2 comunican con otras redes con el Interfaz Virtual de Bridge (BVI1). Esta interfaz se asigna a la zona privada. (Véase el cuadro 2.)**Figura 2: Detalle de la topología de la zona**



Estas directivas son aplicadas, usando las zonas de la red definidas anterior:

- Los host en la zona de Internet pueden alcanzar los servicios DNS, S TP, y de SSH en un servidor en el DMZ. El otro servidor ofrecerá los servicios S TP, HTTP, y HTTPS. Las políticas del firewall restringirán el acceso a los servicios específicos disponibles en cada host.
- Los host DMZ no pueden conectar con los host en ninguna otra zona.
- Los host en la zona del cliente pueden conectar con los host en la zona del servidor en todos los servicios TCP, UDP, y ICMP.
- Los host en la zona del servidor no pueden conectar con los host en la zona del cliente, a menos que un servidor de aplicaciones en lenguaje Unix pueda abrir a las sesiones de cliente del X Windows en los servidores del X Windows en los PC de escritorio en la zona del cliente en los puertos 6900 a 6910.
- Todos los host en la zona privada (combinación de clientes y servidores) pueden acceder los host en el DMZ en los servicios de SSH, FTP, POP, IMAP, ESMTP, y HTTP, y en la zona de Internet en los servicios HTTP, HTTPS, y DNS y el ICMP. Además, la Inspección de la aplicación será aplicada en las conexiones HTTP de la zona privada a la zona de Internet para asegurar que la Mensajería inmediata soportada y las aplicaciones P2P no son el puerto continuado 80. (Véase el cuadro 3.)**Figura 3: Permisos del servicio de los Zona-pares para ser aplicado en el ejemplo de configuración**



Estas políticas del firewall se configuran en orden de la complejidad:

1. Examen de los Cliente-servidores TCP/UDP/ICMP
2. Examen Soldado-DMZ SSH/FTP/POP/IMAP/ESMTP/HTTP
3. Internet - Examen DMZ SMTP/HTTP/DNS restringido por la dirección de host
4. Examen del X Windows de los Servidor-clientes con una asignación de la aplicación del puerto (PAM) - servicio especificado
5. Private internet HTTP/HTTPS/DNS/ICMP con la Inspección de la aplicación HTTP

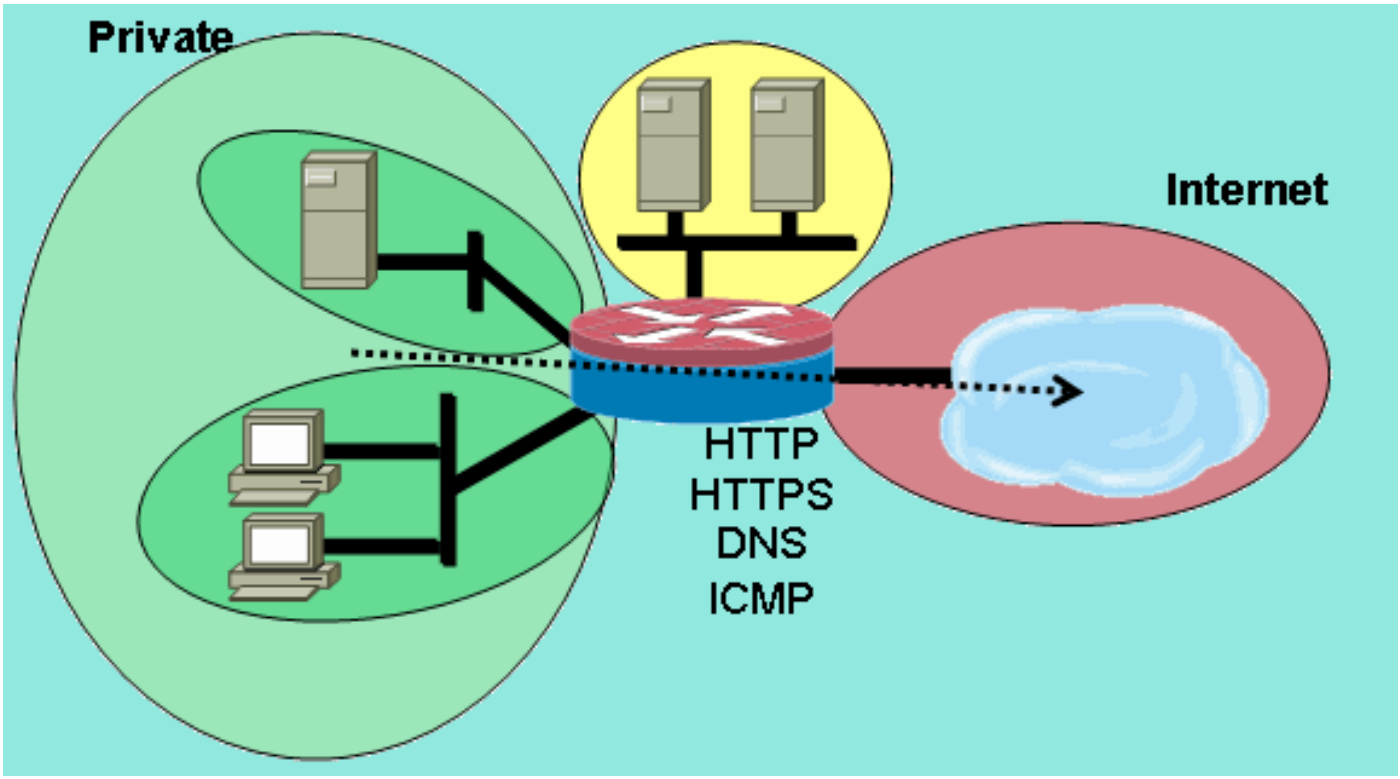
Porque usted aplicará las porciones de la configuración a diversos segmentos de red en los momentos diferentes, es importante recordar que un segmento de red perderá la Conectividad a otros segmentos cuando se pone en una zona. Por ejemplo, cuando se configura la zona privada, los host en la zona privada perderán la Conectividad a las zonas DMZ y de Internet hasta que se definan sus directivas respectivas.

Firewall de la encaminamiento de la inspección con estado

Directiva del private internet de la configuración

El cuadro 4 ilustra la configuración de la directiva del private internet.

Figura 4: Examen de servicio de la zona privada a la zona de Internet



La directiva del private internet aplica el examen de la capa 4 al HTTP, HTTPS, DNS, y acoda el examen 4 para el ICMP de la zona privada a la zona de Internet. Esto permite las conexiones de la zona privada a la zona de Internet, y permite el tráfico de retorno. El examen de la capa 7 lleva las ventajas de un control más apretado de la aplicación, de una mejor Seguridad, y del soporte para las aplicaciones que requieren el fixup. Sin embargo, el examen de la capa 7, según lo mencionado, requiere una mejor comprensión de la actividad de la red, como protocolos de la capa 7 que no se configuren para el examen no sean permitidos entre las zonas.

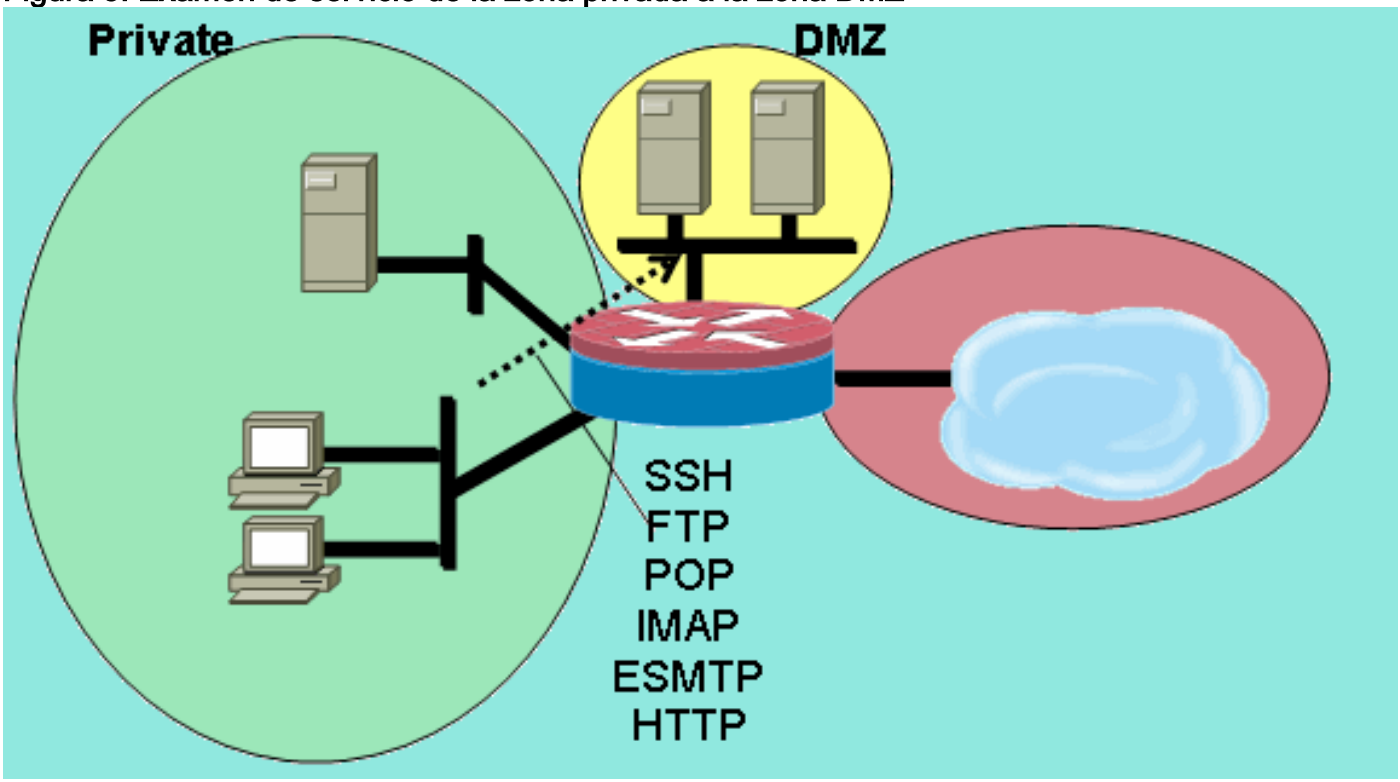
1. Defina class-maps que describa el tráfico que usted quiere permitir entre las zonas, según las directivas descritas anterior:`conf t`
```
class-map type inspect match-any internet-traffic-class
 match protocol http
 match protocol https
 match protocol dns
 match protocol icmp
```
2. Configure un directiva-mapa para examinar el tráfico en el class-maps usted definir:`conf t`
```
policy-map type inspect private-internet-policy
 class type inspect internet-traffic-class
  inspect
```
3. Configure el soldado y las zonas de Internet y asigne las interfaces del router a sus zonas respectivas:`conf t`
```
zone security private
zone security internet
int bvi1
zone-member security private
int fastethernet 0
zone-member security internet
```
4. Configure los zona-pares y aplique el directiva-mapa apropiado.**Nota:** Usted necesita solamente configurar los pares de la zona del private internet actualmente para examinar las conexiones originadas en la zona privada que viaja a la zona del Internet:`conf t`
```
zone-pair security private-internet source private destination internet
 service-policy type inspect private-internet-policy
```
Esto completa la configuración de la directiva del examen de la capa 7 en los zona-pares del private internet para permitir las

conexiones HTTP, HTTPS, DNS, y ICMP de la zona de los clientes a la zona de los servidores y para aplicar la Inspección de la aplicación al tráfico HTTP para asegurar que el tráfico no deseado no está permitido pasar encendido TCP 80, el puerto del servicio HTTP.

Directiva privada de la configuración DMZ

El cuadro 5 ilustra la configuración de la directiva privada DMZ.

Figura 5: Examen de servicio de la zona privada a la zona DMZ



La directiva del soldado DMZ agrega la complejidad porque requiere una mejor comprensión del tráfico de la red entre las zonas. Esta directiva aplica el examen de la capa 7 de la zona privada al DMZ. Esto permite las conexiones de la zona privada al DMZ, y permite el tráfico de retorno. El examen de la capa 7 lleva las ventajas de un control más apretado de la aplicación, de una mejor Seguridad, y del soporte para las aplicaciones que requieren el fixup. Sin embargo, el examen de la capa 7, según lo mencionado, requiere una mejor comprensión de la actividad de la red, como protocolos de la capa 7 que no se configuren para el examen no sean permitidos entre las zonas.

1. Defina class-maps que describa el tráfico que usted quiere permitir entre las zonas, según las directivas descritas anterior:`conf t`
```
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 las correspondencias de políticas para examinar el tráfico en el class-maps usted definir:`conf t`
```
policy-map type inspect private-dmz-policy
 class type inspect L7-inspect-class
  inspect
```
3. Configure el soldado y las zonas DMZ y asigne las interfaces del router a sus zonas

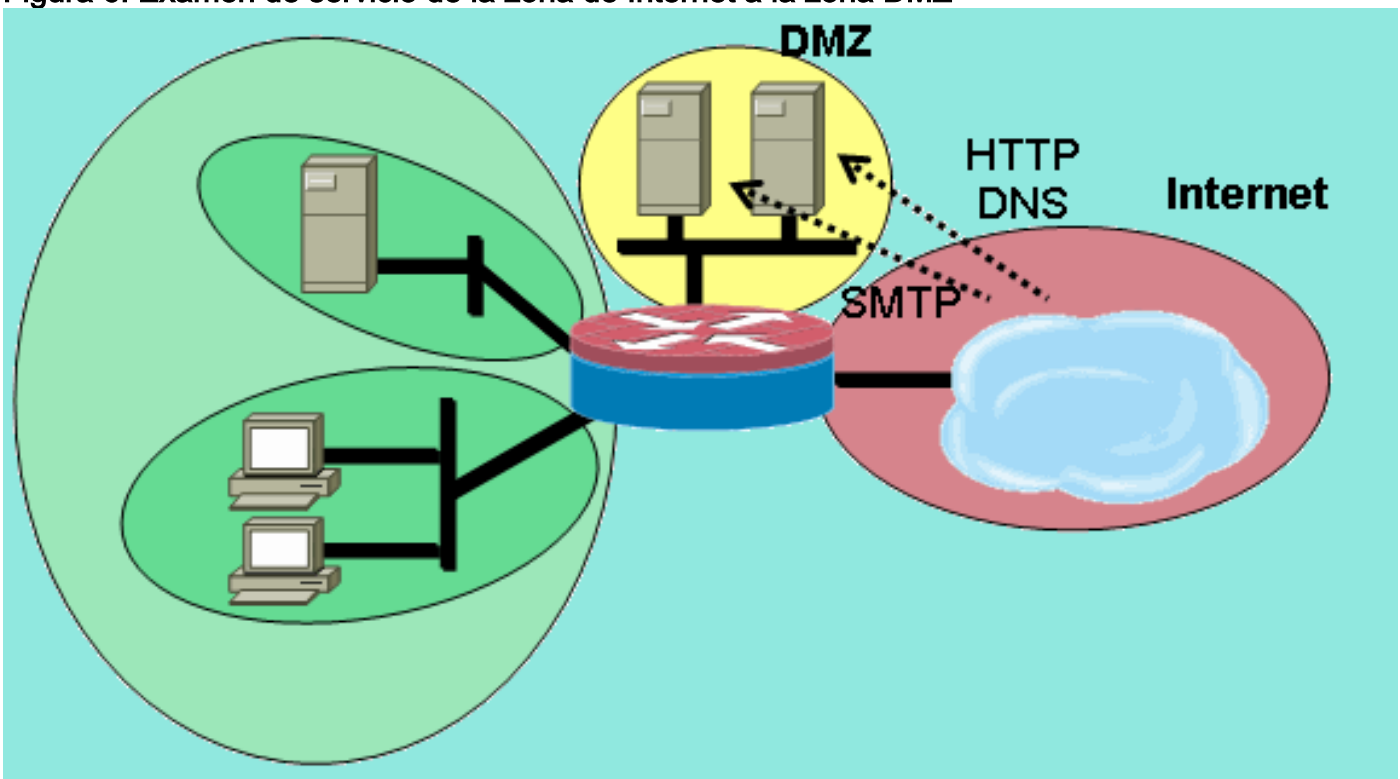
respectivas:
```
conf t
zone security private
zone security dmz
int bvi1
zone-member security private
int fastethernet 1
zone-member security dmz
```

4. Configure los zona-pares y aplique el directiva-mapa apropiado.**Nota:** Usted necesita solamente configurar los zona-pares privados DMZ actualmente para examinar las conexiones originadas en la zona privada que viaja al DMZ:
```
conf t
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```
Esto completa la configuración de la directiva del examen de la capa 7 en el soldado DMZ para permitir todas las conexiones TCP, UDP, y ICMP de la zona de los clientes a la zona de los servidores. La directiva no aplica el fixup para los canales subordinados, sino proporciona un ejemplo de la directiva simple para acomodar la mayoría de las conexiones de la aplicación.

Directiva de Internet DMZ de la configuración

El cuadro 6 ilustra la configuración de la directiva de Internet DMZ.

Figura 6: Examen de servicio de la zona de Internet a la zona DMZ



Esta directiva aplica el examen de la capa 7 de la zona de Internet al DMZ. Esto permite las conexiones de la zona de Internet al DMZ, y permite el tráfico de retorno de los host DMZ a los host de Internet que originaron la conexión. La directiva de Internet DMZ combina el examen de la capa 7 con los grupos de dirección definidos por los ACL para restringir el acceso a los servicios específicos en los host específicos, a los grupos de host, o a las subredes. Esto es lograda jerarquizando un clase-mapa que especifica los servicios dentro de otro clase-mapa que se refiere a un ACL para especificar los IP Addresses.

1. Defina class-maps y los ACL que describan el tráfico que usted quiere permitir entre las

zonas, según las directivas descritas anterior.Class-maps múltiple para los servicios debe ser utilizado, pues las políticas de acceso de diferenciación serán aplicadas para el acceso a dos diversos servidores. Los host de Internet no se prohiben el DNS y las conexiones HTTP a 172.16.2.2, y las conexiones SMTP se permiten a 172.16.2.3. Observe la diferencia en el class-maps. Los servicios que especifican class-maps utilizan la palabra clave del **match-any** para permitir los servicios mencionados uces de los. Los ACL de asociación class-maps con el uso class-maps del servicio la palabra clave **corresponda con todos** de requerir que ambas condiciones en la correspondencia de la clase se deben cumplir para permitir el tráfico:`conf t`

```
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 las correspondencias de políticas para examinar el tráfico en el class-maps usted definir:`conf t`

```
policy-map type inspect internet-dmz-policy
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
```

3. Configure Internet y las zonas DMZ y asigne las interfaces del router a sus zonas respectivas. Salte la configuración de DMZ si usted la fija para arriba en la sección anterior:`conf t`

```
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```

4. Configure los zona-pares y aplique el directiva-mapa apropiado.**Nota:** Usted necesita solamente configurar los pares de la zona del Internet DMZ actualmente, para examinar las conexiones originadas en la zona del Internet que viaja a la zona DMZ:`conf t`

```
zone-pair security internet-dmz source internet destination dmz
 service-policy type inspect internet-dmz-policy
```

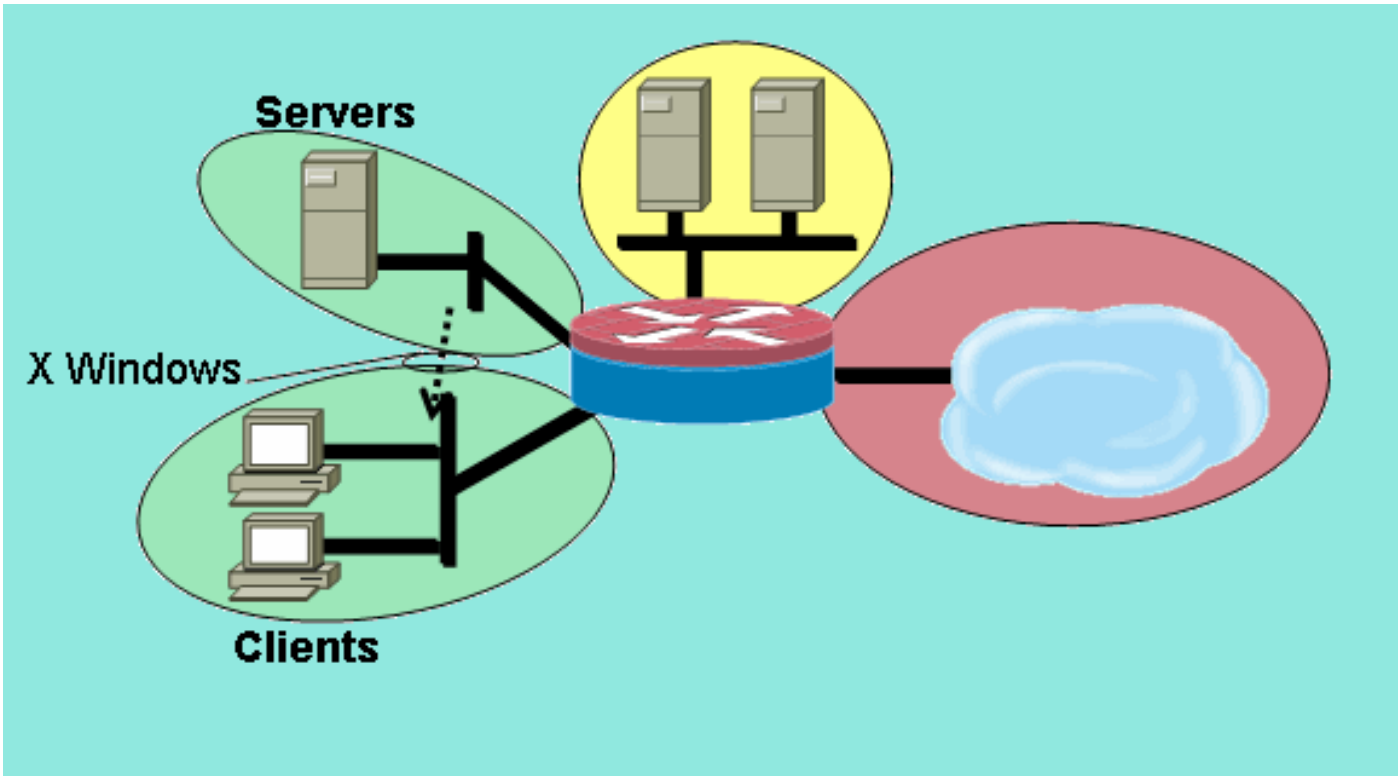
Esto completa la configuración de la directiva direccionamiento-específica del examen de la capa 7 en los zona-pares de Internet DMZ.

Firewall transparente de la inspección con estado

Directiva de los Servidor-clientes de la configuración

El cuadro 7 ilustra la configuración de la directiva del servidor-cliente.

Figura 7: Examen de servicio de la zona de los servidores a la zona de los clientes



La directiva de los servidor-clientes aplica el examen usando un servicio definido por el usario. El examen de la capa 7 es aplicado de la zona de los servidores a la zona de los clientes. Esto permite las conexiones del X Windows a un rango de puertos específico de la zona de los servidores a la zona de los clientes, y permite el tráfico de retorno. El X Windows no es nativo un protocolo admitido en el PAM, así que un servicio del usuario configurado en el PAM debe ser definido así que el ZFW puede reconocer y examinar el tráfico apropiado.

Dos o más interfaces del router se configuran en un bridge-group de IEEE para proporcionar el Integrated Routing and Bridging (IRB) para proporcionar el bridging entre las interfaces en el bridge-group y la encaminamiento a otras subredes vía el (BVI) del Interfaz Virtual de Bridge. Las políticas del firewall transparentes ofrecerán aplican el examen del Firewall para el tráfico “que cruza el Bridge”, pero no para el tráfico que deja el bridge-group vía el BVI. La directiva del examen se aplica solamente para traficar cruzando el bridge-group. Por lo tanto, en este escenario, el examen será aplicado solamente para traficar que los movimientos entre las zonas de los clientes y servidores, que se jerarquizan dentro de la zona privada. La directiva aplicada entre la zona privada, y el público y las zonas DMZ, entra en solamente el juego cuando el tráfico deja el bridge-group vía el BVI. Cuando el tráfico se va vía el BVI de los clientes o de las zonas de los servidores, las políticas del firewall transparentes no serán invocadas.

1. Configure el PAM con una entrada definida por el usario para el X Windows.Conexiones abiertas de los clientes del X Windows (donde se reciben las aplicaciones) para el mostrar información a los clientes (donde el usuario está trabajando) en un rango que comienza en el puerto 6900.Cada conexión adicional utiliza los puertos sucesivos, así que si un cliente visualiza 10 diversas sesiones sobre un host, el servidor utiliza los puertos 6900-6909. Por lo tanto, si usted examina el rango de puertos a partir de 6900 a 6909, las conexiones abiertas a los puertos más allá de 6909 fallarán:`conf t`
   `ip port-map user-Xwindows port tcp from 6900 to 6910`
2. Revise los documentos PAM para dirigir las preguntas adicionales PAM o para marcar la documentación para información granular del examen del protocolo sobre los detalles de la Interoperabilidad entre el PAM y la inspección con estado del Firewall Cisco IOS.
3. Defina class-maps que describa el tráfico que usted quiere permitir entre las zonas, según

las directivas descritas anterior:`conf t`

```
class-map type inspect match-any Xwindows-class
 match protocol user-Xwindows
```

4. Configure las correspondencias de políticas para examinar el tráfico en el class-maps usted definir:`conf t`

```
policy-map type inspect servers-clients-policy
 class type inspect Xwindows-class
  inspect
```

5. Configure las zonas del cliente y servidor y asigne las interfaces del router a sus zonas respectivas.Si usted configuró estas zonas y asignó las interfaces en la sección de configuración de la política de los Cliente-servidores, usted puede saltar a la definición de los zona-pares. Interligar la Configuración de IRB se proporciona para lo completo:`conf t`

```
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 los zona-pares y aplique el directiva-mapa apropiado.**Nota:** Usted necesita solamente configurar los pares de la zona de los servidor-clientes actualmente para examinar las conexiones originadas en la zona de los servidores que viaja a la zona de los clientes:`conf t`

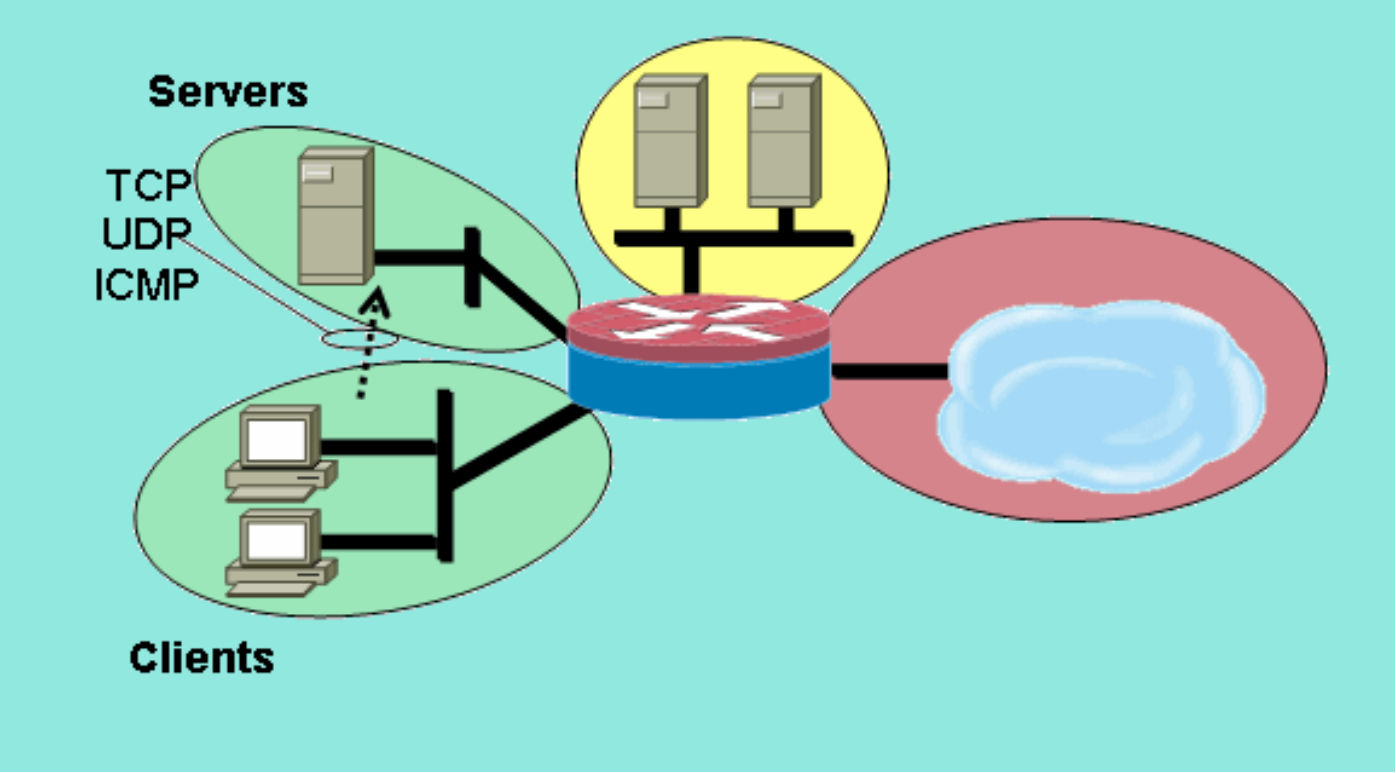
```
zone-pair security servers-clients source servers destination clients
 service-policy type inspect servers-clients-policy
```

Esto completa la configuración de la directiva definida por el usario del examen en los zona-pares de los servidor-clientes para permitir las conexiones del X Windows de la zona del servidor a la zona del cliente.

Directiva de los Cliente-servidores de la configuración

El cuadro 8 ilustra la configuración de la directiva del servidor del cliente.

Figura 8: Examen de servicio de la zona de los clientes a la zona de los servidores



La directiva de los cliente-servidor es menos compleja que las otras. El examen de la capa 4 es aplicado de la zona de los clientes a la zona de los servidores. Esto permite las conexiones de la zona de los clientes a la zona de los servidores, y permite el tráfico de retorno. El examen de la capa 4 lleva la ventaja de la simplicidad en la configuración de escudo de protección, en que solamente algunas reglas están requeridas para permitir la mayoría del tráfico de aplicación. Sin embargo, el examen de la capa 4 también lleva dos desventajas importantes:

- Las aplicaciones tales como FTP o los servicios de medios de flujo continuo negocian con frecuencia un canal subordinado adicional del servidor al cliente. Estas funciones se acomodan generalmente en un fixup del servicio que monitorean el diálogo del canal de control y permiten el canal subordinado. Esta capacidad no está disponible en el examen de la capa 4.
- El examen de la capa 4 permite casi todo el tráfico de la capa de la aplicación. Si el uso de la red se debe controlar tan solamente algunas aplicaciones se permiten con el Firewall, un ACL se deben configurar en el tráfico saliente para limitar los servicios permitidos con el Firewall.

Ambas interfaces del router se configuran en un Grupo de Bridge de IEEE, así que estas políticas del firewall aplicarán el examen transparente del Firewall. Esta directiva se aplica en dos interfaces en un Grupo de Bridge IP de IEEE. La directiva del examen se aplica solamente para traficar cruzando al Grupo de Bridge. Esto explica porqué las zonas de los clientes y servidores se jerarquizan dentro de la zona privada.

1. Defina class-maps que describa el tráfico que usted quiere permitir entre las zonas, según las directivas descritas anterior:`conf t`
```
class-map type inspect match-any L4-inspect-class
match protocol tcp
match protocol udp
match protocol icmp
```
2. Configure las correspondencias de políticas para examinar el tráfico en el class-maps usted definir:`conf t`
```
policy-map type inspect clients-servers-policy
class type inspect L4-inspect-class
 inspect
```

3. Configure las zonas de los clientes y servidores y asigne las interfaces del router a sus zonas respectivas:
```
conf t
zone security clients
zone security servers
int vlan 1
zone-member security clients
int vlan 2
zone-member security servers
```
4. Configure los zona-pares y aplique el directiva-mapa apropiado.**Nota:** Usted necesita solamente configurar los zona-pares de los cliente-servidores actualmente, para examinar las conexiones originadas en la zona de los clientes que viaja a la zona de los servidores:
```
conf t
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```
Esto completa la configuración de la directiva del examen de la capa 4 para que los zona-pares de los cliente-servidores permitan todas las conexiones TCP, UDP, y ICMP de la zona del cliente a la zona del servidor. La directiva no aplica el fixup para los canales subordinados, sino proporciona un ejemplo de la directiva simple para acomodar la mayoría de las conexiones de la aplicación.

Tarifa que limpia para el Firewall Zona-basado de la directiva

Las redes de datos se benefician con frecuencia con la capacidad de limitar a la velocidad de transmisión de los tipos de red específicos trafican, y de limitar el impacto del tráfico de prioridad inferior a un tráfico negocio-más esencial. El Cisco IOS Software ofrece esta capacidad con la Vigilancia de tráfico, que la velocidad nominal y la explosión del tráfico de los límites. El Cisco IOS Software ha soportado la Vigilancia de tráfico desde el Cisco IOS Release 12.1(5)T.

El Cisco IOS Software Release 12.4(9)T aumenta ZFW con la limitación de la tarifa agregando la capacidad para limpiar el tráfico que corresponde con las definiciones de un clase-mapa específico mientras que atraviesa el Firewall a partir de una zona de Seguridad a otra. Esto proporciona la conveniencia de ofrecer una punta de la configuración para describir el tráfico específico, aplicar las políticas del firewall, y la policía el consumo de ancho de banda de ese tráfico. El policing ZFW diferencia del policing basado en la interfaz en que proporciona solamente las acciones transmite para la conformidad y el descenso de la directiva para la infracción de la directiva. El policing ZFW no puede marcar el tráfico para el DSCP.

El policing ZFW puede especificar solamente el uso del ancho de banda en los bytes/en segundo lugar, paquete/en segundo lugar y el policing del porcentaje de ancho de banda no se ofrece. El policing ZFW puede ser aplicado con o sin el policing basado en la interfaz. Por lo tanto, si se requieren las capacidades adicionales del policing, estas características se pueden aplicar por el policing basado en la interfaz. Si el policing basado en la interfaz se utiliza conjuntamente con el policing del Firewall, asegúrese que no estén en conflicto las directivas.

Configurar el policing ZFW

El policing ZFW limita el tráfico en el clase-mapa de una correspondencia de políticas a un valor de velocidad definido por el usario entre 8,000 y 2,000,000,000 bits por segundo, con un valor de ráfaga configurable en el rango de 1,000 a 512,000,000 bytes.

El policing ZFW es configurado por una línea adicional de configuración en el directiva-mapa, que es aplicado después de la acción de 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 sesión

ZFW que limpia el control de sesión también introducido para limitar la cuenta de sesiones para el tráfico en un directiva-mapa que corresponde con un clase-mapa. Esto agrega a la capacidad existente para aplicar la directiva del protección DoS por el clase-mapa. Con eficacia, esto permite el control granular en el número de sesiones que corresponden con cualquier clase-mapa dado que crucen un zona-par. Si el mismo clase-mapa se utiliza en las correspondencias de políticas o los zona-pares múltiples, diversos límites de sesión se pueden aplicar en las diversas aplicaciones del clase-mapa.

El control de sesión es aplicado configurando un parámetro-mapa que contenga el volumen deseado de la sesión, entonces añadiendo el parámetro-mapa al final del fichero a la acción del examen aplicada a un clase-mapa bajo un directiva-mapa:

```
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
```

las Parámetro-correspondencias se pueden aplicar solamente a la acción de la inspección, y no están disponibles en el paso o las acciones de descarte.

Las actividades del control y del policing de la sesión ZFW son visibles con este comando

show policy-map type inspect zone-pair

Inspección de la aplicación

La Inspección de la aplicación introduce la capacidad adicional a ZFW. Las directivas de la Inspección de la aplicación son aplicadas en la capa 7 del modelo de OSI, donde las aplicaciones de usuario envían y reciben los mensajes que permiten que las aplicaciones ofrezcan las capacidades útiles. Algunas aplicaciones pudieron ofrecer las capacidades indeseadas o vulnerables, así que los mensajes asociados a estas capacidades se deben filtrar para limitar las actividades en los servicios de aplicación.

El Cisco IOS Software ZFW ofrece la Inspección de la aplicación y el control en estos servicios de aplicación:

- HTTP
- SMTP
- POP3
- IMAP
- Sun RPC
- Tráfico de aplicación P2P
- IM aplicaciones

La Inspección de la aplicación y el control (AIC) varía en la capacidad por el servicio. El examen HTTP ofrece la filtración granular en varios tipos de actividad de la aplicación, ofreciendo las capacidades para limitar el tamaño de la transferencia, las longitudes de la dirección Web, y la

actividad del navegador para aplicar la conformidad con los estándares de la conducta de la aplicación y para limitar los tipos de contenido que se transfieren sobre el servicio. El AIC para el S TP puede limitar la longitud contenta y aplicar la conformidad del protocolo. El examen POP3 y IMAP puede ayudar a asegurarse de que los usuarios están utilizando aseguran los mecanismos de autenticación para prevenir el compromiso de los credenciales de usuario.

La Inspección de la aplicación se configura como conjunto adicional de class-maps específico a la aplicación y de correspondencias de políticas, que entonces son aplicadas al examen existente class-maps y a las correspondencias de políticas definiendo la directiva de servicio de aplicación en el directiva-mapa del examen.

Inspección de la aplicación HTTP

La Inspección de la aplicación se puede aplicar en el tráfico HTTP para controlar el uso indeseado del puerto del servicio HTTP para otras aplicaciones tales como capacidad de compartir archivos de IM, P2P, y aplicaciones del Tunelización que puedan reorientar las aplicaciones de otra manera firewalled con TCP 80.

Configure un clase-mapa de la Inspección de la aplicación para describir el tráfico que viola 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
```

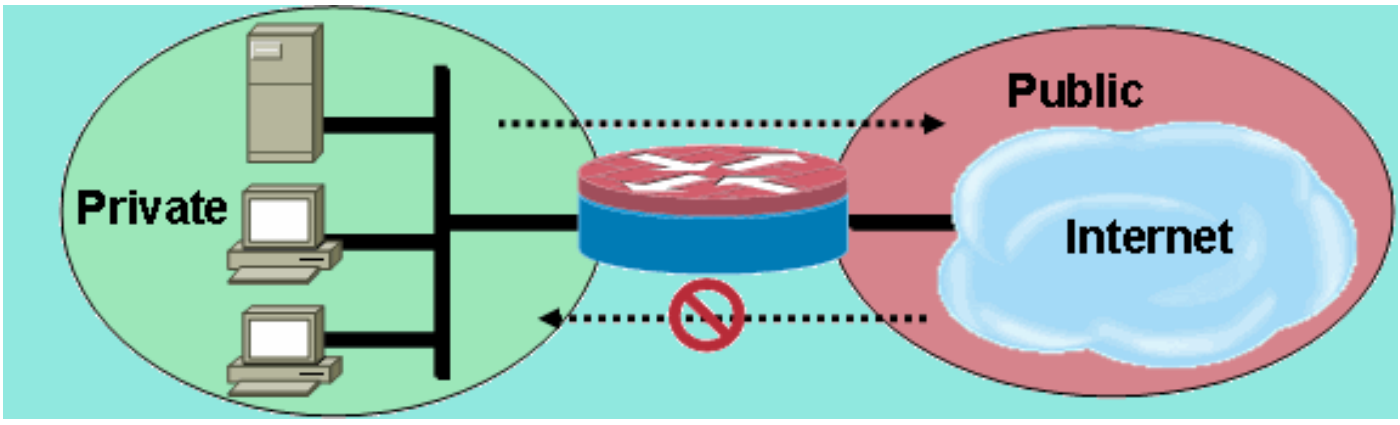
Mejoras de la Inspección de la aplicación HTTP

El Cisco IOS Software Release 12.4(9)T introduce las mejoras a las capacidades del examen HTTP ZFW. Inspección de la aplicación introducida Firewall Cisco IOS HTTP en el Cisco IOS Software Release 12.3(14)T. El Cisco IOS Software Release 12.4(9)T aumenta las capacidades existentes agregando:

- Capacidad de permitir, de negar, y de monitorear las peticiones y las respuestas basadas en el nombre y los valores de encabezado de la encabezado. Esto es útil para bloquear las peticiones y las respuestas que llevan los campos del encabezado vulnerables.

- Capacidad de limitar los tamaños de diversos elementos en el pedido de HTTP y los encabezados de respuesta tales como longitud máxima URL, longitud del encabezado máxima, número máximo de encabezados, longitud de línea del encabezado máxima, etc. Esto es útil para prevenir los desbordamientos de búfer.
- Capacidad de bloquear las peticiones y respuestas que llevan las encabezados múltiples del mismo tipo; por ejemplo, una petición con dos encabezados de la contenido-longitud.
- Capacidad de bloquear las peticiones y las respuestas con las encabezados NON-ASCII. Esto es útil para prevenir los diversos ataques que utilizan el binario y otros caracteres NON-ASCII para entregar los gusanos y el otro contenido malévolo a los servidores Web.
- La capacidad de agrupar los métodos HTTP en las categorías definidas por el usuario y la flexibilidad para bloquear/permiten/monitor que cada uno del grupo se ofrece. El HTTP RFC permite un conjunto restricto de los métodos HTTP. Algunos de los métodos estándars se consideran inseguros porque pueden ser utilizadas para explotar las vulnerabilidades en un servidor Web. Muchos de los métodos no estándar tienen un mún expediente de la Seguridad.
- Método para bloquear los URI específicos basados en una expresión normal del usuario configurado. Esta característica da a usuario la capacidad para bloquear la aduana URI y las interrogaciones.
- La capacidad a la encabezado del spoof teclea (especialmente tipo de la encabezado del servidor) con las cadenas adaptables del usuario. Esto es útil en un caso donde un atacante analiza las respuestas del servidor Web y aprende tanta información como sea posible, después pone en marcha un ataque que explote las debilidades en ese servidor Web especial.
- Capacidad de bloquear o de publicar una alerta en una conexión HTTP si uno o más Valores de parámetro HTTP corresponden con los valores ingresados por el usuario como expresión normal. Algunos de los contextos posibles del valor HTTP incluyen la encabezado, el cuerpo, el nombre de usuario, la contraseña, el agente de usuario, la línea de la petición, la línea del estado, y las variables decodificadas CGI.

Los ejemplos de configuración para las mejoras de la Inspección de la aplicación HTTP asumen una red simple:



El Firewall agrupa el tráfico en dos clases:

- Tráfico HTTP
- El resto del tráfico monocanal TCP, UDP, y ICMP

El HTTP se separa para permitir el examen específico en el tráfico de la Web. Esto permite que usted configuren el policing en la primera sección de este documento, y la Inspección de la aplicación HTTP en la segunda sección. Usted configurará class-maps específico y las

correspondencias de políticas para el P2P e IM tráfico en la tercera sección de este documento. La Conectividad se permite de la zona privada a la zona pública. No se proporciona ninguna Conectividad de la zona pública a la zona privada.

Una configuración completa que implementa la directiva inicial se proporciona en el C del apéndice, configuración de escudo de protección básica de la Zona-directiva para dos zonas.

Configurar las mejoras de la Inspección de la aplicación HTTP

La Inspección de la aplicación HTTP (así como otras directivas de la Inspección de la aplicación) requiere más Configuración compleja que la configuración de la capa básica 4. Usted debe configurar la Clasificación de tráfico y la directiva de la capa 7 para reconocer el tráfico específico que usted desea controlar, y para aplicar la acción deseada al tráfico deseable e indeseable.

La Inspección de la aplicación HTTP (similar a otros tipos de Inspección de la aplicación) se puede aplicar solamente al tráfico HTTP. Así, usted debe definir la capa 7 class-maps y las correspondencias de políticas para el tráfico HTTP específico, después define un clase-mapa Layer-4 específicamente para el HTTP, y aplica la directiva Layer-7 al examen HTTP en un directiva-mapa Layer-4, como tal:

```
!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 características de tráfico de la Inspección de la aplicación HTTP se definen en un clase-mapa de la capa 7:

- **Examen de la encabezado** — Este comando proporciona la capacidad de permitir/niega/las peticiones o las respuestas del monitor cuya encabezado hace juego la expresión normal configurada. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6-HTTP_HDR_REGEX_MATCHED`*Comando usage:*`match {request|response|req-resp} header regex <parameter-map-name>` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear la petición o la respuesta cuya encabezado contiene los caracteres NON-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
```

- **Examen de la longitud del encabezado** — Este comando marca la longitud de una petición o de un encabezado de respuesta y aplica la acción si la longitud excede el umbral configurado. La acción es permite o reajustó. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-4- HTTP_HEADER_LENGTH`*Comando usage:*`match {request|response|req-resp} header length gt <bytes>` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear las peticiones y las respuestas que tienen mayores de 4096 bytes de la longitud del encabezado.
```
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
```

- **Examen de la cuenta de la encabezado** — Este comando verifica el número de líneas del encabezado (campos) en una petición/una respuesta y aplica la acción cuando la cuenta excede el umbral configurado. La acción es permite o reajustó. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6- HTTP_HEADER_COUNT`. *Comando usage:*`match {request|response|req-resp} header count gt <number>` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear una petición que tenga más de 16 campos del 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
```

- **Examen de campo del encabezado** — Este comando proporciona la capacidad de permitir/niega/las peticiones/las respuestas del monitor que contienen un campo del específico encabezado HTTP y lo valoran. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED`*Comando usage:*`match {request|response|req-resp} header <header-name>` *Caso del uso de la muestra*Configure una directiva de la Inspección de la aplicación HTTP para bloquear el spyware/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
```

- **Examen de la longitud de campo del encabezado** — Este comando proporciona una capacidad de limitar la longitud de una línea de campo del encabezado. Permita o reajustar la

acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6-HTTP_HDR_FIELD_LENGTH`. *Comando usage:*`match {request|response|req-resp} header <header-name> length gt <bytes>` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear una petición cuya extensión del campo del Cookie y del agente de usuario exceda el 256 y el 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
```

- **Examen de la repetición del campo del encabezado** — Este comando marca si una petición o una respuesta ha relanzado los campos del encabezado. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. Cuando está habilitada, la acción del registro causa un mensaje de Syslog:`APPFW-6-HTTP_REPEATED_HDR_FIELDS`. *Comando usage:*`match {request|response|req-resp} header <header-name>` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear una petición o una respuesta que tenga líneas del encabezado múltiples de la contenido-longitud. Éste es una de las funciones más útiles usadas para prevenir el contrabando de la sesión.`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
```

- **Examen del método** — El HTTP RFC permite un conjunto restricto de los métodos HTTP. Sin embargo, incluso algunos de los métodos estándars se consideran inseguros mientras que algunos métodos se pueden utilizar para explotar las vulnerabilidades en un servidor Web. Muchos de los métodos no estándar se utilizan con frecuencia para la actividad maliciosa. Esto necesita una necesidad de agrupar los métodos en las diversas categorías y de tener el usuario elegir la acción para cada categoría. Este comando proporciona al usuario una manera flexible de agrupar los métodos en las diversas categorías tales como métodos seguros, métodos inseguros, métodos del webdav, métodos RFC, y métodos extendidos. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que haga juego los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6-HTTP_METHOD`. *Comando usage:*`match request method <method>` *Caso del uso de la muestra*Configure una directiva del appfw HTTP que agrupe los métodos HTTP en tres categorías: caja fuerte, inseguro y webdav. Éstos se muestran en la tabla. Acciones de la configuración tales que:todos los métodos seguros se permiten sin el registrotodos los métodos inseguros se permiten con el registrotodos los métodos del webdav se bloquean con el registro.`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
```

- **Examen de URI** — Este comando proporciona la capacidad de permitir/niega/las peticiones del monitor cuyo URI hace juego el examen regular configurado. Esto da a usuario una capacidad para bloquear la aduana URL y las interrogaciones. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6-HTTP_URI_REGEX_MATCHED` *Comando usage:* `match request uri regex <parameter-map-name>` *Caso del uso de la muestra* Configure una directiva del appfw HTTP para bloquear una petición cuyo URI haga juego ninguno de estos expresiones normales:. *cmd.exe. *sex. el *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
```

- **Examen de la longitud de URI** — Este comando verifica la longitud de URI que es enviado en una petición y aplica la acción configurada cuando la longitud excede el umbral configurado. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6- HTTP_URI_LENGTH`. *Comando usage:* `match request uri length gt <bytes>` *Caso del uso de la muestra* Configure una directiva del appfw HTTP para aumentar una alarma siempre que la longitud de URI de una petición exceda 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
```

- **Examen del argumento** — Este comando proporciona una capacidad de permitir, de negar o de monitorear la petición cuyos argumentos (parámetros) haga juego el examen regular configurado. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6- HTTP_ARG_REGEX_MATCHED` *Comando usage:* `match request arg regex <parameter-map-name>` *Caso del uso de la muestra* Configure una directiva del appfw HTTP para bloquear una petición cuyos argumentos hagan juego ninguno de estos expresiones normales:. *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
```

- **Examen de la longitud del argumento** — Este comando verifica la longitud de los argumentos que son enviados en una petición y aplica la acción configurada cuando la longitud excede el umbral configurado. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6- HTTP_ARG_LENGTH`.*Comando usage:*`match request arg length gt <bytes>` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para aumentar una alarma siempre que la longitud del argumento de una petición exceda 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
```
- **Examen de cuerpo** — Este CLI permite que el usuario especifique la lista de expresiones normales que se corresponderán con contra el cuerpo de la petición o de la respuesta. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6- HTTP_BODY_REGEX_MATCHED`*Comando usage:*`match {request|response|reg-resp} body regex <parameter-map-name>` *Caso del uso de la muestra*Configure un appfw HTTP para bloquear una respuesta cuyo cuerpo contenga el modelo.
```
* [Kk] del [Cc] del [Aa] del [Tt] del [Tt] del [Aa]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
```
- **Examen (contento) de la longitud del cuerpo** — Este comando verifica el tamaño del mensaje que es enviado con la petición o la respuesta. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-4- HTTP_CONTENT_LENGTH`*Comando usage:*`match {request|response|req-resp} body length lt <bytes> gt <bytes>` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear una sesión HTTP que lleve más entonces el mensaje de los bytes 10K en una petición o una 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
```
- **Examen de la línea del estado** — El comando permite que el usuario especifique la lista de expresiones normales que se corresponderán con contra la línea del estado de una respuesta. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6-HTTP_STLINE_REGEX_MATCHED`.*Comando usage:*`match response`

`status-line regex <class-map-name>` *Caso del uso de la muestra*Configure un appfw HTTP para registrar una alarma siempre que una tentativa se haga para acceder una página prohibida. Una página prohibida contiene generalmente un código de estado 403 y los parecer de la línea del estado `HTTP/1.0 403 paginan prohibido \ 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
```

- **Examen del tipo de contenido** — Este comando verifica si el tipo de contenido del encabezado del mensaje está en la lista de los tipos de contenido soportados. También verifica que el tipo de contenido de la encabezado haga juego el contenido de los datos del mensaje o de la porción del cuerpo de entidad. Si se configura la **discordancía de la** palabra clave, el comando verifica el tipo de contenido del mensaje de respuesta contra el valor de campo validado del mensaje request. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa el mensaje de Syslog apropiado:`APPFW-4- HTTP_CONT_TYPE_VIOLATION, APPFW-4- HTTP_CONT_TYPE_MISMATCH, APPFW-4- HTTP_CONT_TYPE_UNKNOWN`*Comando usage:*`match {request|response|req-resp} header content-type [mismatch|unknown|violation]` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear una sesión HTTP que lleve las peticiones y las respuestas que tienen el tipo de contenido desconocido.

```
   match req-resp header content-type unknown

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

- **examen del Puerto-uso erróneo** — Se utiliza este comando de prevenir el puerto HTTP (80) que es empleado mal para otras aplicaciones tales como IM, P2P, Tunelización, los etc. permiten o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa el mensaje de Syslog apropiado:`APPFW-4- HTTP_PORT_MISUSE_TYPE_IM APPFW-4-HTTP_PORT_MISUSE_TYPE_P2P APPFW-4-HTTP_PORT_MISUSE_TYPE_TUNNEL`*Comando usage:*`match request port-misuse {im|p2p|tunneling|any}` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear una sesión HTTP que es empleada mal para IM la aplicación.

```
   match request port-misuse im

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

- **examen Estricto-HTTP** — Este comando habilita el control estricto de la conformidad del protocolo contra los pedidos de HTTP y las respuestas. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-4-HTTP_PROTOCOL_VIOLATION`*Comando usage:*`match req-resp protocol-violation`*Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear las peticiones o las respuestas que violan el 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
```

- **Examen de la Transferencia-codificación** — Este comando proporciona una capacidad de permitir, de negar o de monitorear la petición/la respuesta cuyo tipo de la codificación de la transferencia hace juego con el tipo configurado. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-6-HTTP_TRANSFER_ENCODING` *Comando usage:* `match {request|response|req-resp} header transfer-encoding {regex <parameter-map-name> |gzip|deflate|chunked|identity|all}` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear una petición o una respuesta que tenga codificación del tipo de la compresa.
```
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
```
- **Examen de la Java Applet** — Este comando marca si una respuesta tiene subprogramas java y aplica la acción configurada al detectar el applet. Permita o reajustar la acción se puede aplicar a una petición o a una respuesta que corresponde con los criterios del clase-mapa. La adición de la acción del registro causa un mensaje de Syslog:`APPFW-4- HTTP_JAVA_APPLET` *Comando usage:* `match response body java-applet` *Caso del uso de la muestra*Configure una directiva del appfw HTTP para bloquear los subprogramas 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 ZFW para el control de la aplicación de la Mensajería inmediata y del peer a peer

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

El Cisco IOS Software primero ofreció el soporte para IM el control de la aplicación en el Cisco IOS Software Release 12.4(4)T. La versión inicial de ZFW no hizo aplicación del soporte IM en la interfaz ZFW. Si el control de la aplicación IM fue deseado, los usuarios no podían emigrar a la interfaz de la configuración ZFW. El Cisco IOS Software Release 12.4(9)T introduce el soporte ZFW para IM el examen, soportando Yahoo! Mensajero (YM), MSN Messenger (MSN), y AOL Instant Messenger (AIM).

El Cisco IOS Software Release 12.4(9)T es la primera versión del Cisco IOS Software que ofrece el soporte del Firewall del Native IOS para las aplicaciones de intercambio de archivos P2P.

Directivas de la capa 4 y de la capa 7 de la oferta de ambo examen de IM y P2P para el tráfico de aplicación. Esto significa que ZFW puede proporcionar la inspección con estado básica para permitir el permit or deny el tráfico, así como el control granular de la capa 7 en las actividades específicas en los diversos protocolos, para permitir ciertas actividades de la aplicación mientras que se niegan otras.

Inspección de la aplicación y control P2P

El SDM 2.2 introdujo el control de la aplicación P2P en su sección de configuración de escudo de protección. El SDM aplicó un Network-Based Application Recognition (NBAR) y política de calidad de servicio (QoS) detectar y la actividad de la aplicación P2P de la policía a una línea tarifa de cero, bloqueando todo el tráfico P2P. Esto planteó la cuestión que los usuarios CLI, contando con el soporte P2P en el escudo de protección IOS CLI, no podían configurar el P2P que bloqueaba en el CLI a menos que fueran conscientes de la configuración necesaria NBAR/QoS. El Cisco IOS Software Release 12.4(9)T introduce el control nativo P2P en el ZFW CLI, leveraging el NBAR para detectar la actividad de la aplicación P2P. Este soportes para la versión de software varios protocolos de la aplicación P2P:

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

Las aplicaciones P2P son determinado difíciles de detectar, como resultado del comportamiento de la “puerto-lupulización” y de otros trucos para evitar la detección, así como de los problemas introducidos por los cambios y las actualizaciones frecuentes a las aplicaciones P2P que modifican los comportamientos de los protocolos. ZFW combina la inspección con estado nativa del Firewall con las capacidades del tráfico-reconocimiento NBAR para entregar el control de la aplicación P2P en la interfaz de la configuración COMPLETA ZFW. El NBAR ofrece dos ventajas excelentes:

- El reconocimiento de la aplicación heurístico-basado opcional para reconocer las aplicaciones a pesar del complejo, difícil-a-detecta el comportamiento
- Infraestructura extensible que ofrece un mecanismo de la actualización para permanecer al corriente de las actualizaciones del protocolo y de las modificaciones

Configurar el examen P2P

Según lo mencionado anterior, el examen P2P y el control ofrece la inspección con estado de la capa 4 y acoda el control de 7 aplicaciones.

El examen de la capa 4 se configura semejantemente a otros servicios de aplicación, si el examen de los puertos nativos del servicio de aplicación es adecuado:

```
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]
```

Note la opción adicional de la firma en el [service-name] del protocolo de la coincidencia. Agregando la opción de la firma en el final de la sentencia de protocolo de la coincidencia, la heurística NBAR se aplica al tráfico para buscar para los telltales en el tráfico que indican la actividad específica de la aplicación P2P. Esto incluye la puerto-lupulización y otros cambios en la conducta de la aplicación para evitar la detección del tráfico. Este nivel de examen del tráfico viene en el precio de la utilización de la CPU incrementada y de la capacidad reducida del

rendimiento de la red. Si la opción de la firma no es aplicada, la análisis con detección heurística NBAR-basada no será aplicada para detectar el comportamiento de la puerto-lupulización, y la utilización de la CPU no será afectada al mismo fragmento.

El examen de servicio nativo lleva la desventaja que no puede mantener el control sobre las aplicaciones P2P en caso que la aplicación “salte” a un puerto de origen y de destino no estándar, o si la aplicación se pone al día para comenzar su acción en un número del puerto desconocido:

Aplicación	Puertos nativos (según lo reconocido por la lista 12.4(15)T PAM)
bittorrent	TCP 6881-6889
edonkey	TCP 4662
vía rápida	TCP 1214
gnutella	TCP 6346-6349 TCP 6355,5634 UDP 6346-6348
kazaa2	Dependiente en el PAM
winmx	TCP 6699

Si usted desea permitir (examinar) el tráfico P2P, usted puede ser que necesite proporcionar la configuración adicional. Algunas aplicaciones pudieron utilizar las redes múltiples P2P, o implemente los comportamientos específicos que usted puede ser que necesite para acomodar en su configuración de escudo de protección para permitir que la aplicación trabaje:

- Los clientes de BitTorrent comunican generalmente con los “perseguidores” (los Servidores del directorio del par) vía el HTTP que se ejecuta en algún puerto no estándar. Éste es típicamente TCP 6969, pero usted puede ser que necesite marcar el puerto torrente-específico del perseguidor. Si usted desea permitir BitTorrent, el mejor método para acomodar el puerto adicional es configurar el HTTP como uno de los protocolos de la coincidencia y agregar TCP 6969 al HTTP usando el **comando ip port-map**: **`ip port-map http port tcp 6969`** Usted necesitará definir el HTTP y bittorrent como los criterios de concordancia aplicados en el clase-mapa.
- el eDonkey aparece iniciar las conexiones que se detectan como el eDonkey y Gnutella.
- El examen de KaZaA es totalmente dependiente en la detección de la NBAR-firma.

El examen de la capa 7 (aplicación) aumenta el examen de la capa 4 con la capacidad para reconocer y para aplicar las acciones del servicio específico, tales como selectivamente bloqueo o permitir de la ARCHIVO-búsqueda, de la transferencia de archivos, y de las capacidades de la texto-charla. Las capacidades del servicio específico varían por el servicio.

La Inspección de la aplicación P2P es similar a la Inspección de la aplicación 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 la aplicación P2P ofrece las capacidades específicas a la aplicación para un subconjunto de las aplicaciones soportadas por el examen de la capa 4:

- edonkey
- vía rápida
- gnutella
- kazaa2

Cada uno de estas ofertas de las aplicaciones que varían los criterios de concordancia específicos a la aplicación de las opciones:

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
```

vía rápida

```
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)#match ? file-transfer Match file transfer stream flow Flow based QoS parameters
```

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 o actualizaciones del protocolo P2P a los protocolos existentes P2P se pueden cargar usando las funciones dinámicas de la actualización del pdlm del NBAR. Éste es el comando configuration de cargar el nuevo PDLM:

ip nbar pdlm *<file-location>*

El nuevo protocolo está disponible en los comandos del **protocolo de la coincidencia**… para el tipo de clase examina. Si el nuevo protocolo P2P tiene los servicios (sub-protocolos), la nueva capa 7 examina los tipos del clase-mapa, así como acoda 7 criterios de concordancia, está disponible.

IM Inspección de la aplicación y control

El Cisco IOS Software Release 12.4(4)T introdujo la Inspección de la aplicación IM y el control. El soporte IM no fue introducido con ZFW en 12.4(6)T, así que los usuarios no podían aplicar el control IM y ZFW en las mismas políticas del firewall, pues las características de firewall ZFW y de la herencia no pueden coexistir en una interfaz dada.

El Cisco IOS Software Release 12.4(9)T soporta la inspección con estado y el control de la

aplicación para estos servicios IM:

- AOL Instant Messenger
- MSN Messenger
- Yahoo! Mensajero

El examen IM varía levemente de la mayoría de los servicios, pues el examen IM confía en el acceso que controla a un grupo específico de host para cada servicio dado. Los servicios IM confían generalmente en un grupo relativamente permanente de Servidores del directorio, que los clientes deben poder entrar en contacto para acceder el servicio IM. Las aplicaciones IM tienden a ser muy difíciles de controlar de un punto de vista del protocolo o del servicio. La mayoría de la manera eficaz de controlar estas aplicaciones es limitar el acceso a los servidores fijos IM.

Configurar el examen IM

El examen IM y el control ofrece la inspección con estado de la capa 4 y acoda el control de 7 aplicaciones.

El examen de la capa 4 se configura semejantemente a otros servicios de aplicación:

```
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 IM pueden entrar en contacto sus servidores en los puertos múltiples para mantener sus funciones. Si usted desea permitir un servicio dado IM aplicando la acción de la inspección, usted puede ser que no necesite una lista de servidores definir el acceso permitido a los servidores del servicio IM. Sin embargo, configurar un clase-mapa que especifique un servicio dado IM, tal como AOL Instant Messenger, y aplicación de la acción de descarte en el directiva-mapa asociado puede hacer al cliente IM intentar y localizar un diverso puerto en donde la Conectividad se permite a Internet. Si usted no quiere permitir la Conectividad a un servicio dado, o si usted quiere restringir la texto-charla de la capacidad de servicio IM, usted debe definir una lista de servidores así que el ZFW puede identificar el tráfico asociado a la aplicación 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 Yahoo IM se define como tal:

```
parameter-map type protocol-info ymsgr-pmap
  server name scs.msg.yahoo.com
  server name scsd.msg.yahoo.com
  server ip 66.77.88.99
  server ip range 103.24.5.67 103.24.5.99
```

Usted necesitará aplicar la lista de servidores a la definición del protocolo:

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

Usted debe configurar la **búsqueda de dominio del IP** y los comandos de **ip.ad.re.ss del Servidor de nombres del IP** para habilitar la resolución de nombre.

Los nombres de servidor IM son bastante dinámicos. Usted necesitará marcar periódicamente que sus listas de servidores configuradas IM estén completas y correctas.

El examen de la capa 7 (aplicación) aumenta el examen de la capa 4 con la capacidad para reconocer y para aplicar las acciones del servicio específico, tales como selectivamente bloqueo o permitir de las capacidades de la texto-charla, mientras que niega las capacidades de otro servicio.

IM la Inspección de la aplicación ofrece actualmente la capacidad para distinguir entre la actividad de la texto-charla y el resto de los servicios de aplicación. Para restringir la texto-charla de la actividad IM, configure una directiva de la 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 directiva de la capa 7 a Yahoo! Directiva del mensajero configurada anterior:

```
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
```

Filtrado de URL

ZFW ofrece las capacidades del Filtrado de URL para limitar el acceso al contenido de la Web a ésa especificado por un blanco o una lista negra definida en el router, o remitiendo los Domain Name a un servidor del Filtrado de URL para verificar el acceso a los dominios específicos. El Filtrado de URL ZFW en los Cisco IOS Software Release 12.4(6)T a 12.4(15)T se aplica como acción de política adicional, similar a la Inspección de la aplicación.

Para el Filtrado de URL basado en el servidor, usted debe definir un parámetro-mapa que describa la Configuración del servidor del **urlfilter**:

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

Si se prefieren blancos estáticos o las listas negras, usted puede definir una lista de dominios o de subdomains que se permitan o se nieguen específicamente, mientras que la acción inversa se aplica para traficar que no hace juego la lista:

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

Si una lista negra URL se define usando niegue las opciones en las definiciones del exclusivo-dominio, el resto de los dominios será permitido. Si se definen algunas definiciones del “permiso”,

todos los dominios que serán permitidos se deben especificar explícitamente, similar a la función de las listas de control de acceso IP.

Configure un clase-mapa que haga juego el tráfico HTTP:

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

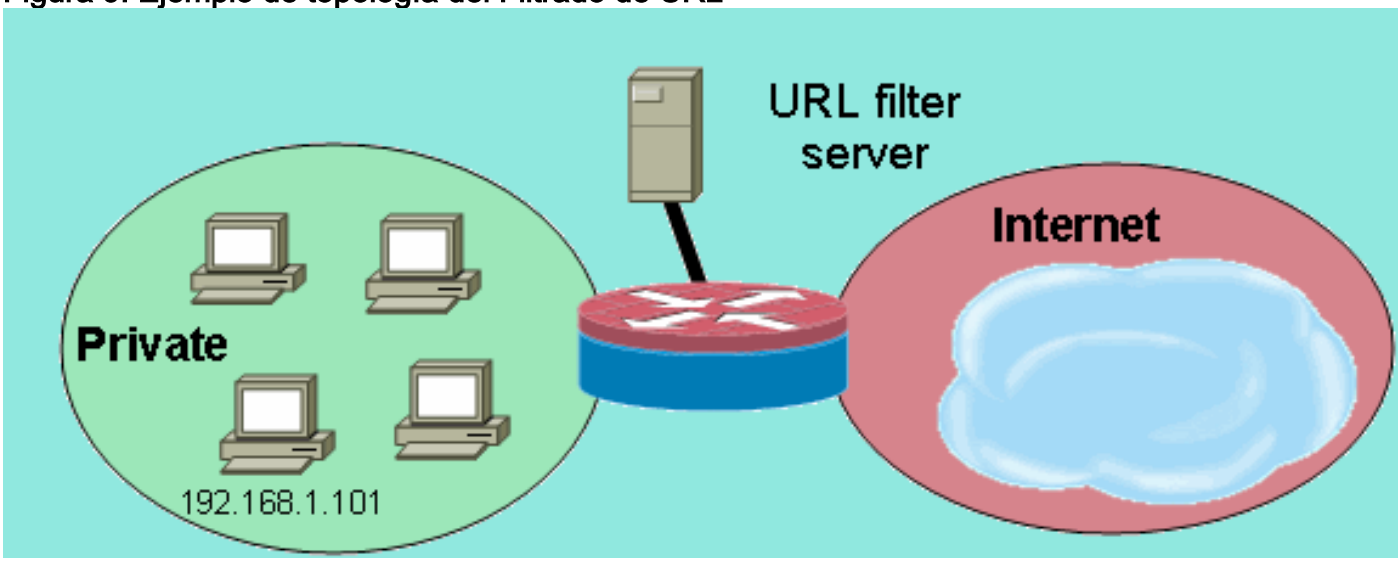
Defina un directiva-mapa con el cual asocie su clase-mapa **examinen** y las acciones del **urlfilter**:

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

Esto configura el requerimiento mínimo de comunicar con un servidor del Filtrado de URL. Varias opciones están disponibles definir el comportamiento adicional del Filtrado de URL.

Algunas instrumentaciones de red pudieron querer aplicar el Filtrado de URL para algunos host o subredes, mientras que desviaban el Filtrado de URL para otros host. Por ejemplo, en el cuadro 9, todos los host en la zona privada deben tener tráfico HTTP marcado por un servidor del filtro URL, a excepción del host específico 192.168.1.101.

Figura 9: Ejemplo de topología del Filtrado de URL



Esto puede ser lograda definiendo dos diversas correspondencias del clase-mapa:

- Un clase-mapa que hace juego solamente el tráfico HTTP para el grupo más grande de host, que recibirán el Filtrado de URL.
- Un clase-mapa para el grupo más pequeño de host, que no recibirán el Filtrado de URL. El segundo clase-mapa hará juego el tráfico HTTP, así como una lista de host que sean eximidos de la directiva del Filtrado de URL.

Ambo class-maps se configura en un directiva-mapa, pero solamente uno recibirá la acción del **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
```

Acceso que controla al router

La mayoría de los ingenieros de la seguridad de la red son incómodos exponiendo las interfaces de administración del router (por ejemplo, SSH, Telnet, HTTP, HTTPS, SNMP, y así sucesivamente) al Internet pública, y en determinadas circunstancias, el control pudo ser necesario para el acceso a LAN al router también. El Cisco IOS Software ofrece varias opciones para limitar el acceso a las diversas interfaces, que incluye la familia de la característica de la protección de la fundación de la red (NFP), los diversos mecanismos del control de acceso para las interfaces de administración, y la uno mismo-zona ZFW. Usted debe revisar las otras funciones, tales como control de acceso del VTY, protección del plano de administración, y control de acceso SNMP para determinar qué combinación de características del control del router trabajará mejor para su aplicación específica.

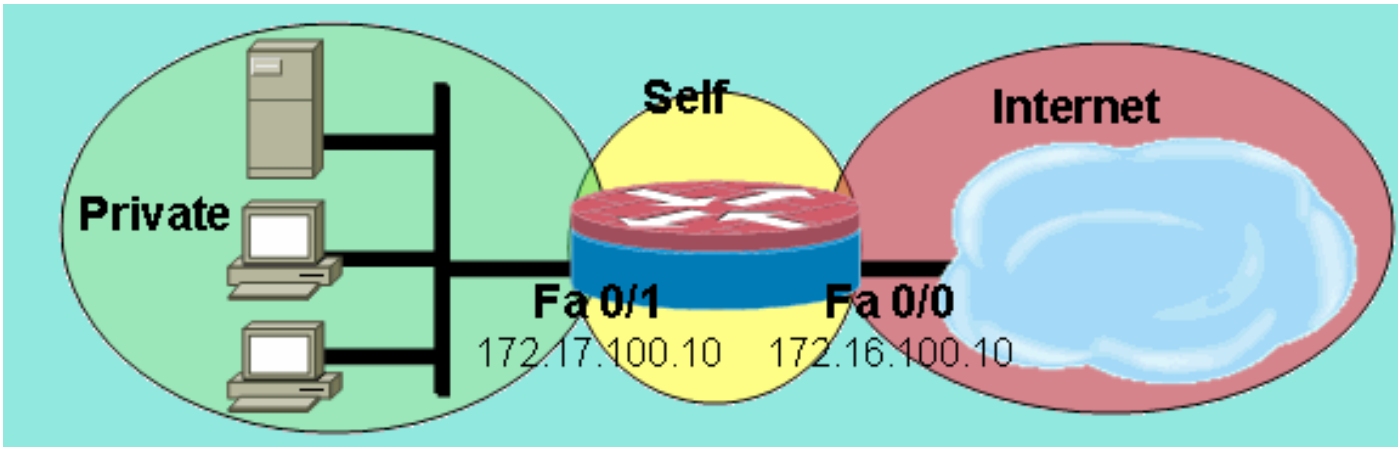
Generalmente, la familia de la característica NFP es más adecuada para el control del tráfico destinado para el router sí mismo. Refiera a la Descripción general de seguridad plana del control en Cisco IOS Software para la información que describe la protección del router usando las características NFP.

Si usted decide aplicar ZFW al tráfico de control a y desde los IP Addresses en el router sí mismo, usted debe entender que la política predeterminada y las capacidades del Firewall diferencian de ésas disponibles para el tráfico de tránsito. El tráfico de tránsito se define como tráfico de la red cuyos IP Address de origen y de destino no correspondan con ningunos IP Addresses aplicados a las interfaces del Routers un de los, y el tráfico no hará el router enviar, por ejemplo, los mensajes del control de red tales como expiración o red/imposible acceder al host mensajes ICMP TTL.

ZFW aplica un valor por defecto negar-toda directiva para traficar la mudanza entre las zonas, excepto, como se menciona en las reglas generales, tráfico en cualquier zona que fluye directamente a los direccionamientos de las interfaces del router se permite implícito. Esto asegura que la Conectividad a las interfaces de administración del router está mantenida cuando una configuración de escudo de protección de la zona se aplica al router. Si la misma negar-toda directiva afectara a la Conectividad directamente al router, una configuración completa de la política de administración tendría que ser aplicada antes de que las zonas se configuren en el router. Esto interrumpiría probablemente la Conectividad de la Administración si la directiva fue implementada o aplicada incorrectamente en la orden incorrecta.

Cuando una interfaz se configura para ser un miembro de la zona, los host conectados con la interfaz se incluyen en la zona. Sin embargo, el flujo de tráfico a y desde los IP Addresses de las interfaces del router no es controlado por las directivas de la zona (a excepción de las circunstancias descritas en la nota después del cuadro 10). En lugar, todas las interfaces IP en el router automáticamente se hacen parte de la zona del uno mismo cuando se configura ZFW. Para controlar el tráfico IP que se mueve a las interfaces del router desde las diversas zonas en un router, las directivas se deben aplicar para bloquear o permitir/examine el tráfico entre la zona y la zona del uno mismo del router, y vice versa. (Véase el cuadro 10.)

Figura 10: Aplique la directiva entre las zonas de la red y la zona del uno mismo del router



Aunque el router ofrezca una directiva de la valor por defecto-permisión entre todas las zonas y la zona del uno mismo, si una directiva se configura de cualquier zona a la zona del uno mismo, y no se configura ninguna directiva del uno mismo a las zonas interfaz-conectadas utilizador configurable del router, todo el tráfico router-originado encuentra la directiva de la uno mismo-zona de la conectar-zona en su vuelta el router y se bloquea. Así, el tráfico router-originado se debe examinar para permitir su vuelta a la zona del uno mismo.

Nota: El Cisco IOS Software utiliza siempre la dirección IP asociada a las computadoras principales de destino “más cercanas” de una interfaz para el tráfico tal como Syslog, tftp, telnet, y otros servicios de la controle de plano, y sujeta estas políticas del firewall de la uno mismo-zona del tráfico. Sin embargo, si un servicio define una interfaz específica como la interfaz de origen usando los comandos que incluyen, pero no limitado al **[type number] de registración de la interfaz de origen**, al **[type number] de la interfaz de origen de tftp del IP**, y al **[type number] de la interfaz de origen telnet del IP**, el tráfico se sujeta a la uno mismo-zona.

Nota: Algunos servicios (determinado servicios de la voz sobre IP del Routers) utilizan las interfaces efímeras o no configurables que no se pueden asignar a las zonas de Seguridad. Estos servicios no pudieron funcionar correctamente si su tráfico no se puede asociar a una zona de Seguridad configurada.

Limitaciones de la directiva de la Uno mismo-zona

la directiva de la Uno mismo-zona ha limitado las funciones con respecto a las directivas disponibles para los zona-pares del tráfico de tránsito:

- Al igual que el caso con la inspección con estado clásica, el tráfico router-generado se limita al TCP, al UDP, al ICMP, y al examen del protocolo complejo para H.323.
- La Inspección de la aplicación no está disponible para las directivas de la uno mismo-zona.
- La sesión y valora la limitación no se puede configurar en las directivas de la uno mismo-zona.

Configuración de la política de la Uno mismo-zona

Bajo la mayoría de circunstancias, éstas son políticas de acceso deseables para los servicios de administración del router:

- Niegue toda la conectividad de Telnet, como el protocolo del texto claro de Telnet expone fácilmente los credenciales de usuario y la otra información vulnerable.
- Permita las conexiones SSH de cualquier usuario en cualquier zona. SSH cifra los

credenciales de usuario y los datos de la sesión, que proporciona la protección contra los usuarios malintencionados que emplean la paquete-captura de las herramientas al fisgón en la actividad del usuario y los credenciales de usuario o información vulnerable del compromiso tal como configuración del router. El SSH versión 2 proporciona una protección más fuerte, y dirige las vulnerabilidades específicas inherentes al SSH versión 1.

- Permita la Conectividad HTTP al router de las zonas privadas, si la zona privada es digna de confianza. Si no, si la zona del soldado abriga el potencial para que los usuarios malintencionados comprometan la información, el HTTP no emplea el cifrado para proteger el tráfico de administración, y pudo revelar la información vulnerable tal como credenciales de usuario o configuración.
- Permita la Conectividad HTTPS de cualquier zona. Similar a SSH, el HTTPS cifra los datos de la sesión y los credenciales de usuario.
- Restrinja el acceso SNMP a un host o a una subred específico. El SNMP se puede utilizar para modificar la configuración del router y para revelar la información de la configuración. El SNMP se debe configurar con el control de acceso en las diversas comunidades.
- Peticiones del bloque ICMP del Internet pública al direccionamiento de la soldado-zona (si se asume que el direccionamiento de la soldado-zona es routable). Una o más direcciones públicas pueden ser expuestas para el tráfico ICMP para el troubleshooting de la red, en caso necesario. Varios ataques ICMP se pueden utilizar para abrumar a los recursos del router o para reconocer la topología de red y la arquitectura.

Un router puede aplicar este tipo de directiva con la adición de dos zona-pares para cada zona que deba ser controlada. Cada zona-par para el tráfico entrante, o saliente, de la uno mismo-zona del router se debe corresponder con por la directiva respectiva en la dirección opuesta, a menos que el tráfico no sea originado en la dirección opuesta. Un directiva-mapa cada uno para los zona-pares entrantes y salientes puede ser aplicado que describe todo el tráfico, o las correspondencias de políticas específicas por los zona-pares pueden ser aplicadas. La configuración de los zona-pares específicos por el directiva-mapa proporciona el granularity para ver la actividad que corresponde con cada directiva-mapa.

Si se asume que una red de muestra con una estación de la administración de SNMP en 172.17.100.11, y a un servidor TFTP en 172.17.100.17, esta salida proporciona un ejemplo de la política de acceso entera de la interfaz de administración:

```
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
```

Desafortunadamente, la directiva de la uno mismo-zona no ofrece la capacidad para examinar las transferencias TFTP. Así, el Firewall debe pasar todo el tráfico a y desde el servidor TFTP si el TFTP debe pasar con el Firewall.

Si el router termina las conexiones del IPSec VPN, usted debe también definir una directiva para pasar el IPSec ESP, IPSec el IPSec AH, ISAKMP, y NAT-T (UDP 4500). Esto depende sobre la base de cuál es necesario le mantiene utilizará. La directiva siguiente puede ser aplicada además de la directiva arriba. Observe el cambio a las correspondencias de políticas donde un clase-mapa para el tráfico VPN se ha insertado con una acción del paso. Típicamente, el tráfico encriptado es digno de confianza, a menos que sus estados de la política de seguridad que usted deba no prohibir a tráfico encriptado a y desde los 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
```

Firewall y Wide Area Application Services Zona-basados

Refiera al Release Note para las nuevas funciones del Wide Area Application Services de Cisco (versión de software 4.0.13) - para la versión de software 4.0.13 para una nota de aplicación que proporcione los ejemplos de configuración y la dirección del uso

Monitorear el Firewall Zona-basado de la directiva con los comandos show and debug

ZFW presenta a los comandos new para ver la actividad del Firewall de la configuración de la política y del monitor.

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

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

Cuando el nombre de zona no es incluido, el comando visualiza la información de todas las zonas configuradas.

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

Visualice la zona de origen, la Zona de destino y la directiva asociadas a los zona-pares:

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

Cuando no se especifica ninguna fuente o destino, todos los zona-pares con la fuente, el destino, y la directiva asociada se visualizan. Cuando solamente se menciona la fuente/la Zona de destino, todos los zona-pares que contienen esta zona mientras que se visualiza la fuente/el destino.

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

Visualiza un directiva-mapa especificado:

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

Cuando el nombre de un directiva-mapa no se especifica, visualiza todas las correspondencias de políticas del tipo examina (correspondencias de políticas incluyendo de la capa 7 que contienen un subtipo).

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

Visualiza el tiempo de ejecución examinan las estadísticas del directiva-mapa del tipo que existen en un zona-par especificado.

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

Cuando no se menciona **ningún nombre de los zona-pares**, las correspondencias de políticas en todos los zona-pares se visualizan.

La opción de las **sesiones** visualiza las sesiones del examen creadas por la aplicación del directiva-mapa en los zona-pares especificados.

```
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 del **urlfilter** visualiza las estadísticas urlfilter-relacionadas que pertenecen al directiva-mapa especificado (o a las correspondencias de políticas en todas las blancos cuando no se especifica ningún nombre de los zona-pares):

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

Cuando la palabra clave del **caché** se especifica junto con el **urlfilter**, visualiza el caché del **urlfilter** (de los IP Addresses).

El resumen del **comando show policy-map** para examina las correspondencias de políticas:

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

Ajustar la protección Zona-basada del servicio negado del Firewall de la directiva

ZFW ofrece el protección DoS para alertar a los ingenieros de red a los cambios espectaculares en la actividad de la red, y para atenuar la actividad indeseada para reducir el impacto de los cambios de la actividad de la red. ZFW mantiene un contador separado para el clase-mapa de cada correspondencia de políticas. Así, si un clase-mapa se utiliza para las dos correspondencias de políticas de diversos zona-pares, dos diversos conjuntos de los contadores del protección DoS serán aplicados.

ZFW proporciona la mitigación del ataque DOS como valor por defecto en las versiones de Cisco IOS Software antes de 12.4(11)T. El comportamiento predeterminado del protección DoS cambiado con el Cisco IOS Software Release 12.4(11)T. Refiera a ajustar la protección del servicio negado del Firewall Cisco IOS para que la discusión adicional y un procedimiento ajusten el protección DoS ZFW.

Refiera a definir las estrategias para proteger contra los establecimientos de rechazo del servicio TCP SYN para más información sobre los ataques DOS TCP SYN.

Apéndice

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 (completa) final

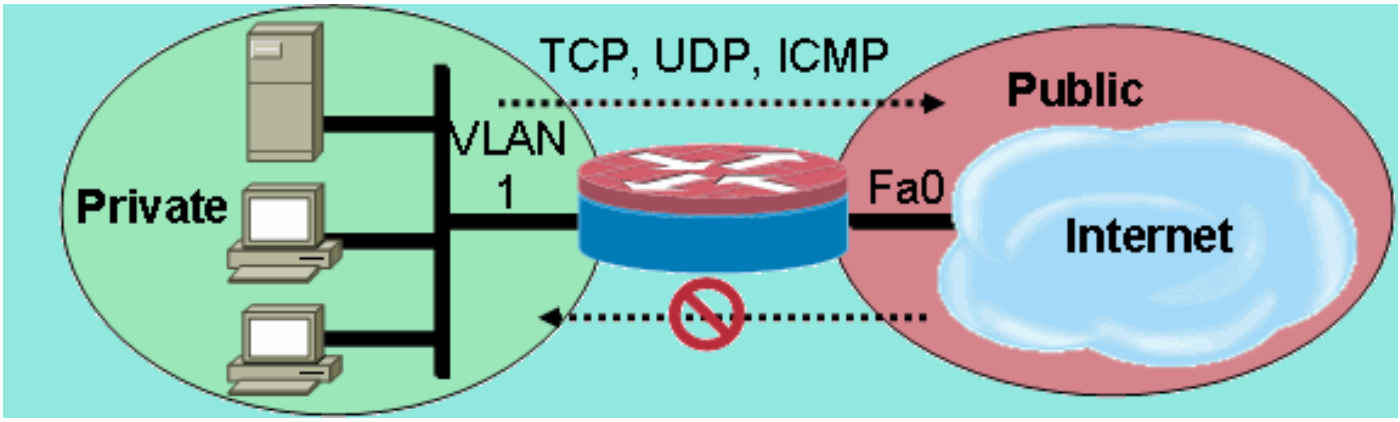
```
ip subnet-zero
ip cef
!
ip port-map user-Xwindows port tcp from 6900 to 6910
!
class-map type inspect match-any L4-inspect-class
```

```
 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 de escudo de protección básica de la Zona-directiva para dos zonas

Este ejemplo proporciona una Configuración simple como base para la prueba de la característica para las mejoras al Cisco IOS Software ZFW. Esta configuración es una configuración modelo para dos zonas, según lo configurado en un 1811 Router. La zona privada se aplica a los puertos del switch fijo del router, así que todos los host en los puertos del switch están conectados con el VLAN1. La zona pública se aplica en el 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