

IOS: La zona basó la Interoperabilidad del Firewall con el despliegue WAAS

Contenido

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Soporte WAAS con el Firewall Cisco IOS](#)

[Despliegue de la bifurcación WAAS con un dispositivo de la Apagado-trayectoria](#)

[Ejemplo de diagrama de red](#)

[Configuración y flujo de paquetes](#)

[Información de la sesión ZBF](#)

[Configuración en funcionamiento del router del lado del cliente \(r1\) con WAAS y ZBF habilitados.](#)

[Despliegue de la bifurcación WAAS con un dispositivo en línea](#)

[Detalles](#)

[Configuración](#)

[Restricciones para la Interoperabilidad ZBF con WAAS](#)

[Información Relacionada](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

El Software Release 12.4(6)T de Cisco IOS® introducido Zona-basó el Firewall de la directiva (ZBPFW), 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.

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 (CBAC) a un modelo zona-basado más flexible, más fácilmente 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.

Prerequisites

Requisitos

Cisco recomienda que usted tiene una comprensión básica del ® CLI del Cisco IOS.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- [Cisco 2900 series routers](#)
- Versión de software IOS 15.2(4) M2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Soporte WAAS con el Firewall Cisco IOS

El soporte WAAS (Wide Area Application Services) con el Firewall Cisco IOS fue introducido en el Cisco IOS Release 12.4(15)T. Proporciona un escudo de protección integrado que optimice los WAN Seguridad-obedientes y las soluciones de la aceleración de la aplicación con las siguientes ventajas:

- Optimiza WAN con las capacidades completas de la inspección con estado.
- Simplifica la conformidad de la industria del indicador luminoso LED amarillo de la placa muestra gravedad menor del pago (PCI).
- Protege el tráfico acelerado WAN transparente.
- Integra las redes WAAS transparente.
- Soporta los módulos del equipo de la Administración de redes (NME) WAE (motor de la aplicación de la área ancha) o el despliegue independiente del dispositivo WAAS.

WAAS tiene un mecanismo de detección automático que utilice las opciones TCP durante la entrada en contacto de tres vías inicial usada para identificar los dispositivos WAE transparente. Después de la detección automática, los flujos de tráfico optimizados (trayectorias) experimentan un cambio en el número de secuencia TCP para permitir que los puntos finales distingan entre los flujos de tráfico optimizados y nooptimized.

El soporte WAAS para el escudo de protección IOS permite el ajuste de las Variables de estado internas TCP usadas para el examen de la capa 4, sobre la base de la rotación en el número de secuencia mencionado anteriormente. Si el Firewall Cisco IOS nota que un flujo de tráfico ha completado con éxito la detección automática WAAS, permite la rotación del número de secuencia inicial para el flujo de tráfico y mantiene el estado de la capa 4 en el flujo de tráfico optimizado.

Escenarios de instrumentación de la optimización del flujo de tráfico WAAS

Las secciones siguientes describen dos diversos escenarios de la optimización del flujo de tráfico WAAS para las implementaciones de la sucursal. La optimización del flujo de tráfico WAAS trabaja con la característica del escudo de protección Cisco en un router de los Servicios integrados de Cisco (ISR).

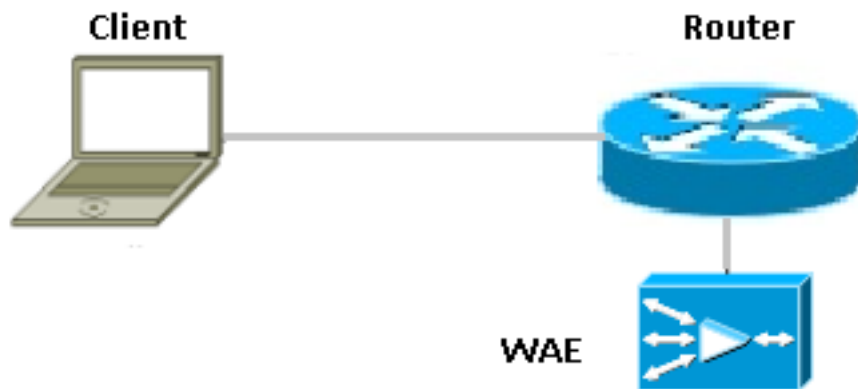
La figura abajo muestra un ejemplo de una optimización de punta a punta del flujo de tráfico WAAS con el escudo de protección Cisco. En este despliegue determinado, un equipo de la Administración de redes (NME) - dispositivo WAE está en el mismo dispositivo que el escudo de protección Cisco. El protocolo web cache communication (WCCP) se utiliza para reorientar el tráfico para la interceptación.

- Despliegue de la bifurcación WAAS con un dispositivo de la Apagado-trayectoria
- Despliegue de la bifurcación WAAS con un dispositivo en línea

Despliegue de la bifurcación WAAS con un dispositivo de la Apagado-trayectoria

Un dispositivo del motor de la aplicación de la área ancha (WAE) puede ser un dispositivo independiente del motor de la automatización del Cisco WAN (WAE) o un módulo de red de Cisco WAAS (NME-WAE) que está instalado en un router de los Servicios integrados (ISR) como motor del servicio integrado (tal y como se muestra en de la figura despliegue de la bifurcación del [WAAS] del servicio de aplicación de la área ancha).

La figura abajo muestra un despliegue de la bifurcación WAAS que utilice el protocolo web cache communication (WCCP) para reorientar el tráfico a una apagado-trayectoria, dispositivo independiente WAE para la interceptación del tráfico. La configuración para esta opción es lo mismo que el despliegue de la bifurcación WAAS con un NME-WAE.



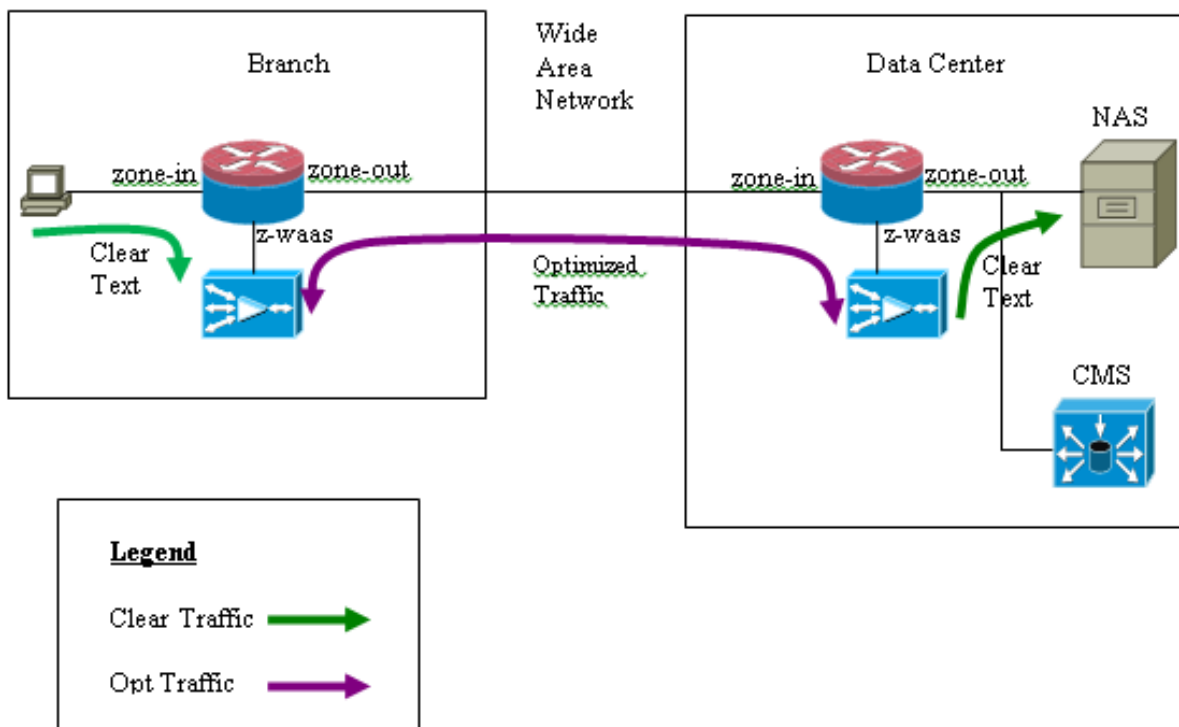
Ejemplo de diagrama de red



Configuración y flujo de paquetes

Lo que sigue es un diagrama que representa una configuración del ejemplo con la optimización WAAS girada para el tráfico de extremo a extremo y CMS

(Sistema de administración centralizada) estando presente en el extremo del servidor. Los módulos de los waas presentes en el extremo de la bifurcación y el extremo del centro de datos necesitan registrarse con CMS para sus operaciones. Se observa que las aplicaciones HTTPS de CMS para él son comunicación con los módulos WAAS.



Flujo de tráfico de punta a punta WAAS

El siguiente ejemplo proporciona una configuración de punta a punta de la optimización del flujo de tráfico WAAS para el Firewall Cisco IOS que utiliza el WCCP para reorientar el tráfico a un dispositivo WAE para la interceptación del tráfico

Sección 1: Config relacionados IOS-FW WCCP

```
ip wccp 61
ip wccp 62
ip inspect waas enable
```

Sección 2: Config de la directiva IOS-FW

```
class-map type inspect most-traffic
 match protocol icmp
 match protocol ftp
 match protocol tcp
 match protocol udp
!
policy-map type inspect p1
 class type inspect most-traffic
 inspect
 class class-default
 drop
```

Sección 3: Zona IOS-FW y config de los Zona-pares

```
zone security zone-in
zone security zone-out
zone security z-waas
```

```
zone-pair security in-out source zone-in destination zone-out
service-policy type inspect p1
```

```
zone-pair security out-in source zone-out destination zone-in
service-policy type inspect p1
```

Sección 4: Config de la interfaz

```
interface GigabitEthernet0/0
description Trusted interface
ip address 172.16.11.1 255.255.255.0
ip wccp 61 redirect in
zone-member security zone-in
```

```
! interface GigabitEthernet0/1 description Untrusted interface ip address 203.0.113.1
255.255.255.0 ip wccp 62 redirect in zone-member security zone-out
```

Observe la nueva configuración en el Cisco IOS Release 12.4(20)T y 12.4(22)T coloca el integrado-servicio-motor en su propia zona y no necesita ser parte de ningunos zona-pares. Los zona-pares se configuran en medio zona-en y zona-hacia fuera.

```
interface Integrated-Service-Engine1/0
ip address 192.168.10.1 255.255.255.0
ip wccp redirect exclude in
zone-member security z-waas
```

Sin la zona configurada en el servicio integrado — El tráfico Engine1/0 consigue caído con el mensaje de descenso siguiente:

```
*Mar 9 11:52:30.647: %FW-6-DR0P_PKT: Dropping tcp session 172.16.11.59:44191 172.16.10.10:80 due
to One of the interfaces not being cfged for zoning with ip ident 0
```

Flujo de tráfico de CMS (dispositivo WAAS que se registra con el administrador central)

El siguiente ejemplo proporciona los config para ambos los escenarios enumerados abajo:

- configuración de punta a punta de la optimización del flujo de tráfico WAAS para el Firewall Cisco IOS que utiliza el WCCP para reorientar el tráfico a un dispositivo WAE para la interceptación del tráfico
- Permitir el tráfico de CMS (el flujo de tráfico de administración WAAS a/desde CMS desde/hasta los dispositivos WAAS).

Sección 1: Config relacionados IOS-FW WCCP

```
ip wccp 61
ip wccp 62
ip inspect waas enable
```

Sección 2: Config de la directiva IOS-FW

```
class-map type inspect most-traffic
match protocol icmp
match protocol ftp
match protocol tcp
match protocol udp
```

```
policy-map type inspect p1
  class type inspect most-traffic
  inspect
  class class-default
  drop
```

2.1 de la sección: Directiva IOS-FW relacionada con el tráfico de CMS

Observe la clase que la correspondencia abajo es necesaria permitir que vaya el tráfico de CMS a través.

```
class-map type inspect waas-special
  match access-group 123
```

```
policy-map type inspect p-waas-man
  class type inspect waas-special
  pass
  class class-default
  drop
```

Sección 3: Zona IOS-FW y config de los Zona-pares

```
zone security zone-in
zone security zone-out
zone security z-waas
```

```
zone-pair security in-out source zone-in destination zone-out
service-policy type inspect p1
```

```
zone-pair security out-in source zone-out destination zone-in
service-policy type inspect p1
```

Sección 3.1: Zona IOS-FW CMS y config relacionados de los Zona-pares

Observe el *waas-out de los zona-pares* y los *out-waas* se requieren para aplicar la directiva creada arriba para el tráfico de CMS.

```
zone-pair security waas-out source z-waas destination zone-out
service-policy type inspect p-waas-man
```

```
zone-pair security out-waas source zone-out destination z-waas
service-policy type inspect p-waas-man
```

Sección 4: Config de la interfaz

```
interface GigabitEthernet0/0
description Trusted interface
ipaddress 172.16.11.1 255.255.255.0
ip wccp 61 redirect in
zone-member security zone-in
!
interface GigabitEthernet0/1
description Untrusted interface
ip address 203.0.113.1 255.255.255.0
ip wccp 62 redirect in
zone-member security zone-out ! interface Integrated-Service-Engine1/0
ip address 192.168.10.1 255.255.255.0
ip wccp redirect exclude in
zone-member security z-waas
```

Sección 5: Lista de acceso para el tráfico de CMS

Observe la lista de acceso que se utiliza para el tráfico de CMS. Está permitiendo el tráfico HTTPS en ambas las direcciones pues el tráfico de CMS es HTTPS.

```
access-list 123 permit tcp any eq 443 any
access-list 123 permit tcp any any eq 443
```

Información de la sesión ZBF

El usuario en 172.16.11.10 detrás del r1 del router está accediendo al servidor de archivos recibido detrás del extremo remoto con una dirección IP de 172.16.10.10, la sesión ZBF se construye en-hacia fuera de los zona-pares y el router reorienta después de eso el paquete al motor WAAS para la optimización.

```
R1#sh policy-map type inspect zone-pair in-out sess
```

```
policy exists on zp in-out
Zone-pair: in-out
```

```
Service-policy inspect : p1
```

```
Class-map: most-traffic (match-any)
```

```
Match: protocol icmp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol ftp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol tcp
```

```
2 packets, 64 bytes
```

```
30 second rate 0 bps
```

```
Match: protocol udp
```

```
0 packets, 0 bytes
```

```
30 second rate 0 bps
```

```
Inspect
```

```
Number of Established Sessions = 1
```

```
Established Sessions
```

```
Session 3D4A32A0 (172.16.11.10:49300)=>(172.16.10.10:445) tcp SIS_OPEN/TCP_ESTAB
```

```
Created 00:00:40, Last heard 00:00:10
```

```
Bytes sent (initiator:responder) [0:0]
```

Sesión construida en R1-WAAS y R2-WAAS por dentro del host al servidor remoto.

R1-WAAS

```
R1-WAAS#show statistics connection
```

```
Current Active Optimized Flows: 1
Current Active Optimized TCP Plus Flows: 1
Current Active Optimized TCP Only Flows: 0
Current Active Optimized Single Sided Flows: 0
Current Active Optimized TCP Preposition Flows: 0
Current Active Auto-Discovery Flows: 1
Current Reserved Flows: 10
```

```
Current Active Pass-Through Flows:      0
Historical Flows:                       13
```

D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,I:ICA,M:MAPI,N:NFS,S:SSL,W:WAN SECURE,V:VIDEO,
X: SMB Signed Connection

```
ConnID      Source IP:Port      Dest IP:Port      PeerID Accel RR
   14      172.16.11.10:49185  172.16.10.10:445 c8:9c:1d:6a:10:61 TCDL  00.0%
```

R2-WAAS

```
R2-WAAS#show statistics connection
```

```
Current Active Optimized Flows:      1
  Current Active Optimized TCP Plus Flows:  1
  Current Active Optimized TCP Only Flows:  0
  Current Active Optimized TCP Preposition Flows:  0
Current Active Auto-Discovery Flows:  0
Current Reserved Flows:              10
Current Active Pass-Through Flows:    0
Historical Flows:                    9
```

D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

```
ConnID      Source IP:Port      Dest IP:Port      PeerID Accel RR
   10      172.16.11.10:49185  172.16.10.10:445 c8:9c:1d:6a:10:81 TCDL  00.0%
```

Configuración en funcionamiento del router del lado del cliente (r1) con WAAS y ZBF habilitados.

```
R1#sh run
Building configuration...
Current configuration : 3373 bytes
!
hostname R1
!
boot-start-marker
boot bootstrap tftp c2900-universalk9-mz.SPA.153-3.M4.bin 255.255.255.255
boot system flash c2900-universalk9-mz.SPA.153-3.M4.bin
boot-end-marker
!
ip wccp 61
ip wccp 62
no ipv6 cef
!
parameter-map type inspect global
  WAAS enable
  log dropped-packets enable
  max-incomplete low 18000
  max-incomplete high 20000
multilink bundle-name authenticated
!
license udi pid CISCO2911/K9 sn FGL171410K8
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
```



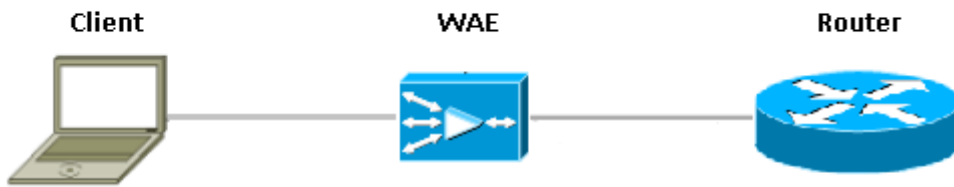
```

license boot module c2900 technology-package datak9
hw-module pvdm 0/1
!
hw-module sm 1
!
class-map type inspect match-any most-traffic
  match protocol icmp
  match protocol ftp
  match protocol tcp
  match protocol udp
!
policy-map type inspect p1
  class type inspect most-traffic
    inspect
  class class-default
    drop
!
zone security in-zone
zone security out-zone
zone security waas-zone
zone-pair security in-out source in-zone destination out-zone
  service-policy type inspect p1
zone-pair security out-in source out-zone destination in-zone
  service-policy type inspect p1
!
interface GigabitEthernet0/0
  description Connection to IPMAN FNN N6006654R
  bandwidth 6000
  ip address 203.0.113.1 255.255.255.0
  ip wccp 62 redirect in
  ip flow ingress
  ip flow egress
  zone-member security out-zone
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 172.16.11.1 255.255.255.0
  no ip redirects
  no ip proxy-arp
  ip wccp 61 redirect in
  zone-member security in-zone
  duplex auto
  speed auto
!
interface SM1/0
  description WAAS Network Module Device Name dciacbra01c07
  ip address 192.168.10.1 255.255.255.0
  ip wccp redirect exclude in
  service-module ip address 192.168.183.46 255.255.255.252
  !Application: Restarted at Sat Jan  5 04:47:14 2008
  service-module ip default-gateway 192.168.183.45
  hold-queue 60 out
!
end

```

Despliegue de la bifurcación WAAS con un dispositivo en línea

La figura abajo muestra un despliegue de la bifurcación del servicio de aplicación de la área ancha (WAAS) que tenga un dispositivo en línea del motor de la aplicación de la área ancha (WAE) que esté físicamente delante del router de los Servicios integrados (ISR). Porque el dispositivo WAE está delante del dispositivo, el escudo de protección Cisco recibe los paquetes optimizados WAAS, y como consecuencia, acode el examen 7 en el cliente que el lado no se soporta.



El router que funciona con el escudo de protección IOS entre los dispositivos WAAS, ve solamente el tráfico optimizado. Los relojes de la característica ZBF para el apretón de manos de tres vías inicial (opción TCP 33 y la rotación del número de secuencia) y él ajustan automáticamente contaban con la ventana de la secuencia TCP (no altera el número de secuencia en el paquete sí mismo). Aplica las características completas del escudo de protección con estado L4 para las sesiones optimizadas WAAS. La solución transparente WAAS facilita el Firewall aplica por el escudo de protección con estado de la sesión y las directivas de QoS.

Detalles

- El Firewall ve un normal paquete TCP Syn con la opción 0x21 y crea una sesión para ella. No hay problemas con las interfaces de entrada o salida puesto que el WCCP no está implicado. La vuelta SYN-ACK no es un paquete reorientado y el Firewall toma la nota de él.
- El Firewall marca para saber si hay la opción 0x21 en el SYN-ACK y realiza el salto del número de secuencia en caso necesario. También apaga el examen L7 si se optimiza la conexión.
- Debe ser observado que el único aspecto que distingue esto del escenario Router-1 es que el tráfico de retorno no está reorientado. No hay "las medias" conexiones en este cuadro.

Configuración

Configuración estándar ZBF sin cualquier zona específica para el tráfico WAAS. Solamente el examen de la capa 7 no será soportado.

Restricciones para la Interoperabilidad ZBF con WAAS

- La capa 2 WCCP reorienta el método no se soporta en el escudo de protección IOS que soporta solamente el cambio de dirección del Generic Routing Encapsulation (GRE).
- El escudo de protección IOS soporta solamente el redireccionamiento de WCCP. Si WAAS utiliza el Routing basado en políticas (PBR) para conseguir los paquetes reorientados, esta solución no asegurará la Interoperabilidad y por lo tanto sin apoyo.
- El escudo de protección IOS no realizará el examen L7 en las sesiones TCP optimizadas WAAS.
- El escudo de protección IOS requiere el "IP examina el permiso de los waas" y el "wccp del IP notifica" los comandos CLI para el redireccionamiento de WCCP.
- El escudo de protección IOS con la Interoperabilidad NAT y WAAS-NM no se soporta actualmente.
- El cambio de dirección del escudo de protección IOS WAAS es solamente aplicado para los paquetes TCP.
- El escudo de protección IOS no soporta el active/las topologías activas. Todos los paquetes que pertenecen a una sesión DEBEN atravesar el cuadro del escudo de protección IOS.

Información Relacionada

[Guía de configuración de seguridad: Firewall Zona-basado de la directiva, Cisco IOS Release 15M&T](#)

[Diseño del Firewall de la directiva y guía Zona-basados de la aplicación](#)