# El cliente de AnyConnect VPN en el router IOS con la zona IOS basó el ejemplo de la configuración del Firewall de la directiva

## Contenido



## Introducción

En el Cisco IOS ® Software release/versión 12.4(20)T y más adelante, una interfaz virtual SSLVPN-VIF0 fue introducida para las conexiones cliente de AnyConnect VPN. Sin embargo, esta interfaz SSLVPN-VIF0 es una interfaz interna que no soporta las configuraciones de usuario. Esto creó un problema con AnyConnect VPN y zona basó el Firewall de la directiva puesto que con el Firewall, el tráfico puede fluir solamente entre dos interfaces cuando ambos interfaces pertenecen a las zonas de Seguridad. Puesto que el usuario no puede configurar el interfaz SSLVPN-VIF0 para hacerle a un miembro de la zona, el tráfico del cliente VPN terminó en el gateway de WebVPN del Cisco IOS después de que el desciframiento no se pueda remitir a ningún otro interfaz que pertenece a una zona de Seguridad. El síntoma de este problema se puede considerar con este mensaje de registro señalado por el Firewall:

```
*Mar 4 16:43:18.251: %FW-6-DROP_PKT: Dropping icmp
   session 192.168.1.12:0 192.168.10.1:0 due to One
   of the interfaces not being cfged for zoning
   with ip ident 0
```

Este problema fue abordado más adelante en más nuevas versiones de software del Cisco IOS. Con el nuevo código, el usuario puede asignar una zona de Seguridad a una interfaz de plantilla virtual, que se refiere bajo contexto de WebVPN, para asociar una zona de Seguridad al contexto de WebVPN.

## prerrequisitos

## Requisitos

Para aprovecharse de la nueva capacidad en el Cisco IOS, usted necesita asegurarse que el dispositivo de gateway de WebVPN del Cisco IOS sea Cisco IOS Software Release 12.4(20)T3, el software Release12.4(22)T2 del Cisco IOS, o el software corriente Release12.4(24)T1 del Cisco IOS y más adelante.

## Componentes Utilizados

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

- Conjunto corriente de la función de seguridad avanzada de la versión 15.0(1)M1 del Cisco IOS 3845 Series Router
- Versión de cliente de Cisco AnyConnect SSL VPN para Windows 2.4.1012

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.

## Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

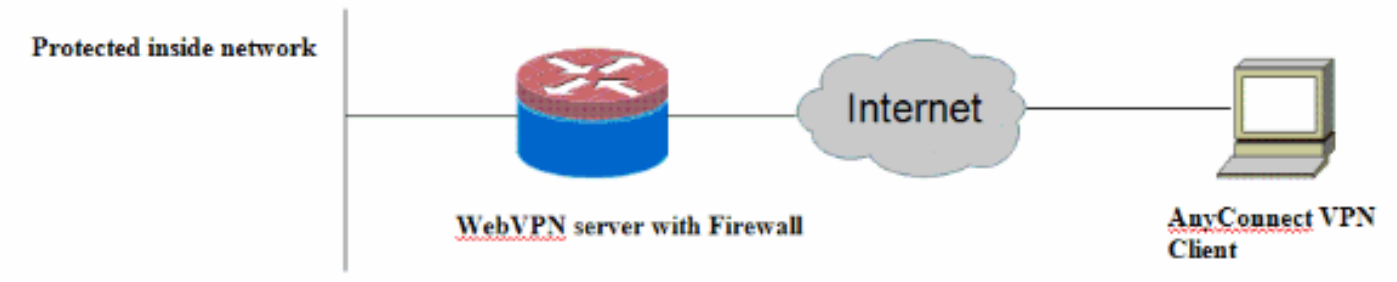
# Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:




## Configure el servidor de AnyConnect del Cisco IOS

Aquí están los pasos para la configuración de alto nivel que necesitan ser realizados en el

servidor de AnyConnect del Cisco IOS para hacer que interopera con el Firewall basado zona de la directiva. La configuración final resultante es incluida para dos decorados de la instalación típica más adelante en este documento.

1. Configure una interfaz de plantilla virtual y asígnela en una zona de Seguridad para el tráfico desencriptado de la conexión de AnyConnect.
2. Agregue la plantilla virtual previamente configurada al contexto de WebVPN para la configuración de AnyConnect.
3. Complete el resto del WebVPN y de la configuración basada zona del Firewall de la directiva.Hay dos escenarios típicos con AnyConnect y ZBF, y aquí es las configuraciones finales del router para cada decorado.

### Escenario de instrumentación 1

El tráfico VPN pertenece a la misma zona de Seguridad que la red interna.

El tráfico de AnyConnect entra la misma zona de Seguridad que el interfaz interior LAN pertenece para fijar el desciframiento.

**Nota:** Una zona del uno mismo también se define para permitir solamente HTTP/el tráfico al router sí mismo de los https para la restricción de acceso.

**Configuración del router**

```
Router#show run
Building configuration...

Current configuration : 5225 bytes
!
! Last configuration change at 16:25:30 UTC Thu Mar 4
2010 by cisco
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot system flash:
boot-end-marker
!
aaa new-model
!
aaa authentication login default local
aaa authentication login webvpn local
!
aaa session-id common
!
!
ip cef
!
!
ip inspect log drop-pkt
no ip domain lookup
!
```

```
!
parameter-map type inspect audit-map
 audit-trail on
 tcp idle-time 20
!
parameter-map type inspect global
!
!
crypto pki trustpoint TP-self-signed-2692466680
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2692466680
 revocation-check none
 rsakeypair TP-self-signed-2692466680
!
!
crypto pki certificate chain TP-self-signed-2692466680
 certificate self-signed 01
 <actual certificate deleted here for brevity>
        quit
!
!
username cisco password 0 cisco
!
!
class-map type inspect match-any test
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all router-access
 match access-group name router-access
!
!
policy-map type inspect firewall-policy
 class type inspect test
  inspect audit-map
 class class-default
  drop
policy-map type inspect out-to-self-policy
 class type inspect router-access
  inspect
 class class-default
  drop
policy-map type inspect self-to-out-policy
 class type inspect test
  inspect
 class class-default
  drop
!
zone security inside
zone security outside
zone-pair security in-out source inside destination
outside
 service-policy type inspect firewall-policy
zone-pair security out-self source outside destination
self
 service-policy type inspect out-to-self-policy
zone-pair security self-out source self destination
outside
 service-policy type inspect self-to-out-policy
!
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
```

```
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security inside
!
interface GigabitEthernet0/1
 ip address 209.165.200.230 255.255.255.224
 ip nat outside
 ip virtual-reassembly
 zone-member security outside
!
interface Virtual-Template1
 ip unnumbered Loopback0
 zone-member security inside
 !
!
ip local pool test 192.168.1.1 192.168.1.100
ip forward-protocol nd
!
ip http server
ip http secure-server
ip nat inside source list 1 interface GigabitEthernet0/1
overload
ip route 0.0.0.0 0.0.0.0 209.165.200.225
!
ip access-list extended router-access
 permit tcp any host 209.165.200.230 eq www
 permit tcp any host 209.165.200.230 eq 443
!
access-list 1 permit 192.168.10.0 0.0.0.255
!
control-plane
 !
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
 modem InOut
 transport input all
line vty 0 4
transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
!
webvpn gateway webvpn_gateway
 ip address 209.165.200.230 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2692466680
 inservice
 !
webvpn install svc flash:/webvpn/svc.pkg sequence 1
 !
webvpn context test
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 !
 policy group policy_1
```

```
   functions svc-enabled
   svc address-pool "test"
   svc keep-client-installed
   svc split include 192.168.10.0 255.255.255.0

 virtual-template 1
 default-group-policy policy_1
 aaa authentication list webvpn
 gateway webvpn_gateway
 inservice
!
end
```

### Escenario de instrumentación 2

El tráfico VPN pertenece a una diversa zona de Seguridad de la red interna.

El tráfico de AnyConnect pertenece a una zona separada VPN, y hay una política de seguridad que controla qué tráfico del vpn puede fluir en la zona interior. En este ejemplo en particular, el tráfico telnet y HTTP se permite del cliente de AnyConnect a la red interior LAN.

**Configuración del router**

```
Router#show run
Building configuration...

Current configuration : 6029 bytes
!
! Last configuration change at 20:57:32 UTC Fri Mar 5
2010 by cisco
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot system flash:
boot-end-marker
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login webvpn local
!
!
aaa session-id common
!
ip cef
!
!
ip inspect log drop-pkt
no ip domain lookup
!
multilink bundle-name authenticated

parameter-map type inspect global
```

```
parameter-map type inspect audit-map
 audit-trail on
 tcp idle-time 20
!
!
crypto pki trustpoint TP-self-signed-2692466680
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2692466680
 revocation-check none
 rsakeypair TP-self-signed-2692466680
!
!
crypto pki certificate chain TP-self-signed-2692466680
 certificate self-signed 01
 <actual certificate deleted for brevity>
        quit
!
!
license udi pid CISCO3845-MB sn FOC09483Y8J
archive
 log config
  hidekeys
username cisco password 0 cisco
!
!
class-map type inspect match-any test
 match protocol tcp
match protocol udp
 match protocol icmp
class-map type inspect match-all router-access
 match access-group name router-access
class-map type inspect match-any http-telnet-ftp
 match protocol http
 match protocol telnet
 match protocol ftp
class-map type inspect match-all vpn-to-inside-cmap
 match class-map http-telnet-ftp
 match access-group name tunnel-traffic
!
!
policy-map type inspect firewall-policy
 class type inspect test
  inspect audit-map
 class class-default
  drop
policy-map type inspect out-to-self-policy
 class type inspect router-access
  inspect
 class class-default
  drop
policy-map type inspect self-to-out-policy
 class type inspect test
  inspect
 class class-default
  pass
policy-map type inspect vpn-to-in-policy
 class type inspect vpn-to-inside-cmap
  inspect
 class class-default
  drop
!
zone security inside
zone security outside
```

```
zone security vpn
zone-pair security in-out source inside destination
outside
 service-policy type inspect firewall-policy
zone-pair security out-self source outside destination
self
 service-policy type inspect out-to-self-policy
zone-pair security self-out source self destination
outside
 service-policy type inspect self-to-out-policy
zone-pair security in-vpn source inside destination vpn
 service-policy type inspect firewall-policy
zone-pair security vpn-in source vpn destination inside
 service-policy type inspect vpn-to-in-policy
!
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
 !
!
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security inside
 !
!
interface GigabitEthernet0/1
 ip address 209.165.200.230 255.255.255.224
 ip nat outside
 ip virtual-reassembly
 zone-member security outside
 !
!
interface Virtual-Template1
 ip unnumbered Loopback0
 zone-member security vpn
 !
!
ip local pool test 192.168.1.1 192.168.1.100
ip forward-protocol nd
!
!
ip http server
ip http secure-server
ip nat inside source list 1 interface GigabitEthernet0/1
overload
ip route 0.0.0.0 0.0.0.0 209.165.200.225

!
ip access-list extended broadcast
 permit ip any host 255.255.255.255
ip access-list extended router-access
 permit tcp any host 209.165.200.230 eq www
 permit tcp any host 209.165.200.230 eq 443
ip access-list extended tunnel-traffic
 permit ip any 192.168.1.0 0.0.0.255
!
access-list 1 permit 192.168.10.0 0.0.0.255
!
!
control-plane
 !
!
```

```
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
 modem InOut
 transport input all
line vty 0 4
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
!
webvpn gateway webvpn_gateway
 ip address 209.165.200.230 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2692466680
 inservice
 !
webvpn install svc flash:/webvpn/svc.pkg sequence 1
 !
webvpn context test
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 !
 policy group policy_1
   functions svc-enabled
   svc address-pool "test"
   svc keep-client-installed
   svc split include 192.168.10.0 255.255.255.0

 virtual-template 1
 default-group-policy policy_1
 aaa authentication list webvpn
 gateway webvpn_gateway
 inservice
!
end
```

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice el OIT para ver un análisis de la **salida del comando show**.

Varios **comandos show se asocian a** WebVPN. Puede ejecutar estos comandos en command-line interface (CLI) para mostrar las estadísticas y otra información. Refiera a verificar la configuración de WebVPN para más información sobre los comandos show. Refiera a la guía de configuración Zona-basada del Firewall de la directiva para más información sobre los comandos usados para verificar la configuración basada zona del Firewall de la directiva.

# Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de

configuración.

## Comandos para resolución de problemas

**Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Varios **comandos debug se asocian a** WebVPN. Refiérase con los comandos Debug de WebVPN para más información sobre estos comandos. Refiera al comando para más información sobre los comandos de debugging basados zona del Firewall de la directiva.

# Información Relacionada

- Cisco IOS Software
- Soporte Técnico y Documentación - Cisco Systems