Configure AnyConnect VPN Client en el router Cisco IOS con ZBF

Contenido

Introducción

En Cisco IOS® Software Release 12.4(20)T y posteriores, se introdujo una interfaz virtual SSLVPN-VIF0 para las conexiones de cliente VPN de AnyConnect. 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 Zone Based Policy Firewall, ya que con el firewall, el tráfico sólo puede fluir entre dos interfaces cuando ambas pertenecen a zonas de seguridad. Dado que el usuario no puede configurar la interfaz SSLVPN-VIF0 para convertirla en miembro de zona, el tráfico del cliente VPN finalizado en el gateway WebVPN de Cisco IOS después del descifrado no se puede reenviar a ninguna otra interfaz que pertenezca a una zona de seguridad. El síntoma de este problema se puede ver con este mensaje de registro informado 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 se abordó posteriormente en las versiones más recientes del software del IOS de Cisco. Con el nuevo código, el usuario puede asignar una zona de seguridad a una interfaz de plantilla virtual, a la que se hace referencia en el contexto WebVPN, para asociar una zona de seguridad con el contexto WebVPN .

Prerequisites

Requirements

Para aprovechar la nueva capacidad del IOS de Cisco, debe asegurarse de que el dispositivo de gateway WebVPN del IOS de Cisco esté ejecutando la versión 12.4(20)T3 del software del IOS de Cisco, la versión 12.4(22)T2 del software del IOS de Cisco o la versión 12.4(24)T1 y posteriores.

Componentes Utilizados

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

- Cisco IOS 3845 Series Router que ejecuta la versión 15.0(1)M1 Advanced Security set
- Cisco AnyConnect SSL VPN Client versión para Windows 2.4.1012

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

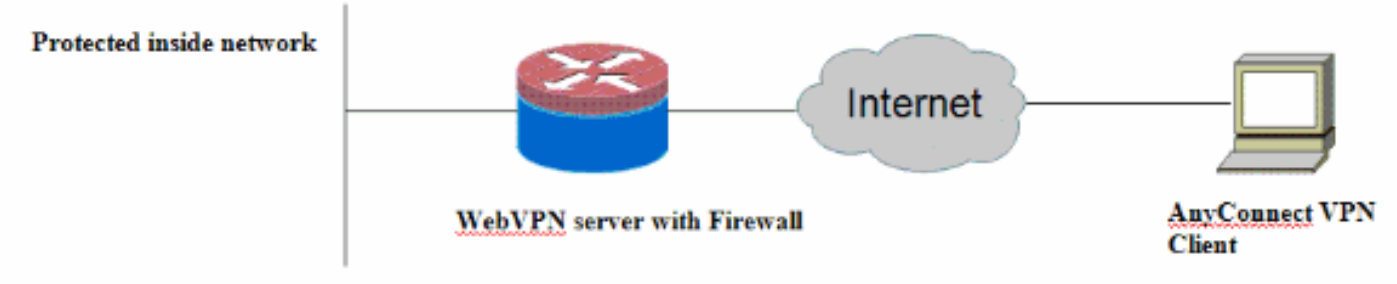
Configurar

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

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración del servidor Cisco IOS AnyConnect

Estos son los pasos de configuración de alto nivel que deben realizarse en el servidor Cisco IOS AnyConnect para que interopere con el firewall de políticas basado en zona. La configuración final resultante se incluye para dos escenarios de implementación típicos más adelante en este documento.

1. Configure una interfaz de plantilla virtual y asígnela en una zona de seguridad para el tráfico

descifrado desde la conexión de AnyConnect.
2. Agregue la plantilla virtual configurada previamente al contexto WebVPN para la configuración de AnyConnect.
3. Complete el resto de la configuración de WebVPN y del firewall de políticas basado en zona.Hay dos escenarios típicos con AnyConnect y ZBF, y aquí están las configuraciones finales del router para cada escenario.

Escenario de implementación 1

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

El tráfico de AnyConnect entra en la misma zona de seguridad que la interfaz LAN interna pertenece al descifrado posterior.

Nota: También se define una zona autónoma para permitir solamente el tráfico http/https al propio router 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 implementación 2

El tráfico VPN pertenece a una zona de seguridad diferente de la red interna.

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

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 la OIT para ver un análisis del resultado 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. Consulte Verificación de la Configuración de WebVPN para obtener más información sobre los comandos show. Refiérase a la Guía de Configuración de Firewall de Políticas Basada en Zona para obtener más información sobre los comandos utilizados para verificar la configuración de firewall de políticas basado en zona.

Troubleshoot

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

Comandos para resolución de problemas

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

Varios comandos debug se asocian a WebVPN. Refiérase a Uso de Comandos Debug WebVPN para obtener más información sobre estos comandos. Consulte el comando para obtener más información sobre los comandos de depuración de firewall de políticas basadas en zonas.

Información Relacionada

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