AnyConnect VPN-client op Cisco IOS-router met ZBF configureren

Inhoud

Inleiding

In Cisco IOS® softwarerelease 12.4(20)T en later is een virtuele interface SLVPN-VIF0 geïntroduceerd voor AnyConnect VPN-clientverbindingen. Maar deze SSLVPN-VIF0-interface is een interne interface, die geen gebruikersconfiguraties ondersteunt. Dit leidde tot een probleem met AnyConnect VPN en Zone Based Policy Firewall aangezien met de firewall het verkeer alleen tussen twee interfaces kan stromen wanneer beide interfaces aan beveiligingszones toebehoren. Aangezien de gebruiker de SSLVPN-VIF0 interface niet kan configureren om er een zone lid van te maken, kan VPN-clientverkeer dat is beëindigd op de Cisco IOS WebVPN-gateway na decryptie niet worden doorgestuurd naar een andere interface die tot een beveiligingszone behoort. De symptomen van dit probleem worden gezien bij dit logbericht dat door de firewall is gemeld:

```
*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
```

Dit probleem werd later aangepakt in nieuwere softwarereleases van Cisco IOS. Met de nieuwe code kan de gebruiker een veiligheidsgebied aan een virtueel-sjabloon interface toewijzen, die onder de WebVPN-context van toepassing is, om een veiligheidszone met de WebVPN-context te associëren.

Voorwaarden

Vereisten

Om voordeel te halen uit de nieuwe mogelijkheid in Cisco IOS, moet u ervoor zorgen dat het Cisco IOS WebVPN gateway-apparaat Cisco IOS-softwarerelease 12.4(20)T3, Cisco IOS-softwarerelease 12.4(22)T2 of Cisco IOS-softwarerelease 12.4(24)T1 en hoger wordt uitgevoerd.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS 3845 Series router met versie 15.0(1)M1 geavanceerde security functieset
- Cisco AnyConnect SSL VPN-clientversie voor Windows 2.4.1012

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

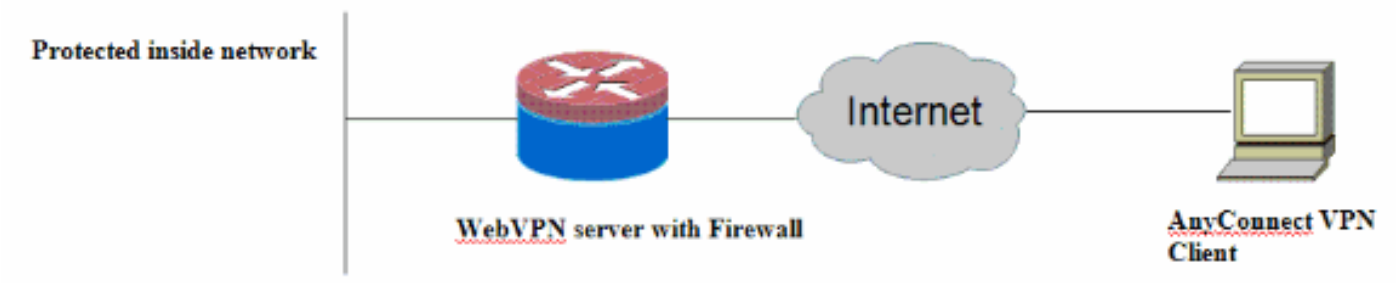
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Cisco IOS AnyConnect-server configureren

Hier zijn de configuratiestappen op hoog niveau die op de Cisco IOS AnyConnect-server moeten worden uitgevoerd om het systeem te laten samenwerken met de Zone Based Policy Firewall. De resulterende definitieve configuratie wordt voor twee typische implementatiescenario's later in dit document opgenomen.

1. Configureer een virtuele sjablooninterface en wijs deze in een beveiligingszone toe voor verkeer dat is versleuteld via de AnyConnect-verbinding.
2. Voeg de eerder gevormde virtuele Sjabloon aan de WebVPN-context toe voor de AnyConnect-configuratie.
3. Voltooi de rest van de configuratie van WebVPN en Zone Based Policy Firewall.Er zijn twee typische scenario's met AnyConnect en ZBF, en hier zijn de definitieve routerconfiguraties voor elk scenario.

Plaatsingsscenario 1

VPN-verkeer behoort tot dezelfde beveiligingszone als het interne netwerk.

Het AnyConnect-verkeer gaat naar dezelfde beveiligingszone waarin de binnen-LAN-interface behoort tot de post-decryptie.

Opmerking: Een zelfzone is ook gedefinieerd om alleen http/https-verkeer naar de router zelf toe te staan voor toegangsbeperking.

Routerconfiguratie

```
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
```

Plaatsingsscenario 2

VPN-verkeer behoort tot een ander beveiligingsgebied dan het binnennetwerk.

Het AnyConnect-verkeer behoort tot een afzonderlijk VPN-gebied en er is een beveiligingsbeleid dat controleert welke VPN-verkeer in de binnenzone kan stromen. In dit specifieke voorbeeld, worden het telnet en het http verkeer toegestaan van de AnyConnect client naar het binnen LAN netwerk.

Routerconfiguratie

```
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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Verschillende **tonen** opdrachten worden geassocieerd met WebVPN. U kunt deze opdrachten via de opdrachtregel-interface (CLI) uitvoeren om statistieken en andere informatie **weer** te **geven**. Raadpleeg de Configuratie WebVPN controleren voor meer informatie over showopdrachten. Raadpleeg de Zone-Based Policy Firewall Configuration voor meer informatie over opdrachten die worden gebruikt om de configuratie van de Zone Based Policy Firewall te controleren.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

Meerdere debug opdrachten worden gekoppeld aan WebVPN. Raadpleeg Beeldopdrachten voor WebVPN gebruiken voor meer informatie over deze opdrachten. Raadpleeg de opdracht voor meer informatie over de opdrachten Firewall van Zone Based Policy.

Gerelateerde informatie

- Cisco IOS-software
- Technische ondersteuning en documentatie – Cisco Systems