

O cliente VPN de AnyConnect no IOS Router com zona IO baseou o exemplo da configuração de firewall da política

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o server de AnyConnect do Cisco IOS](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

No Cisco IOS ® Software libere 12.4(20)T e mais tarde, uma interface virtual SSLVPN-VIF0 foi introduzida para conexões de cliente de VPN de AnyConnect. Porém, esta interface SSLVPN-VIF0 é uma interface interna, que não suporta configurações do usuário. Isto criou um problema com o AnyConnect VPN e zona baseou o Firewall da política desde que com o Firewall, o tráfego pode somente fluir entre duas relações quando ambas as relações pertencem às zonas de Segurança. Desde que o usuário não pode configurar a relação SSLVPN-VIF0 para lhe fazer um membro da zona, o tráfego do cliente VPN terminou no gateway do Cisco IOS WebVPN depois que a descryptografia não pode ser enviada a nenhuma outra relação que pertence a uma zona de Segurança. O sintoma deste problema pode ser considerado com este mensagem de registro relatado pelo 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
```

Esta edição foi endereçada mais tarde em uns software release mais novos do Cisco IOS. Com o código novo, o usuário pode atribuir uma zona de Segurança a uma interface de molde virtual, que seja provida sob o contexto WebVPN, a fim associar uma zona de Segurança com o contexto WebVPN.

[Pré-requisitos](#)

Requisitos

A fim aproveitar-se da capacidade nova no Cisco IOS, você precisa de assegurar-se de que o dispositivo de gateway do Cisco IOS WebVPN seja Cisco IOS Software Release 12.4(20)T3, o Cisco IOS Software Release 12.4(22)T2, ou o Cisco IOS Software running Release 12.4(24)T1 e mais tarde.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Grupo running dos recursos de segurança avançada da versão 15.0(1)M1 do Cisco IOS 3845 Series Router
- Versão do cliente VPN de Cisco AnyConnect SSL para Windows 2.4.1012

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurar o server de AnyConnect do Cisco IOS

Estão aqui as etapas de configuração de nível elevado que precisam de ser executadas no server de AnyConnect do Cisco IOS a fim o fazer interoperar com o Firewall baseado zona da política. A configuração final resultante é incluída para duas encenações da implementação típica mais tarde neste documento.

1. Configurar uma relação virtual do molde e atribua-a em uma zona de Segurança para o tráfego decifrado da conexão de AnyConnect.
2. Adicionar o molde virtual previamente configurado ao contexto WebVPN para a configuração de AnyConnect.
3. Termine o resto do WebVPN e da configuração de firewall baseada zona da política. Há dois

cenários típicos com AnyConnect e ZBF, e está aqui as configurações de roteador finais para cada encenação.

Cenário de distribuição 1

O tráfego VPN pertence à mesma zona de Segurança que a rede interna.

O tráfego de AnyConnect entra na mesma zona de Segurança que a interface de LAN interna pertence para afixar a descryptografia.

Nota: Uma zona do auto é definida igualmente para permitir somente HTTP/tráfego ao roteador próprio dos https para a restrição de acesso.

Configuração do roteador

```
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

```

Cenário de distribuição 2

O tráfego VPN pertence a uma zona de Segurança diferente da rede interna.

O tráfego de AnyConnect pertence a uma zona separada VPN, e há uma política de segurança que controle que tráfego do vpn pode fluir na zona interna. Neste exemplo particular, o telnet e o tráfego HTTP são permitidos do cliente de AnyConnect à rede de LAN interna.

Configuração do roteador

```

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

```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Vários **comandos show** estão associados ao WebVPN. Você pode executar estes comandos na

interface de linha de comando (CLI) para mostrar estatísticas e outras informações. Refira a [verificação da configuração WebVPN](#) para obter mais informações sobre dos comandos show. Refira o [guia de configuração de firewall Zona-baseado da política](#) para obter mais informações sobre dos comandos usados para verificar a configuração de firewall baseada zona da política.

[Troubleshooting](#)

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

[Comandos para Troubleshooting](#)

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

Vários **comandos debug** estão associados ao WebVPN. Refira a [utilização de comandos Debug WebVPN](#) para obter mais informações sobre destes comandos. Refira o comando para obter mais informações sobre dos comandos debugging baseados zona do Firewall da política.

[Informações Relacionadas](#)

- [Cisco IOS Software](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)