具有基于 IOS 区域的策略防火墙配置的 IOS 路由器上的 AnyConnect VPN 客户端示例

Contents

Introduction

在 Cisco IOS® 软件版本 12.4(20)T 及更高版本中，为 AnyConnect VPN 客户端连接引入了虚拟接口 SSLVPN-VIF0。但是，此 SSLVPN-VIF0 接口是内部接口，它不支持用户配置。这使 AnyConnect VPN 和区域策略防火墙出现了问题，因为使用防火墙，流量只能在都属于安全区域的两个接口之间流动。因为用户无法配置 SSLVPN-VIF0 接口以使它成为区域成员，所以在解密无法转发到属于安全区域的任何其他接口后，VPN 客户端流量在 Cisco IOS WebVPN 网关上终止。可以通过防火墙报告的以下日志消息查看此问题的症状：

```
*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
```

后来在 Cisco IOS 的较新软件版本中解决了此问题。使用新代码，用户可以将安全区域分配到 WebVPN 上下文下引用的虚拟模板接口，以将安全区域与 WebVPN 上下文相关联。

Prerequisites

Requirements

若要利用 Cisco IOS 中的新功能，您需要确保 Cisco IOS WebVPN 网关设备运行的是 Cisco IOS 软件版本 12.4(20)T3、Cisco IOS 软件版本 12.4(22)T2 或 Cisco IOS 软件版本 12.4(24)T1 及更高版本。

Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行 15.0(1)M1 版高级安全功能集的 Cisco IOS 3845 系列路由器
- 用于 Windows 的 Cisco AnyConnect SSL VPN Client 版本 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.

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

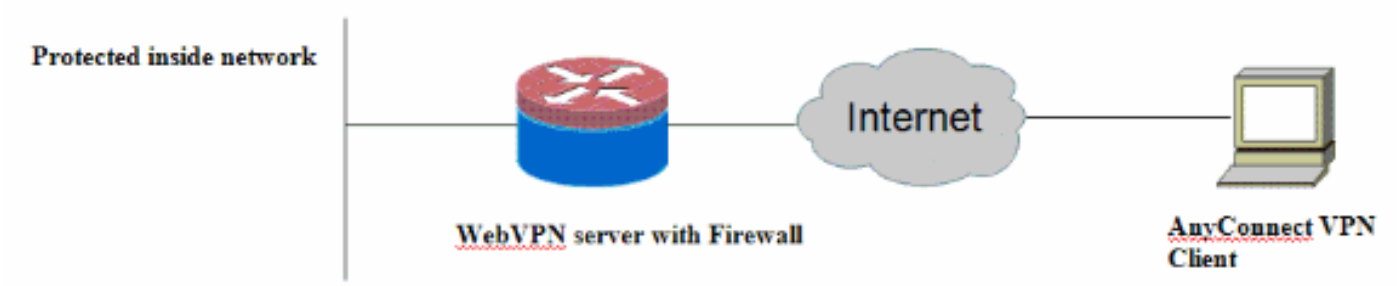
Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

Network Diagram

本文档使用以下网络设置：



配置 Cisco IOS AnyConnect 服务器

以下是在 Cisco IOS AnyConnect 服务器上使其与区域策略防火墙互操作所需执行的概要配置步骤。本文档中稍后包括为两个典型的部署方案生成的最终配置。

1. 配置虚拟模板接口并在安全区域中为从 AnyConnect 连接解密的流量分配它。
2. 将以前配置的虚拟模板添加到 AnyConnect 配置的 WebVPN 上下文中。
3. 完成其余 WebVPN 和区域策略防火墙配置。有两个有关 AnyConnect 和 ZBF 的典型方案，以下是每个方案的最终路由器配置。

部署方案 1

VPN 流量与内部网络属于同一安全区域。

AnyConnect 流量进入内部 LAN 接口所属于的同一安全区域中来发布解密。

Note: 还定义了自身区域来只允许到路由器本身的 http/https 流量以限制访问。

路由器配置

```
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
```

部署方案 2

VPN 流量属于与内部网络不同的安全区域。

AnyConnect 流量属于单独的 VPN 区域，并且有控制什么 vpn 流量可以流入内部区域中的安全策略。在此特定示例中，允许从 AnyConnect 客户端到内部 LAN 网络的 telnet 和 http 流量。

路由器配置

```
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
```

Verify

Use this section to confirm that your configuration works properly.

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

有若干 **show** 命令与 WebVPN 关联。您能执行这些at命令命令行界面(CLI)到**show statistics**和其他信息。有关 show 命令的详细信息，请参阅验证 WebVPN 配置。有关用于验证区域策略防火墙配置的命令的详细信息，请参阅区域策略防火墙配置指南。

Troubleshoot

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

Note: 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

有若干 **debug** 命令与 WebVPN 关联。有关这些命令的详细信息，请参阅使用 WebVPN Debug 命令。有关区域策略防火墙调试命令的详细信息，请参阅相关命令。

Related Information

- Cisco IOS 软件
- Technical Support & Documentation - Cisco Systems