

IOS ゾーン ベースのポリシー ファイアウォールを使用した IOS ルータでの AnyConnect VPN クライアントの設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[Cisco IOS AnyConnect サーバの設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

Cisco IOS® ソフトウェア リリース 12.4(20)T 以降では、AnyConnect VPN クライアントの接続に仮想インターフェイス SSLVPN-VIF0 が導入されています。ただし、この SSLVPN-VIF0 インターフェイスはユーザ設定をサポートしない内部インターフェイスです。そのため、AnyConnect VPN とゾーンベース ポリシー ファイアウォールを併用すると問題が生じていました。2 つのインターフェイスがセキュリティ ゾーンに属している場合、この 2 つのインターフェイス間だけにトラフィック フローが制限されるからです。ユーザは SSLVPN-VIF0 インターフェイスをゾーン メンバとして設定できないため、復号化後に Cisco IOS WebVPN ゲートウェイで終了した VPN クライアントのトラフィックを、セキュリティ ゾーンに属している他のインターフェイスに転送することはできません。ファイアウォールが次のようなログ メッセージをレポートした場合、この現象が発生していると考えられます。

```
*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
```

この問題は、その後、新しい Cisco IOS ソフトウェア リリースで解決されました。新しいコードでは、ユーザはセキュリティ ゾーンを仮想テンプレート インターフェイスに割り当てられます。この仮想テンプレート インターフェイスは WebVPN コンテキストで参照され、セキュリティ ゾーンを WebVPN と関連付けるために使用されます。

前提条件

要件

Cisco IOS の新しい機能を活用するためには、Cisco IOS WebVPN ゲートウェイ デバイスで Cisco IOS ソフトウェア リリース 12.4(20)T3、Cisco IOS ソフトウェア リリース 12.4(22)T2、または Cisco IOS ソフトウェア リリース 12.4(24)T1 以降が稼働している必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- バージョン 15.0(1)M1 の Advanced Security フィーチャ セットが稼働する Cisco IOS 3845 シリーズ ルータ
- Windows 2.4.1012 用のバージョンの Cisco AnyConnect SSL VPN Client

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

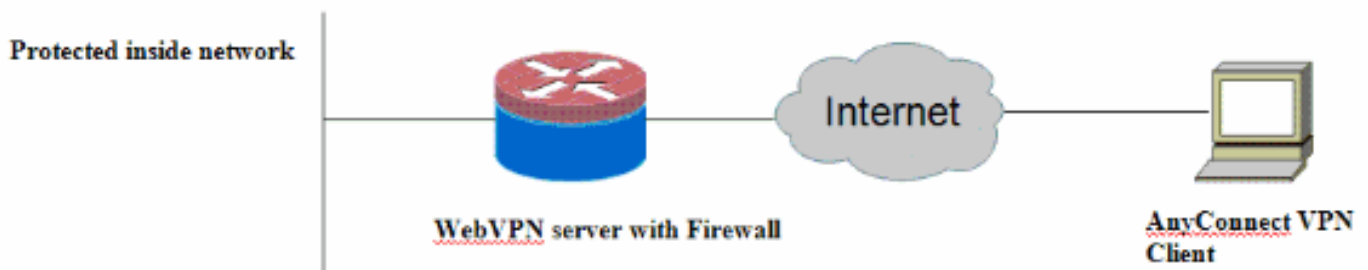
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



Cisco IOS AnyConnect サーバの設定

ここでは、ゾーンベース ポリシー ファイアウォールと連動させるために、Cisco IOS AnyConnect サーバで必要となる設定手順の概要を示します。最終的な設定は、このドキュメントの後半に提示する 2 種類の代表的な導入シナリオを参照してください。

1. 仮想テンプレート インターフェイスを設定し、それを AnyConnect 接続から復号化された

トラフィック用のセキュリティゾーン内に割り当てます。

2. 前の手順で設定した仮想テンプレートを、AnyConnect 設定の WebVPN コンテキストに追加します。
3. WebVPN とゾーンベース ポリシー ファイアウォールの残りの設定を完了させます。
AnyConnect とゾーンベース ポリシー ファイアウォールの代表的なシナリオとして、ここでは 2 種類のシナリオの最終的なルータ設定をそれぞれ示します。

導入シナリオ 1

VPN トラフィックは内部ネットワークと同じセキュリティゾーンに属しています。

AnyConnect トラフィックは、復号化後に、内部 LAN インターフェイスが属している同じセキュリティゾーンに入ります。

注: アクセス制限のため、ルータ自体への http/https トラフィックのみを許可するセルフゾーンも定義されています。

ルータの設定

```
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
```

デプロイメントシナリオ 2

VPN トラフィックは内部ネットワークとは異なるセキュリティゾーンに属しています。

AnyConnect トラフィックは別の VPN ゾーンに属し、内部ゾーンに入ることのできる VPN トラフィックを制御するセキュリティポリシーが設定されています。この例では、AnyConnect クライアントから内部 LAN ネットワークへの telnet トラフィックと http トラフィックが許可されません。

ルータの設定

```
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
```

確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

いくつかの **show** コマンドは WebVPN に関連しています。これらのコマンドをコマンドライン インターフェイス (CLI) で実行して、統計情報や他の情報を表示できます。show コマンドの詳細については、『[WebVPN 設定の確認](#)』を参照してください。ゾーンベース ポリシー ファイアウォールの設定確認に使用するコマンドの詳細については、『[ゾーンベース ポリシー ファイアウォール設定ガイド](#)』を参照してください。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

[トラブルシューティングのためのコマンド](#)

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

いくつかの debug コマンドは、WebVPN に関連しています。これらのコマンドの詳細については、『[WebVPN の Debug コマンドの使用](#)』を参照してください。ゾーンベース ポリシー ファイアウォールの debug コマンドの詳細については、それぞれのコマンドを参照してください。

関連情報

- [Cisco IOS ソフトウェア](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)