

Cisco IOS Firewall Classic とゾーンベースの仮想ファイアウォール アプリケーションの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[機能サポート](#)

[VRF の設定](#)

[VRF 対応 IOS ファイアウォールのための通常の使用に関する概要](#)

[サポートされていない設定](#)

[設定](#)

[VRF 対応 Cisco IOS Classic Firewall](#)

[VRF 対応 Cisco IOS ゾーンベース ポリシー IOS ファイアウォール](#)

[結論](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、VRF 対応の仮想ファイアウォール機能に関する技術的背景、設定手順、および、さまざまなアプリケーション シナリオのための使用例を説明します。

Cisco IOS[®]ソフトウェアリリース12.3(14)Tでは、仮想 (VRF対応) ファイアウォールが導入され、既存のVPN、NAT、QoS、その他のVRFに加えて、ステートフルパケットインスペクション、トランスパレントファイアウォール、アプリケーション検査、URLフィルタリングを提供します。認識機能考えられるアプリケーション シナリオのほとんどでは、NAT が他の機能とともに適用されます。NAT が不要な場合は、インター VRF 接続を提供するために、VRF 間にルーティングを適用できます。Cisco IOS ソフトウェアでは、Cisco IOS Classic Firewall と Cisco IOS のゾーンベース ポリシー ファイアウォールの両方に対して VRF 対応機能が提供されており、さらに、このドキュメントで紹介されている両方の設定モデルの例も提供されています。ゾーンベース ポリシー ファイアウォールの設定に、より重点が置かれています。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細については、『[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。

背景説明

機能サポート

VRF 対応ファイアウォールを利用できるのは Advanced Security、Advanced IP Services、および Advanced Enterprise のイメージで、さらに、Cisco IOS Firewall 機能セットの統合を表す o3 表示の付いた古い表記のイメージでも利用できます。VRF対応ファイアウォール機能は、12.4で Cisco IOSソフトウェアメインラインリリースに統合されました。VRF対応ゾーンベースポリシーファイアウォールを適用するには、Cisco IOSソフトウェアリリース12.4(6)T以降が必要です。Cisco IOSゾーンベースポリシーファイアウォールは、ステートフルフェールオーバーでは動作しません。

VRF の設定

Cisco IOS ソフトウェアでは、グローバル VRF とすべてのプライベート VRF のための設定が同じコンフィギュレーション ファイルに保持されます。コマンドライン インターフェイスからルータのコンフィギュレーションにアクセスする場合、ルータの操作員と管理者の権限の制限に、CLI ビュー機能で提供されるロールベース アクセス コントロールを使用できます。Cisco Security Manager (CSM) などの管理アプリケーションでも、ロールベース アクセス コントロールを提供することにより、確実に操作員の権限を適切なレベルに制限できます。

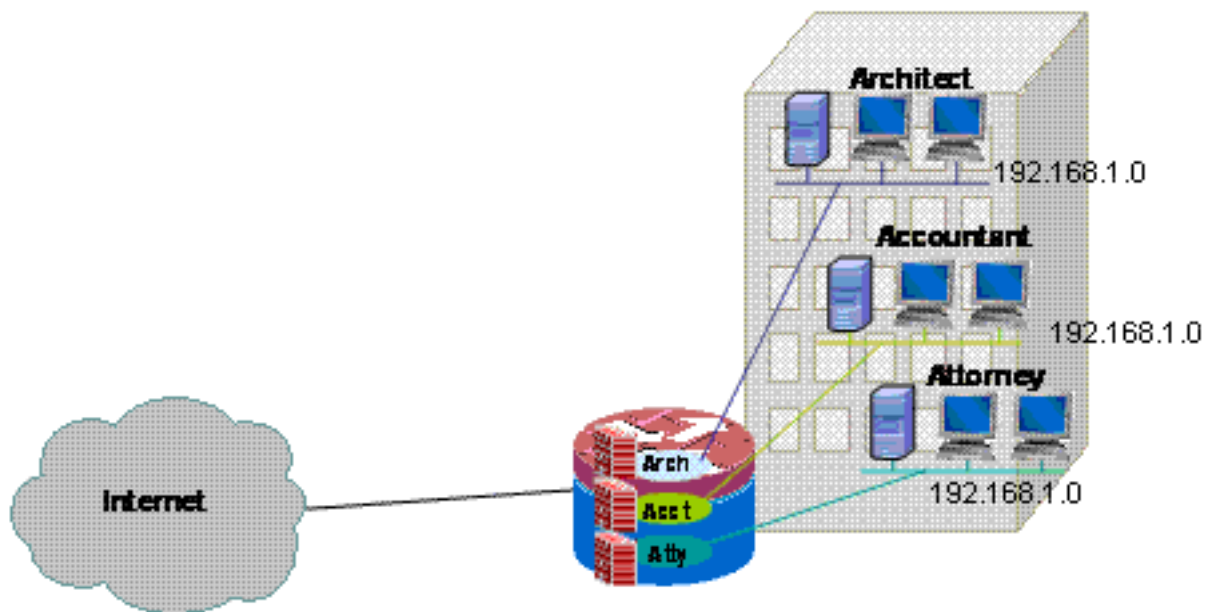
VRF 対応 IOS ファイアウォールのための通常の使用に関する概要

VRF 対応のファイアウォールにより、Cisco IOS Virtual Routing/Forwarding (VRF) 機能にステートフルなパケット検査が付加されます。IPSec VPN、ネットワーク アドレス変換 (NAT) /ポート アドレス変換 (PAT)、侵入防御システム (IPS) および他の Cisco IOS のセキュリティ サービスを VRF 対応のファイアウォールに統合して、VRF でのセキュリティ サービスの完全なセットを提供できます。VRF では、オーバーラップ型 IP アドレス割り当てを採用する複数のルートスペースがサポートされ、これにより、1つのルータを複数の離散型ルーティング インスタンスに分割することにより、トラフィックの分離に対応できます。VRF 対応ファイアウォールには、ルータがトラッキングしているすべての検査アクティビティのためのセッション情報内に VRF ラベルが組み込まれており、これにより、それぞれの別の項目で同一である可能性のある接続状況の情報間での分離が維持されます。VRF 対応のファイアウォールでは、1つの VRF 内のインターフェイス間での検査が可能ですが、さらに、異なる VRF 内のインターフェイス間での検査も可能です。たとえば、VRF の境界をトラフィックが通過するような場合がこれに該当し、これにより、イントラ VRF (VRF 内) トラフィックとインター VRF (VRF 間) トラフィックの両方に対

してきわめて柔軟なファイアウォール検査が実現されます。

VRF 対応の Cisco IOS ファイアウォール アプリケーションは、次の 2 つのカテゴリにグループ分けできます。

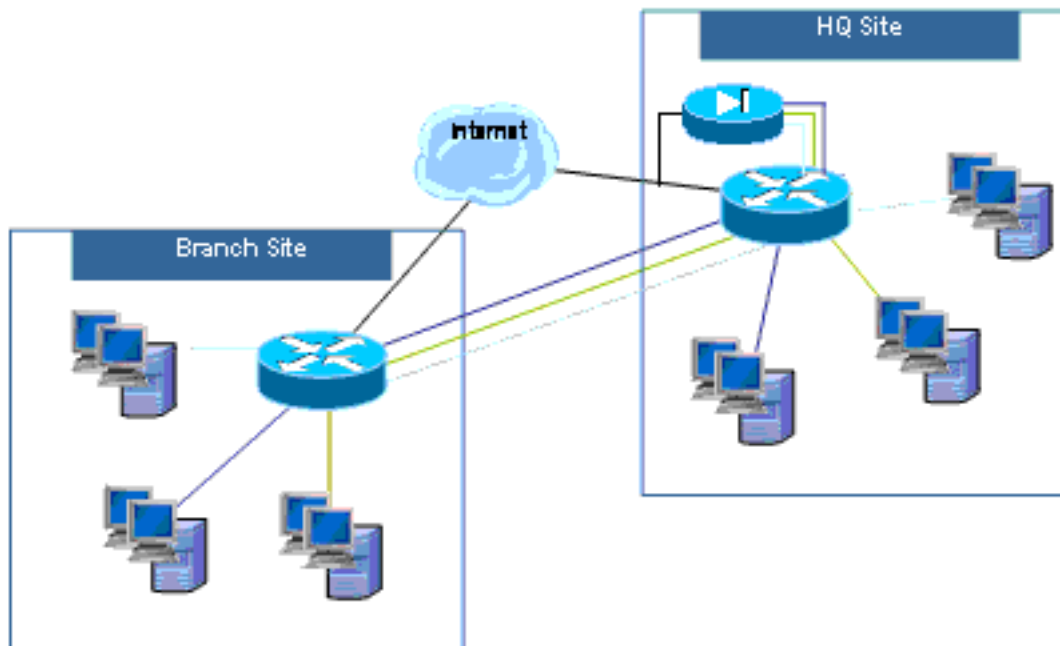
- マルチテナント、シングルサイト：複数のテナントに対するインターネットアクセスで、重複するアドレススペースまたは分離されたルートスペースを単一の構内に持ちます。ステートフルファイアウォールは、各VRFのインターネット接続に適用され、オープンNAT接続を通じて侵害の可能性をさらに低減します。VRF では、ポート転送を適用してサーバへの接続を許可できます。



VR

F 対応の Classic Firewall 構成モデルと VRF 対応のゾーンベース ファイアウォール構成モデルの両方のためのマルチテナント、シングルサイトのアプリケーションの例は、このドキュメントで紹介されています。

- マルチテナント、マルチサイト：大規模ネットワークで機器を共有する複数のテナントは、VPNまたはWAN接続を介して異なるサイトのテナントのVRFを接続することで、複数のサイト間の接続を必要とします。1つあるいは複数のサイトで各テナントがインターネットアクセスを必要としている可能性があります。管理を簡単にするために、一部の部門では各サイトで複数のネットワークを1つのアクセスルータに集約する場合がありますが、多くの部門ではアドレススペースの分離が求められます。



VRF 対応の Classic Firewall 構成モデルと VRF 対応のゾーンベース ファイアウォール構成モデルの両方のためのマルチテナント、マルチサイトのアプリケーションの設定例は、このドキュメントのアップデートで紹介される予定です。

サポートされていない設定

VRF 対応のファイアウォールは、Multi-VRF CE (VRF Lite) と MPLS VPN をサポートする Cisco IOS イメージで利用できます。ファイアウォール機能は非 MPLS インターフェイスに限定されています。つまり、あるインターフェイスが MPLS ラベル付きのトラフィックの処理に関わっている場合、そのインターフェイスにはファイアウォール検査は適用できません。

トラフィックが VRF での発着信を、他の VRF に向けて経由するインターフェイスを介して行う必要がある場合、ルータで可能なのはインター VRF トラフィックの検査だけです。トラフィックが他の VRF に直接ルーティングされる場合、ファイアウォール ポリシーでトラフィックを検査できる物理的なインターフェイスが存在しないので、ルータでは検査を適用できません。

VRF Lite コンフィギュレーションが NAT/PAT と相互運用できるのは、ネットワーク アクティビティのための発信元アドレスや宛先アドレスあるいはポート番号を変更するために NAT/PAT が適用されているインターフェイスに ip nat inside か ip nat outside が設定されている場合だけです。NAT か PAT が適用されているインターフェイスへの ip nat enable 設定の追加で識別される NAT Virtual Interface (NVI) 機能は、インター VRF NAT/PAT アプリケーションに対してはサポートされていません。VRF Lite と NAT Virtual Interface 間で相互運用性が欠如している問題は、改善要求 CSCek35625 でトラッキングされています。

設定

このセクションでは、VRF 対応の Cisco IOS Classic Firewall および VRF 対応のゾーンベース ポリシー ファイアウォールの設定例を説明しています。

注：このセクションで使用され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。

[VRF 対応 Cisco IOS Classic Firewall](#)

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

ip inspect の使用により識別される Cisco IOS VRF 対応 Classic Firewall (以前の CBAC) は、Cisco IOS ソフトウェア リリース 12.3(14)T で VRF 対応の検査をサポートするように Classic Firewall が拡張されて以来、Cisco IOS ソフトウェアで使用が可能になっています。

[Cisco IOS VRF 対応 Classic Firewall の設定](#)

VRF 対応 Classic Firewall では、検査ポリシーの設定に関しては、次のように VRF 非対応のファイアウォールと同じ設定構文が使用されます。

```
router(config)#ip inspect name name service
```

検査パラメータは、次のように、VRF 固有の設定オプションで各 VRF に合わせて修正できます。

```
router(config)#ip inspect [parameter value] vrf vrf-name
```

検査ポリシー リストはグローバルに設定され、個々の検査ポリシーを複数の VRF のインターフェイスに適用できます。

各VRFは、サービス拒否(DoS)保護、TCP/UDP/ICMPセッションタイマー、監査証跡の設定などの値に対して、独自の検査パラメータのセットを保持します。1つのインスペクションポリシーが複数のVRFで使用されている場合、VRF固有のパラメータ設定は、インスペクションポリシーによって伝送されるグローバル設定よりも優先されます。DoS 攻撃防御パラメータを調整する方法についての詳細は、『[Cisco IOS Classic Firewall/IPS : サービス拒絶 \(DoS \) 攻撃防御のためのコンテキストベース アクセス コントロール \(CBAC \) の設定](#)』を参照してください。

[Cisco IOS VRF 対応 Classic Firewall アクティビティの表示](#)

VRF対応ファイアウォールの「show」コマンドは、VRF非対応コマンドとは異なります。これは、VRF対応コマンドでは、「show」コマンドでVRFを指定する必要があるためです。

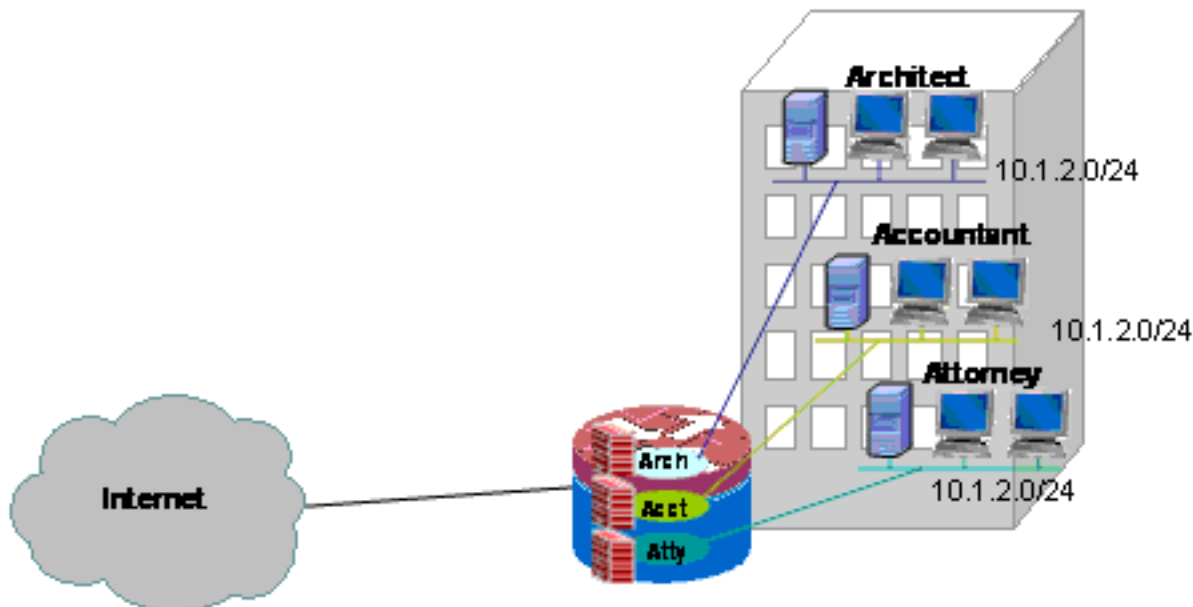
```
router#show ip inspect [ all | config | interfaces | name | sessions | statistics ] vrf vrf-name
```

[マルチ VRF シングルサイトの Classic Firewall](#)

テナント サービスとしてインターネット アクセスを提供するマルチテナント サイトでは、VRF 対応のファイアウォールを使用して、オーバーラップ型アドレス レンジと一律のファイアウォール ポリシーをすべてのテナントに割り当てることができます。それぞれのユーザにとっての VRF 提供の利点により、ルーティング可能スペース、NAT、およびリモート アクセスのための要件、さらにサイト間 VPN サービスに対応可能で、それ以外にも、各テナント用にカスタマイズされたサービスが提供されます。

このアプリケーションでは、アドレス レンジの管理を簡単にするためにオーバーラップ型アドレ

スレンジが使用されています。ところが、これにより、さまざまな VRF 間に接続が提供されてしまうという問題が引き起こされる可能性があります。VRF 間の接続が不要な場合は、従来型の Inside から Outside への NAT を適用できます。次の図では、Architect (arch; 設計部門)、Accountant (acct, 財務部門)、および Attorney (atty; 法務部門) の各 VRF でサーバを提示するために、NAT ポート転送が使用されています。NAT アクティビティには、ファイアウォールの ACL とポリシーで対応する必要があります。



マルチ VRF シングルサイト Classic Network のための Classic Firewall と NAT の設定

テナント サービスとしてインターネット アクセスを提供するマルチテナント サイトでは、VRF 対応のファイアウォールを使用して、オーバーラップ型アドレスレンジと一律のファイアウォールポリシーをすべてのテナントに割り当てることができます。それぞれのユーザにとっての VRF 提供の利点により、ルーティング可能スペース、NAT、およびリモート アクセスのための要件、さらにサイト間 VPN サービスに対応可能で、それ以外にも、各テナント用にカスタマイズされたサービスが提供されます。

Classic Firewall ポリシーが有効になっており、これにより、さまざまな LAN と WAN の接続での双方向のアクセスが次のように定義されます。

		接続元			
		インターネット	Arch (設計部門)	Acct (財務部門)	Atty (法務部門)
接続先	インターネット	N/A	HTTP、HTTPS、FTP、DNS、SMTP	HTTP、HTTPS、FTP、DNS、SMTP	HTTP、HTTPS、FTP、DNS、SMTP
	Arch (設計部門)	FTP	N/A	拒否	拒否

Acct (財務部門)	SMT P	拒否	N/A	拒否
Atty (財務部門)	HTT P、 SMT P	拒否	拒否	N/A

この3つのVRFのそれぞれにあるホストでは、パブリックインターネットでHTTP、HTTPS、FTP、およびDNSのサービスへのアクセスが可能です。3つのVRFすべてで1つのアクセスコントロールリスト(ACL 111)を使用してアクセスが制限されますが(各VRFでは、インターネット上の適合するサービスへのアクセスが許可されりため)、VRF別の検査統計情報を提供する必要があるため、適用される検査ポリシーは異なります。VRF別のACLカウンタを提供するために、個別のACLを使用することもできます。逆に、インターネット上のホストは、ACL 121で定義された前述のポリシーテーブルに従ってサービスに接続できます。反対方向の接続を保護するACLを介したリターンに対応するには、トラフィックを両方向で検査する必要があります。NAT設定にはコメントが付記されており、VRFでの各サービスへのポート転送によるアクセスが説明されています。

シングルサイト、マルチテナントの Classic Firewall と NAT 設定

```

version 12.4
!
ip cef
!
ip vrf acct
!
ip vrf arch
!
ip vrf atty
!
ip inspect name acct-fw ftp
ip inspect name acct-fw tcp
ip inspect name acct-fw udp
ip inspect name acct-fw icmp
ip inspect name arch-fw ftp
ip inspect name arch-fw tcp
ip inspect name arch-fw udp
ip inspect name arch-fw icmp
ip inspect name atty-fw ftp
ip inspect name atty-fw tcp
ip inspect name atty-fw udp
ip inspect name atty-fw icmp
ip inspect name fw-global tcp
ip inspect name fw-global udp
ip inspect name fw-global icmp
!
!
interface FastEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0$
ip address 172.16.100.10 255.255.255.0
ip access-group 121 in
ip nat outside
ip inspect fw-global in
ip virtual-reassembly
speed auto

```

```
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
  no cdp enable  
!  
interface FastEthernet0/1.171  
  encapsulation dot1Q 171  
  ip vrf forwarding acct  
  ip address 10.1.2.1 255.255.255.0  
  ip access-group 111 in  
  ip nat inside  
  ip inspect acct-fw in  
  ip virtual-reassembly  
  no cdp enable  
!  
interface FastEthernet0/1.172  
  encapsulation dot1Q 172  
  ip vrf forwarding arch  
  ip address 10.1.2.1 255.255.255.0  
  ip access-group 111 in  
  ip nat inside  
  ip inspect arch-fw in  
  ip virtual-reassembly  
  no cdp enable  
!  
interface FastEthernet0/1.173  
  encapsulation dot1Q 173  
  ip vrf forwarding atty  
  ip address 10.1.2.1 255.255.255.0  
  ip access-group 111 in  
  ip nat inside  
  ip inspect atty-fw in  
  ip virtual-reassembly  
  no cdp enable  
!  
ip route 0.0.0.0 0.0.0.0 172.16.100.1  
ip route vrf acct 0.0.0.0 0.0.0.0 172.16.100.1 global  
ip route vrf arch 0.0.0.0 0.0.0.0 172.16.100.1 global  
ip route vrf atty 0.0.0.0 0.0.0.0 172.16.100.1 global  
!  
ip nat pool pool-1 172.16.100.100 172.16.100.199 netmask  
255.255.255.0 add-route  
ip nat inside source list 101 pool pool-1 vrf acct  
overload  
ip nat inside source list 101 pool pool-1 vrf arch  
overload  
ip nat inside source list 101 pool pool-1 vrf atty  
overload  
!  
! The following static NAT translations allow access  
from the internet to  
! servers in each VRF. Be sure the static translations  
correlate to "permit"  
! statements in ACL 121, the internet-facing list.  
!  
ip nat inside source static tcp 10.1.2.2 21  
172.16.100.11 21 vrf arch extendable  
ip nat inside source static tcp 10.1.2.3 25  
172.16.100.12 25 vrf acct extendable  
ip nat inside source static tcp 10.1.2.4 25  
172.16.100.13 25 vrf atty extendable  
ip nat inside source static tcp 10.1.2.5 80
```



```

172.16.100.13 80 vrf atty extendable
!
access-list 101 permit ip 10.1.2.0 0.0.0.255 any
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq www
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq 443
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq
smtp
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq ftp
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq
domain
access-list 111 permit udp 10.1.2.0 0.0.0.255 any eq
domain
access-list 111 permit icmp 10.1.2.0 0.0.0.255 any
access-list 121 permit tcp any host 172.16.100.11 eq ftp
access-list 121 permit tcp any host 172.16.100.12 eq
smtp
access-list 121 permit tcp any host 172.16.100.13 eq
smtp
access-list 121 permit tcp any host 172.16.100.13 eq www
end

```

マルチ VRF シングルサイト Classic Network のための Classic Firewall と NAT の確認

ネットワーク アドレス変換とファイアウォールの検査は、次のコマンドで各 VRF につき確認されます。

次のように、**show ip route vrf [vrf-name]** コマンドで各 VRF 内のルートを調べます。

```
stg-2801-L#show ip route vrf acct
```

```
Routing Table: acct
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 172.16.100.1 to network 0.0.0.0
```

```
    172.16.0.0/24 is subnetted, 1 subnets
```

```
S      172.16.100.0 [0/0] via 0.0.0.0, NVI0
```

```
    10.0.0.0/24 is subnetted, 1 subnets
```

```
C      10.1.2.0 is directly connected, FastEthernet0/1.171
```

```
S*    0.0.0.0/0 [1/0] via 172.16.100.1
```

```
stg-2801-L#
```

次のように、**show ip nat tra vrf [vrf-name]** コマンドで各 VRF の NAT アクティビティを調べます。

。

```
stg-2801-L#show ip nat tra vrf acct
```

```
Pro Inside global      Inside local      Outside local      Outside global
```

```
tcp 172.16.100.12:25    10.1.2.3:25      ---                ---
```

```
tcp 172.16.100.100:1078 10.1.2.3:1078    172.17.111.3:80    172.17.111.3:80
```

次のように、**show ip inspect vrf name** コマンドで各 VRF のファイアウォール検査の統計情報を監視します。

```
stg-2801-L#show ip insp se vrf acct
```

```
Established Sessions
```

```
Session 66484034 (10.1.2.3:1078)=>(172.17.111.3:80) tcp SIS_OPEN
```

VRF 対応 Cisco IOS ゾーンベース ポリシー IOS ファイアウォール

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

マルチ VRF ルータ コンフィギュレーションに Cisco IOS ゾーンベース ポリシー ファイアウォールを追加すると、VRF 非対応のアプリケーションでのゾーン ファイアウォールからの差異はほとんど許容されません。つまり、少数のマルチ VRF 固有の条件の追加の場合を除いては、VRF 非対応のゾーンベース ポリシーファイアウォールが従っているものと同じルールに従ってポリシー判定が行われます。

- ゾーンベース ポリシー ファイアウォールのセキュリティ ゾーンに置くことのできるインターフェイスは、1つのゾーンからのインターフェイスだけです。
- 1つの VRF に複数のセキュリティ ゾーンを置くことができます。
- ゾーンベース ポリシー ファイアウォールでは、ルーティングや NAT に依存して、VRF 間のトラフィックの移動が許可されます。インター VRF ゾーンペア間でのトラフィックの検査と通過を行うファイアウォールポリシーは、VRF 間のトラフィックの移動の許可には適切ではありません。

VRF 対応 Cisco IOS ゾーンベース ポリシー ファイアウォールの設定

VRF 対応ゾーンベース ポリシー ファイアウォールでは、VRF 非対応ゾーンベース ポリシー ファイアウォールと同じ設定構文が使用され、インターフェイスがセキュリティ ゾーンに割り当てられ、ゾーン間を移動するトラフィックにセキュリティ ポリシーが定義され、さらに、適切なゾーンペア アソシエーションにセキュリティ ポリシーが割り当てられます。

VRF 個別の設定は不要です。ポリシーマップでの検査にさらに個別のパラメータマップが追加されない限り、グローバル設定パラメータが適用されます。追加で個別設定を適用するためにパラメータマップが使用される場合でも、そのパラメータマップは VRF 固有ではありません。

VRF 対応 Cisco IOS ゾーンベース ポリシー ファイアウォール アクティビティの表示

VRF対応ゾーンベースポリシーファイアウォールのshowコマンドは、非VRF対応コマンドと異なることはありません。ゾーンベースポリシーファイアウォールは、さまざまなインターフェイスのVRF割り当てに関係なく、あるセキュリティゾーンのインターフェイスから別のセキュリティゾーンのインターフェイスに移動するトラフィックを適用します。このようにして、VRF 対応ゾーンベース ポリシー ファイアウォールでは、次のように VRF 非対応アプリケーションでゾーンベース ポリシー ファイアウォールに使用されるのと同じ show コマンドが、ファイアウォール アクティビティの表示に使用されます。

```
router#show policy-map type inspect zone-pair sessions
```

VRF 対応 Cisco IOS ゾーンベース ポリシー ファイアウォールの使用ケース

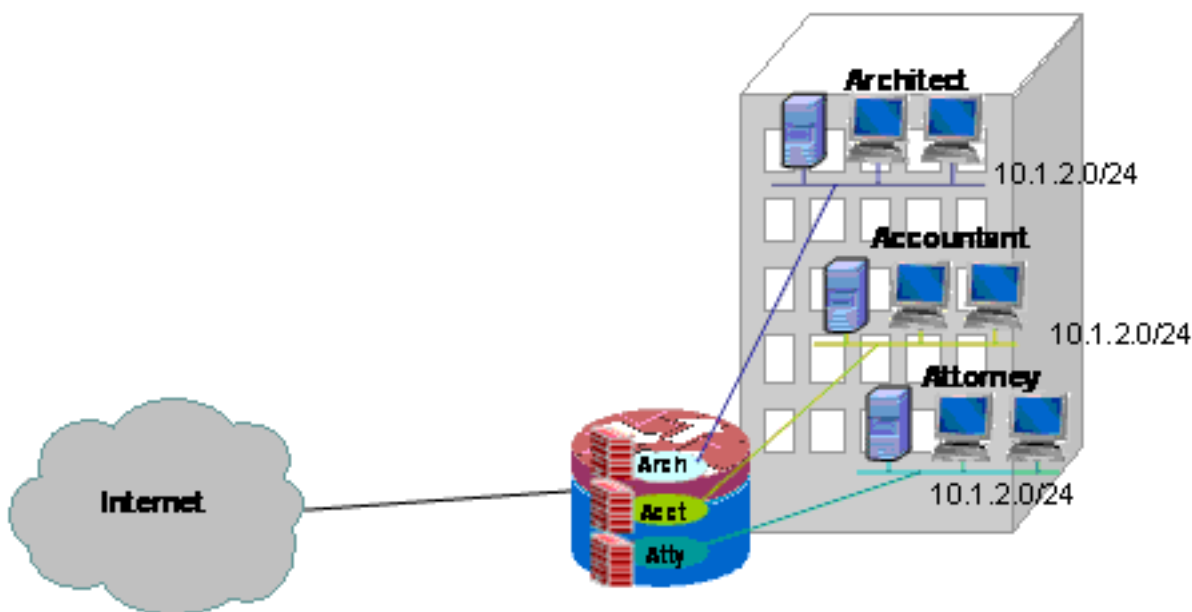
VRF 対応ファイアウォールの使用ケースは広範囲に及びます。次の例がこれに当たります。

- シングルサイト VRF 対応の配備：これは通常、マルチテナント ファシリティやリテール ネットワークに使用されます。
- ブランチ オフィス/リテール/在宅勤務者のアプリケーション：この場合、プライベートネットワークトラフィックがパブリックインターネットトラフィックから分離された VRF に置かれます。インターネット ポリシー アプリケーションに対しては、インターネットアクセスユーザはビジネスネットワーク ユーザからは隔離されており、すべてのビジネスネットワークトラフィックは VPN 接続で HQ サイトに転送されます。

マルチ VRF シングルサイトのゾーンベース ポリシー ファイアウォール

テナント サービスとしてインターネット アクセスを提供するマルチテナント サイトでは、VRF 対応のファイアウォールを使用して、オーバーラップ型アドレスレンジと一律のファイアウォールポリシーをすべてのテナントに割り当てることができます。一般的には、インターネットアクセスに 1 つの Cisco IOS ルータを共有する特定のサイトでの複数の LAN 用であるか、あるいは、DPE 業者や他のサービスなどのビジネスパートナーに対して、ネットワーク ハードウェアやインターネット接続の追加要件なしで、インターネットと構内オーナーのネットワークの特定部分への接続を伴う隔離データ ネットワークを提供する場合に、このアプリケーションが当てはまります。それぞれのユーザにとっての VRF 提供の利点により、ルーティング可能スペース、NAT、およびリモート アクセスのための要件、さらにサイト間 VPN サービスに対応可能で、それ以外にも、各テナント用にカスタマイズされたサービスが提供されます。

このアプリケーションでは、アドレスレンジの管理を簡単にするためにオーバーラップ型アドレスレンジが使用されています。ところが、これにより、さまざまな VRF 間に接続が提供されてしまうという問題が引き起こされる可能性があります。VRF 間の接続が不要な場合は、従来型の Inside から Outside への NAT を適用できます。さらに次の図では、Architect (arch; 設計部門)、Accountant (acct, 財務部門)、および Attorney (atty; 法務部門) の各 VRF でサーバを提示するために、NAT ポート転送が使用されます。NAT アクティビティには、ファイアウォールの ACL とポリシーで対応する必要があります。



マルチ VRF シングルサイトのゾーンベース ポリシー ファイアウォールと NAT の設定

テナント サービスとしてインターネット アクセスを提供するマルチテナント サイトでは、VRF 対応のファイアウォールを使用して、オーバーラップ型アドレスレンジと一律のファイアウォールポリシーをすべてのテナントに割り当てることができます。それぞれのユーザにとっての VRF

提供の利点により、ルーティング可能スペース、NAT、およびリモート アクセスのための要件、さらにサイト間 VPN サービスに対応可能で、それ以外にも、各テナント用にカスタマイズされたサービスが提供されます。

Classic Firewall ポリシーが有効になっており、これにより、さまざまな LAN と WAN の接続での双方向のアクセスが次のように定義されます。

		接続元			
		インターネット	Arch (設計部門)	Acct (財務部門)	Atty (法務部門)
接続先	インターネット	N/A	HTTP、HTTPS、FTP、DNS、SMTP	HTTP、HTTPS、FTP、DNS、SMTP	HTTP、HTTPS、FTP、DNS、SMTP
	Arch (設計部門)	FTP	N/A	拒否	拒否
	Acct (財務部門)	SMTP	拒否	N/A	拒否
	Atty (法務部門)	HTTP、SMTP	拒否	拒否	N/A

この 3 つの VRF のそれぞれにあるホストでは、パブリック インターネットで HTTP、HTTPS、FTP、および DNS のサービスへのアクセスが可能です。3 つの VRF すべてで 1 つのクラスマップ (private-public-cmap) を使用してアクセスが制限されますが (各 VRF では、インターネット上の適合するサービスへのアクセスが許可されるため)、適用されるポリシーマップが異なるので、VRF 別の検査統計情報が提供されます。反対に、前のポリシー テーブルで説明されているように、インターネット上のホストを各サービスに接続することもでき、これは Internet-to-VRF のゾーンペアのための個々のクラスマップとポリシーマップで定義されています。パブリック インターネットからセルフゾーン内のルータの管理サービスへのアクセスを防御するためには、個別のポリシーマップが使用されます。プライベート VRF からルータのセルフゾーンへのアクセスを防御するためにも、同じポリシーを使用できます。

NAT 設定にはコメントが付記されており、VRF での各サービスへのポート転送によるアクセスが説明されています。

```

シングルサイト、マルチテナントのゾーンベース ポリシー  

ファイアウォールと NAT 設定

version 12.4
!
ip cef
!
ip vrf acct

```

```
!  
ip vrf arch  
!  
ip vrf atty  
!  
class-map type inspect match-any out-cmap  
  match protocol http  
  match protocol https  
  match protocol ftp  
  match protocol smtp  
  match protocol ftp  
!  
class-map type inspect match-all pub-arch-cmap  
  match access-group 121  
  match protocol ftp  
!  
class-map type inspect match-all pub-acct-cmap  
  match access-group 122  
  match protocol http  
!  
class-map type inspect pub-atty-mail-cmap  
match access-group 123  
  match protocol smtp  
!  
class-map type inspect pub-atty-web-cmap  
  match access-group 124  
  match protocol http  
!  
policy-map type inspect arch-pub-pmap  
  class type inspect out-cmap  
  inspect  
!  
policy-map type inspect acct-pub-pmap  
  class type inspect out-cmap  
  inspect  
!  
policy-map type inspect atty-pub-pmap  
  class type inspect out-cmap  
  inspect  
!  
policy-map type inspect pub-arch-pmap  
  class type inspect pub-arch-cmap  
  inspect  
!  
policy-map type inspect pub-acct-pmap  
  class type inspect pub-acct-cmap  
  inspect  
!  
policy-map type inspect pub-atty-pmap  
  class type inspect pub-atty-mail-cmap  
  inspect  
  class type inspect pub-atty-web-cmap  
  inspect  
!  
policy-map type inspect pub-self-pmap  
  class class-default  
  drop log  
!  
zone security arch  
zone security acct  
zone security atty  
zone security public  
zone-pair security arch-pub source arch destination  
public
```

```
service-policy type inspect arch-pub-pmap
zone-pair security acct-pub source acct destination
public
service-policy type inspect acct-pub-pmap
zone-pair security atty-pub source atty destination
public
service-policy type inspect atty-pub-pmap
zone-pair security pub-arch source public destination
arch
service-policy type inspect pub-arch-pmap
zone-pair security pub-acct source public destination
acct
service-policy type inspect pub-acct-pmap
zone-pair security pub-atty source public destination
atty
service-policy type inspect pub-atty-pmap
zone-pair security pub-self source public destination
self
service-policy type inspect pub-self-pmap
!
!
interface FastEthernet0/0
description $ETH-LAN$ETH-SW-LAUNCH$$INTF-INFO-FE 0$
ip address 172.16.100.10 255.255.255.0
ip nat outside
zone-member security public
ip virtual-reassembly
speed auto
no cdp enable
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
no cdp enable
!
interface FastEthernet0/1.171
encapsulation dot1Q 171
ip vrf forwarding acct
ip address 10.1.2.1 255.255.255.0
ip nat inside
zone-member security acct
ip virtual-reassembly
no cdp enable
!
interface FastEthernet0/1.172
encapsulation dot1Q 172
ip vrf forwarding arch
ip address 10.1.2.1 255.255.255.0
ip nat inside
zone-member security arch
ip virtual-reassembly
no cdp enable
!
interface FastEthernet0/1.173
encapsulation dot1Q 173
ip vrf forwarding atty
ip address 10.1.2.1 255.255.255.0
ip nat inside
zone-member security atty
ip virtual-reassembly
no cdp enable
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
```

```

ip route vrf acct 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf arch 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf atty 0.0.0.0 0.0.0.0 172.16.100.1 global
!
ip nat pool pool-1 172.16.100.100 172.16.100.199 netmask
255.255.255.0 add-route
ip nat inside source list 101 pool pool-1 vrf acct
overload
ip nat inside source list 101 pool pool-1 vrf arch
overload
ip nat inside source list 101 pool pool-1 vrf atty
overload
!
! The following static NAT translations allow access
from the internet to
! servers in each VRF. Be sure the static translations
correlate to "inspect"
! statements in in the Zone Firewall configuration, the
internet-facing list.
! Note that the ACLs used in the firewall correspond to
the end-host address, not
! the NAT Outside address
!
ip nat inside source static tcp 10.1.2.2 21
172.16.100.11 21 vrf arch extendable
ip nat inside source static tcp 10.1.2.3 25
172.16.100.12 25 vrf acct extendable
ip nat inside source static tcp 10.1.2.4 25
172.16.100.13 25 vrf atty extendable
ip nat inside source static tcp 10.1.2.5 80
172.16.100.13 80 vrf atty extendable
!
access-list 101 permit ip 10.1.2.0 0.0.0.255 any
access-list 121 permit ip any host 10.1.2.2
access-list 122 permit ip any host 10.1.2.3
access-list 123 permit ip any host 10.1.2.4
access-list 124 permit ip any host 10.1.2.5
!
! Disable CDP
!
no cdp run
!
end

```

マルチ VRF シングルサイト Classic Network のための Classic Firewall と NAT の確認

ネットワーク アドレス変換とファイアウォールの検査は、次のコマンドで各 VRF につき確認されます。

次のように、**show ip route vrf [vrf-name]** コマンドで各 VRF 内のルートを調べます。

```
stg-2801-L#show ip route vrf acct
```

```
Routing Table: acct
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 172.16.100.1 to network 0.0.0.0

```
172.16.0.0/24 is subnetted, 1 subnets
S    172.16.100.0 [0/0] via 0.0.0.0, NVI0
10.0.0.0/24 is subnetted, 1 subnets
C    10.1.2.0 is directly connected, FastEthernet0/1.171
S*  0.0.0.0/0 [1/0] via 172.16.100.1
stg-2801-L#
```

show ip nat tra vrf [vrf-name]コマンドを使用して、各VRFのNATアクティビティを確認します。

```
stg-2801-L#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 172.16.100.12:25   10.1.2.3:25      ---               ---
tcp 172.16.100.100:1033 10.1.2.3:1033    172.17.111.3:80   172.17.111.3:80
tcp 172.16.100.11:21   10.1.2.2:23      ---               ---
tcp 172.16.100.13:25   10.1.2.4:25      ---               ---
tcp 172.16.100.13:80   10.1.2.5:80      ---               ---
```

次のように、**show policy-map type inspect zone-pair** コマンドでファイアウォール検査の統計情報を監視します。

```
stg-2801-L#show policy-map type inspect zone-pair
Zone-pair: arch-pub

Service-policy inspect : arch-pub-pmap

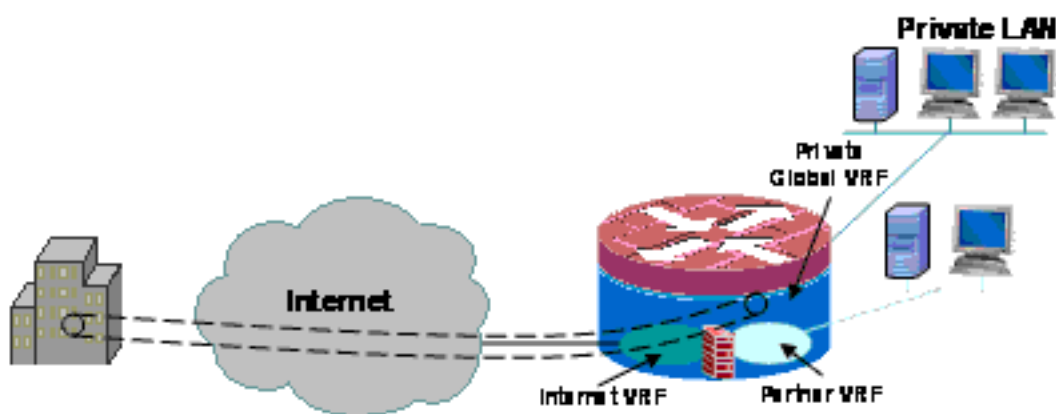
Class-map: out-cmap (match-any)
  Match: protocol http
    1 packets, 28 bytes
    30 second rate 0 bps
  Match: protocol https
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol ftp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol smtp
    0 packets, 0 bytes
    30 second rate 0 bps
Inspect
  Packet inspection statistics [process switch:fast switch]
  tcp packets: [1:15]

  Session creations since subsystem startup or last reset 1
  Current session counts (estab/half-open/terminating) [0:0:0]
  Maxever session counts (estab/half-open/terminating) [1:1:0]
  Last session created 00:09:50
  Last statistic reset never
  Last session creation rate 0
  Maxever session creation rate 1
  Last half-open session total 0

Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    8 packets, 224 bytes
```

[マルチVRFシングルサイトゾーンベースポリシーファイアウォール、「インターネット」ゾーンでのバックアップを使用したインターネット接続、グローバルVRFはHQに接続](#)

このアプリケーションが適しているのは、在宅勤務者の展開、小規模なリテール ロケーション、および、プライベート ネットワーク リソースをパブリック ネットワーク アクセスから隔離する必要のあるその他のリモートサイト ネットワーク展開すべてです。パブリック VRF に対してインターネット接続とホームやパブリック ホットスポット ユーザとを隔離して、VPN トンネル経由ですべてのプライベートネットワークトラフィックをルーティングするグローバル VRF にデフォルト ルートを適用することにより、プライベート、グローバル VRF、および、インターネットに到達可能なパブリック VRF では相互の到達可能性が無くなり、パブリックインターネット アクティビティによるプライベート ネット ホスト侵入の脅威が完全に解消されます。さらに、追加の VRF を配備することにより、宝くじ端末装置、ATM マシン、チャージカード処理端末装置、その他のアプリケーションなどの隔離ネットワーク スペースを必要とする他のユーザに、保護されたルーティング スペースを提供できます。複数の Wi-Fi SSID を配備することにより、プライベート ネットワークとパブリック ホットスポットの両方へのアクセスを提供できます。



この例では、接続の SLA モニタリングにより保証されたインターネット接続による 2 つのブロードバンドインターネット接続が説明されています。ここでは、パブリックインターネットにアクセスするために、パブリック VRF とパートナー VRF 内のホスト用に PAT (NAT オーバーロード) が適用されています。このプライベート ネットワーク (グローバル VRF 内) では、この 2 つのブロードバンドリンクでの HQ (VPN ヘッドエンド ルータ用に取り込まれている設定) への接続を維持するために、GRE-over-IPSec 接続が使用されています。どちらかのブロードバンド接続で障害が発生した場合、VPN ヘッドエンドへの接続は維持されるため、HQ ネットワークへのアクセスが中断されることはありません。トンネルのローカル エンドポイントは、いずれかのインターネット接続に限定的に結び付けられているわけではないのが、この理由です。

ゾーンベース ポリシー ファイアウォールが配備されて、プライベート ネットワークとの VPN によるアクセスと、パブリック LAN およびパートナー LAN とインターネット間のアクセスを制御することにより、アウトバウンドのインターネットアクセスは許可されますが、インターネットからローカル ネットワークへの接続は許可されません。

	インターネット	パブリック	パートナー	VPN	プライベート
インターネット	N/A	拒否	拒否	拒否	拒否
パブリック	HTTP、HTTPS、FTP、DNS	N/A	拒否	拒否	拒否
パートナー		拒否	N/A		
VPN	拒否	拒否	拒否	N/	

				A	
プライベート	拒否	拒否	拒否		N/A

ホットスポットとパートナーネットトラフィック用の NAT アプリケーションにより、パブリックインターネットからの侵入はさらに難しくなっていますが、悪意のあるユーザやソフトウェアによりアクティブな NAT セッションが悪用される可能性は残っています。ステートフルな検査を行うアプリケーションでは、オープンな NAT セッションへの攻撃によるローカルホストへの侵入の可能性が最小化されます。この例では 871W が採用されていますが、このコンフィギュレーションは他の ISR プラットフォームで簡単に複製が可能です。

マルチ VRF シングルサイト ゾーンベース ポリシー ファイアウォール、バックアップを伴うプライマリインターネット接続、グローバル VRF に HQ への VPN のシナリオでの設定

テナントサービスとしてインターネットアクセスを提供するマルチテナントサイトでは、VRF 対応のファイアウォールを使用して、オーバーラップ型アドレスレンジと一律のファイアウォールポリシーをすべてのテナントに割り当てることができます。それぞれのユーザにとっての VRF 提供の利点により、ルーティング可能スペース、NAT、およびリモートアクセスのための要件、さらにサイト間 VPN サービスに対応可能で、それ以外にも、各テナント用にカスタマイズされたサービスが提供されます。

```

version 12.4
!
hostname stg-871
!
aaa new-model
!
aaa authentication login default local
aaa authorization console
aaa authorization exec default local
!
aaa session-id common
ip cef
!
no ip dhcp use vrf connected
!
ip dhcp pool priv-108-net
  import all
  network 192.168.108.0 255.255.255.0
  default-router 192.168.108.1
!
ip vrf partner
  description Partner VRF
  rd 100:101
!
ip vrf public
  description Internet VRF
  rd 100:100
!
no ip domain lookup
ip domain name yourdomain.com
!
track timer interface 5
!
track 123 rtr 1 reachability
  delay down 15 up 10
!
class-map type inspect match-any hotspot-cmap

```

```
match protocol dns
match protocol http
match protocol https
match protocol ftp
class-map type inspect match-any partner-cmap
match protocol dns
match protocol http
match protocol https
match protocol ftp
!
policy-map type inspect hotspot-pmap
class type inspect hotspot-cmap
inspect
class class-default
!
zone security internet
zone security hotspot
zone security partner
zone security hq
zone security office
zone-pair security priv-pub source private destination public
service-policy type inspect priv-pub-pmap
!
crypto keyring hub-ring vrf public
pre-shared-key address 172.16.111.5 key cisco123
!
crypto isakmp policy 1
authentication pre-share
group 2
!
crypto ipsec transform-set md5-des-ts esp-des esp-md5-hmac
!
crypto ipsec profile md5-des-prof
set transform-set md5-des-ts
!
bridge irb
!
interface Tunnel0
ip unnumbered Vlan1
zone-member security public
tunnel source BV11
tunnel destination 172.16.111.5
tunnel mode ipsec ipv4
tunnel vrf public
tunnel protection ipsec profile md5-des-prof
!
interface FastEthernet0
no cdp enable
!
interface FastEthernet1
no cdp enable
!
interface FastEthernet2
switchport access vlan 111
no cdp enable
!
interface FastEthernet3
switchport access vlan 104
no cdp enable
!
interface FastEthernet4
description Internet Intf
ip dhcp client route track 123
ip vrf forwarding public
```

```
ip address dhcp
ip nat outside
ip virtual-reassembly
speed 100
full-duplex
no cdp enable
!
interface Dot11Radio0
no ip address
!
ssid test
    vlan 11
    authentication open
    guest-mode
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
no cdp enable
!
interface Dot11Radio0.1
encapsulation dot1Q 11 native
no cdp enable
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Vlan1
description LAN Interface
ip address 192.168.108.1 255.255.255.0
ip virtual-reassembly
ip tcp adjust-mss 1452
!
interface Vlan104
ip vrf forwarding public
ip address dhcp
ip nat outside
ip virtual-reassembly
!
interface Vlan11
no ip address
ip nat inside
ip virtual-reassembly
bridge-group 1
!
interface BVI1
ip vrf forwarding public
ip address 192.168.108.1 255.255.255.0
ip nat inside
ip virtual-reassembly
!
router eigrp 1
network 192.168.108.0
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Tunnel0
ip route vrf public 0.0.0.0 0.0.0.0 Vlan104 dhcp 10
ip route vrf public 0.0.0.0 0.0.0.0 FastEthernet4 dhcp
!
ip nat inside source route-map dhcp-nat interface Vlan104 vrf public overload
ip nat inside source route-map fixed-nat interface FastEthernet4 vrf public overload
!
ip sla 1
```

```

icmp-echo 172.16.108.1 source-interface FastEthernet4
timeout 1000
threshold 40
vrf public
frequency 3
ip sla schedule 1 life forever start-time now
access-list 110 permit ip 192.168.108.0 0.0.0.255 any
access-list 111 permit ip 192.168.108.0 0.0.0.255 any
no cdp run
!
route-map fixed-nat permit 10
  match ip address 110
  match interface FastEthernet4
!
route-map dhcp-nat permit 10
  match ip address 111
  match interface Vlan104
!
bridge 1 protocol ieee
bridge 1 route ip
!
end

```

次のハブ設定では、VPN 接続の設定例を示しています。

```

version 12.4
!
hostname 3845-bottom
!
ip cef
!
crypto keyring any-peer
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 1
  authentication pre-share
  group 2
crypto isakmp profile profile-name
  keyring any-peer
  match identity address 0.0.0.0
  virtual-template 1
!
crypto ipsec transform-set md5-des-ts esp-des esp-md5-hmac
!
crypto ipsec profile md5-des-prof
  set transform-set md5-des-ts
!
interface Loopback111
  ip address 192.168.111.1 255.255.255.0
  ip nat enable
!
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto
  media-type rj45
  no keepalive
!
interface GigabitEthernet0/0.1
  encapsulation dot1Q 1 native
  ip address 172.16.1.103 255.255.255.0
  shutdown
!

```

```

interface GigabitEthernet0/0.111
 encapsulation dot1Q 111
 ip address 172.16.111.5 255.255.255.0
 ip nat enable
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback111
 ip nat enable
 tunnel source GigabitEthernet0/0.111
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile md5-des-prof
!
router eigrp 1
 network 192.168.111.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 172.16.111.1
!
ip nat source list 111 interface GigabitEthernet0/0.111
!
access-list 1 permit any
access-list 111 deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.0.0 0.0.255.255 any
!
!
End

```

マルチ VRF シングルサイト ゾーンベース ポリシー ファイアウォール、バックアップを伴うプライマリ インターネット接続、グローバル VRF に HQ への VPN のシナリオでの確認

ネットワーク アドレス変換とファイアウォールの検査は、次のコマンドで各 VRF につき確認されます。

次のように、**show ip route vrf [vrf-name]** コマンドで各 VRF 内のルートを調べます。

```
stg-2801-L#show ip route vrf acct
```

次のように、**show ip nat tra vrf [vrf-name]** コマンドで各 VRF の NAT アクティビティを調べます。

```
stg-2801-L#show ip nat translations
```

次のように、**show policy-map type inspect zone-pair** コマンドでファイアウォール検査の統計情報を監視します。

```
stg-2801-L#show policy-map type inspect zone-pair
```

結論

Cisco IOS の VRF 対応 Classic タイプとゾーンベース ポリシーのファイアウォールにより、複数のネットワークに対する統合セキュリティを伴うネットワーク接続を最小のハードウェアで提供するためのコストと管理上の負担が削減されます。複数のネットワークに対するパフォーマンスとスケーラビリティが確保され、投資コストを増加させることなく、ネットワーク インフラストラクチャとサービスのための効果的なプラットフォームが提供されます。

[確認](#)

現在、この設定に使用できる確認手順はありません。

[トラブルシューティング](#)

問題

ルータの Outside インターフェイスからエクステンジ サーバにはアクセスできません。

解決方法

この問題を修正するには、ルータで SMTP 検査をイネーブルにします。

サンプル コンフィギュレーション

```
ip nat inside source static tcp 192.168.1.10 25 10.15.22.2 25 extendable
ip nat inside source static tcp 192.168.1.10 80 10.15.22.2 80 extendable
ip nat inside source static tcp 192.168.1.10 443 10.15.22.2 443 extendable

access-list 101 permit ip any host 192.168.1.10
access-list 103 permit ip any host 192.168.1.10
access-list 105 permit ip any host 192.168.1.10

class-map type inspect match-all sdm-nat-http-1
 match access-group 101
 match protocol http

class-map type inspect match-all sdm-nat-http-2
 match access-group 103
 match protocol http

class-map type inspect match-all sdm-nat-http-3 **
 match access-group 105
 match protocol http

policy-map type inspect sdm-pol-NATOutsideToInside-1
 class type inspect sdm-nat-http-1
 inspect
 class type inspect sdm-nat-user-protocol--1-1
 inspect
 class type inspect sdm-nat-http-2
 inspect
 class class-default

policy-map type inspect sdm-pol-NATOutsideToInside-2 **
 class type inspect sdm-nat-user-protocol--1-2
 inspect
 class type inspect sdm-nat-http-3
 inspect
 class class-default

zone-pair security sdm-zp-NATOutsideToInside-1 source out-zone destination in-zone
 service-policy type inspect sdm-pol-NATOutsideToInside-2
```

[関連情報](#)

- [ゾーンベース ポリシー ファイアウォール設計ガイド](#)
- [VPN でのゾーンベース ポリシー ファイアウォールの使用](#)
- [VRF対応Cisco IOSファイアウォール](#)
- [MPLS VPN での NAT の統合](#)
- [カスタマー エッジ ルータ用の MPLS 拡張機能の設計](#)
- [NAT の動作確認と NAT の基本的なトラブルシューティング](#)
- [PIX/ASA マルチ コンテキストの設定例](#)
- [Cisco IOS ファイアウォール](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)