Cisco IOS防火牆經典和基於區域的虛擬防火牆應用配置示例

目錄

簡介

本檔案介紹VRF感知虛擬防火牆功能、設定程式的技術背景，以及不同應用程式的使用案例。

Cisco IOS®軟體版本12.3(14)T引入虛擬（VRF感知）防火牆，除了現有的VPN、NAT、QoS和其他VRF感知功能外，擴展虛擬路由轉送(VRF)功能系列以提供狀態封包檢測、透明防火牆、應用檢測和URL過濾。大多數可預知的應用場景將應用NAT和其他功能。如果不需要使用NAT，則可在VRF之間應用路由以提供VRF間連線。Cisco IOS軟體在Cisco IOS經典防火牆和Cisco IOS區域型原則防火牆中均提供VRF感知功能，本文提供這兩種組態模式的範例。更加注重基於區域的策略防火牆配置。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

功能支援

VRF感知防火牆在高級安全、高級IP服務、高級企業映像以及具有*o3*標識的舊術語映像中可用，這表示Cisco IOS防火牆功能集的整合。VRF感知防火牆功能合併到12.4版的Cisco IOS軟體主線版本中。要應用VRF感知區域策略防火牆，需要Cisco IOS軟體版本12.4(6)T或更高版本。Cisco IOS基於區域的策略防火牆無法與狀態故障切換配合使用。

VRF組態

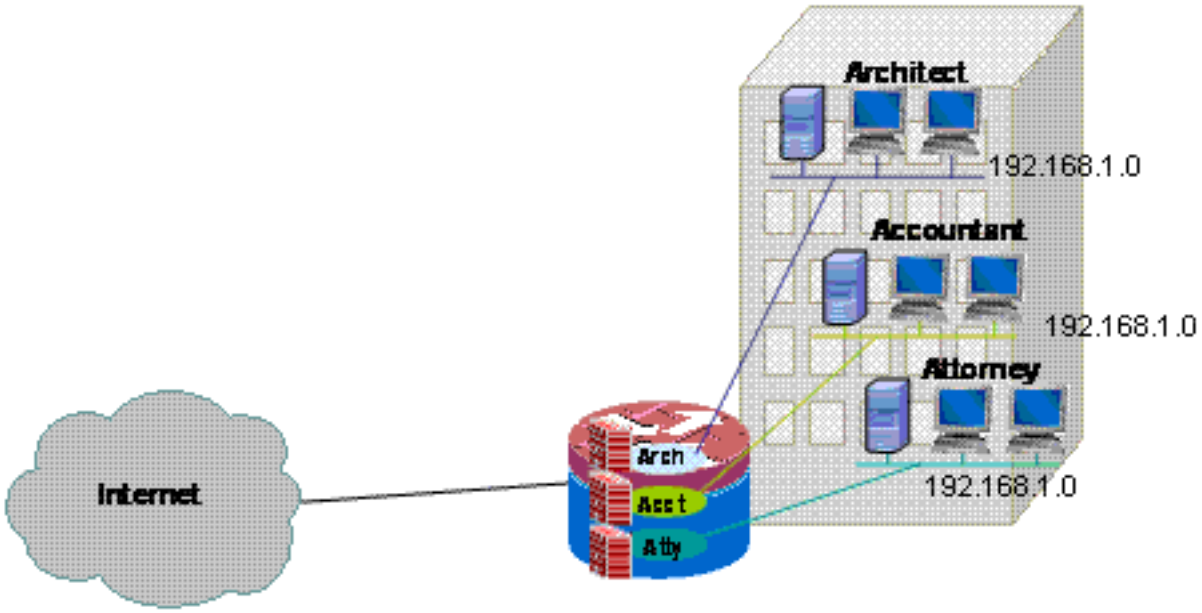
Cisco IOS軟體在同一組態檔中維護全域VRF和所有私人VRF的組態。如果通過命令列介面訪問路由器配置，則可以使用CLI檢視功能中提供的基於角色的訪問控制來限制路由器操作和管理人員的功能。管理應用(如思科安全管理器(CSM))還提供基於角色的訪問控制，確保操作人員被限制到適當的能力級別。

VRF感知IOS防火牆的常見用途概述

VRF感知防火牆為Cisco IOS虛擬路由/轉發(VRF)功能新增了狀態資料包檢測。IPsec VPN、網路位址轉譯(NAT)/連線埠位址轉譯(PAT)、入侵防禦系統(IPS)和其他Cisco IOS安全服務可與VRF感知防火牆結合使用，在VRF中提供一整套安全服務。VRF支援使用重疊IP地址編號的多個路由空間，因此可以將路由器劃分為多個離散路由例項以實現流量分離。VRF感知防火牆在用於路由器正在跟蹤的所有檢查活動的會話資訊中包括VRF標籤，以保持連線狀態資訊之間的分離，該連線狀態資訊在其他方面可以完全相同。VRF感知防火牆可以檢查一個VRF內的介面之間，以及VRF中不同介面之間的檢查，例如流量跨越VRF邊界的情況，從而實現VRF內和VRF間流量的最大防火牆檢查靈活性。

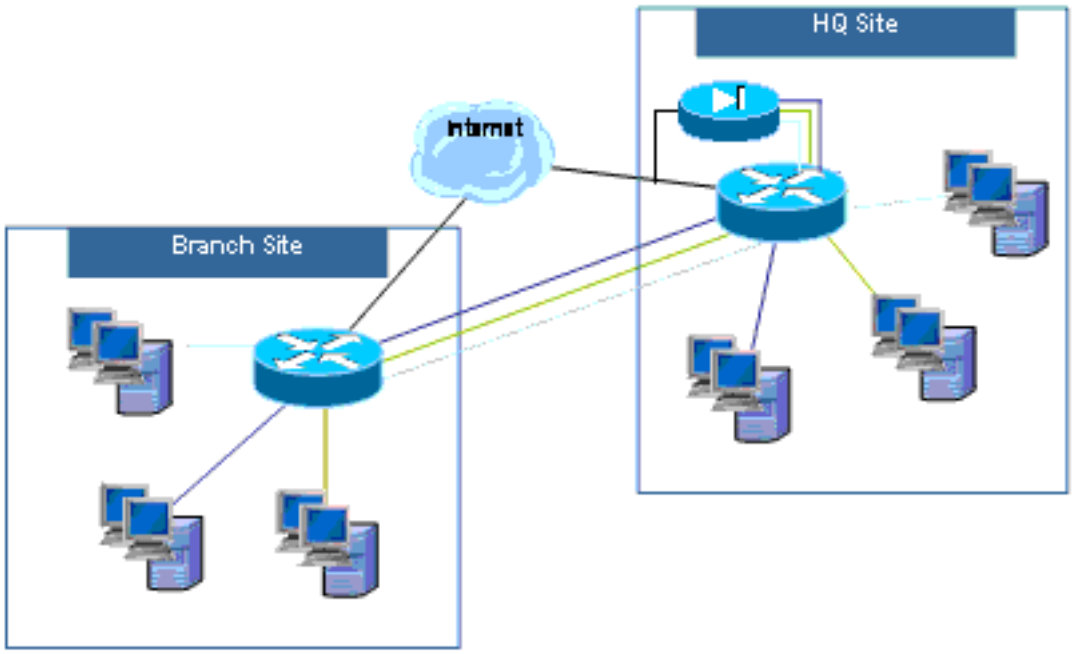
VRF感知Cisco IOS防火牆應用可分為兩個基本類別：

- 多租戶、單站點 — 在單個場所具有重疊地址空間或分離路由空間的多租戶的Internet訪問。狀態防火牆應用於每個VRF的Internet連線，以進一步降低通過開放式NAT連線受到危害的可能性。可以應用埠轉發，以允許連線到VRF中的伺服器。



本文檔中提供了用於VRF感知傳統防火牆配置模型和VRF感知基於區域的防火牆配置模型的多租戶單站點應用的示例。

- 多租戶、多站點 — 大型網路中共用裝置的多個租戶需要通過通過VPN或WAN連線不同站點租戶的VRF連線在多個站點之間連線。一個或多個站點的每個租戶可能需要訪問Internet。為了簡化管理，多個部門可以將自己的網路合併到每個站點的一個接入路由器中，但各個部門都需要進行地址空間隔離。



本文檔即將發佈的更新中將提供VRF感知傳統防火牆配置模型和VRF感知區域防火牆配置模型的多租戶多站點應用的配置示例。

不支援的配置

在支援多VRF CE(VRF Lite)和MPLS VPN的Cisco IOS映像上提供VRF感知防火牆。防火牆功能僅限於非MPLS介面。也就是說，如果一個介面將參與標籤為MPLS的流量，則無法在該介面上應用防火牆檢查。

如果流量必須透過介面進入或離開VRF才能交叉到不同的VRF，則路由器只能檢查VRF間流量。如

果流量直接路由到另一個VRF，則防火牆策略沒有可以檢查流量的物理介面，因此路由器無法應用檢查。

只有在介面上配置了`ip nat inside`或`ip nat outside`時，VRF Lite配置才能與NAT/PAT互操作，在此介面上應用NAT/PAT來修改網路活動的源或目標地址或埠號。VRF間NAT/PAT應用不支援通過向應用NAT或PAT的介面新增`ip nat enable`配置來標識的NAT虛擬介面(NVI)功能。增強請求CSCek35625會跟蹤VRF Lite和NAT虛擬介面之間缺乏互操作性的情況。

設定

本節介紹VRF感知Cisco IOS傳統防火牆和VRF感知區域策略防火牆配置。

註：使用 Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

VRF感知Cisco IOS經典防火牆

本節提供用於設定本文件中所述功能的資訊。

Cisco IOS VRF感知傳統防火牆（以前稱為CBAC）是使用`ip inspect`來識別的，自Cisco IOS軟體版本12.3(14)T擴展傳統防火牆以支援VRF感知檢查以來，它便可用於Cisco IOS軟體。

配置Cisco IOS VRF感知經典防火牆

VRF感知傳統防火牆使用與非VRF防火牆相同的配置語法配置檢查策略：

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

可使用VRF特定的配置選項修改每個VRF的檢查引數：

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

檢測策略清單是全域性配置的，檢測策略可以應用於多個VRF中的介面。

每個VRF都具有自己的值檢查引數集，例如拒絕服務(DoS)保護、TCP/UDP/ICMP會話計時器、審計跟蹤設定等。如果在多個VRF中使用一個檢查策略，則VRF特定的引數配置將取代檢查策略所承載的任何全域性配置。有關如何調整DoS保護引數的詳細資訊，請參閱Cisco IOS經典防火牆和入侵防禦系統拒絕服務保護。

檢視Cisco IOS VRF感知傳統防火牆活動

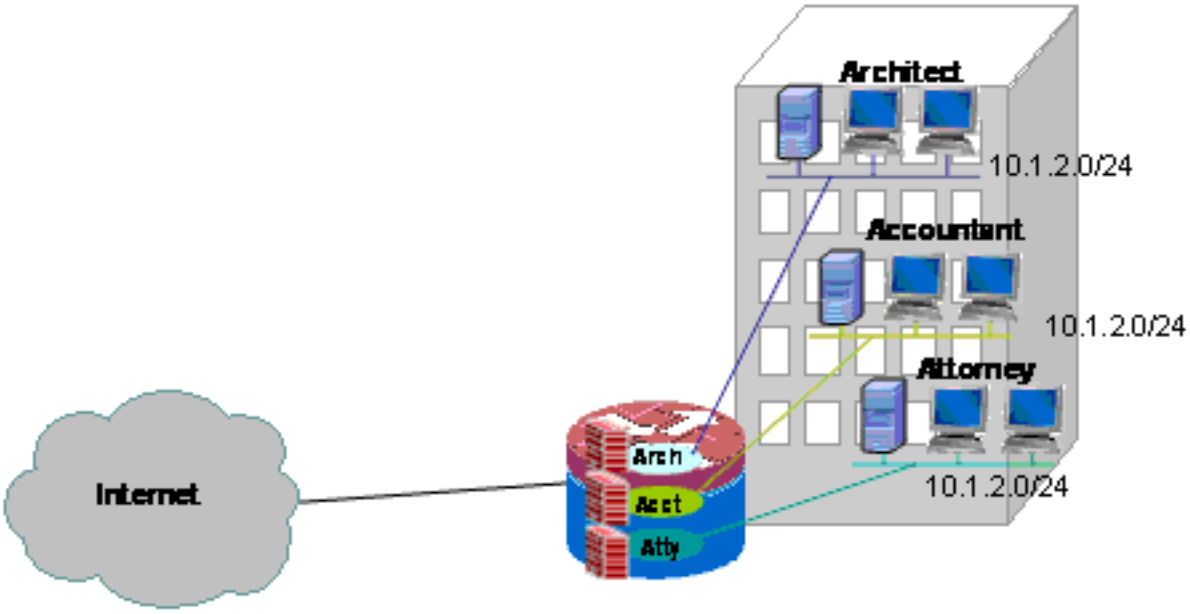
VRF感知防火牆「show」命令與非VRF感知命令不同，因為VRF感知命令要求您在「show」命令中指定VRF:

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

多VRF單站點經典防火牆

提供網際網路接入作為租戶服務的多租戶站點可以使用VRF感知防火牆，以便為所有租戶分配重疊地址空間和樣板防火牆策略。滿足可路由空間、NAT以及遠端訪問和站點到站點VPN服務的要求，並為每個租戶提供定製服務，同時為每個客戶提供VRF。

此應用程式使用重疊的地址空間來簡化地址空間管理。但是，這可能會導致各種VRF之間提供連線的問題。如果VRF之間不需要連線，則可以應用傳統的內部到外部NAT。NAT埠轉發用於暴露架構(arch)、會計(acct)和代理(atty)VRF中的伺服器。防火牆ACL和策略必須適應NAT活動。



為多VRF單站點經典網路配置傳統防火牆和NAT

提供網際網路接入作為租戶服務的多租戶站點可以使用VRF感知防火牆為所有租戶分配重疊地址空間和樣板防火牆策略。滿足可路由空間、NAT以及遠端訪問和站點到站點VPN服務的要求，並為每個租戶提供定製服務，同時為每個客戶提供VRF。

已實施傳統防火牆策略，該策略定義訪問和訪問各種LAN和WAN連線：

		連線源			
		網際網路	拱門	帳戶	阿蒂
連線目標	網際網路	不適用	HTTP、HTTPS、FTP、DNS、SMTP	HTTP、HTTPS、FTP、DNS、SMTP	HTTP、HTTPS、FTP、DNS、SMTP
	拱門	FTP	不適用	拒絕	拒絕
	帳戶	SMTP	拒絕	不適用	拒絕
	阿	H	拒絕	拒絕	不適用

	蒂	TTPSMTP			

三種VRF中的主機均可以訪問公共Internet上的HTTP、HTTPS、FTP和DNS服務。一個訪問控制清單(ACL 111)將用於限制所有三個VRF的訪問（因為每個VRF允許訪問網際網路上的相同服務），但將應用不同的檢查策略，以提供每個VRF的檢查統計資訊。可以使用單獨的ACL為每個VRF提供ACL計數器。相反，Internet上的主機可以連線到ACL 121定義的先前策略表中所述的服務。必須在兩個方向上檢查流量，以適應通過保護相反方向連線的ACL返回的情況。對NAT配置進行註釋以描述埠轉發對VRF中服務的訪問。

單站點多租戶經典防火牆和NAT配置：

```
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
```

驗證多VRF單站點經典網路的傳統防火牆和NAT

使用以下命令驗證每個VRF的網路地址轉換和防火牆檢查：

使用**show ip route vrf [vrf-name]**命令檢查每個VRF中的路由：

```
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#
```

使用**show ip nat tra vrf [vrf-name]**命令檢查每個VRF的NAT活動：

```
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
```

使用**show ip inspect vrf name**命令監控每個VRF的防火牆檢查統計資訊：

```
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感知Cisco IOS基於區域的策略IOS防火牆

本節提供用於設定本文件中所述功能的資訊。

如果將Cisco IOS基於區域的策略防火牆新增到多VRF路由器配置中，則這與非VRF應用中的區域防火牆幾乎沒有區別。也就是說，策略確定遵循非VRF基於區域的策略防火牆遵循的所有規則，除了

新增一些多VRF特定規定外：

- 基於區域的策略防火牆安全區域只能包含來自一個區域的介面。
- VRF可以包含多個安全區域。
- 基於區域的策略防火牆依賴於路由或NAT，以允許流量在VRF之間移動。在VRF間區域對之間檢查或傳遞流量的防火牆策略不足以允許流量在VRF之間移動。

配置VRF感知Cisco IOS基於區域的策略防火牆

VRF感知區域策略防火牆使用與非VRF感知區域策略防火牆相同的配置語法，將介面分配給安全區域，為區域之間移動的流量定義安全策略，並將安全策略分配給適當的區域對關聯。

不需要進行VRF特定配置。除非在策略對映的檢查中新增更具體的引數對映，否則將應用全域性配置引數。即使使用引數對映來應用更具體的配置，引數對映也不是VRF特定的。

檢視VRF感知Cisco IOS基於區域的策略防火牆活動

VRF感知區域策略防火牆**show**命令與非VRF感知命令沒有區別；基於區域的策略防火牆將流量從一個安全區域中的介面移動到另一個安全區域中的介面，而不管各種介面的VRF分配如何。因此，VRF感知區域策略防火牆使用與非VRF應用程式中的區域策略防火牆相同的**show**命令來檢視防火牆活動：

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

VRF感知Cisco IOS基於區域的策略防火牆使用案例

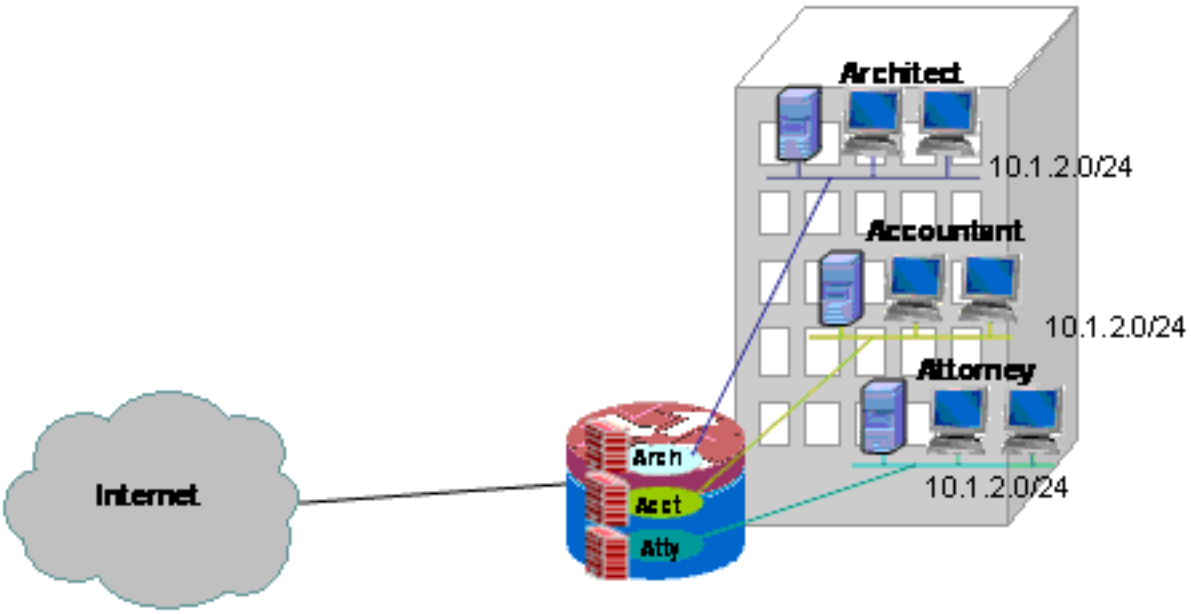
VRF感知防火牆使用案例差異很大。這些示例說明：

- 單站點VRF感知部署，通常用於多租戶設施或零售網路
- 分支機構/零售/電子通勤應用，其中私有網路流量與公共網際網路流量分別儲存在單獨的VRF中。Internet訪問使用者與業務網路使用者隔離，所有業務網路流量通過VPN連線定向到HQ站點以應用網際網路策略。

多VRF單站點基於區域的策略防火牆

提供網際網路接入作為租戶服務的多租戶站點可以使用VRF感知防火牆為所有租戶分配重疊地址空間和樣板防火牆策略。此應用程式通常適用於指定站點上共用一個Cisco IOS路由器以訪問Internet的多個LAN，或者為業務合作夥伴（如影印機或其他服務）提供獨立的資料網路，該網路可以連線到Internet以及房屋所有者網路的特定部分，無需額外的網路硬體或Internet連線。滿足可路由空間、NAT以及遠端訪問和站點到站點VPN服務的要求，並為每個租戶提供定製服務，同時為每個客戶提供VRF。

此應用程式使用重疊的地址空間來簡化地址空間管理。但是，這可能會導致提供各種VRF之間的連線的問題。如果VRF之間不需要連線，則可以應用傳統的內部到外部NAT。此外，NAT埠轉發還用於暴露架構(arch)、會計(acct)和律師(atty)VRF中的伺服器。防火牆ACL和策略必須適應NAT活動。



配置多VRF單站點基於區域的策略防火牆和NAT

作為租戶服務提供Internet訪問的多租戶站點可以使用VRF感知防火牆為所有租戶分配重疊地址空間和樣板防火牆策略。滿足可路由空間、NAT以及遠端訪問和站點到站點VPN服務的要求，並為每個租戶提供定製服務，同時為每個客戶提供VRF。

已實施傳統防火牆策略，該策略定義訪問和訪問各種LAN和WAN連線：

		連線源			
		網際網路	拱門	帳戶	阿蒂
連線目標	網際網路	不適用	HTTP、HTTPS、FTP、DNS、SMTP	HTTP、HTTPS、FTP、DNS、SMTP	HTTP、HTTPS、FTP、DNS、SMTP
	拱門	FTP	不適用	拒絕	拒絕
	帳戶	SMTP	拒絕	不適用	拒絕
	阿蒂	HTTPSMTP	拒絕	拒絕	不適用

三種VRF中的主機均可以訪問公共Internet上的HTTP、HTTPS、FTP和DNS服務。一個類對映(private-public-cmap)用於限制所有三個VRF的訪問，因為每個VRF允許訪問網際網路上的相同服務，但應用不同的策略對映，以便提供每個VRF的檢查統計資訊。相反，Internet上的主機可以連線到前一個策略表中所述的服務，具體由用於Internet到VRF區域對的單個類對映和策略對映定義。單獨的策略對映用於阻止從公共Internet訪問自區中的路由器的管理服務。可以應用相同的策略來阻止從專用VRF訪問路由器的自有區域。

對NAT配置進行註釋以描述埠轉發對VRF中服務的訪問。

單站點多租戶基於區域的策略防火牆和NAT配置：

```
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
```

驗證多VRF單站點經典網路的傳統防火牆和NAT

使用以下命令驗證每個VRF的網路地址轉換和防火牆檢查：

使用**show ip route vrf [vrf-name]**命令檢查每個VRF中的路由：

```
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#
```

使用show ip nat tra vrf [vrf-name]命令檢查每個VRF的NAT活動：

```
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        ---                ---
```

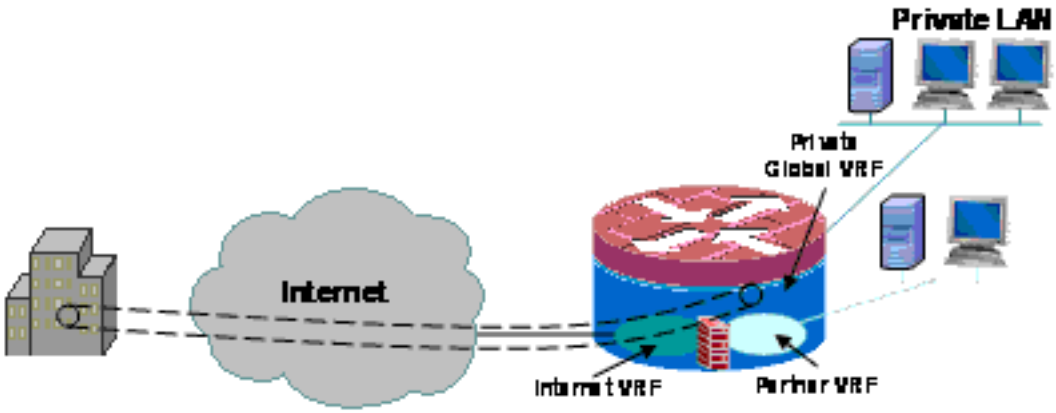
使用**show policy-map type inspect zone-pair**命令監控防火牆檢查統計資訊：

```
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
```

多VRF單站點基於區域的策略防火牆，網際網路連線在「網際網路」區域中備份，全域性VRF連線到HQ

此應用程式非常適合於遠端工作者部署、小型零售場所以及需要將專用網路資源與公共網路訪問隔離的任何其他遠端站點網路部署。通過將網際網路連線和家庭或公共熱點使用者隔離到公共VRF，並在通過VPN隧道路由所有專用網路流量的全域性VRF中應用預設路由，使專用、全域性VRF和網際網路可訪問公共VRF中的資源無法相互訪問，從而完全消除了公共Internet活動對專用網路主機造成的威脅。此外，可配置附加VRF以為需要隔離網路空間的其他消費者提供受保護的路由空間，例如彩票終端、ATM機、充值卡處理終端或其它應用。可配置多個Wi-Fi SSID，以提供對專用網路和公共熱點的訪問。



本示例描述兩個寬頻網際網路連線的配置，將PAT（NAT過載）應用於公共中的主機和*合作夥伴*VRF以訪問公共Internet，同時通過兩個連線上的SLA監控來保證網際網路連線。專用網路（在全域性VRF中）使用GRE-over-IPsec連線通過兩條寬頻鏈路保持與HQ的連線（VPN前端路由器包含配置）。當寬頻連線中的其中一個出現故障時，保持與VPN頭端的連線，這樣便允許不間斷地訪問HQ網路，因為隧道的本地端點不是專門與其中一個Internet連線相連。

基於區域的策略防火牆就位，可控制從VPN訪問和從專用網路訪問VPN，以及公共與合作夥伴LAN與網際網路之間的訪問，以允許出站Internet訪問，但不會從Internet連線到本地網路：

	網際網路	公用	合作夥伴	VPN	私人企業
網際網路	不適用	拒絕	拒絕	拒絕	拒絕
公用	HTTP、HTTPS、FTP、DNS	不適用	拒絕	拒絕	拒絕

合作夥伴		拒絕	不適用		
VPN	拒絕	拒絕	拒絕	不適用	
私人企業	拒絕	拒絕	拒絕		不適用

用於熱點流量和合作夥伴網路流量的NAT應用大大降低了從公共網際網路進行危害的可能性，但惡意使用者或軟體仍有可能利用活動的NAT會話進行攻擊。應用狀態檢測可最大限度地減少本地主機通過攻擊開放的NAT會話而遭到破壞的可能性。此示例使用871W，但配置可以與其他ISR平台輕鬆複製。

配置多VRF單站點基於區域的策略防火牆，主網際網路連線與備份，全域性VRF具有VPN到HQ方案

提供網際網路接入作為租戶服務的多租戶站點可以使用VRF感知防火牆為所有租戶分配重疊地址空間和樣板防火牆策略。滿足可路由空間、NAT以及遠端訪問和站點到站點VPN服務的要求，並為每個租戶提供定製服務，同時為每個客戶提供VRF。

```
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 BVI1
 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
```

此集線器配置提供VPN連線配置的示例：

```
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
```

驗證多VRF單站點基於區域的策略防火牆、具有備份的主網際網路連線、全域性VRF具有VPN到HQ方案

使用以下命令驗證每個VRF的網路地址轉換和防火牆檢查：

使用**show ip route vrf [vrf-name]**命令檢查每個VRF中的路由：

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

使用**show ip nat tra vrf [vrf-name]** 命令檢查每個VRF的NAT活動：

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

使用**show policy-map type inspect zone-pair**命令監控防火牆檢查統計資訊：

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

結論

Cisco IOS VRF感知傳統和基於區域的策略防火牆可降低成本和管理負擔，從而以最小的硬體為多個網路提供整合安全性的網路連線。可保持多個網路的效能和可擴充性，並為網路基礎設施和服務提供有效的平台，而不會增加資本成本。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

問題

無法從路由器的外部介面訪問Exchange伺服器。

解決方案

在路由器中啟用SMTP檢查以解決此問題

示例配置

```
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
```

相關資訊

- 基於區域的策略防火牆設計手冊
- 將基於區域的策略防火牆與VPN配合使用
- VRF感知Cisco IOS防火牆
- 將NAT與MPLS VPN整合
- 為客戶邊緣路由器設計MPLS擴展
- 驗證 NAT 運作情形和基本 NAT 疑難排解
- PIX/ASA多情景配置示例

- Cisco IOS 防火牆
- 技術支援與文件 - Cisco Systems