Cisco IOS 防火墙传统和基于区域的虚拟防火墙应用程序配置示例

目录

简介

本文档介绍了有关 VRF 感知虚拟防火墙功能、配置过程以及各种应用方案的使用案例等方面的技术背景。

Cisco IOS®软件版本12.3(14)T引入了虚拟（VRF感知）防火墙，扩展了虚拟路由转发(VRF)功能系列，除了现有VPN、NAT、QoS和其他VRF外，还提供状态包检测、透明防火墙、应用检测和URL过滤感知功能。多数可预见的应用方案将应用 NAT 和其他功能。如果不需要 NAT，则可以在 VRF 间应用路由，以提供 VRF 间连接。Cisco IOS 软件在 Cisco IOS 传统防火墙和 Cisco IOS 区域策略防火墙中均提供了 VRF 感知功能，本文档提供了这两种配置模型的示例。本文将重点介绍区域策略防火墙配置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

功能支持

在高级安全镜像、高级 IP 服务镜像和高级企业镜像以及带有 *o3* 标识的传统命名原则镜像（该标识表示它集成了 Cisco IOS 防火墙功能集）中均提供了 VRF 感知防火墙。VRF感知防火墙功能合并到12.4版Cisco IOS软件Mainline版本中。要应用VRF感知区域策略防火墙，需要Cisco IOS软件版本12.4(6)T或更高版本。Cisco IOS基于区域的策略防火墙不能用于状态故障切换。

VRF 配置

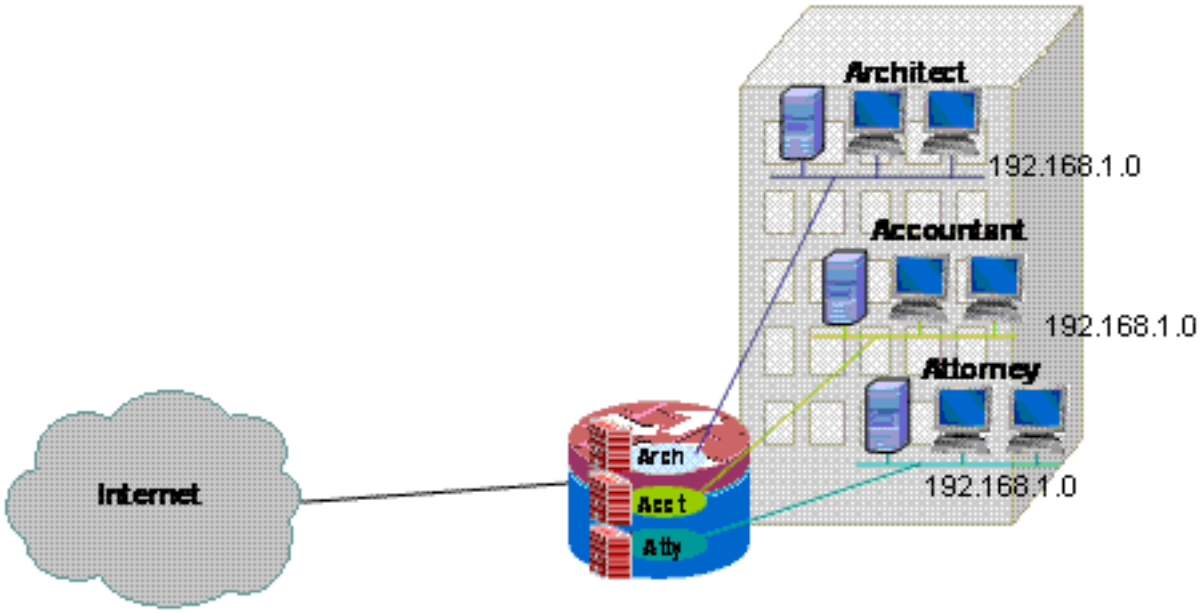
Cisco IOS 软件在相同配置文件中维护全局 VRF 和所有专用 VRF 的配置。如果用户通过命令行界面访问路由器配置，则在 CLI 视图功能中提供的基于角色的访问控制可以用于限制路由器操作和管理人员的能力。管理应用(如思科安全管理器(CSM))还提供基于角色的访问控制，以确保操作人员仅能达到适当的能力级别。

VRF 感知 IOS 防火墙的常见用途概述

VRF感知防火墙将状态数据包检测添加到Cisco IOS虚拟路由/转发(VRF)功能。IPsec VPN、网络地址转换(NAT)/端口地址转换(PAT)、入侵防御系统(IPS)和其他Cisco IOS安全服务可与VRF感知防火墙结合使用，以在VRF中提供一整套安全服务。VRF 支持利用重叠 IP 地址编号实现的多路由空间，因此可以将路由器分成多个分离的路由实例，以进行数据流分离。VRF 感知防火墙在路由器跟踪的所有检查活动的会话信息中包含一个 VRF 标签，从而可以区分可能在其他各方面都相同的连接状态信息。VRF 感知防火墙可以检查一个 VRF 中的接口，也可以检查不同 VRF 中的接口（例如在数据流跨越 VRF 边界的环境中），从而可以非常灵活地对 VRF 内和 VRF 间的数据流进行防火墙检查。

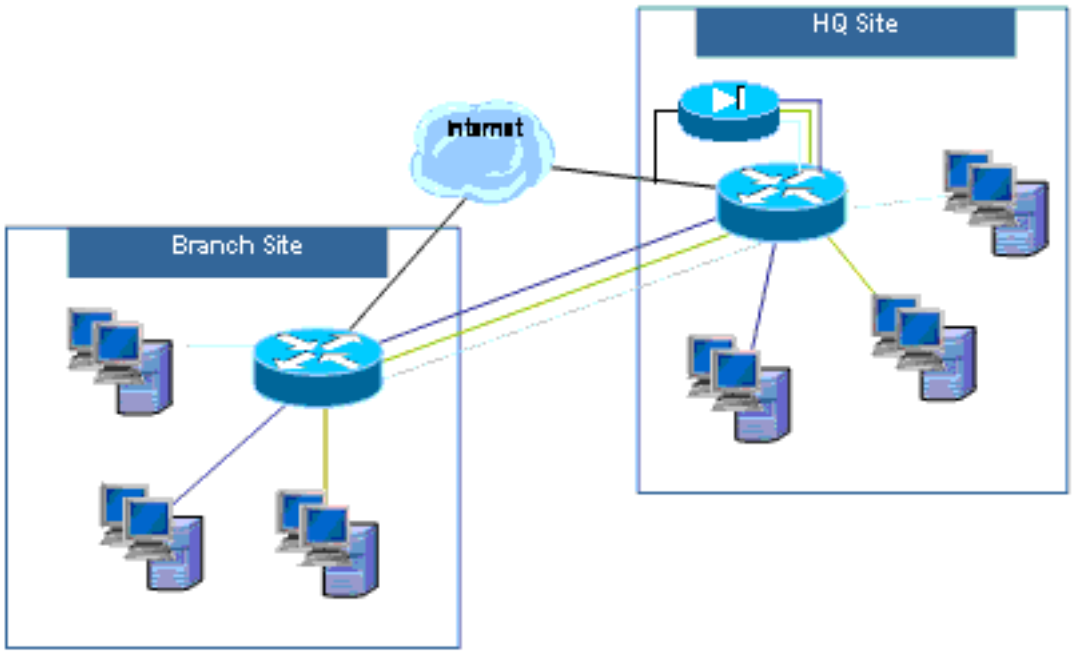
VRF 感知 Cisco IOS 防火墙应用可以分为两种基本类别：

- 多租户单站点 — 使用位于一个位置的重叠地址空间或分离路由空间实现多租户 Internet 访问。状态防火墙应用于每个 VRF 的 Internet 连接，以进一步降低通过开放 NAT 连接带来威胁的可能性。可以应用端口转发以允许连接到 VRF 中的服务器。



本文档针对 VRF 感知传统防火墙配置模型和 VRF 感知区域防火墙配置模型分别提供了一个多租户单站点应用的示例。

- 多租户多站点 — 共享大型网络中设备的多个租户需要通过 VPN 或 WAN 连接来连接位于不同站点的多个租户的 VRF，从而在多个站点间建立连接。位于一个或多个站点的各个租户可能需要能够访问 Internet。为了简化管理，多个部门可以将其网络整合为每个站点具有一个访问路由器，但不同部门需要具有独立的地址空间。



针对 VRF 感知传统防火墙配置模型和 VRF 感知区域防火墙配置模型的多租户多站点配置示例将在本文档未来的内容更新中提供。

不支持的配置

VRF 感知防火墙将在支持多 VRF CE (VRF Lite) 和 MPLS VPN 的 Cisco IOS 镜像中提供。但防火墙功能只能用于非 MPLS 接口。也就是说，如果接口将处理 MPLS 标记的数据流，则不能对此接口应用防火墙检查。

如果数据流必须通过接口进入或离开 VRF 以传递到其他 VRF，则路由器只能检查 VRF 间的数据流

。如果数据流直接路由到另一个 VRF，则没有可供防火墙策略用来检查数据流的物理接口，因此路由器将无法应用检查。

在使用 NAT/PAT 修改网络活动的源地址、目标地址或端口号的接口上，仅当配置了 `ip nat inside` `ip nat outside` `VRF Lite` `NAT/PAT` VRF间NAT/PAT应用不支持通过向应用NAT或PAT的接口添加`ip nat enable`配置来标识的NAT虚拟接口(NVI)功能。这种 VRF Lite 和 NAT 虚拟接口之间缺乏互操作性的信息可以通过增强请求 CSCek35625 跟踪。

配置

本部分介绍了 VRF 感知 Cisco IOS 传统防火墙和 VRF 感知区域策略防火墙配置。

注意：要获取有关本部分中所使用命令的更多信息，可使用命令查找工具（仅限已注册客户）。

VRF 感知 Cisco IOS 传统防火墙

本部分提供有关如何配置本文档所述功能的信息。

自从 Cisco IOS 软件版本 12.3 (14)T 对传统防火墙进行了扩展从而支持 VRF 感知检查之后，Cisco IOS 软件中便已提供 Cisco IOS VRF 感知传统防火墙（以前称为 CBAC）功能（可使用 `IP inspect` 识别此功能）。

配置 Cisco IOS VRF 感知传统防火墙

VRF 感知传统防火墙的检查策略配置与非 VRF 防火墙使用相同的配置语法：

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

您可以使用 VRF 特定的配置选项修改每个 VRF 的检查参数：

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

可以全局配置检查策略列表，并且一个检查策略可以应用于多个 VRF 中的接口。

每个VRF都携带自己的一组检查参数，以用于拒绝服务(DoS)保护、TCP/UDP/ICMP会话计时器、审计跟踪设置等值。如果一个检查策略用于多个 VRF，则 VRF 特定的参数配置将取代检查策略携带的任何全局配置。有关如何调整 DoS 保护参数的详细信息，请参阅 Cisco IOS 传统防火墙和入侵防御系统拒绝服务保护。

查看 Cisco IOS VRF 感知传统防火墙活动

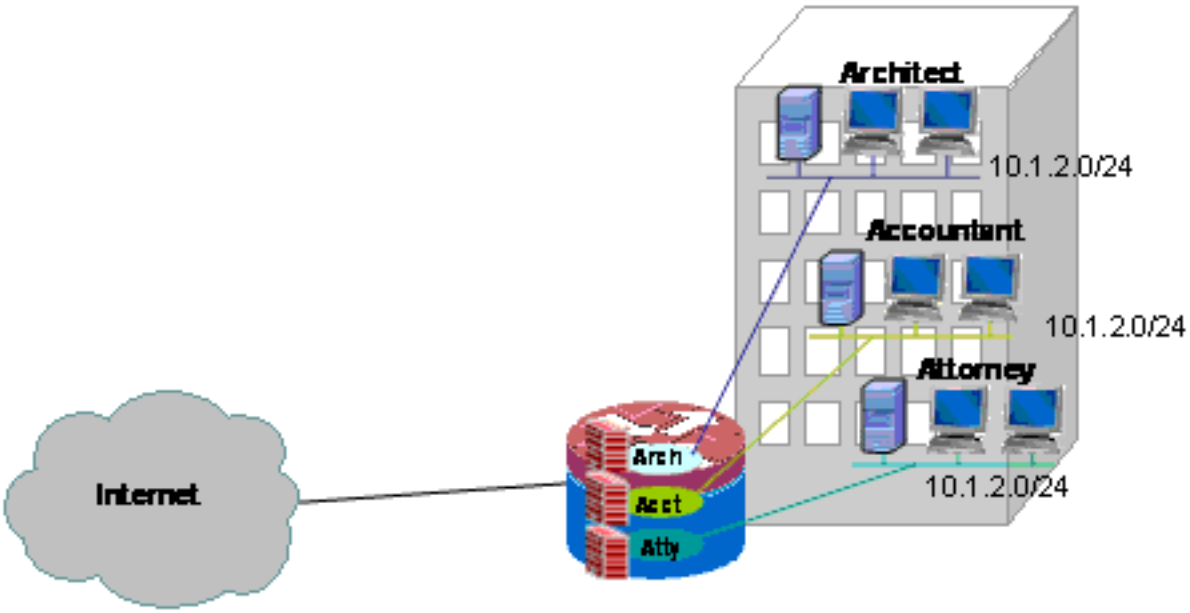
VRF 感知防火墙的“show”命令与非 VRF 感知命令不同，因为 VRF 感知命令要求您在“show”命令中指定 VRF：

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

多 VRF 单站点传统防火墙

以租户服务形式提供 Internet 访问的多租户站点可以使用 VRF 感知防火墙来分配重叠地址空间，并对所有租户使用防火墙策略样板。您可以包含可路由空间、NAT 以及远程访问和站点到站点 VPN 服务等要求，同时由于为每个客户设置了一个 VRF，还可以为每个租户提供自定义服务。

此应用使用重迭地址空间以简化地址空间管理。但是，在多个 VRF 间提供连接时，这可能引起问题。如果不需要 VRF 间连接，则可以应用传统的内部到外部 NAT。NAT 端口转发用于在建筑师 (arch) VRF、会计师 (acct) VRF 和律师 (atty) VRF 中暴露服务器。防火墙 ACL 和策略必须包含 NAT 活动。



为多 VRF 单站点传统网络配置传统防火墙和 NAT

以租户服务形式提供 Internet 访问的多租户站点可以使用 VRF 感知防火墙来分配重叠地址空间，并对所有租户使用防火墙策略样板。您可以包含可路由空间、NAT 以及远程访问和站点到站点 VPN 服务等要求，同时由于为每个客户设置了一个 VRF，还可以为每个租户提供自定义服务。

我们提供了一个传统防火墙策略，它定义了通过各种 LAN 和 WAN 连接的出入访问：

		连接来源			
		互联网	拱门	帐户	阿蒂
连接目标	互联网	不适用	HTTP、HTTPS FTP、DNS、SMTP	HTTP、HTTPS FTP、DNS、SMTP	HTTP、HTTPS FTP、DNS、SMTP
	拱门	FTP	不适用	拒绝	拒绝
	帐户	SMTP	拒绝	不适用	拒绝
	阿	HT	拒绝	拒绝	不适用

	蒂	TP SM TP			

在三个 VRF 中，每个 VRF 中的主机都可以访问公共 Internet 上的 HTTP、HTTPS、FTP 和 DNS 服务。一个访问控制列表 (ACL 111) 用于限制所有三个 VRF 的访问（因为每个 VRF 都允许访问 Internet 上的相同服务），但将应用不同的检查策略，以便可以提供各个 VRF 的检查统计数据。可以使用单独的 ACL 以提供每个 VRF 的 ACL 计数器。相反，Internet上的主机可以按照ACL 121所定义的上一个策略表中所述连接到服务。必须在两个方向上检查流量，以便通过ACL进行返回，从而保护相反方向的连接。我们对 NAT 配置进行了注释，以描述对于 VRF 中各种服务的端口转发访问。

单站点多租户传统防火墙和 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
```

为多 VRF 单站点传统网络验证传统防火墙和 NAT

使用以下命令验证每个 VRF 的网络地址转换和防火墙检查：

使用 **show ip route vrf [vrf-name] 命令检查每个 VRF 中的路由器：**

```
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] 命令检查每个 VRF 的 NAT 活动：**

```
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 命令监视每个 VRF 的防火墙检查统计数据：**

```
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 区域策略 IOS 防火墙

本部分提供有关如何配置本文档所述功能的信息。

如果您将 Cisco IOS 区域策略防火墙添加到多 VRF 路由器配置中，这与非 VRF 应用中的区域防火墙的配置没有多大不同。也就是说，其策略确定的规则与非 VRF 区域策略防火墙完全相同，只是增加了一些多 VRF 特有的规定：

- 区域策略防火墙安全区域只能包含一个区域的接口。

- 一个 VRF 可以包含多个安全区域。
- 区域策略防火墙依赖路由或 NAT 以允许数据流在 VRF 间移动。用于在 VRF 区域对之间检查或传递数据流的防火墙策略不足以允许数据流在 VRF 间移动。

配置 VRF 感知 Cisco IOS 区域策略防火墙

VRF 感知区域策略防火墙使用与非 VRF 感知区域策略防火墙相同的配置语法，并将接口分配到各安全区域，它针对在区域间移动的数据流定义了安全策略，并为相应的关联区域对分配了安全策略。

您不需要进行 VRF 特定的配置。除非在检查的策略映射中添加了更为特定的参数映射，否则将应用全局配置参数。即使在使用参数映射应用特定配置的情况下，参数映射也不是 VRF 特定的。

查看 VRF 感知 Cisco IOS 区域策略防火墙活动

VRF 感知区域策略防火墙的 **show 命令与非 VRF 感知命令没有什么不同**；区域策略防火墙适用于从一个安全区域的接口向另一个安全区域的接口移动的数据流，无论各个接口如何分配 VRF。因此，VRF 感知区域策略防火墙使用与非 VRF 应用中的区域策略防火墙相同的 **show 命令来查看防火墙活动**：

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

VRF 感知 Cisco IOS 区域策略防火墙使用案例

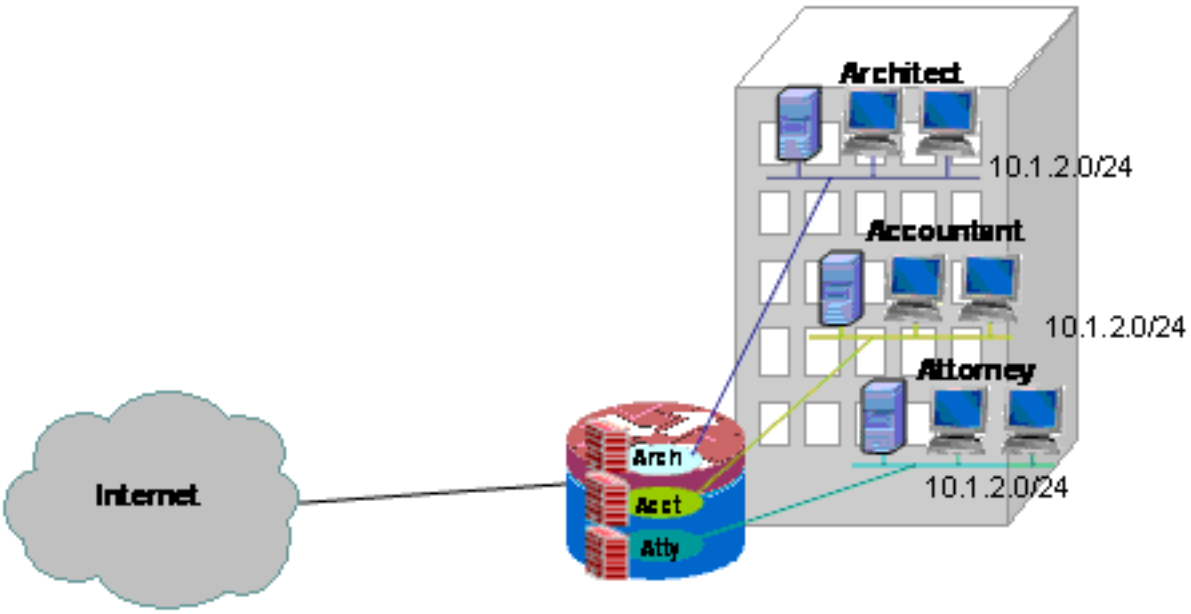
VRF 感知防火墙使用案例各不相同。这些示例适用于：

- 单站点 VRF 感知部署，通常用于多租户设施或零售网络
- 分支办事处/零售/远程工作者应用，在这些环境下专用网络数据流与公共 Internet 数据流位于不同的 VRF 中。Internet 访问用户与企业网络用户相互独立，并且所有企业网络数据流均通过 VPN 连接发往总部站点以应用 Internet 策略。

多 VRF 单站点区域策略防火墙

以租户服务形式提供 Internet 访问的多租户站点可以使用 VRF 感知防火墙来分配重叠地址空间，并对所有租户使用防火墙策略样板。当给定站点中有多个 LAN 共享一个 Cisco IOS 路由器提供 Internet 访问，或者为某个业务伙伴（例如 Photofinisher）或其他服务提供了具备 Internet 连接的独立数据网络以及位置所有者的特定网络部分，并且不要求其他网络硬件或 Internet 连接时，通常使用这种应用。您可以包含可路由空间、NAT 以及远程访问和站点到站点 VPN 服务等要求，同时由于为每个客户设置了一个 VRF，还可以为每个租户提供自定义服务。

此应用使用重迭地址空间以简化地址空间管理。但是，在多个 VRF 间提供连接时，这可能引起问题。如果不需要 VRF 间连接，则可以应用传统的内部到外部 NAT。此外，NAT 端口转发用于在建筑师 (arch)、会计师 (acct) 和律师 (atty) VRF 中暴露服务器。防火墙 ACL 和策略必须包含 NAT 活动。



配置多 VRF 单站点区域策略防火墙和 NAT

以租户服务形式提供 Internet 访问的多租户站点可以使用 VRF 感知防火墙来分配重叠地址空间，并对所有租户使用防火墙策略样板。您可以包含可路由空间、NAT 以及远程访问和站点到站点 VPN 服务等要求，同时由于为每个客户设置了一个 VRF，还可以为每个租户提供自定义服务。

我们提供了一个传统防火墙策略，它定义了通过各种 LAN 和 WAN 连接的出入访问：

		连接来源			
		互联网	拱门	帐户	阿蒂
连接目标	互联网	不适用	HTTP、HTTPS FTP、DNS、SMTP	HTTP、HTTPS FTP、DNS、SMTP	HTTP、HTTPS FTP、DNS、SMTP
	拱门	FTP	不适用	拒绝	拒绝
	帐户	SMTP	拒绝	不适用	拒绝
	阿蒂	HTTP SMTP	拒绝	拒绝	不适用

在三个 VRF 中，每个 VRF 中的主机都可以访问公共 Internet 上的 HTTP、HTTPS、FTP 和 DNS 服务。一个类映射 (private-public-cmap) 用于限制所有三个 VRF 的访问（因为每个 VRF 都允许访问 Internet 上的相同服务），但将应用不同的策略映射，以便可以提供各个 VRF 的检查统计数据。反过来，根据各策略映射和 Internet-to-VRF 区域对策略映射的定义，Internet 上的主机也可以连接到在之前的策略表中描述的服务。单独的策略映射用于防止从公共 Internet 访问路由器自身区域的管理服务。同时可以应用相同的策略以防止从专用 VRF 访问路由器的自身区域。

我们对 NAT 配置进行了注释，以描述对于 VRF 中各种服务的端口转发访问。

单站点多租户区域策略防火墙和 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
```

为多 VRF 单站点传统网络验证传统防火墙和 NAT

使用以下命令验证每个 VRF 的网络地址转换和防火墙检查：

使用 **show ip route vrf [vrf-name]** 命令检查每个 VRF 中的路由器：

```
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] 命令检查每个 VRF 的 NAT 活动：

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

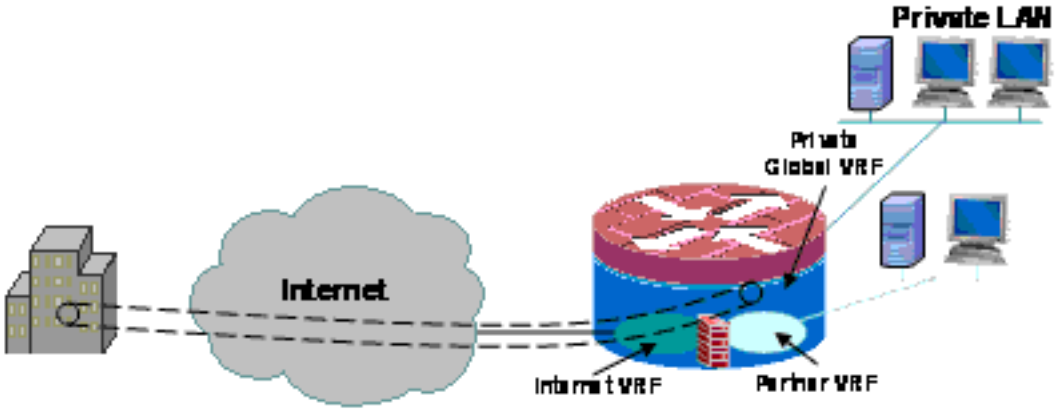
使用 show policy-map type inspect zone-pair 命令监视防火墙检查统计数据：

```
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 单站点区域策略防火墙、“Internet”区域中与备份的 Internet 连接、全局 VRF 具有与总部的连接

此应用非常合适于远程工作者部署、小型零售位置以及任何其他要求专用网络资源独立于公共网络访问的远程站点网络部署。通过将 Internet 连接以及家庭或公共热点用户隔离到*公共 VRF，并在全局 VRF 中应用默认路由（通过 VPN 隧道发送所有专用网络数据流），专用 VRF、全局 VRF 以及可通过 Internet 访问的公共 VRF 中的资源将无法相互访问，从而完全排除了公共 Internet 活动对专用网络主机的威胁*。此外，还可以设置其他 VRF，以便为其他需要独立网络空间的消费者提供受保护的路由空间，例如抽奖终端、ATM 机器、信用卡处理终端或其他应用。可以设置多个 Wi-Fi SSID，以便能够访问这两种专用网络和公共热点。



本示例介绍了两个宽带 Internet 连接的配置，此配置对位于*公共 和合作伙伴 VRF 中的主机访问公共 Internet 应用 PAT（NAT 过载），并在两个连接上使用 SLA 监视保护 Internet 连接的安全*。专用网络（在全局 VRF 中）使用 GRE-over-IPsec 连接维护通过两个宽带链路与总部的连接（包括 VPN 前端路由器的配置）。由于本地隧道端点并未专门附加到某个 Internet 连接，因此在一个或另一个宽带连接失败的情况下，与 VPN 前端的连接将保持畅通，从而可以实现对总部的不间断访问。

我们设置了一个区域策略防火墙，并控制 VPN 与专用网络之间以及公共 LAN 和合作伙伴 LAN 与 Internet 之间的往来访问，以允许出站 Internet 访问，但不能通过 Internet 连接访问本地网络：

	互联网	Public	合作伙伴	VPN	Private
互联网	不适用	拒绝	拒绝	拒绝	拒绝
Public	HTTP、HTTPS、FTP、DNS	不适用	拒绝	拒绝	拒绝
合作伙伴		拒绝	不适用		
VPN	拒绝	拒绝	拒绝	不适用	
Private	拒绝	拒绝	拒绝		不适用

通过对热点和合作伙伴网络数据流应用 NAT，公共 Internet 造成危害的可能性已大大降低，但恶意用户或软件仍可能利用活动 NAT 会话带来威胁。状态检测的应用最大限度降低了通过攻击开放 NAT 会话而危害本地主机的机会。本示例使用 871W，但此配置可以轻松复制到其他 ISR 平台使用。

配置多 VRF 单站点区域策略防火墙、与备份的主要 Internet 连接、全局 VRF 具有用于总部方案的 VPN

以租户服务形式提供 Internet 访问的多租户站点可以使用 VRF 感知防火墙来分配重叠地址空间，并对所有租户使用防火墙策略样板。您可以包含可路由空间、NAT 以及远程访问和站点到站点 VPN 服务等要求，同时由于为每个客户设置了一个 VRF，还可以为每个租户提供自定义服务。

```
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
```

以下集线器配置提供了一个 VPN 连接配置的示例：

```
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
```

验证多 VRF 单站点区域策略防火墙、与备份的主要 Internet 连接、全局 VRF 具有用于总部方案的 VPN

使用以下命令验证每个 VRF 的网络地址转换和防火墙检查：

使用 **show ip route vrf [vrf-name] 命令检查每个 VRF 中的路由器：**

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

使用 **show ip nat tra vrf [vrf-name]** 命令检查每个 VRF 的 NAT 活动：

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

使用 **show policy-map type inspect zone-pair 命令监视防火墙检查统计数据：**

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

结论

Cisco IOS VRF 感知传统防火墙和区域策略防火墙可以使用最少的硬件为多个网络提供集成的安全性，从而减少了建立网络连接的成本和管理负担。它保持了多个网络的性能和可扩展性，同时在不增加成本的前提下为网络基础架构和服务提供了一个有效的平台。

验证

当前没有可用于此配置的验证过程。

故障排除

问题

不能从路由器的外部接口访问 Exchange 服务器。

解决方案

在路由器中启用 SMTP 检查以修复此问题

配置示例

```
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
```

相关信息

- 区域策略防火墙设计指南
- 使用区域策略防火墙与 VPN
- VRF 感知 Cisco IOS 防火墙
- 集成 NAT 与 MPLS VPN
- 设计客户边缘路由器的 MPLS 扩展
- 验证 NAT 的运行和基本的 NAT 故障排除
- PIX/ASA 多上下文配置示例
- Cisco IOS 防火墙
- 技术支持和文档 - Cisco Systems