使用私有地址配置三台路由器之间的 IPSec

目录

简介

本文档介绍了采用专用地址的三个路由器的全网状配置。此示例说明了以下功能：

- 封装安全有效负载 (ESP) — 仅限于数据加密标准 (DES)。
- 预共享密钥
- 每个路由器所配备的专用网络：192.168.1.0、192.168.2.0 和 192.168.3.0
- ISAKMP 策略和加密映射配置
- **access-list** 和 **route-map** 命令用于定义隧道流量。除端口地址转换 (PAT) 外，路由映射还可应用于 Cisco IOS® 软件版本 12.2(4)T2 和更高版本上的一对一静态网络地址转换 (NAT)。有关详情，请参阅 NAT — 将路由映射与静态转换功能配合使用的功能概述。

注意： 加密技术目的是出口控制。您有责任了解与加密技术导出有关的法律。如果您对导出控制有任何疑问，请发送电子邮件至 export@cisco.com。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS 软件版本 12.3(7).T。

- 配置 IPSec 的 Cisco 路由器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- 路由器 1
- 路由器 2
- 路由器 3

路由器 1

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure Internet Key Exchange (IKE) policy and !-
-- pre-shared keys for each peer. !--- IKE policy
defined for peers. crypto isakmp policy 4 authentication
pre-share !--- Pre-shared keys for different peers.
crypto isakmp key xxxxxx1234 address 100.228.202.154
```

```
crypto isakmp key xxxxxx1234 address 200.154.17.130 ! !
!--- IPSec policies: crypto ipsec transform-set encrypt-
des esp-des ! ! crypto map combined local-address
Serial0 !--- Set the peer, transform-set and encryption
traffic for tunnel peers. crypto map combined 20 ipsec-
isakmp set peer 100.228.202.154 set transform-set
encrypt-des match address 106 crypto map combined 30
ipsec-isakmp set peer 200.154.17.130 set transform-set
encrypt-des match address 105 ! ! interface Serial0 ip
address 100.232.202.210 255.255.255.252 ip nat outside
serial restart-delay 0 !--- Apply the crypto map to the
interface. crypto map combined ! interface FastEthernet0
ip address 192.168.1.1 255.255.255.0 ip nat inside ! ip
classless ip route 0.0.0.0 0.0.0.0 100.232.202.209 no ip
http server no ip http secure-server ! !--- Define
traffic for NAT. ip nat inside source route-map nonat
interface Serial0 overload !--- Access control list
(ACL) that shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255 access-list 106 permit ip
192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 !--- ACL to
avoid the traffic through NAT over the tunnel. access-
list 150 deny ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255 access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255 !--- ACL to perform NAT on the
traffic that does not go over the tunnel. access-list
150 permit ip 192.168.1.0 0.0.0.255 any !--- Do not
perform NAT on the IPSec traffic. route-map nonat permit
10 match ip address 150 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! ! end
```

路由器 2

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4 authentication pre-share !--- Pre-shared keys
for different peers. crypto isakmp key xxxxxx1234
address 100.228.202.154 crypto isakmp key xxxxxx1234
address 100.232.202.210 ! ! !--- IPSec policies. crypto
ipsec transform-set encrypt-des esp-des ! ! crypto map
combined local-address Ethernet1 !--- Set the peer,
transform-set and encryption traffic for tunnel peers.
crypto map combined 7 ipsec-isakmp set peer
```

```
100.232.202.210 set transform-set encrypt-des match
address 105 crypto map combined 8 ipsec-isakmp set peer
100.228.202.154 set transform-set encrypt-des match
address 106 ! ! ! interface Ethernet0 ip address
192.168.3.1 255.255.255.0 ip nat inside ! interface
Ethernet1 ip address 200.154.17.130 255.255.255.224 ip
nat outside !--- Apply the crypto map to the interface.
crypto map combined ! ip classless ip route 0.0.0.0
0.0.0.0 200.154.17.129 no ip http server no ip http
secure-server ! !--- Define traffic for NAT. ip nat
inside source route-map nonat interface Ethernet1
overload !--- ACL shows traffic to encrypt over the
tunnel. access-list 105 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255 access-list 106 permit ip
192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255 !--- ACL to
avoid the traffic through NAT over the tunnel. access-
list 150 deny ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255 access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255 !--- ACL to perform NAT on the
traffic that does not go over the tunnel. access-list
150 permit ip any any !--- Do not perform NAT on the
IPSec traffic. route-map nonat permit 10 match ip
address 150 ! ! ! control-plane ! ! line con 0 line aux
0 line vty 0 4 ! ! end
```

路由器 3 配置

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router3
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4 authentication pre-share !--- Pre-shared keys
for different peers. crypto isakmp key xxxxxx1234
address 100.232.202.210 crypto isakmp key xxxxxx1234
address 200.154.17.130 ! ! !--- IPSec policies: crypto
ipsec transform-set encrypt-des esp-des ! ! !--- Set the
peer, transform-set and encryption traffic for tunnel
peers. crypto map combined local-address Serial0 crypto
map combined 7 ipsec-isakmp set peer 100.232.202.210 set
transform-set encrypt-des match address 106 crypto map
combined 8 ipsec-isakmp set peer 200.154.17.130 set
transform-set encrypt-des match address 105 ! !
interface Serial0 ip address 100.228.202.154
255.255.255.252 ip nat outside serial restart-delay 0 !-
-- Apply the crypto map to the interface. crypto map
```

```
combined ! interface FastEthernet0 ip address
192.168.2.1 255.255.255.0 ip nat inside ! ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153 no ip http
server no ip http secure-server ! !--- Define traffic
for NAT. ip nat inside source route-map nonat interface
Serial0 overload !--- ACL that shows traffic to encrypt
over the tunnel. access-list 105 permit ip 192.168.2.0
0.0.0.255 192.168.3.0 0.0.0.255 access-list 106 permit
ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 !--- ACL
to avoid the traffic through NAT over the tunnel.
access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255 access-list 150 deny ip
192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 !--- ACL to
perform NAT on the traffic that does not go over the
tunnel. access-list 150 permit ip 192.168.2.0 0.0.0.255
any !--- Do not perform NAT on the IPSec traffic. route-
map nonat permit 10 match ip address 150 ! ! ! control-
plane ! ! line con 0 line aux 0 line vty 0 4 login ! !
end
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- **show crypto engine connections active** - 显示 IPSec 对等体之间的加密和解密数据包。
- **show crypto isakmp sa** — 显示对等体上的所有当前 IKE 安全关联 (SA)。
- **show crypto ipsec sa** - 显示当前 (IPsec) SA 所采用的设置。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

注意： 在发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

注意： 必须在两个 IPSec 路由器（对等体）上运行以下 debug 命令。必须在两个对等体上清除 SA。

- **debug crypto isakmp** -显示在阶段1期间的错误。
- **debug crypto ipsec** -显示在阶段2期间的错误。
- **debug crypto engine** - 显示来自加密引擎的信息。
- **clear crypto connection connection-id [slot/*rsm*/VIP]** - 终止当前正在进行的加密会话。当会话超时时，加密会话通常会终止。使用 **show crypto cisco connections** 命令可获得连接 ID 值。
- **clear crypto isakmp** - 清除第 1 阶段的 SA。
- **clear crypto sa** - 清除第 2 阶段的 SA。

相关信息

- IPSec 支持页面
- 技术支持 - Cisco Systems