通过 NAT 配置路由器间动态到静态 IPSec

目录

简介

在此示例配置中，远程路由器通过称为 IP 控制协议 (IPCP) 的 PPP 部分接收 IP 地址。远程路由器使用该 IP 地址连接到中心路由器。此配置使中心路由器可以接受动态 IPSec 连接。远程路由器使用网络地址转换 (NAT) 将它后面以特有方式编址的设备“加入”到中心路由器后面以特有方式编址的网络。远程路由器知道端点并可启动到中心路由器的连接。但是中心路由器不知道端点，因此无法启动到远程路由器的连接。

在本示例中，dr_whoovie 是远程路由器，sam-i-am 是中心路由器。一个访问列表指定什么数据流将被加密，因此 dr_whoovie 知道什么数据流将被加密并知道 sam-i-am 端点所在的位置。远程路由器必须启动连接。两端都执行 NAT 过载。

先决条件

要求

本文档需要对 IPSec 协议拥有基本的了解。有关 IPSec 的详细信息，请参见 IP 安全 (IPSec) 加密简介。

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 12.2(24a)
- Cisco 2500 系列路由器

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： 有关本文档所用命令的详细信息，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：

- sam-i-am
- dr_whoovie

sam-i-am

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log up time
no service password-encryption
!
hostname sam-i-am
!
ip subnet-zero
!
!--- These are the IKE policies. crypto isakmp policy 1
!--- Defines an Internet Key Exchange (IKE) policy. !---
Use the crypto isakmp policy command !--- in global
configuration mode. !--- IKE policies define a set of
parameters to be used !--- during the IKE phase I
negotiation. hash md5 authentication pre-share !---
Specifies pre-shared keys as the authentication method.
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 !---
Configures a pre-shared authentication key, !--- used in
global configuration mode. ! !--- These are the IPSec
policies. crypto ipsec transform-set rtpset esp-des esp-
md5-hmac !--- A transform set is an acceptable
combination !--- of security protocols and algorithms.
!--- This command defines a transform set !--- that has
to be matched on the peer router. crypto dynamic-map
rtpmap 10 !--- Use dynamic crypto maps to create policy
templates !--- that can be used to process negotiation
requests !--- for new security associations (SA) from a
remote IPSec peer, !--- even if you do not know all of
```

the crypto map parameters !--- required to communicate with the remote peer, !--- such as the IP address of the peer. **set transform-set rtpset** *!--- Configure IPSec to use the transform set "rtpset" !--- that was defined previously.* **match address 115** *!--- Assign an extended access list to a crypto map entry !--- that is used by IPSec to determine which traffic !--- should be protected by crypto and which traffic !--- does not need crypto protection.* **crypto map rtptrans 10 ipsec-isakmp dynamic rtpmap** *!--- Specifies that this crypto map entry is to reference !--- a preexisting dynamic crypto map. !* **interface Ethernet0 ip address 10.2.2.3 255.255.255.0** no ip directed-broadcast **ip nat inside** *!--- This indicates that the interface is connected to the !--- inside network, which is subject to NAT translation.* no mop enabled ! **interface Serial0 ip address 99.99.99.1 255.255.255.0** no ip directed-broadcast **ip nat outside** *!--- This indicates that the interface is connected !--- to the outside network.* **crypto map rtptrans** *!--- Use the* ***crypto map*** *interface configuration command !--- to apply a previously defined crypto map set to an interface. !* **ip nat inside source route-map nonat interface Serial0 overload** *!--- Except the private network from the NAT process.* ip classless **ip route 0.0.0.0 0.0.0.0 Serial0** no ip http server ! **access-list 115 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list 115 deny ip 10.2.2.0 0.0.0.255 any** *!--- Include the private-network-to-private-network traffic !--- in the encryption process.* **access-list 120 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list 120 permit ip 10.2.2.0 0.0.0.255 any** *!--- Except the private network from the NAT process.* **route-map nonat permit 10 match ip address 120** ! line con 0 transport input none line aux 0 line vty 0 4 password ww login ! end

dr_whoovie

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
ip subnet-zero
!
!--- These are the IKE policies. crypto isakmp policy 1
!--- Defines an Internet Key Exchange (IKE) policy. !---
Use the crypto isakmp policy command !--- in global
configuration mode. !--- IKE policies define a set of
parameters to be used !--- during the IKE phase I
negotiation. hash md5 authentication pre-share !---
Specifies pre-shared keys as the authentication method.
crypto isakmp key cisco123 address 99.99.99.1 !---
Configures a pre-shared authentication key, !--- used in
global configuration mode. ! !--- These are the IPSec
policies. crypto ipsec transform-set rtpset esp-des esp-
md5-hmac !--- A transform set is an acceptable
combination !--- of security protocols and algorithms.
!--- This command defines a transform set !--- that has
to be matched on the peer router. ! crypto map rtp 1
ipsec-isakmp !--- Creates a crypto map and indicates
that IKE will be used !--- to establish the IPSec SAs
```

```
for protecting !--- the traffic specified by this crypto
map entry. set peer 99.99.99.1 !--- Use the set peer
command to specify an IPSec peer in a crypto map entry.
set transform-set rtpset !--- Configure IPSec to use the
transform set "rtpset" !--- that was defined previously.
match address 115 !--- Include the private-network-to-
private-network traffic !--- in the encryption process.
! interface Ethernet0 ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast ip nat inside !--- This
indicates that the interface is connected to the !---
inside network, which is subject to NAT translation. no
mop enabled ! interface Serial0 ip address negotiated !-
-- Specifies that the IP address for this interface !---
is obtained via PPP/IPCP address negotiation. !--- This
example was set up in a lab with an IP address !---
assigned with IPCP. no ip directed-broadcast ip nat
outside !--- This indicates that the interface is
connected !--- to the outside network. encapsulation ppp
no ip mroute-cache no ip route-cache crypto map rtp !---
Use the crypto map interface configuration command !---
to apply a previously defined crypto map set to an
interface. ip nat inside source route-map nonat
interface Serial0 overload !--- Except the private
network from the NAT process. ip classless ip route
0.0.0.0 0.0.0.0 Serial0 no ip http server ! access-list
115 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 115 deny ip 10.1.1.0 0.0.0.255 any !---
Include the private-network-to-private-network traffic
!--- in the encryption process. access-list 120 deny ip
10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255 access-list 120
permit ip 10.1.1.0 0.0.0.255 any !--- Except the private
network from the NAT process. dialer-list 1 protocol ip
permit dialer-list 1 protocol ipx permit route-map nonat
permit 10 match ip address 120 ! line con 0 transport
input none line aux 0 line vty 0 4 password ww 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。

- ping - 用于诊断基本网络连接此示例显示从 dr_whoovie 上的 10.1.1.1 以太网接口到 sam-i-am 上的 10.2.2.3 以太网接口的 ping。`dr_whoovie# ping Protocol [ip]: Target IP address: 10.2.2.3 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 10.1.1.1 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.2.2.3, timeout is 2 seconds: Packet sent with a source address of 10.1.1.1 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 36/38/40 ms`
- show crypto ipsec sa - 显示第 2 阶段安全关联 (SA)。
- show crypto isakmp sa - 显示第 1 阶段 SA。

示例输出

此输出是在中心路由器上发出的 **show crypto ipsec sa** 命令的输出。

```
sam-i-am# show crypto ipsec sa interface: Serial0 Crypto map tag: rtptrans, local addr.
99.99.99.1 local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) current_peer: 100.100.100.1 PERMIT, flags={}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6 #pkts decaps: 6, #pkts decrypt: 6, #pkts
verify 6 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr.
failed: 0, #pkts decompress failed: 0, #send errors 0, #recv errors 0 local crypto endpt.:
99.99.99.1, remote crypto endpt.: 100.100.100.1 path mtu 1500, ip mtu 1500, ip mtu interface
Serial0 current outbound spi: 52456533 inbound esp sas: spi: 0x6462305C(1684156508) transform:
esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto
map: rtptrans sa timing: remaining key lifetime (k/sec): (4607999/3510) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0x52456533(1380279603) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2001, flow_id: 2, crypto map: rtptrans sa timing: remaining key lifetime (k/sec):
(4607999/3510) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
```

此命令显示在对等设备之间建立的 IPSec SA。加密隧道连接 dr_whoovie 上的 100.100.100.1 接口和 sam-i-am 上的 99.99.99.1 接口。此隧道传输在网络 10.2.2.3 和 10.1.1.1 之间流动的数据流。入站和出站时会构建两个封装安全有效负载 (ESP) SA。尽管 sam-i-am 不知道对等体 IP 地址 (100.100.100.1)，还是会建立隧道。由于没有配置 AH，因此未使用身份验证报头 (AH) SA。

这些输出示例显示 dr_whoovie 上的串行接口 0 通过 IPCP 收到 IP 地址 100.100.100.1。

- 在协商 IP 地址前：`dr_whoovie#show interface serial0 Serial0 is up, line protocol is up Hardware is HD64570 Internet address will be negotiated using IPCP MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation PPP, loopback not set`
- 在协商 IP 地址后：`dr_whoovie#show interface serial0 Serial0 is up, line protocol is up Hardware is HD64570 Internet address is 100.100.100.1/32 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation PPP, loopback not set`

此示例在实验室中设置，它使用 **peer default ip address** 命令在 dr_whoovie 上的串行接口 0 的远程端分配 IP 地址。IP 池是使用 **ip local pool** 命令在远程端定义的。

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（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

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

- **debug crypto ipsec - 显示第 2 阶段的 IPsec 协商。**
- debug crypto isakmp - 显示第 1 阶段的 Internet 安全连接和密钥管理协议 (ISAKMP) 协商。
- debug crypto engine - 显示已加密的数据流。
- debug ip nat detailed - （可选）通过显示有关路由器转换的每个数据包的信息来验证 NAT 功能的操作。**警告：** 此命令会生成大量输出。请仅在 IP 网络上的流量很小时使用此命令。
- clear crypto isakmp - 清除与第 1 阶段相关的 SA。
- clear crypto sa - 清除与第 2 阶段相关的 SA。
- clear ip nat translation - 从转换表中清除动态 NAT 转换。

相关信息

- IPSec 支持页面
- 技术支持 - Cisco Systems