使用NAT配置路由器到路由器的動態到靜態IPSec

目錄

簡介

在此示例配置中，遠端路由器透過稱為IP控制協定(IPCP)的PPP的一部分接收IP地址。遠端路由器使用IP地址連線到中心路由器。此配置使中心路由器能夠接受動態IPSec連線。遠端路由器使用網路地址轉換(NAT)將其後面的私有定址裝置「加入」中心路由器後面的私有定址網路。遠端路由器知道端點，並且可以啟動與中心路由器的連線。但是，中心路由器不知道終端，因此無法啟動到遠端路由器的連線。

在本示例中，dr_whoovie是遠端路由器，sam-i-am是中心路由器。訪問清單指定要加密的流量，因此dr_whoovie知道要加密的流量以及sam-i-am終端的位置。遠端路由器必須啟動連線。兩端都在執行NAT過載。

必要條件

需求

本文檔要求對IPSec協定有基本的瞭解。有關IPSec的詳細資訊，請參閱IP安全(IPSec)加密簡介。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科IOS®軟體版本12.2(24a)
- Cisco 2500系列路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

本節提供用於設定本文件中所述功能的資訊。

注意：使用命令查詢工具(僅限註冊客戶)查詢關於用於本文的命令的更多資訊。

網路圖表

此文件使用以下網路設定：

組態

本檔案使用下列組態：

- 山姆
- dr_whoovie

```
<#root>

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 !--
```

```
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

crypto dynamic-map rtpmap 10

!--- Use dynamic crypto maps to create policy templates !--- that can be used to process negotiation re

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 whic

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 NA

 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

<#root>

```
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 !--


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
!
crypto map rtp 1 ipsec-isakmp


!--- Creates a crypto map and indicates that IKE will be used !--- to establish the IPSec SAs for prot

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 NA

 no mop enabled
!

interface Serial0
 ip address negotiated


 !--- Specifies that the IP address for this interface !--- is obtained via PPP/IPCP address negotiatio

 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
```

驗證

本節提供的資訊可用於確認組態是否正常運作。

輸出直譯器工具支援某些show命令(僅供註冊客戶使用)，透過該工具可檢視對show命令輸出的分析。

- ping - 用於診斷基本網路連線

  此範例顯示從dr_whoovie上的10.1.1.1乙太網路介面對sam-i-am上的10.2.2.3乙太網路介面執行ping操作。

  ```
  <#root>

  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 -顯示第2階段安全關聯(SA)。
- show crypto isakmp sa -顯示第1階段SA。

示例輸出

此輸出是在中心路由器上發出的show crypto ipsec sa命令的輸出。

<#root>

```
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:
```

此命令顯示在對等裝置之間構建的IPSec SA。加密隧道連線dr_whoovie上的100.100.100.1介面和sam-i-am上的99.99.99.1介面。此通道傳輸網路10.2.2.3和10.1.1.1之間的流量。兩個封裝安全有效載荷(ESP) SA構建為入站和出站。即使sam-i-am不知道對等體IP地址(100.100.100.1)，仍會建立隧道。由於未配置AH，因此不使用身份驗證報頭(AH) SA。

這些輸出示例顯示dr_whoovie上的串列介面0透過IPCP接收到IP地址100.100.100.1。

- 在協商IP地址之前：

```
<#root>

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
```

- 協商IP位址後：

```
<#root>

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
```

此示例在實驗室中設定，它使用peer default ip address命令在dr_whoovie上的串列介面0的遠端端分配IP地址。IP池是使用ip local pool命令在遠端端定義的。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用) (OIT)支援某些show指令。使用OIT檢視對show命令輸出的分析。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

- debug crypto ipsec -顯示第2階段的IPSec協商。
- debug crypto isakmp -顯示第1階段的Internet安全連線和金鑰管理協定(ISAKMP)協商。
- debug crypto engine -顯示已加密的流量。
- debug ip nat detailed - （可選）透過顯示有關路由器轉換的每個資料包的資訊來驗證NAT功能的操作。

  注意：此命令會生成大量輸出。僅當IP網路上的流量較低時才使用此命令。
- clear crypto isakmp -清除與第1階段相關的SA。
- clear crypto sa -清除與第2階段相關的SA。
- clear ip nat translation - 從轉換表中清除動態NAT轉換。

相關資訊

- IPSec支援頁面

- 技術支援 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。