配置專用和公共網路之間的IPSec路由器到路由器、預共用的NAT過載

目錄

簡介

此組態範例顯示如何使用IPSec對私人網路(10.103.1.x)和公共網路(98.98.98.x)之間的流量進行加密。98.98.98.x網路通過私有地址知道10.103.1.x網路。10.103.1.x網路通過公有地址知道98.98.98.x網路。

必要條件

需求

本文檔需要對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：

- Cisco IOS®軟體版本12.3(5)
- 思科3640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。

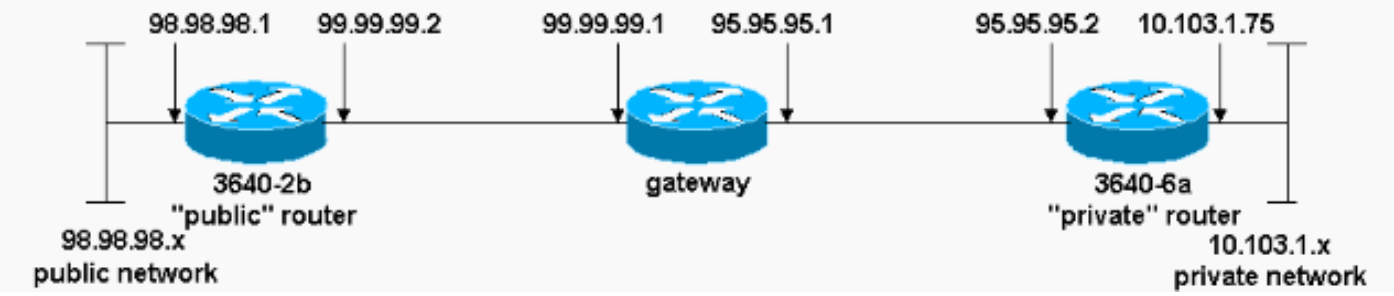
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用下圖中所示的網路設定。



組態

本檔案會使用以下設定：

- 3640-2b「公用」路由器
- 3640-6a「私人」路由器

3640-2b「公用」路由器

```
rp-3640-2b#show running config
Building configuration...

Current configuration:
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-2b
!
ip subnet-zero
!

!
!--- Defines the Internet Key Exchange (IKE) policies.
crypto isakmp policy 1

!--- Defines an IKE policy. Use the crypto isakmp policy
!--- command in global configuration mode. IKE policies
!--- define a set of parameters !--- that are used
during the IKE phase I negotiation.
```

```
hash md5
authentication pre-share

!--- Specifies preshared keys as the authentication
method. crypto isakmp key cisco123 address 95.95.95.2

!--- Configures a preshared authentication key, used in
!--- global configuration mode. ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac

!--- Defines a transform-set. This is an acceptable !---
combination of security protocols and algorithms, !---
which has to be matched on the peer router. ! crypto map
rtp 1 ipsec-isakmp

!--- Indicates that IKE is used to !--- establish the
IPSec security associations (SAs) that protect !--- the
traffic specified by this crypto map entry. set peer
95.95.95.2

!--- Sets the IP address of the remote end. set
transform-set rtpset

!--- Configures IPSec to use the transform-set !---
"rtpset" defined earlier. match address 115

!--- This is used to assign an extended access list to a
!--- crypto map entry which is used by IPSec !--- to
determine which traffic should be protected !--- by
crypto and which traffic does not !--- need crypto
protection. ! interface Ethernet0/0 ip address
98.98.98.1 255.255.255.0 no ip directed-broadcast !
interface Ethernet0/1
ip address 99.99.99.2 255.255.255.0
no ip directed-broadcast
no ip route-cache

!--- Enable process switching for !--- IPSec to encrypt
outgoing packets. !--- This command disables fast
switching. no ip mroute-cache crypto map rtp

!--- Configures the interface to use !--- the crypto map
"rtp" for IPSec. ! . . !--- Output suppressed. . . ip
classless ip route 0.0.0.0 0.0.0.0 99.99.99.1

!--- Default route to the next hop address. no ip http
server ! access-list 115 permit ip 98.98.98.0 0.0.0.255
10.103.1.0 0.0.0.255

!--- This access-list option causes all IP traffic !---
that matches the specified conditions to be !---
protected by IPSec using the policy described by !---
the corresponding crypto map command statements.


access-list 115 deny ip 98.98.98.0 0.0.0.255 any

!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
```

```
end
```

3640-6a「私人」路由器

```
rp-3640-6a#show running config
Building configuration...

Current configuration:
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-6a
!

!
ip subnet-zero



!--- Defines the IKE policies. ! crypto isakmp policy 1

!--- Defines an IKE policy. !--- Use the crypto isakmp
policy !--- command in global configuration mode. IKE
policies !--- define a set of parameters !--- that are
used during the IKE phase I negotiation.


hash md5
authentication pre-share

!--- Specifies preshared keys as the authentication
method. crypto isakmp key cisco123 address 99.99.99.2

!--- Configures a preshared authentication key, !---
used in global configuration mode. ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac

!--- Defines a transform-set. This is an !--- acceptable
combination of security protocols and algorithms, !---
which has to be matched on the peer router. crypto map
rtp 1 ipsec-isakmp

!--- Indicates that IKE is used to establish !--- the
IPSec SAs that protect the traffic !--- specified by
this crypto map entry. set peer 99.99.99.2

!--- Sets the IP address of the remote end. set
transform-set rtpset

!--- Configures IPSec to use the transform-set !---
"rtpset" defined earlier. match address 115

!--- Used to assign an extended access list to a !---
crypto map entry which is used by IPSec !--- to
determine which traffic should be protected !--- by
crypto and which traffic does not !--- need crypto
protection. . . !--- Output suppressed. . . ! interface
Ethernet3/0 ip address 95.95.95.2 255.255.255.0 no ip
directed-broadcast ip nat outside
```

```
!--- Indicates that the interface is !--- connected to
the outside network. no ip route-cache

!--- Enable process switching for !--- IPSec to encrypt
outgoing packets. !--- This command disables fast
switching. no ip mroute-cache crypto map rtp

!--- Configures the interface to use the !--- crypto map
"rtp" for IPSec. ! interface Ethernet3/2 ip address
10.103.1.75 255.255.255.0 no ip directed-broadcast ip
nat inside

!--- Indicates that the interface is connected to !---
the inside network (the network subject to NAT
translation). ! ip nat pool FE30 95.95.95.10 95.95.95.10
netmask 255.255.255.0

!--- Used to define a pool of IP addresses for !--- NAT.
Use the ip nat pool command in !--- global configuration
mode.


ip nat inside source route-map nonat pool FE30 overload

!--- Used to enable NAT of !--- the inside source
address. Use the ip nat inside source !--- command in
global configuration mode. !--- The 'overload' option
enables the router to use one global !--- address for
many local addresses.


ip classless
ip route 0.0.0.0 0.0.0.0 95.95.95.1

!--- Default route to the next hop address. no ip http
server ! access-list 110 deny ip 10.103.1.0 0.0.0.255
98.98.98.0 0.0.0.255
access-list 110 permit ip 10.103.1.0 0.0.0.255 any

!--- Addresses that match this ACL are NATed while !---
they access the Internet. They are not NATed !--- if
they access the 98.98.98.0 network. access-list 115
permit ip 10.103.1.0 0.0.0.255 98.98.98.0 0.0.0.255

!--- This access-list option causes all IP traffic that
!--- matches the specified conditions to be !---
protected by IPSec using the policy described !--- by
the corresponding crypto map command statements.


access-list 115 deny ip 10.103.1.0 0.0.0.255 any

route-map nonat permit 10
match ip address 110
!

!
line con 0


line vty 0 4

!
end
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

若要驗證此設定，請嘗試從私人路由器10.103.1.75上的乙太網路介面發出**ping**延伸命令，目的地為公共路由器98.98.98.1上的乙太網路介面

- ping — 用於診斷基本網路連線。

```
rp-3640-6a#ping
Protocol [ip]:
Target IP address: 98.98.98.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.103.1.75
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 98.98.98.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
```

- show crypto ipsec sa — 顯示當前(IPSec)SA使用的設定。
- show crypto isakmp sa — 顯示對等體上的所有當前IKE SA。
- show crypto engine — 顯示加密引擎的配置資訊摘要。在特權EXEC模式下使用**show crypto engine**命令。

show輸出示例

此輸出來自在集線器路由器上發出的**show crypto ipsec sa**命令。

```
rp-3640-6a#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: rtp, local addr. 95.95.95.2

   protected vrf:
   local  ident (addr/mask/prot/port): (10.103.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (98.98.98.0/255.255.255.0/0/0)
   current_peer: 99.99.99.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 95.95.95.2, remote crypto endpt.: 99.99.99.2
     path mtu 1500, media mtu 1500
```

```
current outbound spi: 75B6D4D7

inbound esp sas:
 spi: 0x71E709E8(1910966760)
   transform: esp-des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
   sa timing: remaining key lifetime (k/sec): (4576308/3300)
   IV size: 8 bytes
   replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x75B6D4D7(1974916311)
   transform: esp-des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
   sa timing: remaining key lifetime (k/sec): (4576310/3300)
   IV size: 8 bytes
   replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

此命令顯示對等體之間構建的IPSec SA。加密通道會建置於 95.95.95.2 和 99.99.99.2 間，適用於流動於 98.98.98.0 和 10.103.1.0 間的流量。 您可以看到內傳和外傳流量所建置的兩個封裝安全性裝載 (ESP) SA。由於沒有AH，因此不使用驗證標頭(AH)SA。

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)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出debug指令之前，請先參閱有關Debug指令的重要資訊。

- **debug crypto ipsec sa** — 用於檢視階段2的IPSec協商。
- **debug crypto isakmp sa** — 用於檢視階段1的ISAKMP協商。
- **debug crypto engine** — 用於顯示加密會話。

相關資訊

- NAT操作順序
- IP安全性疑難排解 — 瞭解和使用debug命令
- IPSec支援頁面
- NAT支援頁面
- 技術支援 - Cisco Systems