使用IOS防火牆和NAT在GRE通道上配置路由器到路由器IPsec（預共用金鑰）

目錄

簡介

本檔案介紹使用網路位址轉譯(NAT)的基本Cisco IOS®防火牆組態。 此配置允許流量從10.1.1.x和172.16.1.x網路內部發起到Internet並在途中進行NAT。通用路由封裝(GRE)通道新增到兩個私人網路之間的通道IP和IPX流量。當封包到達路由器的傳出介面時，如果透過通道傳送該封包，首先使用GRE進行封裝，然後使用IPsec進行加密。換句話說，任何允許進入GRE通道的流量也會被IPsec加密。

要使用開放最短路徑優先(OSPF)配置IPsec上的GRE隧道，請參閱使用OSPF配置IPSec上的GRE隧道。

要在三台路由器之間配置集中星型IPsec設計，請參閱配置IPsec路由器到路由器的集中星型與分支之間的通訊。

必要條件

需求

本文件沒有特定需求。

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12.2(21a)和12.3(5a)
- Cisco 3725和3640

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。

背景資訊

本節中的提示可幫助您實施配置：

- 在兩台路由器上實施NAT以測試Internet連線。
- 將GRE新增到配置和測試。非加密流量應在專用網路之間流動。
- 將IPsec新增到配置和測試。應加密專用網路之間的流量。
- 將Cisco IOS防火牆新增到外部介面、出站檢查清單和入站訪問清單，然後進行測試。
- 如果您使用低於12.1.4的Cisco IOS軟體版本，則需要允許存取清單103中172.16.1.x和 — 10.0.0.0之間的IP流量。如需詳細資訊，請參閱Cisco錯誤ID CSCdu58486(僅限註冊客戶)和Cisco錯誤ID CSCdm0118(僅限註冊客戶)。

設定

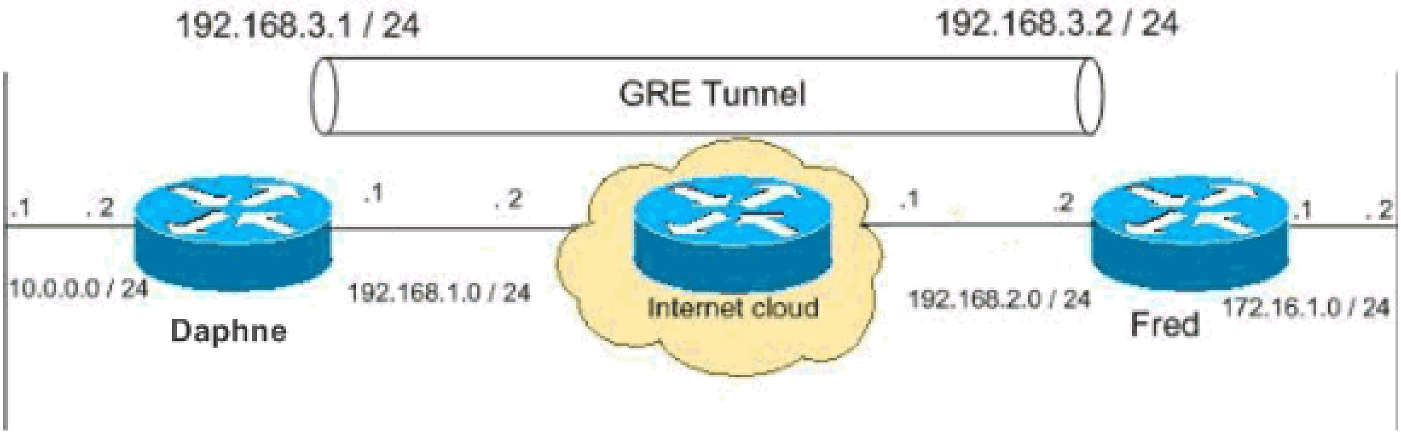
本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

附註： 此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

網路圖表

本檔案會使用此網路設定。



組態

本檔案會使用這些設定。

- Daphne組態
- 弗雷德配置

Daphne組態

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname daphne
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$r2sh$XKZR118vcId11ZGzhbz5C/
!
no aaa new-model
ip subnet-zero
!
!
!--- This is the Cisco IOS Firewall configuration and
what to inspect. !--- This is applied outbound on the
external interface. ip inspect name myfw tcp
ip inspect name myfw udp
ip inspect name myfw ftp
ip inspect name myfw realaudio
ip inspect name myfw smtp
ip inspect name myfw streamworks
ip inspect name myfw vdolive
ip inspect name myfw tftp
ip inspect name myfw rcmd
ip inspect name myfw http
ip telnet source-interface FastEthernet0/0
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!--- This is the IPsec configuration. ! crypto isakmp
policy 10
 authentication pre-share

crypto isakmp key ciscokey address 192.168.2.2
!
!
crypto ipsec transform-set to_fred esp-des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp

 set peer 192.168.2.2
 set transform-set to_fred
 match address 101
!
!
!
!
!
!--- This is one end of the GRE tunnel. ! interface
```

```
Tunnel0

ip address 192.168.3.1 255.255.255.0
!--- Associate the tunnel with the physical interface.
tunnel source FastEthernet0/1

tunnel destination 192.168.2.2

!--- This is the internal network. interface
FastEthernet0/0
ip address 10.0.0.2 255.255.255.0
 ip nat inside
 speed 100
 full-duplex
!
!--- This is the external interface and one end of the
GRE tunnel. interface FastEthernet0/1
ip address 192.168.1.1 255.255.255.0
 ip access-group 103 in
 ip nat outside
 ip inspect myfw out
 speed 100
 full-duplex
 crypto map myvpn
!
!--- Define the NAT pool.
ip nat pool ourpool 192.168.1.10 192.168.1.20 netmask
255.255.255.0
ip nat inside source route-map nonat pool ourpool
overload
ip classless

ip route 0.0.0.0 0.0.0.0 192.168.1.2

!--- Force the private network traffic into the tunnel.
- ip route 172.16.1.0 255.255.255.0 192.168.3.2 ip http
server no ip http secure-server ! ! !--- All traffic
that enters the GRE tunnel is encrypted by IPsec. !---
Other ACE statements are not necessary. access-list 101
permit gre host 192.168.1.1 host 192.168.2.2 !--- Access
list for security reasons. Allow !--- IPsec and GRE
traffic between the private networks.
access-list 103 permit gre host 192.168.2.2 host
192.168.1.1
access-list 103 permit esp host 192.168.2.2 host
192.168.1.1
access-list 103 permit udp host 192.168.2.2 eq isakmp
host 192.168.1.1
access-list 103 deny   ip any any log

!--- See the Background Information section if you use
!--- a Cisco IOS Software release earlier than 12.1.4
for access list 103. access-list 175 deny ip 10.0.0.0
0.0.0.255 172.16.1.0 0.0.0.255 access-list 175 permit ip
10.0.0.0 0.0.0.255 any !--- Use access list in route-map
to address what to NAT. route-map nonat permit 10
 match ip address 175
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
```

```
 password ww
 login
!
!
end
```

弗雷德配置

```

version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname fred
!
enable secret 5 $1$AtxD$MycLGaJvF/tAIFXkikCes1
!
ip subnet-zero
!
!
ip telnet source-interface FastEthernet0/0
!
ip inspect name myfw tcp
ip inspect name myfw udp
ip inspect name myfw ftp
ip inspect name myfw realaudio
ip inspect name myfw smtp
ip inspect name myfw streamworks
ip inspect name myfw vdolive
ip inspect name myfw tftp
ip inspect name myfw rcmd
ip inspect name myfw http
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
 authentication pre-share
-
crypto isakmp key ciscokey address 192.168.1.1
!
!
crypto ipsec transform-set to_daphne esp-des esp-md5-
hmac
!
crypto map myvpn 10 ipsec-isakmp

set peer 192.168.1.1
 set transform-set to_daphne
 match address 101
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface Tunnel0
 -
 ip address 192.168.3.2 255.255.255.0
 tunnel source FastEthernet0/1
```

```
-
tunnel destination 192.168.1.1
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 speed 100
 full-duplex
!
interface Serial0/0
 no ip address
 clockrate 2000000
!
interface FastEthernet0/1

 ip address 192.168.2.2 255.255.255.0
 ip access-group 103 in
 ip nat outside
 ip inspect myfw out
 speed 100
 full-duplex
 crypto map myvpn
!


!--- Output is supressed. !
ip nat pool ourpool 192.168.2.10 192.168.2.20 netmask
255.255.255.0
ip nat inside source route-map nonat pool ourpool
overload
ip classless

ip route 0.0.0.0 0.0.0.0 192.168.2.1
ip route 10.0.0.0 255.255.255.0 192.168.3.1
ip http server
!

access-list 101 permit gre host 192.168.2.2 host
192.168.1.1
access-list 103 permit gre host 192.168.1.1 host
192.168.2.2
access-list 103 permit udp host 192.168.1.1 eq isakmp
host 192.168.2.2
access-list 103 permit esp host 192.168.1.1 host
192.168.2.2
access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.0.0.0
0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 175
!
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
```

```
 password ww
 login
!
end
```

驗證

使用本節內容，確認您的組態是否正常運作。

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

嘗試從172.16.1.x網路中的主機ping遠端子網中的主機 — 10.0.0.x，以檢查VPN配置。此流量應通過GRE通道並進行加密。

使用**show crypto ipsec sa**命令驗證IPsec隧道是否已啟動。首先檢查SPI編號是否不同於0。您應該還會看到`pkts encrypt`和`pkts decrypt`計數器的增加。

- **show crypto ipsec sa** — 驗證IPsec隧道是否已啟動。
- **show access-lists 103** — 驗證Cisco IOS防火牆配置是否正常工作。
- **show ip nat translations** — 驗證NAT是否正常工作。

```
fred#show crypto ipsec sa

interface: FastEthernet0/1

Crypto map tag: myvpn, local addr. 192.168.2.2

   local  ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)
   current_peer: 192.168.1.1
     PERMIT, flags={transport_parent,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #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.: 192.168.2.2, remote crypto endpt.: 192.168.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:


   -
```

```
  local  ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
   current_peer: 192.168.1.1
     PERMIT, flags={origin_is_acl,parent_is_transport,}
    #pkts encaps: 42, #pkts encrypt: 42, #pkts digest 42
    #pkts decaps: 39, #pkts decrypt: 39, #pkts verify 39
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0


     local crypto endpt.: 192.168.2.2, remote crypto endpt.: 192.168.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 3C371F6D

     inbound esp sas:
      spi: 0xF06835A9(4033361321)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 940, flow_id: 1, crypto map: myvpn
        sa timing: remaining key lifetime (k/sec): (4607998/2559)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:


     outbound esp sas:
      spi: 0x3C371F6D(1010245485)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 941, flow_id: 2, crypto map: myvpn
        sa timing: remaining key lifetime (k/sec): (4607998/2559)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

若要確認Cisco IOS防火牆組態是否正常運作，請首先發出以下命令。

```
fred#show access-lists 103

Extended IP access list 103
    permit gre host 192.168.1.1 host 192.168.2.2 (4 matches)
    permit udp host 192.168.1.1 eq isakmp host 192.168.2.2 (4 matches)
    permit esp host 192.168.1.1 host 192.168.2.2 (4 matches)
```

然後，從172.16.1.x網路中的主機，嘗試Telnet至Internet上的遠端主機。您可以首先檢查NAT是否正常工作。本地地址172.16.1.2已轉換為192.168.2.10。

```
fred#show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
tcp 192.168.2.10:11006  172.16.1.2:11006   192.168.2.1:23     192.168.2.1:23
```

再次檢查存取清單時，可以看到已動態新增額外線路。

```
fred#show access-lists 103
Extended IP access list 103
    permit tcp host 192.168.2.1 eq telnet host 192.168.2.10 eq 11006 (11 matches)
    permit gre host 192.168.1.1 host 192.168.2.2 (4 matches)
    permit udp host 192.168.1.1 eq isakmp host 192.168.2.2 (4 matches)
    permit esp host 192.168.1.1 host 192.168.2.2 (4 matches)
```

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(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**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。

NAT:

- **debug ip nat** ***access-list number*** — 顯示由IP NAT功能轉換的IP資料包的相關資訊。

IPSec:

- **debug crypto ipsec** — 顯示IPsec事件。
- **debug crypto isakmp** — 顯示有關Internet金鑰交換(IKE)事件的消息。
- **debug crypto engine** — 顯示來自加密引擎的資訊。

CBAC:

- **debug ip inspect {*protocol* | detailed}** — 顯示有關Cisco IOS防火牆事件的消息。

存取清單：

- **debug ip packet(**在介面上沒有**ip route-cache)** — 顯示常規IP調試資訊和IP安全選項(IPSO)安全事務。

```
daphne#show version
Cisco Internetwork Operating System Software
IOS (tm) 3700 Software (C3725-ADVSECURITYK9-M), Version 12.3(5a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 24-Nov-03 20:36 by kellythw
Image text-base: 0x60008AF4, data-base: 0x613C6000

ROM: System Bootstrap, Version 12.2(8r)T2, RELEASE SOFTWARE (fc1)

daphne uptime is 6 days, 19 hours, 39 minutes
System returned to ROM by reload
System image file is "flash:c3725-advsecurityk9-mz.123-5a.bin"
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 3725 (R7000) processor (revision 0.1) with 196608K/65536K bytes of memory.
Processor board ID JHY0727K212
R7000 CPU at 240MHz, Implementation 39, Rev 3.3, 256KB L2 Cache
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
1 Virtual Private Network (VPN) Module(s)
DRAM configuration is 64 bits wide with parity disabled.
55K bytes of non-volatile configuration memory.
125952K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2002


fred#show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-JK9O3S-M), Version 12.2(21a), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 09-Jan-04 16:23 by kellmill
Image text-base: 0x60008930, data-base: 0x615DE000

ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

fred uptime is 6 days, 19 hours, 36 minutes
System returned to ROM by reload
System image file is "flash:c3640-jk9o3s-mz.122-21a.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 3640 (R4700) processor (revision 0x00) with 124928K/6144K bytes of memory.
Processor board ID 25120505
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
```

```
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
4 Serial(sync/async) network interface(s)
1 Virtual Private Network (VPN) Module(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2002
```

注意：如果按步驟實施此配置，則要使用的**debug命令取決於故障部件。**

相關資訊

- IPSec 協商/IKE 通訊協定
- 技術支援與文件 - Cisco Systems