使用IOS防火墙和NAT的GRE隧道上配置路由器到路由器的IPSec (预先共享密钥)

目录

简介

本文档说明了使用网络地址转换 (NAT) 的基本 Cisco IOS® 防火墙配置。此配置允许从 10.1.1.x 和 172.16.1.x 网络内部发起到 Internet 的流量，并在路径中对该流量执行 NAT 操作。添加的通用路由封装 (GRE) 隧道用于在两个专用网络之间通过隧道传输 IP 和 IPX 流量。当数据包到达路由器的出站接口并沿隧道发送时，将首先使用 GRE 封装该数据包，然后使用 IPsec 对该数据包进行加密。换句话说，还将使用 IPsec 对允许进入 GRE 隧道的所有流量进行加密。

要使用开放最短路径优先 (OSPF) 配置基于 IPsec 的 GRE 隧道，请参阅使用 OSPF 配置基于 IPSec 的 GRE 隧道。

要在三个路由器之间配置星型 IPSec 设计，请参阅配置 IPSec 路由器到路由器星型结构的分支之间的通信。

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 12.2(21a) 和 12.3(5a)
- Cisco 3725 和 3640

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。

背景信息

此部分中的提示有助于您实现以下配置：

- 在两个路由器上实现 NAT 以测试 Internet 连接。
- 向配置添加 GRE 并进行测试。应在专用网络之间传输未加密的流量。
- 向配置添加 IPsec 并进行测试。应对专用网络之间的流量进行加密。
- 向外部接口、出站检查列表和入站访问列表添加 Cisco IOS 防火墙，并进行测试。
- 如果使用 Cisco IOS 软件版本 12.1.4 之前的版本，则需要在访问列表 103 中允许 172.16.1.x 和 - 10.0.0.0 之间的 IP 流量。有关详细信息，请参阅 Cisco Bug ID CSCdu58486（仅限注册用户）和 Cisco Bug ID CSCdm01118（仅限注册用户）。

配置

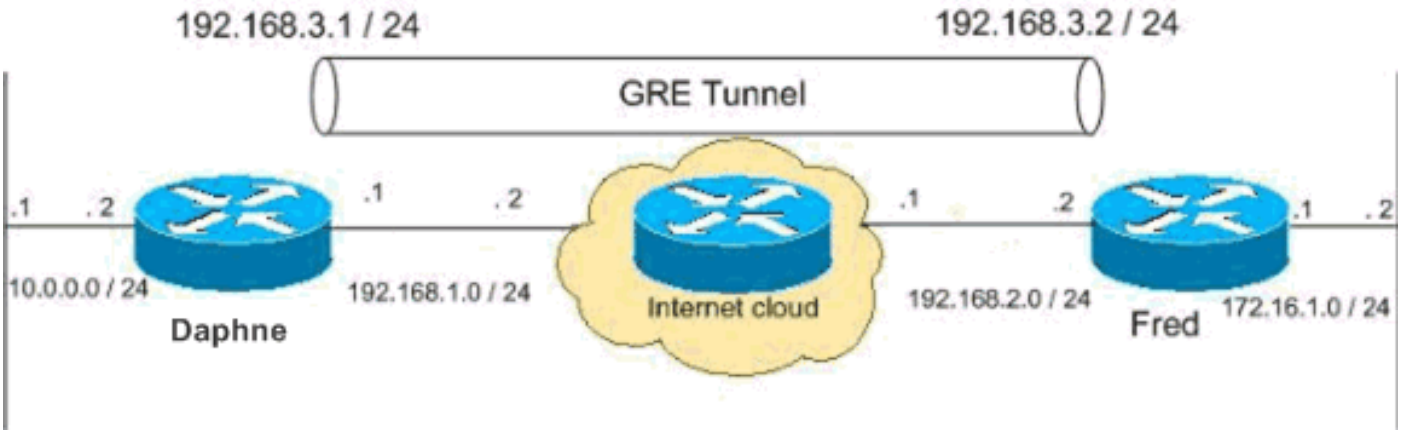
本部分提供有关如何配置本文档所述功能的信息。

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）。

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

网络图

本文档使用此网络设置。



配置

本文档使用以下配置。

- Daphne 配置
- Fred 配置

Daphne 配置

```
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
```

Fred 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
```

验证

使用本部分可确认配置能否正常运行。

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。

尝试从 172.16.1.x 网络中的主机对远程子网 10.0.0..x 中的主机执行 ping，以便检查 VPN 配置。此流量应经 GRE 隧道通过，并进行加密。

使用 **show crypto ipsec sa** 命令验证 IPSec 隧道是否已开启。首先，请检查 SPI 编号不为 0。此外，还应看到 pkts encrypt 和 pkts decrypt 计数器的值增加了。

- **show crypto ipsec sa** - 验证 IPSec 隧道是否已开启。
- **show access-lists 103** - 验证 Cisco IOS 防火墙配置是否工作正常。
- **show ip nat translations** - 验证 NAT 是否工作正常。

```
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:
```

要验证 Cisco IOS 防火墙配置是否工作正常，请首先发出以下命令。

```
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)
```

然后，尝试从 172.16.1.x 网络中的主机使用 Telnet 登录到 Internet 中的远程主机。您可以首先检查 NAT 是否运行正常。172.16.1.2 的本地地址已转换为 192.168.2.10。

```
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)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
```

当再次检查访问列表时，您将看到已动态添加额外的一行。

```
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)
```

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。

NAT:

- **debug ip nat access-list number** - 显示有关 IP NAT 功能转换的 IP 数据包的信息。

IPSec ：

- **debug crypto ipsec** — 显示 IPSec 事件。
- **debug crypto isakmp** — 显示有关 Internet 密钥交换 (IKE) 事件的消息。
- **debug crypto engine** - 显示来自加密引擎的信息。

CBAC ：

- **debug ip inspect {protocol|detailed}** - 显示有关 Cisco IOS 防火墙事件的消息。

访问列表：

- **debug ip packet**（在接口上未启用 ip 路由缓存）- 显示一般 IP 调试信息和 IP 安全选项 (IPSO) 安全事务。

```
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： 如果分步实现此配置，所使用的 **debug** 命令取决于发生故障的部件。

相关信息

- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems