IOS 방화벽 및 NAT를 사용하여 GRE 터널에서 라우터 간 IPsec(사전 공유 키) 구성

목차

소개

이 문서에서는 NAT(Network Address Translation)를 사용하는 기본 Cisco IOS® 방화벽 컨피그레이션을 설명합니다. 이 컨피그레이션을 사용하면 10.1.1.x 및 172.16.1.x 네트워크 내에서 인터넷 및 NAT로 트래픽을 시작할 수 있습니다.일반 GRE(Routing Encapsulation) 터널이 두 프라이빗 네트워크 간의 터널 IP 및 IPX 트래픽에 추가됩니다.패킷이 라우터의 아웃바운드 인터페이스에 도착하고 터널에서 전송되면 먼저 GRE를 사용하여 캡슐화된 다음 IPsec으로 암호화됩니다.즉, GRE 터널에 들어갈 수 있는 모든 트래픽도 IPsec에 의해 암호화됩니다.

OSPF(Open Shortest Path First)를 사용하여 IPsec을 통한 GRE 터널을 구성하려면 OSPF를 사용하여 IPSec을 통한 GRE 터널 구성을 참조하십시오.

세 라우터 간에 허브 및 스포크 IPsec 설계를 구성하려면 스포크 간 통신으로 IPsec 라우터 간 허브 및 스포크 구성을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.2(21a) 및 12.3(5a)
- Cisco 3725 및 3640

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

이 섹션의 팁은 구성을 구현하는 데 도움이 됩니다.

- 두 라우터에 NAT를 구현하여 인터넷 연결을 테스트합니다.
- 컨피그레이션 및 테스트에 GRE를 추가합니다.암호화되지 않은 트래픽은 프라이빗 네트워크 간에 전달되어야 합니다.
- 구성에 IPsec을 추가하고 테스트합니다.프라이빗 네트워크 간의 트래픽은 암호화되어야 합니다.
- 외부 인터페이스, 아웃바운드 검사 목록 및 인바운드 액세스 목록에 Cisco IOS 방화벽을 추가하고 테스트합니다.
- 12.1.4 이전 버전의 Cisco IOS Software 릴리스를 사용하는 경우 액세스 목록 103에서 172.16.1.x에서 -10.0.0.0 사이의 IP 트래픽을 허용해야 합니다. 자세한 내용은 Cisco 버그 ID CSCdu58486(등록된 고객만 해당) 및 Cisco 버그 ID CSC11118(등록된 고객만)을 참조하십시오.

구성

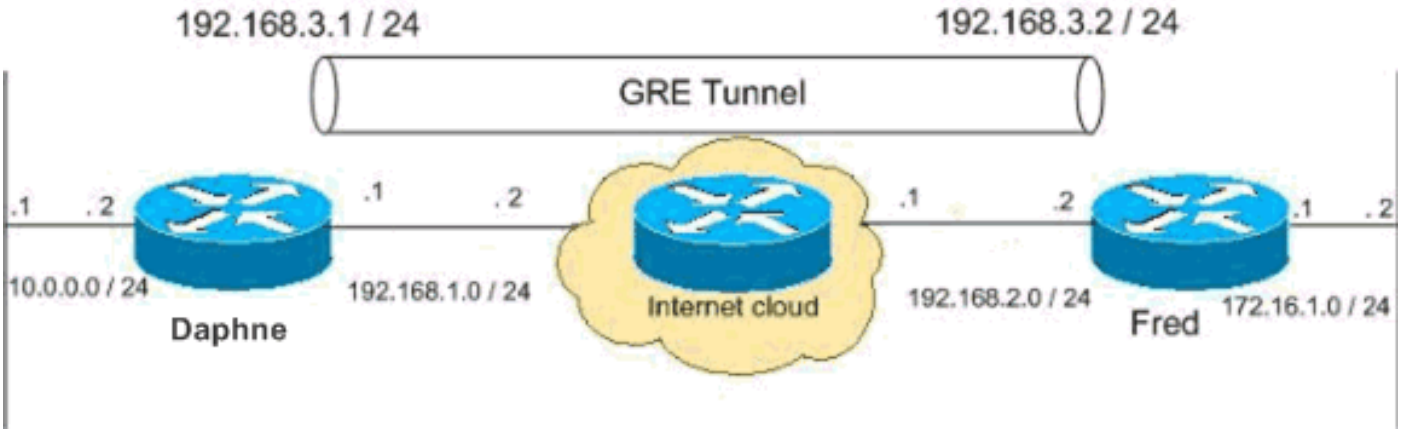
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

참고: 이 컨피그레이션에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



구성

이 문서에서는 이러한 구성을 사용합니다.

- 다프네 컨피그레이션
- Fred 구성

다프네 컨피그레이션

```
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 구성

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

VPN 컨피그레이션을 확인하려면 172.16.1.x 네트워크의 호스트에서 원격 서브넷 10.0.0..x의 호스트를 ping해 보십시오.이 트래픽은 GRE 터널을 통과하고 암호화되어야 합니다.

show crypto ipsec **sa** 명령을 사용하여 IPsec 터널이 작동 중인지 확인합니다.먼저 SPI 번호가 0과 다른지 확인합니다. pkts `encrypt` 및 pkts `decrypt` 카운터 증가해야 합니다.

- **show crypto ipsec sa** - IPsec 터널이 작동 중인지 확인합니다.
- **show access-lists 103** - Cisco IOS Firewall 컨피그레이션이 올바르게 작동하는지 확인합니다.
- **show ip nat translations** - NAT가 제대로 작동하는지 확인합니다.

```
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:
```

Cisco IOS Firewall 컨피그레이션이 제대로 작동하는지 확인하려면 먼저 이 명령을 실행합니다.

```
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)
```

그런 다음 172.16.1.x 네트워크의 호스트에서 인터넷의 원격 호스트에 텔넷으로 연결합니다.먼저 NAT가 제대로 작동하는지 확인할 수 있습니다.172.16.1.2의 로컬 주소가 192.168.2.10으로 변환되었습니다.

```
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
```

access-list를 다시 선택하면 추가 행이 동적으로 추가됨을 알 수 있습니다.

```
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)
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

NAT:

- **debug ip nat** ***access-list number***—IP NAT 기능으로 변환된 IP 패킷에 대한 정보를 표시합니다.

IPSec:

- **debug crypto ipsec** - IPsec 이벤트를 표시합니다.
- **debug crypto isakmp** - IKE(Internet Key Exchange) 이벤트에 대한 메시지를 표시합니다.
- **debug crypto engine** - 암호화 엔진의 정보를 표시합니다.

CBAC:

- **디버그 ip 검사 {***protocol* **| detailed}** - Cisco IOS Firewall 이벤트에 대한 메시지를 표시합니다.

액세스 목록:

- **debug ip packet** (**no ip route-cache** on the interface) - 일반 IP 디버깅 정보 및 IP 보안 옵션 (IPSO) 보안 트랜잭션을 표시합니다.

```
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
```

참고: 이 컨피그레이션이 단계에서 구현된 경우 사용할 debug 명령은 결함이 있는 부품에 따라 달라집니다.

관련 정보

- IPsec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems