Het configureren van router-to-Router IPsec (pre-gedeelde sleutels) op GRE-tunnels met IOS-firewall en NAT

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Conventies
Achtergrondinformatie
Configureren
Netwerkdiagram
Configuraties
Verifiëren
Problemen oplossen
Opdrachten voor troubleshooting
Gerelateerde informatie

Inleiding

Dit document illustreert een basisconfiguratie van Cisco IOS® Firewall met netwerkadresomzetting (NAT). Deze configuratie maakt het mogelijk dat verkeer gestart wordt vanuit de 10.1.1.x- en 172.16.1.x-netwerken naar internet en NATed onderweg. Een generieke Routing Encapsulation (GRE)-tunnel wordt toegevoegd aan tunnelIP en IPX-verkeer tussen twee particuliere netwerken. Wanneer een pakket op de uitgaande interface van de router aankomt en als het door de tunnel wordt verstuurd, wordt het eerst ingekapseld met GRE en dan versleuteld met IPsec. Met andere woorden: elk verkeer dat de GRE-tunnel mag betreden, wordt ook versleuteld door IPsec.

Om de GRE Tunnel via IPsec te configureren met Open Shortest Path First (OSPF), raadpleegt u een GRE-Tunnel via IPSec configureren met OSPF.

Om een hub te configureren en een IPsec-ontwerp tussen drie routers te bespreken, raadpleegt u het configureren van IPsec router-to-router hub en het oproepen met communicatie tussen de Spoelen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-softwarerelease 12.2(21a) en 12.3(5a)
- Cisco 3725 en 3640 switch

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Met de tips in deze sectie kunt u de configuratie implementeren:

- Voer NAT op beide routers in om de internetconnectiviteit te testen.
- Voeg GRE aan de configuratie en de test toe. Niet-versleuteld verkeer moet tussen de particuliere netwerken lopen.
- Voeg IPsec toe aan de configuratie en test. Het verkeer tussen de particuliere netwerken moet worden versleuteld.
- Voeg de Cisco IOS Firewall aan de externe interfaces toe, de lijst van de inspectie van de uitgang en de inkomende toegangslijst, en test.
- Als u een Cisco IOS-softwarerelease eerder dan 12.1.4 gebruikt, moet u IP-verkeer tussen 172.16.1.x en - 10.0.0 toestaan in toegangslijst 103. Raadpleeg Cisco bug ID CSCdu58486 (alleen geregistreerde klanten) en Cisco ID Cdm01118 (alleen geregistreerde klanten) voor meer informatie.

Configureren

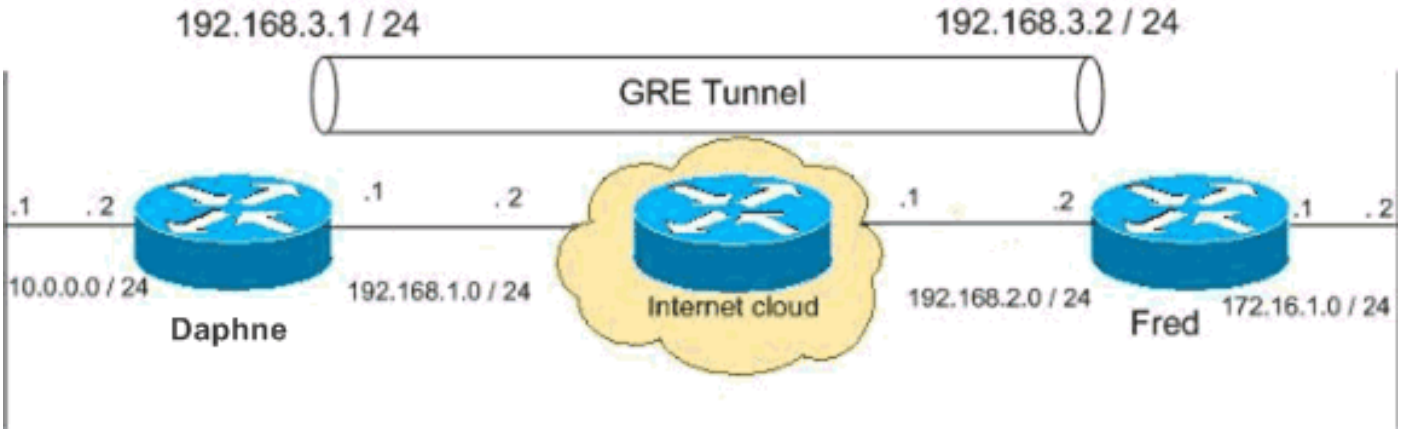
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Opmerking: De IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Netwerkdiagram

Dit document maakt gebruik van deze netwerkinstellingen.



Configuraties

Dit document gebruikt deze configuraties.

- Daphne-configuratie
- Fred Configuration

Daphne-configuratie

```
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 Configuration

```
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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Probeer een host in het afstandsnetwerk te pingelen - 10.0.0.x van een host in het 172.16.1.x-netwerk om de VPN-configuratie te controleren. Dit verkeer moet door de GRE-tunnel gaan en versleuteld worden.

Gebruik de opdracht **show crypto ipsec als** om te controleren of de IPsec-tunnel is geopend. Controleer eerst dat de SPI-getallen anders zijn dan 0. U dient ook een toename te zien in de `pkts-encryptie` en de `pkts-decrypt` tellers.

- **toon crypto ipsec sa**-Verifieert dat de IPsec-tunnel omhoog is.
- **tonen toegang-lijsten 103** - verifieert dat de configuratie van de Firewall van Cisco IOS correct werkt.
- **ip nat vertalingen tonen**—Controleer of NAT correct werkt.

```
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:
```

Om te verifiëren dat de configuratie van de Firewall van Cisco IOS correct werkt, geef deze opdracht eerst uit.

```
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)
```

Vanaf een host in het 172.16.1.x-netwerk probeert u vervolgens te tellen naar een externe host op het internet. U kunt eerst controleren of NAT correct werkt. Het plaatselijke adres van 172.16.1.2 is vertaald naar 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
```

Wanneer u de toegangslijst opnieuw controleert, ziet u dat een extra lijn dynamisch wordt toegevoegd.

```
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)
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

NAT:

- **debug ip** *toegangsnummer*-informatie over IP-pakketten die door de IP NAT-functie zijn vertaald.

IPsec:

- **debug van crypto ipsec**-displays IPsec gebeurtenissen.

- **debug crypto isakmp**-displays over de gebeurtenissen op de Internet Key Exchange (IKE).
- **debug van crypto motor**—informatie van de crypto motor.

CBAC:

- **IP-inspectie reinigen {*protocol* |** Gedetailleerde —displays over Cisco IOS Firewall gebeurtenissen.

Toegangslijsten:

- **debug ip pakket** (zonder **ip route-cache** op de interface)-Hiermee geeft u algemene IP-zuiveringsinformatie en IP-beveiligingsopties (IPSO) op.

```
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
```

Opmerking: Als deze configuratie in stappen is geïmplementeerd, is de **debug** opdracht om te gebruiken afhankelijk van het defecte onderdeel.

Gerelateerde informatie

- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems