Configuring Router−to−Router IPsec (Pre−shared Keys) on GRE Tunnel with IOS Firewall and NAT

Document ID: 9221

Contents

Introduction

This document illustrates a basic Cisco IOS® Firewall configuration with Network Address Translation (NAT). This configuration allows traffic to be initiated from inside the 10.1.1.x and 172.16.1.x networks to the Internet and NATed along the way. A generic routing encapsulation (GRE) tunnel is added to tunnel IP and IPX traffic between two private networks. When a packet arrives at the outbound interface of the router and if it is sent down the tunnel, it is first encapsulated using GRE and then encrypted with IPsec. In other words, any traffic permitted to enter the GRE tunnel is also encrypted by IPsec.

In order to configure the GRE Tunnel over IPsec with Open Shortest Path First (OSPF), refer to Configuring a GRE Tunnel over IPSec with OSPF.

In order to configure a hub and spoke IPsec design between three routers, refer to Configuring IPsec Router−to−Router Hub and Spoke with Communication Between the Spokes.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 12.2(21a) and 12.3(5a)
- Cisco 3725 and 3640

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The tips in this section help you to implement the configuration:

- Implement NAT on both routers to test the Internet connectivity.
- Add GRE to the configuration and test. Non−encrypted traffic should flow between the private networks.
- Add IPsec to the configuration and test. The traffic between the private networks should be encrypted.
- Add the Cisco IOS Firewall to the external interfaces, the outbound inspect list and inbound access list, and test.
- If you use a Cisco IOS Software release earlier than 12.1.4, you need to permit IP traffic between 172.16.1.x and − 10.0.0.0 in access list 103. Refer to Cisco bug ID CSCdu58486 (registered customers only) and Cisco bug ID CSCdm01118 (registered customers only) for more information.

Configure

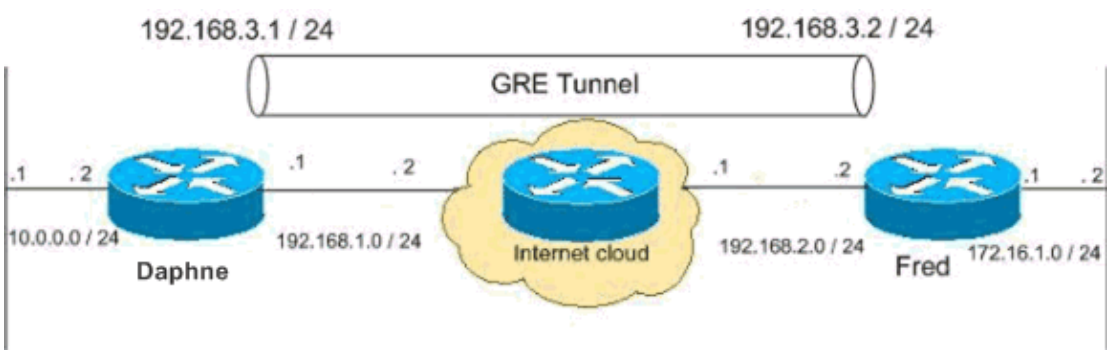
In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Network Diagram

This document uses this network setup.



Configurations

This document uses these configurations.

- Daphne Configuration
- Fred Configuration

Daphne Configuration

```
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
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Try to ping a host in the remote subnet − 10.0.0..x from a host in the 172.16.1.x network in order to check the VPN configuration. This traffic should go through the GRE tunnel and be encrypted.

Use the **show crypto ipsec sa** command to verify that the IPsec tunnel is up. First check that the SPI numbers are different than 0. You should also see an increase in the `pkts encrypt` and `pkts decrypt` counters.

- **show crypto ipsec sa** Verifies that the IPsec tunnel is up.
- **show access−lists 103** Verifies that the Cisco IOS Firewall configuration works correctly.
- **show ip nat translations** Verifies that NAT works properly.

```
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:
```

In order to verify that the Cisco IOS Firewall configuration works correctly, first issue this command.

```
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)
```

Then from a host in the 172.16.1.x network, try to Telnet to a remote host on the Internet. You can first check that NAT works properly. The local address of 172.16.1.2 has been translated to 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
```

When you check the access−list again, you see that an extra line is dynamically added.

```
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)
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

NAT:

- **debug ip nat** *access−list number* Displays information about IP packets translated by the IP NAT feature.

IPSec:

- **debug crypto ipsec** Displays IPsec events.
- **debug crypto isakmp** Displays messages about Internet Key Exchange (IKE) events.
- **debug crypto engine** Displays information from the crypto engine.

CBAC:

- **debug ip inspect {***protocol* **| detailed}** Displays messages about Cisco IOS Firewall events.

Access Lists:

- **debug ip packet** (with **no ip route−cache** on the interface) Displays general IP debugging information and IP security option (IPSO) security transactions.

```
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
```

Note: If this configuration is implemented in steps, the **debug** command to use depends on the failing part.

Related Information

- **IPsec Negotiation/IKE Protocols**
- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 06, 2007 Document ID: 9221