

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

このドキュメントでは、Network Address Translation (NAT; ネットワーク アドレス変換) を使用する基本的な Cisco IOS® ファイアウォールの設定について説明します。この設定では、10.1.1.x および 172.16.1.x のネットワーク内部からインターネットへのトラフィックが開始され、その後は NAT 処理されるようにします。この 2 つのプライベート ネットワーク間にあるトンネル IP と IPX トラフィックには、Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) トンネルが追加されます。パケットがルータの発信インターフェイスに到着するときに、そのパケットがトンネル経由で送信された場合には、まず GRE を使用してカプセル化され、その後 IPsec を使用して暗号化されます。つまり、GRE トンネルに入ることが許可されたトラフィックであれば、同時に IPsec により暗号化されることとなります。

Open Shortest Path First (OSPF) を使用した IPsec 環境での GRE トンネルを設定するには、『[OSPF を使用した IPsec 環境での GRE トンネルの設定](#)』を参照してください。

3 つのルータ間にハブ アンド スポーク IPsec 設計を設定するには、『[スポーク間の通信における IPsec ルータ間ハブ アンド スポークの設定](#)』を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 12.2(21a) および 12.3(5a)

- Cisco 3725 および 3640

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

このセクションで説明するヒントには、実際の設定に役立つ情報が含まれています。

- 両方のルータに NAT を実装し、インターネットとの接続をテストします。
- 設定に GRE を追加してテストします。これらのプライベート ネットワーク間に暗号化されていないトラフィックを流します。
- 設定に IPsec を追加してテストします。プライベート ネットワーク間には暗号化されていないトラフィックを流します。
- 外部インターフェイス、発信検査リスト、および着信アクセス リストに、Cisco IOS ファイアウォールを追加し、テストします。
- 12.1.4 より前のバージョンの Cisco IOS を使用している場合には、アクセス リスト 103 で 172.16.1.x と - 10.0.0.0 の間の IP トラフィックを許可する必要があります。詳細については、Cisco Bug ID [CSCdu58486](#) ([登録ユーザ専用](#)) および Cisco Bug ID [CSCdm01118](#) ([登録ユーザ専用](#)) を参照して下さい。

設定

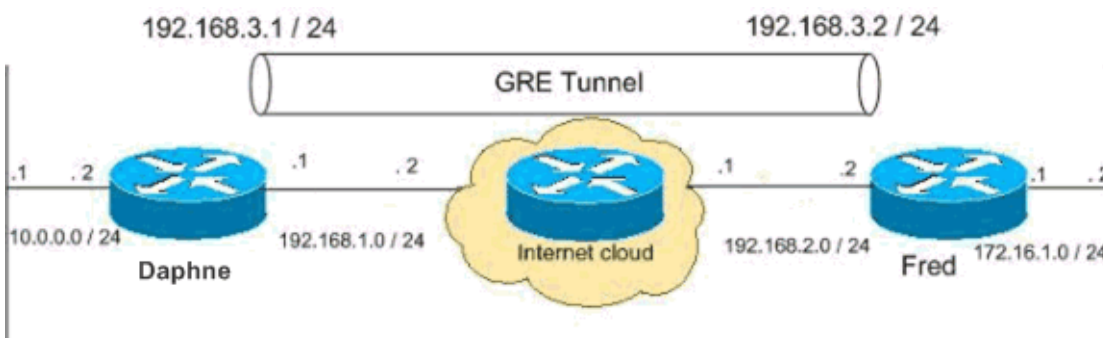
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

注 この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。これらはラボ環境で使用された RFC 1918 でのアドレスです。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の設定を使用します。

- [Daphne の設定](#)
- [Fred の設定](#)

Daphne の設定

```
version 12.3
service timestamps debug datetime
service timestamps log datetime msec
no service password-encryption
hostname daphne
boot-start-marker
boot-end-marker
enable secret 5
$1$r2sh$XKZR118vcId11ZGzhhbz5C/!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 streamwork
ip inspect name myfw vdo
ip inspect name myfw tftp
ip inspect name myfw rcmd
ip inspect name myfw http
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
0line aux 0line vty 0 4 password ww login!!end
```

Fred の設定

```
version 12.2service 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
tcpip inspect name myfw udpip inspect name myfw ftpip
inspect name myfw realaudiopip inspect name myfw smtpip
inspect name myfw streamworksip inspect name myfw
vdoliveip inspect name myfw tftpip inspect name myfw
rcmdip inspect name myfw httpip audit notify logip 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 suppressed.!ip nat pool ourpool
192.168.2.10 192.168.2.20 netmask 255.255.255.0ip nat
inside source route-map nonat pool ourpool overloadip
classlessip route 0.0.0.0 0.0.0.0 192.168.2.1ip route
10.0.0.0 255.255.255.0 192.168.3.1ip http server!access-
list 101 permit gre host 192.168.2.2 host
192.168.1.1access-list 103 permit gre host 192.168.1.1
host 192.168.2.2access-list 103 permit udp host
192.168.1.1 eq isakmp host 192.168.2.2access-list 103
permit esp host 192.168.1.1 host 192.168.2.2access-list
175 deny ip 172.16.1.0 0.0.0.255 10.0.0.0
0.0.0.255access-list 175 permit ip 172.16.1.0 0.0.0.255
anyroute-map nonat permit 10 match ip address
175!!!dial-peer cor custom!!!!line con 0 exec-timeout 0
0line aux 0line vty 0 4 password ww login!end
```

確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の show コマンドがサポートされています。OIT を使用して、show コマンド出力の解析を表示できます。

ネットワーク 172.16.1.x のホストから、リモートのサブネット - 10.0.0.x のホストに ping を送信して、VPN 設定をチェックします。このトラフィックは GRE トンネルに流して、暗号化される必要があります。

show crypto ipsec sa コマンドを使用して、IPsec トンネルがアップ状態であることを確認します。まず、SPI 番号が 0 以外になっているかどうかをチェックします。また、pkts encrypt および pkts decrypt のカウンタが増加していることを確認する必要があります。

- **show crypto ipsec sa** が。IPSecトンネルが稼働していることを確認します。
- Cisco IOS ファイアウォール 設定が正しく機能する **show access-lists 103?Verifies**。
- **show ip nat translations** が。NAT がきちんとはたらくことを確認します。

```
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 ファイアウォールの設定が正しく機能していることを確認するには、まずこのコマンドを発行します。

```
fred#show access-lists 103Extended 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)
```

次に、ネットワーク 172.16.1.x のホストから、Telnet でインターネット上のリモート ホストに接続してみます。最初に、NAT が適切に動作していることをチェックできます。ローカル アドレス 172.16.1.2 は 192.168.2.10 に変換されています。

```
fred#show access-lists 103Extended 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 globaltcp 192.168.2.10:11006
172.16.1.2:11006 192.168.2.1:23 192.168.2.1:23
```

再びアクセス リストをチェックするときには、動的に新しい行が追加されていることがわかります。

```
fred#show access-lists 103Extended 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)
```

[トラブルシューティング](#)

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

[トラブルシューティングのためのコマンド](#)

[Output Interpreter Tool](#) (OIT) ([登録](#)ユーザ専用) では、特定の **show** コマンドがサポートされ

ています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注 [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

NAT :

- **debug ip nat access-list number** か。IP ネットワークアドレス交換 機能によって変換される IP パケットについての情報を表示する。

IPsec :

- **debug crypto ipsec** か。IPSec イベントを表示する。
- **debug crypto isakmp** か。インターネット キー エクスチェンジ (IKE) イベントについてのメッセージを表示する。
- **debug crypto engine** か。暗号化エンジンからの情報を表示する。

CBAC :

- **debug ip inspect {protocol | 詳しい}** か。Cisco IOS ファイアウォール イベントについてのメッセージを表示する。

アクセス リスト :

- **debug ip packet (インターフェイスの IP ルート キャッシュ無しで)** か。一般的な IP デバッグ情報および IP Security Option (IPSO) セキュリティ トランザクションを表示する。

```
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 kellythwImage text-base: 0x60008AF4, data-base: 0x613C6000ROM: System Bootstrap, Version 12.2(8r)T2, RELEASE SOFTWARE (fc1)daphne uptime is 6 days, 19 hours, 39 minutesSystem returned to ROM by reloadSystem 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 JHY0727K212R7000 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 0x2002fred#show version
Cisco Internetwork Operating System Software IOS (tm) 3600 Software (C3640-JK903S-M), Version 12.2(21a), RELEASE SOFTWARE (fc2)Copyright (c) 1986-2004 by cisco Systems, Inc.Compiled Fri 09-Jan-04 16:23 by kellmillImage text-base: 0x60008930, data-base: 0x615DE000ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)fred uptime is 6 days, 19 hours, 36 minutesSystem returned to ROM by reloadSystem 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 toexport@cisco.com. cisco 3640 (R4700) processor (revision 0x00) with 124928K/6144K bytes of memory. Processor board ID 25120505R4700 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

注この設定がステップごとに実装された場合、使用する debug コマンドは障害が発生した箇所によって異なります。

関連情報

- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)