Configuration d'IPSec de routeur à routeur (clés pré-partagées) sur un tunnel GRE avec pare-feu IOS Firewall et NAT

Contenu

Introduction

Ce document montre une configuration de pare-feu Cisco IOS® de base avec la traduction d'adresses réseau (NAT). Cette configuration permet au trafic d'être lancé de l'intérieur des réseaux 10.1.1.x et 172.16.1.x vers Internet et que ses adresses réseau soient traduites le long de la route. Un tunnel d'encapsulation de routage générique (GRE) est ajouté pour transmettre le trafic IP et IPX entre deux réseaux privés. Quand un paquet arrive à l'interface de sortie du routeur et s'il est envoyé vers le tunnel, il est d'abord encapsulé à l'aide de GRE et ensuite chiffré avec IPsec. En d'autres termes, n'importe quel trafic autorisé à entrer dans le tunnel GRE est également chiffré par IPsec.

Afin de configurer le tunnel GRE sur IPsec avec Open Shortest Path First (OSPF), consultez Configuration d'un tunnel GRE sur IPSec avec OSPF.

Afin de configurer une conception IPsec Hub and Spoke entre trois routeurs, consultez Configuration de la technologie Hub and Spoke IPSec de routeur à routeur avec communication entre rayons.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS versions 12.2(21a) et 12.3(5a)
- Cisco 3725 et 3640

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Les conseils dans cette section vous aident à implémenter la configuration :

- Implémentez NAT sur les deux routeurs pour tester la connectivité Internet.
- Ajoutez GRE à la configuration et testez. Le trafic non chiffré devrait circuler entre les réseaux privés.
- Ajoutez IPsec à la configuration et testez. Le trafic entre les réseaux privés devrait être chiffré.
- Ajoutez le pare-feu Cisco IOS aux interfaces externes, la liste d'inspection sortante et la liste d'accès entrante, et testez.
- Si vous utilisez une version du logiciel Cisco IOS antérieure à 12.1.4, vous devez permettre le trafic IP entre 172.16.1.x et - 10.0.0.0 dans la liste d'accès 103. Consultez l'ID de bogue Cisco CSCdu58486 (clients enregistrés seulement) et l'ID de bogue Cisco CSCdm01118 (clients enregistrés seulement) pour plus d'informations.

Configurez

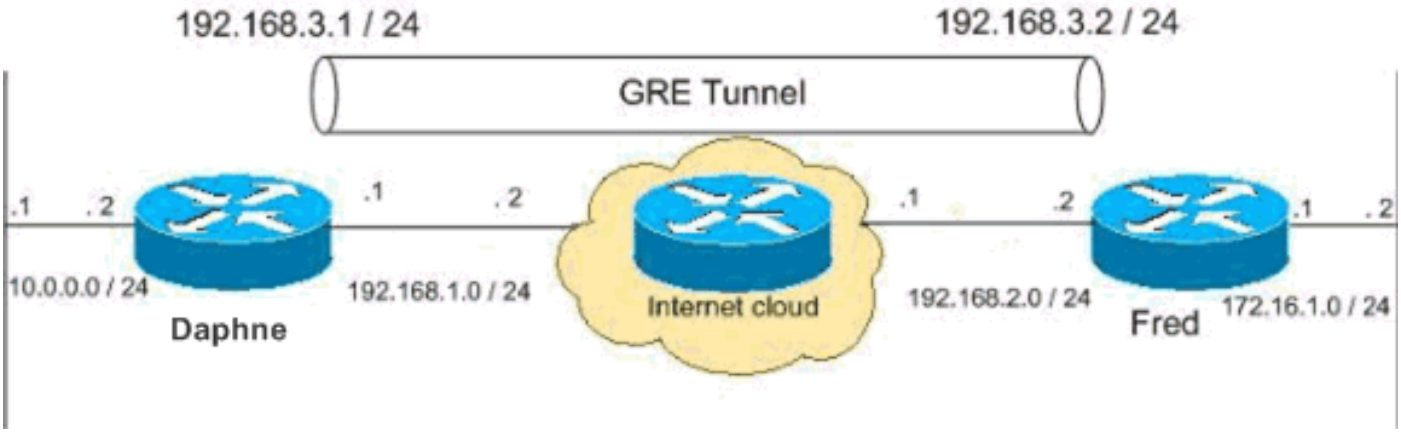
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Diagramme du réseau

Ce document utilise cette configuration du réseau.



Configurations

Ce document utilise les configurations suivantes.

- Configuration de Daphne
- Configuration de Fred

Configuration de Daphne

```
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
```

Configuration de Fred

```
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
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Essayez d'exécuter une commande ping sur un hôte dans le sous-réseau distant - 10.0.0..x à partir d'un hôte dans le réseau 172.16.1.x afin de vérifier la configuration VPN. Ce trafic devrait passer par le tunnel GRE et être chiffré.

Utilisez la commande **show crypto ipsec sa** pour vérifier que le tunnel IPsec est actif. Contrôlez d'abord que les numéros SPI sont différents de 0. Vous devriez également voir une augmentation des compteurs pkts encrypt et pkts decrypt.

- **show crypto ipsec sa** — Vérifie que le tunnel IPsec est actif.
- **show access-lists 103** — Vérifie que la configuration de pare-feu Cisco IOS fonctionne correctement.
- **show ip nat translations** — Vérifie que NAT fonctionne correctement.

```
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:
```

Afin de vérifier que la configuration de pare-feu Cisco IOS fonctionne correctement, émettez d'abord cette commande.

```
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)
```

Ensuite, à partir d'un hôte dans le réseau 172.16.1.x, essayez d'utiliser Telnet sur un hôte distant sur Internet. Vous pouvez d'abord vérifier que NAT fonctionne correctement. L'adresse locale 172.16.1.2 a été traduite en 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
```

Quand vous vérifiez de nouveau l'élément access-list, vous voyez qu'une ligne supplémentaire est dynamiquement ajoutée.

```
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)
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

NAT :

- **debug ip nat access-list number** — Affiche des informations sur les paquets IP traduits par la fonctionnalité IP NAT.

IPSec :

- **debug crypto ipsec** : affiche des événements IPsec.
- **debug crypto isakmp** — Affiche des messages sur des événements d'Échange de clés Internet (IKE).
- **debug crypto engine** — Affiche des informations du moteur de chiffrement.

CBAC :

- **debug ip inspect {protocol | detailed}** — Affiche des messages sur des événements de pare-feu Cisco IOS.

Listes d'accès :

- **debug ip packet** (sans **ip route-cache** sur l'interface) — Affiche des informations de débogage IP générales et les transactions de sécurité IPSO (IP Security Option).

```
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
```

Remarque: Si cette configuration est mise en application par étapes, la commande **debug** à utiliser dépend de la partie défaillante.

Informations connexes

- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems