

OSPF を使用した GRE トンネル over IPsec の設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[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

通常の IP Security (IPsec) の設定では、Enhanced Interior Gateway Routing Protocol (EIGRP) や Open Shortest Path First (OSPF) などのルーティング プロトコル、Internetwork Packet Exchange (IPX) や AppleTalk などの非 IP 系のトラフィックを送信することはできません。このドキュメントでは、ルーティング プロトコルおよび非 IP 系のトラフィックを使用するさまざまなネットワーク間で、IPsec を使用してルーティングを行う方法について説明します。この例では、さまざまなネットワーク間のルーティングを行うために、総称ルーティング カプセル化 (GRE) を使用します。

Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.x または Cisco 適応型セキュリティ アプライアンス (ASA) で、Open Shortest Path First (OSPF) を使用して GRE トンネルのない VPN/IPsec を設定する方法の詳細については、[PIX/ASA 7.x 以降：OSPF を使用した VPN/IPsec の設定例](#) (英語) を参照してください。

3 台のルータ間にハブ アンド スポーク IPsec 設計を設定する方法については、[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](#) (英語) を参照してください。

ネットワーク アドレス変換 (NAT) を使用して GRE トンネル上に基本的な Cisco IOS[®] ファイアウォールを設定する方法については、[IOS ファイアウォールと NAT を使用した GRE トンネル上のルータ間 IPsec \(事前共有鍵 \) の設定](#) (英語) を参照してください。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- 暗号マップを適用する前に、トンネルが機能していることを確認します。
- 可能な最大伝送ユニット (MTU) の問題の詳細については、[Windows および Sun のシステムでの IP MTU、TCP MSS、および PMTUD の調整](#) (英語) を参照してください。

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 12.4(8) が稼働している Cisco 3600
- Cisco IOS ソフトウェア リリース 12.4(8) が稼働している Cisco 2600
- PIX Firewall (Lion) ソフトウェア リリース 6.3(5)
- PIX Firewall (Tiger) ソフトウェア リリース 6.3(5)

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。

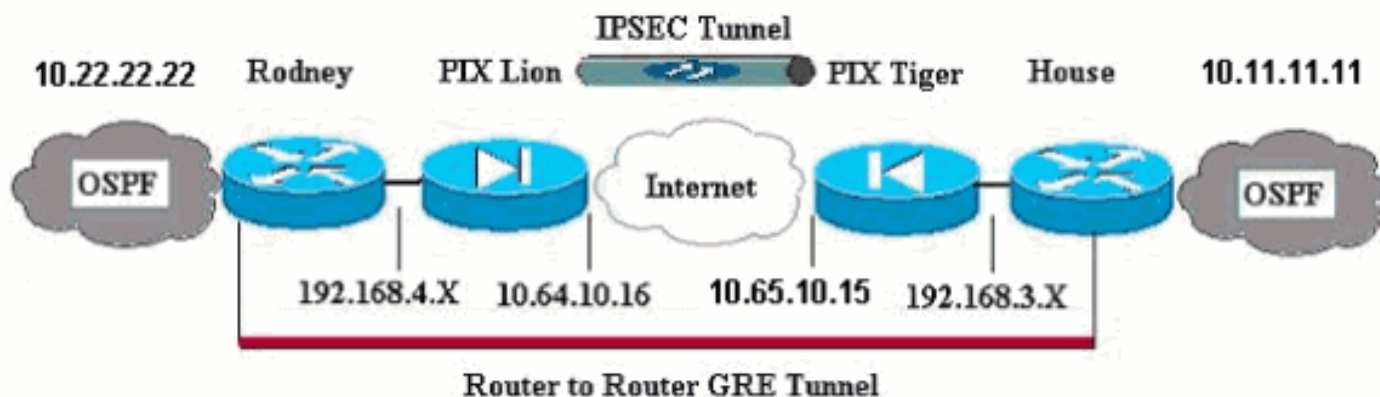
設定

このセクションでは、このドキュメントで説明する機能を設定するための情報を提供します。

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。

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。



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](#) のアドレスです。

注: 暗号化では、Cisco 7600 シリーズ ルータはサポートされません。これを機能させるには、

VPN モジュールのインストールが必要になる場合があります。

設定

このドキュメントでは、次の設定を使用します。

- [PIX Lion](#)
- [PIX トリガ](#)
- [ルータ Rodney](#)
- [Router House](#)

PIX Lion

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Lion fixup protocol dns maximum-length 512
fixup protocol ftp 21 fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719 fixup protocol http 80
fixup protocol rsh 514 fixup protocol rtsp 554 fixup
protocol sip 5060 fixup protocol sip udp 5060 fixup
protocol skinny 2000 fixup protocol smtp 25 fixup
protocol sqlnet 1521 fixup protocol tftp 69 names !---
Defines interesting traffic that is protected by the
IPsec tunnel. access-list 101 permit gre 192.168.4.0
255.255.255.0 192.168.3.0 255.255.255.0 !--- Do not
perform NAT for traffic to other PIX Firewall. access-
list nonat permit ip 192.168.4.0 255.255.255.0
192.168.3.0 255.255.255.0 pager lines 24 mtu outside
1500 mtu inside 1500 mtu intf2 1500 mtu intf3 1500 mtu
intf4 1500 mtu intf5 1500 ip address outside 10.64.10.16
255.255.255.224 ip address inside 192.168.4.1
255.255.255.0 !--- Output suppressed. global (outside) 1
interface !--- Do not Network Address Translate (NAT)
traffic. nat (inside) 0 access-list nonat nat (inside) 1
0.0.0.0 0.0.0.0 0 0 route outside 0.0.0.0 0.0.0.0
10.64.10.1 1 timeout xlate 3:00:00 timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
s0 timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout sip-disconnect 0:02:00 sip-
invite 0:03:00 timeout uauth 0:05:00 absolute aaa-server
TACACS+ protocol tacacs+ aaa-server TACACS+ max-failed-
attempts 3 aaa-server TACACS+ deadtime 10 aaa-server
RADIUS protocol radius aaa-server RADIUS max-failed-
attempts 3 aaa-server RADIUS deadtime 10 aaa-server
LOCAL protocol local no snmp-server location no snmp-
server contact snmp-server community public no snmp-
server enable traps floodguard enable !--- Trust IPsec
traffic and avoid going through !--- access control
```

```
lists (ACLs)/NAT. sysopt connection permit-ipsec !---
IPsec configuration. crypto ipsec transform-set pixset
esp-des esp-md5-hmac crypto map pixmap 20 ipsec-isakmp
crypto map pixmap 20 match address 101 crypto map pixmap
20 set peer 10.65.10.15 crypto map pixmap 20 set
transform-set pixset crypto map pixmap interface outside
isakmp enable outside !--- IKE parameters. isakmp key
***** address 10.65.10.15 netmask 255.255.255.255
isakmp identity address isakmp policy 20 authentication
pre-share isakmp policy 20 encryption des isakmp policy
20 hash md5 isakmp policy 20 group 1 isakmp policy 20
lifetime 3600 telnet timeout 5 ssh 10.104.205.124
255.255.255.255 outside ssh timeout 5 terminal width 80
Cryptochecksum:d39b3d449563c7cd434b43f82f0f0a21 : end
```

PIX トリガ

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Tiger fixup protocol dns maximum-length 512
fixup protocol ftp 21 fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719 fixup protocol http 80
fixup protocol rsh 514 fixup protocol rtsp 554 fixup
protocol sip 5060 fixup protocol sip udp 5060 fixup
protocol skinny 2000 fixup protocol smtp 25 fixup
protocol sqlnet 1521 fixup protocol tftp 69 names
access-list 101 permit gre 192.168.3.0 255.255.255.0
192.168.4.0 255.255.255.0 access-list nonat permit ip
192.168.3.0 255.255.255.0 192.168.4.0 255.255.255.0 mtu
outside 1500 mtu inside 1500 mtu intf2 1500 mtu intf3
1500 mtu intf4 1500 mtu intf5 1500 ip address outside
10.65.10.15 255.255.255.224 ip address inside
192.168.3.1 255.255.255.0 !--- Output suppressed. global
(outside) 1 interface !--- Do not NAT traffic. nat
(inside) 0 access-list nonat nat (inside) 1 0.0.0.0
0.0.0.0 0 0 route outside 0.0.0.0 0.0.0.0 10.64.10.1 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 s0 timeout
h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute aaa-server TACACS+
protocol tacacs+ aaa-server TACACS+ max-failed-attempts
3 aaa-server TACACS+ deadtime 10 aaa-server RADIUS
protocol radius aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10 aaa-server LOCAL protocol
local no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps
floodguard enable sysopt connection permit-ipsec !---
IPsec parameters. crypto ipsec transform-set pixset esp-
des esp-md5-hmac crypto map pixmap 20 ipsec-isakmp
crypto map pixmap 20 match address 101 crypto map pixmap
20 set peer 10.64.10.16 crypto map pixmap 20 set
```

```
transform-set pixset crypto map pixmap interface outside
!--- IKE parameters. isakmp enable outside isakmp key
***** address 10.64.10.16 netmask 255.255.255.255
isakmp identity address isakmp policy 20 authentication
pre-share isakmp policy 20 encryption des isakmp policy
20 hash md5 isakmp policy 20 group 1 isakmp policy 20
lifetime 3600 telnet timeout 5 ssh timeout 5 terminal
width 80 Cryptochecksum:a0a7ac847b05d9d080d1c442ef053a0b
: end
```

ルータ Rodney

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rodney ! memory-size iomem 15 ip subnet-zero !
ip audit notify log ip audit po max-events 100 ! !
interface Loopback1 ip address 10.22.22.22 255.255.255.0
! interface Tunnel0 ip address 10.1.1.2 255.255.255.0 !-
-- Tunnel source. tunnel source Ethernet0/1 !--- Tunnel
destination. tunnel destination 192.168.3.2 ! interface
Ethernet0/0 no ip address ! interface Serial0/0 no ip
address shutdown ! interface Ethernet0/1 ip address
192.168.4.2 255.255.255.0 ! interface Serial0/1 no ip
address shutdown ! router ospf 22 log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0 network 10.22.22.0
0.0.0.255 area 0 ! ip classless ip route 0.0.0.0 0.0.0.0
192.168.4.1 !--- The 10.11.11.0 traffic is passed
through !--- the GRE tunnel. ip route 10.11.11.0
255.255.255.0 Tunnel0 no ip http server ! line con 0
line aux 0 line vty 0 4 login ! end! End
```

Router House

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house ! ip subnet-zero no ip domain-lookup ! !
interface Loopback1 ip address 10.11.11.11 255.255.255.0
! interface Tunnel0 ip address 10.1.1.1 255.255.255.0 !-
-- Tunnel source. tunnel source FastEthernet0/1 !---
Tunnel destination. tunnel destination 192.168.4.2 !
interface FastEthernet0/0 no ip address shutdown duplex
auto speed auto ! interface FastEthernet0/1 ip address
192.168.3.2 255.255.255.0 duplex auto speed auto !
interface FastEthernet4/0 no ip address shutdown duplex
auto speed auto ! router ospf 11 log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0 network 10.11.11.0
0.0.0.255 area 0 ! ip classless ip route 0.0.0.0 0.0.0.0
192.168.3.1 !--- The 10.22.22.0 traffic is passed
through !--- the GRE tunnel. ip route 10.22.22.0
255.255.255.0 Tunnel0 ip http server ! line con 0 line
aux 0 line vty 0 4
```

確認

現在、この設定に使用できる確認手順はありません。

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。

PIX および IPSec トンネルのトラブルシューティングの詳細については、[確立された IPSec トンネル上での PIX からのデータの受け渡しに関するトラブルシューティング](#) (英語) を参照してください。

[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。

PIX IPsec の正しいデバッグ

- **show crypto isakmp sa** : ピア間で構築された Internet Security Association Management Protocol (ISAKMP) セキュリティ アソシエーション (SA) を表示します。Lion#`show crypto isakmp sa` Total : 1 Embryonic : 0 dst src state pending created 10.65.10.15 10.64.10.16 QM_IDLE 0 1 Tiger#`show crypto isakmp sa` Total SAs : 1 Embryonic : 0 dst src state pending created 10.65.10.15 10.64.10.16 QM_IDLE 0 1
- **show crypto engine connection active** : 確立されたフェーズ 2 の各 SA と送信されたトラフィック量を表示します。Lion#`show crypto engine connection active` Crypto Engine Connection Map: size = 8, free = 6, used = 2, active = 2 Tiger#`show crypto engine connection active` Crypto Engine Connection Map: size = 8, free = 6, used = 2, active = 2
- **show debug - デバッグ出力を表示します**。Lion#`show debug debug crypto ipsec debug crypto isakmp debug crypto engine` crypto_isakmp_process_block: src 10.65.10.15, dest 10.64.10.16 OAK_MM exchange ISAKMP (0): processing SA payload. message ID = 0 ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy ISAKMP: encryption DES-CBC ISAKMP: hash MD5 ISAKMP: default group 1 ISAKMP: auth pre-share ISAKMP: life type in seconds ISAKMP: life duration (basic) of 3600 ISAKMP (0): atts are acceptable. Next payload is 0 ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR return status is IKMP_NO_ERROR# crypto_isakmp_process_block: src 10.65.10.15, dest 10.64.10.16 OAK_MM exchange ISAKMP (0): processing KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0 ISAKMP (0): processing vendor id payload ISAKMP (0): speaking to another IOS box! ISAKMP (0): ID payload next-payload : 8 type : 1 protocol : 17 port : 500 length : 8 ISAKMP (0): Total payload length: 12 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 10.65.10.15, dest 10.64.10.16 OAK_MM exchange ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing HASH payload. message ID = 0 ISAKMP (0): SA has been authenticated ISAKMP (0): beginning Quick Mode exchange, M-ID of 1220019031:48b80357IPSEC(key. IPSEC(spi_response): getting spi 0xa67177c5(2792454085) for SA from 10.65.10.15 to 10.64.10.16 for prot 3 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 10.65.10.15, dest 10.64.10.16 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 1220019031 ISAKMP : Checking IPsec proposal 1 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-MD5 ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part, (key eng. msg.) dest= 10.65.10.15, src= 10.64.10.16, dest_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4), src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE payload. message ID = 1220019031 ISAKMP (0): processing ID payload. message ID = 1220019031 ISAKMP (0): processing ID payload. message ID = 1220019031map_alloc_entry: allo2 map_alloc_entry: allocating entry 1 ISAKMP (0): Creating IPsec SAs inbound SA from 10.65.10.15 to 10.64.10.16 (proxy 192.168.3) has spi 2792454085 and conn_id 2 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytes outbound SA from 10.64.10.16 to 10.65.10.15 (proxy 192.168.) has spi 285493108 and conn_id 1 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...

```
IPSEC(initialize_sas): , (key eng. msg.) dest= 10.64.10.16, src= 10.65.10.15, dest_proxy=
192.168.4.0/255.255.255.0/0/0 (type=4), src_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi=
0xa67177c5(2792454085), conn_id= 2, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key
eng. msg.) src= 10.64.10.16, dest= 10.65.10.15, src_proxy= 192.168.4.0/255.255.255.0/0/0
(type=4), dest_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-
des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0x11044774(285493108), conn_id= 1,
keysize= 0, flags= 0x4 return status is IKMP_NO_ERROR
```

GRE によってルーティングと Ping を通過させるルータ

- **show ip route** : IP ルーティング テーブルのエントリを表示します。rodney#**show ip route**
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF
NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort
is 192.168.4.1 to network 0.0.0.0 10.0.0.0/24 is subnetted, 1 subnets C 10.1.1.0 is directly
connected, Tunnel0 10.0.0.0/24 is subnetted, 1 subnets C 10.20.20.0 is directly connected,
Loopback0 10.0.0.0/24 is subnetted, 1 subnets C 10.22.22.0 is directly connected, Loopback1
C 192.168.4.0/24 is directly connected, Ethernet0/1 10.0.0.0/24 is subnetted, 1 subnets S
10.10.10.0 is directly connected, Tunnel0 10.0.0.0/32 is subnetted, 1 subnets O 10.11.11.11
[110/11112] via 10.1.1.1, 03:34:01, Tunnel0 S* 0.0.0.0/0 [1/0] via 192.168.4.1 rodney#
rodney#**ping 10.11.11.11** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to
10.11.11.11, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip
min/avg/max = 1/2/4 ms house#**show ip route** Codes: C - connected, S - static, I - IGRP, R -
RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 -
OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 -
OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded
static route Gateway of last resort is 192.168.3.1 to network 0.0.0.0 10.0.0.0/24 is
subnetted, 1 subnets C 1.1.1.0 is directly connected, Tunnel0 10.0.0.0/24 is subnetted, 1
subnets S 10.20.20.0 is directly connected, Tunnel0 10.0.0.0/32 is subnetted, 1 subnets O
10.22.22.22 [110/11112] via 10.1.1.2, 03:33:39, Tunnel0 10.0.0.0/24 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, Loopback0 10.0.0.0/24 is subnetted, 1 subnets C
10.11.11.0 is directly connected, Loopback1 C 192.168.3.0/24 is directly connected,
FastEthernet0/1 S* 0.0.0.0/0 [1/0] via 192.168.3.1 house#**ping 10.22.22.22** Type escape
sequence to abort. Sending 5, 100-byte ICMP Echos to 10.22.22.22, timeout is 2 seconds:
!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

関連情報

- [IPSec ネゴシエーション/IKE プロトコル](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [PIX 製品に関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)