Sonicwall 製品と Cisco のセキュリティ アプライアンスかんの VPN 設定例

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[関連製品](#)
[表記法](#)
[設定](#)
[ネットワーク図](#)
[Sonicwall の設定](#)
[IPsec メイン モード設定](#)
[IPsec アグレッシブ モード設定](#)
[確認](#)
[トラブルシュート](#)
[関連情報](#)

概要

このドキュメントでは、アグレッシブ モードとメイン モードの両方を使用して 2 つのプライベート ネットワーク間の通信を行う、事前共有キーを使用した IPsec トンネルの設定方法の例を示します。この例では、通信するネットワークは、Cisco セキュリティ アプライアンス（PIX/ASA）内部の 192.168.1.x プライベート ネットワークと SonicwallTM TZ170 ファイアウォール内部の 172.22.1.x プライベート ネットワークです。

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。

- この設定を開始する前に、Cisco セキュリティ アプライアンス内部および Sonicwall TZ170 内部からのトラフィックがインターネット（ここでは 10.x.x.x ネットワークと表現します）に流れている必要があります。
- ユーザが IPsec のネゴシエーションに精通している必要があります。この処理は、2 つの Internet Key Exchange（IKE; インターネット キー エクスチェンジ）フェーズを含む、次の 5 つの手順に分けることができます。対象トラフィックによって IPsec トンネルが開始されます。IPsec ピアの間を転送されるトラフィックは、対象トラフィックとみなされます。IKE フ

エーズ 1 では、IPsec ピア同士が、IKE セキュリティ アソシエーション（SA）ポリシーについてネゴシエートします。ピアが認証されると、Internet Security Association and Key Management Protocol（ISAKMP）を使用して安全なトンネルが作成されます。IKE フェーズ 2 では、IPsec ピア同士が認証済みの安全なトンネルを使用して、IPsec SA トランスフォームをネゴシエートします。共有ポリシーのネゴシエーションによって、IPsec トンネルの確立方法が決まります。IPsec トンネルが作成され、IPsec トランスフォーム セットに設定された IPsec パラメータに基づいて、IPsec 間でデータが伝送されます。IPsec SA が削除されるか、そのライフタイムの有効期限が切れると、IPsec トンネルは終了します。

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いています。

- Cisco PIX 515E バージョン 6.3(5)
- Cisco PIX 515 バージョン 7.0(2)
- Sonicwall TZ170、SonicOS Standard 2.2.0.1

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定は、次のバージョンのハードウェアとソフトウェアにも使用できます。

- PIX 6.3(5) の設定は、同じバージョンのソフトウェアが動作する他のすべての Cisco PIX ファイアウォール製品（PIX 501、506 など）で使用できます。
- PIX/ASA 7.0(2) の設定が使用できるのは、PIX 7.0 トレインのソフトウェアが動作するデバイス（501、506、および一部の古い 515 を除く）と Cisco 5500 シリーズ ASA だけです。

表記法

ドキュメント表記の詳細については、『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

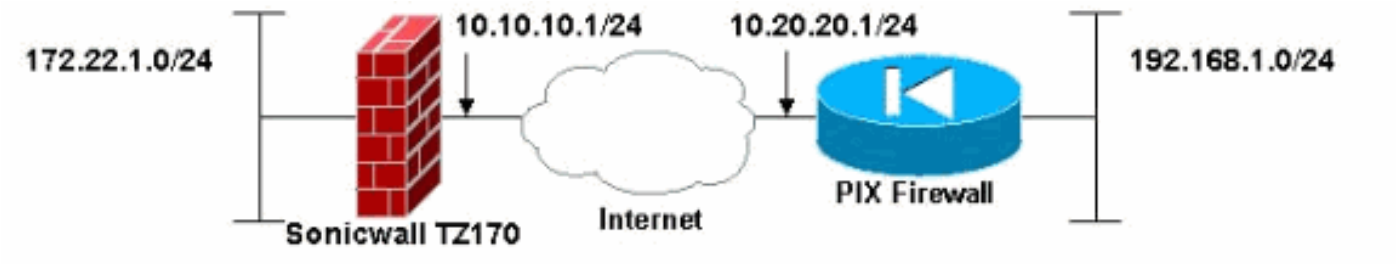
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクション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）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

注：IPSecアグレッシブモードでは、SonicwallがPIXへのIPSecトンネルを開始する必要があります。この設定のデバッグ情報を解析すれば、これがわかります。これは IPsec のアグレッシブ モードの動作方法に起因するものです。

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 セットアップを使用します。

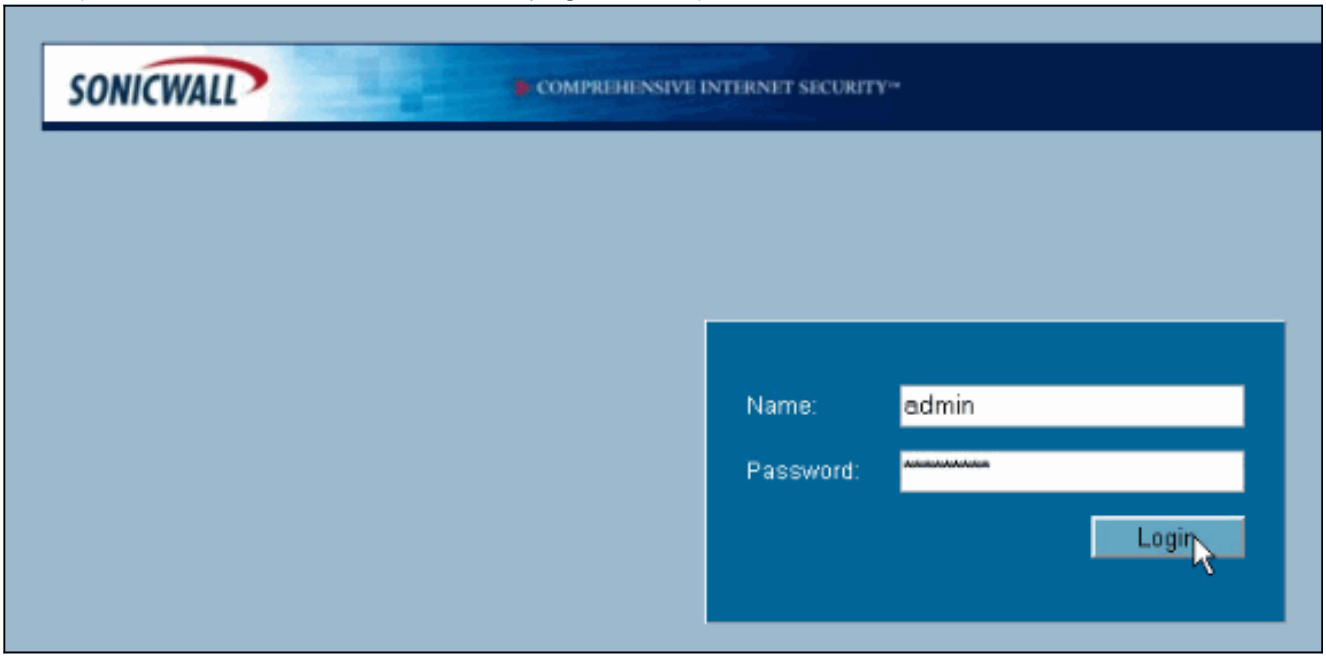


Sonicwall の設定

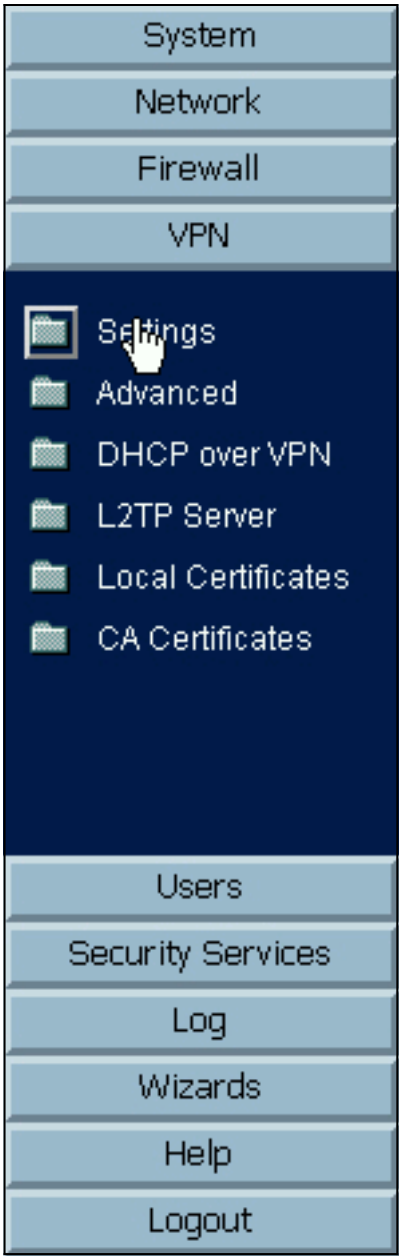
Sonicwall TZ170 の設定は、Web ベースのインターフェイスで行います。

次のステップを実行します。

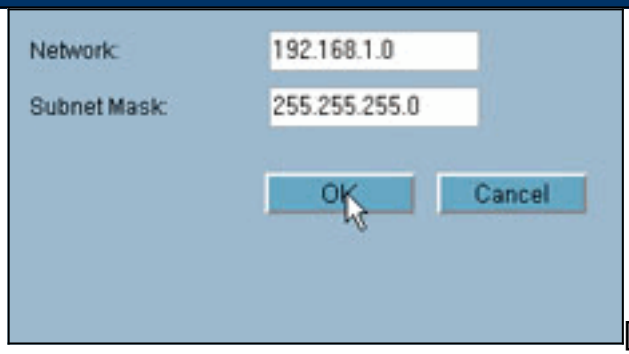
1. 標準の Web ブラウザで、いずれかの内部インターフェイス上のルータの IP アドレスに接続します。次のログイン ウィンドウが表示されます。



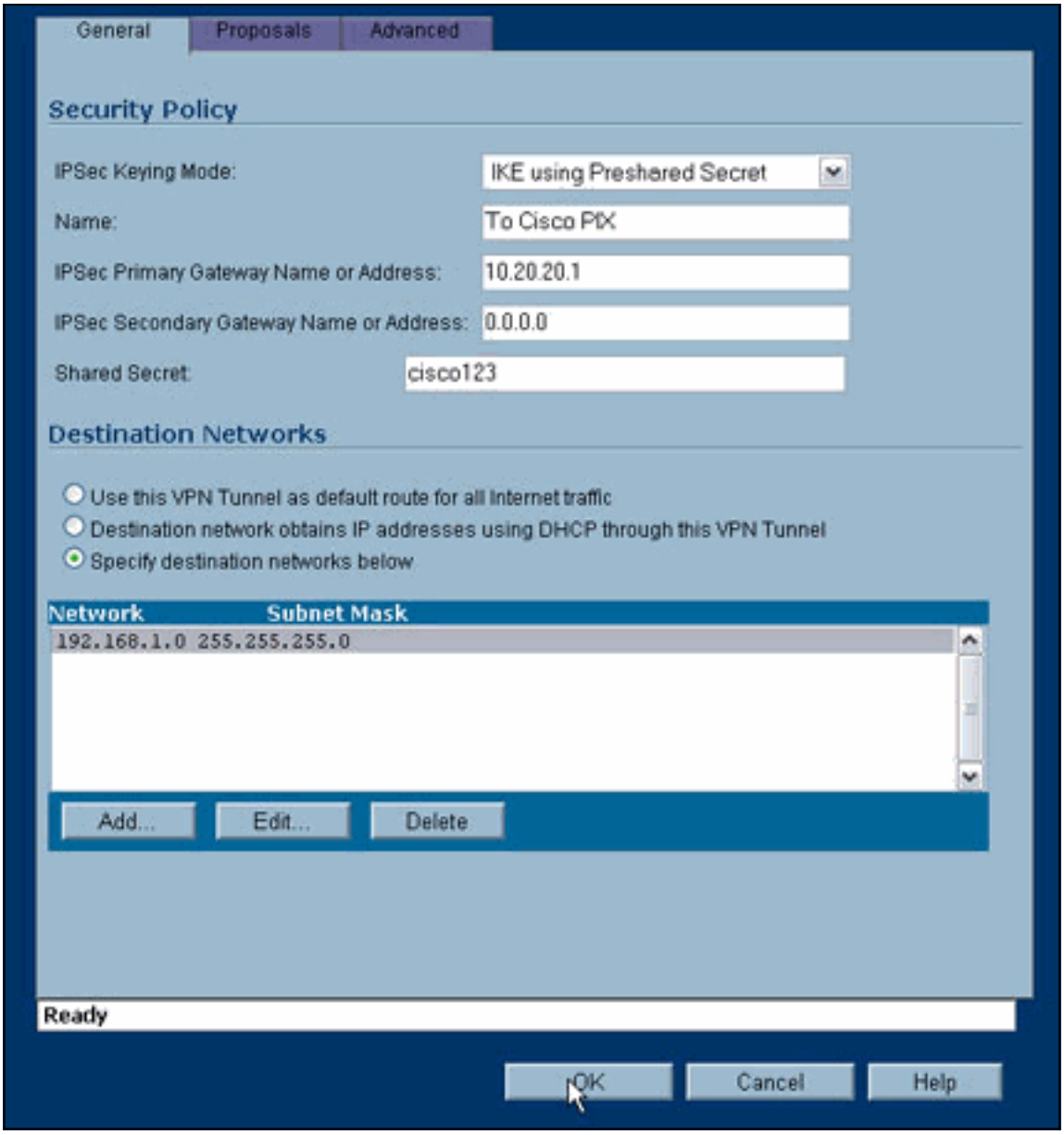
2. Sonicwall デバイスにログインし、[VPN] > [Settings]を選択します。



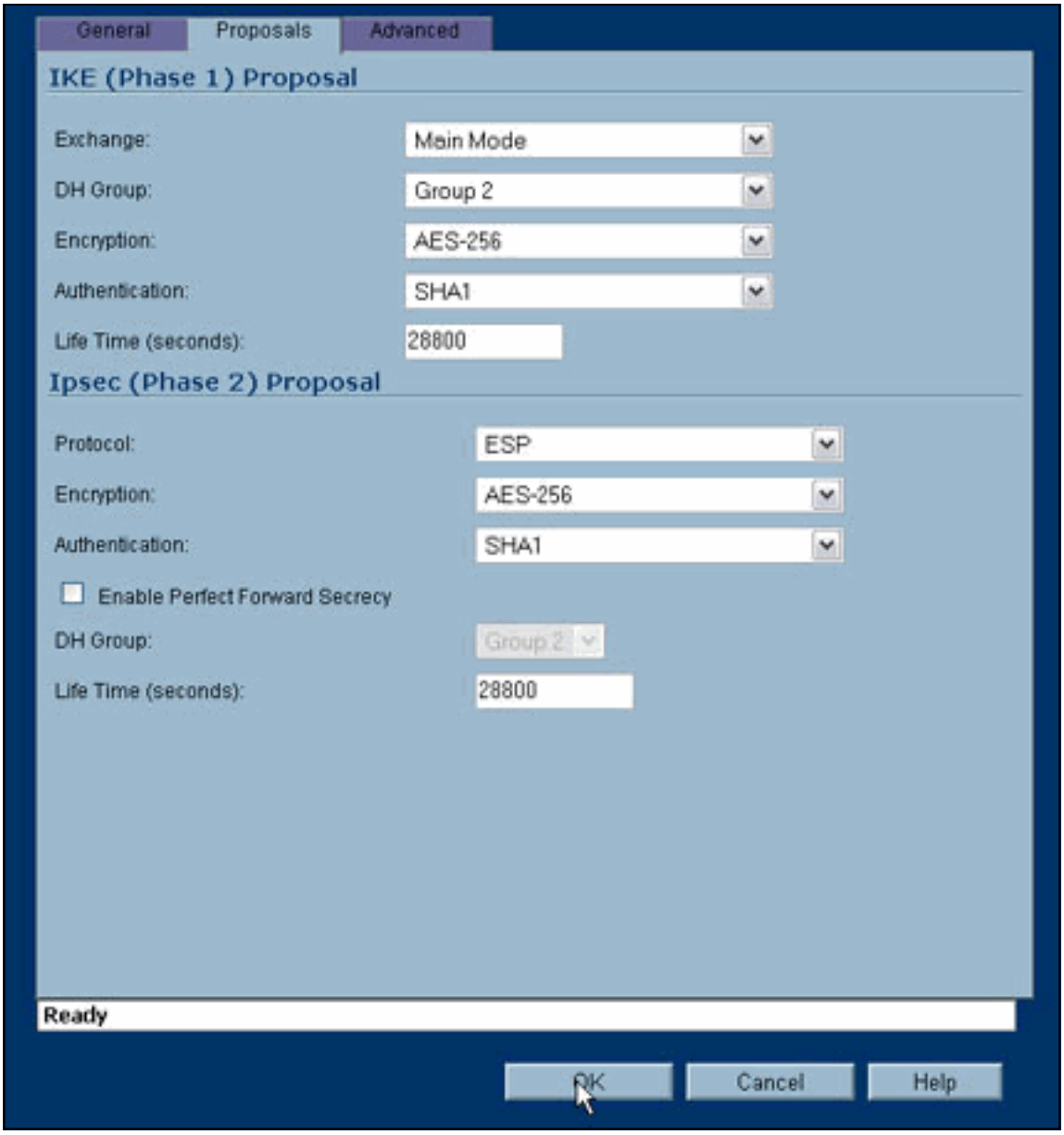
3. 使用する VPN ピアと事前共有秘密の IP アドレスを入力します。[Destination Networks] の下の [Add] をクリックします。



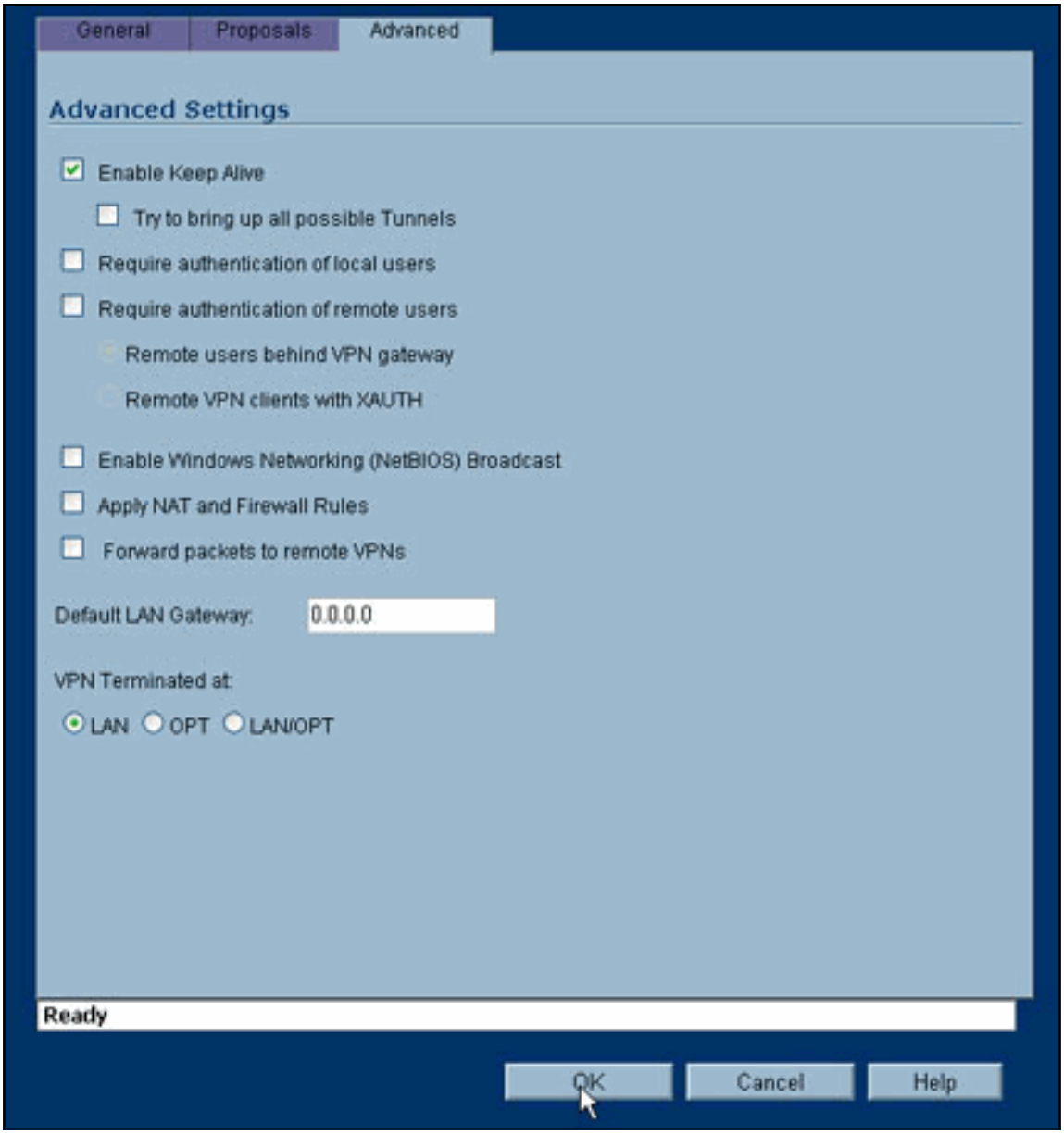
4. 宛先ネットワークを入力します。[Settings] ウィンドウが表示されます。



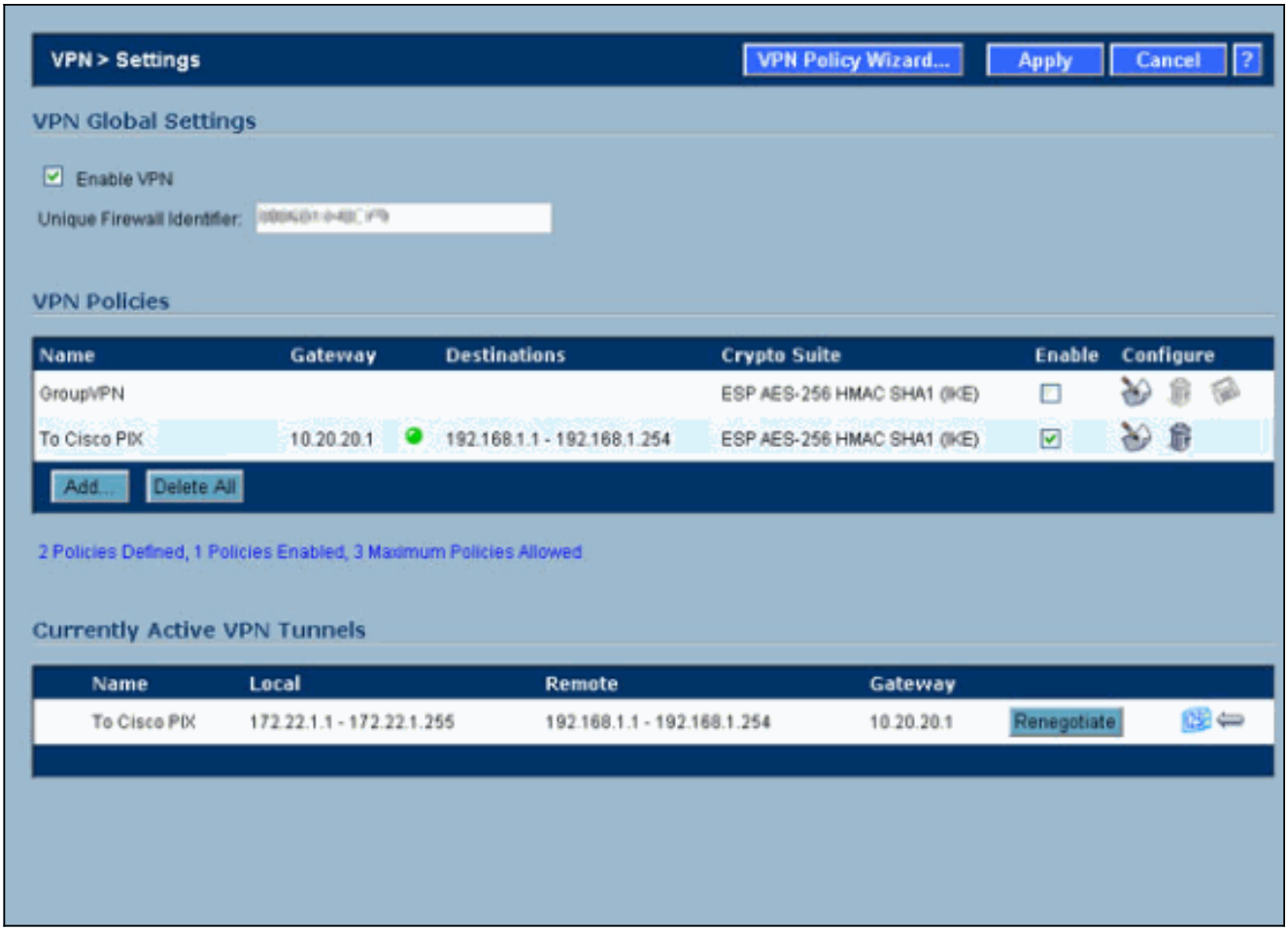
5. [Settings] ウィンドウの上部にある [Proposals] タブをクリックします。
6. この設定で使用する交換モード（メイン モードまたはアグレッシブ モード）を、フェーズ 1 とフェーズ 2 の他の設定とともに選択します。この設定例では、両方のフェーズで AES-256 暗号化を使用し、認証には SHA1 ハッシュ アルゴリズム、IKE ポリシーには 1024 ビット Diffie-Hellman グループ 2 を使用しています。



7. [Advanced] タブをクリックします。このタブでは、さらに追加オプションを設定する必要がある場合もあります。この設定例では、次のように設定されています。



8. [OK] をクリックします。この設定とリモート PIX の設定が終わったら、Settings ウィンドウは、次の Settings ウィンドウの例のようになっている必要があります。



IPsec メイン モード設定

このセクションでは、次の設定例を使用しています。

- Cisco PIX 515e バージョン 6.3(5)
- Cisco PIX 515 バージョン 7.0(2)

Cisco PIX 515e バージョン 6.3(5)

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
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 !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
```

```
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 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 !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION: !--- Defines the transform set
for Phase 2 encryption and authentication. !---
Austinlab is the name of the transform set that uses
aes-256 encryption !--- as well as the SHA1 hash
algorithm for authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies IKE is used to establish the IPsec SAs
for the map "maptosw". crypto map maptosw 67 ipsec-
isakmp !--- Specifies the ACL "pixtosw" to use with this
map . crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map. crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Specifies the interface
to use for the IPsec tunnel.

isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used with the preshared key cisco123. isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

Cisco PIX 515 バージョン 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS®. !--- This output configures the IP
address, interface name, !--- and security level for
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies the ACL pixtosw to use with this map.
crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map . crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Defines how the PIX
```

```
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration !--- settings specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

IPsec アグレッシブ モード設定

このセクションでは、次の設定例を使用しています。

- Cisco PIX 515e バージョン 6.3(5)
- Cisco PIX 515 バージョン 7.0(2)

Cisco PIX 515e バージョン 6.3(5)

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
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 !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
```

```
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 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 !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION !--- Defines the transform set for
Phase 2 encryption and authentication. !--- Austinlab is
the name of the transform set that uses aes-256
encryption !--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map ciscopix for the transform
set. crypto dynamic-map ciscopix 1 set transform-set
austinlab !--- Specifies the IKE that should be used to
establish SAs !--- for the dynamic map. crypto map
dynmaptosw 66 ipsec-isakmp dynamic ciscopix !--- Applies
the settings above to the outside interface. crypto map
dynmaptosw interface outside !--- PHASE 1 CONFIGURATION
!--- Specifies the interface to use for the IPsec tunnel
.
isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used as the preshared key "cisco123". isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

Cisco PIX 515 バージョン 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS. !--- This output configures the IP
```

```
address, interface name, and security level for !---
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map "ciscopix" for the defined
transform set. crypto dynamic-map ciscopix 1 set
transform-set austinlab !--- Specifies that IKE should
be used to establish SAs !--- for the defined dynamic
map. crypto map dynmaptosw 66 ipsec-isakmp dynamic
ciscopix !--- Applies the settings to the outside
interface. crypto map dynmaptosw interface outside !---
PHASE 1 CONFIGURATION !--- Defines how the PIX
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration settings !--- specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
```

```
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show crypto isakmp sa：現在ピアにあるすべての IKE SA を表示します。**
- **show crypto ipsec sa**：現在の SA で使用されている設定を表示します。

次の表は、トンネルが完全に確立された後の、PIX 6.3(5) と PIX 7.0(2) 両方のメイン モードとアグレッシブ モードのデバッグ出力の一部を示しています。

注：この2つのタイプのハードウェア間でIPSecトンネルを確立するには、十分な情報が必要です。コメントがある場合は、このドキュメントの左側のフィードバック フォームを使用します。

- Cisco PIX 515e バージョン 6.3(5) - メイン モード
- Cisco PIX 515 バージョン 7.0(2) - メイン モード
- Cisco PIX 515e バージョン 6.3(5) - アグレッシブ モード
- Cisco PIX 515 バージョン 7.0(2) - アグレッシブ モード

Cisco PIX 515e バージョン 6.3(5) - メイン モード

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src         state     pending
created
      10.10.10.1       10.20.20.1    QM_IDLE          0
1
pix515e-635#



pix515e-635#show crypto ipsec sa


           interface: outside
           Crypto map tag: maptosw, local addr.
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1:500
           PERMIT, flags={origin_is_acl,}
           #pkts encaps: 4, #pkts encrypt: 4, #pkts
```

```
digest 4
          #pkts decaps: 4, #pkts decrypt: 4, #pkts
verify 4
          #pkts compressed: 0, #pkts decompressed: 0
          #pkts not compressed: 0, #pkts compr. failed:
0, #pkts decompress failed: 0
          #send errors 1, #recv errors 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
          path mtu 1500, ipsec overhead 72, media mtu
1500
          current outbound spi: ed0afa33

 inbound esp sas:
          spi: 0xac624692(2892121746)
          transform: esp-aes-256 esp-sha-hmac ,
          in use settings ={Tunnel, }
          slot: 0, conn id: 1, crypto map: maptosw
          sa timing: remaining key lifetime (k/sec):
(4607999/28718)
          IV size: 16 bytes
          replay detection support: Y


          inbound ah sas:


          inbound pcp sas:


          outbound esp sas:
          spi: 0xed0afa33(3976919603)
          transform: esp-aes-256 esp-sha-hmac ,
          in use settings ={Tunnel, }
          slot: 0, conn id: 2, crypto map: maptosw
          sa timing: remaining key lifetime (k/sec):
(4607999/28718)
          IV size: 16 bytes
          replay detection support: Y


          outbound ah sas:


          outbound pcp sas:

pix515e-635#
```

Cisco PIX 515 バージョン 7.0(2) - メイン モード

```
pix515-702#show crypto isakmp sa

 Active SA: 1
          Rekey SA: 0 (A tunnel will report 1 Active
and 1 Rekey SA during rekey)
          Total IKE SA: 1

1 IKE Peer: 10.10.10.1
          Type : L2L Role : initiator
          Rekey : no State : MM_ACTIVE
          pix515-702#
```

```
pix515-702#show crypto ipsec sa
interface: outside
    Crypto map tag: maptosw, local addr: 10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: 2D006547

 inbound esp sas:
           spi: 0x309F7A33 (815757875)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28739)
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0x2D006547 (755000647)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28737)
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

Cisco PIX 515e バージョン 6.3(5) - アグレッシブ モード

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending
created
      10.20.20.1       10.10.10.1    QM_IDLE         0
1

pix515e-635#show crypto ipsec sa



           interface: outside
           Crypto map tag: dynmaptosw, local addr.
10.20.20.1

 local ident (addr/mask/prot/port):
```

```
(192.168.1.0/255.255.255.0/0/0)
          remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
          current_peer: 10.10.10.1:500
          PERMIT, flags={}
          #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.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
          path mtu 1500, ipsec overhead 72, media mtu
1500
          current outbound spi: efb1149d

 inbound esp sas:
          spi: 0x2ad2c13c(718455100)
          transform: esp-aes-256 esp-sha-hmac ,
          in use settings ={Tunnel, }
          slot: 0, conn id: 2, crypto map: dynmaptosw
          sa timing: remaining key lifetime (k/sec):
(4608000/28736)
          IV size: 16 bytes
          replay detection support: Y


          inbound ah sas:


          inbound pcp sas:


          outbound esp sas:
          spi: 0xefb1149d(4021359773)
          transform: esp-aes-256 esp-sha-hmac ,
          in use settings ={Tunnel, }
          slot: 0, conn id: 1, crypto map: dynmaptosw
          sa timing: remaining key lifetime (k/sec):
(4608000/28727)
          IV size: 16 bytes
          replay detection support: Y


          outbound ah sas:


          outbound pcp sas:

pix515e-635#
```

Cisco PIX 515 バージョン 7.0(2) - アグレッシブ モード

```
pix515-702#show crypto isakmp sa

 Active SA: 1
          Rekey SA: 0 (A tunnel will report 1 Active
and 1 Rekey SA during rekey)
          Total IKE SA: 1
```

```
1 IKE Peer: 10.10.10.1
           Type : L2L Role : responder
           Rekey : no State : AM_ACTIVE
           pix515-702#

pix515-702#show crypto ipsec sa
           interface: outside
           Crypto map tag: ciscopix, local addr:
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: D7E2F5FD

 inbound esp sas:
           spi: 0xDCBF6AD3 (3703532243)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28703
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0xD7E2F5FD (3621975549)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28701
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco PIX Firewall ソフトウェア

- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems