PIX/ASA 7.x 以降： PIX-to-PIX VPN トンネルの設定例

目次

概要

このドキュメントでは、Cisco Adaptive Security Device Manager（ASDM）を使用して 2 つの PIX Firewall 間の VPN トンネルを設定する手順について説明します。 ASDM は、GUI によって PIX Firewall をセットアップ、設定、モニタするために設計されたアプリケーション ベースの設定ツールです。 PIX Firewall は、2 つの異なるサイトに配置されます。

トンネルは IPsec を使用して形成されます。 IPSec とは、IPSec ピア間でデータの機密性、データの完全性、およびデータの発信元の認証を提供するオープン スタンダードの組み合わせです。

注: PIX 7.1 およびそれ以降では、**sysopt connection permit-ipsec コマンドは sysopt 接続許可 VPN** に変更されます。 このコマンドはトラフィックが VPN トンネルによってセキュリティ アプライアンス モデルを入力し、復号化される、インターフェイス アクセス リストをバイパスするようにします。 グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます。 この機能をディセーブルにするために、このコマンドの **no 形式を**使用して下さい。 このコマンドは CLI 設定で目に見えません。

PIX がルータからのダイナミック IPsec 接続を受け入れるシナリオの詳細については、『ACS 6.x： 簡単なPIX-to-PIX VPNトンネル 設定例 Cisco PIX セキュリティ アプライアンス モデルがソ

フトウェア バージョン 6.x を実行するほぼ同じ位のシナリオを学ぶため。

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

この文書に記載されている情報は接続するため適切なピアを判別するためにこのピアが最初の独自の交換を始めること規定 します。

- バージョン 7.x および それ 以降が付いている Cisco PIX 500 シリーズ セキュリティ アプライアンス モデル
- ASDM バージョン 5.x 以降

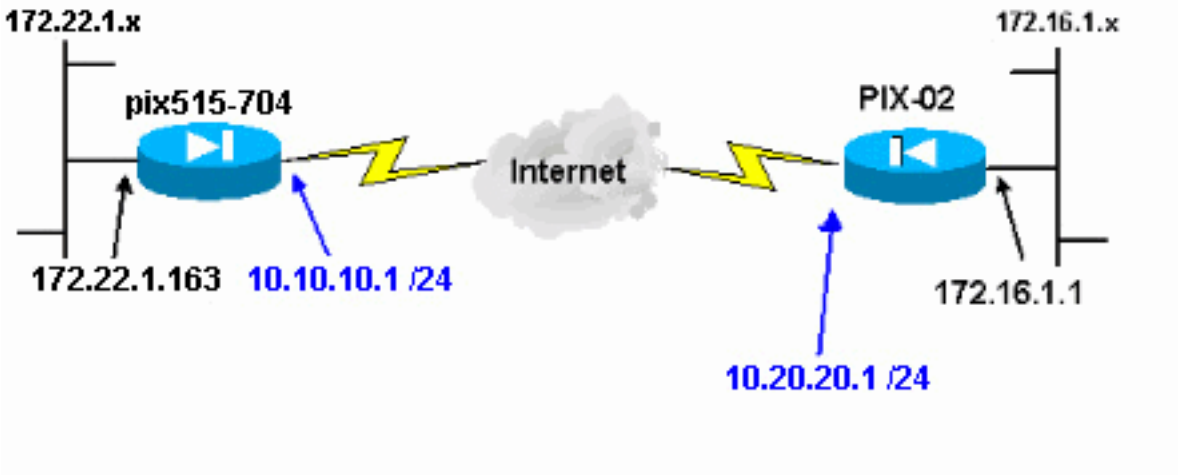
注: ASA を ASDM で設定できるようにするには、『ASDM 用の HTTPS アクセスの許可』を参照してください。

注: ASA 5500 シリーズ バージョン 7.x/8.x は PIXバージョン 7.x/8.x で参照される同じソフトウェアを実行します。 このドキュメントで使用する設定は、両方の製品ラインに適用できます。

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。

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。



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

IPsec ネゴシエーションは 5 つのステップ分割することができ 2 インターネット キー エクスチェンジ（IKE）フェーズが含まれています。

1. 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。
2. IKE フェーズ 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。
3. 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。
4. 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。
5. 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。**注:** ピア同士でどちらか一方の IKE フェーズが一致しない場合、2 台の PIX 間の IPsec ネゴシエーションは失敗します。

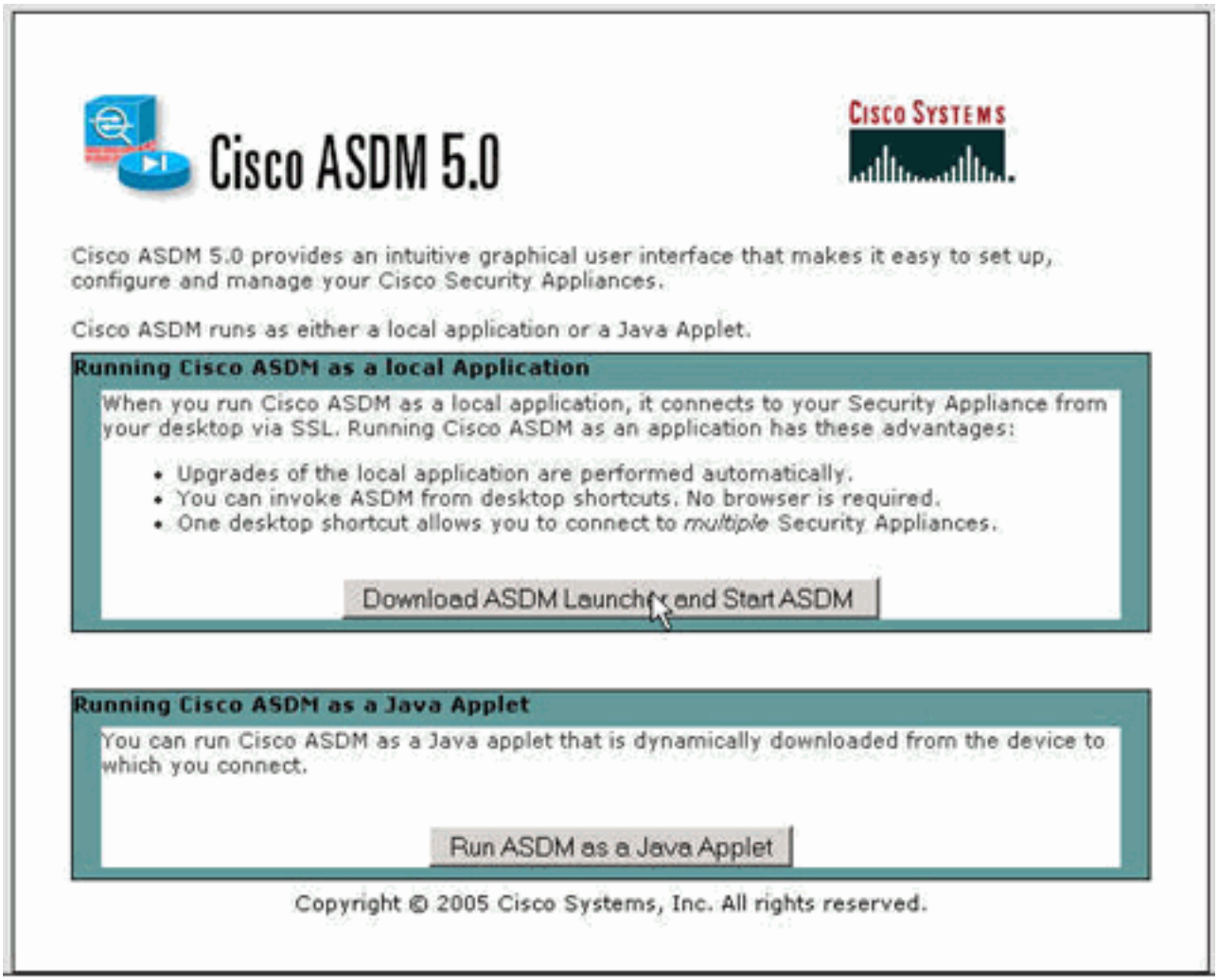
設定

- ASDM の設定
- PIX CLI コンフィギュレーション

ASDM の設定

次の手順を実行します。

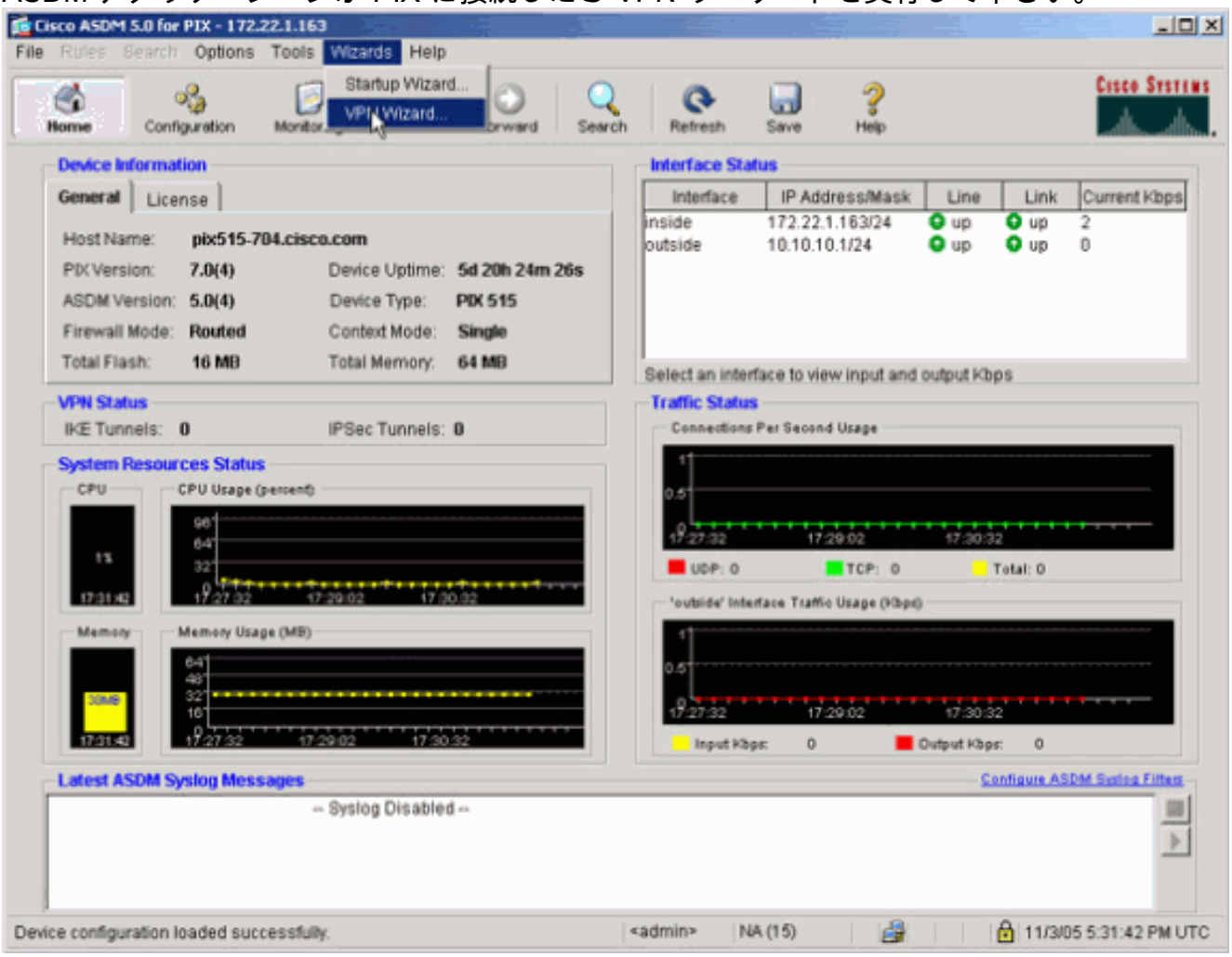
1. ブラウザを開き、PIX の ASDM にアクセスするために **https:// <Inside_IP_Address_of_PIX> を**入力して下さい。SSL 証明書の信憑性に関連してブラウザから出力されるすべての警告を認可します。 デフォルトのユーザ名とパスワードは、両方とも空白です。PIX は ASDM アプリケーションのダウンロードを可能にするためにこのウィンドウを示します。 次の例の場合、アプリケーションはローカル コンピュータにロードされ、Java アプレットでは動作しません。



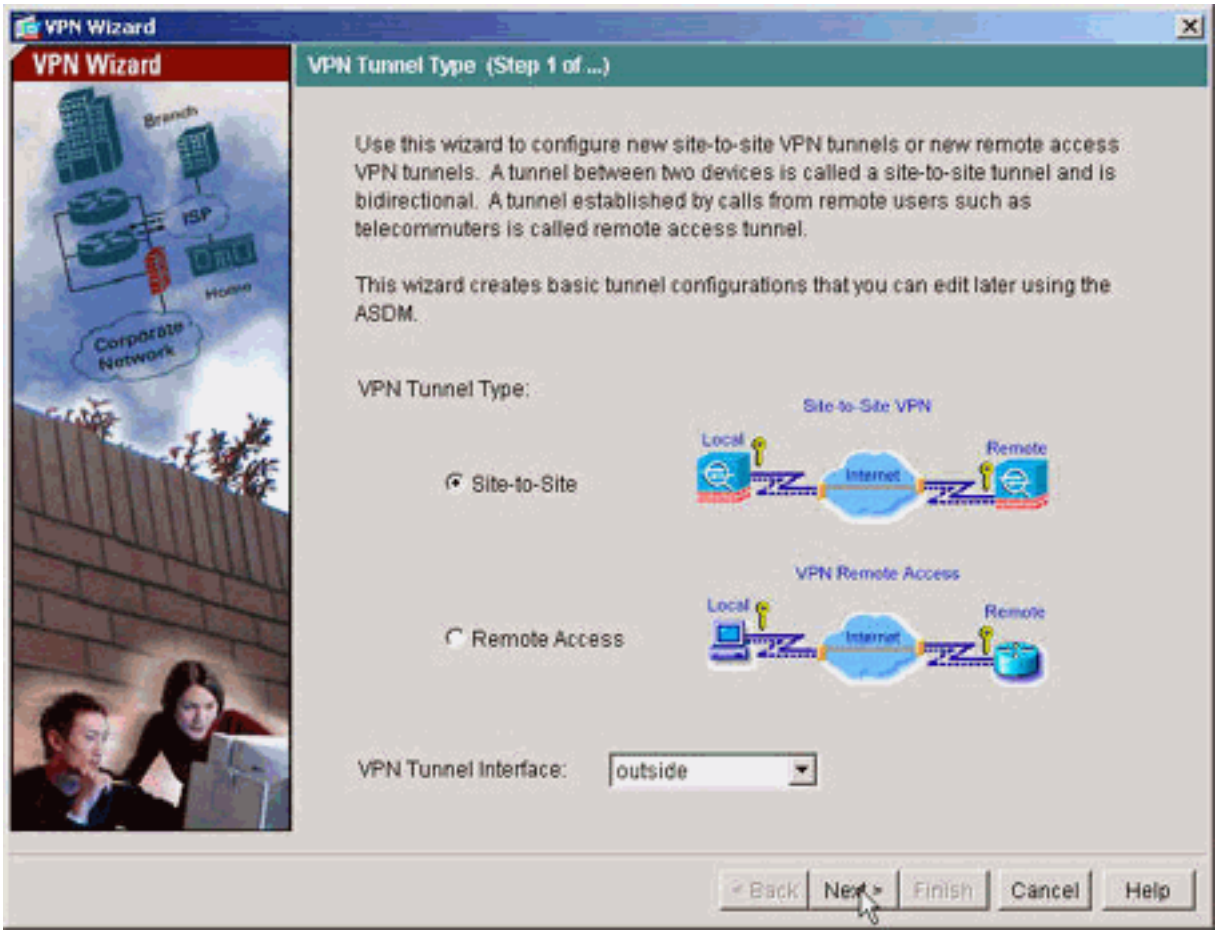
2. ASDM アプリケーションのためのインストーラをダウンロードするために『Download ASDM Launcher and Start ASDM』 をクリック して下さい。
3. ソフトウェアをインストールし、Cisco ASDM ランチャーを実行するために ASDM ランチャー ダウンロードが、プロンプトに従えば。
4. **http -** コマンドで設定したインターフェイスの IP アドレス、およびユーザ名とパスワード（指定した場合）を入力します。この例では、デフォルトの空のユーザ名とパスワードを使

用します。

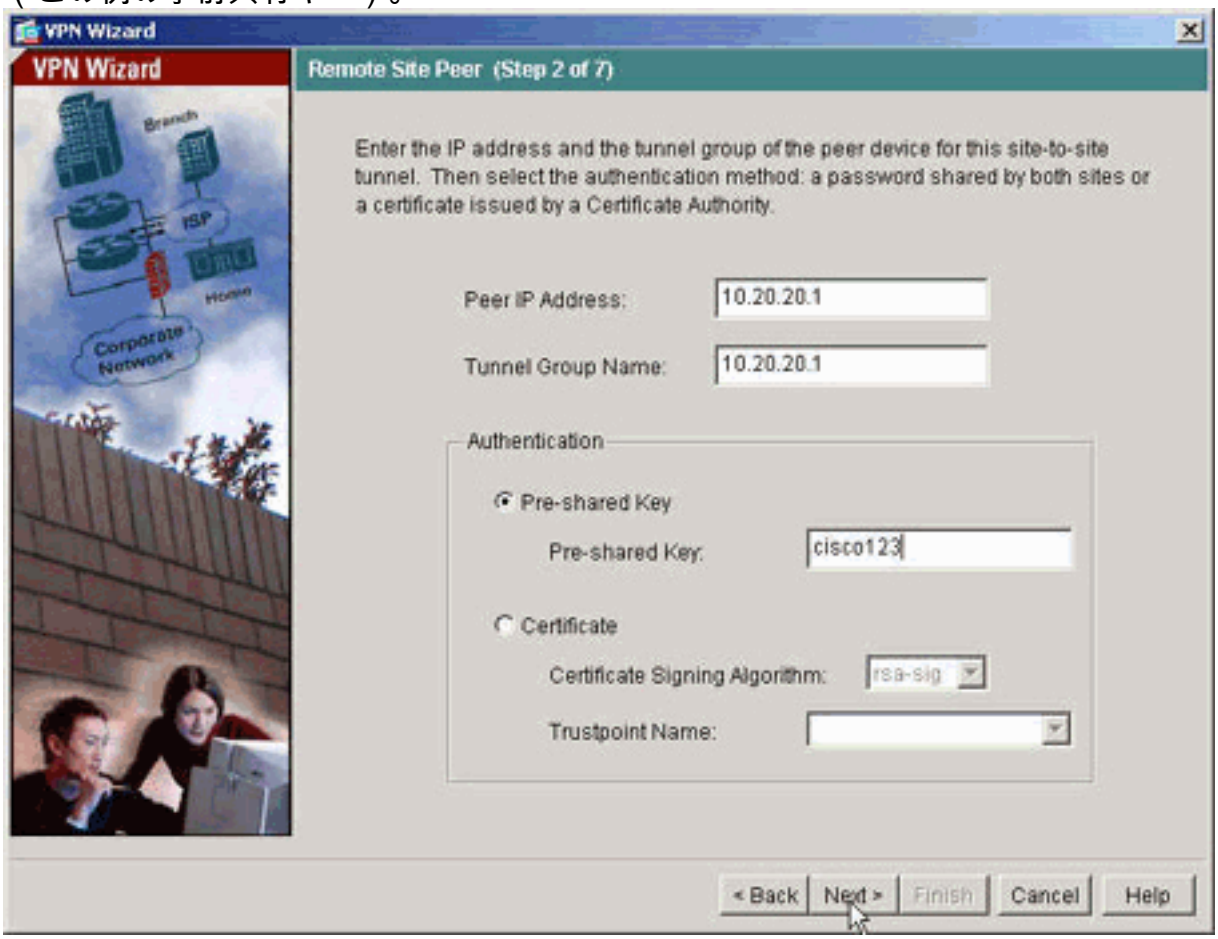
5. ASDM アプリケーションが PIX に接続したら VPN ウィザードを実行して下さい。



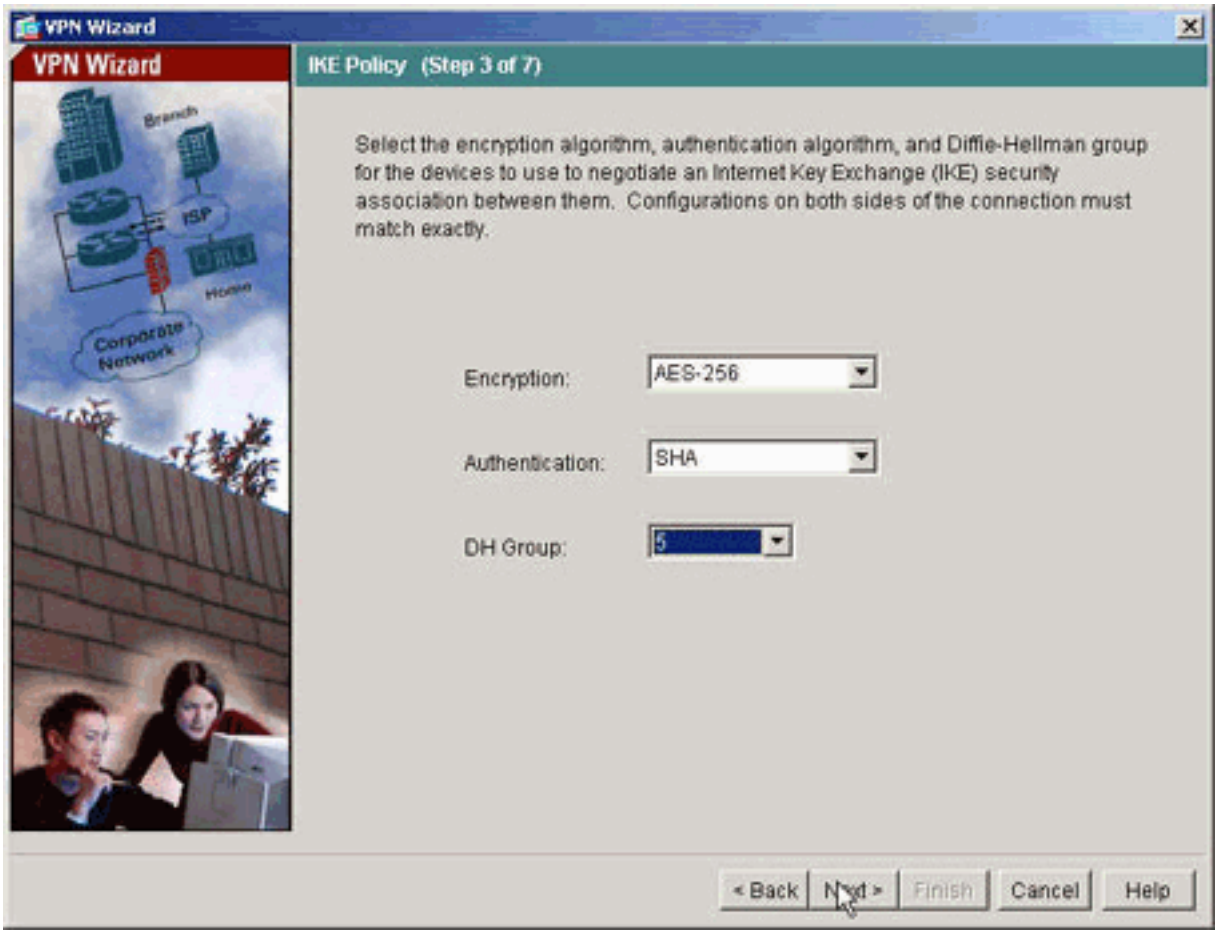
6. **サイト間VPN** トンネルタイプを選択して下さい。



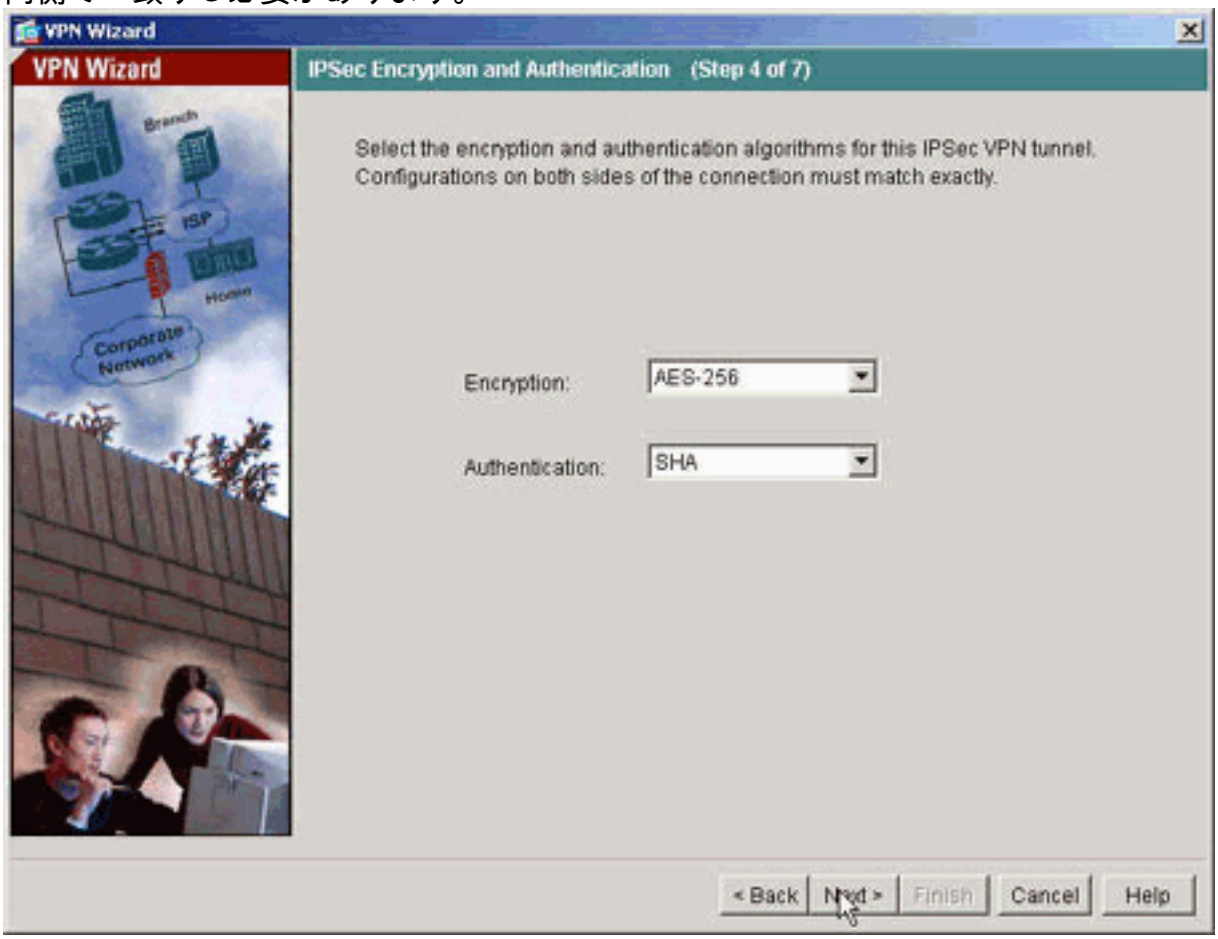
7. リモート ピアの外部 IP アドレスを指定します。 使用するために認証情報を入力して下さい（この例の事前共有キー）。



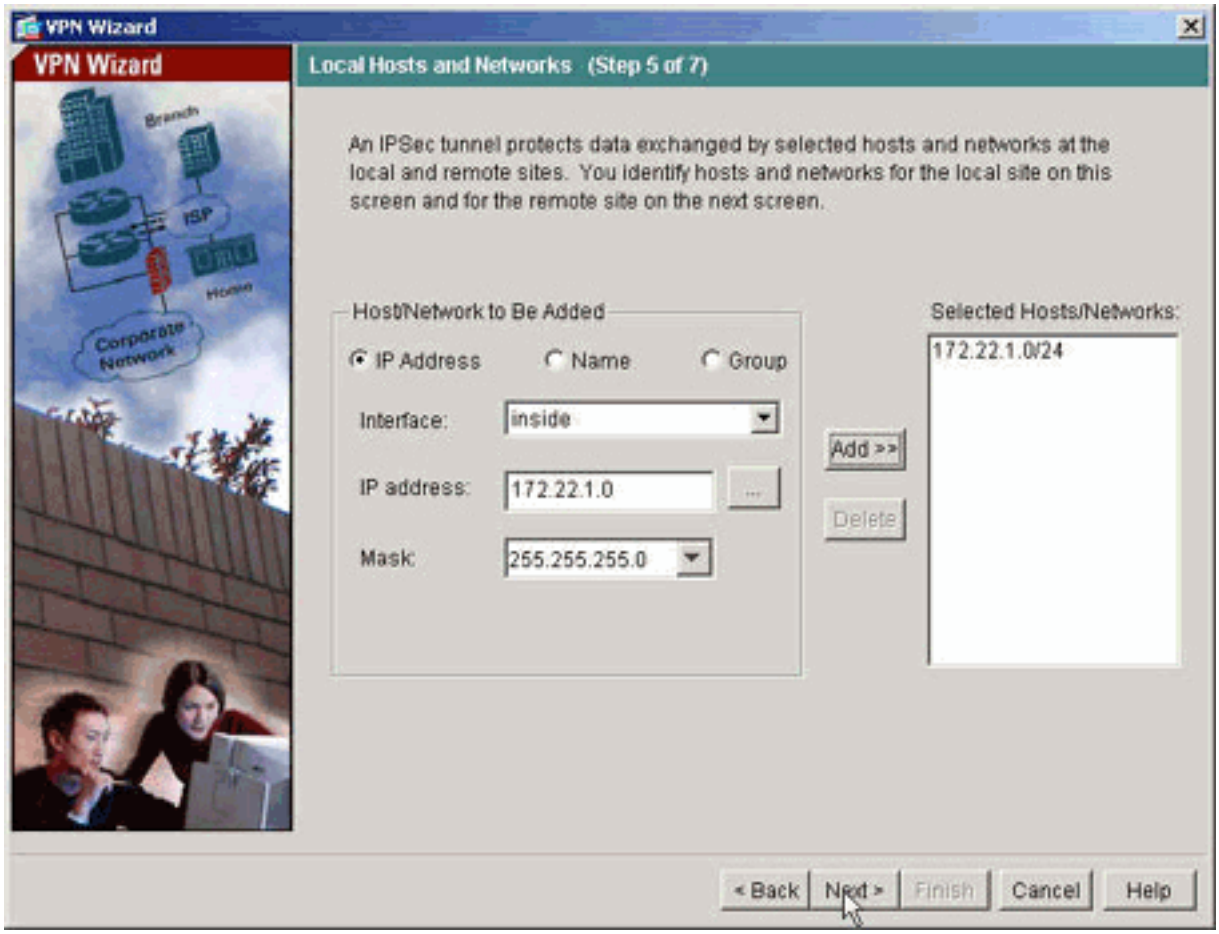
8. IKE、別名「フェーズ 1" の間使用するために属性を規定 して下さい。 これらの属性は、トンネルの両側で同じにする必要があります。



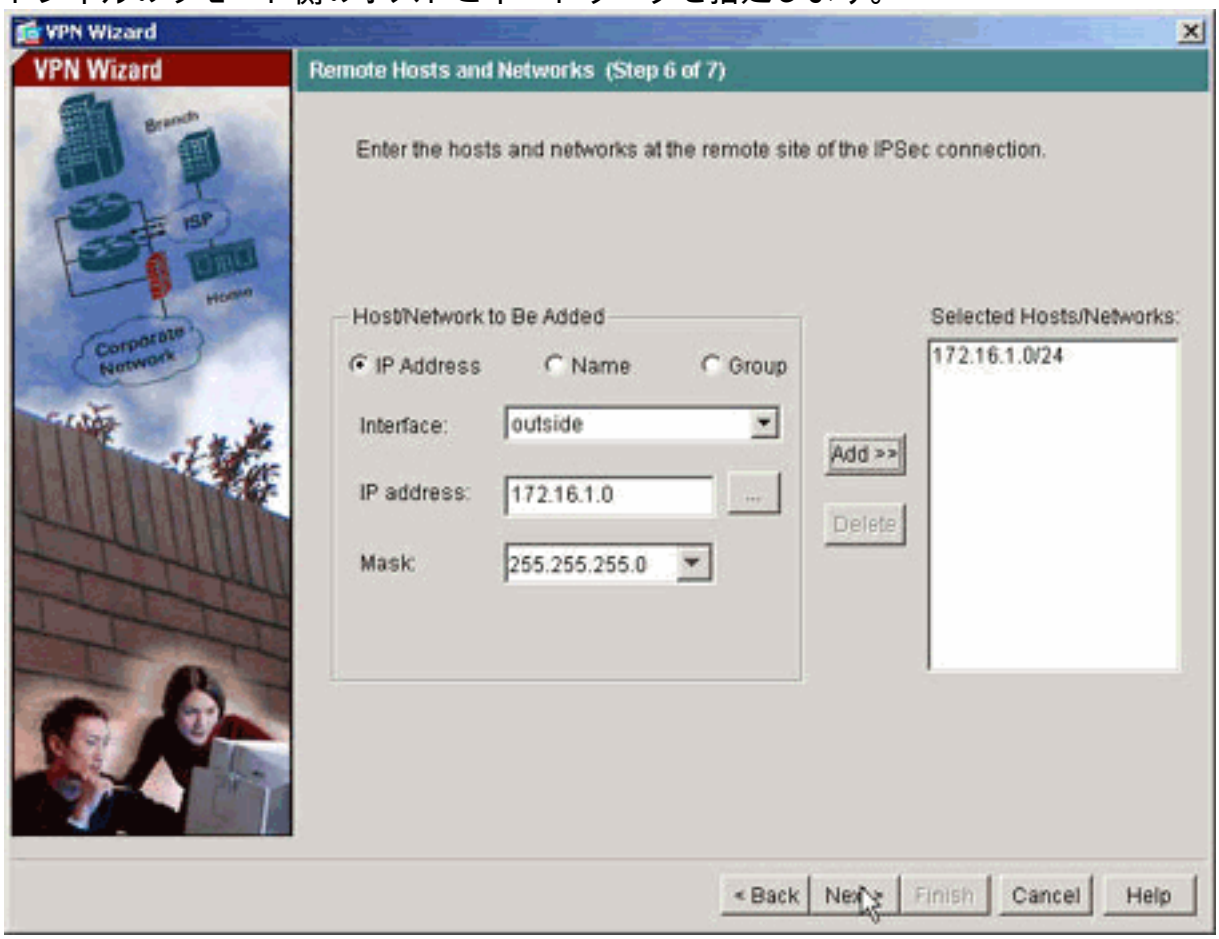
9. IPsec、別名「フェーズ 2" の間使用するために属性を規定 して下さい。 これらの属性は、両側で一致する必要があります。



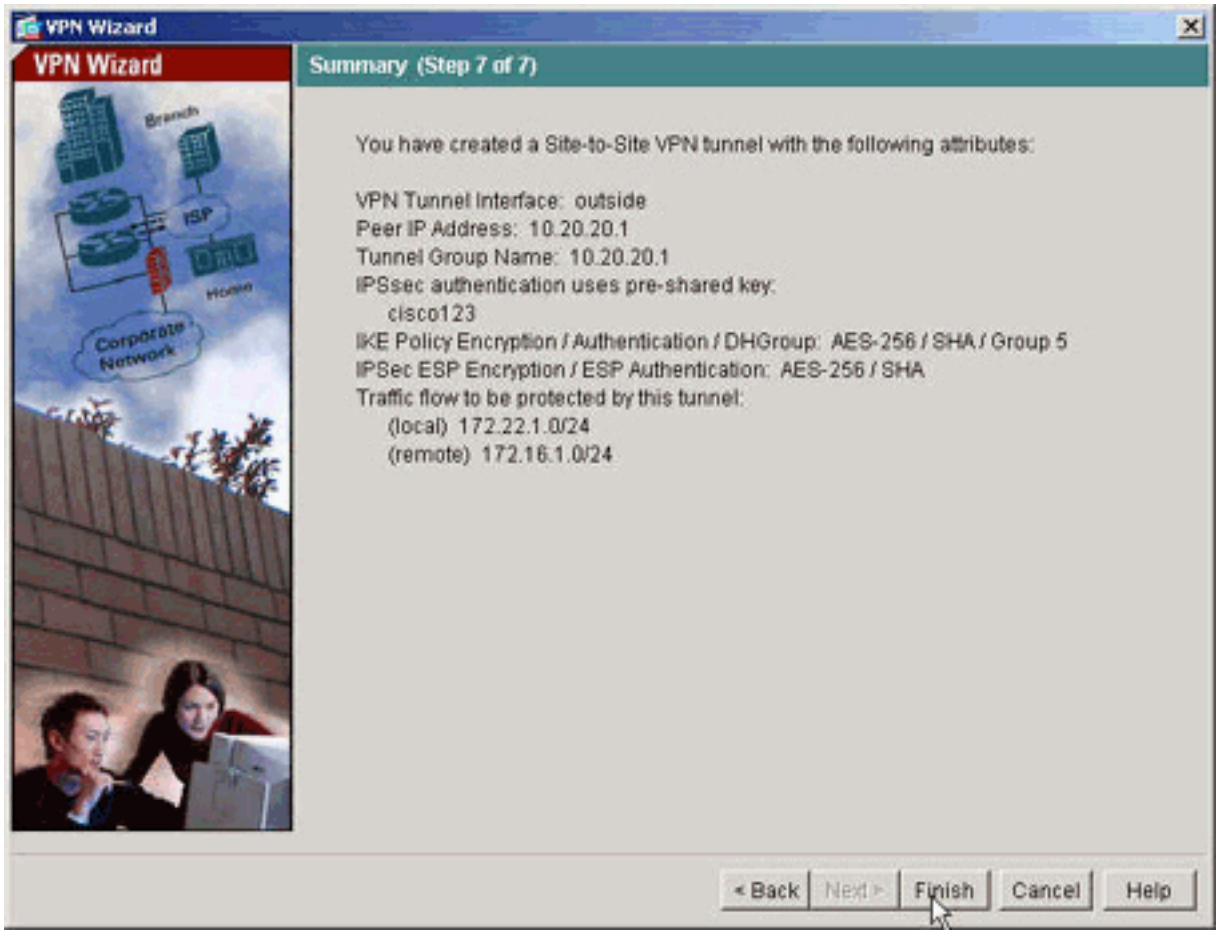
10. VPN トンネルを通過できるようなトラフィックのホストを指定します。 このステップでは、pix515-704 にローカル ホストは規定 されます。



11. トンネルのリモート側のホストとネットワークを指定します。



12. VPN Wizardによって定義された属性が、次の要約画面に表示されます。. 設定を再確認し、設定が正しいことを確認したら [Finish] をクリックします。



PIX CLI 設定

pix515-704

```
pixfirewall#show run : Saved PIX Version 7.1(1) !
hostname pixfirewall domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface Ethernet0 nameif outside security-level 0 ip
address 10.10.10.1 255.255.255.0 !--- Configure the
outside interface. ! interface Ethernet1 nameif inside
security-level 100 ip address 172.22.1.163 255.255.255.0
!--- Configure the inside interface. ! !-- Output
suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list inside_nat0_outbound
extended permit ip 172.22.1.0 255.255.255.0 172 .16.1.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used with the nat zero
command. !--- This prevents traffic which matches the
access list from undergoing !--- network address
translation (NAT). The traffic specified by this ACL is
!--- traffic that is to be encrypted and !--- sent
across the VPN tunnel. This ACL is intentionally !---
the same as (outside_cryptomap_20). !--- Two separate
access lists should always be used in this
configuration. access-list outside_cryptomap_20 extended
permit ip 172.22.1.0 255.255.255.0 172 .16.1.0
255.255.255.0 !--- This access list
(outside_cryptomap_20) is used with the crypto map !---
outside_map to determine which traffic should be
encrypted and sent !--- across the tunnel. !--- This ACL
is intentionally the same as (inside_nat0_outbound). !--
- Two separate access lists should always be used in
```

```
this configuration. pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image flash:/asdm-511.bin
!--- Enter this command to specify the location of the
ASDM image. asdm history enable arp timeout 14400 nat
(inside) 0 access-list inside_nat0_outbound !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound. route outside 0.0.0.0 0.0.0.0
10.10.10.2 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 http server enable !---
Enter this command in order to enable the HTTPS server
for ASDM. http 172.22.1.1 255.255.255.255 inside !---
Identify the IP addresses from which the security
appliance !--- accepts HTTPS connections. no snmp-server
location no snmp-server contact !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. crypto ipsec transform-set ESP-AES-
256-SHA esp-aes-256 esp-sha-hmac !--- Define the
transform set for Phase 2. crypto map outside_map 20
match address outside_cryptomap_20 !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec
peer crypto map outside_map 20 set transform-set ESP-
AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-
256-SHA" !--- to be used with the crypto map entry
"outside_map". crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- Policy 65535 is included in the config
by default. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. isakmp
enable outside isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256 isakmp policy 10
hash sha isakmp policy 10 group 5 isakmp policy 10
lifetime 86400 isakmp policy 65535 authentication pre-
share isakmp policy 65535 encryption 3des isakmp policy
65535 hash sha isakmp policy 65535 group 2 isakmp policy
65535 lifetime 86400 tunnel-group 10.20.20.1 type ipsec-
l2l !--- In order to create and manage the database of
connection-specific records !--- for ipsec-l2l–IPsec
(LAN-to-LAN) tunnels, use the tunnel-group !--- command
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer. tunnel-group 10.20.20.1 ipsec-
attributes pre-shared-key * !--- Enter the pre-shared-
key in order to configure the authentication method.
telnet timeout 5 ssh timeout 5 console timeout 0 !
class-map inspection_default match default-inspection-
traffic ! ! policy-map global_policy class
inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf : end
```

PIX-02

```
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
inside_nat0_outbound !--- ACL on pix515-704. access-list
outside_cryptomap_20 extended permit ip 172.16.1.0
255.255.255.0 172 .22.1.0 255.255.255.0 !--- Note that
this ACL is a mirror of the outside_cryptomap_20 !---
ACL on pix515-704. pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image flash:/asdm-511.bin
no asdm history enable arp timeout 14400 nat (inside) 0
access-list inside_nat0_outbound 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
http server enable http 0.0.0.0 0.0.0.0 inside no snmp-
server location no snmp-server contact crypto ipsec
transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto map outside_map 20 match address
outside_cryptomap_20 crypto map outside_map 20 set peer
10.10.10.1 crypto map outside_map 20 set transform-set
ESP-AES-256-SHA crypto map outside_map interface outside
isakmp enable outside isakmp policy 10 authentication
pre-share isakmp policy 10 encryption aes-256 isakmp
policy 10 hash sha isakmp policy 10 group 5 isakmp
policy 10 lifetime 86400 tunnel-group 10.10.10.1 type
ipsec-l2l tunnel-group 10.10.10.1 ipsec-attributes pre-
shared-key * telnet timeout 5 ssh timeout 5 console
timeout 0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map global_policy class
inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:6774691244870705f858ad4e9b810874 : end
pixfirewall#
```

バックアップ サイトツーサイト トンネル

この暗号マップエントリのバックアップ サイト間の機能に対する接続タイプを規定 するために、グローバル コンフィギュレーション モードで**クリプト マップ一定接続タイプ** コマンドを使用して下さい。 デフォルト設定に戻るためにこのコマンドの no 使用して下さい。

構文：

crypto map *map-name seq-num set* **connection-type {answer-only | originate-only | bidirectional}**

- **返事だけ**—これは接続するため適切なピアを判別するためにこのピアが最初の独自の交換の間に受信 IKE 接続にだけ最初に応答すること規定 します。
- **双方向**—これはこのピアがこの暗号マップエントリに基づいて接続を許可し、開始できること規定 します。 これはすべてのサイト間接続に対するデフォルトの接続タイプです。
- **起こだけ**—これは接続するため適切なピアを判別するためにこのピアが最初の独自の交換を始めること規定 します。

クリプト マップ一定接続タイプ コマンドはバックアップ LAN-to-LAN な 機能に対する接続タイプを規定 したものです。 それは複数のバックアップ ピアが接続の一端で規定 されることを可能にします。 この機能はこれらのプラットフォームの間でだけ動作します:

- 2 つの Cisco ASA 5500 シリーズ セキュリティ アプライアンス モデル
- Cisco ASA 5500 シリーズ セキュリティ アプライアンス モデルおよび Cisco VPN 3000 コンセントレータ
- Cisco ASA 5500 シリーズ セキュリティ アプライアンス モデルおよび Cisco PIX セキュリティ アプライアンス モデル ソフトウェア バージョン 7.0 またはそれ以降を実行するセキュリティ アプライアンス モデル

バックアップ LAN-to-LAN接続を設定するために、Cisco は起こだけ起こキーワードの接続の一端を同様に設定する、複数のバックアップ ピアでの端ことを推奨し返事キーワードと返事だけ。 起こだけ端で、同位の優先順位を整理するために**クリプト マップ set peer コマンドを**使用して下さい。 リストの最初のピアとネゴシエートする起こだけセキュリティ アプライアンス モデル試み。ピアが応答しない場合、セキュリティ アプライアンスはピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。

このように設定されたとき、起こだけピアは最初に独自のトンネルを確立し、ピアとネゴシエートすることを試みます。 その後、どちらかのピアは正常な LAN-to-LAN接続を確立、どちらかの端からのデータはトンネル接続を開始できます。

注: 暗号 エントリのためのマルチプルピア IP アドレスで VPN を設定した場合、VPN はバックアップ ピア IP とプライマリ ピアがダウン状態になれば確立されます。 しかし、プライマリ ピアが復帰しても、VPN はプライマリ IP アドレスにプリエンプションしません。 プライマリ IP アドレスに切り替えるための VPN ネゴシエーションを再び開始するには、既存の SA を手動で削除する必要があります。 結論が言うと同時に、VPN preempt はサイトツーサイト トンネルでサポートされません。

サポートされたバックアップ LAN-to-LAN接続コネクション タイプ

リモート側	中央側面
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

例

グローバル コンフィギュレーション モードで入るこの例は**クリプト マップ mymap を**設定し、起こだけに接続タイプを設定 したものです。

```
hostname(config)#crypto map outside_map 20 connection-type originate-only
```

セキュリティ アソシエーション（SA）の消去

PIX の特権 モードでは、次をコマンド使用して下さい:

- **clear [crypto] ipsec sa**：アクティブな IPSec SA を削除します。 crypto キーワードはオプションです。
- **clear [crypto] ipsec sa**：アクティブな IKE SA を削除します。 crypto キーワードはオプションです。

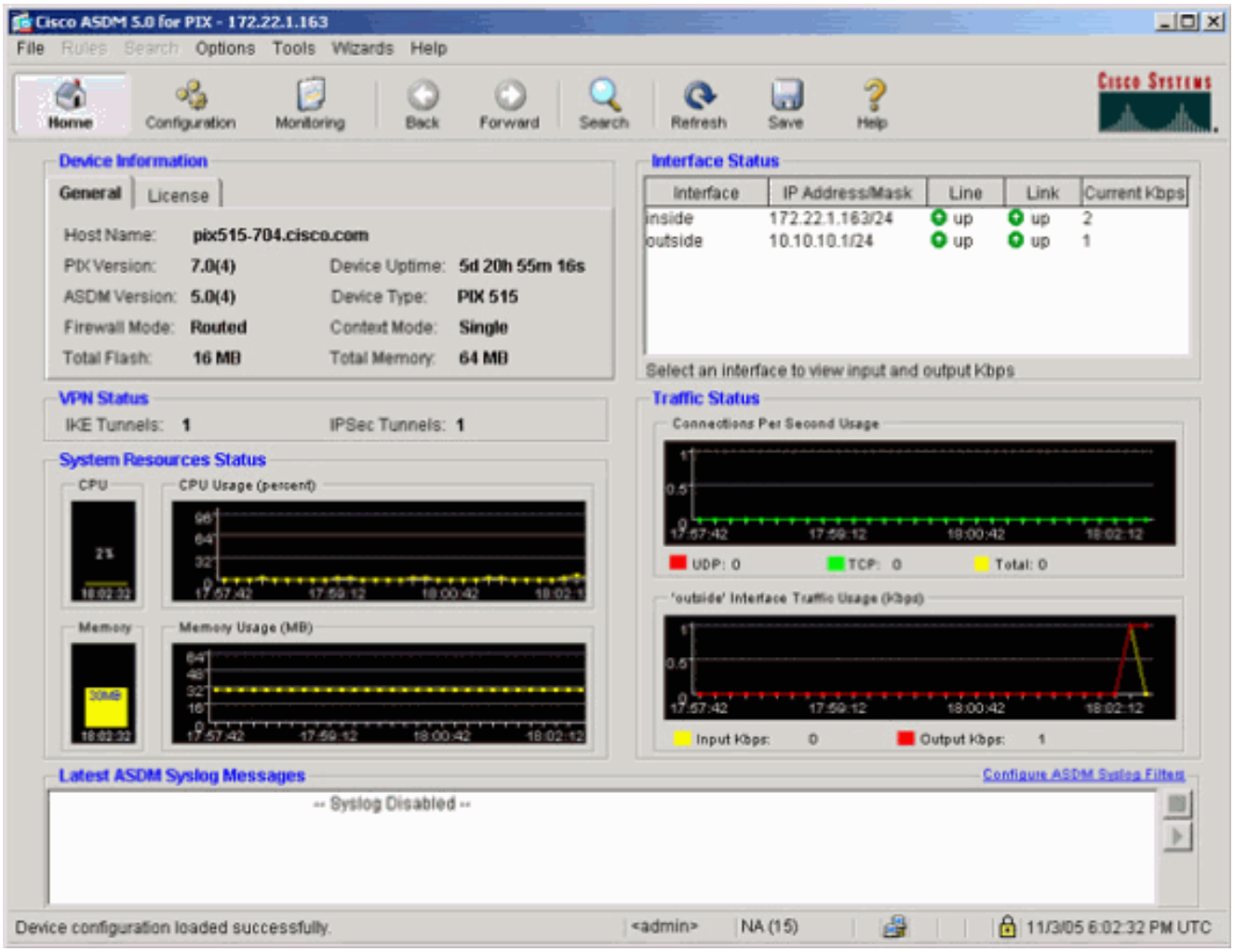
確認

ここでは、設定が正常に動作していることを確認します。

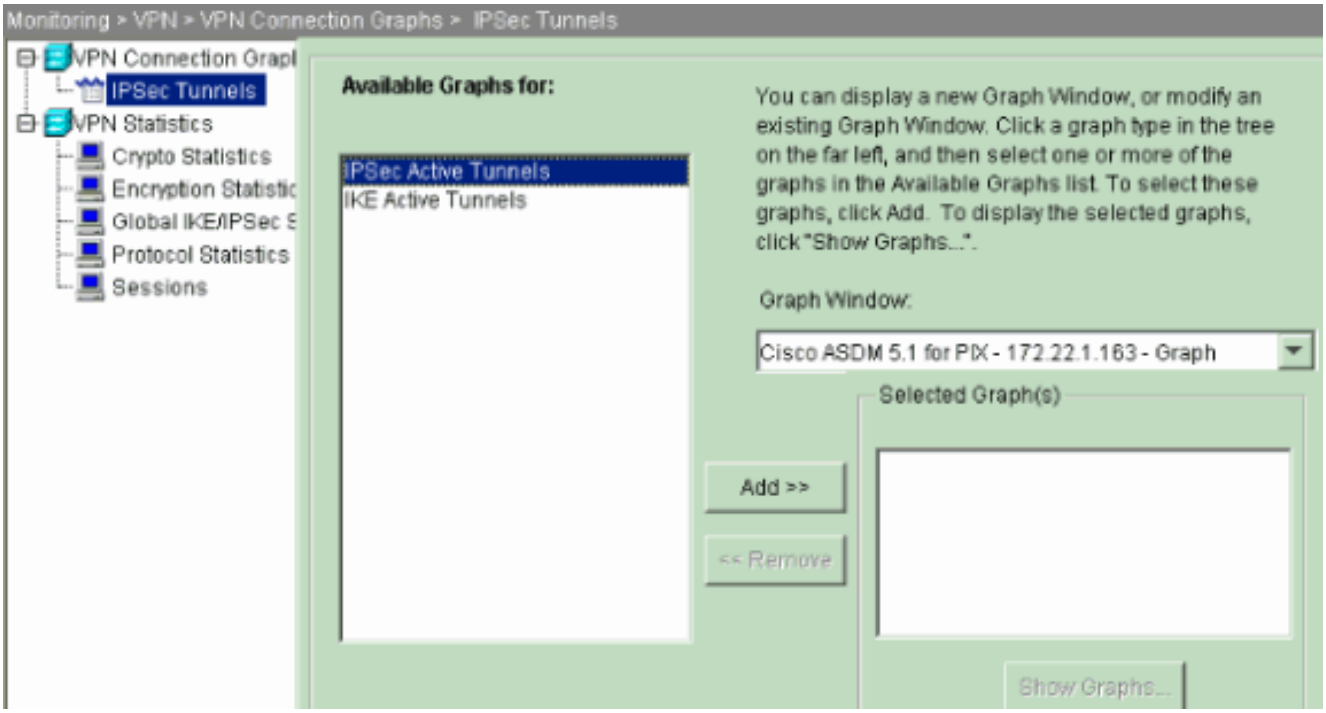
Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

関連 トラフィックがピアへある場合、トンネルは pix515-704 と PIX-02 の間で確立されます。

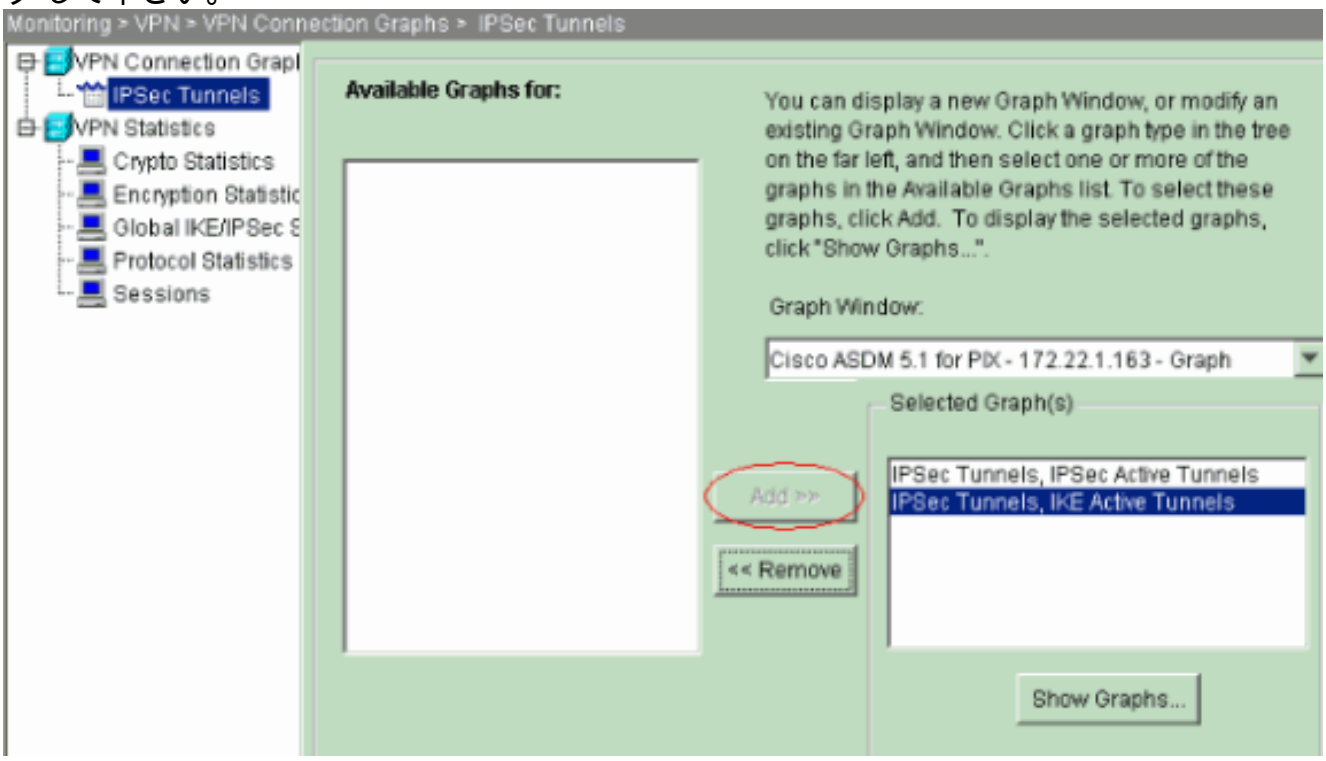
1. トンネルの形成を確認するために ASDM の**ホーム**の下で VPN ステータスを表示して下さい。



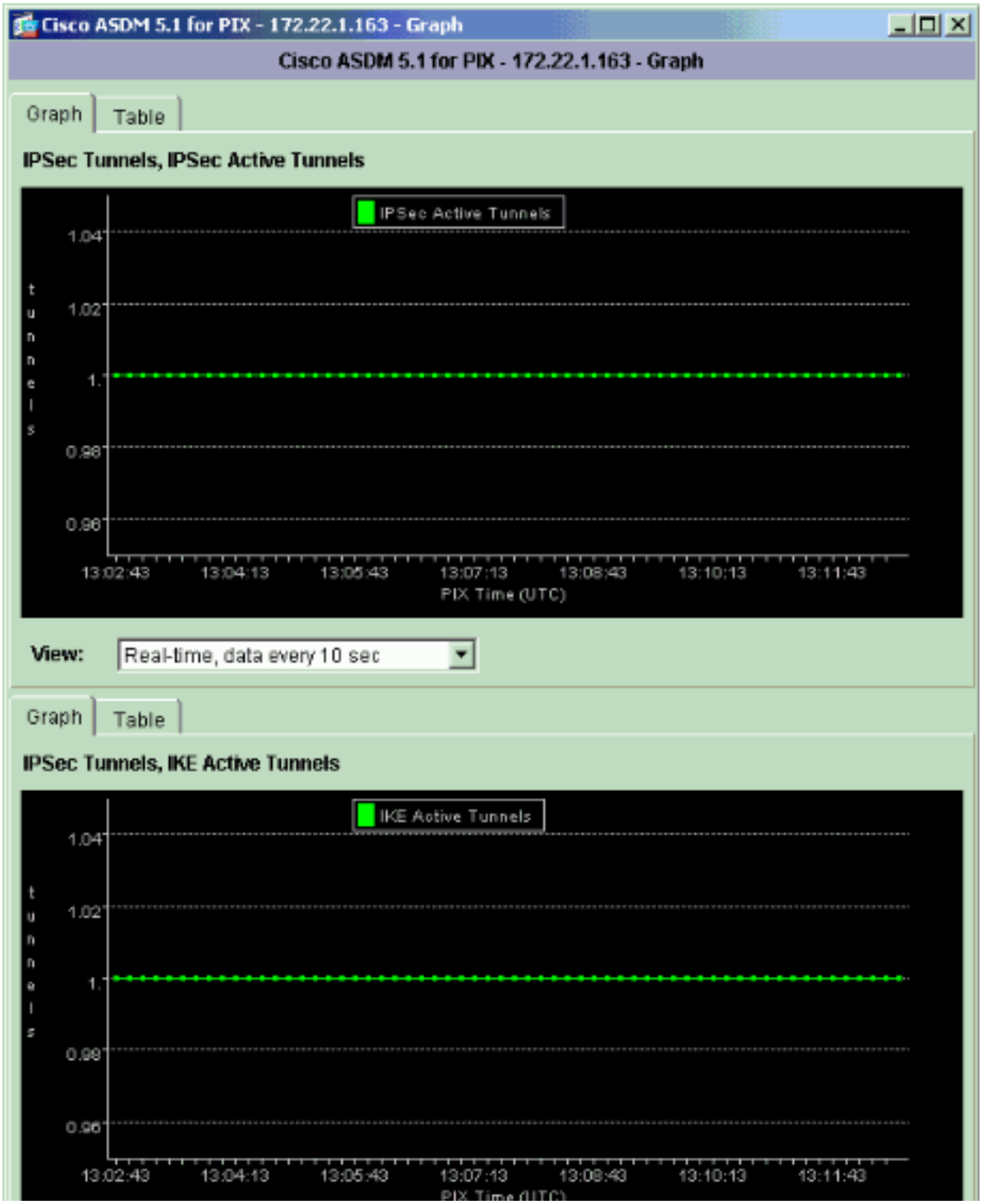
2. **> VPN > VPN 接続グラフ > IPSecトンネル** トンネル確立についての詳細を確認するために『Monitoring』 を選択 して下さい。



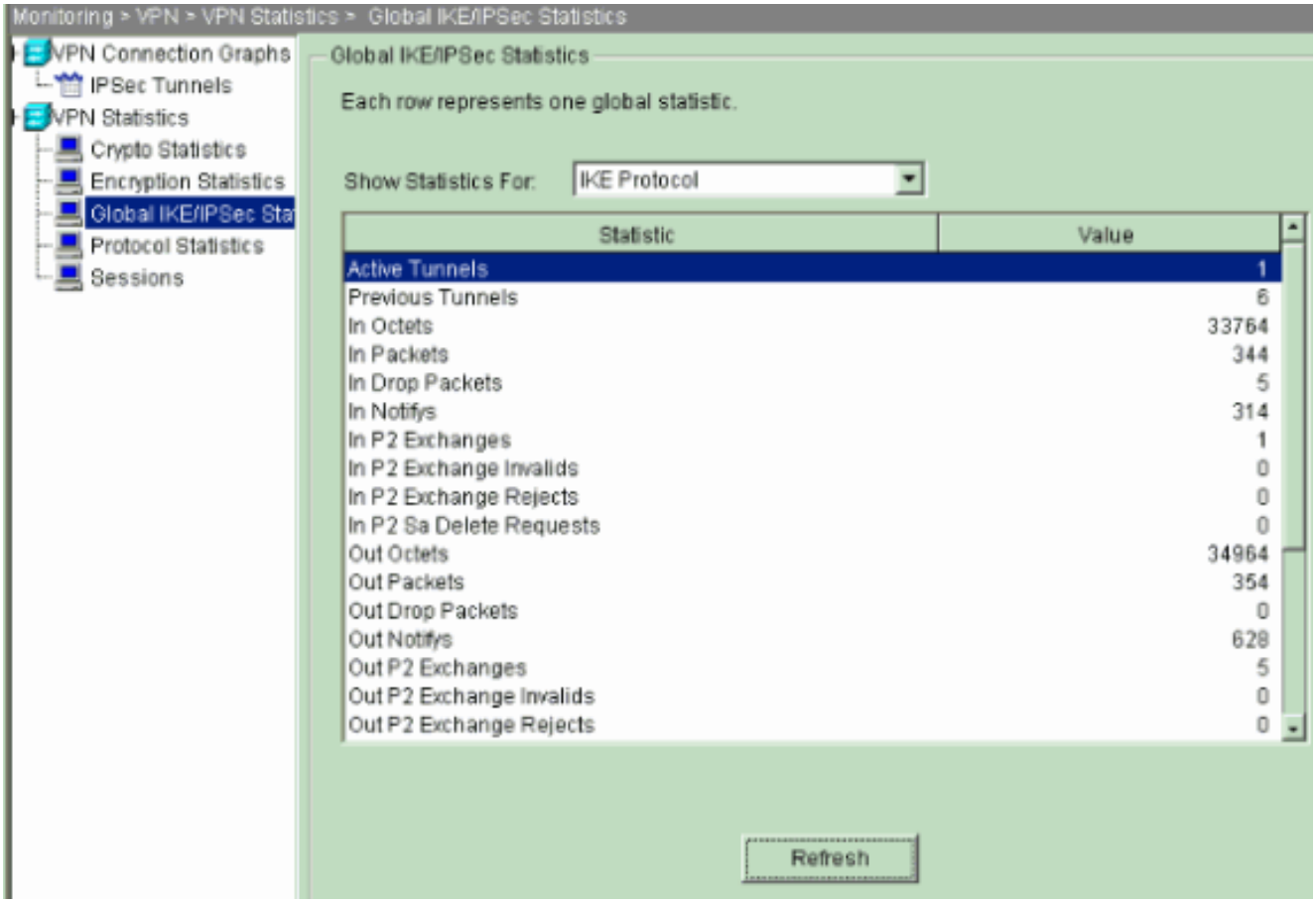
3. 利用可能 なグラフをグラフ ウィンドウで表示するために選択するために『Add』 をクリック して下さい。



4. IKE および IPsec 両方アクティブなトンネルのグラフを表示するために『Show Graphs』 をクリック して下さい。



5. **> VPN > VPN 統計情報 > グローバル な IKE/IPSec 統計情報** VPN トンネルの統計情報について確認するために『Monitoring』 を選択 して下さい。



また CLI を使用してトンネルの形成を確認できます。 暗号化されるトンネルの形成をチェックし、カプセル化される観察するパケットの数を **show crypto ipsec sa コマンドを**発行する **show crypto isakmp sa コマンドを**等発行して下さい。

pix515-704

```
pixfirewall(config)#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: 10.20.20.1
Type : L2L Role : initiator Rekey : no State : MM_ACTIVE
```

pix515-704

```
pixfirewall(config)#show crypto ipsec sa interface:
outside Crypto map tag: outside_map, seq num: 20, local
addr: 10.10.10.1 access-list outside_cryptomap_20 permit
ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0
local ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 10.20.20.1 #pkts encaps: 20, #pkts
encrypt: 20, #pkts digest: 20 #pkts decaps: 20, #pkts
decrypt: 20, #pkts verify: 20 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 20, #pkts comp
failed: 0, #pkts decomp failed: 0 #send errors: 0, #recv
errors: 0 local crypto endpt.: 10.10.10.1, remote crypto
endpt.: 10.20.20.1 path mtu 1500, ipsec overhead 76,
media mtu 1500 current outbound spi: 44532974 inbound
esp sas: spi: 0xA87AD6FA (2826622714) transform: esp-
aes-256 esp-sha-hmac in use settings ={L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (3824998/28246) IV
size: 16 bytes replay detection support: Y outbound esp
sas: spi: 0x44532974 (1146300788) transform: esp-aes-256
esp-sha-hmac in use settings ={L2L, Tunnel, } slot: 0,
conn_id: 1, crypto-map: outside_map sa timing: remaining
```

```
key lifetime (kB/sec): (3824998/28245) IV size: 16 bytes
replay detection support: Y
```

トラブルシューティング

PFS

IPSec のネゴシエーションでは、Perfect Forward Secrecy (PFS; 完全転送秘密) によって、それぞれの新しい暗号鍵が以前の鍵とは独立したものであることが保証されます。 両方のトンネルピアのイネーブルかディセーブル PFS は PIX/ASA で、他では L2L IPSecトンネル確立されません。

PFS はデフォルトでディセーブルになっています。 PFS をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **pfs** コマンドを使用します。 PFS を無効にするには、**disable** キーワードを指定します。

```
hostname(config-group-policy)#pfs {enable | disable}
```

実行コンフィギュレーションから PFS アトリビュートを削除するには、このコマンドの **no** 形式を入力します。 グループ ポリシーでは PFS に関する値を他のグループ ポリシーから継承できます。 値を継承しないようにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)#no pfs
```

管理アクセス

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。

グローバル コンフィギュレーション モードで management-access コマンドが設定されていないと、PIX の内部インターフェイスではトンネルの反対側からの ping を受信できません。

```
PIX-02(config)#management-access inside PIX-02(config)#show management-access management-access
inside
```

debug コマンド

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。

debug crypto isakmp — ディスプレイは IPSec接続についての情報をデバッグし、最初に属性の両端の非交換性が原因で否定される設定 される示します。

debug crypto isakmp

```
pixfirewall(config)#debug crypto isakmp 7 Nov 27
12:01:59 [IKEv1 DEBUG]: Pitcher: received a key acquire
message, spi 0x0 Nov 27 12:01:59 [IKEv1]: IP =
10.20.20.1, IKE Initiator: New Phase 1, Intf 2, IKE Peer
10.20.20.1 local Proxy Address 172.22.1.0, remote Proxy
Address 172.16.1.0, Crypto map (outside_map) Nov 27
12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing
ISAKMP SA payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP =
10.20.20.1, constructing Fragmentation VID + extended
capabilities payload Nov 27 12:01:59 [IKEv1]: IP =
10.20.20.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total
length : 148 Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1,
IKE_DECODE RECEIVED Message (msgid=0) with payloads :
```

HDR + SA (1) + VENDOR (13) + NONE (0) total length : 112 Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing SA payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley proposal is acceptable Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Fragmentation VID Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer included IKE fragmentation capability flags : **Main Mode**: True Aggressive Mode: True Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ke payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Cisco Unity VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing xauth V6 VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send Altiga/ Cisco VPN3000/Cisco ASA GW VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 320 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 320 Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ke payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ISA_KE payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Cisco Unity client VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received xauth V6 VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing VPN3000/ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Altiga/Cisco VPN3000/Cisco ASA GW VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating keys for Initiator... Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Computing hash for ISAKMP Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing IOS keep alive payload: proposal=32767/32767 sec. Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing dpd vid payload Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) total length : 119 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH

(8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) total length : 96 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Computing hash for ISAKMP Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing IOS keep alive payload: proposal=32767/32767 sec. Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Received DPD VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Oakley begin quick mode Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, **PHASE 1 COMPLETED** Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive type for this connection: DPD Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Starting phase 1 rekey timer: 73440000 (ms) Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, IKE got SPI from key engine: SPI = 0x44ae0956 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, oakley constucting quick mode Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing blank hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing IPSec SA payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing IPSec nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing proxy ID Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Transmitting Proxy Id: Local subnet: 172.22.1.0 mask 255.255.255.0 Protocol 0 Port 0 Remote subnet: 172.16.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing qm hash payload Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=d723766b) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=d723766b) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing SA payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, loading all IPSEC SAs Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating Quick Mode Key! Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating Quick Mode Key! Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, Security negotiation complete for LAN-to-LAN Group (10.20.20.1) Initiator, Inbound SPI = 0x44ae0956, Outbound SPI = 0x4a6429ba Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, oakley constructing final

```
quick mode Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1,
IKE_DECODE SENDING Message (msgid=d723766b) with
payloads : HDR + HASH (8) + NONE (0) total length : 76
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1, IKE got a KEY_ADD msg for SA: SPI =
0x4a6429ba Nov 27 12:02:00 [IKEv1 DEBUG]: Group =
10.20.20.1, IP = 10.20.20.1, Pitcher: received
KEY_UPDATE, spi 0x44ae0956 Nov 27 12:02:00 [IKEv1]:
Group = 10.20.20.1, IP = 10.20.20.1, Starting P2 Rekey
timer to expire in 24480 seconds Nov 27 12:02:00
[IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, PHASE 2
COMPLETED (msgid=d723766b)
```

debug crypto ipsec：IPsec 接続に関するデバッグ情報を表示します。

debug crypto ipsec

```
pix1(config)#debug crypto ipsec 7 exec mode
commands/options: <1-255> Specify an optional debug
level (default is 1) <cr> pix1(config)# debug crypto
ipsec 7 pix1(config)# IPSEC: New embryonic SA created @
0x024211B0, SCB: 0x0240AEB0, Direction: inbound SPI :
0x2A3E12BE Session ID: 0x00000001 VPIF num : 0x00000001
Tunnel type: l2l Protocol : esp Lifetime : 240 seconds
IPSEC: New embryonic SA created @ 0x0240B7A0, SCB:
0x0240B710, Direction: outbound SPI : 0xB283D32F Session
ID: 0x00000001 VPIF num : 0x00000001 Tunnel type: l2l
Protocol : esp Lifetime : 240 seconds IPSEC: Completed
host OBSA update, SPI 0xB283D32F IPSEC: Updating
outbound VPN context 0x02422618, SPI 0xB283D32F Flags:
0x00000005 SA : 0x0240B7A0 SPI : 0xB283D32F MTU : 1500
bytes VCID : 0x00000000 Peer : 0x00000000 SCB :
0x0240B710 Channel: 0x014A45B0 IPSEC: Completed outbound
VPN context, SPI 0xB283D32F VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
Rule ID: 0x01FA0290 IPSEC: New outbound permit rule, SPI
0xB283D32F Src addr: 10.10.10.1 Src mask:
255.255.255.255 Dst addr: 10.20.20.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0xB283D32F Use SPI: true IPSEC:
Completed outbound permit rule, SPI 0xB283D32F Rule ID:
0x0240AF40 IPSEC: Completed host IBSA update, SPI
0x2A3E12BE IPSEC: Creating inbound VPN context, SPI
0x2A3E12BE Flags: 0x00000006 SA : 0x024211B0 SPI :
0x2A3E12BE MTU : 0 bytes VCID : 0x00000000 Peer :
0x02422618 SCB : 0x0240AEB0 Channel: 0x014A45B0 IPSEC:
Completed inbound VPN context, SPI 0x2A3E12BE VPN
handle: 0x0240BF80 IPSEC: Updating outbound VPN context
0x02422618, SPI 0xB283D32F Flags: 0x00000005 SA :
0x0240B7A0 SPI : 0xB283D32F MTU : 1500 bytes VCID :
0x00000000 Peer : 0x0240BF80 SCB : 0x0240B710 Channel:
0x014A45B0 IPSEC: Completed outbound VPN context, SPI
0xB283D32F VPN handle: 0x02422618 IPSEC: Completed
outbound inner rule, SPI 0xB283D32F Rule ID: 0x01FA0290
IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F
Rule ID: 0x0240AF40 IPSEC: New inbound tunnel flow rule,
SPI 0x2A3E12BE Src addr: 172.16.1.0 Src mask:
255.255.255.0 Dst addr: 172.22.1.0 Dst mask:
255.255.255.0 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use
protocol: false SPI: 0x00000000 Use SPI: false IPSEC:
Completed inbound tunnel flow rule, SPI 0x2A3E12BE Rule
```

```
ID: 0x0240B108 IPSEC: New inbound decrypt rule, SPI
0x2A3E12BE Src addr: 10.20.20.1 Src mask:
255.255.255.255 Dst addr: 10.10.10.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0x2A3E12BE Use SPI: true IPSEC:
Completed inbound decrypt rule, SPI 0x2A3E12BE Rule ID:
0x02406E98 IPSEC: New inbound permit rule, SPI
0x2A3E12BE Src addr: 10.20.20.1 Src mask:
255.255.255.255 Dst addr: 10.10.10.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0x2A3E12BE Use SPI: true IPSEC:
Completed inbound permit rule, SPI 0x2A3E12BE Rule ID:
0x02422C78
```

関連情報

- PDM を使用したファイアウォール間の冗長トンネルの作成
- Cisco PIX Firewall ソフトウェア
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- 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（RFC）
- テクニカルサポートとドキュメント - Cisco Systems