PIX/ASA 7.x und höher: Konfigurationsbeispiel eines PIX-zu-PIX-VPN-Tunnels

Inhalt

Einführung

Dieses Dokument beschreibt das Verfahren zur Konfiguration von VPN-Tunneln zwischen zwei PIX-Firewalls mithilfe des Cisco Adaptive Security Device Manager (ASDM). ASDM ist ein anwendungsbasiertes Konfigurationstool, das Sie beim Einrichten, Konfigurieren und Überwachen Ihrer PIX-Firewall über eine grafische Benutzeroberfläche unterstützt. PIX-Firewalls werden an zwei verschiedenen Standorten platziert.

Ein Tunnel wird mithilfe von IPsec gebildet. IPsec ist eine Kombination offener Standards, die Datensicherheit, Datenintegrität und Datenursprungsauthentifizierung zwischen IPsec-Peers bieten.

Hinweis: In PIX 7.1 und höher wird der Befehl **sysopt connection permit-ipsec** in **sysopt connection permit-vpn** geändert. Mit diesem Befehl kann Datenverkehr, der über einen VPN-Tunnel in die Security Appliance gelangt und anschließend entschlüsselt wird, Schnittstellenzugriffslisten umgehen. Für den Datenverkehr gelten weiterhin Gruppenrichtlinien und Zugriffskontrolllisten für einzelne Benutzer. Um diese Funktion zu deaktivieren, verwenden Sie die **no-**Form dieses Befehls. Dieser Befehl wird in der CLI-Konfiguration nicht angezeigt.

Siehe PIX 6.x: Einfaches PIX-zu-PIX VPN-Tunnel-Konfigurationsbeispiel, um mehr über dasselbe Szenario zu erfahren, in dem die Cisco PIX Security Appliance die Softwareversion 6.x ausführt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument geben an, dass dieser Peer den ersten firmeneigenen Austausch initiiert, um den passenden Peer zu bestimmen, mit dem eine Verbindung hergestellt werden soll.

- Cisco Security Appliance der Serie PIX 500 mit Version 7.x und höher
- ASDM Version 5.x.x und höher

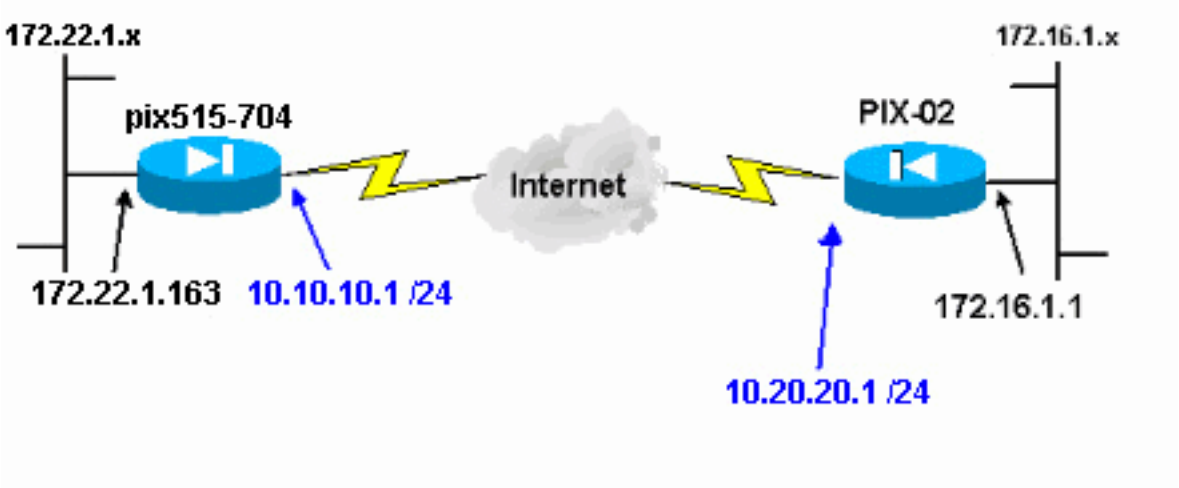
Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

Hinweis: Auf der ASA 5500-Serie, Version 7.x/8.x, wird die gleiche Software ausgeführt wie in PIX-Version 7.x/8.x. Die Konfigurationen in diesem Dokument gelten für beide Produktlinien.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Die IPsec-Aushandlung kann in fünf Schritte unterteilt werden und umfasst zwei IKE-Phasen (Internet Key Exchange).

1. Ein IPsec-Tunnel wird durch interessanten Datenverkehr initiiert. Datenverkehr gilt als interessant, wenn er zwischen den IPsec-Peers übertragen wird.
2. In IKE Phase 1 handeln die IPsec-Peers die etablierte IKE Security Association (SA)-Richtlinie aus. Nach der Authentifizierung der Peers wird ein sicherer Tunnel mithilfe von Internet Security Association und Key Management Protocol (ISAKMP) erstellt.
3. In IKE Phase 2 verwenden die IPsec-Peers den authentifizierten und sicheren Tunnel, um IPsec-SA-Transformationen auszuhandeln. Die Aushandlung der freigegebenen Richtlinie bestimmt, wie der IPsec-Tunnel eingerichtet wird.
4. Der IPsec-Tunnel wird erstellt, und Daten werden zwischen den IPsec-Peers übertragen, basierend auf den in den IPsec-Transformationssätzen konfigurierten IPsec-Parametern.
5. Der IPsec-Tunnel endet, wenn die IPsec-SAs gelöscht werden oder ihre Lebensdauer abläuft.**Hinweis:** Die IPsec-Aushandlung zwischen den beiden PIXs schlägt fehl, wenn die SAs in beiden IKE-Phasen auf den Peers nicht übereinstimmen.

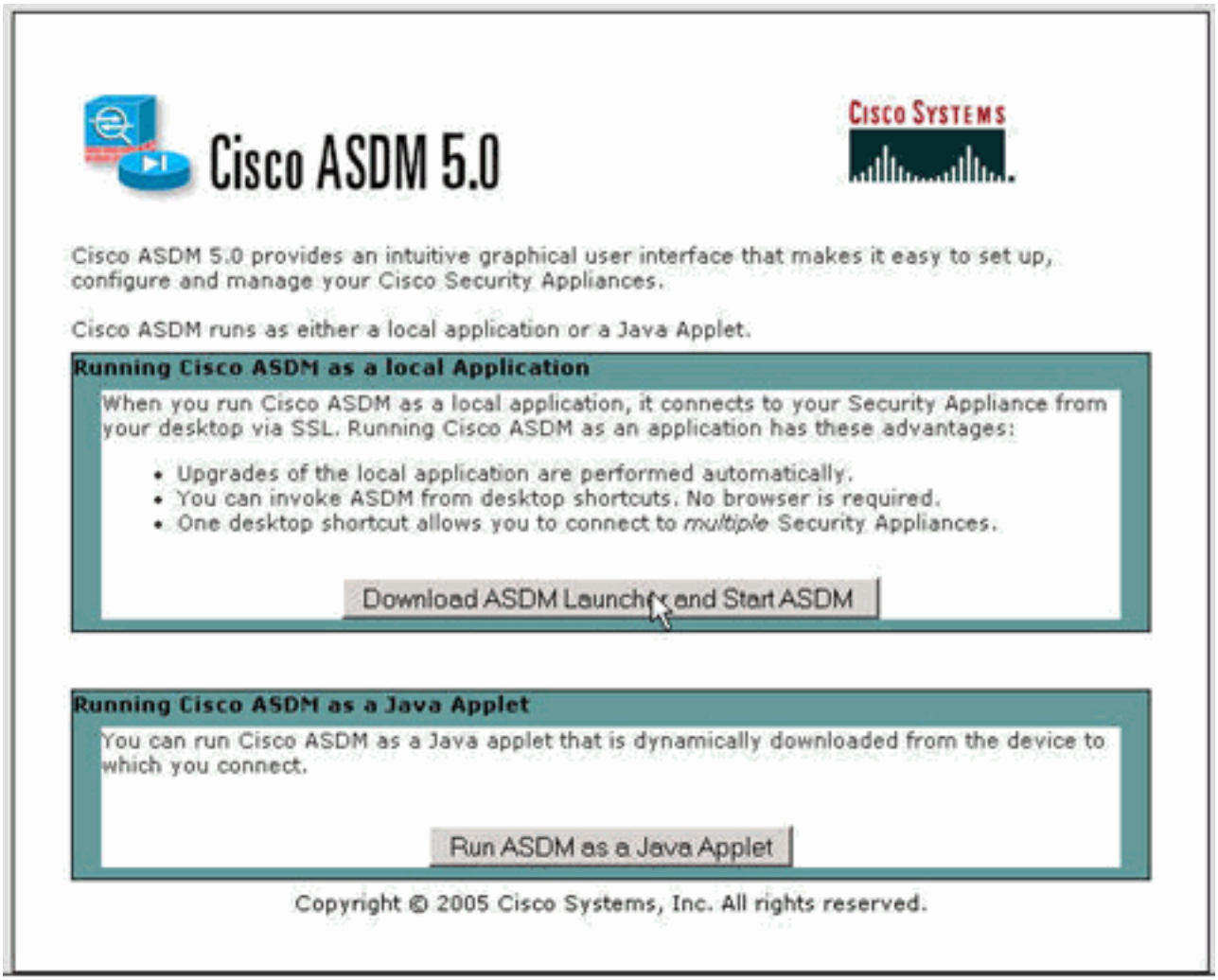
Konfiguration

- ASDM-Konfiguration
- PIX CLI-Konfigurationen

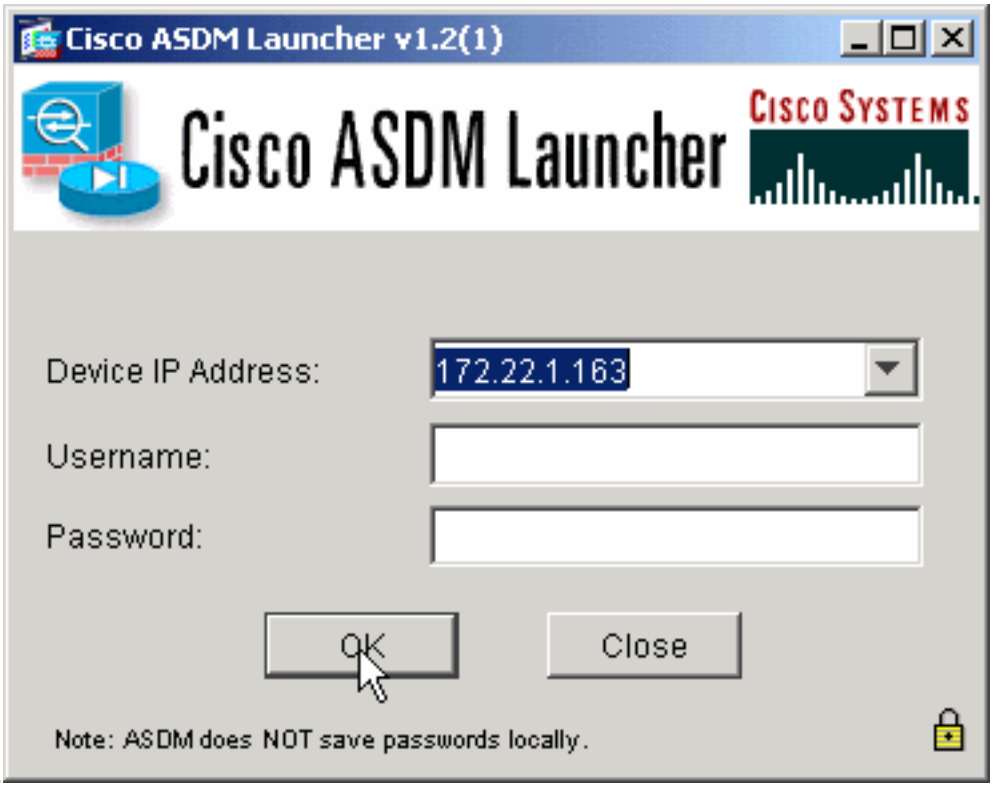
ASDM-Konfiguration

Gehen Sie wie folgt vor:

1. Öffnen Sie Ihren Browser, und geben Sie **https://<Inside_IP_Address_of_PIX>** ein, um auf das ASDM auf dem PIX zuzugreifen.Achten Sie darauf, alle Warnungen zu autorisieren, die Ihr Browser bezüglich der Authentizität von SSL-Zertifikaten ausgibt. Standardmäßig sind Benutzername und Kennwort leer.Das PIX zeigt dieses Fenster an, um den Download der ASDM-Anwendung zu ermöglichen. In diesem Beispiel wird die Anwendung auf den lokalen Computer geladen und nicht in einem Java-Applet
ausgeführt.

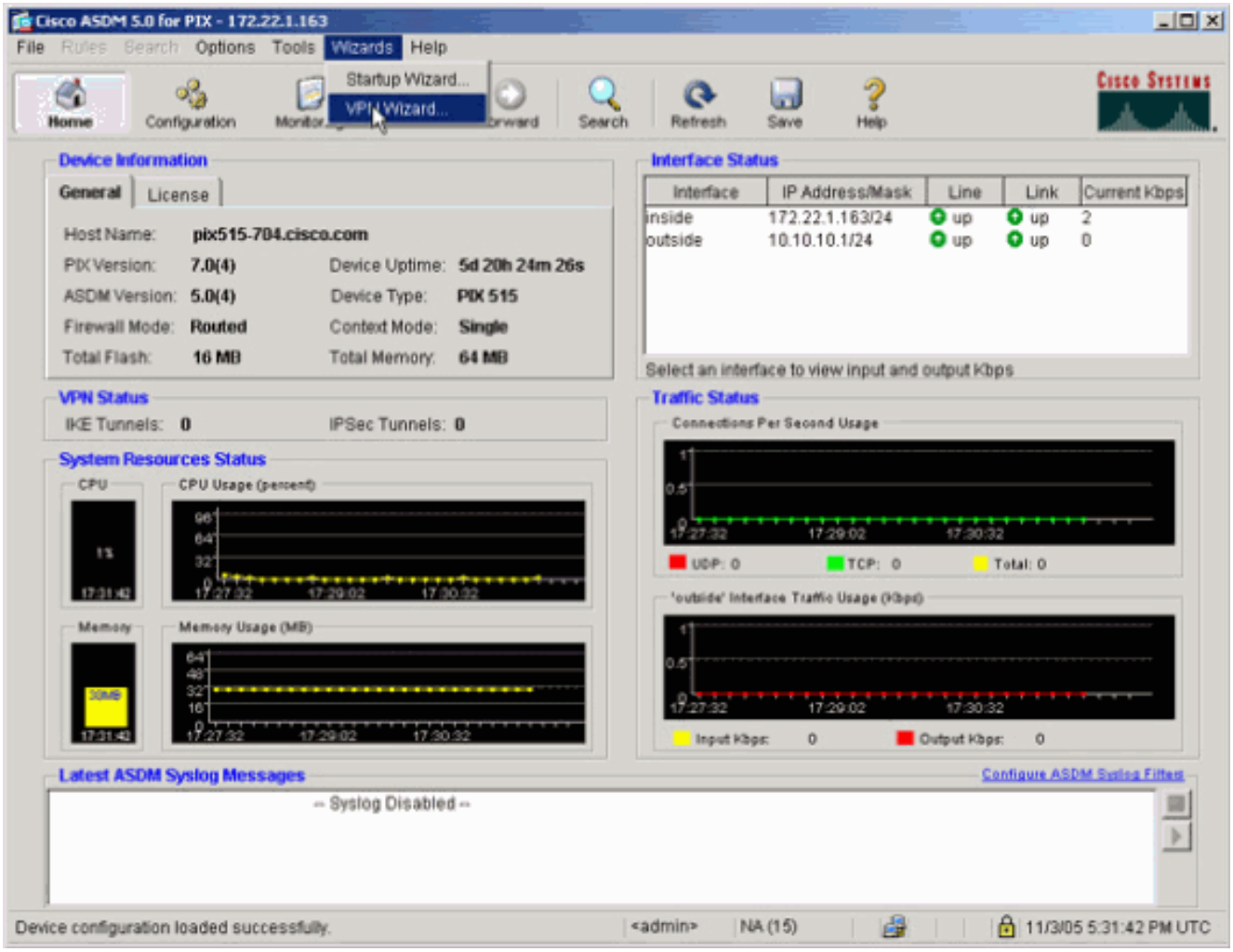


2. Klicken Sie auf **ASDM Launcher herunterladen und ASDM starten**, um das Installationsprogramm für die ASDM-Anwendung herunterzuladen.
3. Wenn der ASDM Launcher heruntergeladen wurde, folgen Sie den Anweisungen, um die Software zu installieren und den Cisco ASDM Launcher auszuführen.
4. Geben Sie die IP-Adresse für die Schnittstelle ein, die Sie mit dem Befehl **http** konfiguriert haben, sowie einen Benutzernamen und ein Kennwort, wenn Sie einen Befehl angegeben haben.In diesem Beispiel werden ein leerer Benutzername und ein leeres Kennwort

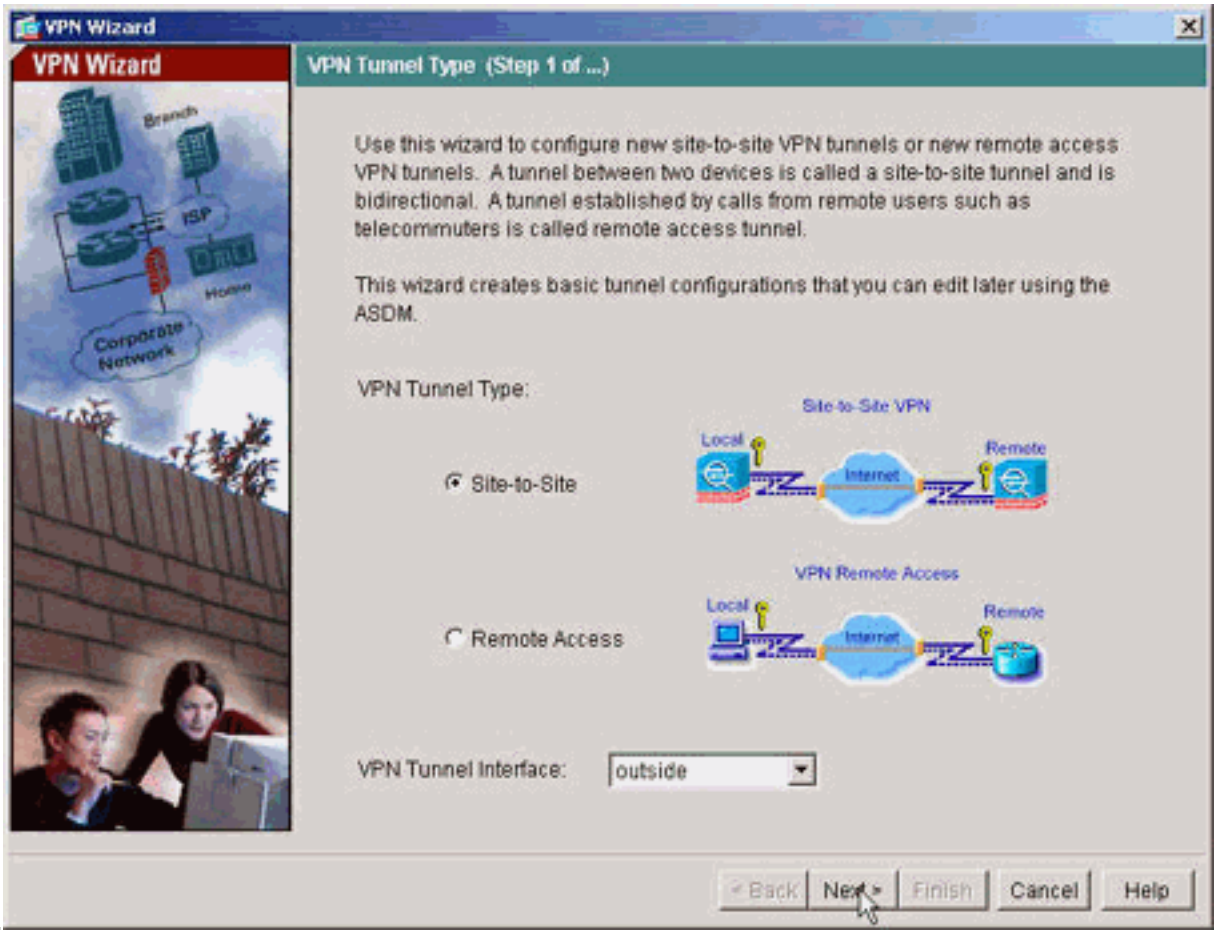


verwendet.

5. Führen Sie den VPN-Assistenten aus, sobald die ASDM-Anwendung eine Verbindung mit dem PIX
herstellt.

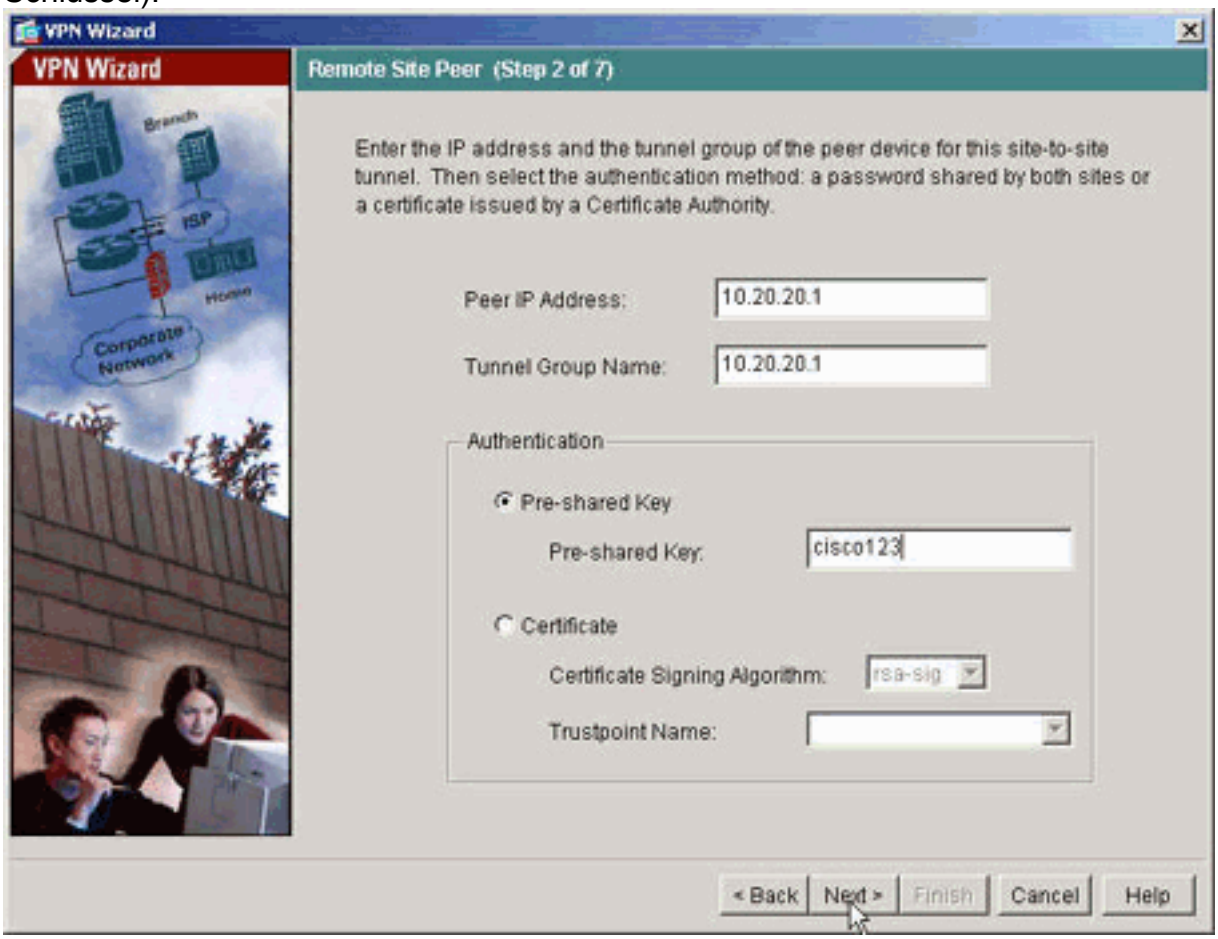


6. Wählen Sie den **Site-to-Site**-VPN-Tunneltyp



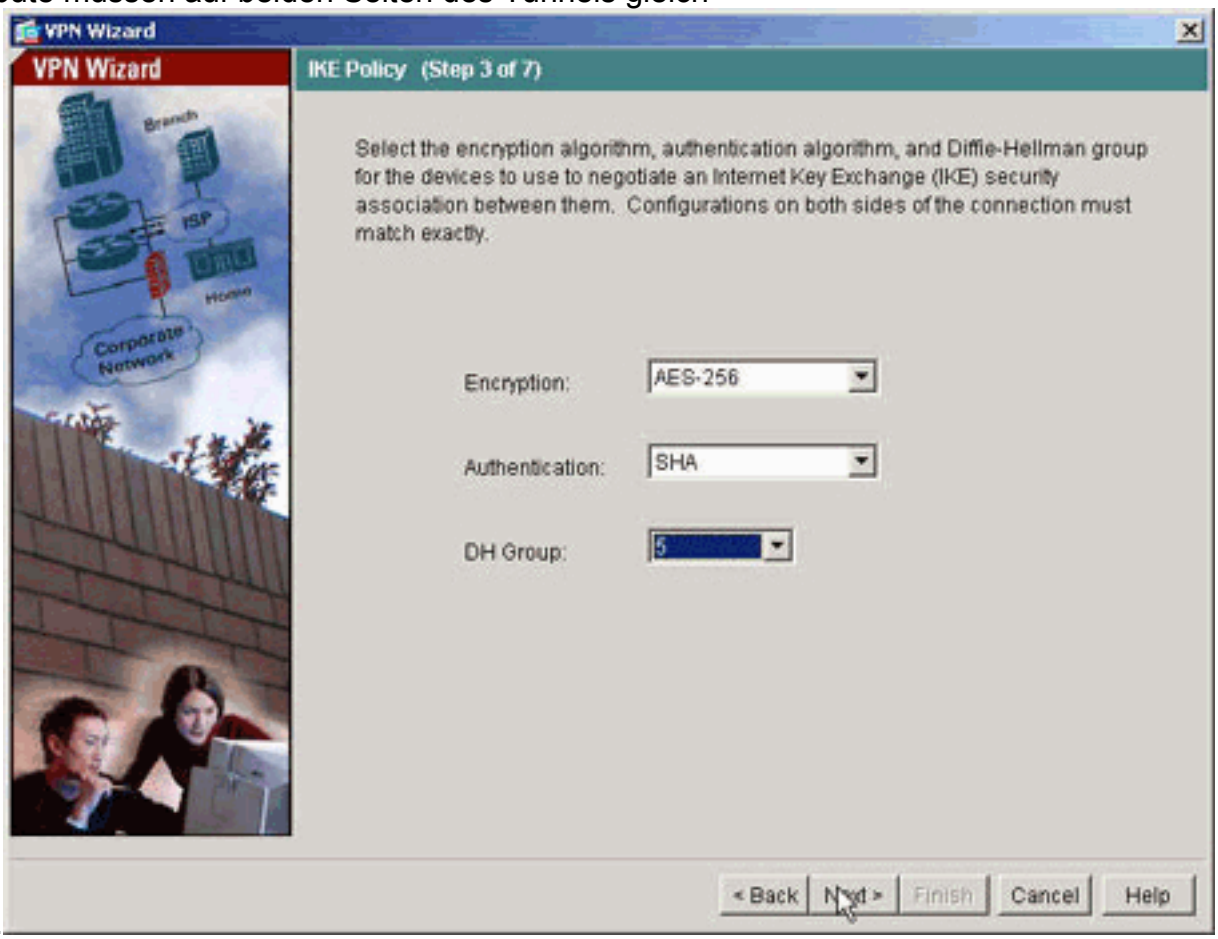
aus.

7. Geben Sie die externe IP-Adresse des Remote-Peers an. Geben Sie die zu verwendenden Authentifizierungsinformationen ein (in diesem Beispiel einen vorinstallierten Schlüssel).

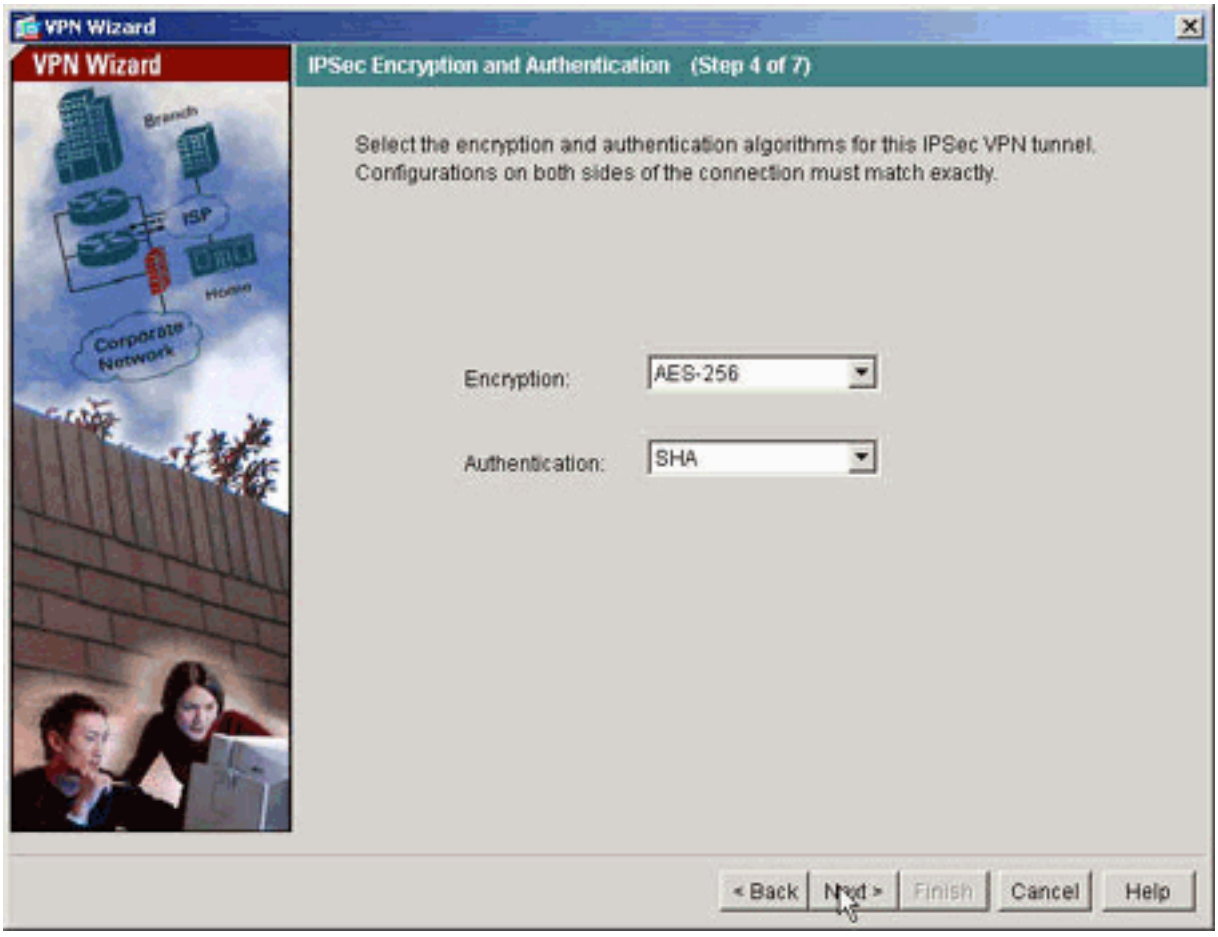


8. Geben Sie die Attribute für IKE an, die auch als "Phase 1" bezeichnet werden. Diese

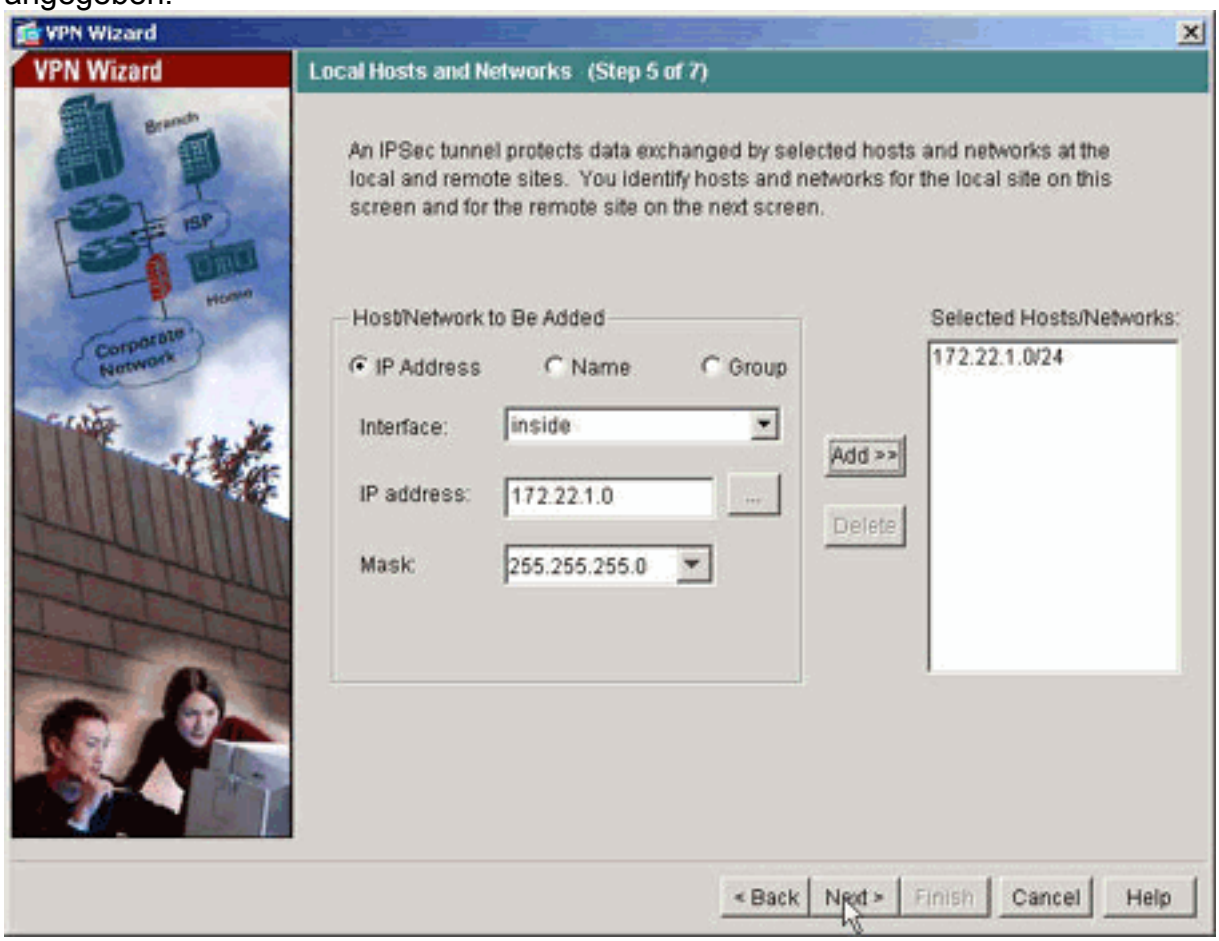
Attribute müssen auf beiden Seiten des Tunnels gleich sein.



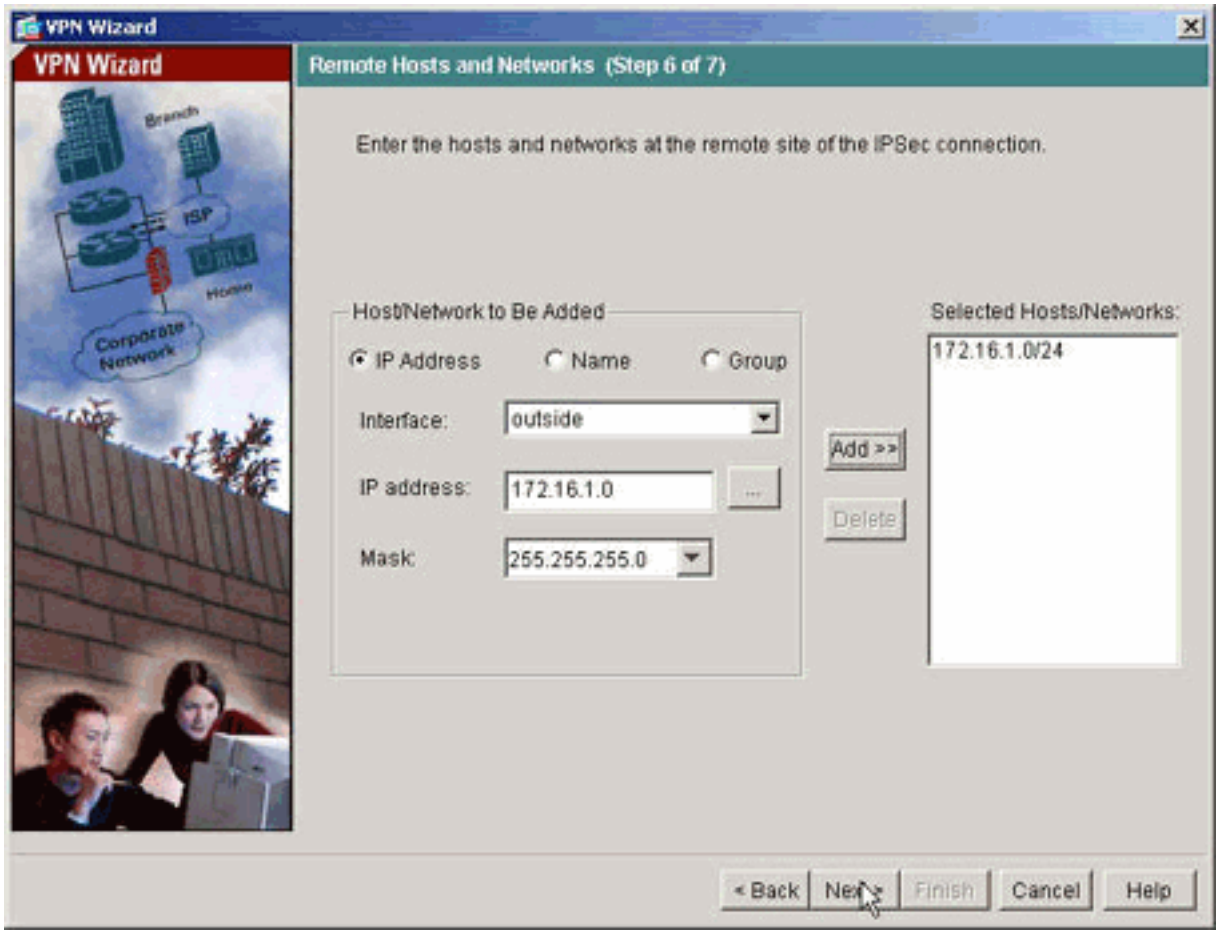
9. Geben Sie die Attribute an, die für IPsec verwendet werden sollen. Dies wird auch als "Phase 2" bezeichnet. Diese Attribute müssen auf beiden Seiten übereinstimmen.



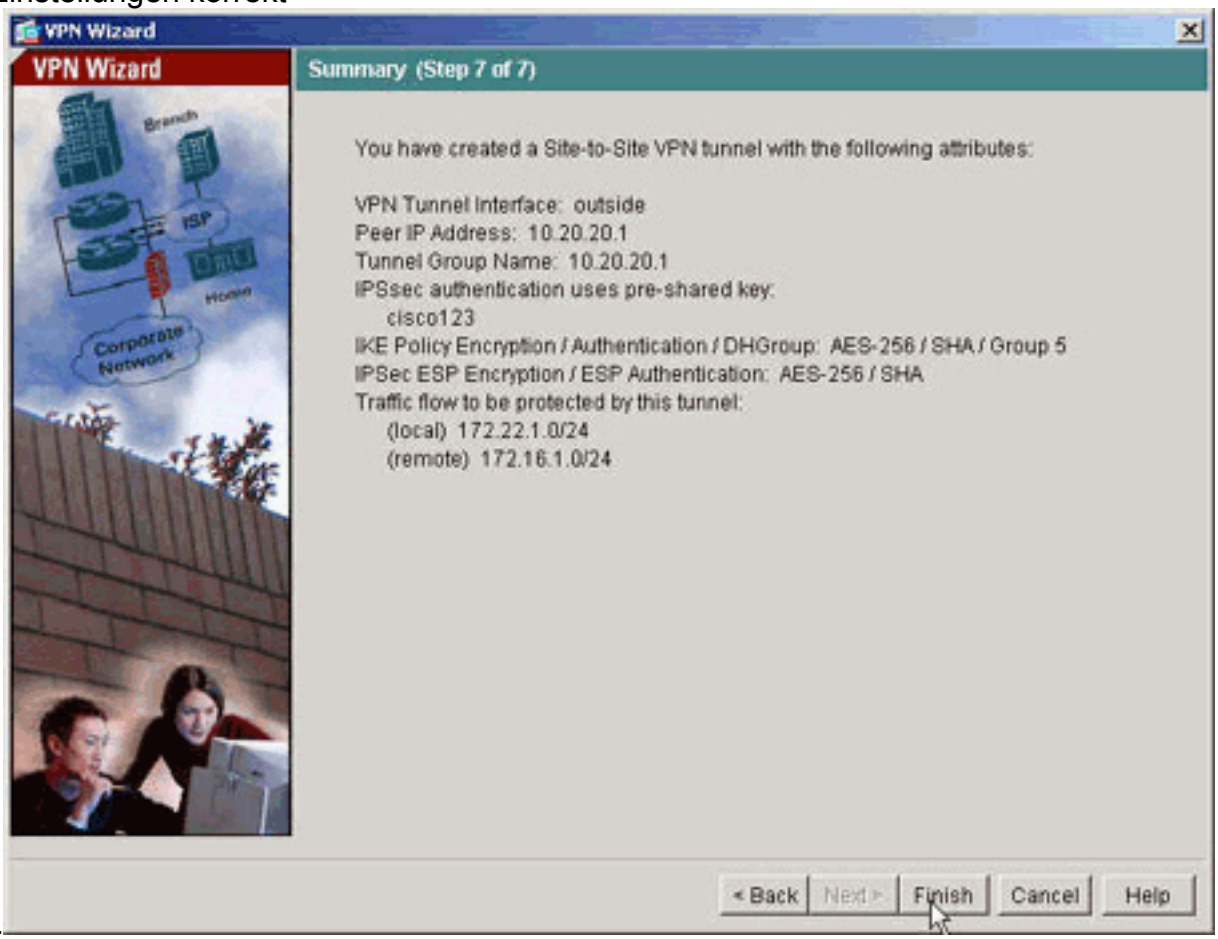
10. Geben Sie die Hosts an, deren Datenverkehr den VPN-Tunnel passieren darf. In diesem Schritt werden die lokalen Hosts für pix515-704 angegeben.



11. Die Hosts und Netzwerke auf der Remote-Seite des Tunnels werden angegeben.



12. Die vom VPN-Assistenten definierten Attribute werden in dieser Zusammenfassung angezeigt. Überprüfen Sie die Konfiguration erneut, und klicken Sie auf **Fertig stellen**, wenn die Einstellungen korrekt sind.



PIX CLI-Konfiguration

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#
```

Backup Site-to-Site-Tunnel

Um den Verbindungstyp für die Backup Site-to-Site-Funktion für diesen Crypto Map-Eintrag anzugeben, verwenden Sie den Befehl **crypto map set connection-type** im globalen Konfigurationsmodus. Verwenden Sie die `no`-Form dieses Befehls, um zur Standardeinstellung zurückzukehren.

Syntax:

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

- **response-only**: Dieser Peer gibt an, dass eingehender IKE-Verbindungen erst beim ersten proprietären Austausch beantwortet werden, um den passenden Peer zu bestimmen, mit dem eine Verbindung hergestellt werden soll.
- **bidirektional** - Dieser Parameter gibt an, dass dieser Peer Verbindungen basierend auf diesem Crypto Map-Eintrag akzeptieren und erstellen kann. Dies ist der Standardverbindungstyp für alle Site-to-Site-Verbindungen.
- **originate-only** (Nur Originate): Dieser Peer gibt an, dass er den ersten proprietären Austausch initiiert, um den passenden Peer zu bestimmen, mit dem eine Verbindung hergestellt werden soll.

Der Befehl **crypto map set connection-type** gibt die Verbindungstypen für die Funktion Backup

LAN-to-LAN an. Es ermöglicht die Angabe mehrerer Backup-Peers an einem Ende der Verbindung. Diese Funktion funktioniert nur zwischen diesen Plattformen:

- Zwei Cisco Security Appliances der Serie ASA 5500
- Cisco Security Appliance der Serie ASA 5500 und Cisco VPN 3000 Concentrator
- Cisco Security Appliance der Serie ASA 5500 und eine Security Appliance, die Cisco PIX Security Appliance Software 7.0 oder höher ausführt

Um eine Backup-LAN-zu-LAN-Verbindung zu konfigurieren, empfiehlt Cisco, ein Ende der Verbindung als Nur-Ausgangspunkt mit dem `Original-`Schlüsselwort und das Ende mit mehreren Backup-Peers als Antwort-only mit dem `Nur-Antwort-`Schlüsselwort zu konfigurieren. Verwenden Sie am ursprünglichen Ende den Befehl **crypto map set peer**, um die Priorität der Peers anzuordnen. Die ursprüngliche Sicherheits-Appliance versucht, mit dem ersten Peer in der Liste zu verhandeln. Wenn dieser Peer nicht antwortet, arbeitet die Security Appliance in der Liste nach unten, bis entweder ein Peer antwortet oder keine Peers mehr in der Liste vorhanden sind.

Bei einer solchen Konfiguration versucht der ursprüngliche Peer zunächst, einen proprietären Tunnel einzurichten und mit einem Peer zu verhandeln. Danach kann jeder Peer eine normale LAN-zu-LAN-Verbindung herstellen, und die Tunnelverbindung kann durch Daten von beiden Enden initiiert werden.

Hinweis: Wenn Sie VPN mit mehreren Peer-IP-Adressen für einen Verschlüsselungseintrag konfiguriert haben, wird das VPN mit der Backup-Peer-IP eingerichtet, sobald der primäre Peer ausfällt. Sobald der primäre Peer wiederhergestellt ist, wird die primäre IP-Adresse vom VPN jedoch nicht vorbelegt. Sie müssen die vorhandene SA manuell löschen, um die VPN-Aushandlung erneut zu initiieren und auf die primäre IP-Adresse umzustellen. Wie die Schlussfolgerung besagt, wird die VPN-Freischaltung im Site-to-Site-Tunnel nicht unterstützt.

Unterstützte Backup LAN-to-LAN-Verbindungstypen

Remote-Seite	Mittelseite
`Originate-Only`	`Answer-Only`
`Bi-Directional`	`Answer-Only`
`Bi-Directional`	`Bi-Directional`

Beispiel

In diesem Beispiel, das im globalen Konfigurationsmodus eingegeben wird, wird die **Crypto Map mymap** konfiguriert und der Verbindungstyp auf *Nur-Originate* festgelegt.

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

Clear Security Associations (SAs)

Verwenden Sie im privilegierten Modus des PIX die folgenden Befehle:

- **clear [crypto] ipsec sa**: Löscht die aktiven IPsec-SAs. Das Schlüsselwort *crypto* ist optional.
- **clear [crypto] isakmp sa**: Löscht die aktiven IKE-SAs. Das Schlüsselwort *crypto* ist optional.

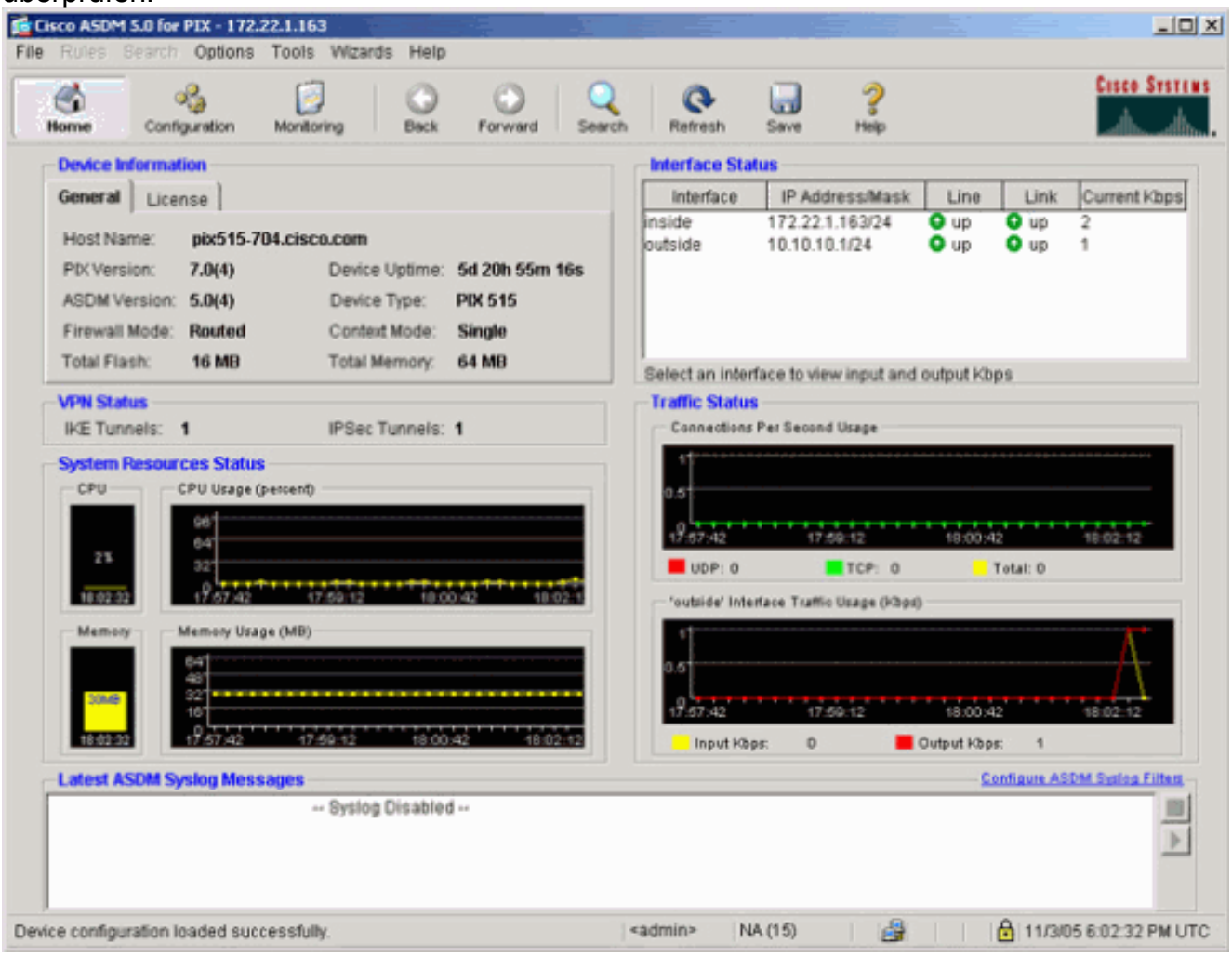
Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

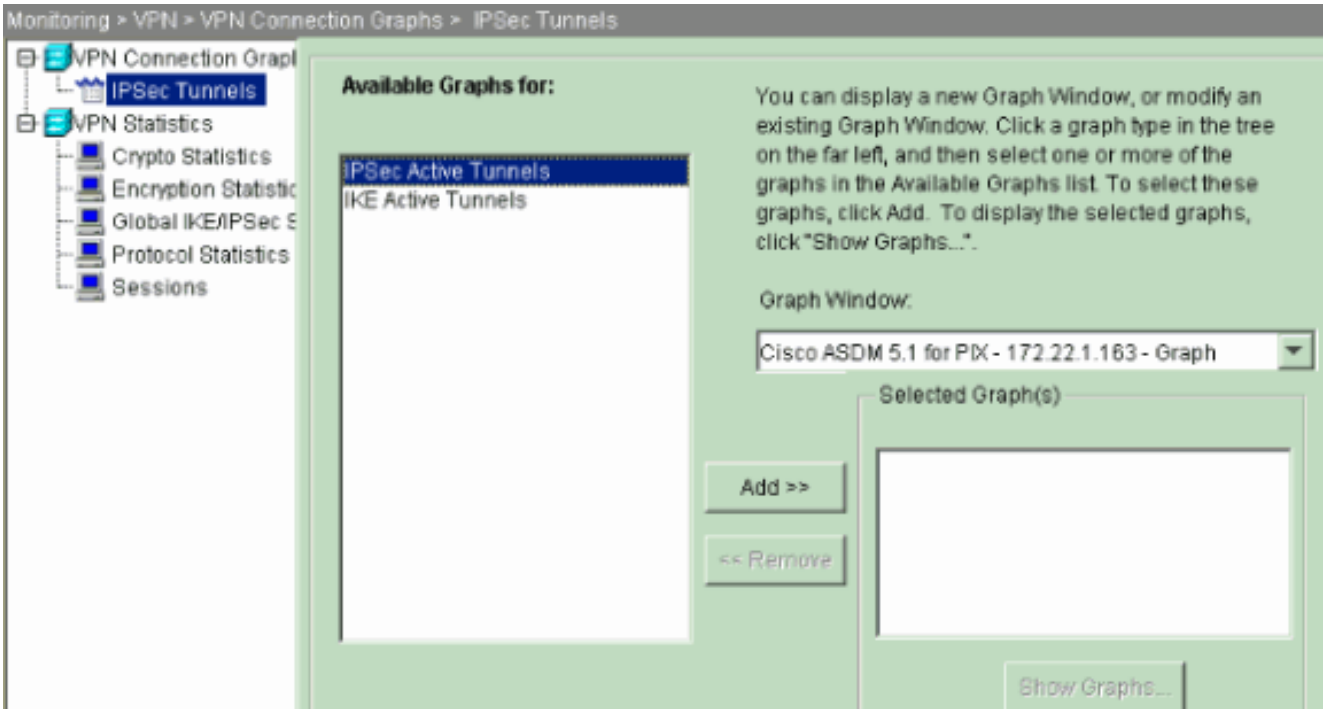
Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Wenn interessanter Datenverkehr zum Peer besteht, wird der Tunnel zwischen pix515-704 und PIX-02 aufgebaut.

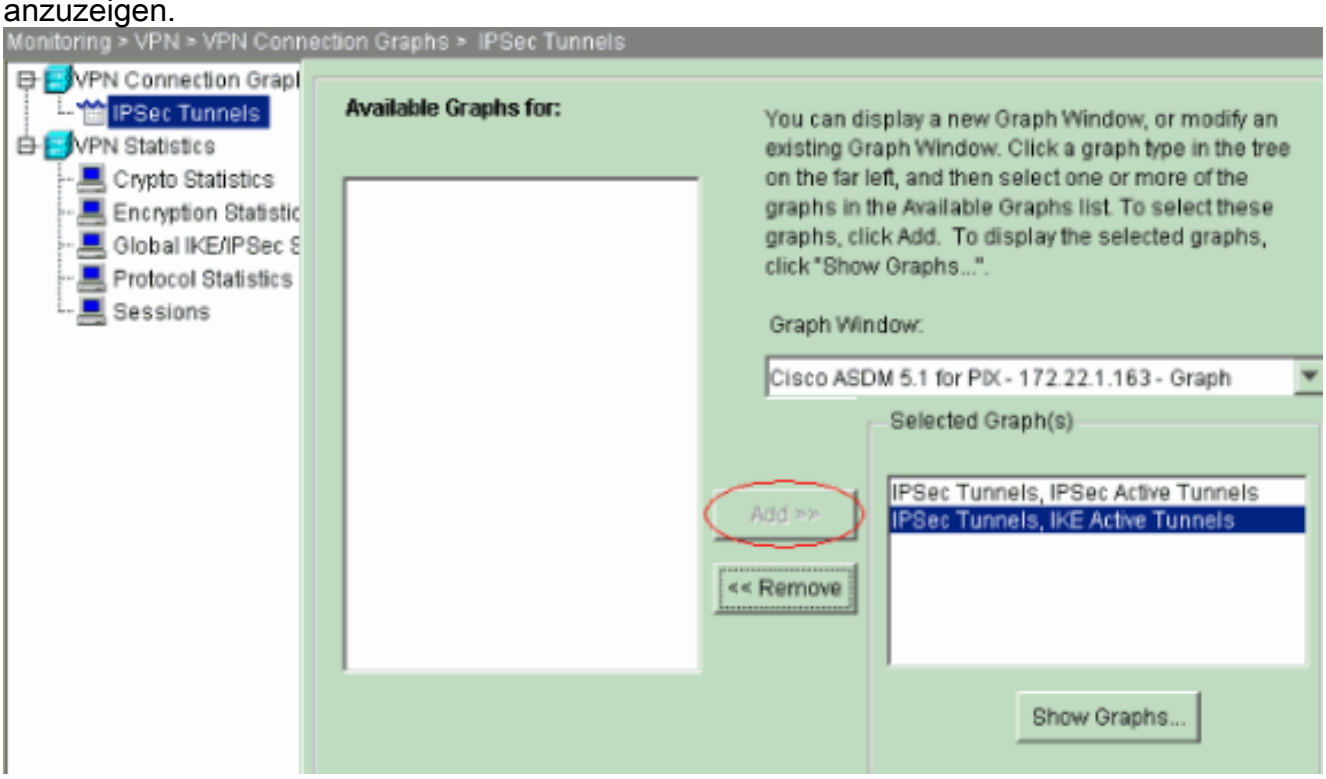
1. Zeigen Sie den VPN-Status unter **Home** im ASDM an, um die Bildung des Tunnels zu überprüfen.



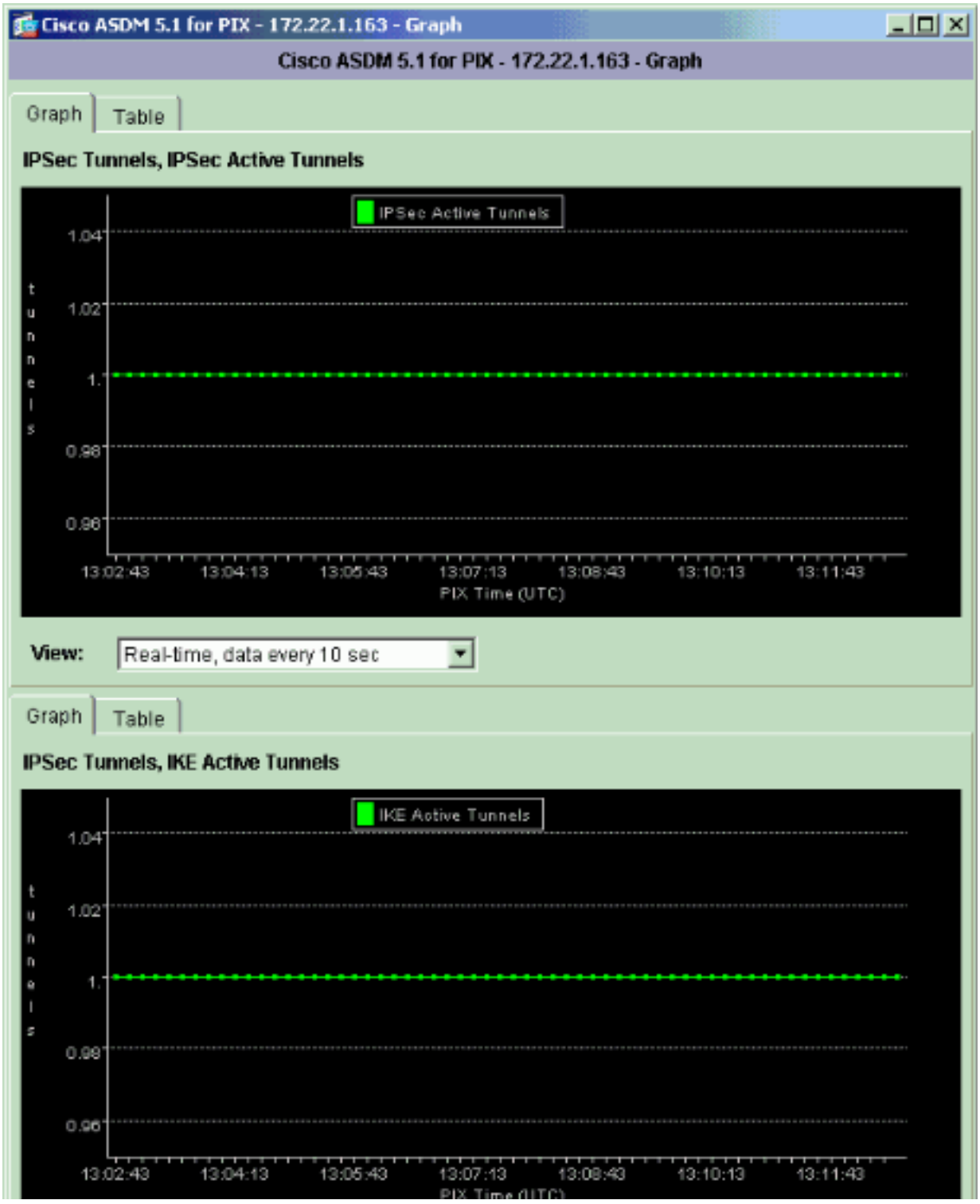
2. Wählen Sie **Monitoring > VPN > VPN Connection Graphs (Überwachung > VPN-Verbindungsdiagramme) > IPSec Tunnels**, um die Details zur Tunneleinrichtung zu überprüfen.



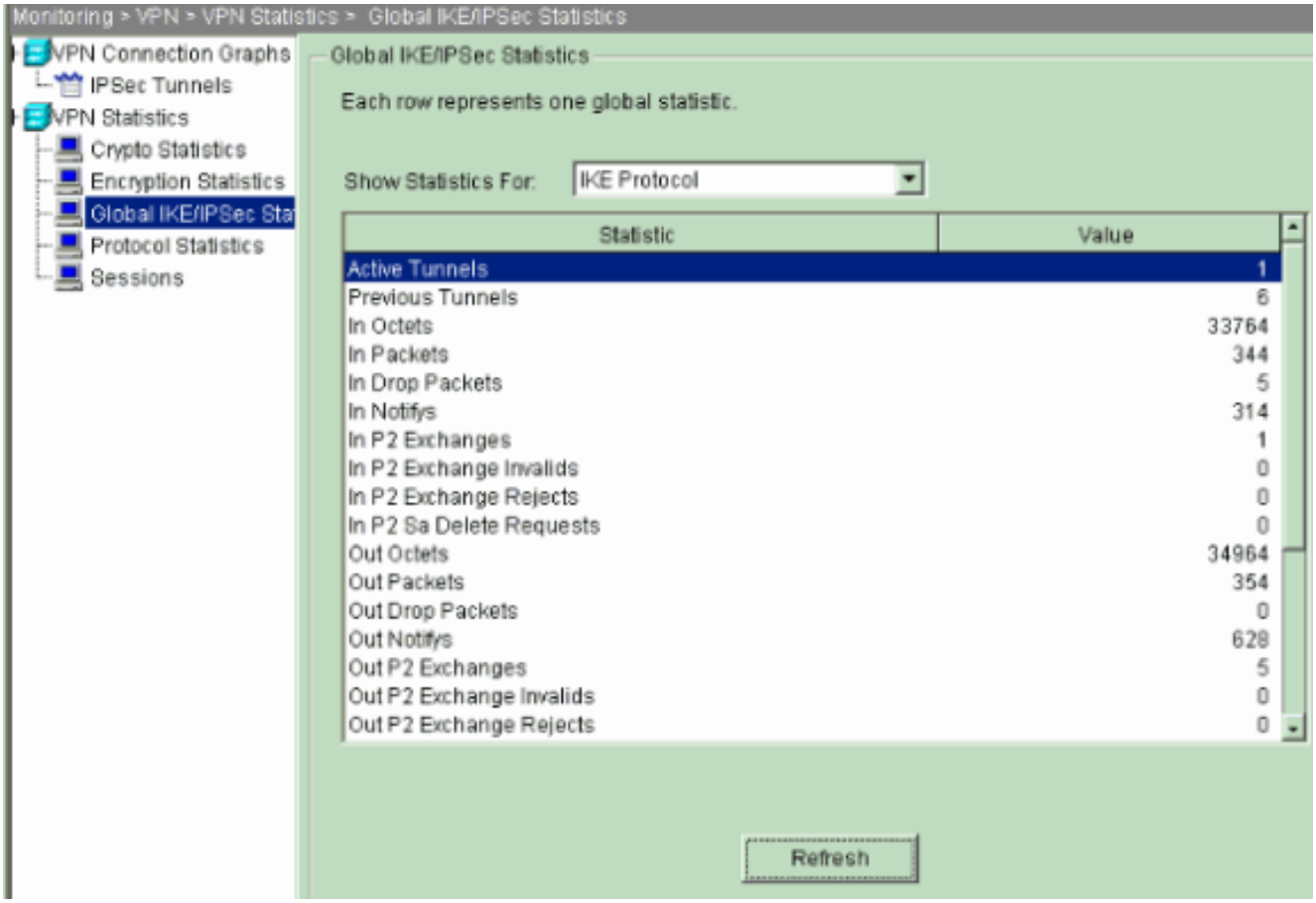
3. Klicken Sie auf **Hinzufügen**, um die verfügbaren Diagramme auszuwählen, um sie im Diagrammfenster
anzuzeigen.



4. Klicken Sie auf **Diagramme anzeigen**, um die Diagramme der aktiven IKE- und IPsec-Tunnel anzuzeigen.



5. Wählen Sie **Monitoring > VPN > VPN Statistics > Global IKE/IPSec Statistics** aus, um die statistischen Informationen des VPN-Tunnels anzuzeigen.



Sie können auch die Bildung von Tunneln mithilfe der CLI überprüfen. Geben Sie den Befehl **show crypto isakmp sa** ein, um die Bildung von Tunneln zu überprüfen und den Befehl **show crypto ipsec als** Befehl auszugeben, um die Anzahl der eingekapselten, verschlüsselten Pakete usw. zu beobachten.

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
```

Fehlerbehebung

PFS

Bei IPsec-Verhandlungen stellt Perfect Forward Secrecy (PFS) sicher, dass jeder neue kryptografische Schlüssel nicht mit einem vorherigen Schlüssel in Beziehung steht. Aktivieren oder deaktivieren Sie PFS auf beiden Tunnel-Peers, andernfalls wird der L2L IPsec-Tunnel in PIX/ASA nicht eingerichtet.

PFS ist standardmäßig deaktiviert. Um PFS zu aktivieren, verwenden Sie den Befehl **pfs** mit dem **Schlüsselwort *enable*** im Gruppenrichtlinienkonfigurationsmodus. Um PFS zu deaktivieren, geben Sie das *disable*-Schlüsselwort ein.

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

Um das PFS-Attribut aus der aktuellen Konfiguration zu entfernen, geben Sie die **no**-Form dieses Befehls ein. Eine Gruppenrichtlinie kann einen Wert für PFS von einer anderen Gruppenrichtlinie erben. Geben Sie die **no**-Form dieses Befehls ein, um zu verhindern, dass ein Wert geerbt wird.

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

Management-Zugriff

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Die interne Schnittstelle des PIX kann nicht vom anderen Ende des Tunnels angepingt werden, es sei denn, der Befehl **für den Management-Zugriff** wird im globalen Konfigurationsmodus konfiguriert.

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

Debugbefehle

Hinweis: Lesen Sie vor dem Ausgabe von **Debug**-Befehlen unter Wichtige Informationen zu Debug-Befehlen nach.

debug crypto isakmp: Zeigt Debuginformationen über IPsec-Verbindungen an und zeigt den ersten Satz von Attributen an, die aufgrund von Inkompatibilitäten an beiden Enden abgelehnt werden.

debuggen 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: Zeigt Debuginformationen über IPsec-Verbindungen an.

debuggen 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
```

Zugehörige Informationen

- Redundante Tunnelerstellung zwischen Firewalls mithilfe von PDM
- Cisco PIX Firewall-Software
- Cisco Adaptive Security Device Manager
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems