

Konfigurieren des Cisco VPN-Clients für PIX mit AES

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurationen](#)

[Netzwerkdigramm](#)

[Konfigurieren des PIX](#)

[Konfigurieren des VPN-Clients](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Diese Beispielkonfiguration zeigt, wie eine VPN-Verbindung für den Remote-Zugriff von einem Cisco VPN-Client zu einer PIX-Firewall mithilfe von Advanced Encryption Standard (AES) für die Verschlüsselung eingerichtet wird. In diesem Beispiel wird mithilfe von Cisco Easy VPN der sichere Kanal eingerichtet, und die PIX-Firewall wird als Easy VPN-Server konfiguriert.

In der Cisco Secure PIX Firewall-Software 6.3 und höher wird der neue internationale Verschlüsselungsstandard AES für die Sicherung von Site-to-Site- und Remote Access-VPN-Verbindungen unterstützt. Zusätzlich zu den Verschlüsselungsalgorithmen DES (Data Encryption Standard) und 3DES (3DES). Die PIX-Firewall unterstützt AES-Schlüsselgrößen von 128, 192 und 256 Bit.

Der VPN-Client unterstützt AES als Verschlüsselungsalgorithmus ab Version 3.6.1 des Cisco VPN-Clients. Der VPN-Client unterstützt nur Schlüsselgrößen von 128 Bit und 256 Bit.

Voraussetzungen

Anforderungen

Bei dieser Beispielkonfiguration wird davon ausgegangen, dass das PIX vollständig betriebsbereit ist und mit den erforderlichen Befehlen konfiguriert ist, um den Datenverkehr gemäß den Sicherheitsrichtlinien der Organisation zu verarbeiten.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX Softwareversion 6.3(1)**Hinweis:** Diese Konfiguration wurde mit Version 6.3(1) der PIX-Software getestet und soll auch mit allen späteren Versionen funktionieren.
- Cisco VPN Client Version 4.0.3(A)**Hinweis:** Dieses Setup wurde mit VPN Client Version 4.0.3(A) getestet, funktioniert jedoch mit früheren Versionen bis 3.6.1 und bis zur aktuellen Version.

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.

Konventionen

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

Hintergrundinformationen

VPNs für Remote-Zugriff erfüllen die Anforderung mobiler Mitarbeiter, eine sichere Verbindung zum Netzwerk des Unternehmens herzustellen. Mobile Benutzer können mithilfe der auf ihren PCs installierten VPN Client-Software eine sichere Verbindung herstellen. Der VPN-Client initiiert eine Verbindung zu einem Gerät an einem zentralen Standort, das so konfiguriert ist, dass er diese Anfragen annimmt. In diesem Beispiel ist das Gerät des zentralen Standorts eine PIX-Firewall, die als Easy VPN-Server konfiguriert ist und dynamische Kryptozuordnungen verwendet.

Cisco Easy VPN vereinfacht die VPN-Bereitstellung, da die Konfiguration und Verwaltung von VPNs vereinfacht wird. Sie besteht aus dem Cisco Easy VPN-Server und dem Cisco Easy VPN Remote. Für Easy VPN Remote ist eine minimale Konfiguration erforderlich. Easy VPN Remote initiiert eine Verbindung. Bei erfolgreicher Authentifizierung überträgt der Easy VPN-Server die VPN-Konfiguration auf diese. Weitere Informationen zur Konfiguration einer PIX-Firewall als Easy VPN-Server finden Sie unter [Verwalten des VPN-Remote-Zugriffs](#).

Dynamische Kryptokarten werden für die IPsec-Konfiguration verwendet, wenn einige Parameter, die für die Einrichtung des VPN erforderlich sind, nicht vorgegeben werden können, wie dies bei mobilen Benutzern der Fall ist, die dynamisch zugewiesene IP-Adressen beziehen. Die dynamische Crypto Map fungiert als Vorlage, und die fehlenden Parameter werden während der IPsec-Aushandlung festgelegt. Weitere Informationen zu dynamischen Crypto Maps finden Sie unter [Dynamic Crypto Maps](#).

Konfigurationen

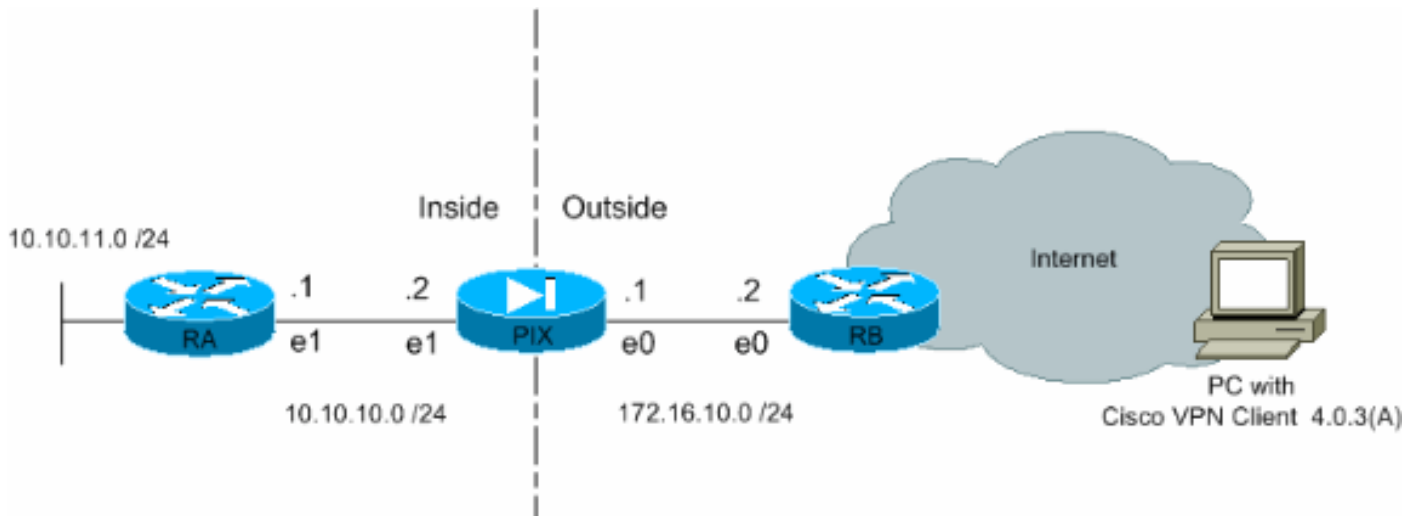
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere

Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurieren des PIX

Die erforderliche Konfiguration für die PIX-Firewall wird in dieser Ausgabe angezeigt. Die Konfiguration gilt nur für VPN.

PIX

```
PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Pixfirewall
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
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
names

!--- Define the access list to enable split tunneling.
access-list 101 permit ip 10.10.10.0 255.255.255.0
10.10.8.0 255.255.255.0 access-list 101 permit ip
10.10.11.0 255.255.255.0 10.10.8.0 255.255.255.0 !---
Define the access list to avoid network address !---
```

```

translation (NAT) on IPsec packets. access-list 102
permit ip 10.10.10.0 255.255.255.0 10.10.8.0
255.255.255.0 access-list 102 permit ip 10.10.11.0
255.255.255.0 10.10.8.0 255.255.255.0 pager lines 24 mtu
outside 1500 mtu inside 1500 mtu intf2 1500 !---
Configure the IP address on the interfaces. ip address
outside 172.16.10.1 255.255.255.0 ip address inside
10.10.10.2 255.255.255.0 no ip address intf2 ip audit
info action alarm ip audit attack action alarm !---
Create a pool of addresses from which IP addresses are
assigned !--- dynamically to the remote VPN Clients. ip
local pool vpnpool1 10.10.8.1-10.10.8.254 pdm history
enable arp timeout 14400 !--- Disable NAT for IPsec
packets. nat (inside) 0 access-list 102 route outside
0.0.0.0 0.0.0.0 172.16.10.2 1 route inside 10.10.11.0
255.255.255.0 10.10.10.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h225 1:00:00 timeout h323 0:05:00 mgcp 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server LOCAL protocol local no snmp-
server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Permit packet that came from an IPsec tunnel
to pass through without !--- checking them against the
configured conduits/access lists. sysopt connection
permit-ipsec !--- Define the transform set to be used
during IPsec !--- security association (SA) negotiation.
Specify AES as the encryption algorithm. crypto ipsec
transform-set trmset1 esp-aes-256 esp-sha-hmac !---
Create a dynamic crypto map entry !--- and add it to a
static crypto map. crypto dynamic-map map2 10 set
transform-set trmset1 crypto map map1 10 ipsec-isakmp
dynamic map2 !--- Bind the crypto map to the outside
interface. crypto map map1 interface outside !--- Enable
Internet Security Association and Key Management !---
Protocol (ISAKMP) negotiation on the interface on which
the IPsec !--- peer communicates with the PIX Firewall.
isakmp enable outside isakmp identity address !---
Define an ISAKMP policy to be used while !---
negotiating the ISAKMP SA. Specify !--- AES as the
encryption algorithm. The configurable AES !--- options
are aes, aes-192 and aes-256. !--- Note: AES 192 is not
supported by the VPN Client.

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- Create a VPN group and configure the policy
attributes which are !--- downloaded to the Easy VPN
Clients. vpngroup groupmarketing address-pool vpnpool1
vpngroup groupmarketing dns-server 10.10.11.5 vpngroup
groupmarketing wins-server 10.10.11.5 vpngroup
groupmarketing default-domain org1.com vpngroup
groupmarketing split-tunnel 101 vpngroup groupmarketing
idle-time 1800 vpngroup groupmarketing password *****
telnet timeout 5 ssh timeout 5 console timeout 0
terminal width 80
Cryptochecksum:c064abce81996b132025e83e421ee1c3 : end

```

Hinweis: In dieser Konfiguration wird empfohlen, aes-192 nicht anzugeben, während Sie den

Transformationsatz oder die ISAKMP-Richtlinie konfigurieren. VPN-Clients unterstützen keine AES-192-Verschlüsselung.

Hinweis: Bei früheren Versionen waren die Befehle **isakmp client configuration address-pool** und **crypto map client-configuration** erforderlich. Bei neueren Versionen (3.x und höher) sind diese Befehle jedoch nicht mehr erforderlich. Mehrere Adresspools können jetzt mit dem Befehl **vpngroup address-pool** angegeben werden.

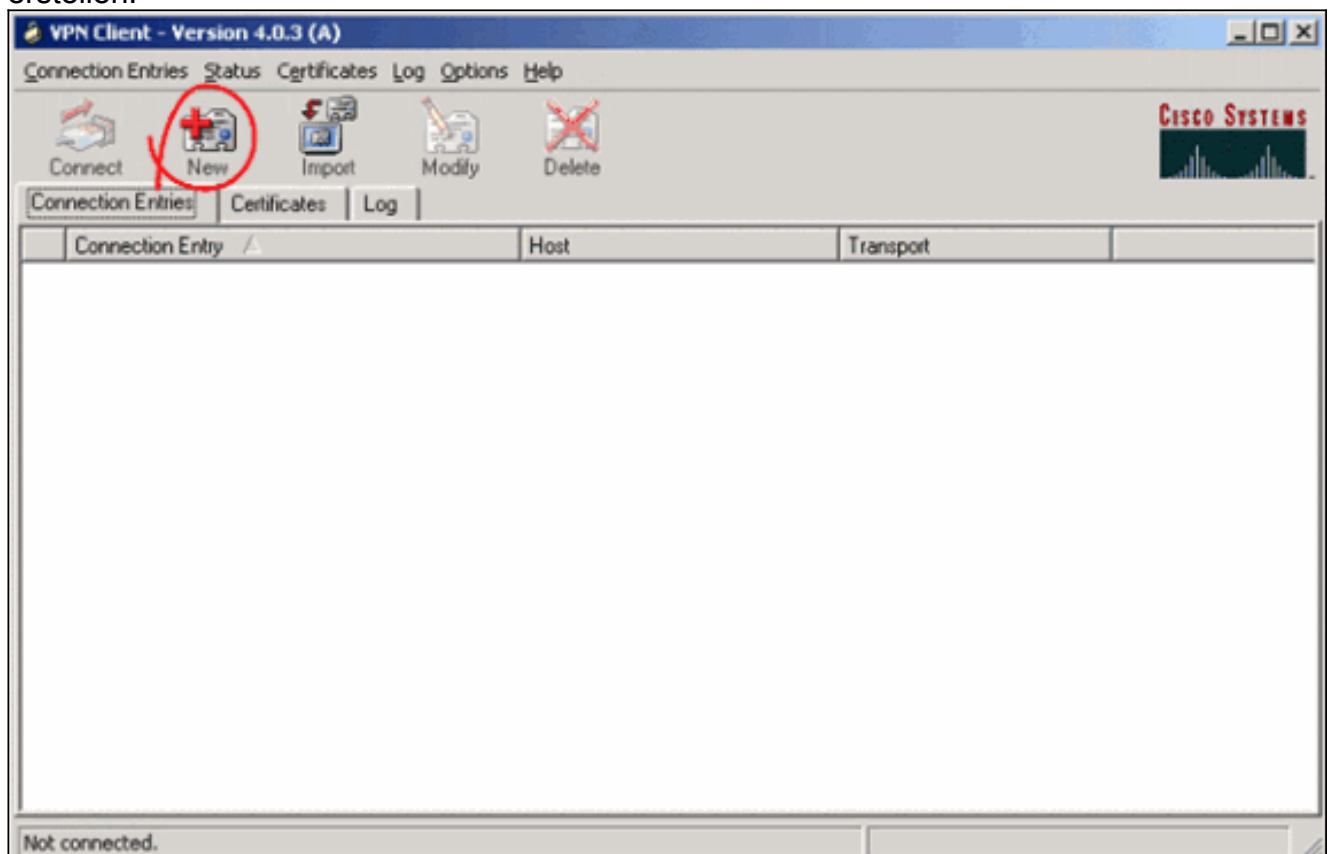
Hinweis: Bei VPN-Gruppennamen wird die Groß- und Kleinschreibung beachtet. Dies bedeutet, dass die Benutzerauthentifizierung fehlschlägt, wenn der im PIX angegebene Gruppenname und der Gruppenname im VPN-Client in Bezug auf Groß- oder Kleinschreibung unterschiedlich sind.

Hinweis: Wenn Sie z. B. den Gruppennamen **GroupMarketing** auf einem Gerät eingeben und **Groupmarketing** auf einem anderen Gerät eingeben, funktioniert das Gerät nicht.

Konfigurieren des VPN-Clients

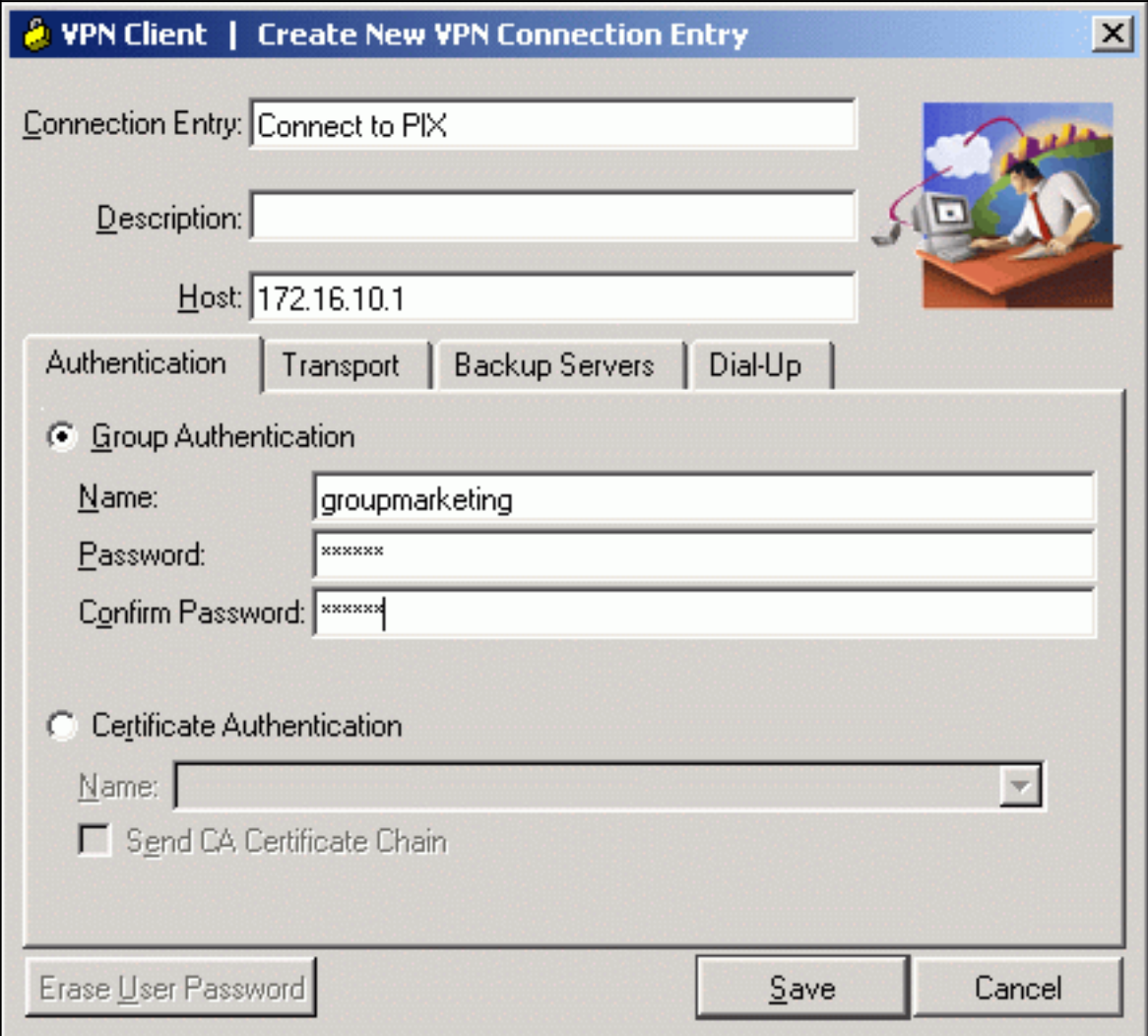
Nachdem Sie den VPN-Client auf dem PC installiert haben, erstellen Sie eine neue Verbindung, wie in den folgenden Schritten gezeigt:

1. Starten Sie die VPN-Client-Anwendung, und klicken Sie auf **Neu**, um einen neuen Verbindungseintrag zu erstellen.



2. Neues Dialogfeld mit dem Titel VPN Client | Neuen VPN-Verbindungseintrag erstellen wird angezeigt. Geben Sie Konfigurationsinformationen für die neue Verbindung ein. Weisen Sie dem neu erstellten Eintrag im Feld Verbindungseintrag einen Namen zu. Geben Sie im Feld Host (Host) die IP-Adresse der öffentlichen Schnittstelle des PIX ein. Wählen Sie die Registerkarte Authentifizierung aus, und geben Sie dann den Gruppennamen und das Kennwort (zweimal - zur Bestätigung) ein. Dies muss mit dem Befehl **vpngroup password**

den auf dem PIX eingegebenen Informationen entsprechen. Klicken Sie auf **Speichern**, um die eingegebenen Informationen zu speichern. Die neue Verbindung wird jetzt



VPN Client | Create New VPN Connection Entry

Connection Entry: Connect to PIX

Description:

Host: 172.16.10.1

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication

Name: groupmarketing

Password: xxxxxx

Confirm Password: xxxxxx

Certificate Authentication

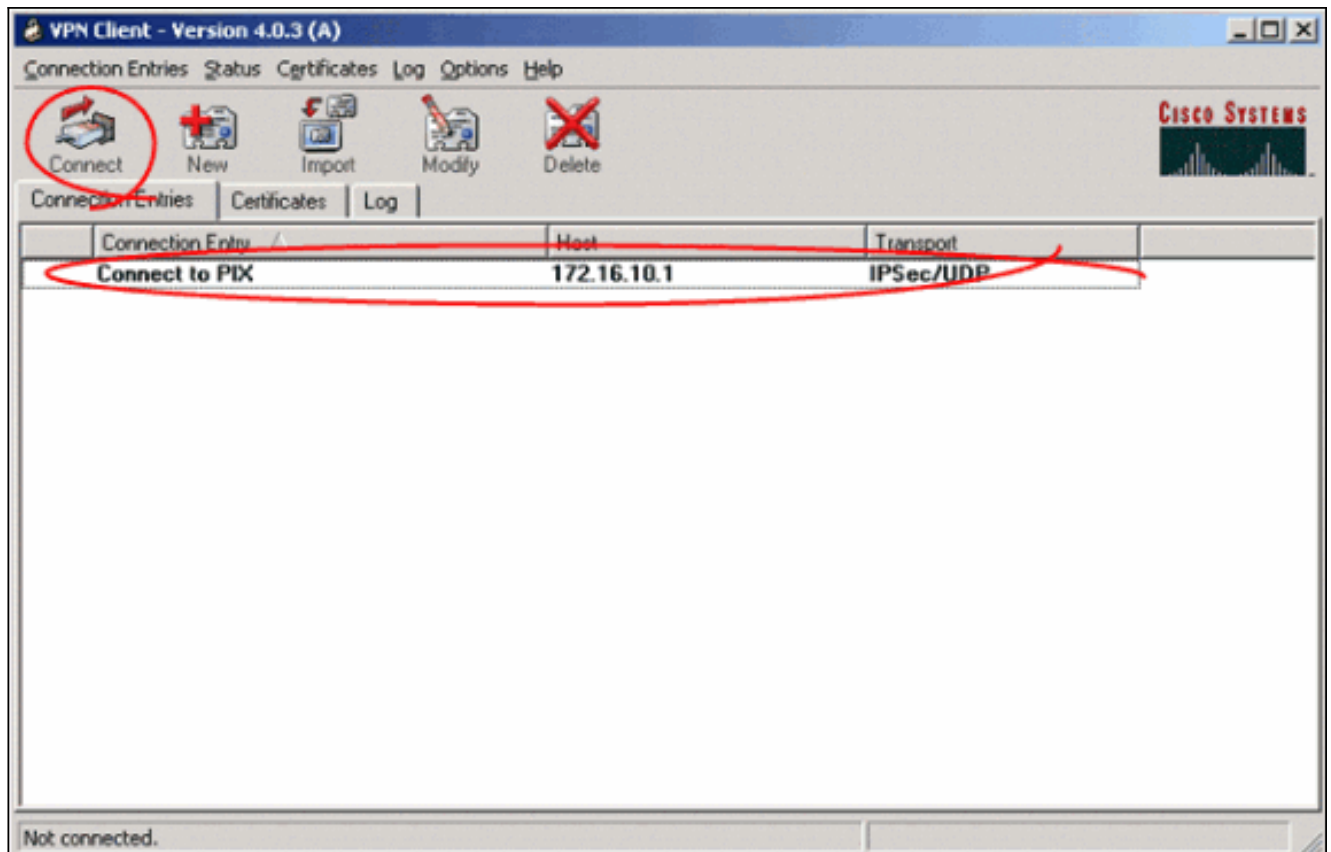
Name:

Send CA Certificate Chain

Erase User Password | **Save** | Cancel

erstellt.

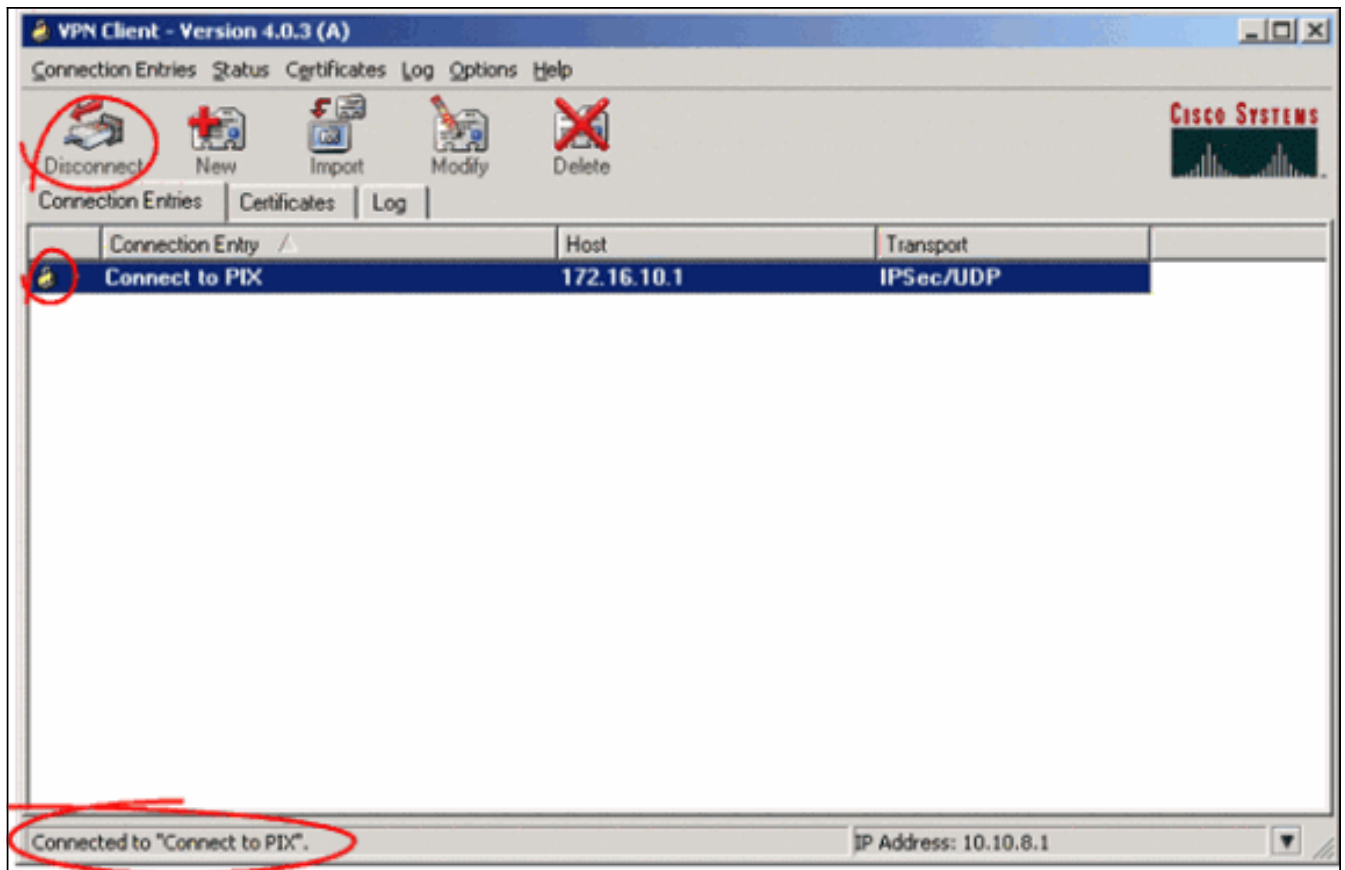
- Um über den neuen Verbindungseintrag eine Verbindung zum Kabelmodem herzustellen, wählen Sie den Verbindungseintrag aus, indem Sie einmal darauf klicken und dann auf das Symbol **Verbinden** klicken. Ein Doppelklick auf den Verbindungseintrag hat dieselbe Wirkung.



Überprüfen

Auf dem VPN-Client wird eine erfolgreich eingerichtete Verbindung zum Remote-Gateway durch folgende Elemente angezeigt:

- Ein gelbes geschlossenes Sperrsymbol wird beim aktiven Verbindungseintrag angezeigt.
- Das Symbol Connect (Verbinden) in der Symbolleiste (neben der Registerkarte Connection Entries) ändert sich in Disconnect (Verbindung trennen).
- Die Statuszeile am Ende des Fensters zeigt den Status als "Verbunden mit" gefolgt vom Namen des Verbindungs-Eintrags an.



Hinweis: Sobald die Verbindung hergestellt ist, minimiert der VPN Client standardmäßig ein geschlossenes Symbol im Systembereich in der unteren rechten Ecke der Windows-Taskleiste. Doppelklicken Sie auf das Sperrsymbol, um das Fenster des VPN-Clients erneut anzuzeigen.

Auf der PIX-Firewall können diese **show**-Befehle verwendet werden, um den Status der eingerichteten Verbindungen zu überprüfen.

Hinweis: Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) unterstützt, mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto ipsec sa** - Zeigt alle aktuellen IPsec-SAs auf dem PIX an. Darüber hinaus zeigt die Ausgabe die tatsächliche IP-Adresse des Remote-Peers, die zugewiesene IP-Adresse, die lokale IP-Adresse und -Schnittstelle sowie die angewendete Crypto Map an.

```
Pixfirewall#show crypto ipsec sa
```

```
interface: outside
```

```
  Crypto map tag: map1, local addr. 172.16.10.1
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.10.8.1/255.255.255.255/0/0)
```

```
current_peer: 172.16.12.3:500
```

```
dynamic allocated peer ip: 10.10.8.1
```

```
  PERMIT, flags={}
```

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
```

```
#pkts decaps: 25, #pkts decrypt: 25, #pkts verify 25
```

```
#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.: 172.16.10.1, remote crypto endpt.: 172.16.12.3
```

```
path mtu 1500, ipsec overhead 64, media mtu 1500
```

```
current outbound spi: cbabd0ce
```



```
inbound esp sas:
spi: 0x4d8a971d(1300928285)
transform: esp-aes-256 esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: map1
sa timing: remaining key lifetime (k/sec): (4607996/28685)
IV size: 16 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0xcbabd0ce(3417034958)
transform: esp-aes-256 esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: map1
sa timing: remaining key lifetime (k/sec): (4608000/28676)
IV size: 16 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

- **show crypto isakmp sa:** Zeigt den Status der ISAKMP SA an, die zwischen Peers erstellt wurde.

```
Pixfirewall#show crypto isakmp sa
Total      : 1
Embryonic  : 0
      dst          src          state    pending    created
      172.16.10.1  172.16.12.3  QM_IDLE      0          1
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Diese Debugbefehle können bei der Fehlerbehebung von Problemen mit der VPN-Einrichtung helfen.

Hinweis: Lesen Sie [vor dem](#) Ausgabe von **Debug**-Befehlen unter [Wichtige Informationen zu Debug-Befehlen nach](#).

- **debug crypto isakmp** - Zeigt die erstellte ISAKMP SA und die ausgehandelten IPsec-Attribute an. Während der ISAKMP SA-Aushandlung kann der PIX möglicherweise mehrere Vorschläge als "nicht akzeptabel" verwerfen, bevor er sie annimmt. Sobald die ISAKMP SA vereinbart ist, werden die IPsec-Attribute ausgehandelt. Wieder können mehrere Vorschläge abgelehnt werden, bevor sie angenommen werden, wie in dieser **Debugausgabe** gezeigt.

```
crypto_isakmp_process_block:src:172.16.12.3, dest:172.16.10.1 spt:500 dpt:500
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
```

```
ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
```

```

ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
!--- Proposal is rejected since extended auth is not configured. ISAKMP (0): atts are not
acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share (init)
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
!--- Proposal is rejected since MD5 is not specified as the hash algorithm. ISAKMP (0): atts
are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption AES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP:      keylength of 256
!--- This proposal is accepted since it matches ISAKMP policy 10. ISAKMP (0): atts are
acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
!--- Output is suppressed. OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3348522173

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_AES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
ISAKMP:    key length is 256
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
!--- This proposal is not accepted since transform-set !--- trmset1 does not use MD5. ISAKMP
(0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (1)
ISAKMP : Checking IPSec proposal 2

ISAKMP: transform 1, ESP_AES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-SHA
ISAKMP:    key length is 256
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
!--- This proposal is accepted since it matches !--- transform-set trmset1. ISAKMP (0): atts
are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 3
!--- Output is suppressed.

```

- **debug crypto ipsec:** Zeigt Informationen über IPsec SA-Aushandlungen an.

```
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
```

```

IPSEC(key_engine_delete_sas): delete all SAs shared with      172.16.12.3
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 2) not
supported
IPSEC(validate_proposal): transform proposal (prot 3, trans 12, hmac_alg 1) not
supported
IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
src_proxy= 10.10.8.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xfb0cb69(263244649) for SA
from      172.16.12.3 to      172.16.10.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.16.10.1, src= 172.16.12.3,
dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
src_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0xfb0cb69(263244649), conn_id= 2, keysize= 256, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.16.10.1, dest= 172.16.12.3,
src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
dest_proxy= 10.10.8.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-aes-256 esp-sha-hmac ,
lifedur= 2147483s and 0kb,
spi= 0xda6c054a(3664512330), conn_id= 1, keysize= 256, flags= 0x4

```

Mit den in diesem Dokument gezeigten Konfigurationen kann der VPN-Client mithilfe von AES erfolgreich eine Verbindung mit dem PIX am zentralen Standort herstellen. Es wird gelegentlich beobachtet, dass der VPN-Tunnel erfolgreich eingerichtet wurde, Benutzer jedoch nicht in der Lage sind, gängige Aufgaben wie das Ping von Netzwerkressourcen, die Anmeldung bei der Domäne oder das Durchsuchen der Netzwerkumgebung auszuführen. Weitere Informationen zur Behebung solcher Probleme finden Sie unter [Fehlerbehebung bei Microsoft Network Neighborhood After Setup a VPN Tunnel With the Cisco VPN Client](#).

Zugehörige Informationen

- [Advanced Encryption Standard \(AES\)](#)
- [Eine Einführung in die IP Security \(IPSec\)-Verschlüsselung](#)
- [IP Security Troubleshooting - Understanding and Using debug Commands](#)
- [Support-Seite für IPsec-Aushandlung/IKE-Protokolle](#)
- [PIX-Support-Seite](#)
- [Support-Seite für Cisco VPN-Clients](#)
- [PIX-Befehlsreferenz](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)