PIX/ASA 7.x Easy VPN mit ASA 5500 als Server und PIX 506E als Client (NEM) - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für IPsec zwischen einer Cisco Adaptive Security Appliance (ASA) 5520 und einem Cisco PIX 506E mit EasyVPN. Die ASA 5520 fungiert als EasyVPN-Server, und das PIX 506E fungiert als EasyVPN-Remote-Client. Bei dieser Konfiguration wird ein ASA 5520-Gerät verwendet, auf dem die ASA-Software Version 7.0(4) ausgeführt wird. Sie können diese Konfiguration jedoch auch für PIX-Firewall-Geräte verwenden, auf denen das PIX-Betriebssystem Version 7.0 und höher ausgeführt wird.

Weitere Informationen zu einem ähnlichen Szenario, in dem der Cisco 871 Router als Easy VPN-Remote fungiert, finden Sie unter PIX/ASA 7.x Easy VPN mit ASA 5500 als Server und Cisco 871 als Easy VPN Remote-Konfigurationsbeispiel.

Weitere Informationen zu einem ähnlichen Szenario, in dem der Cisco VPN 3000 Concentrator als Easy VPN-Server fungiert, finden Sie im VPN Hardware Client auf einer Sicherheitslösung der Serie PIX 501/506 mit VPN 3000 Concentrator.

Unter PIX 501/506 Easy VPN Remote zu einem IOS® Router im Netzwerkerweiterungsmodus mit erweiterter Authentifizierungskonfiguration (Konfigurationsbeispiel) finden Sie weitere Informationen zu einem ähnlichen Szenario, in dem der Cisco IOS Router als Easy VPN-Server fungiert.

Weitere Informationen finden Sie unter PIX-to-PIX 6.x: Easy VPN (NEM)-Konfigurationsbeispiel für weitere Informationen zu einem ähnlichen Szenario, in dem das PIX 506 6.x als Easy VPN-Server fungiert.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Vergewissern Sie sich, dass Sie über grundlegende Kenntnisse der Betriebssysteme IPsec und ASA/PIX 6.x und 7.x verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Der Remote-Hardware-Client von EasyVPN ist ein PIX 506E, der Version 6.3(5) ausführt.
- Der EasyVPN-Server ist eine ASA 5520, die Version 7.0(4) ausführt.

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

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

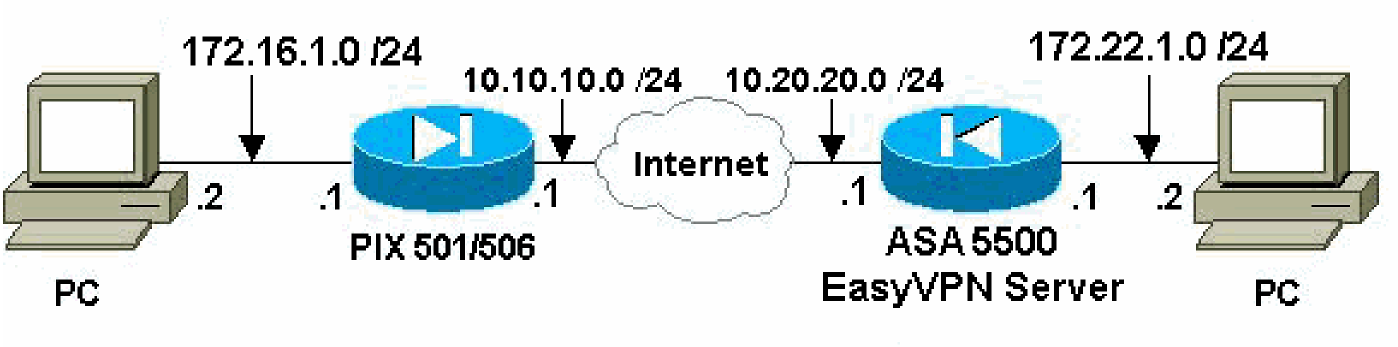
Konfiguration

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

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:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Easy VPN-Server (ASA 5520)
- Easy VPN Remote Hardware Client

Easy VPN-Server (ASA 5520)

```
ASA5520-704#write terminal
: Saved
:
ASA Version 7.0(4)
!
hostname ASA5520-704
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!

!--- Configure the outside and inside interfaces.
interface GigabitEthernet0/0 nameif outside security-
level 0 ip address 10.20.20.1 255.255.255.0 ! interface
GigabitEthernet0/1 nameif inside security-level 100 ip
address 172.22.1.1 255.255.255.0 ! interface
GigabitEthernet0/2 shutdown no nameif no security-level
no ip address ! interface GigabitEthernet0/3 shutdown no
nameif no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive !--- This access list is used for a nat zero
command that prevents !--- traffic which matches the
access list from undergoing !--- network address
translation (NAT).

access-list no-nat extended permit ip 172.22.1.0
255.255.255.0 172.16.1.0 255.255.255.0
!--- This access list is used to define the traffic !---
that should pass through the tunnel. !--- It is bound to
the group policy which defines !--- a dynamic crypto
map. access-list ezvpn1 extended permit ip 172.22.1.0
255.255.255.0 172.16.1.0 255.255.255.0 pager lines 24
mtu outside 1500 mtu inside 1500 no failover icmp permit
any echo-reply outside icmp permit any inside no asdm
history enable arp timeout 14400 !--- Specify the NAT
configuration. !--- NAT 0 prevents NAT for the ACL
defined in this configuration. !--- The nat 1 command
specifies NAT for all other traffic.
```

```
global (outside) 1 interface
nat (inside) 0 access-list no-nat
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- This defines the group policy you use with EasyVPN.
!--- Specify the networks !--- that should pass through
the tunnel and that you want to !--- use network
extension mode. group-policy myGROUP internal group-
policy myGROUP attributes split-tunnel-policy
tunnelspecified split-tunnel-network-list value ezvpn1
nem enable webvpn !--- Here the username and password
associated with !--- this VPN connection are defined.
You !--- can also use AAA for this function. username
cisco password 3USUcOPFUiMCO4Jk encrypted no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !--- PHASE
2 CONFIGURATION ---! !--- The encryption types for Phase
2 are defined here. !--- A single DES encryption with !-
-- the md5 hash algorithm is used. crypto ipsec
transform-set mySET esp-des esp-md5-hmac !--- Defines a
dynamic crypto map with !--- the specified encryption
settings. crypto dynamic-map myDYN-MAP 5 set transform-
set mySET !--- Binds the dynamic map to the IPsec/ISAKMP
process. crypto map myMAP 60 ipsec-isakmp dynamic myDYN-
MAP !--- Specifies the interface to be used with !---
the settings defined in this configuration. crypto map
myMAP interface outside !--- PHASE 1 CONFIGURATION ---!
!--- This configuration uses isakmp policy 1. !---
Policy 65535 is included in the default !---
configuration. The configuration commands here define
the Phase !--- 1 policies that are used. isakmp enable
outside isakmp policy 1 authentication pre-share isakmp
policy 1 encryption des isakmp policy 1 hash md5 isakmp
policy 1 group 2 isakmp policy 1 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 !--- The tunnel-group commands bind the
configurations !--- defined in this configuration to the
tunnel that is !--- used for EasyVPN. This tunnel name
is the one specified on the remote side. tunnel-group
mytunnel type ipsec-ra tunnel-group mytunnel general-
attributes default-group-policy myGROUP tunnel-group
mytunnel ipsec-attributes !--- The pre-shared-key used
here is "cisco". 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:42123a94a33d8d10ae6a1505fb4ba653 : end
[OK] ASA5520-704#
```

Easy VPN Remote Hardware Client

```
pix506-635#write terminal
Building configuration...
: Saved
:
PIX Version 6.3(5)
!--- Brings the interfaces out of a shutdown state.
interface ethernet0 auto interface ethernet1 auto !---
Assign the interface names. nameif ethernet0 outside
security0 nameif ethernet1 inside security100 enable
password 8Ry2YjIyt7RRXU24 encrypted passwd
2KFQnbNIdI.2KYOU encrypted hostname pix506-635 domain-
name cisco.com fixup protocol dns maximum-length 512
fixup protocol ftp 21 fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719 fixup protocol http 80
fixup protocol rsh 514 fixup protocol rtsp 554 fixup
protocol sip 5060 fixup protocol sip udp 5060 fixup
protocol skinny 2000 fixup protocol smtp 25 fixup
protocol sqlnet 1521 fixup protocol tftp 69 names pager
lines 24 icmp permit any outside mtu outside 1500 mtu
inside 1500 !--- Assign the interface IP addresses. ip
address outside 10.10.10.1 255.255.255.0 ip address
inside 172.16.1.1 255.255.255.0 ip audit info action
alarm ip audit attack action alarm pdm history enable
arp timeout 14400 !--- Set the standard NAT
configuration. !--- EasyVPN provides the NAT exceptions
needed. global (outside) 1 interface nat (inside) 1
0.0.0.0 0.0.0.0 0 0 !--- Specify the default route.
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 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-
disconnect 0:02:00 sip-invite 0:03:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3 aaa-server
TACACS+ deadtime 10 aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3 aaa-server
RADIUS deadtime 10 aaa-server LOCAL protocol local no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable telnet timeout 5 ssh timeout 5 console timeout 0
!--- EasyVPN Client Configuration ---! !--- Specify the
IP address of the VPN server. vpnclient server
10.20.20.1 !--- This example uses network extension
mode. vpnclient mode network-extension-mode !--- Specify
the group name and the pre-shared key. vpnclient
vpngroup mytunnel password ******** !--- Specify the
authentication username and password. vpnclient username
cisco password ******** !---- After you issue this
command, the tunnel is established. vpnclient enable
terminal width 80
Cryptochecksum:1564fd62a9e4312020f51846bd1b3534 : end
[OK] pix506-635#
```

Überprüfung

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**.

- PIX EasyVPN-Server zeigt Befehle und Beispielausgabe an
- PIX EasyVPN Remote-Hardware-Client zeigt Befehle und Beispielausgabe

PIX EasyVPN-Server zeigt Befehle und Beispielausgabe an

- **show crypto isakmp sa**: Zeigt alle aktuellen Internet Key Exchange (IKE)-Sicherheitszuordnungen (SA) auf einem Peer an.

```
ASA5520-704#show crypto isakmp sa

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

1 IKE Peer: 10.10.10.1
Type : user Role : responder
Rekey : no State : AM_ACTIVE
ASA5520-704#
```

- **show crypto ipsec sa**: Zeigt zwischen Peers erstellte IPsec-SAs an.

```
ASA5520-704#show crypto ipsec sa
interface: outside
    Crypto map tag: myDYN-MAP, seq num: 5, local addr: 10.20.20.1

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: 10.10.10.1, username: cisco
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 655, #pkts encrypt: 655, #pkts digest: 655
#pkts decaps: 706, #pkts decrypt: 706, #pkts verify: 706
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 655, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

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

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3EA12BBE

inbound esp sas:
spi: 0x9B94D824 (2610223140)
transform: esp-des esp-md5-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 25015
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x3EA12BBE (1050749886)
transform: esp-des esp-md5-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 25011
IV size: 8 bytes
replay detection support: Y

ASA5520-704#
```

PIX EasyVPN Remote-Hardware-Client zeigt Befehle und Beispielausgabe

- **vpnclient enable**: Aktiviert eine EasyVPN-Remoteverbindung. Im Network Extension Mode (NEM) ist der Tunnel auch dann aktiv, wenn kein interessanter Datenverkehr mit dem Headend-EasyVPN-Server ausgetauscht werden soll.

  ```
  pix506-635(config)#vpnclient enable
  ```

- **show crypto isakmp policy**: Zeigt die Parameter für jede IKE-Richtlinie an.

  ```
  pix506-635#show crypto isakmp policy

  Default protection suite
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Secure Hash Standard
      authentication method:  Rivest-Shamir-Adleman Signature
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
  ```

  Diese Ausgabe zeigt den Befehl **show crypto isakmp policy**, nachdem der Hardware-Client aktiviert wurde.

  ```
  pix506-635(config)#show crypto isakmp policy

  Protection suite of priority 65001
       encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
       hash algorithm:         Secure Hash Standard
       authentication method:  Pre-Shared Key with XAUTH
       Diffie-Hellman group:   #2 (1024 bit)
       lifetime:               86400 seconds, no volume limit
  Protection suite of priority 65002
       encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
       hash algorithm:         Message Digest 5
       authentication method:  Pre-Shared Key with XAUTH
       Diffie-Hellman group:   #2 (1024 bit)
       lifetime:               86400 seconds, no volume limit
  Protection suite of priority 65003
       encryption algorithm:   AES - Advanced Encryption Standard (192 bit keys).
       hash algorithm:         Secure Hash Standard
       authentication method:  Pre-Shared Key with XAUTH
       Diffie-Hellman group:   #2 (1024 bit)
       lifetime:               86400 seconds, no volume limit
  Protection suite of priority 65004
       encryption algorithm:   AES - Advanced Encryption Standard (192 bit keys).
       hash algorithm:         Message Digest 5
       authentication method:  Pre-Shared Key with XAUTH
       Diffie-Hellman group:   #2 (1024 bit)
       lifetime:               86400 seconds, no volume limit
  Protection suite of priority 65005
       encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
       hash algorithm:         Secure Hash Standard
       authentication method:  Pre-Shared Key with XAUTH
       Diffie-Hellman group:   #2 (1024 bit)
       lifetime:               86400 seconds, no volume limit
  Protection suite of priority 65006
       encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
       hash algorithm:         Message Digest 5
       authentication method:  Pre-Shared Key with XAUTH
       Diffie-Hellman group:   #2 (1024 bit)
       lifetime:               86400 seconds, no volume limit
  Protection suite of priority 65007
       encryption algorithm:   Three key triple DES
       hash algorithm:         Secure Hash Standard
       authentication method:  Pre-Shared Key with XAUTH
       Diffie-Hellman group:   #2 (1024 bit)
       lifetime:               86400 seconds, no volume limit
  Protection suite of priority 65008
  ```

```
     encryption algorithm:   Three key triple DES
     hash algorithm:         Message Digest 5
     authentication method:  Pre-Shared Key with XAUTH
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65009
     encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
     hash algorithm:         Message Digest 5
     authentication method:  Pre-Shared Key with XAUTH
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65010
     encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
     hash algorithm:         Secure Hash Standard
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65011
     encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
     hash algorithm:         Message Digest 5
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65012
     encryption algorithm:   AES - Advanced Encryption Standard (192 bit keys).
     hash algorithm:         Secure Hash Standard
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65013
     encryption algorithm:   AES - Advanced Encryption Standard (192 bit keys).
     hash algorithm:         Message Digest 5
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65014
     encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
     hash algorithm:         Secure Hash Standard
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65015
     encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
     hash algorithm:         Message Digest 5
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65016
     encryption algorithm:   Three key triple DES
     hash algorithm:         Secure Hash Standard
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65017
     encryption algorithm:   Three key triple DES
     hash algorithm:         Message Digest 5
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
Protection suite of priority 65018
     encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
     hash algorithm:         Message Digest 5
     authentication method:  Pre-Shared Key
     Diffie-Hellman group:   #2 (1024 bit)
     lifetime:               86400 seconds, no volume limit
```

- **show crypto isakmp sa**: Zeigt alle aktuellen IKE-SAs in einem Peer an.

```
pix506-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending     created
      10.20.20.1       10.10.10.1    QM_IDLE         0           4
pix506-635#
```

- **show crypto ipsec sa**: Zeigt zwischen Peers erstellte IPsec-SAs an.

```
pix506-635#show crypto ipsec sa


interface: outside
Crypto map tag: _vpnc_cm, local addr. 10.10.10.1

local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.22.1.0/255.255.255.0/0/0)
current_peer: 10.20.20.1:500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 706, #pkts encrypt: 706, #pkts digest 706
#pkts decaps: 655, #pkts decrypt: 655, #pkts verify 655
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress f ailed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.20.20.1
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 9b94d824

inbound esp sas:
spi: 0x3ea12bbe(1050749886)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3, crypto map: _vpnc_cm
sa timing: remaining key lifetime (k/sec): (4607941/24712)
IV size: 8 bytes
replay detection support: Y


inbound ah sas:


inbound pcp sas:


outbound esp sas:
spi: 0x9b94d824(2610223140)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 4, crypto map: _vpnc_cm
sa timing: remaining key lifetime (k/sec): (4607958/24712)
IV size: 8 bytes
replay detection support: Y


outbound ah sas:


outbound pcp sas:
```

- **show vpnclient**: Zeigt Konfigurationsinformationen für VPN-Client oder EasyVPN-Remote-Geräte an.

```
pix506-635#show vpnclient
```

```
LOCAL CONFIGURATION
vpnclient server 10.20.20.1
vpnclient mode network-extension-mode
vpnclient vpngroup mytunnel password ********
vpnclient username cisco password ********
vpnclient enable

DOWNLOADED DYNAMIC POLICY
Current Server : 10.20.20.1
PFS Enabled : No
Secure Unit Authentication Enabled : No
User Authentication Enabled : No
Split Networks : 172.22.1.0/255.255.255.0
Backup Servers : None

pix506-635#
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Wenn Sie den EasyVPN-Remote-Hardware-Client und den EasyVPN-Server wie in diesem Dokument beschrieben eingerichtet haben und weiterhin Probleme auftreten, sammeln Sie die **Debug-**Ausgabe jedes PIX und die Ausgabe der Befehle **show** zur Analyse durch den technischen Support von Cisco. Weitere Informationen finden Sie unter Fehlerbehebung bei PIX zur Weiterleitung des Datenverkehrs an einen etablierten IPSec-Tunnel oder IP Security Troubleshooting - Understanding and Using debug Commands. Aktivieren Sie IPsec-Debugging auf dem PIX.

In diesen Abschnitten werden PIX-**Debug-**Befehle und Beispielausgaben angezeigt.

- EasyVPN-Serverbefehle
- Befehle des EasyVPN-Remote-Hardware-Client

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**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

EasyVPN-Serverbefehle

- **debug crypto ipsec**: Zeigt die IPsec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen von Phase 1 an.

Beispielausgaben werden hier angezeigt.

```
ASA5520-704#debug crypto ipsec 2
ASA5520-704#debug crypto isakmp 2
ASA5520-704# Sep 15 23:02:42 [IKEv1]: IP = 10.10.10.1, Connection landed
on tunnel_group mytunnel
Sep 15 23:02:43 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
User (cisco) authenticated.
Sep 15 23:02:48 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
PHASE 1 COMPLETED
```

```
Sep 15 23:02:48 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
IKE: requesting SPI!
Sep 15 23:02:48 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
Security negotiation complete for User (cisco)  Responder, Inbound SPI = 0x436fbef1,
Outbound SPI = 0x5c6b5137
Sep 15 23:02:48 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
IKE: requesting SPI!
Sep 15 23:02:48 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
Starting P2 Rekey timer to expire in 27360 seconds
Sep 15 23:02:48 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
PHASE 2 COMPLETED (msgid=dc3aa1ef)
Sep 15 23:02:48 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
Security negotiation complete for User (cisco)  Responder, Inbound SPI = 0x69352d74,
Outbound SPI = 0x4a7e47fc
Sep 15 23:02:48 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
Starting P2 Rekey timer to expire in 27360 seconds
Sep 15 23:02:48 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1,
PHASE 2 COMPLETED (msgid=58a397ad)
```

Befehle des EasyVPN-Remote-Hardware-Client

- **debug crypto ipsec**: Zeigt die IPsec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen von Phase 1 an.

```
pix506-635(config)#vpnclient enable

ISAKMP (0): ID payload
next-payload : 13
type : 11
protocol : 17
port : 0
length : 12pix506-635(config)#
ISAKMP (0): Total payload length: 16
ISAKMP (0:0): sending NAT-T vendor ID - rev 2 & 3
ISAKMP (0): beginning Aggressive Mode exchange
crypto_isakmp_process_block:src:10.20.20.1, dest:10.10.10.1 spt:500 dpt:500
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 9 against priority 65001 policy
ISAKMP: encryption DES-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 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 9 against priority 65002 policy
ISAKMP: encryption DES-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 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 9 against priority 65003 policy
ISAKMP: encryption DES-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 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 9 against priority 65004 policy
```

```
ISAKMP: encryption DES-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 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 9 against priority 65005 policy
ISAKMP: encryption DES-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 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 9 against priority 65006 policy
ISAKMP: encryption DES-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 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 9 against priority 65007 policy
ISAKMP: encryption DES-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 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 9 against priority 65008 policy
ISAKMP: encryption DES-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 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
ISAKMP (0): Checking ISAKMP transform 9 against priority 65009 policy
ISAKMP: encryption DES-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 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
crypto_isakmp_process_block:src:10.20.20.1, dest:10.10.10.1 spt:500 dpt:500
crypto_isakmp_process_block:src:10.20.20.1, dest:10.10.10.1 spt:500 dpt:500
ISAKMP : attributes being requested

crypto_isakmp_process_block:src:10.20.20.1, dest:10.10.10.1 spt:500 dpt:500
ISAKMP (0): beginning Quick Mode exchange, M-ID of 1567562998:5d6f1cf6IPSEC
(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x411cf95(68276117) for SA
from 10.20.20.1 to 10.10.10.1 for prot 3

crypto_isakmp_process_block:src:10.20.20.1, dest:10.10.10.1 spt:500 dpt:500
```

```
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1567562998

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: encaps is 1
ISAKMP: authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
proposal part #1,
(key eng. msg.) dest= 10.20.20.1, src= 10.10.10.1,
dest_proxy= 172.22.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1567562998

ISAKMP (0): processing ID payload. message ID = 1567562998
ISAKMP (0): processing ID payload. message ID = 1567562998
ISAKMP (0): Creating IPSec SAs
inbound SA from 10.20.20.1 to 10.10.10.1 (proxy 172.22.1.0 to 10.10.10.1)
has spi 68276117 and conn_id 5 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 10.10.10.1 to 10.20.20.1 (proxy 10.10.10.1 to 172.22.1.0)
has spi 418090151 and conn_id 6 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 10.10.10.1, src= 10.20.20.1,
dest_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1),
src_proxy= 172.22.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x411cf95(68276117), conn_id= 5, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 10.10.10.1, dest= 10.20.20.1,
src_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1),
dest_proxy= 172.22.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x18eb8ca7(418090151), conn_id= 6, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:10.20.20.1/500 Ref cnt incremented to:2
Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:10.20.20.1/500 Ref cnt incremented to:3
Total VPN Peers:1
return status is IKMP_NO_ERROR
ISAKMP (0): beginning Quick Mode exchange,
M-ID of 43279810:29465c2IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xa12022dd(2703237853) for SA
from 10.20.20.1 to 10.10.10.1 for prot 3

crypto_isakmp_process_block:src:10.20.20.1, dest:10.10.10.1 spt:500 dpt:500
OAK_QM exchange
```

```
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 43279810

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: encaps is 1
ISAKMP: authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal
part #1,
(key eng. msg.) dest= 10.20.20.1, src= 10.10.10.1,
dest_proxy= 10.20.20.1/255.255.255.255/0/0 (type=1),
src_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 43279810

ISAKMP (0): processing ID payload. message ID = 43279810
ISAKMP (0): processing ID payload. message ID = 43279810
ISAKMP (0): Creating IPSec SAs
inbound SA from 10.20.20.1 to 10.10.10.1 (proxy 10.20.20.1 to 10.10.10.1)
has spi 2703237853 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 10.10.10.1 to 10.20.20.1 (proxy 10.10.10.1 to 10.20.20.1)
has spi 1010314457 and conn_id 4 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 10.10.10.1, src= 10.20.20.1,
dest_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1),
src_proxy= 10.20.20.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xa12022dd(2703237853), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 10.10.10.1, dest= 10.20.20.1,
src_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1),
dest_proxy= 10.20.20.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x3c382cd9(1010314457), conn_id= 4, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:10.20.20.1/500 Ref cnt incremented to:4 Total
VPN Peers:1
VPN Peer: IPSEC: Peer ip:10.20.20.1/500 Ref cnt incremented to:5 Total
VPN Peers:1
return status is IKMP_NO_ERROR
ISAKMP (0): sending NOTIFY message 36136 protocol 1
crypto_isakmp_process_block:src:10.20.20.1, dest:10.10.10.1 spt:500 dpt:500
ISAKMP (0): processing NOTIFY payload 36137 protocol 1
spi 0, message ID = 1608818011
ISAMKP (0): received DPD_R_U_THERE_ACK from peer 10.20.20.1
return status is IKMP_NO_ERR_NO_TRANS
pix506-635(config)#
```

- **debug vpnclient**: Zeigt die Verhandlungen speziell für den VPN-Client an.

```
pix506-635(config)#vpnclient enable
pix506-635(config)# 44: VPNC CFG: transform set unconfig attempt done
45: VPNC CLI: no isakmp keepalive 10 5
46: VPNC CLI: no isakmp nat-traversal 20
47: VPNC CFG: IKE unconfig successful
48: VPNC CLI: no crypto map _vpnc_cm
49: VPNC CFG: crypto map deletion attempt done
50: VPNC CFG: crypto unconfig successful
51: VPNC CLI: no global (outside) 65001
52: VPNC CLI: no nat (inside) 0 access-list _vpnc_acl
53: VPNC CFG: nat unconfig attempt failed
54: VPNC CLI: no http 172.16.1.1 255.255.255.0 inside
55: VPNC CLI: no http server enable
56: VPNC CLI: no access-list _vpnc_acl
57: VPNC CFG: ACL deletion attempt failed
58: VPNC CLI: no crypto map _vpnc_cm interface outside
59: VPNC CFG: crypto map de/attach failed
60: VPNC CLI: no sysopt connection permit-ipsec
61: VPNC CLI: sysopt connection permit-ipsec
62: VPNC CFG: transform sets configured
63: VPNC CFG: crypto config successful
64: VPNC CLI: isakmp keepalive 10 5
65: VPNC CLI: isakmp nat-traversal 20
66: VPNC CFG: IKE config successful
67: VPNC CLI: http 172.16.1.1 255.255.255.0 inside
68: VPNC CLI: http server enable
69: VPNC CLI: aaa-server _vpnc_nwp_server protocol tacacs+
70: VPNC CLI: aaa-server _vpnc_nwp_server (outside) host 10.20.20.1
71: VPNC CLI: access-list _vpnc_nwp_acl permit ip any 172.22.1.0 255.255.255.0
72: VPNC CLI: aaa authentication match _vpnc_nwp_acl outbound _vpnc_nwp_server
73: VPNC CLI: no access-list _vpnc_acl
74: VPNC CFG: ACL deletion attempt failed
75: VPNC CLI: access-list _vpnc_acl permit ip host 10.10.10.1 host 10.20.20.1
76: VPNC CLI: crypto map _vpnc_cm 10 match address _vpnc_acl
77: VPNC CFG: crypto map acl update successful
78: VPNC CLI: no crypto map _vpnc_cm interface outside
79: VPNC CLI: crypto map _vpnc_cm interface outside
80: VPNC INF: IKE trigger request done
81: VPNC INF: Constructing policy download req
82: VPNC INF: Packing attributes for policy request
83: VPNC INF: Attributes being requested
84: VPNC ATT: ALT_SPLIT_INCLUDE
85: VPNC INF:   172.22.1.0/255.255.255.0
86: VPNC ATT: ALT_PFS: 0
87: VPNC INF: Received application version 'Cisco Systems, Inc
ASA5520 Version 7.0(4) built by builders on Thu 13-Oct-05 21:43'
88: VPNC ATT: ALT_CFG_SEC_UNIT: 0
89: VPNC ATT: ALT_CFG_USER_AUTH: 0
90: VPNC CLI: no aaa authentication match _vpnc_nwp_acl outbound _vpnc_nwp_server
91: VPNC CLI: no access-list _vpnc_nwp_acl permit ip any 172.22.1.0 255.255.255.0
92: VPNC CLI: no aaa-server _vpnc_nwp_server
93: VPNC CLI: no access-list _vpnc_acl
94: VPNC CLI: access-list _vpnc_acl permit ip 172.16.1.0 255.255.255.0
172.22.1.0 255.255.255.0
95: VPNC CLI: access-list _vpnc_acl permit ip host 10.10.10.1 172.22.1.0
255.255.255.0
96: VPNC CLI: access-list _vpnc_acl permit ip host 10.10.10.1 host 10.20.20.1
97: VPNC CFG: _vpnc_acl ST define done
98: VPNC CFG: Split DNS config attempt done
99: VPNC CLI: crypto map _vpnc_cm 10 match address _vpnc_acl
100: VPNC CFG: crypto map acl update successful
101: VPNC CLI: no crypto map _vpnc_cm interface outside
```

```
102: VPNC CLI: crypto map _vpnc_cm interface outside
103: VPNC CLI: no global (outside) 65001
104: VPNC CLI: no nat (inside) 0 access-list _vpnc_acl
105: VPNC CFG: nat unconfig attempt failed
106: VPNC CLI: nat (inside) 0 access-list _vpnc_acl
107: VPNC INF: IKE trigger request done
108: VPNC INF: IKE trigger request done

pix506-635(config)#
```

Zugehörige Informationen

- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation für Cisco Systeme