Terminierende IPSec-Tunnel auf mehreren Cisco Secure PIX Firewall-Schnittstellen mit Xauth

Inhalt

Einführung

In diesem Dokument wird eine IPSec-Konfiguration mit den folgenden Elementen veranschaulicht: Crypto Maps werden auf mehrere Schnittstellen des PIX angewendet; erweiterte Authentifizierung (xauth) von VPN-Clients; dynamische Zuweisung einer privaten IP-Adresse aus einem Pool zu VPN-Clients; Befehlsfunktionalität und **nat 0-Zugriffslisten**, mit der Hosts in einem LAN private IP-Adressen mit einem Remote-Benutzer verwenden können und dennoch eine NAT-Adresse (Network Address Translation) vom PIX erhalten, um ein nicht vertrauenswürdiges Netzwerk aufzurufen.

Diese Konfiguration hat die folgenden Ziele:

- Authentifizierung eines Remote-Benutzers anhand einer TACACS+-Datenbank.
- Dynamische Zuweisung einer privaten IP-Adresse zu einem Remote-Benutzer.
- Verschlüsselung des Datenverkehrs von einem Remote-Benutzer zu einem Hub-PIX
- Verschlüsselung des Datenverkehrs von einem Hub-PIX zu einem LAN

Hinweis: Bei der Erstellung dieses Dokuments werden die erstellten Sicherheitszuordnungen (Security Associations, SAs) durch eine falsche Anmeldung beim AAA-Server (Authentication, Authorization, Accounting) gelöscht.

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Diese Konfiguration wurde mit den unten stehenden Software- und Hardwareversionen entwickelt und getestet.

- Cisco IOS® Software Version 12.2.8.T oder höher
- Cisco PIX IOS Version 6.1(1)
- Cisco VPN Client 3.5

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

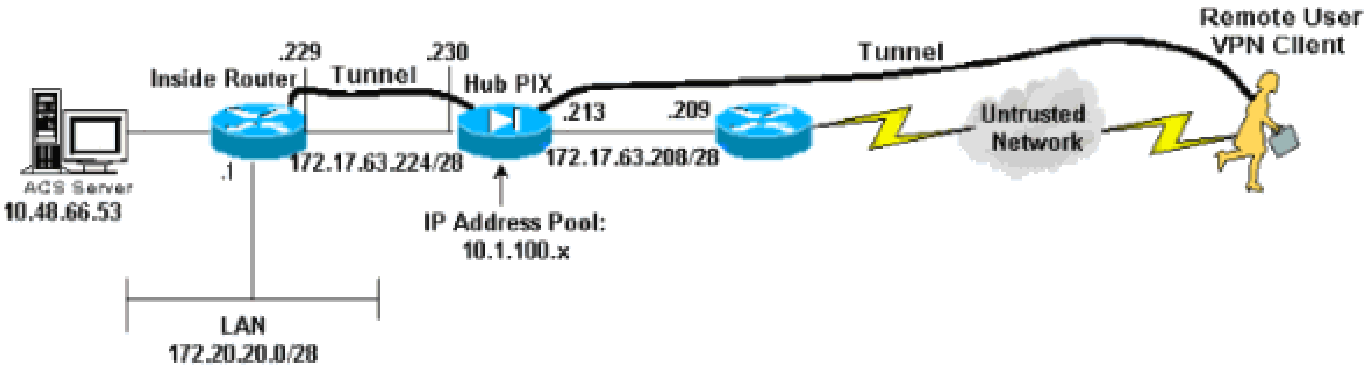
Konfigurieren

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

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden die unten angegebenen Konfigurationen verwendet.

- Hub-PIX-Konfiguration

- Konfiguration des internen Routers
- VPN-Client-Konfiguration

Hub-PIX-Konfiguration

```
PIX Version 6.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname HubPix
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list nonat permit ip 172.20.20.0 255.255.255.0
10.1.100.0 255.255.255.0
access-list 125 permit ip 10.1.100.0 255.255.255.0
172.20.20.0 255.255.255.0
pager lines 24
logging console debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
ip address outside 172.17.63.213 255.255.255.240
ip address inside 172.17.63.230 255.255.255.240
ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 25(B5.255.255.255
ip audit info action alarm
ip audit attack action alarm
ip local pool mypool 10.1.100.1-10.1.100.254
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
failover ip address intf3 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 172.17.63.210
nat (inside) 0 access-list nonat
nat (inside) 1 172.20.20.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 172.17.63.209 1
route inside 10.48.66.53 255.255.255.255 172.17.63.229 1
route inside 172.20.20.0 255.255.255.0 172.17.63.229 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00
```

```
h323 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 partner protocol tacacs+
aaa-server partner (inside) host 10.48.66.53 cisco123
timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt ipsec pl-compatible
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map internal 10 ipsec-isakmp
crypto map internal 10 match address 125
crypto map internal 10 set peer 172.17.63.229
crypto map internal 10 set transform-set myset
crypto map internal interface inside
crypto map dyn-map 10 ipsec-isakmp dynamic dynmap
crypto map dyn-map client authentication partner
crypto map dyn-map interface outside
isakmp enable outside
isakmp enable inside
isakmp key ******** address 172.17.63.229 netmask
255.255.255.255
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password ********
vpngroup vpn3 address-pool mypool
vpngroup vpn3 dns-server 172.20.20.2
vpngroup vpn3 wins-server 172.20.20.2
vpngroup vpn3 default-domain cisco.com
vpngroup vpn3 idle-time 1800
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:fcd6d79f6a662b82e5f450ed833f34e6
: end
[OK]
```

Konfiguration des internen Routers

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname inside
!
enable password ww
!
ip subnet-zero
ip cef
!
```

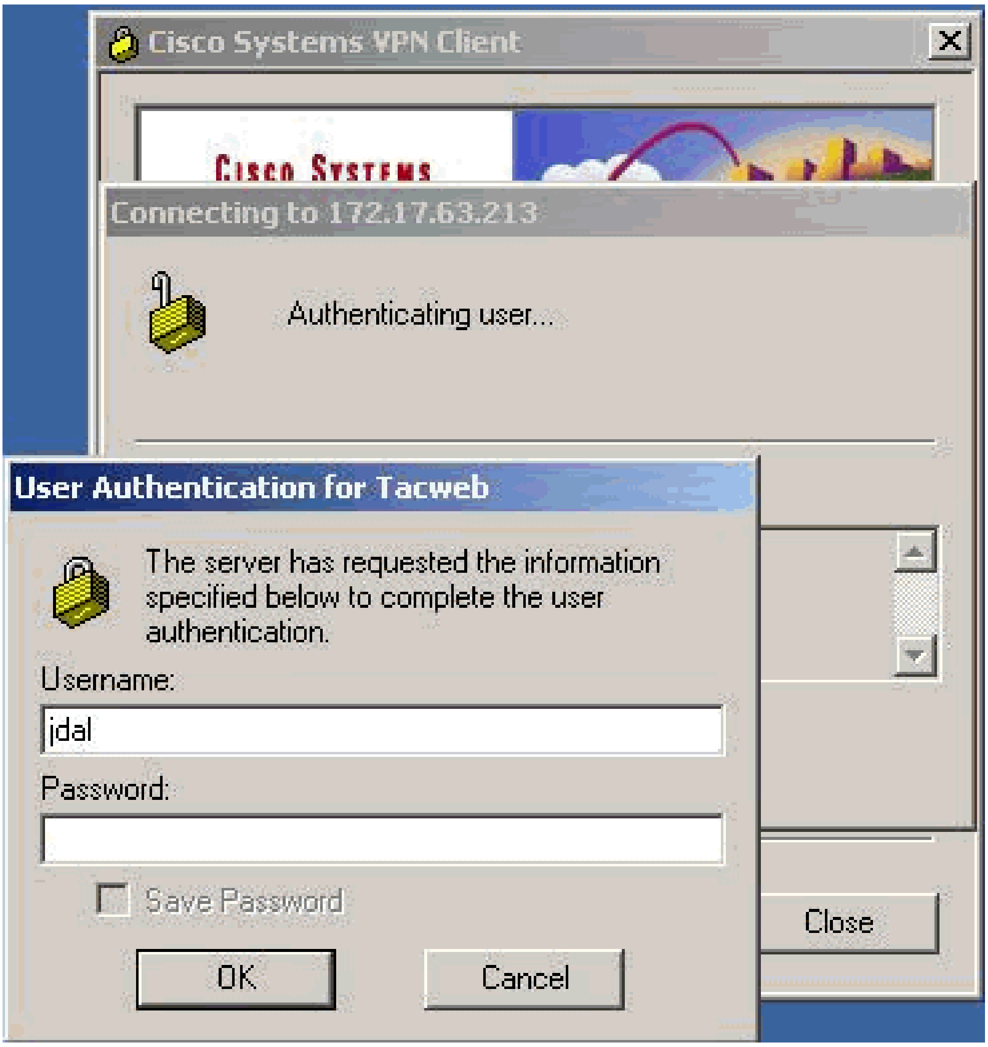
```
!
!
ip audit notify log
ip audit po max-events 100
!
!--- Create an Internet Security Association and Key
Management Protocol (ISAKMP) !--- policy for Phase 1
negotiations for the VPN 3.x Clients. crypto isakmp
policy 10
 hash md5
 authentication pre-share
 group 2
!--- Specify the pre-shared key for the LAN-to-LAN
tunnel. crypto isakmp key ciscotac address 172.17.63.230
!
!
!--- Create the Phase 2 Policy for actual data
encryption. crypto ipsec transform-set tacset esp-des
esp-md5-hmac
!
!--- Create the actual crypto map. crypto map tacmap 25
ipsec-isakmp
 set peer 172.17.63.230
 set transform-set tacset
 match address 105
!
!
!
!
!
!
!
!
!
controller ISA 6/1
!
!
!
!
interface Serial2/0
 no ip address
 shutdown
 serial restart_delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart_delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart_delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart_delay 0
!
interface FastEthernet3/0
 ip address 10.48.66.46 255.255.254.0
 duplex half
!
!--- Apply the crypto map on the outside interface.
```

```
interface FastEthernet3/1 ip address 172.17.63.229
255.255.255.240
 duplex half
 crypto map tacmap
!
interface FastEthernet5/0
 ip address 172.20.20.20 255.255.255.0
 duplex half
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.63.230
no ip http server
ip pim bidir-enable
!
!
access-list 105 permit ip 172.20.20.0 0.0.0.255
10.1.100.0 0.0.0.255
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

VPN-Client-Konfiguration

Die folgenden Schritte beschreiben die Konfiguration für den VPN-Client.

1. Doppelklicken Sie nach der Anmeldung beim VPN-Client auf das gelbe Vorhängeschloss in Ihrer Taskleiste, und melden Sie sich an, indem Sie **Connect**



The server has requested the information specified below to complete the user authentication.

Username: jdal

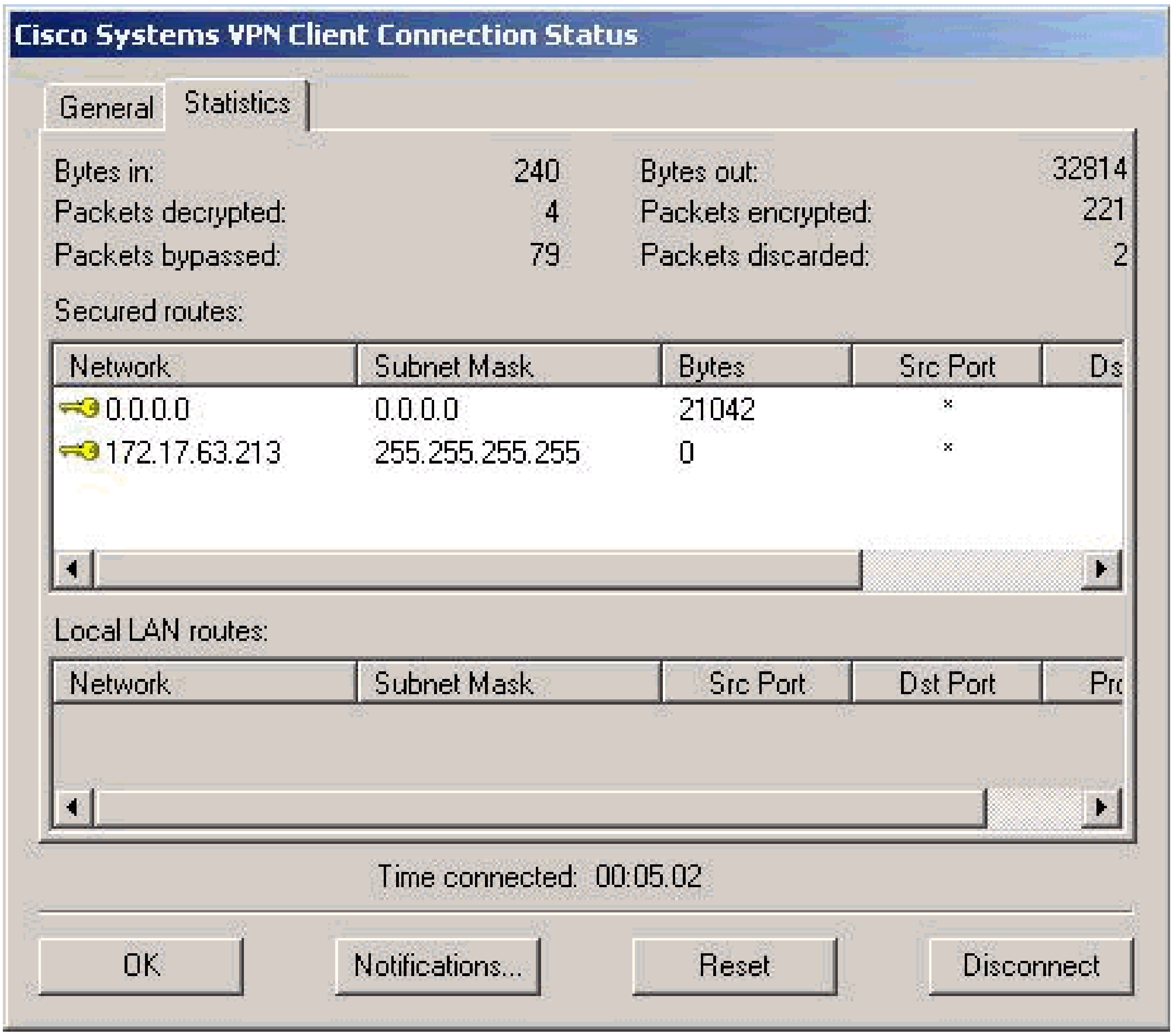
Password:

□ Save Password

OK Cancel

auswählen.

2. Um Verbindungsstatistiken anzuzeigen, doppelklicken Sie beim Herstellen des Tunnels auf das gelbe Vorhängeschloss, und der folgende Bildschirm wird angezeigt.



Bytes in: 240 Bytes out: 32814
Packets decrypted: 4 Packets encrypted: 221
Packets bypassed: 79 Packets discarded: 2

Secured routes:

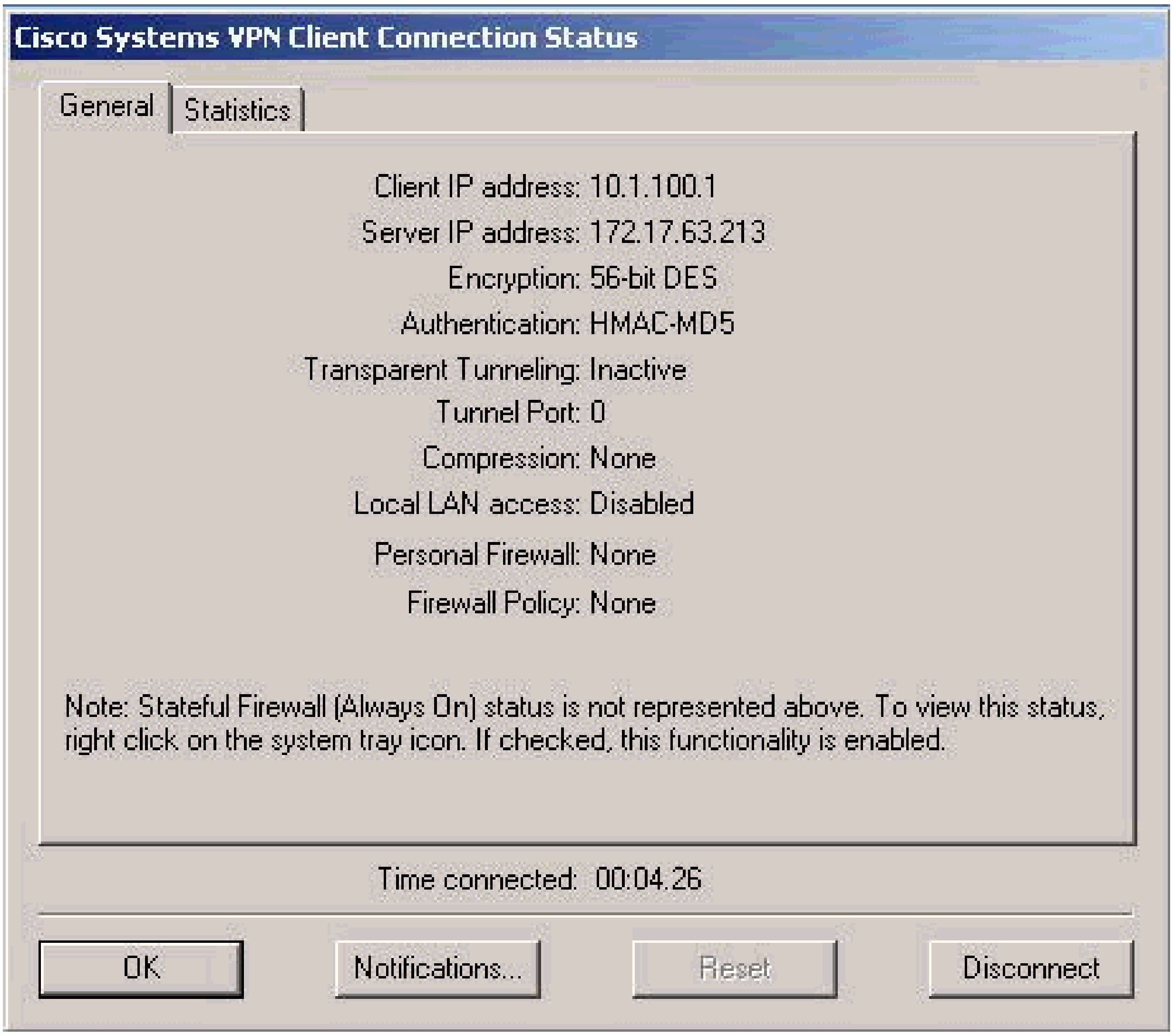
Network	Subnet Mask	Bytes	Src Port	Ds
0.0.0.0	0.0.0.0	21042	*	
172.17.63.213	255.255.255.255	0	*	

Local LAN routes:

Network	Subnet Mask	Src Port	Dst Port	Prc

Time connected: 00:05.02

3. Wählen Sie die Registerkarte Allgemein für Konfigurationsinformationen des VPN-Clients



Cisco Systems VPN Client Connection Status

Client IP address: 10.1.100.1
Server IP address: 172.17.63.213
Encryption: 56-bit DES
Authentication: HMAC-MD5
Transparent Tunneling: Inactive
Tunnel Port: 0
Compression: None
Local LAN access: Disabled
Personal Firewall: None
Firewall Policy: None

Note: Stateful Firewall (Always On) status is not represented above. To view this status, right click on the system tray icon. If checked, this functionality is enabled.

Time connected: 00:04.26

aus.

```
Remote Party Identity and Addressing

   ID Type:  IP Subnet
   Subnet:   172.20.20.0
   Mask:     255.255.255.0
   Port:     all

Connect Using Secure Gateway Tunnel - Checked

   Type:     IP Address
   Address:  172.17.63.213


My Identity:
     Preshared Key


Authentication (Phase I -- Proposal 1)
     Authentication Method:     Preshared Key
     Encryption Algorithm:      DES
     Hash Algorithm:            MD5
     SALife:                    Unspecified
     Key Group:                 Diffie-Hellmen 1



Key Exchange (PhaseII -- Proposal 1)
     SALife:                     Unspecified
     Encapsulation Protocol:     ESP
     Encryption Algorithm:       DES
```

```
          Hash Algorithm:                MD5
          Encapsulation:                 Tunnel
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

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

Die **show**-Befehle können auf dem PIX und dem Router ausgeführt werden.

- **show crypto isakmp sa** - Zeigt Sicherheitszuordnungen für Phase 1 an.
- **show crypto ipsec sa** - Zeigt Sicherheitszuordnungen und Proxy-, Verschlüsselungs-, Entschlüsselungs-, Entschlüsselungs- und Entschlüsselungsinformationen in Phase 1 an.
- **show crypto engine connections active** - (nur Router) Zeigt aktuelle verbindungen und Informationen über verschlüsselte und entschlüsselte pakete

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Bevor Sie einen der folgenden Debugbefehle ausprobieren, lesen Sie bitte Wichtige Informationen über Debug-Befehle. Weitere Informationen finden Sie auch in den folgenden Debugausgaben.

- Hub-PIX-Debugger
- Debugger für interne Router
- VPN-Clientprotokoll

Das Löschen von Sicherheitszuordnungen muss auf beiden Peers erfolgen. Die PIX-Befehle werden im Konfigurationsmodus ausgeführt.

- **clear crypto isakmp sa** - (PIX) Löscht die Sicherheitszuordnungen für Phase 1.
- **clear crypto ipsec sa** - (PIX) Löscht die Sicherheitszuordnungen für Phase 2.
- **clear crypto isakmp** - (Router) Löscht die Sicherheitszuordnungen für Phase 1.
- **clear crypto sa** - (Router) Löscht die Sicherheitszuordnungen in Phase 2.

Die folgenden Debuggings müssen auf beiden IPSec-Peers ausgeführt werden.

- **debug crypto isakmp** - (Router und PIX) zeigt während Phase 1 Fehler an.
- **debug crypto ipsec** - (Router und PIX) Zeigt während Phase 2 Fehler an.
- **debug crypto engine** - (nur Router) Zeigt Informationen von der Crypto Engine an.

Hub-PIX-Debugger

```
HubPix(config)#
 crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
 VPN Peer: ISAKMP: Added new peer: ip:30.30.30.2 Total VPN Peers:1
 VPN Peer: ISAKMP: Peer ip:30.30.30.2 Ref cnt incremented to:1
    Total VPN Peers:1
```

```
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption 3DES-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 (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
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 vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload
ISAKMP (0): speaking to a Unity client

ISAKMP: Created a peer node for 30.30.30.2
ISAKMP (0): ID payload
        next-payload : 10
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
        spi 0, message ID = 0
ISAKMP (0): processing notify INITIAL_CONTACT
IPSEC(key_engine): got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 30.30.30.2

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 30.30.30.2.
   ID = 1990788923 (0x76a9073b)
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 30.30.30.2. message ID = 76
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
ISAKMP (0:0): phase 2 packet is a duplicate of a previous packet.
ISAKMP (0:0): initiating peer config to 30.30.30.2. ID = 167380747 (0x9fa070b)
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 30.30.30.2. message ID = 60
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 30.30.30.2. message ID = 0
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute    IP4_ADDRESS (1)
ISAKMP: attribute    IP4_NETMASK (2)
ISAKMP: attribute    IP4_DNS (3)
ISAKMP: attribute    IP4_NBNS (4)
ISAKMP: attribute    ADDRESS_EXPIRY (5)
        Unsupported Attr: 5
ISAKMP: attribute    APPLICATION_VERSION (7)
        Unsupported Attr: 7
ISAKMP: attribute    UNKNOWN (28672)
        Unsupported Attr: 28672
ISAKMP: attribute    UNKNOWN (28673)
        Unsupported Attr: 28673
ISAKMP: attribute    UNKNOWN (28674)
ISAKMP: attribute    UNKNOWN (28676)
ISAKMP: attribute    UNKNOWN (28679)
        Unsupported Attr: 28679
ISAKMP: attribute    UNKNOWN (28680)
        Unsupported Attr: 28680
```

```
ISAKMP: attribute    UNKNOWN (28677)
        Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 30.30.30.2. ID = 2994966739
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2019793958

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 3, hmac_alg 1) not supported

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_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (2)
ISAKMP : Checking IPSec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
```

```
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (6)
ISAKMP : Checking IPSec proposal 7

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.17.63.213, src= 30.30.30.2,
    dest_proxy= 172.17.63.213/255.255.255.255/0/0 (type=1),
    src_proxy= 10.1.100.1/255.255.255.255/0/0 (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 = 2019793958

ISAKMP (0): processing ID payload. message ID = 2019793958
ISAKMP (0): ID_IPV4_ADDR src 10.1.100.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 2019793958
ISAKMP (0): ID_IPV4_ADDR dst 172.17.63.213 prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x91e92b8(152998584) for SA
        from 30.30.30.2 to 172.17.63.213 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3584084796

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 6
map_alloc_entry: allocating entry 5
```

```
ISAKMP (0): Creating IPSec SAs
        inbound SA from 30.30.30.2 to 172.17.63.213
        (proxy 10.1.100.1 to 172.17.63.213)
        has spi 152998584 and conn_id 6 and flags 4
        lifetime of 2147483 seconds
        outbound SA from 172.17.63.213 to 30.30.30.2
       (proxy 172.17.63.213 to 10.1.100.1)
        has spi 2121955223 and conn_id 5 and flags 4
        lifetime of 2147483 seconds
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.17.63.213, src= 30.30.30.2,
    dest_proxy= 172.17.63.213/0.0.0.0/0/0 (type=1),
    src_proxy= 10.1.100.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0x91e92b8(152998584), conn_id= 6, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.17.63.213, dest= 30.30.30.2,
    src_proxy= 172.17.63.213/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.1.100.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0x7e7a7797(2121955223), conn_id= 5, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:30.30.30.2 Ref cnt incremented to:2
   Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:30.30.30.2 Ref cnt incremented to:3
   Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 4
map_alloc_entry: allocating entry 3

ISAKMP (0): Creating IPSec SAs
        inbound SA from 30.30.30.2 to 172.17.63.213
        (proxy 10.1.100.1 to 0.0.0.0)
        has spi 3202697335 and conn_id 4 and flags 4
        lifetime of 2147483 seconds
        outbound SA from 172.17.63.213 to 30.30.30.2
        (proxy 0.0.0.0 to 10.1.100.1)
        has spi 771522089 and conn_id 3 and flags 4
        lifetime of 2147483 seconds
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.17.63.213, src= 30.30.30.2,
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.1.100.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xbee54877(3202697335), conn_id= 4, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.17.63.213, dest= 30.30.30.2,
    src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    dest_proxy= 10.1.100.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0x2dfc7e29(771522089), conn_id= 3, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:30.30.30.2 Ref cnt incremented to:4
   Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:30.30.30.2 Ref cnt incremented to:5
```

```
   Total VPN Peers:1
return status is IKMP_NO_ERROR
VPN Peer: ISAKMP: Added new peer: ip:172.17.63.229 Total VPN Peers:2
VPN Peer: ISAKMP: Peer ip:172.17.63.229 Ref cnt incremented to:1
   Total VPN Peers:2
ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block: src 172.17.63.229, dest 172.17.63.230
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using
   id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.17.63.229, dest 172.17.63.230
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

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

ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

ISAKMP (0): processing vendor id payload

ISAKMP (0): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
        spi 0, message ID = 409920160
ISAMKP (0): received DPD_R_U_THERE from peer 30.30.30.2
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block: src 172.17.63.229, dest 172.17.63.230
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange, M-ID of -498320091:e24c3d25
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xcad23b33(3402775347) for SA
        from   172.17.63.229 to   172.17.63.230 for prot 3

return status is IKMP_NO_ERROR
```

```
ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 172.17.63.229, dest 172.17.63.230
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3796647205

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
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:      authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.17.63.229, src= 172.17.63.230,
    dest_proxy= 172.20.20.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.1.100.0/255.255.255.0/0/0 (type=4),
    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 = 3796647205

ISAKMP (0): processing ID payload. message ID = 3796647205
ISAKMP (0): processing ID payload. message ID = 3796647205
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
        spi 691534456, message ID = 3796647205
ISAKMP (0): processing responder lifetime
ISAKMP (0): responder lifetime of 3600smap_alloc_entry: allocating entry 8
map_alloc_entry: allocating entry 7

ISAKMP (0): Creating IPSec SAs
        inbound SA from 172.17.63.229 to 172.17.63.230
       (proxy 172.20.20.0 to 10.1.100.0)
        has spi 3402775347 and conn_id 8 and flags 4
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytes
        outbound SA from 172.17.63.230 to 172.17.63.229
       (proxy 10.1.100.0 to 172.20.20.0)
        has spi 691534456 and conn_id 7 and flags 4
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytes
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.17.63.230, src= 172.17.63.229,
    dest_proxy= 10.1.100.0/255.255.255.0/0/0 (type=4),
    src_proxy= 172.20.20.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xcad23b33(3402775347), conn_id= 8, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.17.63.230, dest= 172.17.63.229,
    src_proxy= 10.1.100.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 172.20.20.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x2937fa78(691534456), conn_id= 7, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:172.17.63.229 Ref cnt incremented to:2
```

```
    Total VPN Peers:2
 VPN Peer: IPSEC: Peer ip:172.17.63.229 Ref cnt incremented to:3
    Total VPN Peers:2
 return status is IKMP_NO_ERROR
 HubPix(config)#
 HubPix(config)#
 crypto_isakmp_process_block: src 30.30.30.2, dest 172.17.63.213
 ISAKMP (0): processing NOTIFY payload 36136 protocol 1
         spi 0, message ID = 2020571710
 ISAMKP (0): received DPD_R_U_THERE from peer 30.30.30.2
 ISAKMP (0): sending NOTIFY message 36137 protocol 1
 return status is IKMP_NO_ERR_NO_TRANS
 HubPix(config)#
```

Debugger für interne Router

```
inside#
 01:45:06: ISAKMP (0:0): received packet from 172.17.63.230 (N) NEW SA
 01:45:06: ISAKMP: local port 500, remote port 500
 01:45:06: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
 Old State = IKE_READY  New State = IKE_R_MM1

 01:45:06: ISAKMP (0:1): processing SA payload. message ID = 0
 01:45:06: ISAKMP (0:1): found peer pre-shared key matching 172.17.63.230
 01:45:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 10 policy
 01:45:06: ISAKMP:      encryption DES-CBC
 01:45:06: ISAKMP:      hash MD5
 01:45:06: ISAKMP:      default group 2
 01:45:06: ISAKMP:      auth pre-share
 01:45:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
 01:45:06: CryptoEngine0: generate alg parameter
 01:45:06: CryptoEngine0: CRYPTO_ISA_DH_CREATE(hw)(ipsec)
 01:45:06: CRYPTO_ENGINE: Dh phase 1 status: 0
 01:45:06: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
 Old State = IKE_R_MM1  New State = IKE_R_MM1

 01:45:06: ISAKMP (0:1): sending packet to 172.17.63.230 (R) MM_SA_SETUP
 01:45:06: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
 Old State = IKE_R_MM1  New State = IKE_R_MM2

 01:45:06: ISAKMP (0:1): received packet from 172.17.63.230 (R) MM_SA_SETUP
 01:45:06: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
 Old State = IKE_R_MM2  New State = IKE_R_MM3

 01:45:06: ISAKMP (0:1): processing KE payload. message ID = 0
 01:45:06: CryptoEngine0: generate alg parameter
 01:45:06: CryptoEngine0: CRYPTO_ISA_DH_SHARE_SECRET(hw)(ipsec)
 01:45:07: ISAKMP (0:1): processing NONCE payload. message ID = 0
 01:45:07: ISAKMP (0:1): found peer pre-shared key matching 172.17.63.230
 01:45:07: CryptoEngine0: create ISAKMP SKEYID for conn id 1
 01:45:07: CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw)(ipsec)
 01:45:07: ISAKMP (0:1): SKEYID state generated
 01:45:07: ISAKMP (0:1): processing vendor id payload
 01:45:07: ISAKMP (0:1): vendor ID is Unity
 01:45:07: ISAKMP (0:1): processing vendor id payload
 01:45:07: ISAKMP (0:1): vendor ID is DPD
 01:45:07: ISAKMP (0:1): processing vendor id payload
 01:45:07: ISAKMP (0:1): speaking to another IOS box!
 01:45:07: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
 Old State = IKE_R_MM3  New State = IKE_R_MM3

 01:45:07: ISAKMP (0:1): sending packet to 172.17.63.230 (R) MM_KEY_EXCH
 01:45:07: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
```

```
Old State = IKE_R_MM3  New State = IKE_R_MM4

01:45:07: ISAKMP (0:1): received packet from 172.17.63.230 (R) MM_KEY_EXCH
01:45:07: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
01:45:07: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_R_MM4  New State = IKE_R_MM5

01:45:07: ISAKMP (0:1): processing ID payload. message ID = 0
01:45:07: ISAKMP (0:1): processing HASH payload. message ID = 0
01:45:07: CryptoEngine0: generate hmac context for conn id 1
01:45:07: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
01:45:07: ISAKMP (0:1): SA has been authenticated with 172.17.63.230
01:45:07: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5  New State = IKE_R_MM5

01:45:07: ISAKMP (0:1): SA is doing pre-shared key authentication using
   id type ID_IPV4_ADDR
01:45:07: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
01:45:07: ISAKMP (1): Total payload length: 12
01:45:07: CryptoEngine0: generate hmac context for conn id 1
01:45:07: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
01:45:07: CryptoEngine0: clear dh number for conn id 1
01:45:07: CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw)(ipsec)
01:45:07: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
01:45:07: ISAKMP (0:1): sending packet to 172.17.63.230 (R) QM_IDLE
01:45:07: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

01:45:07: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

01:45:08: ISAKMP (0:1): received packet from 172.17.63.230 (R) QM_IDLE
01:45:08: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
01:45:08: CryptoEngine0: generate hmac context for conn id 1
01:45:08: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
01:45:08: ISAKMP (0:1): processing HASH payload. message ID = -498320091
01:45:08: ISAKMP (0:1): processing SA payload. message ID = -498320091
01:45:08: ISAKMP (0:1): Checking IPSec proposal 1
01:45:08: ISAKMP: transform 1, ESP_DES
01:45:08: ISAKMP:   attributes in transform:
01:45:08: ISAKMP:      encaps is 1
01:45:08: ISAKMP:      SA life type in seconds
01:45:08: ISAKMP:      SA life duration (basic) of 28800
01:45:08: ISAKMP:      SA life type in kilobytes
01:45:08: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
01:45:08: ISAKMP:      authenticator is HMAC-MD5
01:45:08: validate proposal 0
01:45:08: ISAKMP (0:1): atts are acceptable.
01:45:08: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.17.63.229, remote= 172.17.63.230,
    local_proxy= 172.20.20.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.100.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
01:45:08: validate proposal request 0
01:45:08: ISAKMP (0:1): processing NONCE payload. message ID = -498320091
01:45:08: ISAKMP (0:1): processing ID payload. message ID = -498320091
01:45:08: ISAKMP (0:1): processing ID payload. message ID = -498320091
```

```
01:45:08: ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1
        spi 0, message ID = -498320091, sa = 62EF984C
01:45:08: ISAKMP (0:1): Process initial contact,
   bring down existing phase 1 and 2 SA's
01:45:08: ISAKMP (0:1): peer does not do paranoid keepalives.

01:45:08: ISAKMP (0:1): asking for 1 spis from ipsec
01:45:08: ISAKMP (0:1): Node -498320091,
   Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY  New State = IKE_QM_SPI_STARVE

01:45:08: IPSEC(key_engine): got a queue event...
01:45:08: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
01:45:08: IPSEC(key_engine_delete_sas): delete all SAs shared
   with 172.17.63.230
01:45:08: IPSEC(key_engine): got a queue event...
01:45:08: IPSEC(spi_response): getting spi 691534456 for SA
        from 172.17.63.229   to 172.17.63.230   for prot 3
01:45:08: ISAKMP: received ke message (2/1)
01:45:08: CryptoEngine0: generate hmac context for conn id 1
01:45:08: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
01:45:08: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
01:45:08: ISAKMP (0:1): sending packet to 172.17.63.230 (R) QM_IDLE
01:45:08: ISAKMP (0:1): Node -498320091,
   Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE  New State = IKE_QM_R_QM2

01:45:09: ISAKMP (0:1): received packet from 172.17.63.230 (R) QM_IDLE
01:45:09: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
01:45:09: CryptoEngine0: generate hmac context for conn id 1
01:45:09: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
01:45:09: ipsec allocate flow 0
01:45:09: ipsec allocate flow 0
01:45:09: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
01:45:09: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
01:45:09: ISAKMP (0:1): Creating IPSec SAs
01:45:09:         inbound SA from 172.17.63.230 to 172.17.63.229
        (proxy 10.1.100.0 to 172.20.20.0)
01:45:09:         has spi 0x2937FA78 and conn_id 2029 and flags 4
01:45:09:         lifetime of 28800 seconds
01:45:09:         lifetime of 4608000 kilobytes
01:45:09:         outbound SA from 172.17.63.229 to 172.17.63.230
        (proxy 172.20.20.0 to 10.1.100.0)
01:45:09:         has spi -892191949 and conn_id 2030 and flags C
01:45:09:         lifetime of 28800 seconds
01:45:09:         lifetime of 4608000 kilobytes
01:45:09: ISAKMP (0:1): deleting node -498320091 error FALSE
   reason "quick mode done (await()"
01:45:09: ISAKMP (0:1): Node -498320091,
   Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2  New State = IKE_QM_PHASE2_COMPLETE

01:45:09: IPSEC(key_engine): got a queue event...
01:45:09: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 172.17.63.229, remote= 172.17.63.230,
    local_proxy= 172.20.20.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.100.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x2937FA78(691534456), conn_id= 2029, keysize= 0, flags= 0x4
01:45:09: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 172.17.63.229, remote= 172.17.63.230,
    local_proxy= 172.20.20.0/255.255.255.0/0/0 (type=4),
    remote_proxy= 10.1.100.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0xCAD23B33(3402775347), conn_id= 2030, keysize= 0, flags= 0xC
01:45:09: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.17.63.229, sa_prot= 50,
    sa_spi= 0x2937FA78(691534456),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2029
01:45:09: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.17.63.230, sa_prot= 50,
    sa_spi= 0xCAD23B33(3402775347),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2030
inside#
```

VPN-Clientprotokoll

```
1679   13:21:53.420  04/13/02  Sev=Info/6       DIALER/0x63300002
 Initiating connection.

 1680   13:21:53.420  04/13/02  Sev=Info/4       CM/0x63100002
 Begin connection process

 1681   13:21:53.430  04/13/02  Sev=Info/4       CM/0x63100004
 Establish secure connection using Ethernet

 1682   13:21:53.430  04/13/02  Sev=Info/4       CM/0x63100026
 Attempt connection with server "172.17.63.213"

 1683   13:21:53.430  04/13/02  Sev=Info/6       IKE/0x6300003B
 Attempting to establish a connection with 172.17.63.213.

 1684   13:21:53.470  04/13/02  Sev=Info/4       IKE/0x63000013
 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID)
    to 172.17.63.213

 1685   13:21:53.671  04/13/02  Sev=Info/5       IKE/0x6300002F
 Received ISAKMP packet: peer = 172.17.63.213

 1686   13:21:53.671  04/13/02  Sev=Info/4       IKE/0x63000014
 RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH)
    from 172.17.63.213

 1687   13:21:53.671  04/13/02  Sev=Info/5       IKE/0x63000059
 Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

 1688   13:21:53.671  04/13/02  Sev=Info/5       IKE/0x63000001
 Peer is a Cisco-Unity compliant peer

 1689   13:21:53.671  04/13/02  Sev=Info/5       IKE/0x63000059
 Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

 1690   13:21:53.671  04/13/02  Sev=Info/5       IKE/0x63000001
 Peer supports DPD

 1691   13:21:53.671  04/13/02  Sev=Info/5       IKE/0x63000059
 Vendor ID payload = 4565726A4035E50EA2133A5813561EF2

 1692   13:21:53.701  04/13/02  Sev=Info/4       IKE/0x63000013
 SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
    to 172.17.63.213

 1693   13:21:54.071  04/13/02  Sev=Info/4       IPSEC/0x63700014
 Deleted all keys
```

```
1694   13:21:56.725  04/13/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 172.17.63.213

1695   13:21:56.725  04/13/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.17.63.213

1696   13:21:56.725  04/13/02  Sev=Info/4       CM/0x63100015
Launch xAuth application

1697   13:22:05.187  04/13/02  Sev=Info/4       CM/0x63100017
xAuth application returned

1698   13:22:05.187  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.17.63.213

1699   13:22:10.214  04/13/02  Sev=Info/4       IKE/0x63000056
Phase 2 exchange timed out (message id = 0x76A9073B). Retry count: 1

1700   13:22:10.214  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(Retransmission) to 172.17.63.213

1701   13:22:10.654  04/13/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 172.17.63.213

1702   13:22:10.654  04/13/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.17.63.213

1703   13:22:10.654  04/13/02  Sev=Info/4       CM/0x6310000E
Established Phase 1 SA.  1 Phase 1 SA in the system

1704   13:22:10.665  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.17.63.213

1705   13:22:10.675  04/13/02  Sev=Info/5       IKE/0x6300005D
Client sending a firewall request to concentrator

1706   13:22:10.675  04/13/02  Sev=Info/5       IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client,
   Capability= (Centralized Policy Push).

1707   13:22:10.675  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.17.63.213

1708   13:22:10.735  04/13/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 172.17.63.213

1709   13:22:10.735  04/13/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.17.63.213

1710   13:22:10.735  04/13/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.1.100.1

1711   13:22:10.735  04/13/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 172.20.20.2

1712   13:22:10.735  04/13/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : ,
   value = 172.20.20.2

1713   13:22:10.735  04/13/02  Sev=Info/5       IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = cisco.com

1714   13:22:10.735  04/13/02  Sev=Info/4       CM/0x63100019
```

```
Mode Config data received

1715   13:22:10.755  04/13/02  Sev=Info/5       IKE/0x63000055
Received a key request from Driver for IP address 172.17.63.213,
   GW IP = 172.17.63.213

1716   13:22:10.755  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.17.63.213

1717   13:22:10.755  04/13/02  Sev=Info/5       IKE/0x63000055
Received a key request from Driver for IP address 10.10.10.255,
   GW IP = 172.17.63.213

1718   13:22:10.755  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.17.63.213

1719   13:22:11.115  04/13/02  Sev=Info/4       IPSEC/0x63700014
Deleted all keys

1720   13:22:11.616  04/13/02  Sev=Info/5       IKE/0x63000055
Received a key request from Driver for IP address 144.254.6.77,
   GW IP = 172.17.63.213

1721   13:22:11.616  04/13/02  Sev=Warning/3    IKE/0xE3000002
Function initialize_qm failed with an error code
   of 0x00000000(INITIATE:811)

1722   13:22:12.097  04/13/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 172.17.63.213

1723   13:22:12.097  04/13/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
   NOTIFY:STATUS_RESP_LIFETIME) from 172.17.63.213

1724   13:22:12.097  04/13/02  Sev=Info/5       IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

1725   13:22:12.097  04/13/02  Sev=Info/5       IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

1726   13:22:12.097  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 172.17.63.213

1727   13:22:12.097  04/13/02  Sev=Info/5       IKE/0x63000058
Loading IPsec SA (Message ID = 0x78639C26 OUTBOUND SPI = 0x091E92B8
   INBOUND SPI = 0x7E7A7797)

1728   13:22:12.097  04/13/02  Sev=Info/5       IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x091E92B8

1729   13:22:12.097  04/13/02  Sev=Info/5       IKE/0x63000026
Loaded INBOUND ESP SPI: 0x7E7A7797

1730   13:22:12.097  04/13/02  Sev=Info/4       CM/0x6310001A
One secure connection established

1731   13:22:12.117  04/13/02  Sev=Info/6       DIALER/0x63300003
Connection established.

1732   13:22:12.477  04/13/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 172.17.63.213

1733   13:22:12.477  04/13/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
   NOTIFY:STATUS_RESP_LIFETIME) from 172.17.63.213

1734   13:22:12.477  04/13/02  Sev=Info/5       IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

1735   13:22:12.477  04/13/02  Sev=Info/5       IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

1736   13:22:12.477  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 172.17.63.213

1737   13:22:12.477  04/13/02  Sev=Info/5       IKE/0x63000058
Loading IPsec SA (Message ID = 0xD5A0CB3C OUTBOUND SPI = 0xBEE54877
   INBOUND SPI = 0x2DFC7E29)

1738   13:22:12.477  04/13/02  Sev=Info/5       IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xBEE54877

1739   13:22:12.477  04/13/02  Sev=Info/5       IKE/0x63000026
Loaded INBOUND ESP SPI: 0x2DFC7E29

1740   13:22:12.477  04/13/02  Sev=Info/4       CM/0x63100022
Additional Phase 2 SA established.

1741   13:22:12.477  04/13/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

1742   13:22:12.477  04/13/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

1743   13:22:12.477  04/13/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0xb8921e09 into key list

1744   13:22:12.477  04/13/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

1745   13:22:12.477  04/13/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x97777a7e into key list

1746   13:22:12.477  04/13/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x7748e5be into key list

1747   13:22:12.477  04/13/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

1748   13:22:12.477  04/13/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x297efc2d into key list

1749   13:22:21.229  04/13/02  Sev=Info/6       IKE/0x6300003D
Sending DPD request to 172.17.63.213, seq# = 1723178673

1750   13:22:21.229  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to 172.17.63.213

1751   13:22:21.259  04/13/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 172.17.63.213

1752   13:22:21.259  04/13/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK) from 172.17.63.213

1753   13:22:21.259  04/13/02  Sev=Info/5       IKE/0x6300003F
Received DPD ACK from 172.17.63.213, seq# received = 1723178673,
   seq# expected = 1723178673
```

```
1754   13:22:31.744  04/13/02  Sev=Info/4       IPSEC/0x63700019
Activate outbound key with SPI=0x7748e5be for inbound key
   with SPI=0x297efc2d

1755   13:22:46.765  04/13/02  Sev=Info/6       IKE/0x6300003D
Sending DPD request to 172.17.63.213, seq# = 1723178674

1756   13:22:46.765  04/13/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to 172.17.63.213

1757   13:22:46.765  04/13/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 172.17.63.213
```

Zugehörige Informationen

- Produkt-Support für die Cisco PIX Firewall
- Cisco Secure PIX Firewall - Befehlsreferenzen
- IPSec-Support-Seite
- Einführung in IPSec
- Konfigurieren von IPSec
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems