Konfigurieren des Routers zum VPN-Client, Modus-Konfig., Freigegebener Schlüssel (Wild Card Pre-Shared Key) mit NAT

Inhalt

Einführung

Diese Beispielkonfiguration zeigt einen Router, der für die Konfiguration des Modus konfiguriert wurde (Benutzer erhält eine IP-Adresse aus dem Pool), vorinstallierte Platzhalterschlüssel (alle PC-Clients teilen einen gemeinsamen Schlüssel) und Network Address Translation (NAT). Bei dieser Konfiguration kann ein externer Benutzer in das Netzwerk eintreten und eine interne IP-Adresse aus dem Pool erhalten. Benutzer scheinen sich im Netzwerk zu befinden. Da es sich um eine private Adressierung (also NAT) handelt, muss dem Router mitgeteilt werden, was übersetzt werden soll und was nicht.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- Cisco IOS® Softwareversion 12.0.7T oder höher
- Hardware, die diese Softwareversion unterstützt
- Cisco Secure VPN Client 1.0/10A oder 1.1 (als 2.0.7/E bzw. 2.1.12 angezeigt): Gehen Sie zu **Hilfe** > **Info**, um zu überprüfen.

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 .

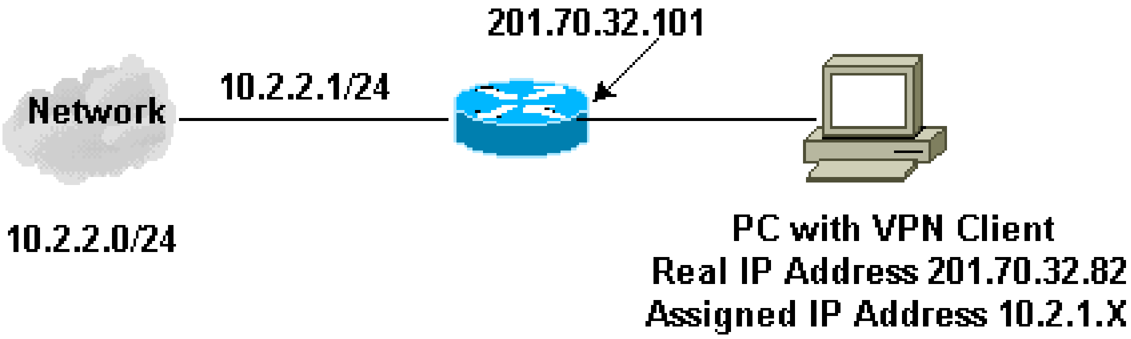
Konfigurieren

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 in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- VPN-Client
- Router

VPN-Client-Konfiguration

```
Network Security policy:

1- Myconn
        My Identity = ip address
```

```
                Connection security: Secure
                Remote Party Identity and addressing
                        ID Type: IP subnet
                        10.2.2.0
                        Port all Protocol all

                Connect using secure tunnel
                        ID Type: IP address
                        201.70.32.101

        Authentication (Phase 1)
        Proposal 1
                Authentication method: pre-shared key
                Encryp Alg: DES
                Hash Alg: MD5
                SA life: Unspecified
                Key Group: DH 1

        Key exchange (Phase 2)
        Proposal 1
                Encapsulation ESP
                Encrypt Alg: DES
                Hash Alg: MD5
                Encap: tunnel
                SA life: Unspecified
                no AH

2- Other Connections
            Connection security: Non-secure
            Local Network Interface
                Name: Any
                IP Addr: Any
                Port: All
```

Routerkonfiguration

```

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable secret 5 $1$v5OP$mPuiEQn8ULa8hVMYVOV1D.
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- IKE configuration.  crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
!--- IPSec configuration. crypto ipsec transform-set
trans1 esp-des esp-md5-hmac
!
crypto dynamic-map dynmap 10
```

```
set transform-set trans1
!
crypto map intmap client configuration address initiate
crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
 !
 interface Ethernet0
ip address 201.70.32.101 255.255.255.0
 no ip directed-broadcast
ip nat outside
no ip route-cache
no ip mroute-cache
 crypto map intmap
 !
interface Serial1
ip address 10.2.2.1 255.255.255.0
no ip directed-broadcast
ip nat inside
!
 ip local pool ourpool 10.2.1.1 10.2.1.254
ip nat pool outsidepool 201.70.32.150 201.70.32.160
netmask 255.255.255.0
!--- Except the private network to private network
traffic !--- from the NAT process. ip nat inside source
route-map nonat pool outsidepool
 ip classless
ip route 0.0.0.0 0.0.0.0 201.70.32.1
no ip http server
!--- Except the private network to private network
traffic !--- from the NAT process. access-list 101 deny
ip 10.2.2.0 0.0.0.255 10.2.1.0 0.0.0.255 access-list 101
permit ip 10.2.2.0 0.0.0.255 any route-map nonat permit
10 match ip address 101 ! line con 0 transport input
none line aux 0 line vty 0 4 password ww login ! end
```

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.

- **show crypto engine connections active** - Zeigt die verschlüsselten und entschlüsselten Pakete an.
- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** - Zeigt die Sicherheitszuordnungen für Phase 1 an.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

Diese Debug-Prozesse müssen auf beiden IPSec-Routern (Peers) ausgeführt werden. Das Löschen von Sicherheitszuordnungen muss auf beiden Peers erfolgen.

- **debug crypto ipsec**: Zeigt die IPSec-Verhandlungen für Phase 2 an.
- **debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen für Phase 1 an.
- **debug crypto engine**: Zeigt den verschlüsselten Datenverkehr an.
- **clear crypto isakmp**: Löscht die Sicherheitszuordnungen für Phase 1.
- **clear crypto sa**: Löscht die Sicherheitszuordnungen für Phase 2.

Beispielausgabe für Debugging

Router-Debugger

```
Apr 18 15:17:59: ISAKMP (4): received packet from
    201.70.32.82 (R) MM_NO_STATE
Apr 18 15:17:59: ISAKMP (4): received packet from
    201.70.32.82 (R) MM_NO_STATE
Apr 18 15:18:03: ISAKMP (0): received packet from
    201.70.32.82 (N) NEW SA
Apr 18 15:18:03: ISAKMP (0:5): processing SA payload.
    message ID = 0
Apr 18 15:18:03: ISAKMP (0:5): Checking ISAKMP transform
1
    against priority 1 policy
Apr 18 15:18:03: ISAKMP:      encryption DES-CBC
Apr 18 15:18:03: ISAKMP:      hash MD5
Apr 18 15:18:03: ISAKMP:      default group 1
Apr 18 15:18:03: ISAKMP:      auth pre-share
Apr 18 15:18:03: ISAKMP (0:5): atts are acceptable.
    Next payload is 0
Apr 18 15:18:03: CryptoEngine0: generate alg parameter
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-shared
    key authentication
Apr 18 15:18:05: ISAKMP (5): SA is doing pre-shared
    key authentication using id type ID_IPV4_ADDR
Apr 18 15:18:05: ISAKMP (5): sending packet to
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (5): received packet from
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (0:5): processing KE payload.
    message ID = 0
Apr 18 15:18:05: CryptoEngine0: generate alg parameter
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-shared
    key authentication
Apr 18 15:18:05: ISAKMP (5): SA is doing pre-shared
    key authentication using id
type ID_IPV4_ADDR
Apr 18 15:18:05: ISAKMP (5): sending packet to
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (5): received packet from
    201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (0:5): processing KE payload.
    message ID = 0
Apr 18 15:18:05: CryptoEngine0: generate alg parameter
Apr 18 15:18:07: ISAKMP (0:5): processing NONCE payload.
```

```
    message ID = 0
Apr 18 15:18:07: CryptoEngine0: create ISAKMP SKEYID for
    conn id 5
Apr 18 15:18:07: ISAKMP (0:5): SKEYID state generated
Apr 18 15:18:07: ISAKMP (0:5): processing vendor id
payload
Apr 18 15:18:07: ISAKMP (0:5): processing vendor id
payload
Apr 18 15:18:07: ISAKMP (5): sending packet to
201.70.32.82
    (R) MM_KEY_EXCH
Apr 18 15:18:07: ISAKMP (0:4): purging SA.
Apr 18 15:18:07: ISAKMP (0:4): purging node -1412157317
Apr 18 15:18:07: ISAKMP (0:4): purging node 1875403554
Apr 18 15:18:07: CryptoEngine0: delete connection 4
Apr 18 15:18:08: ISAKMP (5): received packet from
    201.70.32.82 (R) MM_KEY_EXCH
Apr 18 15:18:08: ISAKMP (0:5): processing ID payload.
    message ID = 0
Apr 18 15:18:08: ISAKMP (0:5): processing HASH payload.
    message ID = 0
Apr 18 15:18:08: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:08: ISAKMP (5): processing NOTIFY payload
    24578 protocol 1 spi 0, message ID = 0
Apr 18 15:18:08: ISAKMP (0:5): SA has been authenticated
    with 201.70.32.82
Apr 18 15:18:08: ISAKMP (5): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
Apr 18 15:18:08: ISAKMP (5): Total payload length: 12
Apr 18 15:18:08: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:08: CryptoEngine0: clear dh number
    for conn id 1
Apr 18 15:18:08: ISAKMP (5): sending packet to
    201.70.32.82 (R) QM_IDLE
Apr 18 15:18:08: ISAKMP (5): received packet from
    201.70.32.82 (R) QM_IDLE
Apr 18 15:18:08: ISAKMP (0:5): Locking struct 14D0DC
    on allocation
Apr 18 15:18:08: ISAKMP (0:5): allocating address
    10.2.1.1
Apr 18 15:18:08: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:08: ISAKMP (0:5): initiating peer config to
    201.70.32.82. message ID = 1226793520
Apr 18 15:18:08: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (0:5): processing transaction
payload
    from 201.70.32.82. message ID = 1226793520
Apr 18 15:18:09: ISAKMP: recieved config from
201.70.32.82   .
Apr 18 15:18:09: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:09: ISAKMP:     Config payload type: 4
Apr 18 15:18:09: ISAKMP (0:5): peer accepted the
address!
Apr 18 15:18:09: ISAKMP (0:5): adding static route for
10.2.1.1
Apr 18 15:18:09: ISAKMP (0:5): deleting node 1226793520
Apr 18 15:18:09: CryptoEngine0: generate hmac context
for
    conn id 5
Apr 18 15:18:09: ISAKMP (0:5): processing SA payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (0:5): Checking IPSec proposal 1
Apr 18 15:18:09: ISAKMP: transform 1, ESP_DES
Apr 18 15:18:09: ISAKMP:   attributes in transform:
Apr 18 15:18:09: ISAKMP:      authenticator is HMAC-MD5
Apr 18 15:18:09: ISAKMP:      encaps is 1
Apr 18 15:18:09: validate proposal 0
Apr 18 15:18:09: ISAKMP (0:5): atts are acceptable.
Apr 18 15:18:09: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.) dest=
201.70.32.101,
    src= 201.70.32.82, dest_proxy=
10.2.2.0/255.255.255.0/0/0
    (type=4), src_proxy= 10.2.1.1/255.255.255.255/0/0
(type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 0,
    flags= 0x4
Apr 18 15:18:09: validate proposal request 0
Apr 18 15:18:09: ISAKMP (0:5): processing NONCE payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (0:5): processing ID payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1
    prot 0 port 0
Apr 18 15:18:09: ISAKMP (0:5): processing ID payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (5): ID_IPV4_ADDR_SUBNET dst
    10.2.2.0/255.255.255.0 prot 0 port 0
Apr 18 15:18:09: IPSEC(key_engine): got a queue event...
Apr 18 15:18:09: IPSEC(spi_response): getting spi
    153684796 for SA from 201.70.32.82    to
201.70.32.101
    for prot 3
Apr 18 15:18:09: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:09: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:09: ISAKMP (0:5): processing SA payload.
    message ID = -1078114754
Apr 18 15:18:09: ISAKMP (0:5): Checking IPSec proposal 1
Apr 18 15:18:10: ISAKMP: transform 1, ESP_DES
Apr 18 15:18:10: ISAKMP:   attributes in transform:
Apr 18 15:18:10: ISAKMP:      authenticator is HMAC-MD5
Apr 18 15:18:10: ISAKMP:      encaps is 1
Apr 18 15:18:10: validate proposal 0
Apr 18 15:18:10: ISAKMP (0:5): atts are acceptable.
Apr 18 15:18:10: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.) dest=
201.70.32.101,
    src= 201.70.32.82, dest_proxy=
10.2.2.0/255.255.255.0/0/0
    (type=4), src_proxy= 10.2.1.1/255.255.255.255/0/0
(type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 0,
    flags= 0x4
Apr 18 15:18:10: validate proposal request 0
Apr 18 15:18:10: ISAKMP (0:5): processing NONCE payload.
    message ID = -1078114754
Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
    message ID = -1078114754
Apr 18 15:18:10: ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1
    prot 0 port 0
Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
    message ID = -1078114754
Apr 18 15:18:10: ISAKMP (5): ID_IPV4_ADDR_SUBNET dst
    10.2.2.0/255.255.255.0 prot 0 port 0
Apr 18 15:18:10: IPSEC(key_engine): got a queue event...
Apr 18 15:18:10: IPSEC(spi_response): getting spi
224008976
    for SA from 201.70.32.82    to 201.70.32.101
    for prot 3
Apr 18 15:18:10: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:10: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:10: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:10: CryptoEngine0: generate hmac context
    for conn id 5
Apr 18 15:18:10: ipsec allocate flow 0
Apr 18 15:18:10: ipsec allocate flow 0
Apr 18 15:18:10: ISAKMP (0:5): Creating IPSec SAs
Apr 18 15:18:10:         inbound SA from 201.70.32.82
    to 201.70.32.101   (proxy 10.2.1.1        to
10.2.2.0)
Apr 18 15:18:10:         has spi 224008976 and conn_id
2000
    and flags 4
Apr 18 15:18:10:         outbound SA from 201.70.32.101
    to 201.70.32.82    (proxy 10.2.2.0        to
10.2.1.1)
Apr 18 15:18:10:         has spi -1084694986 and conn_id
2001
    and flags 4
Apr 18 15:18:10: ISAKMP (0:5): deleting node -1078114754
Apr 18 15:18:10: IPSEC(key_engine): got a queue event...
Apr 18 15:18:10: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 201.70.32.101, src=
201.70.32.82,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.1.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xD5A1B10(224008976), conn_id= 2000, keysize=
0,
    flags= 0x4
Apr 18 15:18:10: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 201.70.32.101, dest=
201.70.32.82,
    src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.1.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xBF58DE36(3210272310), conn_id= 2001, keysize=
0,
    flags= 0x4
Apr 18 15:18:10: IPSEC(create_sa): sa created,
  (sa) sa_dest= 201.70.32.101, sa_prot= 50,
    sa_spi= 0xD5A1B10(224008976),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
Apr 18 15:18:10: IPSEC(create_sa): sa created,
  (sa) sa_dest= 201.70.32.82, sa_prot= 50,
    sa_spi= 0xBF58DE36(3210272310),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
Apr 18 15:18:10: ISAKMP: Locking struct 14D0DC for IPSEC
Apr 18 15:18:24: ISAKMP (0:5): retransmitting
    phase 2 -617682048 ...
Apr 18 15:18:24: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE

Router#show crypto ipsec
Apr 18 15:18:39: ISAKMP (0:5): retransmitting
    phase 2 -617682048 ...
Apr 18 15:18:39: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE      sa

interface: Ethernet0
    Crypto map tag: intmap, local addr. 201.70.32.101

   local  ident (addr/mask/prot/port):
   (10.2.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
   (10.2.1.1/255.255.255.255/0/0)
   current_peer: 201.70.32.82
     PERMIT, flags={}
    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
    #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.: 201.70.32.101, remote
     crypto endpt.: 201.70.32.82
     path mtu 1500, media mtu 1500
     current outbound spi: BF58DE36

     inbound esp sas:
      spi: 0xD5A1B10(224008976)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1,
        crypto map: intmap
        sa timing: remaining key lifetime
       (k/sec): (4607999/3500)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:
      spi: 0xBF58DE36(3210272310)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2,
     crypto map: intmap
        sa timing: remaining key lifetime
        (k/sec): (4607999/3500)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:

     outbound pcp sas:

Router#sho crypto engine connections active

  ID Interface       IP-Address      State  Algorithm
Encrypt  Decrypt
   5                     set    HMAC_MD5+DES_56_CB
0        0
2000 Ethernet0       201.70.32.101   set
HMAC_MD5+DES_56_CB  0        7
2001 Ethernet0       201.70.32.101   set
HMAC_MD5+DES_56_CB  7        0
Crypto adjacency count : Lock: 0, Unlock: 0
```

VPN-Clientinformationen

```
Client configuration:
C:\>ping -t 10.2.2.5
Reply from 10.2.2.5: bytes=32 time<0ms TTL=352

Reply from 10.2.2.5: bytes=32 time<10ms TTL=352

From Logview:
14:25:34.044 New Connection - Initiating IKE
    Phase 1 (IP ADDR=201.70.32.101)

14:25:34.144 New Connection - SENDING>>>> ISAKMP
    OAK MM (SA)
14:25:35.886 New Connection - RECEIVED<<< ISAKMP
    OAK MM (SA)
14:25:36.067 New Connection - SENDING>>>> ISAKMP
    OAK MM (KE, NON, VID, VID)
14:25:38.310 New Connection - RECEIVED<<< ISAKMP
    OAK MM (KE, NON, VID)
14:25:38.460 New Connection - SENDING>>>> ISAKMP
    OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT)
14:25:38.610 New Connection - RECEIVED<<< ISAKMP
    OAK MM *(ID, HASH)
14:25:38.710 New Connection - Established IKE SA
14:25:38.811 New Connection - Initiating IKE Phase
    2 with Client IDs (message id
: B01876)
14:25:38.911   Initiator = IP ADDR=201.70.32.82,
    prot = 0 port = 0

14:25:39.011   Responder = IP
SUBNET/MASK=10.2.2.0/255.255.255.0,
    prot = 0 port = 0

14:25:39.111 New Connection - SENDING>>>>
    ISAKMP OAK QM *(HASH, SA, NON, ID, ID)
14:25:39.251 New Connection - RECEIVED<<< ISAKMP
    OAK TRANS *(HASH, ATTR)
14:25:39.351 New Connection - Received Private IP
    Address = IP ADDR=10.2.1.1

14:25:39.451 New Connection - Discarding IPSec SA
    negotiation (message id: B01876)
14:25:39.552 New Connection - SENDING>>>> ISAKMP OAK
    TRANS *(HASH, ATTR)
14:25:40.022 New Connection - Received message for
discarded
    IPSec SA negotiation (message id: B01876)
14:25:40.122 New Connection - Initiating IKE Phase 2
with
    Client IDs (message id: C8CB0CE)
14:25:40.223   Initiator = IP ADDR=10.2.1.1, prot = 0
port = 0
14:25:40.323   Responder = IP
SUBNET/MASK=10.2.2.0/255.255.255.0,
    prot = 0 port = 0
14:25:40.423 New Connection - SENDING>>>> ISAKMP OAK
    QM *(HASH, SA, NON, ID, ID)
14:25:40.873 New Connection - RECEIVED<<< ISAKMP OAK
    QM *(HASH, SA, NON, ID, ID,
 NOTIFY:STATUS_RESP_LIFETIME)
14:25:40.974 New Connection - SENDING>>>> ISAKMP OAK
    QM *(HASH)
14:25:41.074 New Connection - Loading IPSec SA
    (Message ID = C8CB0CE OUTBOUND SPI = 19A22423
    INBOUND SPI = E4829433)
14:25:41.174
```

Zugehörige Informationen

- Konfigurieren der IPSec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- Einführung in IPSec
- Support-Seiten für IP Security-Produkte (IPSec)
- Technischer Support - Cisco Systems