

Het configureren van de PIX 501/506 Easy VPN-afstandsbediening naar een IOS-router in Network Extension Mode met uitgebreide verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[PIX-show Opdrachten en voorbeelduitvoer](#)

[IOS toont opdrachten en uitvoer van voorbeelden](#)

[Problemen oplossen](#)

[PIX-debug en uitvoer van monsters](#)

[IOS debug van opdrachten en uitvoer van voorbeelden](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document illustreert de configuratie van IPSec tussen de PIX Easy VPN Remote hardware client en de optie Easy VPN Server beschikbaar in latere releases van Cisco IOS®-software. De Easy VPN Remote optie voor PIX is geïntroduceerd in PIX versie 6.2 en wordt ook aangeduid als hardware client/EzVPN-client. Wanneer de Easy VPN-afstandsbediening op een head-end apparaat aansluit, zijn er minimaal vijf beveiligingsassociaties (SA's), waaronder één Internet Key Exchange (IKE) en vier IPSec-associaties. Wanneer de Easy VPN-afstandsbediening op het head-end aangesloten is, begeeft deze altijd twee IPSec SA's met het IP-adres van de PIX-externe interface naar elk adres achter de VPN-server. Dit kan voor beheerdoeleinden gebruikt worden om verbinding te maken met de externe interface van de PIX vanaf het netwerk achter de Cisco IOS-router (via Secure Shell [SSH], Secure HTTP voor PIX-apparaatbeheer [PDM] of telnet). Het SA wordt gecreëerd door standaard zonder om het even welke configuratie, en de andere twee SAs worden gemaakt voor het gegevensverkeer tussen de netwerken achter de PIX en de Cisco IOS router.

Raadpleeg [PIX-to-PIX 6.x: Easy VPN \(NEM\) Configuration Voorbeeld](#) voor meer informatie over een vergelijkbaar scenario waarin PIX 506 6.x werkt als de Easy VPN-server.

Raadpleeg [PIX/ASA 7.x Easy VPN met een ASA 5500 als de server en PIX 506E als het voorbeeld voor de configuratie van de client \(NEM\)](#) voor meer informatie over een vergelijkbaar scenario waarin PIX/ASA 7.x als de Easy VPN-server werkt.

Raadpleeg [PIX/ASA 7.x Easy VPN met een ASA 5500 als de server en Cisco 871 als het Easy VPN Remote Configuration-voorbeeld](#) voor meer informatie over een vergelijkbaar scenario waarin Cisco 871 router werkt als de Easy VPN-afstandsbediening.

Raadpleeg [VPN-hardwareclient voor een PIX 501/506 Series security applicatie met VPN 3000 Concentrator Configuratie Voorbeeld](#) voor meer informatie over een vergelijkbaar scenario waarin Cisco VPN 3000 Concentrator fungeert als de Easy VPN-server.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX-firewall voor softwareversie 6.3(5)**Opmerking:** De optie Easy VPN Client op de PIX is geïntroduceerd in versie 6.2.
- Cisco 7200 Series IOS-router met softwareversie 12.4(4)T1**Opmerking:** De functie Makkelijk VPN Server is geïntroduceerd in versie 12.2(8)T.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Gebruik het [Opdrachtupgereedschap](#) (alleen geregistreeerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:


```
!  
interface ATM2/0  
  no ip address  
  shutdown  
  no atm ilmi-keepalive  
!  
interface FastEthernet4/0  
  no ip address  
  shutdown  
  duplex half  
!  
interface Ethernet5/0  
  ip address 172.22.1.1 255.255.255.0  
  duplex half  
!  
interface Ethernet5/1  
  no ip address  
  shutdown  
  duplex half  
!  
interface Ethernet5/2  
  no ip address  
  shutdown  
  duplex half  
!  
interface Ethernet5/3  
  no ip address  
  shutdown  
  duplex half  
!  
!--- Create a pool of addresses to be assigned to the  
VPN Clients. ip local pool ippool 172.22.1.50  
172.22.1.70  
ip classless  
no ip http server  
no ip http secure-server  
!  
!  
!  
logging alarm informational  
!  
!  
!  
control-plane  
!  
!  
!  
!  
!  
gatekeeper  
  shutdown  
!  
!  
line con 0  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4  
!  
!  
end
```

```
ezvpn_server#
```

PIX

```
pix506#show running-config
: Saved
:
PIX Version 6.3(5)

!--- Specify speed and duplex settings. interface
ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password WwXYvtKrnjXqGbul encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix506
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
mtu outside 1500
mtu inside 1500

!--- Define IP addresses for the PIX's inside and
outside interfaces. 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

!--- Define the outside router as the default gateway.
!--- Typically this is the IP address of your ISP's
router. 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

!--- Define the VPN peer IP address. vpnclient server
10.10.10.2

!--- Specify whether Client/PAT (Port Address
Translation) mode !--- is to be used or whether Network
Extension Mode (NEM) is to be used. vpnclient mode
network-extension-mode

!--- Define Easy VPN Remote parameters. !--- This is the
pre-shared key used in IKE negotiation. vpnclient
vpngroup hwclient password *****

!--- This is the extended authentication username and
password. vpnclient username cisco password *****

!---This enables vpnclient on the PIX. vpnclient enable
terminal width 80
Cryptochecksum:fdbd365f0b4cdc6707a50efeeeb8ed44
: end

```

Verifiëren

PIX-show Opdrachten en voorbeelduitvoer

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het [Uitvoer Tolk](#) (uitsluitend [geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **VPN-client maakt opdracht** mogelijk - maakt een eenvoudige VPN-afstandsverbinding mogelijk. In NEM, is de tunnel zelfs op wanneer er geen interessant verkeer is om te ruilen met de head-end Easy VPN Server.

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

- **toon crypto isakmp beleid**-Toont de parameters voor elk IKE beleid.

```
pix506(config)#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

```

Dit voorbeeld toont output van de **show crypto isakmp beleidsopdracht** nadat de hardwareclient is ingeschakeld.

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

```

Protection suite of priority 65001
  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 65002
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

```

- **toon crypto ipsec transformatie**-displays de huidige IPSec transformaties.

```
pix506(config)#show crypto ipsec transform
```

Dit voorbeeld toont uitvoer van het **bevel tot transformatie** van de **show crypto ipsec** nadat de hardwareclient is geactiveerd. Voordat de **client**-opdracht wordt gebruikt, was er slechts één standaardopdracht voor ISAKMP. Nadat de opdracht is gegeven, bouwt Easy VPN automatisch vier voorstellen naast de standaardbeschermingsreeks. Daarnaast is er geen IPSec transformatie set voordat **Enable** wordt gebruikt. De transformatieset wordt dynamisch gebouwd nadat de opdracht is afgegeven.

```
pix506(config)#show crypto ipsec transform-set
```

```
Transform set _vpnc_tset_9: { esp-des esp-md5-hmac }
will negotiate = { Tunnel, },
```

```
Transform set _vpnc_tset_10: { esp-null esp-md5-hmac }
will negotiate = { Tunnel, },
```

```
Transform set _vpnc_tset_11: { esp-null esp-sha-hmac }
will negotiate = { Tunnel, },
```

- **toon crypto isakmp sa**-Toont alle huidige IKE SAs bij een peer.

```
pix506(config)#show crypto isakmp sa
```

```
Total      : 1
Embryonic  : 0
```

dst	src	state	pending	created
10.10.10.2	10.10.10.1	QM_IDLE	0	2

- **Laat VPN-client**-displays VPN-client of Makkelijk VPN-configuratieinformatie zien.

```
pix506(config)#show vpnclient
```

```
LOCAL CONFIGURATION
vpnclient server 10.10.10.2
vpnclient mode network-extension-mode
vpnclient vpngroup hwclient password *****
vpnclient username cisco password *****
vpnclient enable
```

```
DOWNLOADED DYNAMIC POLICY
Current Server           : 10.10.10.2
Primary DNS              : 172.22.1.101
Primary WINS             : 172.22.1.102
Default Domain          : cisco.com
PFS Enabled              : No
Secure Unit Authentication Enabled : No
User Authentication Enabled : No
Backup Servers           : Deleted by order of the headend
```

- **toon crypto ipsec sa**-displays IPSec SA's die tussen peers zijn gebouwd.

```
pix506(config)#show crypto ipsec sa
```

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

local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
```



```

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 10.10.10.2:500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0
  #send errors 0, #recv errors 0
!--- As shown here, ping packets were successfully exchanged !--- between the Easy VPN
Remote (PIX) and the Easy VPN Server (IOS). local crypto endpt.: 10.10.10.1, remote crypto
endpt.: 10.10.10.2 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi:
533f74a9 inbound esp sas: spi: 0xad0984cc(2903082188) 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): (4607999/3001) IV size: 8 bytes replay detection support: Y inbound ah
sas: inbound pcp sas: outbound esp sas: spi: 0x533f74a9(1396667561) 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): (4607999/3001) IV size: 8 bytes replay detection support: Y
outbound ah sas: outbound pcp sas: local ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 10.10.10.2:500 PERMIT, flags={origin_is_acl,} #pkts encaps: 5, #pkts encrypt:
5, #pkts digest 5 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5 #pkts compressed: 0,
#pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
failed: 0 #send errors 0, #recv errors 0 !--- As shown here, ping packets were successfully
exchanged !--- between hosts behind the Easy VPN Remote (PIX) and the Easy !--- VPN Server
(IOS). local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2 path mtu 1500,
ipsec overhead 56, media mtu 1500 current outbound spi: 2eca448b inbound esp sas: spi:
0xc82c0695(3358328469) transform: esp-des esp-md5-hmac , in use settings = {Tunnel, } slot:
0, conn id: 2, crypto map: _vpnc_cm sa timing: remaining key lifetime (k/sec):
(4607999/2997) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas:
outbound esp sas: spi: 0x2eca448b(785007755) transform: esp-des esp-md5-hmac , in use
settings = {Tunnel, } slot: 0, conn id: 1, crypto map: _vpnc_cm sa timing: remaining key
lifetime (k/sec): (4607999/2988) IV size: 8 bytes replay detection support: Y outbound ah
sas: outbound pcp sas:

```

- **Toon toegang-lijst-Toont de inhoud van toegangslijsten.**

```

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 1024)
  alert-interval 300
access-list _vpnc_acl; 2 elements
access-list _vpnc_acl line 1 permit ip 172.16.1.0 255.255.255.0
  any (hitcnt=18)
access-list _vpnc_acl line 2 permit ip host 10.10.10.1
  any (hitcnt=6)

```

!--- The above output shows the dynamically built access lists to identify !--- interesting traffic for encryption.

[IOS toont opdrachten en uitvoer van voorbeelden](#)

- **toon crypto isakmp sa-Toont alle huidige IKE SAs bij een peer.**

```

ezvpn_server#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.10.10.2   10.10.10.1   QM_IDLE       1026     0 ACTIVE

```

- **toon crypto ipsec sa-displays IPsec SA's die tussen peers zijn gebouwd.**

```

ezvpn_server#show crypto ipsec sa

```

!--- As shown above, ping packets were successfully exchanged !--- between the Easy VPN Remote (PIX) and the Easy VPN Server (IOS) !--- as well as hosts behind them. interface: FastEthernet0/0 Crypto map tag: clientmap, local addr 10.10.10.2 protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0) current_peer 10.10.10.1 port 500 PERMIT, flags={ } #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3 #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr.

```
failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors
0 local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1 path mtu 1500, ip mtu
1500 current outbound spi: 0xAD0984CC(2903082188) inbound esp sas: spi:
0x533F74A9(1396667561) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn
id: 21, flow_id: SW:21, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4470133/2836) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas:
inbound pcp sas: outbound esp sas: spi: 0xAD0984CC(2903082188) transform: esp-des esp-md5-
hmac , in use settings ={Tunnel, } conn id: 22, flow_id: SW:22, crypto map: clientmap sa
timing: remaining key lifetime (k/sec): (4470133/2834) IV size: 8 bytes replay detection
support: Y Status: ACTIVE outbound ah sas: outbound pcp sas: protected vrf: (none) local
ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0) current_peer 10.10.10.1 port 500 PERMIT, flags={ } #pkts
encaps: 5, #pkts encrypt: 5, #pkts digest: 5 #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr.
failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors
0 local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1 path mtu 1500, ip mtu
1500 current outbound spi: 0xC82C0695(3358328469) inbound esp sas: spi:
0x2ECA448B(785007755) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } conn id:
23, flow_id: SW:23, crypto map: clientmap sa timing: remaining key lifetime (k/sec):
(4589382/2832) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas:
inbound pcp sas: outbound esp sas: spi: 0xC82C0695(3358328469) transform: esp-des esp-md5-
hmac , in use settings ={Tunnel, } conn id: 24, flow_id: SW:24, crypto map: clientmap sa
timing: remaining key lifetime (k/sec): (4589382/2830) IV size: 8 bytes replay detection
support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:
```

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Als u de Easy VPN Remote (PIX) en Easy VPN Server (IOS) hebt ingesteld zoals in dit document wordt beschreven en nog steeds problemen ondervindt, verzamel dan de debug-uitvoer van de PIX en de IOS-uitvoer en de **show**-opdracht voor analyse door het Cisco Technical Assistance Center (TAC). Zie ook [Problemen oplossen de PIX om gegevensverkeer door te geven op een bestaande IPSec Tunnel](#) of [IP Security Problemen oplossen - Het begrijpen en gebruiken van debug Opdrachten](#). Schakel IPSec-debugging in op de PIX.

PIX-debug en uitvoer van monsters

PIX-debug opdrachten

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u debug-opdrachten gebruikt.

- **debug crypto ipsec-displays** de IPSec-onderhandelingen van fase 2.
- **debug crypto isakmp** — Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

PIX-voorbeelduitvoer

```
ISAKMP (0): ID payload
next-payload : 13
type         : 11
protocol     : 17
port         : 0
length       : 12pix506(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:10.10.10.2, dest:10.10.10.1 spt:500 dpt:500
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

!--- The PIX checks the received proposal against !--- its dynamically generated policies looking for a match. ISAKMP (0): Checking ISAKMP transform 1 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 1 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 1 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 1 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 1 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 1 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 1 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 1 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 1 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 vendor id payload ISAKMP (0): processing vendor id payload ISAKMP (0): remote peer supports dead peer detection ISAKMP (0): processing vendor id payload
crypto_isakmp_process_block:src:10.10.10.2, dest:10.10.10.1 spt:500 dpt:500
crypto_isakmp_process_block:src:10.10.10.2, dest:10.10.10.1 spt:500 dpt:500 ISAKMP : attributes being requested crypto_isakmp_process_block:src:10.10.10.2, dest:10.10.10.1 spt:500 dpt:500
ISAKMP (0): beginning Quick Mode exchange, M-ID of -582033986:dd4eddbbeIPSEC (key_engine): got a queue event... IPSEC(spi_response): getting spi 0x61cf8d08(1640992008) for SA from 10.10.10.2 to 10.10.10.1 for prot 3 crypto_isakmp_process_block:src:10.10.10.2, 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 = 3712933310 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= 10.10.10.2, src= 10.10.10.1, dest_proxy= 0.0.0.0/0.0.0.0/0/0 (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 = 3712933310 ISAKMP (0): processing ID payload. message ID = 3712933310 ISAKMP (0): processing ID payload. message ID = 3712933310 ISAKMP (0): processing NOTIFY payload 24576 protocol 3 spi 1327036890, message ID = 3712933310 ISAKMP (0): processing responder lifetime ISAKMP (0): responder lifetime of 3600s ISAKMP (0): Creating IPsec SAs inbound SA from 10.10.10.2 to 10.10.10.1 (proxy 0.0.0.0 to 10.10.10.1) has spi 1640992008 and conn_id 1 and flags 4 lifetime of 3600 seconds lifetime of 4608000 kilobytes outbound SA from 10.10.10.1 to 10.10.10.2 (proxy 10.10.10.1 to 0.0.0.0) has spi 1327036890 and conn_id 2 and flags 4 lifetime of 3600 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 10.10.10.1, src= 10.10.10.2, dest_proxy=

```
10.10.10.1/255.255.255.255/0/0 (type=1), src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP,
transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi= 0x61cf8d08(1640992008),
conn_id= 1, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 10.10.10.1,
dest= 10.10.10.2, src_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), dest_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s
and 4608000kb, spi= 0x4f18f9da(1327036890), conn_id= 2, keysize= 0, flags= 0x4 !--- The IPsec
SAs shown above are for management purposes. VPN Peer: IPSEC: Peer ip:10.10.10.2/500 Ref cnt
incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:10.10.10.2/500 Ref cnt incremented
to:3 Total VPN Peers:1 return status is IKMP_NO_ERROR ISAKMP (0): beginning Quick Mode exchange,
M-ID of -419501328:e6feeaf0IPSEC (key_engine): got a queue event... IPSEC(spi_response): getting
spi 0xf3d52246(4090831430) for SA from 10.10.10.2 to 10.10.10.1 for prot 3
crypto_isakmp_process_block:src:10.10.10.2, 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 =
3875465968 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= 10.10.10.2,
src= 10.10.10.1, dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), src_proxy=
172.16.1.0/255.255.255.0/0/0 (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 = 3875465968 ISAKMP (0): processing ID payload. message ID = 3875465968
ISAKMP (0): processing ID payload. message ID = 3875465968 ISAKMP (0): processing NOTIFY payload
24576 protocol 3 spi 465396864, message ID = 3875465968 ISAKMP (0): processing responder
lifetime ISAKMP (0): responder lifetime of 3600s ISAKMP (0): Creating IPsec SAs inbound SA from
10.10.10.2 to 10.10.10.1 (proxy 0.0.0.0 to 172.16.1.0) has spi 4090831430 and conn_id 3 and
flags 4 lifetime of 3600 seconds lifetime of 4608000 kilobytes outbound SA from 10.10.10.1 to
10.10.10.2 (proxy 172.16.1.0 to 0.0.0.0) has spi 465396864 and conn_id 4 and flags 4 lifetime of
3600 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): , (key eng. msg.) dest= 10.10.10.1, src= 10.10.10.2, dest_proxy=
172.16.1.0/255.255.255.0/0/0 (type=4), src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP,
transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi= 0xf3d52246(4090831430),
conn_id= 3, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 10.10.10.1,
dest= 10.10.10.2, src_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), dest_proxy=
0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s
and 4608000kb, spi= 0x1bbd6480(465396864), conn_id= 4, keysize= 0, flags= 0x4 !--- The IPsec SAs
shown above are for actual data traffic. VPN Peer: IPSEC: Peer ip:10.10.10.2/500 Ref cnt
incremented to:4 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:10.10.10.2/500 Ref cnt incremented
to:5 Total VPN Peers:1
```

[IOS debug van opdrachten en uitvoer van voorbeelden](#)

IOS-debug van opdrachten

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u debug-opdrachten gebruikt.

- debug van crypto ipsec-displays gedetailleerde IPsec-gebeurtenissen.
- debug van crypto isakmp-displays over IKE gebeurtenissen.
- debug van crypto motor-displays het verkeer dat versleuteld wordt.

IOS-voorbeelduitvoer

```
!--- As soon as the vpnclient enable command is issued on the PIX, !--- the IOS device receives
an IKE negotiation request.
```

```
*Jan 20 16:48:22.267: ISAKMP (0:0): received packet from 10.10.10.1 dport
500 sport 500 Global (N) NEW
```

SA

*Jan 20 16:48:22.271: ISAKMP: Created a peer struct for 10.10.10.1,
peer port 500

*Jan 20 16:48:22.271: ISAKMP: New peer created peer = 0x6758C6D0
peer_handle = 0x80000026

*Jan 20 16:48:22.271: ISAKMP: Locking peer struct 0x6758C6D0,
refcount 1 for

crypto_isakmp_process_block

*Jan 20 16:48:22.271: ISAKMP:(0):Setting client config settings 6679B340

*Jan 20 16:48:22.271: ISAKMP:(0):(Re)Setting client xauth list and state

*Jan 20 16:48:22.271: ISAKMP/xauth: initializing AAA request

*Jan 20 16:48:22.271: ISAKMP: local port 500, remote port 500

*Jan 20 16:48:22.271: insert sa successfully sa = 658E0874

*Jan 20 16:48:22.271: ISAKMP:(0): processing SA payload. message ID = 0

*Jan 20 16:48:22.271: ISAKMP:(0): processing ID payload. message ID = 0

*Jan 20 16:48:22.271: ISAKMP (0:0): ID payload

next-payload : 13

type : 11

group id : hwclient

protocol : 17

port : 0

length : 16

*Jan 20 16:48:22.271: ISAKMP:(0):: peer matches *none* of the profiles

*Jan 20 16:48:22.271: ISAKMP:(0): processing vendor id payload

*Jan 20 16:48:22.271: ISAKMP:(0): vendor ID seems Unity/DPD but
major 215 mismatch

*Jan 20 16:48:22.271: ISAKMP:(0): vendor ID is XAUTH

*Jan 20 16:48:22.271: ISAKMP:(0): processing vendor id payload

*Jan 20 16:48:22.271: ISAKMP:(0): vendor ID is DPD

*Jan 20 16:48:22.271: ISAKMP:(0): processing vendor id payload

*Jan 20 16:48:22.271: ISAKMP:(0): claimed IOS but failed authentication

*Jan 20 16:48:22.271: ISAKMP:(0): processing vendor id payload

*Jan 20 16:48:22.271: ISAKMP:(0): vendor ID is Unity

*Jan 20 16:48:22.271: ISAKMP:(0): Authentication by xauth preshared

*Jan 20 16:48:22.271: ISAKMP:(0):Checking ISAKMP transform 1 against
priority 10 policy

*Jan 20 16:48:22.271: ISAKMP: encryption AES-CBC

*Jan 20 16:48:22.271: ISAKMP: keylength of 256

*Jan 20 16:48:22.271: ISAKMP: hash SHA

*Jan 20 16:48:22.271: ISAKMP: default group 2

*Jan 20 16:48:22.271: ISAKMP: auth XAUTHInitPreShared

*Jan 20 16:48:22.271: ISAKMP: life type in seconds

*Jan 20 16:48:22.271: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80

*Jan 20 16:48:22.271: ISAKMP:(0):Encryption algorithm offered does
not match policy!

*Jan 20 16:48:22.271: ISAKMP:(0):atts are not acceptable. Next payload is 3

*Jan 20 16:48:22.271: ISAKMP:(0):Checking ISAKMP transform 2 against
priority 10 policy

*Jan 20 16:48:22.271: ISAKMP: encryption AES-CBC

*Jan 20 16:48:22.275: ISAKMP: keylength of 256

*Jan 20 16:48:22.275: ISAKMP: hash MD5

*Jan 20 16:48:22.275: ISAKMP: default group 2

*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared

*Jan 20 16:48:22.275: ISAKMP: life type in seconds

*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80

*Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered
does not match policy!

*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3

*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 3 against
priority 10 policy

*Jan 20 16:48:22.275: ISAKMP: encryption AES-CBC

*Jan 20 16:48:22.275: ISAKMP: keylength of 192

*Jan 20 16:48:22.275: ISAKMP: hash SHA
*Jan 20 16:48:22.275: ISAKMP: default group 2
*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared
*Jan 20 16:48:22.275: ISAKMP: life type in seconds
*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered
does not match policy!
*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3
*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 4 against
priority 10 policy
*Jan 20 16:48:22.275: ISAKMP: encryption AES-CBC
*Jan 20 16:48:22.275: ISAKMP: keylength of 192
*Jan 20 16:48:22.275: ISAKMP: hash MD5
*Jan 20 16:48:22.275: ISAKMP: default group 2
*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared
*Jan 20 16:48:22.275: ISAKMP: life type in seconds
*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered
does not match policy!
*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3
*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 5 against
priority 10 policy
*Jan 20 16:48:22.275: ISAKMP: encryption AES-CBC
*Jan 20 16:48:22.275: ISAKMP: keylength of 128
*Jan 20 16:48:22.275: ISAKMP: hash SHA
*Jan 20 16:48:22.275: ISAKMP: default group 2
*Jan 20 16:48:2f 0x0 0x1 0x51 0x80
*Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered
does not match policy!
*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3
*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 6 against
priority 10 policy
*Jan 20 16:48:22.275: ISAKMP: encryption AES-CBC
*Jan 20 16:48:22.275: ISAKMP: keylength of 128
*Jan 20 16:48:22.275: ISAKMP: hash MD52.275: ISAKMP: auth XAUTHInitPreShared
*Jan 20 16:48:22.275: ISAKMP: life type in seconds
*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) o
*Jan 20 16:48:22.275: ISAKMP: default group 2
*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared
*Jan 20 16:48:22.275: ISAKMP: life type in seconds
*Jan 20 16:48:22.275: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Jan 20 16:48:22.275: ISAKMP:(0):Encryption algorithm offered
does not match policy!
*Jan 20 16:48:22.275: ISAKMP:(0):atts are not acceptable. Next payload is 3
*Jan 20 16:48:22.275: ISAKMP:(0):Checking ISAKMP transform 7 against
priority 10 policy
*Jan 20 16:48:22.275: ISAKMP: encryption 3DES-CBC
*Jan 20 16:48:22.275: ISAKMP: hash SHA
*Jan 20 16:48:22.275: ISAKMP: default group 2
*Jan 20 16:48:22.275: ISAKMP: auth XAUTHInitPreShared
*Jan 20 16:48:22.279: ISAKMP: life type in seconds
*Jan 20 16:48:22.279: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Jan 20 16:48:22.279: ISAKMP:(0):Encryption algorithm offered
does not match policy!
*Jan 20 16:48:22.279: ISAKMP:(0):atts are not acceptable. Next payload is 3
*Jan 20 16:48:22.279: ISAKMP:(0):Checking ISAKMP transform 8 against
priority 10 policy
*Jan 20 16:48:22.279: ISAKMP: encryption 3DES-CBC
*Jan 20 16:48:22.279: ISAKMP: hash MD5
*Jan 20 16:48:22.279: ISAKMP: default group 2
*Jan 20 16:48:22.279: ISAKMP: auth XAUTHInitPreShared
*Jan 20 16:48:22.279: ISAKMP: life type in seconds
*Jan 20 16:48:22.279: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
*Jan 20 16:48:22.279: ISAKMP:(0):Encryption algorithm offered

does not match policy!

*Jan 20 16:48:22.279: ISAKMP:(0):atts are not acceptable. Next payload is 3

*Jan 20 16:48:22.279: ISAKMP:(0):Checking ISAKMP transform 9 against
priority 10 policy

*Jan 20 16:48:22.279: ISAKMP: encryption DES-CBC

*Jan 20 16:48:22.279: ISAKMP: hash MD5

*Jan 20 16:48:22.279: ISAKMP: default group 2

*Jan 20 16:48:22.279: ISAKMP: auth XAUTHInitPreShared

*Jan 20 16:48:22.279: ISAKMP: life type in seconds

*Jan 20 16:48:22.279: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80

*Jan 20 16:48:22.279: ISAKMP:(0):atts are acceptable. Next payload is 3

!--- Both the IOS device and the PIX accept the policy for ISAKMP. *Jan 20 16:48:22.279:

ISAKMP:(0): processing KE payload. message ID = 0 *Jan 20 16:48:22.279: crypto_engine: Create DH

shared secret *Jan 20 16:48:22.279: crypto_engine: Modular Exponentiation *Jan 20 16:48:22.319:

ISAKMP:(0): processing NONCE payload. message ID = 0 *Jan 20 16:48:22.319: ISAKMP:(0): vendor ID

is NAT-T v3 *Jan 20 16:48:22.319: ISAKMP:(0): vendor ID is NAT-T v2 *Jan 20 16:48:22.319:

ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH *Jan 20 16:48:22.319: ISAKMP:(0):Old State =

IKE_READY New State = IKE_R_AM_AAA_AWAIT *Jan 20 16:48:22.319: crypto_engine: Create IKE SA *Jan

20 16:48:22.319: crypto engine: deleting DH phase 2 SW:38 *Jan 20 16:48:22.319: crypto_engine:

Delete DH shared secret *Jan 20 16:48:22.319: ISAKMP:(1030): constructed NAT-T vendor-03 ID *Jan

20 16:48:22.319: ISAKMP:(1030):SA is doing pre-shared key authentication plus XAUTH using id

type ID_IPV4_ADDR *Jan 20 16:48:22.323: ISAKMP (0:1030): ID payload next-payload : 10 type : 1

address : 10.10.10.2 protocol : 17 port : 0 length : 12 *Jan 20 16:48:22.323:

ISAKMP:(1030):Total payload length: 12 *Jan 20 16:48:22.323: crypto_engine: Generate IKE hash

*Jan 20 16:48:22.323: ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R)

AG_INIT_EXCH *Jan 20 16:48:22.323: ISAKMP:(1030):Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY

*Jan 20 16:48:22.323: ISAKMP:(1030):Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2 *Jan 20

16:48:22.479: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R)

AG_INIT_EXCH *Jan 20 16:48:22.479: crypto_engine: Decrypt IKE packet *Jan 20 16:48:22.479:

ISAKMP:received payload type 20 *Jan 20 16:48:22.479: ISAKMP:received payload type 20 *Jan 20

16:48:22.479: ISAKMP:(1030): processing HASH payload. message ID = 0 *Jan 20 16:48:22.479:

crypto_engine: Generate IKE hash *Jan 20 16:48:22.483: ISAKMP:(1030): processing NOTIFY

INITIAL_CONTACT protocol 1 spi 0, message ID = 0, sa = 658E0874 *Jan 20 16:48:22.483:

ISAKMP:(1030):SA authentication status: authenticated *Jan 20 16:48:22.483: ISAKMP:(1030):SA has

been authenticated with 10.10.10.1 *Jan 20 16:48:22.483: ISAKMP:(1030):SA authentication status:

authenticated *Jan 20 16:48:22.483: ISAKMP:(1030): Process initial contact, bring down existing

phase 1 and 2 SA's with local 10.10.10.2 remote 10.10.10.1 remote port 500 *Jan 20 16:48:22.483:

ISAKMP:(1030):returning IP addr to the address pool *Jan 20 16:48:22.483: ISAKMP: Trying to

insert a peer 10.10.10.2/10.10.10.1/500/, and inserted successfully 6758C6D0. *Jan 20

16:48:22.483: IPSEC(key_engine): got a queue event with 1 KMI message(s) *Jan 20 16:48:22.483:

ISAKMP: set new node -1980405900 to CONF_XAUTH *Jan 20 16:48:22.483: crypto_engine: Generate IKE

hash *Jan 20 16:48:22.483: ISAKMP:(1030):Sending NOTIFY RESPONDER_LIFETIME protocol 1 spi

1727476520, message ID = -1980405900 *Jan 20 16:48:22.483: crypto_engine: Encrypt IKE packet

*Jan 20 16:48:22.483: ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R)

QM_IDLE *Jan 20 16:48:22.483: ISAKMP:(1030):purging node -1980405900 *Jan 20 16:48:22.483:

ISAKMP: Sending phase 1 responder lifetime 86400 *Jan 20 16:48:22.483: ISAKMP:(1030):Input =

IKE_MSG_FROM_PEER, IKE_AM_EXCH *Jan 20 16:48:22.483: ISAKMP:(1030):Old State = IKE_R_AM2 New

State = IKE_P1_COMPLETE *Jan 20 16:48:22.483: ISAKMP:(1030):Need XAUTH *!--- The IOS device now*

processes the Extended Authentication phase !--- after Phase 1 is successful. *Jan 20

16:48:22.483: ISAKMP: set new node -791275911 to CONF_XAUTH *Jan 20 16:48:22.487: ISAKMP/xauth:

request attribute XAUTH_USER_NAME_V2 *Jan 20 16:48:22.487: ISAKMP/xauth: request attribute

XAUTH_USER_PASSWORD_V2 *Jan 20 16:48:22.487: crypto_engine: Generate IKE hash *Jan 20

16:48:22.487: ISAKMP:(1030): initiating peer config to 10.10.10.1. ID = -791275911 *Jan 20

16:48:22.487: crypto_engine: Encrypt IKE packet *Jan 20 16:48:22.487: ISAKMP:(1030): sending

packet to 10.10.10.1 my_port 500 peer_port 500 (R) CONF_XAUTH *Jan 20 16:48:22.487:

ISAKMP:(1030):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE *Jan 20 16:48:22.487:

ISAKMP:(1030):Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_REQ_SENT *Jan 20 16:48:22.519:

ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R) CONF_XAUTH *Jan

20 16:48:22.519: crypto_engine: Decrypt IKE packet *Jan 20 16:48:22.519:

ISAKMP:(1030):processing transaction payload from 10.10.10.1. message ID = -791275911 *Jan 20

16:48:22.519: crypto_engine: Generate IKE hash *Jan 20 16:48:22.519: ISAKMP: Config payload

REPLY *Jan 20 16:48:22.519: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2 *Jan 20

16:48:22.519: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2 *Jan 20 16:48:22.519:

ISAKMP:(1030):deleting node -791275911 error FALSE reason "Done with xauth request/reply exchange" *Jan 20 16:48:22.519: ISAKMP:(1030):Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY *Jan 20 16:48:22.519: ISAKMP:(1030):Old State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT *Jan 20 16:48:22.519: ISAKMP: set new node 44674085 to CONF_XAUTH *Jan 20 16:48:22.519: crypto_engine: Generate IKE hash *Jan 20 16:48:22.519: ISAKMP:(1030): initiating peer config to 10.10.10.1. ID = 44674085 *Jan 20 16:48:22.519: crypto_engine: Encrypt IKE packet *Jan 20 16:48:22.519: ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R) CONF_XAUTH *Jan 20 16:48:22.519: ISAKMP:(1030):Input = IKE_MSG_FROM_AAA, IKE_AAA_CONT_LOGIN *Jan 20 16:48:22.519: ISAKMP:(1030):Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State = IKE_XAUTH_SET_SENT *Jan 20 16:48:22.571: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R) CONF_XAUTH *Jan 20 16:48:22.571: crypto_engine: Decrypt IKE packet *Jan 20 16:48:22.571: ISAKMP:(1030):processing transaction payload from 10.10.10.1. message ID = 44674085 *Jan 20 16:48:22.571: crypto_engine: Generate IKE hash *Jan 20 16:48:22.571: ISAKMP: Config payload ACK *Jan 20 16:48:22.571: ISAKMP:(1030): XAUTH ACK Processed *Jan 20 16:48:22.571: ISAKMP:(1030):deleting node 44674085 error FALSE reason "Transaction mode done" *Jan 20 16:48:22.571: ISAKMP:(1030):Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK *Jan 20 16:48:22.571: ISAKMP:(1030):Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE *Jan 20 16:48:22.571: ISAKMP:(1030):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE *Jan 20 16:48:22.571: ISAKMP:(1030):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *!--- Extended authentication is complete, !--- and mode configuration is now processed.* *Jan 20 16:48:22.619: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R) QM_IDLE *Jan 20 16:48:22.619: ISAKMP: set new node - 2005047200 to QM_IDLE *Jan 20 16:48:22.619: crypto_engine: Decrypt IKE packet *Jan 20 16:48:22.623: ISAKMP:(1030):processing transaction payload from 10.10.10.1. message ID = - 2005047200 *Jan 20 16:48:22.623: crypto_engine: Generate IKE hash *Jan 20 16:48:22.623: ISAKMP: Config payload REQUEST *Jan 20 16:48:22.623: ISAKMP:(1030):checking request: *Jan 20 16:48:22.623: ISAKMP: DEFAULT_DOMAIN *Jan 20 16:48:22.623: ISAKMP: IP4_NBNS *Jan 20 16:48:22.623: ISAKMP: IP4_DNS *Jan 20 16:48:22.623: ISAKMP: SPLIT_INCLUDE *Jan 20 16:48:22.623: ISAKMP: SPLIT_DNS *Jan 20 16:48:22.623: ISAKMP: PFS *Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7800 *Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7801 *Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7802 *Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7803 *Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7804 *Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7805 *Jan 20 16:48:22.623: ISAKMP: CONFIG_MODE_UNKNOWN Unknown Attr: 0x7806 *Jan 20 16:48:22.623: ISAKMP: BACKUP_SERVER *Jan 20 16:48:22.623: ISAKMP: APPLICATION_VERSION *Jan 20 16:48:22.623: ISAKMP/author: Author request for group hw client successfully sent to AAA *Jan 20 16:48:22.623: ISAKMP:(1030):Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST *Jan 20 16:48:22.623: ISAKMP:(1030):Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT *Jan 20 16:48:22.623: ISAKMP:(1030):attributes sent in message: *Jan 20 16:48:22.623: ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com *Jan 20 16:48:22.623: ISAKMP: Sending IP4_NBNS server address: 172.22.1.102 *Jan 20 16:48:22.623: ISAKMP: Sending IP4_DNS server address: 172.22.1.101 *Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7800) *Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7801) *Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7802) *Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7803) *Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7804) *Jan 20 16:48:22.623: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7805) *Jan 20 16:48:22.627: ISAKMP (0/1030): Unknown Attr: CONFIG_MODE_UNKNOWN (0x7806) *Jan 20 16:48:22.627: ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(4)T1, RELEASE SOFTWARE (fc4) Technical Support: <http://www.cisco.com/techsupport> Copyright (c) 1986-2005 by Cisco Systems, Inc. Compiled Wed 21-Dec-05 22:58 by ccai *Jan 20 16:48:22.627: crypto_engine: Generate IKE hash *Jan 20 16:48:22.627: ISAKMP:(1030): responding to peer config from 10.10.10.1. ID = - 2005047200 *Jan 20 16:48:22.627: crypto_engine: Encrypt IKE packet *Jan 20 16:48:22.627: ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R) CONF_ADDR *Jan 20 16:48:22.627: ISAKMP:(1030):deleting node -2005047200 error FALSE reason "No Error" *Jan 20 16:48:22.627: ISAKMP:(1030):Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR *Jan 20 16:48:22.627: ISAKMP:(1030):Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE *Jan 20 16:48:22.627: ISAKMP:(1030):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE *Jan 20 16:48:22.627: ISAKMP:(1030):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE *Jan 20 16:48:27.695: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500 Global (R) QM_IDLE *Jan 20 16:48:27.695: ISAKMP: set new node 1887305923 to QM_IDLE *Jan 20 16:48:27.695: crypto_engine: Decrypt IKE packet *Jan 20 16:48:27.699: crypto_engine: Generate IKE hash *Jan 20 16:48:27.699: ISAKMP:(1030): processing HASH payload. message ID = 1887305923 *Jan 20 16:48:27.699: ISAKMP:(1030): processing SA payload. message ID = 1887305923 *Jan 20 16:48:27.699:

ISAKMP:(1030):Checking IPsec proposal 1 *Jan 20 16:48:27.699: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.699: ISAKMP: attributes in transform: *Jan 20 16:48:27.699: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.699: ISAKMP: SA life type in seconds *Jan 20 16:48:27.699: ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.699: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.699: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.699: ISAKMP: authenticator is HMAC-SHA *Jan 20 16:48:27.699: ISAKMP: key length is 256 *Jan 20 16:48:27.699: CryptoEngine0: validate proposal *Jan 20 16:48:27.699: ISAKMP:(1030):atts are acceptable. *Jan 20 16:48:27.699: IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.699: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0 *Jan 20 16:48:27.699: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 256 esp-sha-hmac } *Jan 20 16:48:27.699: ISAKMP:(1030): IPsec policy invalidated proposal *Jan 20 16:48:27.699: ISAKMP:(1030):Checking IPsec proposal 2 *Jan 20 16:48:27.699: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.699: ISAKMP: attributes in transform: *Jan 20 16:48:27.699: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.699: ISAKMP: SA life type in seconds *Jan 20 16:48:27.699: ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.699: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.699: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.699: ISAKMP: authenticator is HMAC-MD5 *Jan 20 16:48:27.699: ISAKMP: key length is 256 *Jan 20 16:48:27.699: CryptoEngine0: validate proposal *Jan 20 16:48:27.699: ISAKMP:(1030):atts are acceptable. *!--- Proceed for processing Phase 2.* *Jan 20 16:48:27.699: IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.699: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0 *Jan 20 16:48:27.699: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 256 esp-md5-hmac } *Jan 20 16:48:27.699: ISAKMP:(1030): IPsec policy invalidated proposal *Jan 20 16:48:27.703: ISAKMP:(1030):Checking IPsec proposal 3 *Jan 20 16:48:27.703: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.703: ISAKMP: attributes in transform: *Jan 20 16:48:27.703: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.703: ISAKMP: SA life type in seconds *Jan 20 16:48:27.703: ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.703: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.703: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.703: ISAKMP: authenticator is HMAC-SHA *Jan 20 16:48:27.703: ISAKMP: key length is 192 *Jan 20 16:48:27.703: CryptoEngine0: validate proposal *Jan 20 16:48:27.703: ISAKMP:(1030):atts are acceptable. *Jan 20 16:48:27.703: IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.703: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 192 esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 192, flags= 0x0 *Jan 20 16:48:27.703: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 192 esp-sha-hmac } *Jan 20 16:48:27.703: ISAKMP:(1030): IPsec policy invalidated proposal *Jan 20 16:48:27.703: ISAKMP:(1030):Checking IPsec proposal 4 *Jan 20 16:48:27.703: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.703: ISAKMP: attributes in transform: *Jan 20 16:48:27.703: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.703: ISAKMP: SA life type in seconds *Jan 20 16:48:27.703: ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.703: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.703: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.703: ISAKMP: authenticator is HMAC-MD5 *Jan 20 16:48:27.703: ISAKMP: key length is 192 *Jan 20 16:48:27.703: CryptoEngine0: validate proposal *Jan 20 16:48:27.703: ISAKMP:(1030):atts are acceptable. *Jan 20 16:48:27.703: IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.703: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 192 esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 192, flags= 0x0 *Jan 20 16:48:27.703: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes 192 esp-md5-hmac } *Jan 20 16:48:27.703: ISAKMP:(1030): IPsec policy invalidated proposal *Jan 20 16:48:27.703: ISAKMP:(1030):Checking IPsec proposal 5 *Jan 20 16:48:27.703: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.703: ISAKMP: attributes in transform: *Jan 20 16:48:27.703: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.703: ISAKMP: SA life type in seconds *Jan 20 16:48:27.703: ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.703: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.703: ISAKMP: SA life duration

(VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.707: ISAKMP: authenticator is HMAC-SHA *Jan 20 16:48:27.707: ISAKMP: key length is 128 *Jan 20 16:48:27.707: CryptoEngine0: validate proposal *Jan 20 16:48:27.707: ISAKMP:(1030):atts are acceptable. *Jan 20 16:48:27.707: IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.707: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0 *Jan 20 16:48:27.707: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes esp-sha-hmac } *Jan 20 16:48:27.707: ISAKMP:(1030): IPsec policy invalidated proposal *Jan 20 16:48:27.707: ISAKMP:(1030):Checking IPsec proposal 6 *Jan 20 16:48:27.707: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.707: ISAKMP: attributes in transform: *Jan 20 16:48:27.707: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.707: ISAKMP: SA life type in seconds *Jan 20 16:48:27.707: ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.707: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.707: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.707: ISAKMP: authenticator is HMAC-MD5 *Jan 20 16:48:27.707: ISAKMP: key length is 128 *Jan 20 16:48:27.707: CryptoEngine0: validate proposal *Jan 20 16:48:27.707: ISAKMP:(1030):atts are acceptable. *Jan 20 16:48:27.707: IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.707: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0 *Jan 20 16:48:27.707: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-aes esp-md5-hmac } *Jan 20 16:48:27.707: ISAKMP:(1030): IPsec policy invalidated proposal *Jan 20 16:48:27.707: ISAKMP:(1030):Checking IPsec proposal 7 *Jan 20 16:48:27.707: ISAKMP: transform 1, ESP_3DES *Jan 20 16:48:27.707: ISAKMP: attributes in transform: *Jan 20 16:48:27.707: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.707: ISAKMP: SA life type in seconds *Jan 20 16:48:27.707: ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.707: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.707: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.707: ISAKMP: authenticator is HMAC-SHA *Jan 20 16:48:27.711: CryptoEngine0: validate proposal *Jan 20 16:48:27.711: ISAKMP:(1030):atts are acceptable. *Jan 20 16:48:27.711: IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.711: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0 *Jan 20 16:48:27.711: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-3des esp-sha-hmac } *Jan 20 16:48:27.711: ISAKMP:(1030): IPsec policy invalidated proposal *Jan 20 16:48:27.711: ISAKMP:(1030):Checking IPsec proposal 8 *Jan 20 16:48:27.711: ISAKMP: transform 1, ESP_3DES *Jan 20 16:48:27.711: ISAKMP: attributes in transform: *Jan 20 16:48:27.711: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.711: ISAKMP: SA life type in seconds *Jan 20 16:48:27.711: ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.711: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.711: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.711: ISAKMP: authenticator is HMAC-MD5 *Jan 20 16:48:27.711: CryptoEngine0: validate proposal *Jan 20 16:48:27.711: ISAKMP:(1030):atts are acceptable. *Jan 20 16:48:27.711: IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.711: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0 *Jan 20 16:48:27.715: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for identity: {esp-3des esp-md5-hmac } *Jan 20 16:48:27.715: ISAKMP:(1030): IPsec policy invalidated proposal *Jan 20 16:48:27.715: ISAKMP:(1030):Checking IPsec proposal 9 *Jan 20 16:48:27.715: ISAKMP: transform 1, ESP_DES *Jan 20 16:48:27.715: ISAKMP: attributes in transform: *Jan 20 16:48:27.715: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.715: ISAKMP: SA life type in seconds *Jan 20 16:48:27.715: ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.715: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.715: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.715: ISAKMP: authenticator is HMAC-MD5 *Jan 20 16:48:27.715: CryptoEngine0: validate proposal *Jan 20 16:48:27.715: ISAKMP:(1030):atts are acceptable. *Jan 20 16:48:27.715: IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.715: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 10.10.10.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0 *Jan 20

16:48:27.715: ISAKMP:(1030): processing NONCE payload. message ID = 1887305923 *Jan 20
16:48:27.715: ISAKMP:(1030): processing ID payload. message ID = 1887305923 *Jan 20
16:48:27.715: ISAKMP:(1030): processing ID payload. message ID = 1887305923 *Jan 20
16:48:27.715: ISAKMP:(1030): asking for 1 spis from ipsec *Jan 20 16:48:27.715:
ISAKMP:(1030):Node 1887305923, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH *Jan 20 16:48:27.715:
ISAKMP:(1030):Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE *Jan 20 16:48:27.719:
IPSEC(key_engine): got a queue event with 1 KMI message(s) *Jan 20 16:48:27.719:
IPSEC(spi_response): getting spi 185206738 for SA from 10.10.10.2 to 10.10.10.1 for prot 3 *Jan
20 16:48:27.719: crypto_engine: Generate IKE hash *Jan 20 16:48:27.719: crypto_engine: Generate
IKE QM keys *Jan 20 16:48:27.719: crypto_engine: Create IPsec SA (by keys) *Jan 20 16:48:27.719:
crypto_engine: Generate IKE QM keys *Jan 20 16:48:27.719: crypto_engine: Create IPsec SA (by
keys) *Jan 20 16:48:27.719: ISAKMP:(1030): Creating IPsec SAs *Jan 20 16:48:27.719: inbound SA
from 10.10.10.1 to 10.10.10.2 (f/i) 0/ 0 (proxy 10.10.10.1 to 0.0.0.0) *Jan 20 16:48:27.719: has
spi 0xB0A07D2 and conn_id 0 *Jan 20 16:48:27.719: lifetime of 28800 seconds *Jan 20
16:48:27.719: lifetime of 4608000 kilobytes *Jan 20 16:48:27.719: outbound SA from 10.10.10.2 to
10.10.10.1 (f/i) 0/0 (proxy 0.0.0.0 to 10.10.10.1) *Jan 20 16:48:27.719: has spi 0xB22446D and
conn_id 0 *Jan 20 16:48:27.719: lifetime of 28800 seconds *Jan 20 16:48:27.719: lifetime of
4608000 kilobytes *Jan 20 16:48:27.719: crypto_engine: Encrypt IKE packet *Jan 20 16:48:27.719:
ISAKMP:(1030): sending packet to 10.10.10.1 my_port 500 peer_port 500 (R) QM_IDLE *Jan 20
16:48:27.719: ISAKMP:(1030):Node 1887305923, Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY *Jan 20
16:48:27.719: ISAKMP:(1030):Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 *Jan 20
16:48:27.719: IPSEC(key_engine): got a queue event with 1 KMI message(s) *Jan 20 16:48:27.723:
IPsec: Flow_switching Allocated flow for sibling 80000014 *Jan 20 16:48:27.723:
IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.10.10.1, dest_port 0 *Jan 20 16:48:27.723:
IPSEC(create_sa): sa created, (sa) sa_dest= 10.10.10.2, sa_proto= 50, sa_spi=
0xB0A07D2(185206738), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 37 *Jan 20 16:48:27.723:
IPSEC(create_sa): sa created, (sa) sa_dest= 10.10.10.1, sa_proto= 50, sa_spi=
0xB22446D(186795117), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 38 *!--- The two IPsec SAs
shown above are for management purposes.* *Jan 20 16:48:27.771: ISAKMP (0:1030): received packet
from 10.10.10.1 dport 500 sport 500 Global (R) QM_IDLE *Jan 20 16:48:27.771: crypto_engine:
Decrypt IKE packet *Jan 20 16:48:27.771: crypto_engine: Generate IKE hash *Jan 20 16:48:27.771:
ISAKMP:(1030):deleting node 1887305923 error FALSE reason "QM done (await)" *Jan 20
16:48:27.771: ISAKMP:(1030):Node 1887305923, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH *Jan 20
16:48:27.771: ISAKMP:(1030):Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE *Jan 20
16:48:27.771: IPSEC(key_engine): got a queue event with 1 KMI message(s) *Jan 20 16:48:27.771:
IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP *Jan 20 16:48:27.771:
IPSEC(key_engine_enable_outbound): enable SA with spi 186795117/50 *Jan 20 16:48:27.771:
IPSEC(update_current_outbound_sa): updated peer 10.10.10.1 current outbound sa to SPI B22446D
*Jan 20 16:48:27.771: ISAKMP (0:1030): received packet from 10.10.10.1 dport 500 sport 500
Global (R) QM_IDLE *Jan 20 16:48:27.771: ISAKMP: set new node -1259355083 to QM_IDLE *Jan 20
16:48:27.771: crypto_engine: Decrypt IKE packet *Jan 20 16:48:27.775: crypto_engine: Generate
IKE hash *Jan 20 16:48:27.775: ISAKMP:(1030): processing HASH payload. message ID = -1259355083
*Jan 20 16:48:27.775: ISAKMP:(1030): processing SA payload. message ID = -1259355083 *Jan 20
16:48:27.775: ISAKMP:(1030):Checking IPsec proposal 1 *Jan 20 16:48:27.775: ISAKMP: transform 1,
ESP_AES *Jan 20 16:48:27.775: ISAKMP: attributes in transform: *Jan 20 16:48:27.775: ISAKMP:
encaps is 1 (Tunnel) *Jan 20 16:48:27.775: ISAKMP: SA life type in seconds *Jan 20 16:48:27.775:
ISAKMP: SA life duration (basic) of 28800 *Jan 20 16:48:27.775: ISAKMP: SA life type in
kilobytes *Jan 20 16:48:27.775: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Jan 20
16:48:27.775: ISAKMP: authenticator is HMAC-SHA *Jan 20 16:48:27.775: ISAKMP: key length is 256
*Jan 20 16:48:27.775: CryptoEngine0: validate proposal *Jan 20 16:48:27.775: ISAKMP:(1030):atts
are acceptable. *Jan 20 16:48:27.775: IPSEC(validate_proposal_request): proposal part #1 *Jan 20
16:48:27.775: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local=
10.10.10.2, remote= 10.10.10.1, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=
172.16.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-aes 256 esp-sha-hmac
(Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0 *Jan 20
16:48:27.775: IPSEC(crypto_ipsec_process_proposal): transform proposal not supported for
identity: {esp-aes 256 esp-sha-hmac } *Jan 20 16:48:27.775: ISAKMP:(1030): IPsec policy
invalidated proposal *Jan 20 16:48:27.775: ISAKMP:(1030):Checking IPsec proposal 2 *Jan 20
16:48:27.775: ISAKMP: transform 1, ESP_AES *Jan 20 16:48:27.775: ISAKMP: attributes in
transform: *Jan 20 16:48:27.775: ISAKMP: encaps is 1 (Tunnel) *Jan 20 16:48:27.775: ISAKMP: SA
life type in seconds *Jan 20 16:48:27.775: ISAKMP: SA life duration (basic) of 28800 *Jan 20
16:48:27.775: ISAKMP: SA life type in kilobytes *Jan 20 16:48:27.775: ISAKMP: SA life duration
(VPI) of 0x0 0x46 0x50 0x0 *Jan 20 16:48:27.775: ISAKMP: authenticator is HMAC-MD5 *Jan 20
16:48:27.775: ISAKMP: key length is 256 *Jan 20 16:48:27.775: CryptoEngine0: validate proposal

*Jan 20 16:48:27.775: ISAKMP:(1030):atts are acceptable. *Jan 20 16:48:27.775:
IPSEC(validate_proposal_request): proposal part #1 *Jan 20 16:48:27.799: IPSEC(create_sa): sa
created, (sa) sa_dest= 10.10.10.2, sa_proto= 50, sa_spi= 0x990A0C2C(2567572524), sa_trans= esp-
des esp-md5-hmac , sa_conn_id= 39 *Jan 20 16:48:27.799: IPSEC(create_sa): sa created, (sa)
sa_dest= 10.10.10.1, sa_proto= 50, sa_spi= 0x9FBC4C0D(2679917581), sa_trans= esp-des esp-md5-
hmac , sa_conn_id= 40 !--- *The two IPSec SAs shown above are for actual data traffic.*

Gerelateerde informatie

- [IPsec-onderhandeling/IKE-protocollen](#)
- [PIX 500 Series security applicaties](#)
- [PIX-opdrachtreferenties](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)