ASA/PIX: IPsec VPN-clientadressering met DHCP-server met ASDM-configuratievoorbeeld

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Verwante producten
Conventies
Achtergrondinformatie
Configureren
Netwerkdiagram
Externe toegang instellen (IPSec)
ASA/PIX configureren met CLI
Cisco VPN-clientconfiguratie
Verifiëren
Opdrachten tonen
Problemen oplossen
Beveiligingsassociaties wissen
Opdrachten voor probleemoplossing
Monster debug-uitvoer
Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u de Cisco 5500 Series adaptieve security applicatie (ASA) kunt configureren om van de DHCP-server het IP-adres van de client te maken naar alle VPN-clients met behulp van de Adaptieve Security Devices Manager (ASDM) of CLI. De ASDM levert veiligheidsbeheer en controle van wereldklasse door middel van een intuïtieve, makkelijk te gebruiken web-gebaseerde beheerinterface. Nadat de Cisco ASA-configuratie is voltooid, kan deze worden geverifieerd met behulp van de Cisco VPN-client.

Raadpleeg PIX/ASA 7.x en Cisco VPN-client 4.x met Windows 2003 IAS RADIUS (Against Active Directory) verificatievoorbeeld voor het instellen van de VPN-verbinding op afstand tussen een Cisco VPN-client (4.x voor Windows) en de PIX 500 Series security applicatie 7.x. De externe VPN-clientgebruiker authenticeert de actieve map met een Microsoft Windows 2003-server voor internetverificatie (IAS) RADIUS.

Raadpleeg PIX/ASA 7.x en Cisco VPN-client 4.x voor Cisco Secure ACS-verificatie Configuratievoorbeeld om een VPN-verbinding op afstand in te stellen tussen een Cisco VPN-client (4.x voor Windows) en PIX 500 Series security applicatie 7.x met een Cisco Secure Access

Control Server (ACS versie 3.2) voor uitgebreide verificatie (Xauth).

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de ASA volledig operationeel en geconfigureerd is om Cisco ASDM of CLI in staat te stellen configuratiewijzigingen door te voeren.

Opmerking: Raadpleeg HTTPS-toegang voor ASDM of PIX/ASA 7.x: SSH in het Voorbeeld van de configuratie van binnen en buiten om het apparaat extern te kunnen configureren door de ASDM of Secure Shell (SSH).

Gebruikte componenten

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

- Software voor Cisco adaptieve security applicatie, versie 7.x en hoger
- Adaptieve Security Office Manager versie 5.x en hoger
- Cisco VPN-clientversie 4.x en hoger

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.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco PIX security applicatie versie 7.x en hoger.

Conventies

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

Achtergrondinformatie

VPN’s voor externe toegang voldoen aan de vereisten van de mobiele medewerkers om zich veilig aan te sluiten op het netwerk van de organisatie. Mobiele gebruikers kunnen een beveiligde verbinding opzetten met behulp van de VPN-clientsoftware die op hun pc’s is geïnstalleerd. De VPN-client initieert een verbinding met een centraal siteapparaat dat is geconfigureerd om deze verzoeken te aanvaarden. In dit voorbeeld is het centrale plaatsapparaat een ASA 5500 Series adaptieve security applicatie die dynamische crypto kaarten gebruikt.

In het beheer van het veiligheidsapparaat moeten we IP adressen configureren die een client verbinden met een resource op het privénetwerk, door de tunnel en de client laten functioneren alsof deze direct verbonden is met het privénetwerk. Bovendien hebben we alleen te maken met de privé IP-adressen die aan klanten worden toegewezen. De IP-adressen die aan andere bronnen op uw privénetwerk zijn toegewezen, maken deel uit van uw netwerkbeheerverantwoordelijkheden en maken geen deel uit van VPN-beheer. Daarom, wanneer

IP adressen hier worden besproken, bedoelen we die IP adressen beschikbaar in uw privé netwerk adresseringsschema die de client als tunneleindpunt laten functioneren.

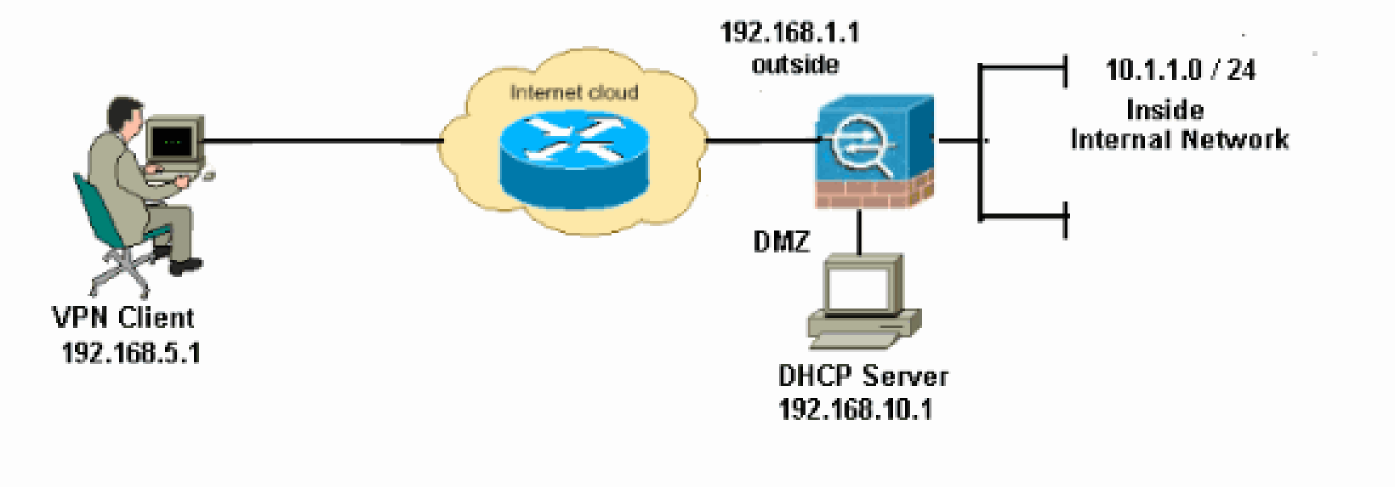
Configureren

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

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



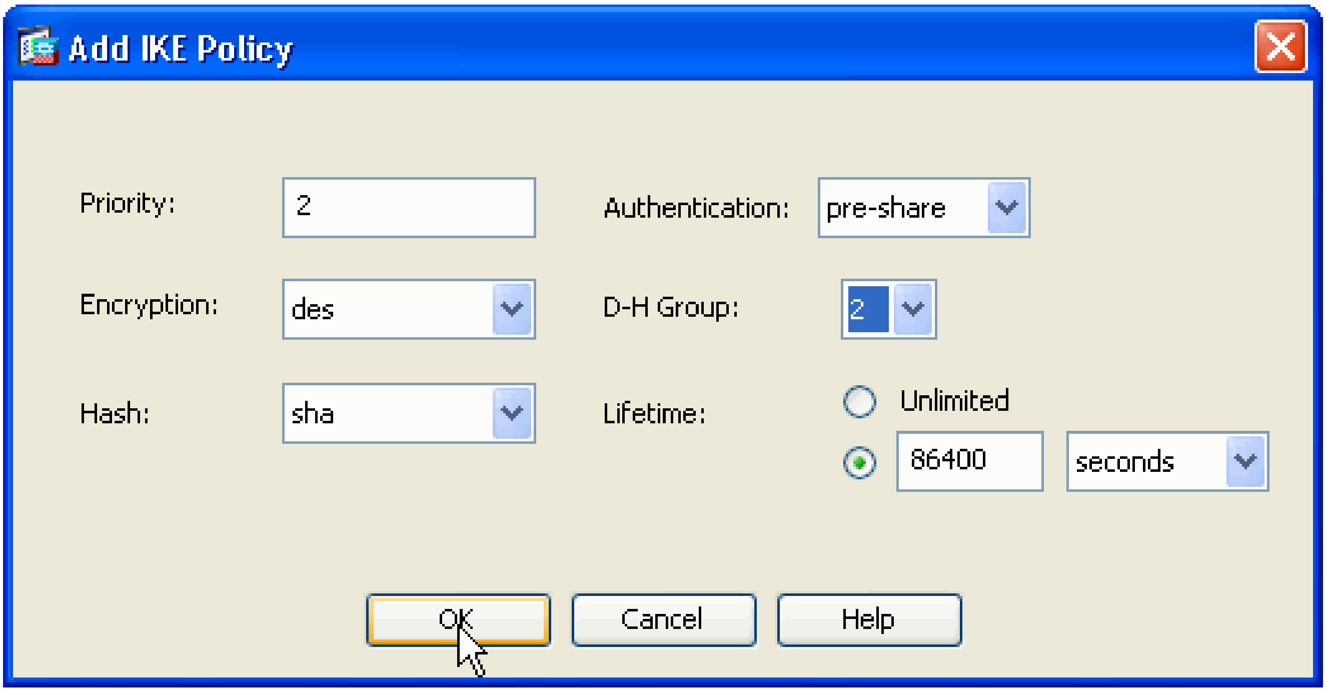
Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918-adressen die in een labomgeving werden gebruikt.

Externe toegang instellen (IPSec)

ASDM-procedure

Voltooi deze stappen om de externe VPN-toegang te configureren:

1. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE-beleid > Add** om een ISAKMP-beleid 2 te maken, zoals wordt getoond.



Priority: 2

Authentication: pre-share

Encryption: des

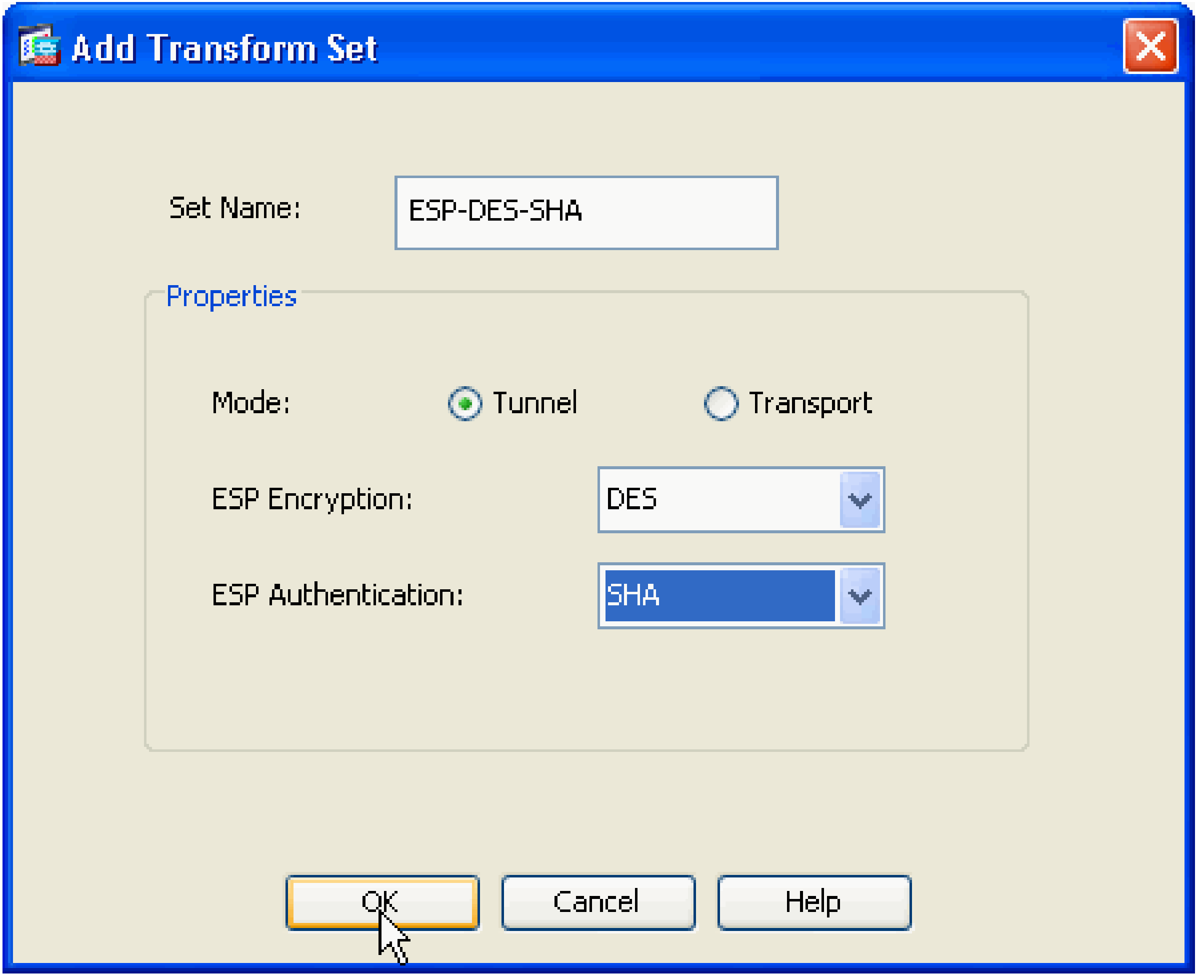
D-H Group: 2

Hash: sha

Lifetime: ○ Unlimited ● 86400 seconds

Klik op **OK** en **Toepassen**.

2. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transformatiesets > Add** om de **ESP-DES-SHA** transformatieset te maken, zoals



Set Name: ESP-DES-SHA

Properties

Mode: ● Tunnel ○ Transport

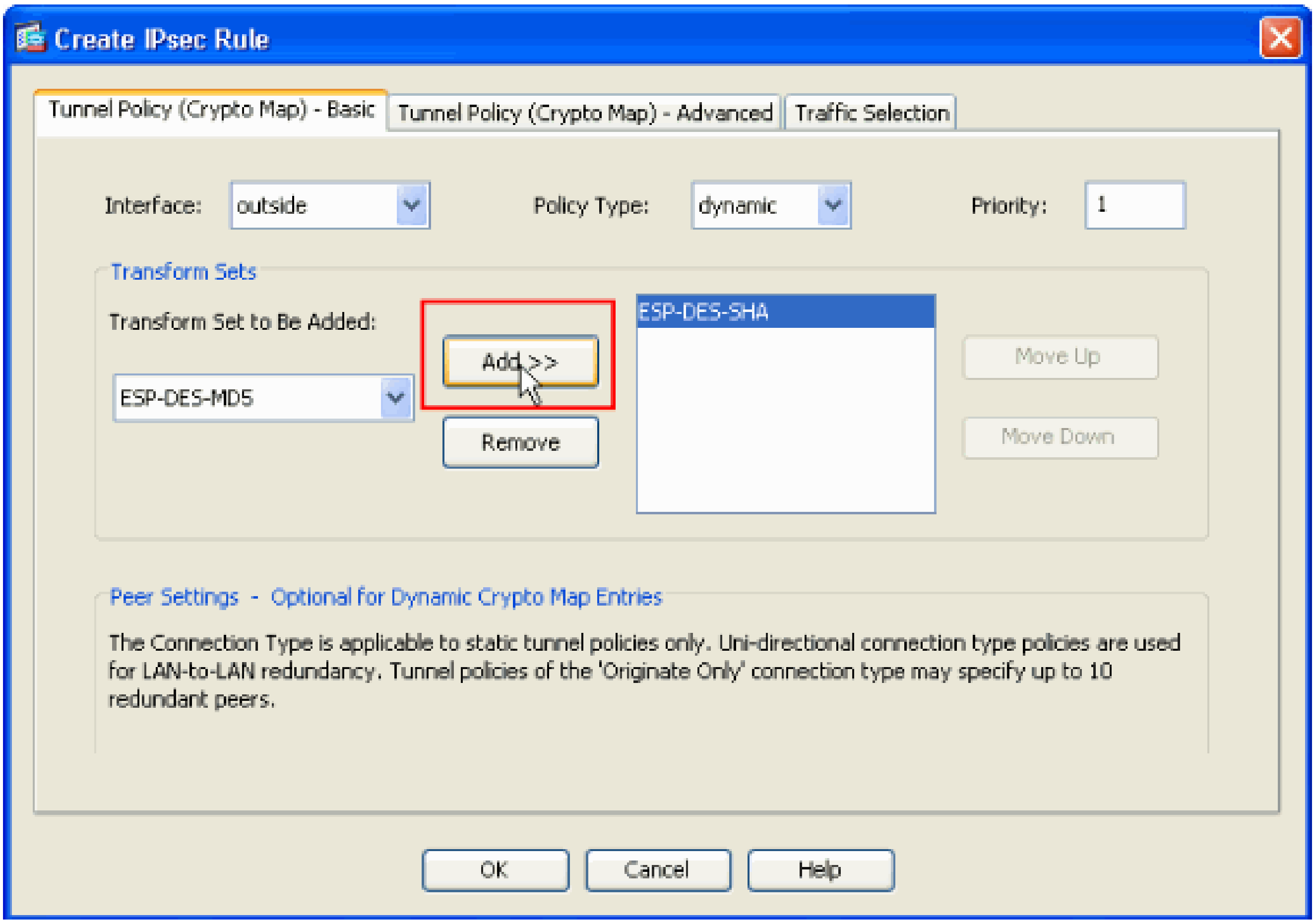
ESP Encryption: DES

ESP Authentication: SHA

getoond.

Klik op **OK** en **Toepassen**.

3. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add** om een crypto-kaart te maken met dynamisch beleid van prioriteit 1, zoals
getoond.



Create IPsec Rule

Interface: outside

Policy Type: dynamic

Priority: 1

Transform Sets

Transform Set to Be Added: ESP-DES-MD5

ESP-DES-SHA

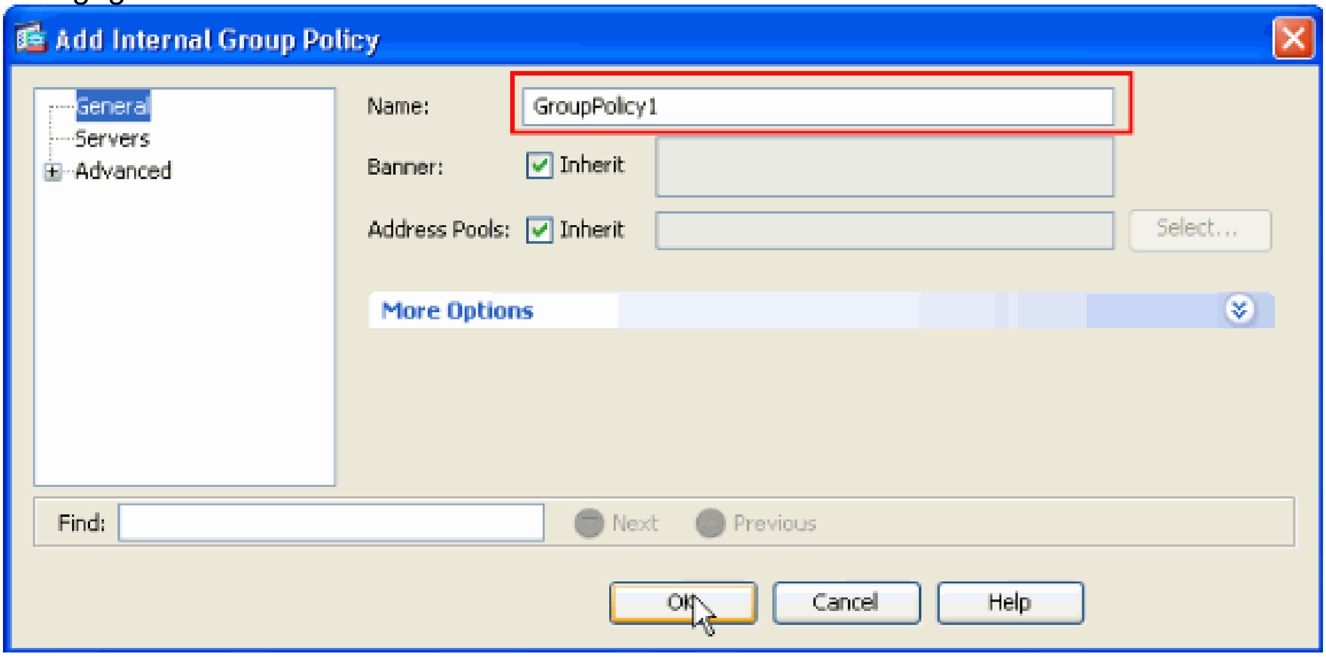
Peer Settings - Optional for Dynamic Crypto Map Entries

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
Add >>
Remove
Move Up
Move Down
OK
Cancel
Help

Klik op **OK** en **Toepassen**.

4. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policy > Add>Intern Group Policy** om een groepsbeleid (bijvoorbeeld **Group** Policy**1**) te maken, zoals wordt weergegeven.



Add Internal Group Policy

Name: GroupPolicy1

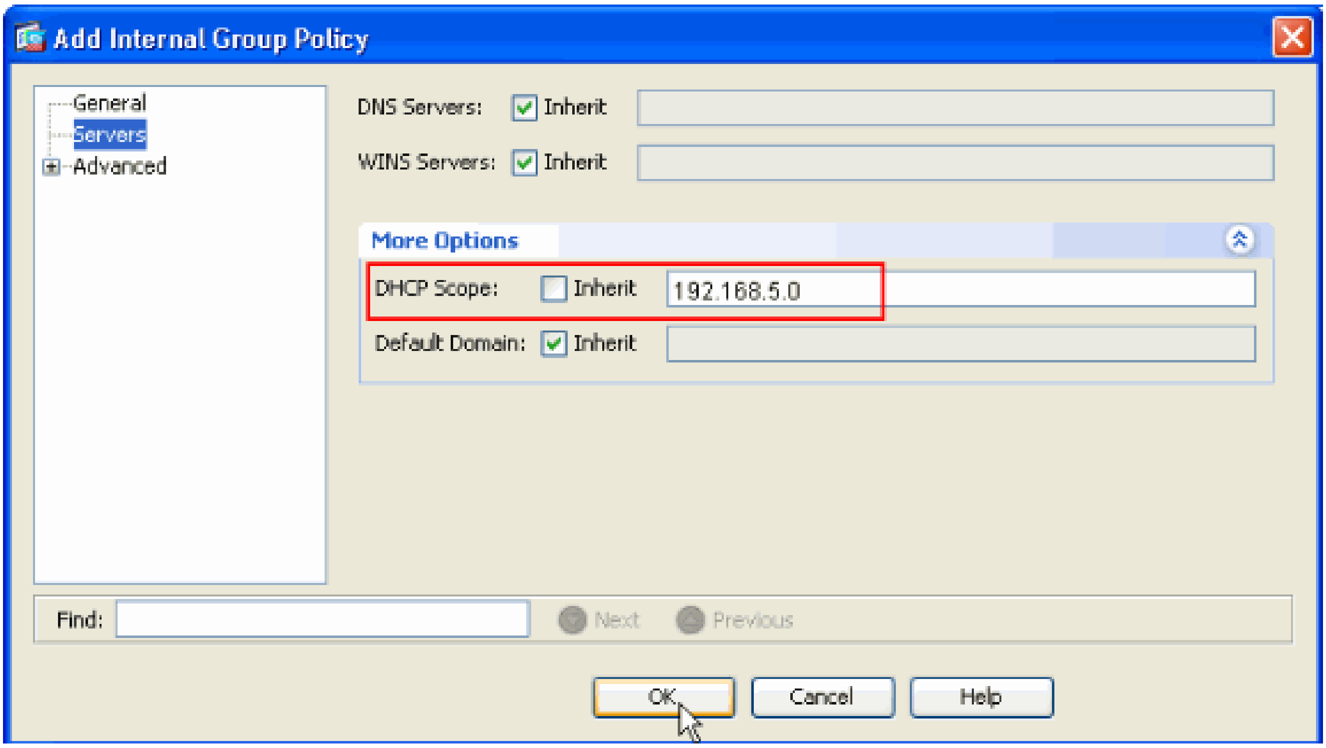
Banner: ☑ Inherit

Address Pools: ☑ Inherit

Find:

Klik op **OK** en **Toepassen**.

5. Kies **Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policy > Add>Intern groepsbeleid>servers>** om de **DHCP-toepassingsbereik** voor de VPN-clientgebruikers dynamisch te configureren.


Add Internal Group Policy

DNS Servers: ☑ Inherit

WINS Servers: ☑ Inherit

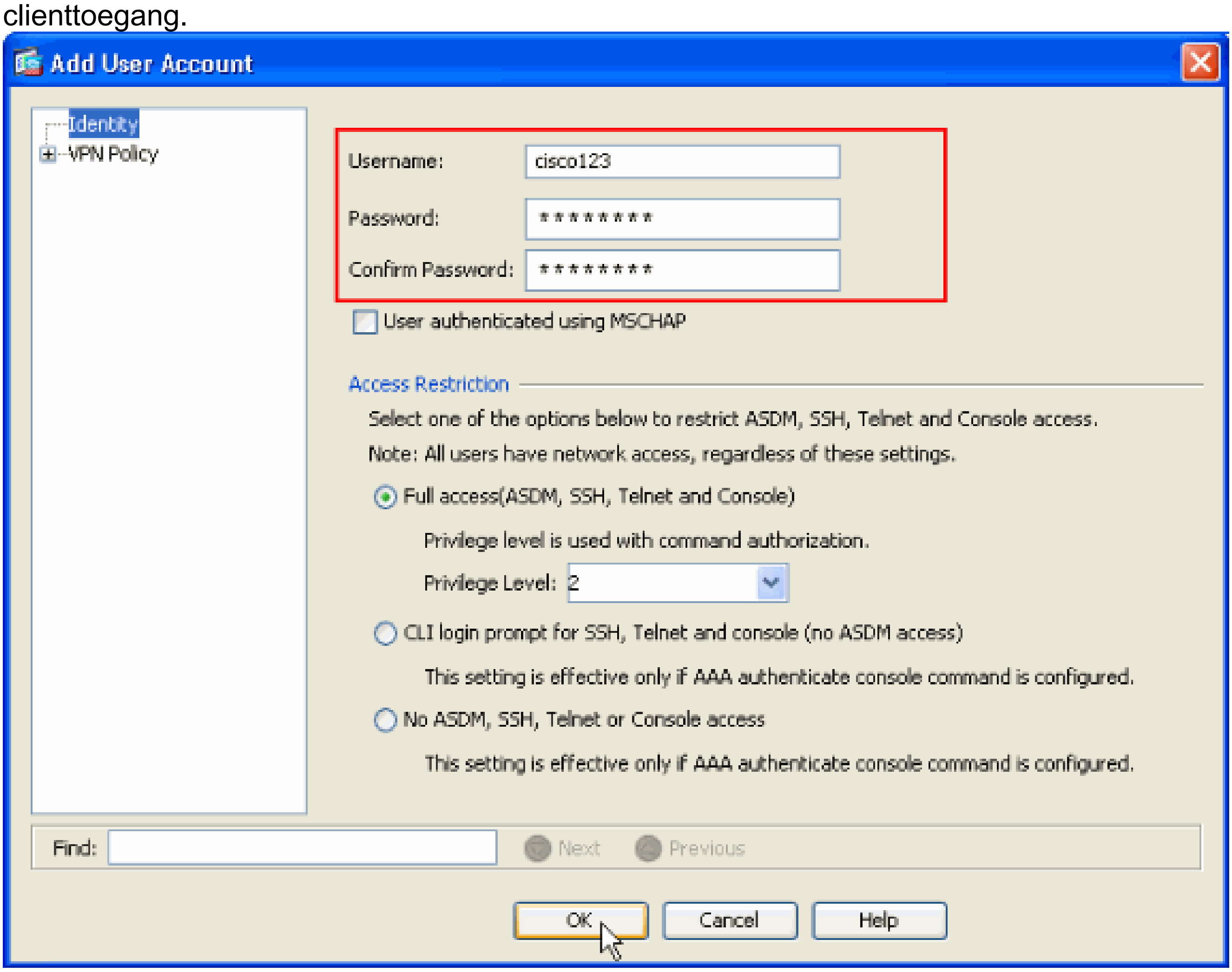
More Options

DHCP Scope: □ Inherit 192.168.5.0

Default Domain: ☑ Inherit

Klik op **OK** en **Toepassen.Opmerking: de** configuratie van DHCP Relay is optioneel. Raadpleeg DHCP-adressering voor meer informatie configureren.

6. Kies **Configuration > Remote Access VPN > AAA-instelling > Local Gebruikers > Add** om de gebruikersaccount te maken (bijvoorbeeld gebruikersnaam - cisco123 en Wachtwoord - cisco123) voor VPN-clienttoegang.


Add User Account

Username: cisco123

Password: ********

Confirm Password: ********

□ User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

● Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 2

○ CLI login prompt for SSH, Telnet and console (no ASDM access)

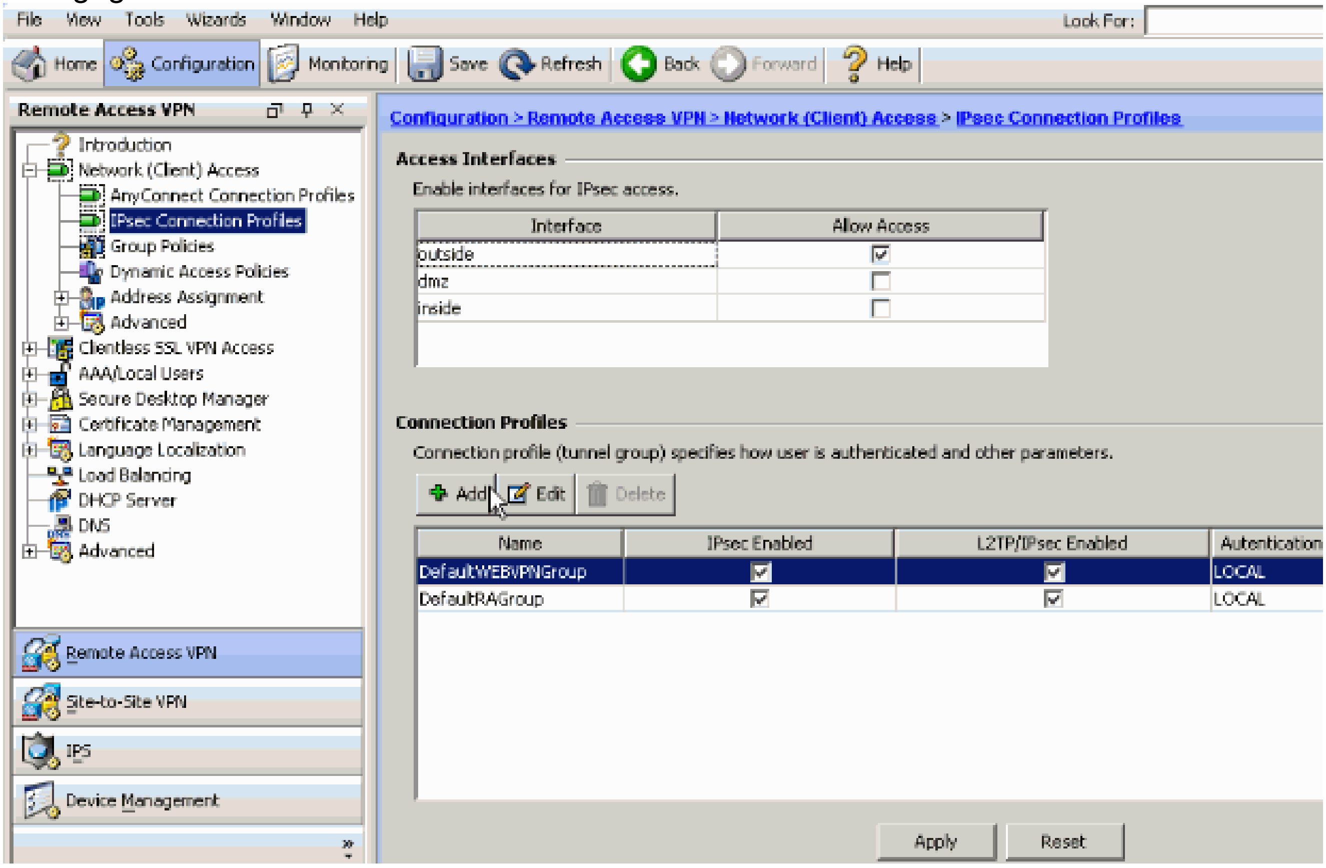
This setting is effective only if AAA authenticate console command is configured.

○ No ASDM, SSH, Telnet or Console access

This setting is effective only if AAA authenticate console command is configured.

7. Kies **Configuration > Remote Access VPN > Network (Client) Access > IPSec Connection**

Profiles > Add> om een tunnelgroep toe te voegen (bijvoorbeeld **TunnelGroup1** en de PreShared Key zoals cisco123), zoals wordt
weergegeven.



Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

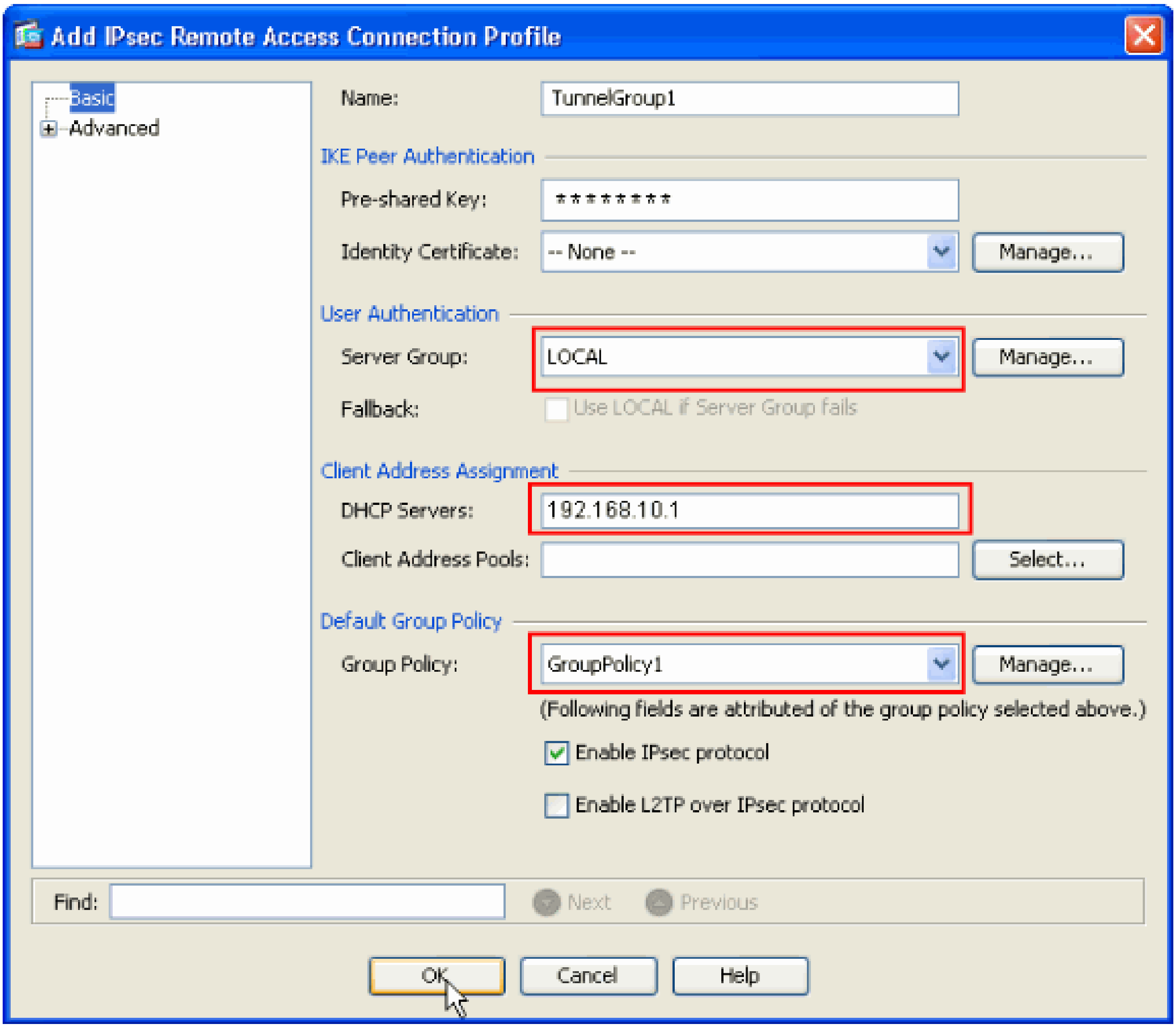
Interface	Allow Access
outside	☑
dmz	□
inside	□

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

Name	IPsec Enabled	L2TP/IPsec Enabled	Autentication
DefaultWEBVPNGroup	☑	☑	LOCAL
DefaultRAGroup	☑	☑	LOCAL

Kies onder het tabblad **Basic** de servergroep als **LOCAL** voor het veld Gebruikersverificatie.Kies **Groepsbeleid1** als het groepsbeleid voor het veld Standaardgroepsbeleid.Geef het IP-adres van de DHCP-server op in de ruimte die voor **DHCP-servers** is
meegeleverd.



Name: TunnelGroup1

IKE Peer Authentication

Pre-shared Key: ********

Identity Certificate: -- None --

User Authentication

Server Group: LOCAL

Fallback: □ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers: 192.168.10.1

Client Address Pools:

Default Group Policy

Group Policy: GroupPolicy1

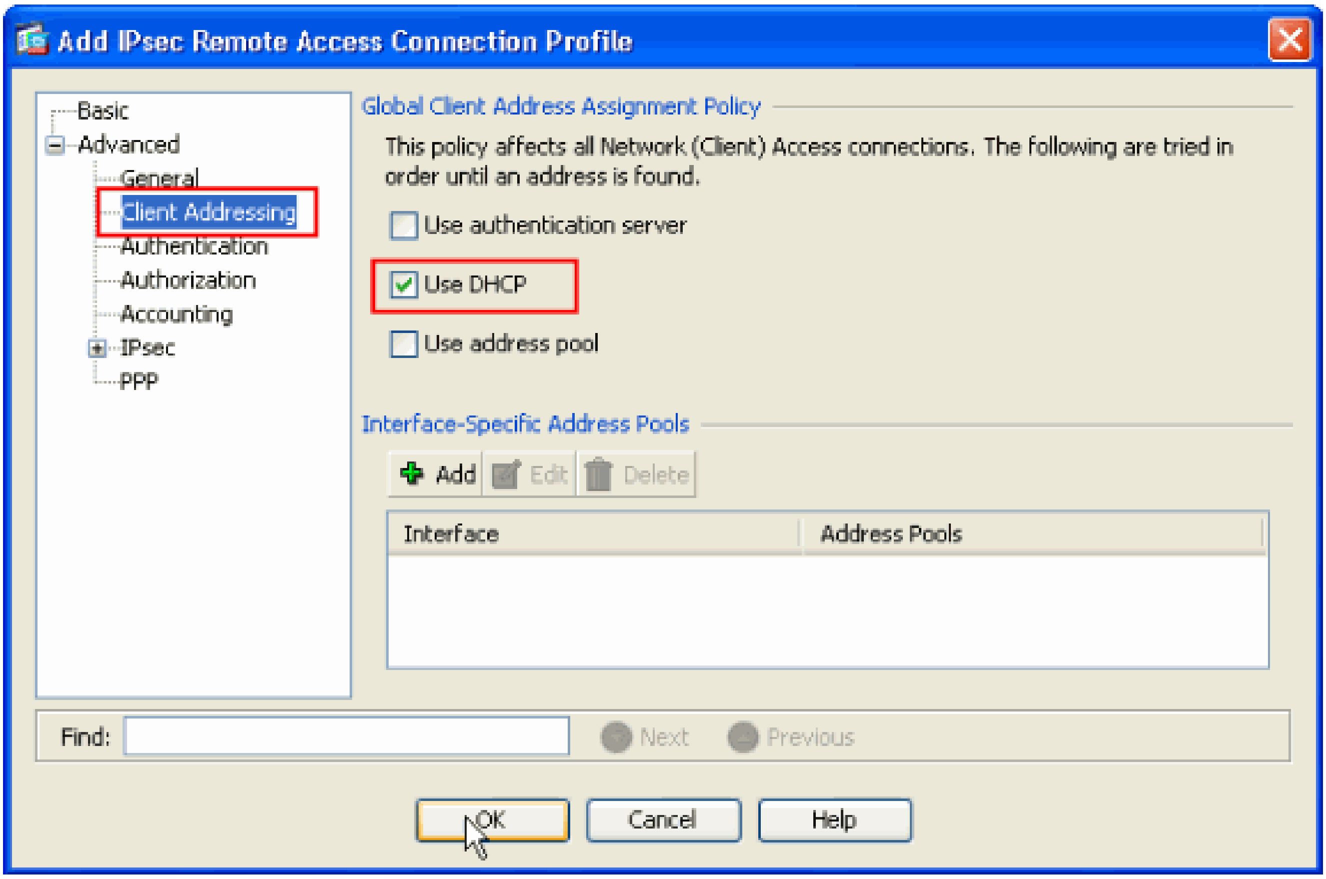
(Following fields are attributed of the group policy selected above.)

☑ Enable IPsec protocol

□ Enable L2TP over IPsec protocol

Klik op **OK**.

8. Kies **Geavanceerd > Clientadressering >** en controleer het selectiekader **met DHCP** voor de DHCP-server om IP-adres aan de VPN-clients toe te wijzen.**Opmerking:** Schakel de vinkjes uit voor **gebruik van de authenticatieserver** en **gebruik de adrestoewijzing**.



Global Client Address Assignment Policy

This policy affects all Network (Client) Access connections. The following are tried in order until an address is found.

□ Use authentication server

☑ Use DHCP

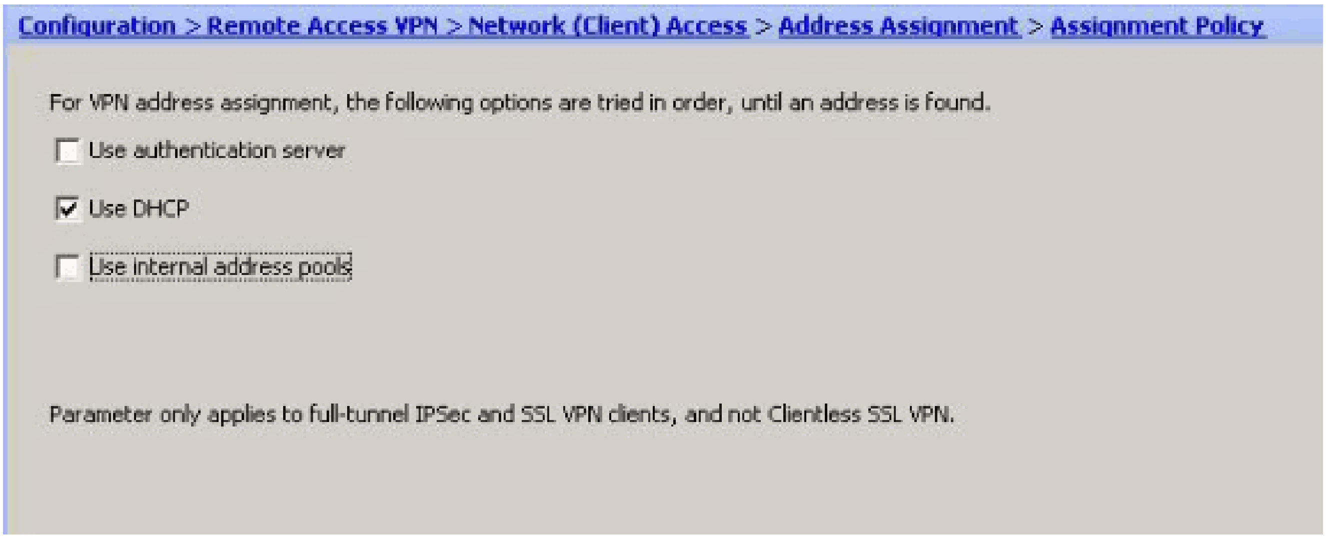
□ Use address pool

Interface-Specific Address Pools

Configuratie voor ASDM 6.x

De zelfde ASDM configuratie werkt prima met de ASDM versie 6.x, behalve voor sommige kleinere aanpassingen in termen van de ASDM paden. De ASDM-paden naar bepaalde velden hadden een afwijking van ASDM versie 6.2 en hoger. De aanpassingen samen met de bestaande paden worden hieronder weergegeven. Hier worden de grafische beelden niet toegevoegd in de gevallen waarin zij voor alle belangrijke ASDM-versies hetzelfde blijven.

1. Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE-beleid > Add
2. Configuratie > Remote Access VPN > Toegang voor netwerk (client) > Geavanceerd > IPSec > IPSec Transformatiesets > Add
3. Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add
4. Kies Configuration > Remote Access VPN > Network (Client) Access > Group Policy > Add > Intern Group Policy
5. Kies Configuration > Remote Access VPN > Network (Client) Access > Group Policy > Add >Intern Group Policy > Server
6. Kies Configuration > Remote Access VPN > AAA-instellingen/lokale gebruikers > Local Gebruikers > Add
7. Configuratie > Remote Access VPN > Toegang tot netwerk (client) > IPSec Connection-profielen > Add
8. Kies Configuration > Remote Access VPN > Network (Client) Access > Address Asmission Policy



Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy

For VPN address assignment, the following options are tried in order, until an address is found.

□ Use authentication server

☑ Use DHCP

□ Use internal address pools

Parameter only applies to full-tunnel IPSec and SSL VPN clients, and not Clientless SSL VPN.

Al deze drie opties zijn standaard ingeschakeld. Cisco ASA volgt de zelfde volgorde om adressen aan de VPN cliënten toe te wijzen. Wanneer u de andere twee opties niet controleert, verifieert Cisco ASA de server en de lokale pool opties niet. De standaard enabled opties kunnen worden geverifieerd door de **show run all | in vpn-add** opdracht. Dit is een voorbeelduitvoer voor uw referentie:

```
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local reuse-delay 0
```

Raadpleeg voor meer informatie over deze opdracht vpn-**addr-toewijzen**.

ASA/PIX configureren met CLI

Voltooi deze stappen om de DHCP-server te configureren om IP-adres aan de VPN-clients te geven vanuit de opdrachtregel. Raadpleeg Beelden voor externe toegang VPN's of Cisco ASA 5500 Series adaptieve security applicaties-commando-referenties voor meer informatie over elke opdracht die wordt gebruikt.

Config op het ASA-apparaat uitvoeren

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 no failover icmp unreachable rate-limit 1 burst-
size 1 !--- Specify the location of the ASDM image for
ASA to fetch the image for ASDM access. asdm image
disk0:/asdm-613.bin no asdm history enable arp timeout
14400 global (outside) 1 192.168.1.5 nat (inside) 0
```

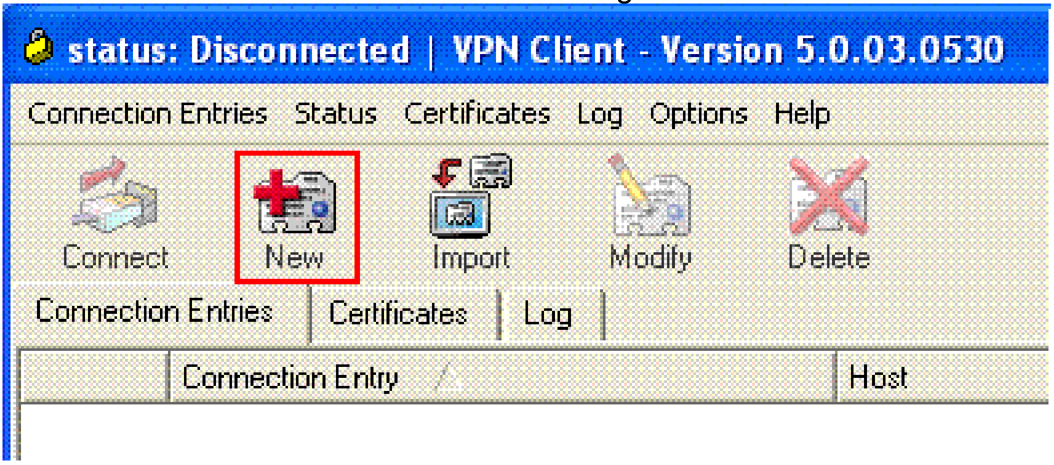
```
access-list 101 nat (inside) 1 0.0.0.0 0.0.0.0 route
outside 0.0.0.0 0.0.0.0 192.168.1.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart crypto
ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set
ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp
dynamic outside_dyn_map !--- Specifies the interface to
be used with !--- the settings defined in this
configuration. crypto map outside_map interface outside
!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policy 2. !--- The configuration commands
here define the Phase !--- 1 policy parameters that are
used. crypto isakmp enable outside crypto isakmp policy
2 authentication pre-share encryption des hash sha group
2 lifetime 86400 no crypto isakmp nat-traversal !---
Specifies that the IP address to the vpn clients are
assigned by the DHCP Server and now by AAA or the Local
pool.The CLI vpn-addr-assign dhcp for VPN address
assignment through DHCP Server is hidden in the CLI
provided by show run command.

no vpn-addr-assign aaa
no vpn-addr-assign local

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
!
```

```
group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes

!--- define the DHCP network scope in the group
policy.This configuration is Optional dhcp-network-scope
192.168.5.0

!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. username cisco123
password ffIRPGpDSOJh9YLq encrypted

!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access !--- Define the DHCP server address to the
tunnel group. tunnel-group TunnelGroup1 general-
attributes default-group-policy GroupPolicy1 dhcp-server
192.168.10.1

!--- Enter the pre-shared-key to configure the
authentication method. tunnel-group TunnelGroup1 ipsec-
attributes pre-shared-key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

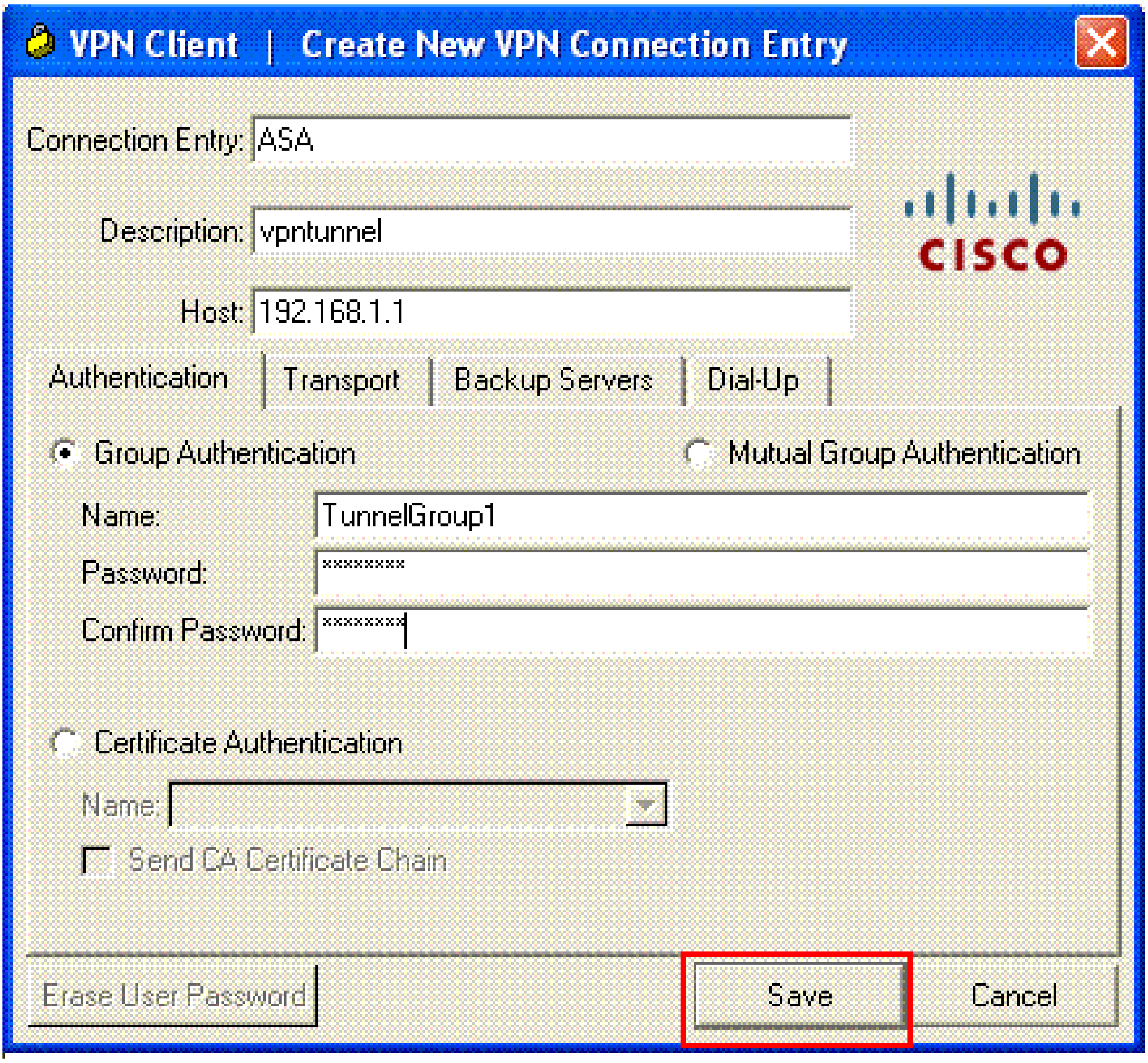
Cisco VPN-clientconfiguratie

Probeer met de Cisco ASA te verbinden aan het gebruik van de Cisco VPN-client om te controleren of de ASA met succes is geconfigureerd.

1. Selecteer **Start > Programma's > Cisco Systems VPN-client > VPN-client**.
2. Klik op **New** om het venster Nieuwe VPN-verbinding maken te starten.



3. Vul de gegevens in van uw nieuwe aansluiting.Voer de naam van de verbindingsbocht in samen met een beschrijving. Voer het **externe IP-adres van de ASA** in het hostvak in. Voer vervolgens de naam van de VPN-tunnelgroep (TunnelGroup1) en het wachtwoord in (Voorgedeelde sleutel - cisco123) zoals in ASA ingesteld. Klik op



VPN Client | Create New VPN Connection Entry

Connection Entry: ASA

Description: vpntunnel

Host: 192.168.1.1

Authentication | Transport | Backup Servers | Dial-Up

● Group Authentication ○ Mutual Group Authentication

Name: TunnelGroup1

Password: ********

Confirm Password: ********

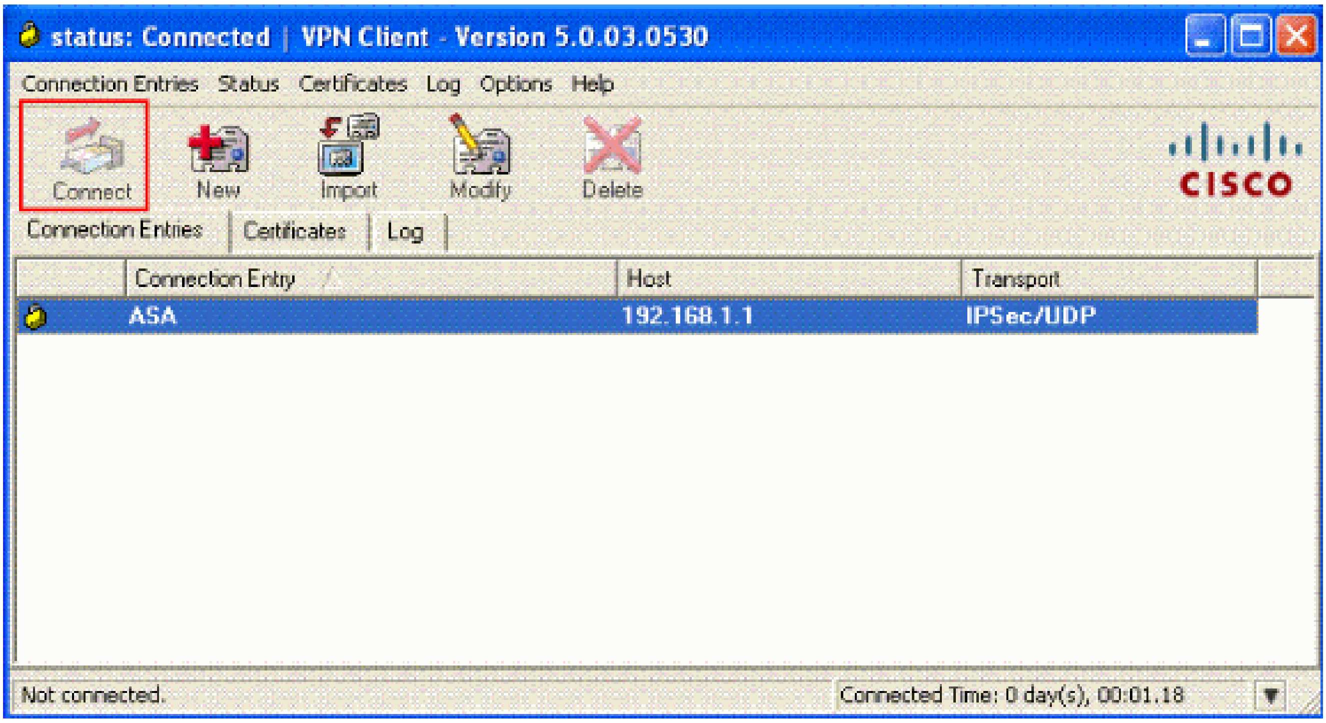
○ Certificate Authentication

Name:

□ Send CA Certificate Chain

Opslaan.

4. Klik op de verbinding die u wilt gebruiken en klik op **Connect** vanuit het hoofdvenster van VPN-
   client.



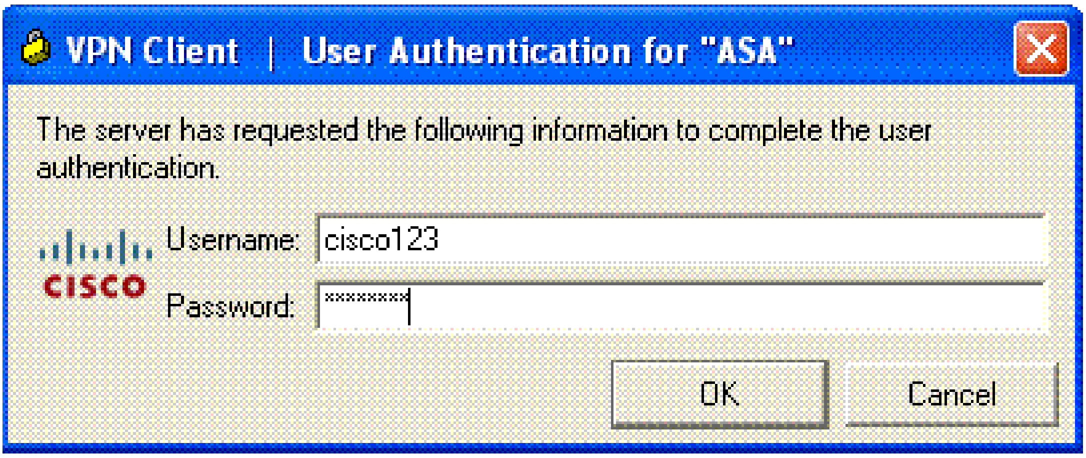
status: Connected | VPN Client - Version 5.0.03.0530

Connection Entry	Host	Transport
ASA	192.168.1.1	IPSec/UDP

Not connected. Connected Time: 0 day(s), 00:01.18

5. Voer desgevraagd de **gebruikersnaam** in **: Cisco123** en **Wachtwoord: cisco123** zoals in de ASA hierboven voor meer informatie ingesteld en klik op **OK** om verbinding te maken met het

externe netwerk.

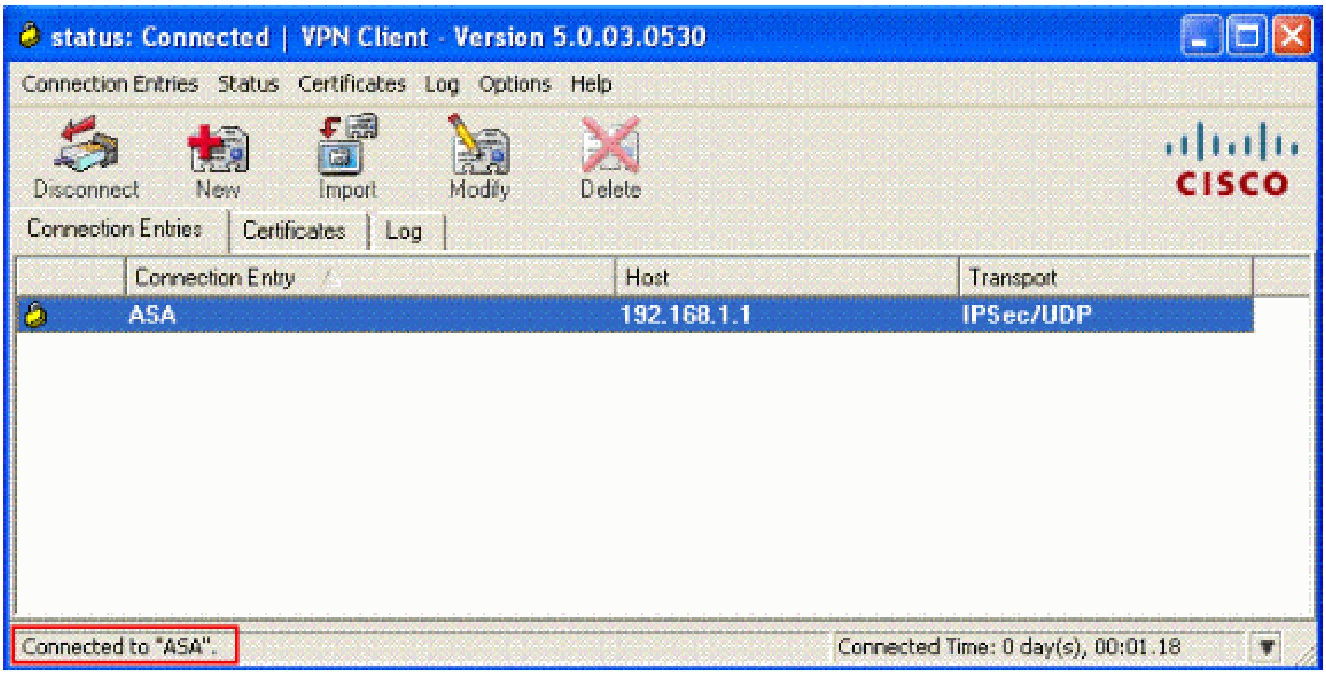

VPN Client | User Authentication for "ASA"

The server has requested the following information to complete the user authentication.

Username: cisco123

Password: ********

6. De VPN-client is verbonden met de ASA op de centrale site.

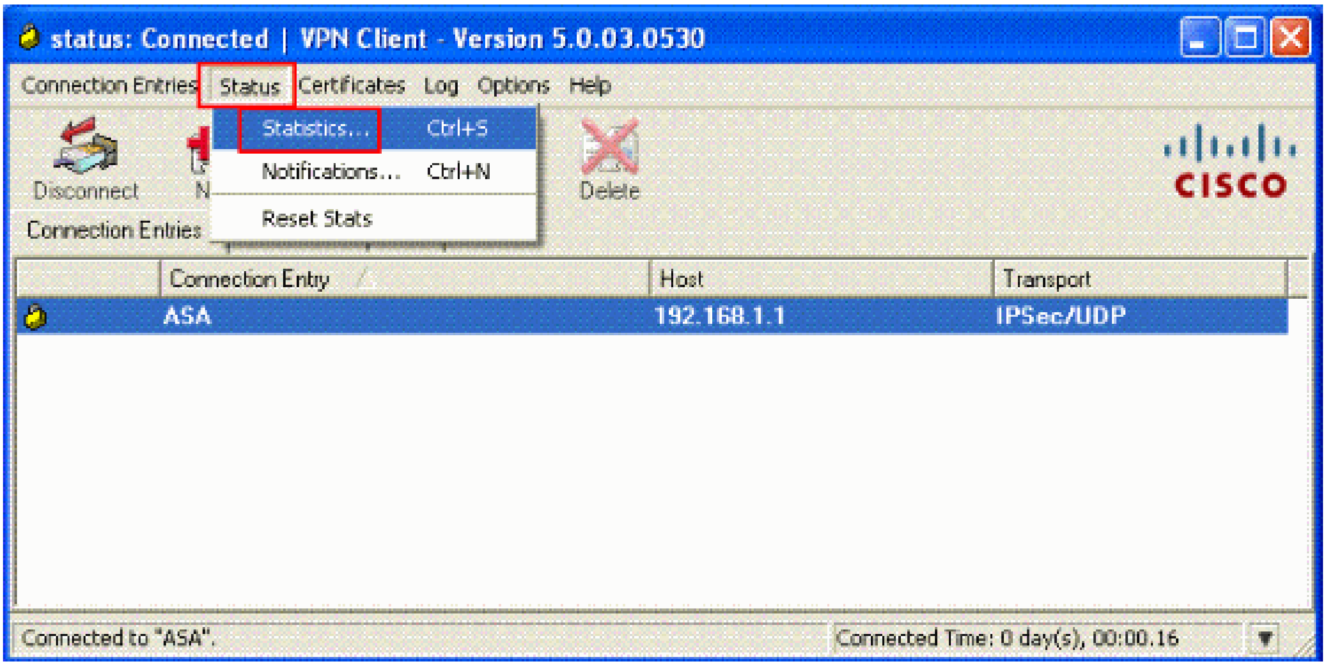

status: Connected | VPN Client - Version 5.0.03.0530

	Connection Entry	Host	Transport
	ASA	192.168.1.1	IPSec/UDP

Connected to "ASA".

Connected Time: 0 day(s), 00:01.18

7. Zodra de verbinding met succes is tot stand gebracht, selecteert u **Statistieken** in het menu Status om de details van de tunnel te controleren.


status: Connected | VPN Client - Version 5.0.03.0530

	Connection Entry	Host	Transport
	ASA	192.168.1.1	IPSec/UDP

Connected to "ASA".

Connected Time: 0 day(s), 00:00.16

Verifiëren

Opdrachten tonen

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

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

- **toon crypto isakmp sa**-toont alle huidige IKE Security Associations (SAs) bij een peer.
- **toon crypto ipsec sa**-Toont de instellingen die worden gebruikt door huidige SA's.

```
ASA #show crypto ipsec sa
interface: outside
    Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.1

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0)
      current_peer: 192.168.1.2, username: cisco123
      dynamic allocated peer ip: 192.168.5.1

      #pkts encaps: 55, #pkts encrypt: 55, #pkts digest: 55
      #pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.1.2

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: C2C25E2B

    inbound esp sas:
      spi: 0x69F8C639 (1777911353)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 40960, crypto-map: dynmap
         sa timing: remaining key lifetime (sec): 28337
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xC2C25E2B (3267517995)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 40960, crypto-map: dynmap
         sa timing: remaining key lifetime (sec): 28337
         IV size: 8 bytes
         replay detection support: Y

ASA #show crypto isakmp sa

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

1   IKE Peer: 192.168.1.2
```

```
    Type     : user              Role     : responder
    Rekey    : no                State    : AM_ACTIVE
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen. Ook wordt een voorbeelduitvoer van debug-uitvoer weergegeven.

Opmerking: Voor meer informatie over het oplossen van problemen bij externe toegang, IPsec, zie de meest gebruikelijke L2L- en Remote Access IPSec VPN-probleemoplossing

Beveiligingsassociaties wissen

Wanneer u een probleem oplossen, zorg er dan voor dat de bestaande beveiligingsassociaties worden gewist nadat u een wijziging hebt aangebracht. In de bevoorrechte modus van de PIX, gebruik deze opdrachten:

- **Schakel [crypto] ipsec sa**-Verwijdert de actieve IPsec SAs. Het sleutelwoord crypto is optioneel.
- **Schakel [crypto] isakmp sa**—Verwijdert de actieve IKE SA's. Het sleutelwoord crypto is optioneel.

Opdrachten voor probleemoplossing

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

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug crypto ipsec 7**-displays de IPsec onderhandelingen van fase 2.
- **debug crypto isakmp 7** — Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.

Monster debug-uitvoer

- ASA 8.0
- VPN-client 5.0 voor Windows

ASA 8.0

```
ASA#debug crypto isakmp 7
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message
 (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le
ngth : 856
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ISA_KE payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received xauth V6 VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Fragmentation VID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, IKE Peer included IKE fragmenta
tion capability flags:  Main Mode:        True  Aggressive Mode:  False
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received NAT-Traversal ver 02 V
ID
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity client VID
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group Tun
nelGroup1
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g IKE SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, IKE SA Pr
oposal # 1, Transform # 13 acceptable  Matches global IKE entry # 2
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ISAKMP SA payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ke payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing nonce payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Generatin
g keys for Responder...
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing ID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing
 hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing Cisco Unity VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing xauth V6 VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing dpd vid payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing Fragmentation VID + extended capabilities payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Alti
ga/Cisco VPN3000/Cisco ASA GW VID
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le
ngth : 368
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0)
 with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE
 (0) total length : 116
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing
 hash for ISAKMP
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g notify payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
g IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408)
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin
g VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Received
```

```
Cisco Unity client VID
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing blank hash payload
Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct
ing qm hash payload
Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a
1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=e8
a1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 84
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, process_a
ttr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin
g MODE_CFG Reply attributes.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: primary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: secondary DNS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: primary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: secondary WINS = cleared
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: IP Compression = disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKEGetUserAttributes: Browser Proxy Bypass Local = disable
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, User (cisco123) authenticated.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=143
60de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=14
360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, process_attr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Processing cfg ACK attributes
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=26
63a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, process_attr(): Enter!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Processing cfg Request attributes
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for IPV4 address!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for IPV4 net mask!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for DNS server address!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for WINS server address!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received unsupported transaction mode attribute: 5
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Banner!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Save PW setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
```

```
92.168.1.2, MODE_CFG: Received request for Default Domain Name!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Split Tunnel List!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Split DNS!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for PFS setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Client Browser Proxy Setting!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for backup ip-sec peer list!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received unknown transaction mode attribute: 28684
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for Application Version!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Client Type: WinNT  Client Application Version: 5.0.03.0530
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for FWTYPE!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for DHCP hostname for DDNS is: Wireless12
3!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, MODE_CFG: Received request for UDP Port!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth e
nabled)
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Assigned private IP address 192.168.5.1 to remote user
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Send Client Browser Proxy Attributes!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Browser Proxy set to No-Modify. Browser Proxy data will NOT be inclu
ded in the mode-cfg reply
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=266
3a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, PHASE 1 COMPLETED
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection:
DPD
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Starting P1 rekey timer: 950 seconds.
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, sending notify message
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f44
35669) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 84
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54
1f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
 NONE (0) total length : 1022
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
```

```
92.168.1.2, processing SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing ID payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received remote Proxy Host data in ID Payload:  Address 192.168.5.1, Proto
col 0, Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing ID payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Received local IP Proxy Subnet data in ID Payload:   Address 0.0.0.0, Mask
 0.0.0.0, Protocol 0, Port 0
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, QM IsRekeyed old sa not found by addr
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, IKE Remote Peer configured for crypto map: dynmap
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing IPSec SA payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IPSec SA Proposal # 14, Transform # 1 acceptable  Matches global IPS
ec SA entry # 10
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, IKE: requesting SPI!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, oakley constucting quick mode
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing blank hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing IPSec SA payload
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 secon
ds
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing IPSec nonce payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing proxy ID
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Transmitting Proxy Id:
  Remote host: 192.168.5.1  Protocol 0  Port 0
  Local subnet:  0.0.0.0  mask 0.0.0.0 Protocol 0  Port 0
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Sending RESPONDER LIFETIME notification to Initiator
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, constructing qm hash payload
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=541
f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NOTIFY (11) + NONE (0) total length : 176
Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54
1f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, processing hash payload
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, loading all IPSEC SAs
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Generating Quick Mode Key!
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Generating Quick Mode Key!
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Security negotiation complete for User (cisco123)  Responder, Inbound SPI
= 0x31de01d8, Outbound SPI = 0x8b7597a9
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
```

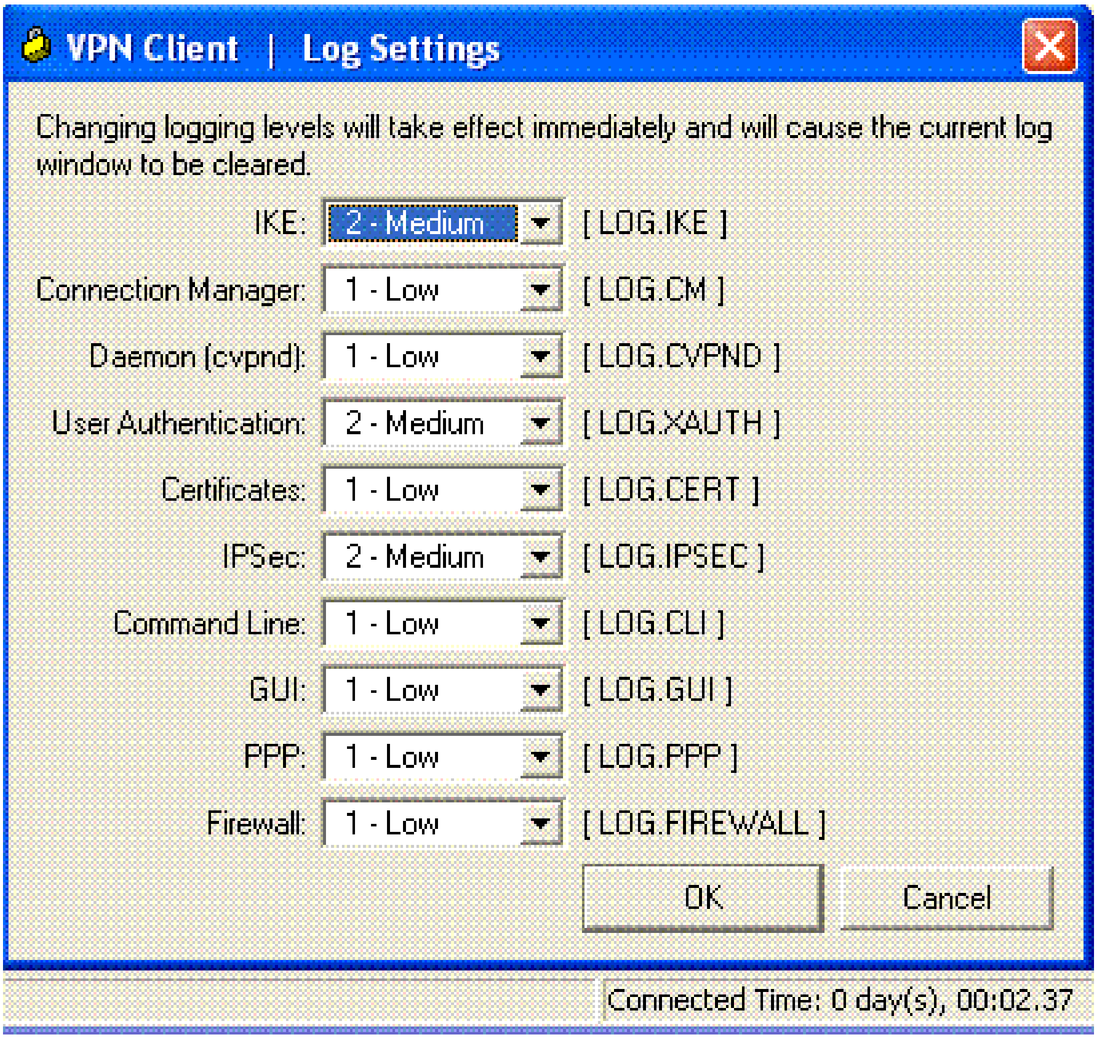
```
92.168.1.2, IKE got a KEY_ADD msg for SA: SPI = 0x8b7597a9
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Pitcher: received KEY_UPDATE, spi 0x31de01d8
Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1
92.168.1.2, Starting P2 rekey timer: 27360 seconds.
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, Adding static route for client address: 192.168.5.1
Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168
.1.2, PHASE 2 COMPLETED (msgid=541f8e43)
Jan 22 22:21:41 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=78
f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 8
0
```

```
ASA#debug crypto ipsec 7
```

```
!--- Deletes the old SAs. ASA# IPSEC: Deleted inbound decrypt rule, SPI 0x7F3C985A Rule ID:
0xD5567DB0 IPSEC: Deleted inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 IPSEC: Deleted
inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: Deleted inbound VPN context,
SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Deleted outbound encrypt rule, SPI 0xC921E280 Rule
ID: 0xD517EE30 IPSEC: Deleted outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC:
Deleted outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 !--- Creates new SAs. ASA#
IPSEC: New embryonic SA created @ 0xD4EF2390, SCB: 0xD4EF22C0, Direction: inbound SPI :
0x7F3C985A Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime
: 240 seconds IPSEC: New embryonic SA created @ 0xD556B118, SCB: 0xD556B048, Direction: outbound
SPI : 0xC921E280 Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp
Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0xC921E280 IPSEC: Creating
outbound VPN context, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU :
1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC:
Completed outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: New outbound
encrypt rule, SPI 0xC921E280 Src addr: 0.0.0.0 Src mask: 0.0.0.0 Dst addr: 192.168.5.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore
Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound encrypt
rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: New outbound permit rule, SPI 0xC921E280 Src
addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.1.2 Dst mask: 255.255.255.255 Src
ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0xC921E280 Use SPI: true IPSEC: Completed outbound permit rule, SPI
0xC921E280 Rule ID: 0xD5123250 IPSEC: Completed host IBSA update, SPI 0x7F3C985A IPSEC: Creating
inbound VPN context, SPI 0x7F3C985A Flags: 0x00000006 SA : 0xD4EF2390 SPI : 0x7F3C985A MTU : 0
bytes VCID : 0x00000000 Peer : 0x00040AB4 SCB : 0x0132B2C3 Channel: 0xD4160FA8 IPSEC: Completed
inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Updating outbound VPN context
0x00040AB4, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes
VCID : 0x00000000 Peer : 0x0004678C SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed
outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: Completed outbound inner
rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Completed outbound outer SPD rule, SPI
0xC921E280 Rule ID: 0xD5123250 IPSEC: New inbound tunnel flow rule, SPI 0x7F3C985A Src addr:
192.168.5.1 Src mask: 255.255.255.255 Dst addr: 0.0.0.0 Dst mask: 0.0.0.0 Src ports Upper: 0
Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false
SPI: 0x00000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x7F3C985A Rule
ID: 0xD556AF60 IPSEC: New inbound decrypt rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask:
255.255.255.255 Dst addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op :
ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A
Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC:
New inbound permit rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst
addr: 192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports
Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0
```

VPN-client 5.0 voor Windows

Selecteer **Log > Instellingen** loggen om de logniveaus in de VPN-client in te schakelen.

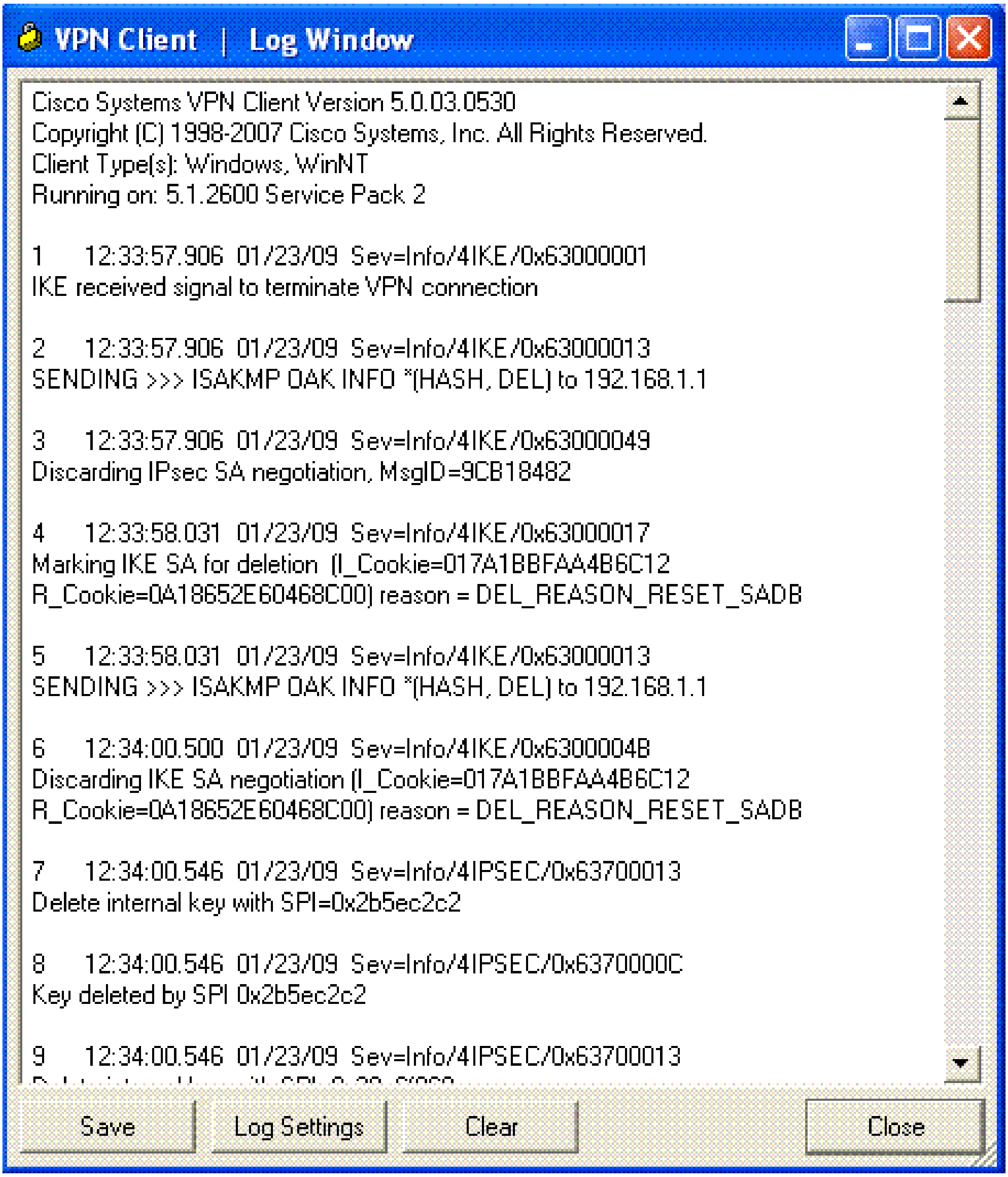


Changing logging levels will take effect immediately and will cause the current log window to be cleared.

IKE:	2 - Medium	[LOG.IKE]
Connection Manager:	1 - Low	[LOG.CM]
Daemon (cvpnd):	1 - Low	[LOG.CVPND]
User Authentication:	2 - Medium	[LOG.XAUTH]
Certificates:	1 - Low	[LOG.CERT]
IPSec:	2 - Medium	[LOG.IPSEC]
Command Line:	1 - Low	[LOG.CLI]
GUI:	1 - Low	[LOG.GUI]
PPP:	1 - Low	[LOG.PPP]
Firewall:	1 - Low	[LOG.FIREWALL]

Connected Time: 0 day(s), 00:02.37

Selecteer **Log > venster in** om de logitems in de VPN-client te bekijken.



```
Cisco Systems VPN Client Version 5.0.03.0530
Copyright (C) 1998-2007 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      12:33:57.906  01/23/09  Sev=Info/4IKE/0x63000001
IKE received signal to terminate VPN connection

2      12:33:57.906  01/23/09  Sev=Info/4IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 192.168.1.1

3      12:33:57.906  01/23/09  Sev=Info/4IKE/0x63000049
Discarding IPsec SA negotiation, MsgID=9CB18482

4      12:33:58.031  01/23/09  Sev=Info/4IKE/0x63000017
Marking IKE SA for deletion  (I_Cookie=017A1BBFAA4B6C12
R_Cookie=0A18652E60468C00) reason = DEL_REASON_RESET_SADB

5      12:33:58.031  01/23/09  Sev=Info/4IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 192.168.1.1

6      12:34:00.500  01/23/09  Sev=Info/4IKE/0x6300004B
Discarding IKE SA negotiation (I_Cookie=017A1BBFAA4B6C12
R_Cookie=0A18652E60468C00) reason = DEL_REASON_RESET_SADB

7      12:34:00.546  01/23/09  Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2b5ec2c2

8      12:34:00.546  01/23/09  Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2b5ec2c2

9      12:34:00.546  01/23/09  Sev=Info/4IPSEC/0x63700013
```

Gerelateerde informatie

- Cisco ASA 5500 Series ondersteuningspagina voor adaptieve security applicaties
- Cisco ASA 5500 Series Opdrachten voor adaptieve security applicaties
- Ondersteuning van Cisco PIX 500 Series security applicaties
- Cisco PIX 500 Series security applicaties, opdracht
- Cisco adaptieve security apparaatbeheer
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen