

IPsec-tunnelheid tussen IOS-router en Cisco VPN-client 4.x voor Windows met Configuratievoorbeeld van TACACS+ gebruikersverificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor troubleshooting](#)

[Routerkaarten](#)

[Clientvastlegging](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document beschrijft hoe u een IPsec-verbinding kunt configureren tussen een router en de Cisco Virtual Private Network (VPN) Client 4.x met Terminal Access Control System Plus (TACACS+) voor gebruikersverificatie. Cisco IOS-software release 12.2(8)T en releases later ondersteuningsverbindingen van Cisco VPN-client 4.x. VPN Client 4.x gebruikt Diffie-Hellman (D-H) groepsbeleid 2. De opdracht **isakmp beleid # groep 2** stelt de 4.x klanten in staat om aan te sluiten.

Dit document toont verificatie op de TACACS+ server met toestemming, zoals Windows Internet Naming Service (WINS) en DNS-opdrachten (Domain Naming Service), die lokaal door de router worden uitgevoerd.

Raadpleeg [Cisco VPN-client 3.x configureren voor Windows om lokale uitgebreide verificatie te gebruiken](#) om meer te weten te komen over het scenario waarin de gebruikersverificatie lokaal plaatsvindt in de Cisco IOS-router.

Raadpleeg [IPSec configureren tussen een Cisco IOS-router en een Cisco VPN-client 4.x voor Windows Gebruikend RADIUS voor gebruikersverificatie](#) om meer te weten te komen over het scenario waarin de gebruikersverificatie extern met RADIUS-protocol plaatsvindt.

Voorwaarden

Vereisten

Zorg er voordat u deze configuratie probeert voor dat u aan deze vereisten voldoet:

- Een pool van adressen die moet worden toegewezen voor IPsec
- Een groep met de naam "Vpngroup" met een wachtwoord voor "cisco123"
- Verificatie door gebruiker op een TACACS+ server

Gebruikte componenten

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

- Cisco VPN-client voor Windows versie 4.0.2D (een VPN-client 3.x of hoger moet werken)
- Cisco Secure voor Windows versie 3.0 (elke TACACS+ server moet werken)
- Cisco IOS 1710 routerversie 12.2(8)T1 geladen met de IPsec-functieset Uitvoer uit de opdracht **Versie** van het programma op de router wordt hier weergegeven.

```
1710#show version
```

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1710-K9O3SY-M),
  Version 12.2(8)T1, RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 30-Mar-02 13:30 by ccai
Image text-base: 0x80008108, data-base: 0x80C1E054
```

```
ROM: System Bootstrap, Version 12.2(1r)XE1, RELEASE SOFTWARE (fc1)
```

```
1710 uptime is 1 week, 6 days, 22 hours, 30 minutes
System returned to ROM by reload
System image file is "flash:c1710-k9o3sy-mz.122-8.T1"
```

```
cisco 1710 (MPC855T) processor (revision 0x200)
  with 27853K/4915K bytes of memory.
Processor board ID JAD052706CX (3234866109), with hardware revision 0000
MPC855T processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 Virtual Private Network (VPN) Module(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
```

```
Configuration register is 0x2102
```

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 Convention](#) voor informatie over documentconventies.

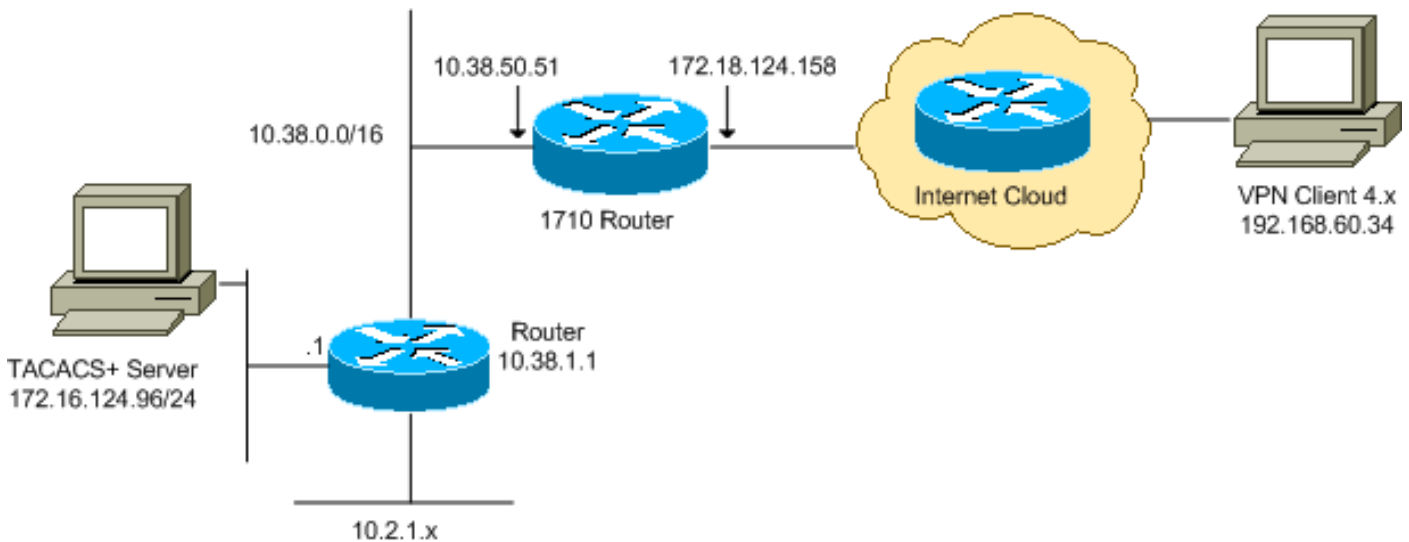
Configureren

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

N.B.: Gebruik het [Opdrachtuppgereedschap](#) ([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:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn [RFC 1918](#) adressen die in een labomgeving gebruikt zijn.

Configuraties

Dit document gebruikt deze configuraties:

- [Cisco 1710 router](#)
- [TACACS+ server](#)
- [VPN-client 4.x](#)
- [Split-tunneling](#)

Cisco 1710 router

Cisco 1710 router

```
1710#show run
Building configuration...

Current configuration : 1884 bytes
!
version 12.2
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname 1710
!
!--- Enable authentication, authorization and accounting
(AAA) !--- for user authentication and group
authorization. aaa new-model
!
!--- In order to enable extended authentication (Xauth)
for user authentication, !--- enable the aaa
authentication commands. !--- The group TACACS+ command
specifies TACACS+ user authentication.

aaa authentication login userauthen group tacacs+
!--- In order to enable group authorization, !--- enable
the aaa authorization commands.

aaa authorization network groupauthor local
!
!
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!--- Create an Internet Security Association and !---
Key Management Protocol (ISAKMP) policy for Phase 1
negotiations. crypto isakmp policy 3
encr 3des
authentication pre-share
group 2
!
!--- Create a group in order to specify the !--- WINS
and DNS server addresses to the VPN Client, !--- along
with the pre-shared key for authentication. crypto
isakmp client configuration group vpngroup
key cisco123
dns 10.2.1.10
wins 10.2.1.20
domain cisco.com
pool ippool
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-sha-hmac
!
!--- Create a dynamic map, and !--- apply the transform
set that was previously created. crypto dynamic-map
dynmap 10
set transform-set myset
!
!--- Create the actual crypto map, !--- and apply the
AAA lists that were created earlier. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap client configuration address
respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
```

```

!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!
!--- Apply the crypto map on the outside interface.
interface FastEthernet0
ip address 172.18.124.158 255.255.255.0
crypto map clientmap
!
interface Ethernet0
ip address 10.38.50.51 255.255.0.0
!

!--- Create a pool of addresses to be assigned to the
VPN Clients. ip local pool ippool 10.1.1.100 10.1.1.200
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip route 172.16.124.0 255.255.255.0 10.38.1.1
ip route 10.2.1.0 255.255.255.0 10.38.1.1
ip http server
ip pim bidir-enable
!
!
!
!--- Specify the IP address of the TACACS+ server, !---
along with the TACACS+ shared secret key. tacacs-server
host 172.16.124.96 key cisco123
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
!
!
end

```

[TACACS+ server](#)

Voltooi de volgende stappen om de TACACS+ server te configureren:

1. Klik op **Ingang toevoegen** om een ingang voor de router in de TACACS+ serverdatabase toe te voegen.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
340	172.18.124.151	RADIUS (Cisco Aironet)
Aironet-340-Lab	10.36.1.99	RADIUS (Cisco Aironet)
others	<Default>	TACACS+ (Cisco IOS)

[Add Entry](#)

2. Ga in op de pagina AAA-client toevoegen de routerinformatie in zoals in deze

afbeelding:

Add AAA Client

AAA Client Hostname: 1710Router

AAA Client IP Address: 10.38.50.51

Key: cisco123

Authenticate Using: TACACS+ (Cisco IOS)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Submit Submit + Restart Cancel

Typ in het veld AAA-clientnaam een naam voor de router. Typ **10.38.50.51** in het veld AAA client-IP-adres. Voer in het veld Key **cisco123** in als gedeelde geheime sleutel. Selecteer in de vervolgkeuzelijst Verifiëren met behulp van **TACACS+ (Cisco IOS)** en klik op **Inzenden**.

3. Typ in het veld Gebruiker de gebruikersnaam voor de VPN-gebruiker in de Cisco Secure-database en klik op **Toevoegen/bewerken**. In dit voorbeeld is de gebruikersnaam *cisco*.

User: cisco

Find Add/Edit

List users beginning with letter/number:

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

List All Users

Get to Help

- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

User Setup enables you to configure individual user information, add users, and delete users in the database.

4. Voer in de volgende pagina het wachtwoord voor *Cisco-gebruikersinterface* in en bevestig. In dit voorbeeld is het wachtwoord ook *cisco*.

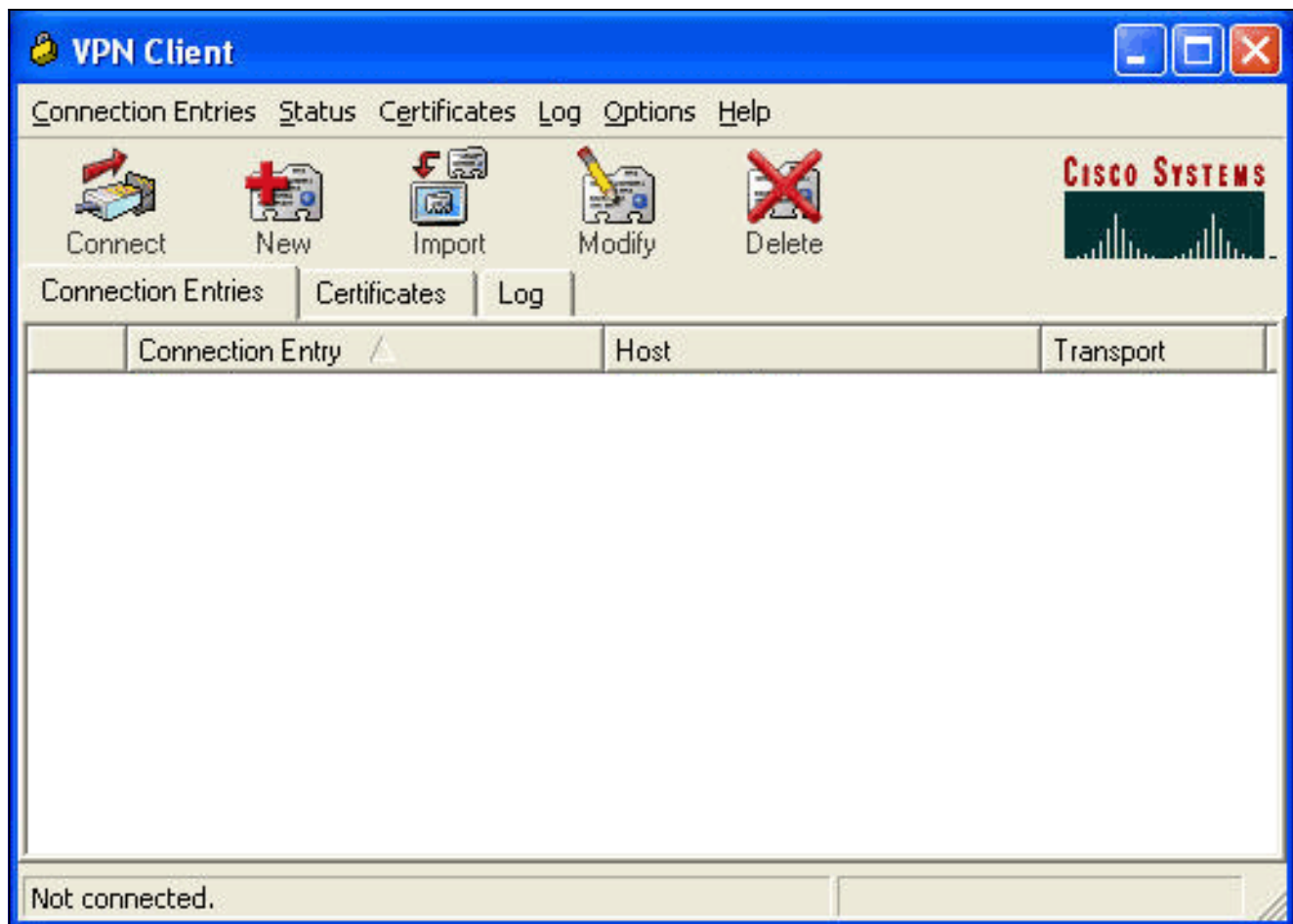
The screenshot shows a web-based configuration interface. On the left is a vertical navigation menu with icons for User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administrative Control, External User Database, Reports and Activity, and Online Documentation. The main content area is divided into two sections: 'Supplementary User Info' and 'User Setup'. The 'Supplementary User Info' section has input fields for 'Real Name' and 'Description'. The 'User Setup' section is titled 'Password Authentication:' and includes a dropdown menu set to 'CiscoSecure Database'. Below this, it says 'CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)'. There are two sets of 'Password' and 'Confirm Password' fields. The first set is for the main authentication, and the second set is preceded by a checkbox labeled 'Separate (CHAP/MS-CHAP/ARAP)'. Below the fields is a text block explaining that a separate CHAP password is useful for token card authentication. At the bottom of the 'User Setup' section is a dropdown menu for 'Group to which the user is assigned', currently showing 'Group 19'. 'Submit' and 'Cancel' buttons are at the bottom. To the right of the main content is a list of blue links: Account Disabled, Deleting a Username, Supplementary User Info, Password Authentication, Group to which the user is assigned, Callback, Client IP Address Assignment, Advanced Settings, Network Access Restrictions, Max Sessions, Usage Quotas, Account Disable, Downloadable ACLs, Advanced TACACS+ Settings, TACACS+ Enable Control, TACACS+ Enable Password, TACACS+ Outbound Password, TACACS+ Shell Command Authorization, TACACS+ Unknown Services, IETF RADIUS Attributes, and RADIUS Vendor-Specific Attributes. Below this list is a section titled 'Account Disabled Status' with a paragraph explaining the checkbox and a '[Back to Top]' link.

5. Als u de gebruikersaccount aan een groep wilt toewijzen, moet u deze stap nu uitvoeren. Klik op **Inzenden** als u klaar bent.

[VPN-client 4.x](#)

Voltooi de volgende stappen om VPN-client 4.x te configureren:

1. Start de VPN-client en klik op **Nieuw** om een nieuwe verbinding te maken.



Het dialoogvenster VPN-client voor Nieuwe VPN-verbinding maken

VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name:

Password:

Confirm Password:

Certificate Authentication

Name:

Send CA Certificate Chain

Erase User Password | Save | Cancel

verschijnt.

2. Typ in het dialoogvenster Nieuwe VPN-verbinding maken informatie over de verbinding zoals in deze afbeelding:

VPN Client | Create New VPN Connection Entry

Connection Entry:

Description:

Host:

Authentication |
 Transport |
 Backup Servers |
 Dial-Up

Group Authentication
 Mutual Group Authentication

Name:

Password:

Confirm Password:

Certificate Authentication

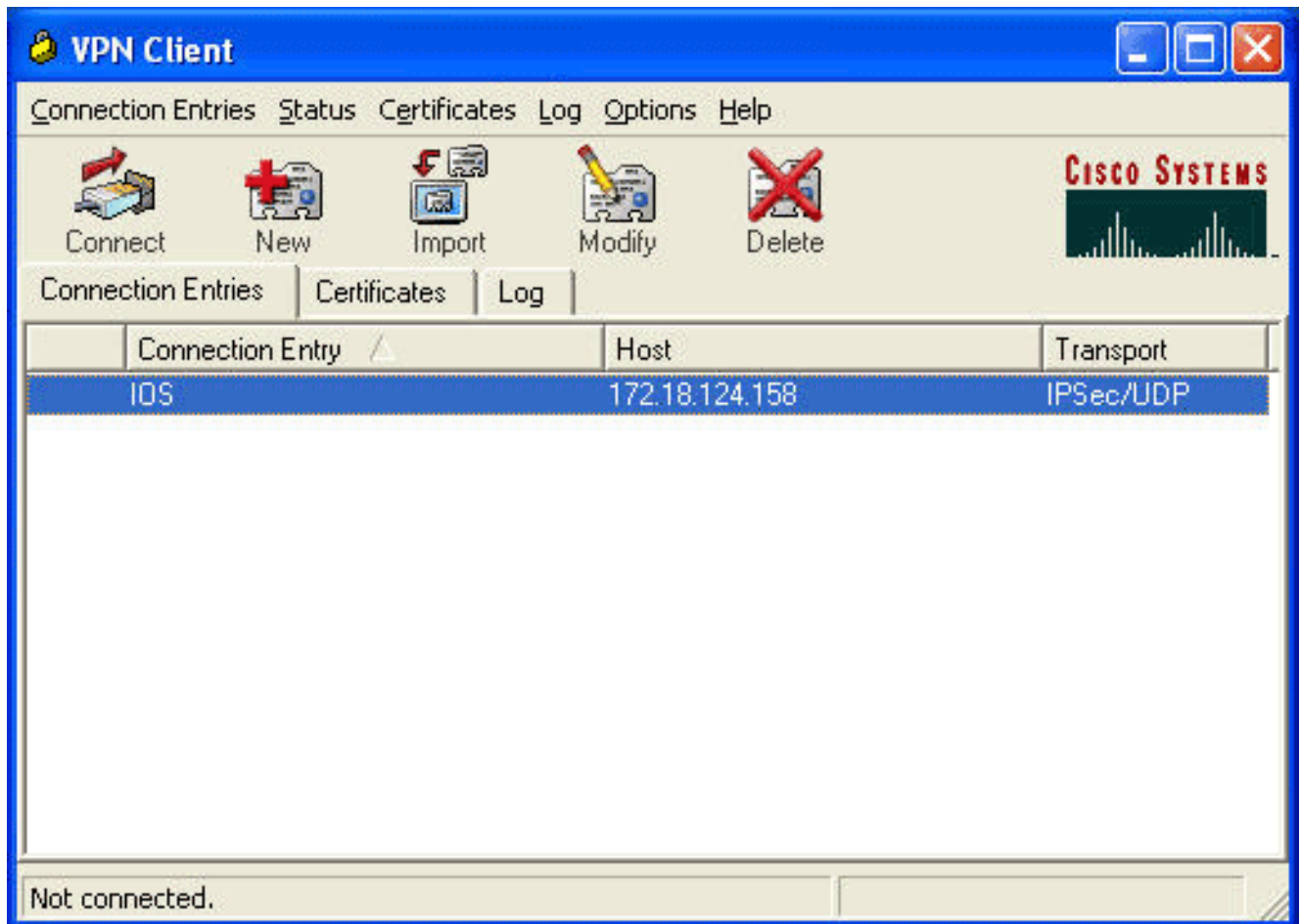
Name:

Send CA Certificate Chain

Voer in het veld Toegang tot verbinding een naam in voor de verbinding. Typ in de velden Description en Host een beschrijving en het IP-adres van de host voor de verbinding. Klik in het tabblad

Verificatie op de radioknop **groepsverificatie** en voer de naam en het wachtwoord van de gebruiker in. Klik op **Opslaan** om de verbinding op te slaan.

3. Selecteer in het venster VPN-client de verbindingssingang die u hebt gemaakt en klik op **Connect** om verbinding te maken met de router.



4. Aangezien IPsec onderhandelt, wordt u gevraagd om een gebruikersnaam en een wachtwoord. Voer een naam en wachtwoord in. Het venster toont deze berichten: "Onderhandelingen over beveiligingsprofielen." "Je link is nu veilig."

Split-tunneling

Om een gesplitste tunneling voor de VPN-verbindingen mogelijk te maken, moet u een toegangscontrolelijst (ACL) op de router configureren. In dit voorbeeld wordt de opdracht **toegangslijst 102** geassocieerd met de groep voor het splitsen van tunneling, en de tunnel gevormd naar de 10.38.X.X /16 en 10.2.x.x netwerken. Verkeersstromen niet versleuteld met apparaten die niet in ACL 102 (bijvoorbeeld het internet) zijn geplaatst.

```
access-list 102 permit ip 10.38.0.0 0.0.255.255 10.1.1.0 0.0.0.255
access-list 102 permit ip 10.2.0.0 0.0.255.255 10.1.1.0 0.0.0.255
```

Pas ACL op de groepeigenschappen toe.

```
crypto isakmp client configuration group vpngroup
key cisco123
dns 10.2.1.10
wins 10.2.1.20
domain cisco.com
pool ippool
acl 102
```

Verifiëren

Deze sectie bevat informatie over de manier waarop u kunt controleren of de configuratie goed werkt.

Bepaalde opdrachten **worden** ondersteund door de [uitvoertolk](#) (alleen [geregistreerde](#) klanten). Met dit gereedschap kunt u een analyse van de opdrachtoutput **weergeven**.

```
1710#show crypto isakmp sa
dst          src          state          conn-id    slot
172.18.124.158 192.168.60.34 QM_IDLE          3          0

1710#show crypto ipsec sa

interface: FastEthernet0
Crypto map tag: clientmap, local addr. 172.18.124.158

local ident (addr/mask/prot/port): (172.18.124.158/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.1.1.114/255.255.255.255/0/0)
current_peer: 192.168.60.34
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.18.124.158, remote crypto endpt.: 192.168.60.34
path mtu 1500, media mtu 1500
current outbound spi: 8F9BB05F

inbound esp sas:
spi: 0x61C53A64(1640315492)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 200, flow_id: 1, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3294)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8F9BB05F(2409345119)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4608000/3294)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (10.38.0.0/255.255.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.1.1.114/255.255.255.255/0/0)
current_peer: 192.168.60.34
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 decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.18.124.158, remote crypto endpt.: 192.168.60.34
path mtu 1500, media mtu 1500
current outbound spi: 8B57E45E
```

```
inbound esp sas:
spi: 0x89898D1A(2307493146)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 202, flow_id: 3, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/3452)
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
spi: 0x8B57E45E(2337793118)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 203, flow_id: 4, crypto map: clientmap
sa timing: remaining key lifetime (k/sec): (4607999/3452)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

```
1710#show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
2	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	0	0
200	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	0	0
201	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	0	0
202	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	0	3
203	FastEthernet0	172.18.124.158	set	HMAC_SHA+3DES_56_C	3	0

[Problemen oplossen](#)

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

[Opdrachten voor troubleshooting](#)

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

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

opdrachten gebruikt.

- **debug van crypto ipsec**—displays debug informatie over IPsec-verbindingen.
- **debug crypto isakmp**—displays debug informatie over IPsec verbindingen en toont de eerste reeks eigenschappen die worden ontkend als gevolg van onverenigbaarheden op beide eindpunten.
- **debug van crypto motor**—informatie van de crypto motor.
- **debug van verificatie**—informatie over AAA/TACACS+-verificatie wordt weergegeven.
- **debug van autorisatie**—informatie over AAA/TACACS+ autorisatie wordt weergegeven.
- **bug van tacacs**—displays die u in staat stellen om de communicatie tussen de TACACS+ server en de router te problemen oplossen.

Routerkaarten

```
1710#show debug
```

```
General OS:
```

```
TACACS access control debugging is on
```

```
AAA Authentication debugging is on
```

```
AAA Authorization debugging is on
```

```
Cryptographic Subsystem:
```

```
Crypto ISAKMP debugging is on
```

```
Crypto Engine debugging is on
```

```
Crypto IPSEC debugging is on
```

```
1710#
```

```
1w6d: ISAKMP (0:0): received packet from 192.168.60.34 (N) NEW SA
```

```
1w6d: ISAKMP: local port 500, remote port 500
```

```
1w6d: ISAKMP (0:2): (Re)Setting client xauth list userauthen and state
```

```
1w6d: ISAKMP: Locking CONFIG struct 0x8158B894 from
```

```
crypto_ikmp_config_initialize_sa, count 2
```

```
1w6d: ISAKMP (0:2): processing SA payload. message ID = 0
```

```
1w6d: ISAKMP (0:2): processing ID payload. message ID = 0
```

```
1w6d: ISAKMP (0:2): processing vendor id payload
```

```
1w6d: ISAKMP (0:2): vendor ID seems Unity/DPD but bad major
```

```
1w6d: ISAKMP (0:2): vendor ID is XAUTH
```

```
1w6d: ISAKMP (0:2): processing vendor id payload
```

```
1w6d: ISAKMP (0:2): vendor ID is DPD
```

```
1w6d: ISAKMP (0:2): processing vendor id payload
```

```
1w6d: ISAKMP (0:2): vendor ID is Unity
```

```
1w6d: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 3 policy
```

```
1w6d: ISAKMP: encryption 3DES-CBC
```

```
1w6d: ISAKMP: hash SHA
```

```
1w6d: ISAKMP: default group 2
```

```
1w6d: ISAKMP: auth XAUTHInitPreShared
```

```
1w6d: ISAKMP: life type in seconds
```

```
1w6d: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
```

```
1w6d: ISAKMP (0:2): atts are acceptable. Next payload is 3
```

```
1w6d: CryptoEngine0: generate alg parameter
```

```
1w6d: CryptoEngine0: CRYPTO_ISA_DH_CREATE(hw) (ipsec)
```

```
1w6d: CRYPTO_ENGINE: Dh phase 1 status: 0
```

```
1w6d: ISAKMP (0:2): processing KE payload. message ID = 0
```

```
1w6d: CryptoEngine0: generate alg parameter
```

```
1w6d: CryptoEngine0: CRYPTO_ISA_DH_SHARE_SECRET(hw) (ipsec)
```

```
1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 0
```

```
1w6d: ISAKMP (0:2): processing vendor id payload
```

```
1w6d: ISAKMP (0:2): processing vendor id payload
```

```
1w6d: ISAKMP (0:2): processing vendor id payload
```

```
1w6d: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x817F63F4) user='vpngroup' ruser='NULL' ds0=0
    port='ISAKMP-ID-AUTH' rem_addr='192.168.60.34' authen_type=NONE
    service=LOGIN priv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894):
    Port='ISAKMP-ID-AUTH' list='groupauthor' service=NET
1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(1472763894) user='vpngroup'
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV service=ike
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): send AV protocol=ipsec
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): found list "groupauthor"
1w6d: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(1472763894): Method=LOCAL
1w6d: AAA/AUTHOR (1472763894): Post authorization status = PASS_ADD
1w6d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV service=ike
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV timeout*0
AAA/AUTHOR/IKE: Processing AV idletime*0
AAA/AUTHOR/IKE: Processing AV inacl*102
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
1w6d: CryptoEngine0: create ISAKMP SKEYID for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_SA_CREATE(hw) (ipsec)
1w6d: ISAKMP (0:2): SKEYID state generated
1w6d: ISAKMP (0:2): SA is doing pre-shared key authentication plux
    XAUTH using id type ID_IPV4_ADDR
1w6d: ISAKMP (2): ID payload
next-payload : 10
type : 1
protocol : 17
port : 500
length : 8
1w6d: ISAKMP (2): Total payload length: 12
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw) (ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) AG_INIT_EXCH
1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY
Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

1w6d: AAA/MEMORY: free_user (0x817F63F4) user='vpngroup'
    ruser='NULL' port='ISAK MP-ID-AUTH' rem_addr='192.168.60.34'
    authen_type=NONE service=LOGIN priv=0
1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) AG_INIT_EXCH
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw) (ipsec)
1w6d: ISAKMP (0:2): processing HASH payload. message ID = 0
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw) (ipsec)
1w6d: ISAKMP (0:2): processing NOTIFY INITIAL_CONTACT protocol 1
    spi 0, message ID = 0, sa = 81673884
1w6d: ISAKMP (0:2): Process initial contact, bring down
    existing phase 1 and 2 SA's
1w6d: ISAKMP (0:2): returning IP addr to the address pool: 10.1.1.113
1w6d: ISAKMP (0:2): returning address 10.1.1.113 to pool
1w6d: ISAKMP (0:2): peer does not do paranoid keepalives.

1w6d: ISAKMP (0:2): SA has been authenticated with 192.168.60.34
1w6d: CryptoEngine0: clear dh number for conn id 1
1w6d: CryptoEngine0: CRYPTO_ISA_DH_DELETE(hw) (ipsec)
```

1w6d: IPSEC(key_engine): got a queue event...
1w6d: IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
1w6d: IPSEC(key_engine_delete_sas): delete all SAs shared with 192.168.60.34
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
1w6d: ISAKMP (0:2): purging node 1324880791
1w6d: ISAKMP: Sending phase 1 responder lifetime 86400

1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

1w6d: ISAKMP (0:2): Need XAUTH
1w6d: AAA: parse name=ISAKMP idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x812F79FC) user='NULL'
ruser='NULL' ds0=0 port='
ISAKMP' rem_addr='192.168.60.34' authn_type=ASCII service=LOGIN
priv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

1w6d: AAA/AUTHEN/START (2017610393): port='ISAKMP' list='userauthen'
action=LOGIN service=LOGIN
1w6d: AAA/AUTHEN/START (2017610393): found list userauthen
1w6d: AAA/AUTHEN/START (2017610393): Method=tacacs+ (tacacs+)
1w6d: TAC+: send AUTHEN/START packet ver=192 id=2017610393
1w6d: TAC+: Using default tacacs server-group "tacacs+" list.
1w6d: TAC+: Opening TCP/IP to 172.16.124.96/49 timeout=5
1w6d: TAC+: Opened TCP/IP handle 0x8183D638 to 172.16.124.96/49
1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/START/LOGIN/ASCII queued
1w6d: TAC+: (2017610393) AUTHEN/START/LOGIN/ASCII processed
1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETUSER
1w6d: AAA/AUTHEN(2017610393): Status=GETUSER
1w6d: ISAKMP: got callback 1
1w6d: ISAKMP/xauth: request attribute XAUTH_TYPE_V2
1w6d: ISAKMP/xauth: request attribute XAUTH_MESSAGE_V2
1w6d: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
1w6d: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1641488057
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_XAUTH
1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_START_LOGIN
Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
New State = IKE_XAUTH_REQ_SENT

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF_XAUTH
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.
message ID = 1641488057
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP: Config payload REPLY
1w6d: ISAKMP/xauth: reply attribute XAUTH_TYPE_V2 unexpected
1w6d: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
1w6d: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
1w6d: ISAKMP (0:2): deleting node 1641488057 error FALSE
reason "done with xauth request/reply exchange"
1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY
Old State = IKE_XAUTH_REQ_SENT
New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

1w6d: AAA/AUTHEN/CONT (2017610393): continue_login (user='(undef)')

1w6d: AAA/AUTHEN(2017610393): Status=GETUSER

1w6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)

1w6d: TAC+: send AUTHEN/CONT packet id=2017610393

1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued

1w6d: TAC+: (2017610393) AUTHEN/CONT processed

1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = GETPASS

1w6d: AAA/AUTHEN(2017610393): Status=GETPASS

1w6d: AAA/AUTHEN/CONT (2017610393): continue_login (user='cisco')

1w6d: AAA/AUTHEN(2017610393): Status=GETPASS

1w6d: AAA/AUTHEN(2017610393): Method=tacacs+ (tacacs+)

1w6d: TAC+: send AUTHEN/CONT packet id=2017610393

1w6d: TAC+: 172.16.124.96 (2017610393) AUTHEN/CONT queued

1w6d: TAC+: (2017610393) AUTHEN/CONT processed

1w6d: TAC+: ver=192 id=2017610393 received AUTHEN status = PASS

1w6d: AAA/AUTHEN(2017610393): Status=PASS

1w6d: ISAKMP: got callback 1

1w6d: TAC+: Closing TCP/IP 0x8183D638 connection to 172.16.124.96/49

1w6d: CryptoEngine0: generate hmac context for conn id 2

1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw) (ipsec)

1w6d: ISAKMP (0:2): initiating peer config to 192.168.60.34. ID = 1736579999

1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw) (ipsec)

1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_XAUTH

1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_CONT_LOGIN

Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

New State = IKE_XAUTH_SET_SENT

1w6d: AAA/MEMORY: free_user (0x812F79FC) user='cisco' ruser='NULL'

port='ISAKMP' rem_addr='192.168.60.34' authen_type=ASCII

service=LOGIN priv=0

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) CONF_XAUTH

1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw) (ipsec)

1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.

message ID = 1736579999

1w6d: CryptoEngine0: generate hmac context for conn id 2

1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw) (ipsec)

1w6d: ISAKMP: Config payload ACK

1w6d: ISAKMP (0:2): XAUTH ACK Processed

1w6d: ISAKMP (0:2): deleting node 1736579999 error FALSE

reason "done with transaction"

1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK

Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

1w6d: ISAKMP (0:2): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE

Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE

1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw) (ipsec)

1w6d: ISAKMP (0:2): processing transaction payload from 192.168.60.34.

message ID = 398811763

1w6d: CryptoEngine0: generate hmac context for conn id 2

1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw) (ipsec)

1w6d: ISAKMP: Config payload REQUEST

1w6d: ISAKMP (0:2): checking request:

1w6d: ISAKMP: IP4_ADDRESS

1w6d: ISAKMP: IP4_NETMASK

1w6d: ISAKMP: IP4_DNS

1w6d: ISAKMP: IP4_NBNS

1w6d: ISAKMP: ADDRESS_EXPIRY

1w6d: ISAKMP: APPLICATION_VERSION

1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7000

1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7001

1w6d: ISAKMP: DEFAULT_DOMAIN

1w6d: ISAKMP: SPLIT_INCLUDE

```
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7007
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7008
1w6d: ISAKMP: UNKNOWN Unknown Attr: 0x7005
1w6d: AAA: parse name=ISAKMP-GROUP-AUTH idb type=-1 tty=-1
1w6d: AAA/MEMORY: create_user (0x812F79FC) user='vpngroup' ruser='NULL' ds0=0 po
rt='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34' authen_type=NONE service=LOGIN pr
iv=0 initial_task_id='0'
1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
  Port='ISAKMP-GROUP-AUTH' list='groupauthor' service=NET
1w6d: AAA/AUTHOR/CRYPTO AAA: ISAKMP-GROUP-AUTH(1059453615)
  user='vpngroup'
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
  send AV service=ike
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
  send AV protocol=ipsec
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
  found list "groupauthor"
1w6d: ISAKMP-GROUP-AUTH AAA/AUTHOR/CRYPTO AAA(1059453615):
  Method=LOCAL
1w6d: AAA/AUTHOR (1059453615): Post authorization status = PASS_ADD
1w6d: ISAKMP: got callback 1
AAA/AUTHOR/IKE: Processing AV service=ike
AAA/AUTHOR/IKE: Processing AV protocol=ipsec
AAA/AUTHOR/IKE: Processing AV tunnel-password=cisco123
AAA/AUTHOR/IKE: Processing AV default-domain*cisco.com
AAA/AUTHOR/IKE: Processing AV addr-pool*ippool
AAA/AUTHOR/IKE: Processing AV key-exchange=ike
AAA/AUTHOR/IKE: Processing AV timeout*0
AAA/AUTHOR/IKE: Processing AV idletime*0
AAA/AUTHOR/IKE: Processing AV inacl*102
AAA/AUTHOR/IKE: Processing AV dns-servers*10.1.1.10 0.0.0.0
AAA/AUTHOR/IKE: Processing AV wins-servers*10.1.1.20 0.0.0.0
1w6d: ISAKMP (0:2): attributes sent in message:
1w6d: Address: 0.2.0.0
1w6d: ISAKMP (0:2): allocating address 10.1.1.114
1w6d: ISAKMP: Sending private address: 10.1.1.114
1w6d: ISAKMP: Unknown Attr: IP4_NETMASK (0x2)
1w6d: ISAKMP: Sending IP4_DNS server address: 10.1.1.10
1w6d: ISAKMP: Sending IP4_NBNS server address: 10.1.1.20
1w6d: ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address: 86396
1w6d: ISAKMP: Sending APPLICATION_VERSION string:
  Cisco Internetwork Operating System Software IOS (tm) C1700 Software
  (C1710-K9O3SY-M), Version 12.2(8)T1, RELEASE SOFTWARE (fc2)
  TAC Support: http://www.cisco.com/tac
  Copyright (c) 1986-2002 by cisco Systems, Inc.
  Compiled Sat 30-Mar-02 13:30 by ccai
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7000)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7001)
1w6d: ISAKMP: Sending DEFAULT_DOMAIN default domain name: cisco.com
1w6d: ISAKMP: Sending split include name 102 network 10.38.0.0
  mask 255.255.0.0 protocol 0, src port 0, dst port 0

1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7007)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7008)
1w6d: ISAKMP: Unknown Attr: UNKNOWN (0x7005)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ISAKMP (0:2): responding to peer config from 192.168.60.34. ID = 398811763
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) CONF_ADDR
1w6d: ISAKMP (0:2): deleting node 398811763 error FALSE reason ""
```

1w6d: ISAKMP (0:2): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR
Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

1w6d: AAA/MEMORY: free_user (0x812F79FC) user='vpngroup'
ruser='NULL' port='ISAKMP-GROUP-AUTH' rem_addr='192.168.60.34'
authen_type=NONE service=LOGIN priv=0

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE

1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)

1w6d: CryptoEngine0: generate hmac context for conn id 2

1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)

1w6d: ISAKMP (0:2): processing HASH payload. message ID = 1369459046

1w6d: ISAKMP (0:2): processing SA payload. message ID = 1369459046

1w6d: ISAKMP (0:2): Checking IPsec proposal 1

1w6d: ISAKMP: transform 1, ESP_3DES

1w6d: ISAKMP: attributes in transform:

1w6d: ISAKMP: authenticator is HMAC-MD5

1w6d: ISAKMP: encaps is 1

1w6d: ISAKMP: SA life type in seconds

1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B

1w6d: validate proposal 0

1w6d: IPSEC(validate_proposal): transform proposal

(prot 3, trans 3, hmac_alg 1) not supported

1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0

1w6d: ISAKMP (0:2): skipping next ANDED proposal (1)

1w6d: ISAKMP (0:2): Checking IPsec proposal 2

1w6d: ISAKMP: transform 1, ESP_3DES

1w6d: ISAKMP: attributes in transform:

1w6d: ISAKMP: authenticator is HMAC-SHA

1w6d: ISAKMP: encaps is 1

1w6d: ISAKMP: SA life type in seconds

1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B

1w6d: validate proposal 0

1w6d: ISAKMP (0:2): atts are acceptable.

1w6d: ISAKMP (0:2): Checking IPsec proposal 2

1w6d: ISAKMP (0:2): transform 1, IPPCP LZS

1w6d: ISAKMP: attributes in transform:

1w6d: ISAKMP: encaps is 1

1w6d: ISAKMP: SA life type in seconds

1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B

1w6d: IPSEC(validate_proposal): transform proposal

(prot 4, trans 3, hmac_alg 0) not supported

1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0

1w6d: ISAKMP (0:2): Checking IPsec proposal 3

1w6d: ISAKMP: transform 1, ESP_3DES

1w6d: ISAKMP: attributes in transform:

1w6d: ISAKMP: authenticator is HMAC-MD5

1w6d: ISAKMP: encaps is 1

1w6d: ISAKMP: SA life type in seconds

1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B

1w6d: validate proposal 0

1w6d: IPSEC(validate_proposal): transform proposal

(prot 3, trans 3, hmac_alg 1) not supported

1w6d: ISAKMP (0:2): atts not acceptable. Next payload is 0

1w6d: ISAKMP (0:2): Checking IPsec proposal 4

1w6d: ISAKMP: transform 1, ESP_3DES

1w6d: ISAKMP: attributes in transform:

1w6d: ISAKMP: authenticator is HMAC-SHA

1w6d: ISAKMP: encaps is 1

1w6d: ISAKMP: SA life type in seconds

1w6d: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B

1w6d: validate proposal 0

1w6d: ISAKMP (0:2): atts are acceptable.

1w6d: IPSEC(validate_proposal_request): proposal part #1,

(key eng. msg.) INBOUND local= 172.18.124.158,

```
remote= 192.168.60.34, local_proxy= 172.18.124.158/255.255.255.255/0/0
(type=1), remote_proxy= 10.1.1.114/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
1w6d: validate proposal request 0
1w6d: ISAKMP (0:2): processing NONCE payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
1w6d: ISAKMP (0:2): processing ID payload. message ID = 1369459046
1w6d: ISAKMP (0:2): asking for 1 spis from ipsec
1w6d: ISAKMP (0:2): Node 1369459046, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

1w6d: IPSEC(key_engine): got a queue event...
1w6d: IPSEC(spi_response): getting spi 1640315492 for SA
    from 172.18.124.158 to 192.168.60.34 for prot 3
1w6d: ISAKMP: received ke message (2/1)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_ENCRYPT(hw)(ipsec)
1w6d: ISAKMP (0:2): sending packet to 192.168.60.34 (R) QM_IDLE
1w6d: ISAKMP (0:2): Node 1369459046,
    Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

1w6d: ISAKMP (0:2): received packet from 192.168.60.34 (R) QM_IDLE
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_DECRYPT(hw)(ipsec)
1w6d: CryptoEngine0: generate hmac context for conn id 2
1w6d: CryptoEngine0: CRYPTO_ISA_IKE_HMAC(hw)(ipsec)
1w6d: ipsec allocate flow 0
1w6d: ipsec allocate flow 0
1w6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
1w6d: CryptoEngine0: CRYPTO_ISA_IPSEC_KEY_CREATE(hw)(ipsec)
1w6d: ISAKMP (0:2): Creating IPsec SAs
1w6d: inbound SA from 192.168.60.34 to 172.18.124.158
    (proxy 10.1.1.114 to 172.18.124.158)
1w6d: has spi 0x61C53A64 and conn_id 200 and flags 4
1w6d: lifetime of 2147483 seconds
1w6d: outbound SA from 172.18.124.158 to 192.168.60.34
    (proxy 172.18.124.158 to 10.1.1.114 )
1w6d: has spi -1885622177 and conn_id 201 and flags C
1w6d: lifetime of 2147483 seconds
1w6d: ISAKMP (0:2): deleting node 1369459046 error FALSE
    reason "quick mode done (await())"
1w6d: ISAKMP (0:2): Node 1369459046,
    Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

1w6d: IPSEC(key_engine): got a queue event...
1w6d: IPSEC(initialize_sas): ,
    (key eng. msg.) INBOUND local= 172.18.124.158,
    remote= 192.168.60.34, local_proxy= 172.18.124.158/0.0.0.0/0/0
    (type=1), remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 2147483s and 0kb, spi= 0x61C53A64(1640315492),
    conn_id= 200, keysize= 0, flags= 0x4
1w6d: IPSEC(initialize_sas): , (key eng. msg.)
    OUTBOUND local= 172.18.124.158, remote= 192.168.60.34,
    local_proxy= 172.18.124.158/0.0.0.0/0/0 (type=1),
    remote_proxy= 10.1.1.114/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 2147483s and 0kb, spi= 0x8F9BB05F(2409345119),
    conn_id= 201, keysize= 0, flags= 0xC
1w6d: IPSEC(create_sa): sa created, (sa) sa_dest= 172.18.124.158,
sa_prot= 50, sa_spi= 0x61C53A64(1640315492),
```

```
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 200
1w6d: IPSEC(create_sa): sa created, (sa) sa_dest= 192.168.60.34,
sa_prot= 50, sa_spi= 0x8F9BB05F(2409345119),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 201
```

Clientvastlegging

Om de logbestanden te bekijken, start u het logvenster op de VPN-client en stelt u het filter in op *Hoog* voor alle geconfigureerde klassen.

Hier wordt een voorbeeldloguitvoer weergegeven.

```
1 11:56:06.609 06/05/02 Sev=Info/6 DIALER/0x63300002
Initiating connection.

2 11:56:06.609 06/05/02 Sev=Info/4 CM/0x63100002
Begin connection process

3 11:56:06.609 06/05/02 Sev=Info/4 CM/0x63100004
Establish secure connection using Ethernet

4 11:56:06.609 06/05/02 Sev=Info/4 CM/0x63100026
Attempt connection with server "172.18.124.158"

5 11:56:06.609 06/05/02 Sev=Info/6 IKE/0x6300003B
Attempting to establish a connection with 172.18.124.158.

6 11:56:06.669 06/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to 172.18.124.158

7 11:56:07.250 06/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 172.18.124.158

8 11:56:07.250 06/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, VID, KE, ID, NON, HASH) from
172.18.124.158

9 11:56:07.250 06/05/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

10 11:56:07.250 06/05/02 Sev=Info/5 IKE/0x63000001
Peer is a Cisco-Unity compliant peer

11 11:56:07.250 06/05/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

12 11:56:07.250 06/05/02 Sev=Info/5 IKE/0x63000001
Peer supports DPD

13 11:56:07.250 06/05/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 0A0E5F2A15C0B2F2A41B00897B816B3C

14 11:56:07.250 06/05/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 09002689DFD6B712

15 11:56:07.280 06/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) to
172.18.124.158

16 11:56:07.320 06/05/02 Sev=Info/5 IKE/0x6300002F
```

Received ISAKMP packet: peer = 172.18.124.158

17 11:56:07.320 06/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME) from
172.18.124.158

18 11:56:07.320 06/05/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 86400 seconds

19 11:56:07.320 06/05/02 Sev=Info/5 IKE/0x63000046
This SA has already been alive for 1 seconds, setting expiry to 86399 seconds
from now

20 11:56:07.561 06/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 172.18.124.158

21 11:56:07.561 06/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.18.124.158

22 11:56:07.561 06/05/02 Sev=Info/4 CM/0x63100015
Launch xAuth application

23 11:56:07.571 06/05/02 Sev=Info/4 IPSEC/0x63700014
Deleted all keys

24 11:56:09.734 06/05/02 Sev=Info/4 CM/0x63100017
xAuth application returned

25 11:56:09.734 06/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.18.124.158

26 11:56:10.174 06/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 172.18.124.158

27 11:56:10.184 06/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.18.124.158

28 11:56:10.184 06/05/02 Sev=Info/4 CM/0x6310000E
Established Phase 1 SA. 1 Phase 1 SA in the system

29 11:56:10.184 06/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.18.124.158

30 11:56:10.204 06/05/02 Sev=Info/5 IKE/0x6300005D
Client sending a firewall request to concentrator

31 11:56:10.204 06/05/02 Sev=Info/5 IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client, Capability= (Centralized
Policy Push).

32 11:56:10.204 06/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.18.124.158

33 11:56:10.265 06/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 172.18.124.158

34 11:56:10.265 06/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.18.124.158

35 11:56:10.265 06/05/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.1.1.114

36 11:56:10.265 06/05/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.10

37 11:56:10.265 06/05/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value =
10.1.1.20

38 11:56:10.265 06/05/02 Sev=Info/5 IKE/0xA3000017
MODE_CFG_REPLY: The received (INTERNAL_ADDRESS_EXPIRY) attribute and value
(86396) is not supported

39 11:56:10.265 06/05/02 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
value = Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1710-K9O3SY-M), Version 12.2(8)T1,
RELEASE SOFTWARE (fc2)
TAC Support: <http://www.cisco.com/tac>
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 30-Mar-02 13:30 by ccai

40 11:56:10.265 06/05/02 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = cisco.com

41 11:56:10.265 06/05/02 Sev=Info/5 IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets),
value = 0x00000001

42 11:56:10.265 06/05/02 Sev=Info/5 IKE/0x6300000F
SPLIT_NET #1
subnet = 10.38.0.0
mask = 255.255.0.0
protocol = 0
src port = 0
dest port=0

43 11:56:10.265 06/05/02 Sev=Info/4 CM/0x63100019
Mode Config data received

44 11:56:10.275 06/05/02 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 172.18.124.158, GW IP =
172.18.124.158

45 11:56:10.275 06/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 172.18.124.158

46 11:56:10.575 06/05/02 Sev=Info/4 IPSEC/0x63700014
Deleted all keys

47 11:56:10.605 06/05/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 172.18.124.158

48 11:56:10.605 06/05/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 172.18.124.158

49 11:56:10.605 06/05/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 3600 seconds

50 11:56:10.605 06/05/02 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

51 11:56:10.605 06/05/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 172.18.124.158

52 11:56:10.605 06/05/02 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0x51A04966 OUTBOUND SPI = 0x61C53A64 INBOUND

SPI = 0x8F9BB05F)

53 11:56:10.605 06/05/02 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x61C53A64

54 11:56:10.605 06/05/02 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x8F9BB05F

55 11:56:10.605 06/05/02 Sev=Info/4 CM/0x6310001A
One secure connection established

56 11:56:10.625 06/05/02 Sev=Info/6 DIALER/0x63300003
Connection established.

57 11:56:10.735 06/05/02 Sev=Info/6 DIALER/0x63300008
MAPI32 Information - Outlook not default mail client

58 11:56:11.677 06/05/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

59 11:56:11.677 06/05/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x643ac561 into key list

60 11:56:11.677 06/05/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

61 11:56:11.677 06/05/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x5fb09b8f into key list

[Gerelateerde informatie](#)

- [Ondersteuning van Terminal Access Control System \(TACACS+\)](#)
- [Cisco Secure Access Control Server voor Unix-ondersteuning](#)
- [Cisco Secure ACS voor Windows-ondersteuning](#)
- [Cisco VPN-clientondersteuning](#)
- [Ondersteuning van IPSec-onderhandeling/IKE-protocollen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)