AnyConnect Secure Mobility-client met eenmalig wachtwoord configureren

Inhoud

Inleiding

Dit document beschrijft een configuratievoorbeeld voor adaptieve security applicatie (ASA) en Cisco AnyConnect Secure Mobility Client-toegang.

Voorwaarden

Vereisten

In dit document wordt ervan uitgegaan dat de ASA volledig operationeel is en geconfigureerd om Cisco Adaptive Security Device Manager (ASDM) of Command Line Interface (CLI) in staat te stellen configuratiewijzigingen aan te brengen.

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van ASA's CLI en ASDM
- SSL VPN-configuratie op de Cisco ASA head-end
- Basiskennis van Twee Factoren Verificatie

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversies:

- Cisco adaptieve security applicatie ASA 5506
- Software voor Cisco adaptieve security applicatie versie 9.6(1)
- Adaptieve Security Device Manager versie 7.8(2)
- AnyConnect versie 4.5.02033

Opmerking: Download het AnyConnect VPN-clientpakket (AnyConnect-win*.pkg) van Cisco Software Download (alleen geregistreerde klanten). Kopieer de AnyConnect VPN-client naar het flitsgeheugen van de ASA, dat wordt gedownload naar de externe gebruikerscomputers om de SSL VPN-verbinding met de ASA tot stand te brengen. Raadpleeg het gedeelte AnyConnect-client installeren in de ASA-configuratiehandleiding voor meer informatie.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Adaptieve security applicatie (ASA) Voor Cisco AnyConnect Secure Mobility Client-toegang wordt tweevoudige verificatie gebruikt met behulp van One-Time Password (OTP). Men moet de juiste referenties en token opgeven voor een AnyConnect-gebruiker om verbinding te kunnen maken met succes.

Twee-factor authenticatie gebruikt twee verschillende authenticatiemethoden die elk 2 van deze kunnen zijn.

- Iets wat je weet
- Iets wat je hebt
- Iets wat jij bent

In het algemeen bestaat het uit iets dat een gebruiker kent (gebruikersnaam en wachtwoord), en iets dat een gebruiker heeft (bijvoorbeeld een entiteit met informatie die alleen een individu bezit zoals een token of certificaat). Dit is veiliger dan traditionele verificatieontwerpen waarbij een gebruiker authenticeert via referenties die zijn opgeslagen in de lokale database van ASA of in Active Directory (AD)-server die is geïntegreerd met ASA. Een eenmalig wachtwoord is een van de eenvoudigste en populairste vormen van tweevoudige verificatie voor het beveiligen van de netwerktoegang. In grote ondernemingen vereist de Virtual Private Network-toegang bijvoorbeeld vaak het gebruik van eenmalige wachtwoordtoken voor externe gebruikersverificatie.

In dit scenario gebruikt u OpenOTP-verificatieserver als AAA-server die radiusprotocol gebruikt voor communicatie tussen ASA- en AAA-server. Gebruikersreferenties zijn configuraties op de OpenOTP-server die is gekoppeld aan Google Authenticator Application servicing als een zacht token voor de tweevoudige verificatie.

De OpenOTP-configuratie valt hier niet onder omdat deze buiten het bereik van dit document valt. U kunt deze links controleren voor meer informatie.

OpenOTP instellen
https://www.rcdevs.com/docs/howtos/openotp_quick_start/openotp_quick_start/

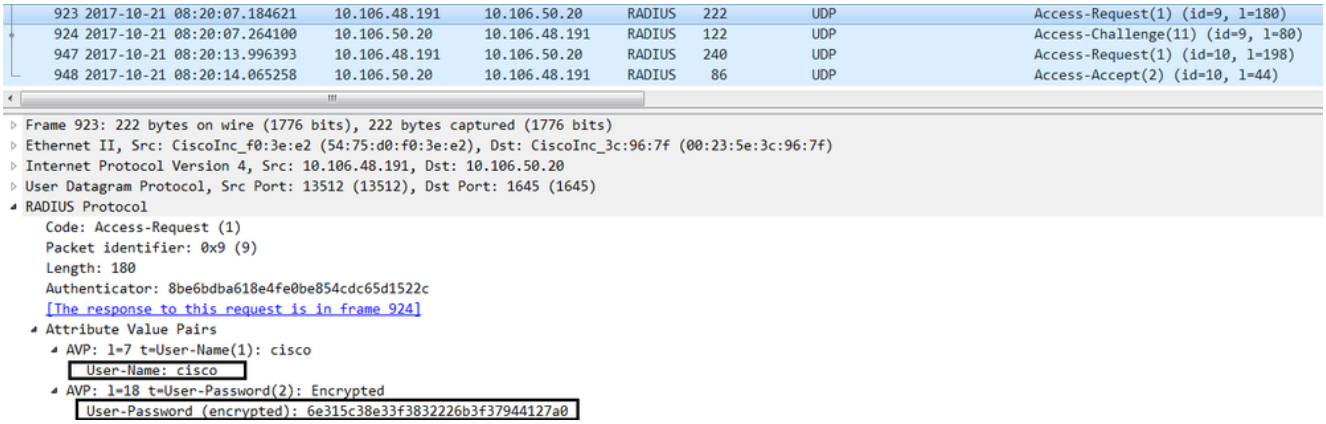
ASA configureren voor OpenOTP-verificatie
https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/

Pakketstroom

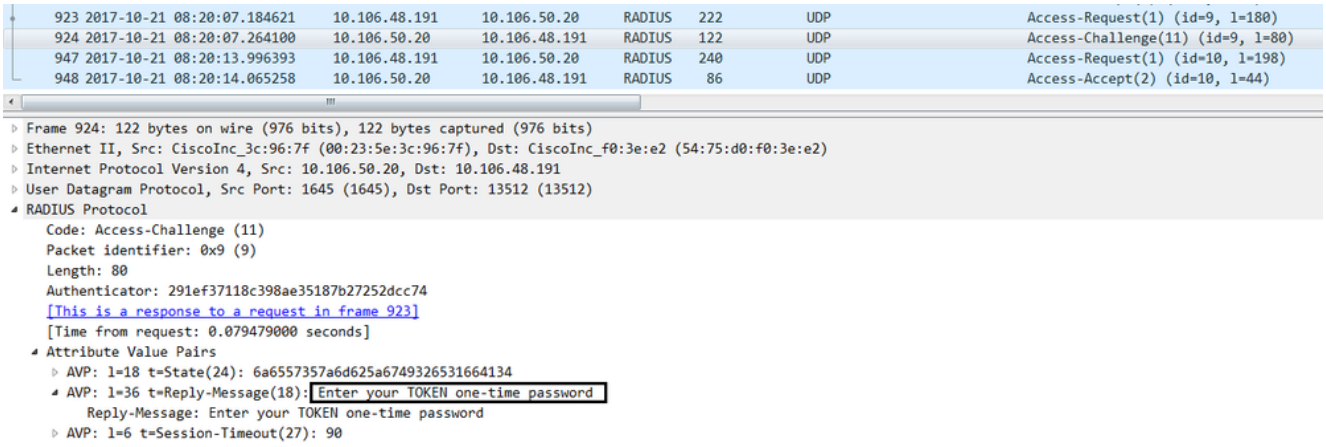
Deze pakketopname is op de buiteninterface van ASA genomen en met AAA-server verbonden op 10.106.50.20.

1. AnyConnect-gebruiker initieert een clientverbinding met ASA en is afhankelijk van de geconfigureerde groep-url- en groep-alias, de verbinding landt op een specifieke tunnelgroep (verbindingsprofiel). Op dit punt wordt de gebruiker gevraagd de referenties in te voeren.

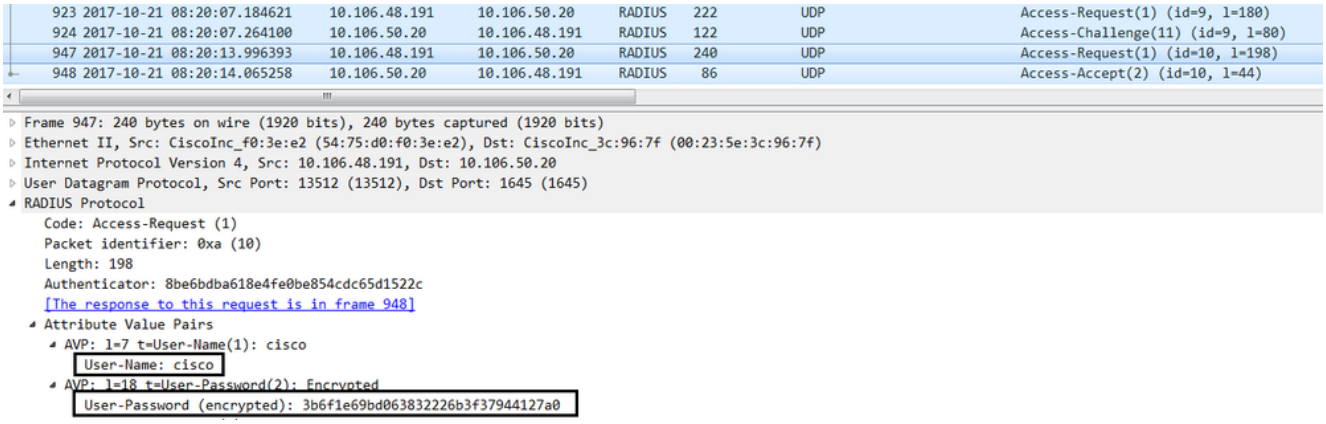
2. Zodra de gebruiker de referenties invoert, wordt het verificatieverzoek (access-request pakket) doorgestuurd naar de AAA-server vanuit de ASA.



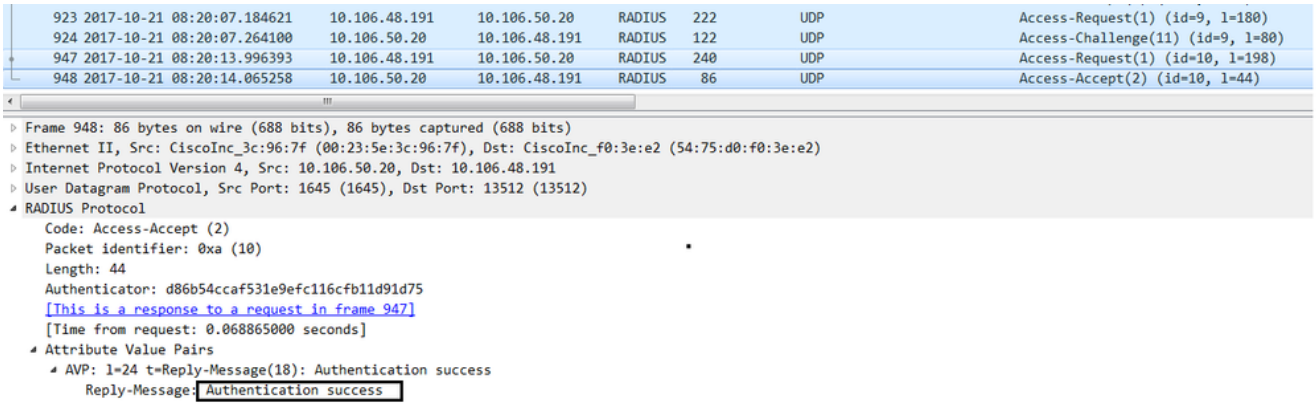
3. Nadat het verificatieverzoek de AAA-server heeft bereikt, worden de referenties gevalideerd. Als zij correct zijn, antwoordt de AAA-server met een Access-Challenge waarbij de gebruiker wordt gevraagd een eenmalig wachtwoord in te voeren. In het geval van onjuiste referenties wordt een access-reject-pakket naar de ASA verzonden.



4. Aangezien de gebruiker het eenmalige wachtwoord invoert, wordt het verificatieverzoek in de vorm van een access-request-pakket van de ASA naar de AAA-server verzonden



5. Zodra het eenmalige wachtwoord op de AAA-server is gevalideerd, wordt een pakket met toegangsrechten verzonden van de server naar de ASA, wordt de gebruiker met succes geverifieerd en wordt het tweevoudige verificatieproces voltooid.



Informatie over AnyConnect-licenties

Hier is een aantal links naar nuttige informatie over de Cisco AnyConnect Secure Mobility Client-licenties:

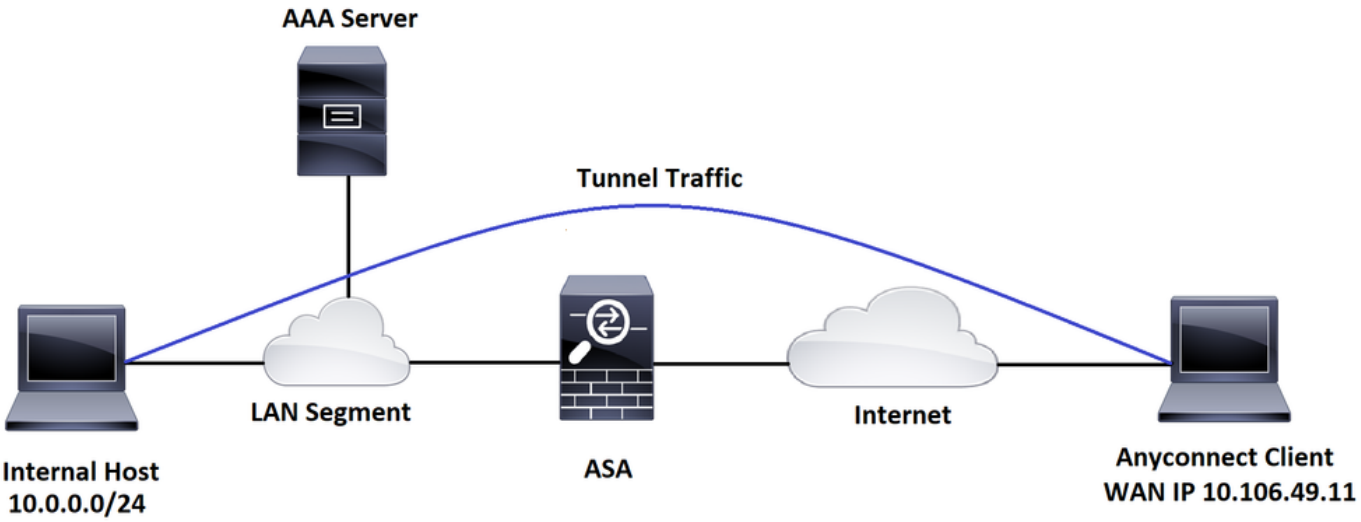
- Raadpleeg dit document voor veelgestelde AnyConnect-licentievragen.
- Raadpleeg de Cisco Bestelgids voor AnyConnect voor informatie over AnyConnect Apex- en Plus-licenties.

Configureren

In dit gedeelte wordt beschreven hoe u de Cisco AnyConnect Secure Mobility Client op de ASA kunt configureren.

> **Opmerking**: Gebruik de Command Lookup Tool (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram



ASDM AnyConnect-configuratiewizard

De AnyConnect-configuratiewizard kan worden gebruikt om de AnyConnect Secure Mobility Client te configureren. Zorg ervoor dat een AnyConnect-clientpakket is geüpload naar de flash/schijf van de ASA-firewall voordat u verdergaat.

Volg de volgende stappen om de AnyConnect Secure Mobility Client te configureren met de configuratiewizard:

Raadpleeg dit document voor gesplitste tunnelconfiguratie via ASDM om AnyConnect te downloaden en te installeren.
[AnyConnect beveiligde mobiliteit-client]

ASA CLI-configuratie

Deze sectie bevat de CLI-configuratie voor Cisco AnyConnect Secure Mobility Client ter referentie.

```
!--------------------Client pool configuration------------ ------

ip local pool ANYCONNECT-POOL 192.168.100.1-192.168.100.254 mask 255.255.255.0

!

interface GigabitEthernet1/1

 nameif outside
```

```
 security-level 0
 ip address dhcp setroute
!

!--------------------Split ACL configuration--------------------

access-list SPLIT-TUNNEL standard permit 10.0.0.0 255.255.255.0

pager lines 24
logging enable
logging timestamp
mtu tftp 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any outside
asdm image disk0:/asdm-782.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
route outside 0.0.0.0 0.0.0.0 10.106.56.1 1

!------------------Configure AAA server --------------------

aaa-server RADIUS_OTP protocol radius
aaa-server RADIUS_OTP (outside) host 10.106.50.20
 key *****


!------Configure Trustpoint containing ASA Identity Certificate ------

crypto ca trustpoint ASDM_Trustpoint 0
 enrollment self
```

```
 subject-name CN=bglanyconnect.cisco.com
 keypair self



!-------Apply trustpoint on outside interface------

ssl trust-point ASDM_Trustpoint0 outside

!-------Enable AnyConnect and configuring AnyConnect Image------

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.5.02033-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable


!--------------------Group Policy configuration--------------------

group-policy GroupPolicy_ANYCONNECT-PROFILE internal
group-policy GroupPolicy_ANYCONNECT-PROFILE attributes
 dns-server value 10.10.10.99
 vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT-TUNNEL
 default-domain value cisco.com

!----------Tunnel-Group (Connection Profile) Configuration----------

tunnel-group ANYCONNECT_PROFILE type remote-access
tunnel-group ANYCONNECT_PROFILE general-attributes
 address-pool ANYCONNECT-POOL
 authentication-server-group RADIUS_OTP
```

```
 default-group-policy GroupPolicy_ANYCONNECT-PROFILE

tunnel-group ANYCONNECT_PROFILE webvpn-attributes

 group-alias ANYCONNECT-PROFILE enable


: end
```

Raadpleeg dit document voor het configureren en installeren van een certificaat van een derde partij op de ASA voor AnyConnect-clientverbindingen.

ASA SSL digitaal certificaat configureren

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

> **Opmerking**: De Output Interpreter Tool (alleen geregistreerde klanten) ondersteunt bepaalde **show** opdrachten. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

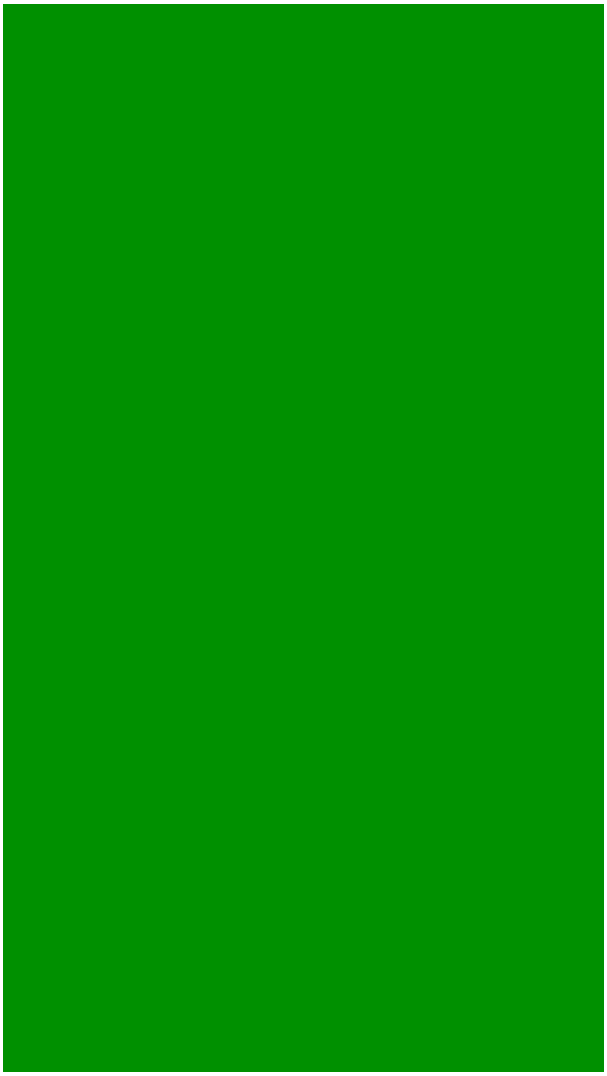
Deze showopdrachten kunnen worden uitgevoerd om de status van AnyConnect-client en de statistieken ervan te bevestigen.

```
ASA(config)# show vpn-sessiondb anyconnect


Session Type: AnyConnect


Username     : cisco                  Index        : 1

Assigned IP  : 192.168.100.1          Public IP    : 10.106.49.111

Protocol     : AnyConnect-Parent DTLS-Tunnel

License      : AnyConnect Premium

Encryption   : AnyConnect-Parent: (1)none  DTLS-Tunnel: (1)AES256

Hashing      : AnyConnect-Parent: (1)none  DTLS-Tunnel: (1)SHA1

Bytes Tx     : 15122                  Bytes Rx     : 5897

Group Policy : GroupPolicy_ANYCONNECT-PROFILE

Tunnel Group : ANYCONNECT_PROFILE

Login Time   : 14:47:09 UTC Wed Nov 1 2017

Duration     : 1h:04m:52s
```

```
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000100059f9de6d
Security Grp : none

ASA(config)# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 1
Assigned IP  : 192.168.100.1          Public IP    : 10.106.49.111
Protocol     : AnyConnect-Parent DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15122                  Bytes Rx     : 5897
Pkts Tx      : 10                     Pkts Rx      : 90
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : GroupPolicy_ANYCONNECT-PROFILE
Tunnel Group : ANYCONNECT_PROFILE
Login Time   : 14:47:09 UTC Wed Nov 1 2017
Duration     : 1h:04m:55s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000100059f9de6d
Security Grp : none

AnyConnect-Parent Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
 Tunnel ID    : 1.1
```

```
 Public IP    : 10.106.49.111

 Encryption   : none                  Hashing      : none

 TCP Src Port : 53113                 TCP Dst Port : 443

 Auth Mode    : userPassword

 Idle Time Out: 30 Minutes            Idle TO Left : 1 Minutes

 Client OS    : win

 Client OS Ver: 6.1.7601 Service Pack 1

 Client Type  : AnyConnect

 Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.5.02033

 Bytes Tx     : 7561                  Bytes Rx     : 0

 Pkts Tx      : 5                     Pkts Rx      : 0

 Pkts Tx Drop : 0                     Pkts Rx Drop : 0


DTLS-Tunnel:

 Tunnel ID    : 1.3

 Assigned IP  : 192.168.100.1         Public IP    : 10.106.49.111

 Encryption   : AES256                Hashing      : SHA1

 Ciphersute  : AES256-SHA

 Encapsulation: DTLSv1.0              UDP Src Port : 63257

 UDP Dst Port : 443                   Auth Mode    : userPassword

 Idle Time Out: 30 Minutes            Idle TO Left : 0 Minutes

 Client OS    : Windows

 Client Type  : DTLS VPN Client

 Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.5.02033

 Bytes Tx     : 0                     Bytes Rx     : 5801

 Pkts Tx      : 0                     Pkts Rx      : 88

 Pkts Tx Drop : 0                     Pkts Rx Drop : 0
```

Gebruikerservaring



Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

> **Opmerking**: Raadpleeg Belangrijke informatie over debug commando's voordat u **debug** commando's gebruikt.

> **Waarschuwing**: op de ASA kunt u verschillende debug-niveaus instellen; standaard wordt niveau 1 gebruikt. Als u het debug-niveau wijzigt, kan de breedheid van de debugs toenemen. Doe dit met omzichtigheid, vooral in productieomgevingen.

U kunt deze debugs gebruiken om het volledige verificatieproces voor een inkomende AnyConnect-clientverbinding op te lossen:

- debug radius all
- debug aaa authentication
- debug wrbvpn anyconnect

Deze opdrachten bevestigen dat de gebruikersreferenties correct zijn of niet.

test aaa-server verificatie <aaa_server_group> [<host_ip>] gebruikersnaam <user> wachtwoord

<wachtwoord>

In geval van juiste gebruikersnaam en wachtwoord,

```
ASA(config)# test aaa authentication RADIUS_OTP host 10.106.50.20

Username: cisco

Password: *****

INFO: Attempting Authentication test to IP address <10.106.50.20> (timeout: 12 seconds)

ERROR: Authentication Challenged: No error
```

De laatste fout heeft betrekking op het feit dat aangezien de AAA-server verwacht dat de gebruiker een eenmalig wachtwoord invoert na succesvolle verificatie van gebruikersnaam en wachtwoord, en deze test niet impliceert dat een gebruiker actief OTP invoert, u ziet Access-Challenge verzonden door AAA-server in antwoord waarop geen fout wordt gezien op de ASA.

In geval van een onjuiste gebruikersnaam en/of wachtwoord,

```
ASA(config)# test aaa authentication RADIUS_OTP host 10.106.50.20

Username: cisco

Password: ***

INFO: Attempting Authentication test to IP address <10.106.50.20> (timeout: 12 seconds)

ERROR: Authentication Rejected: AAA failure
```

Debugs van een werkopstelling zien er ongeveer zo uit:

legenda

AnyConnect client voor echte IP: 10.106.49.11

ASA IP: 10.106.48.191

```
ASA(config)# debug radius all

ASA(config)# debug aaa authentication

debug aaa authentication enabled at level 1

radius mkreq: 0x8

alloc_rip 0x74251058

   new request 0x8 --> 7 (0x74251058)

got user 'cisco'

got password

add_req 0x74251058 session 0x8 id 7
```

```
RADIUS_REQUEST

radius.c: rad_mkpkt

rad_mkpkt: ip:source-ip=10.106.49.111


RADIUS packet decode (authentication request)


--------------------------------------

Raw packet data (length = 180).....

01 07 00 b4 b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca    |  .......%..S..=..

74 05 27 5c 01 07 63 69 73 63 6f 02 12 d7 99 45    |  t.'\..cisco....E

6e 0f 46 71 bc 52 47 b0 81 b4 18 ae 34 05 06 00    |  n.Fq.RG.....4...

00 40 00 1e 0f 31 30 2e 31 30 36 2e 34 38 2e 31    |  .@...10.106.48.1

39 31 1f 0f 31 30 2e 31 30 36 2e 34 39 2e 31 31    |  91..10.106.49.11

31 3d 06 00 00 00 05 42 0f 31 30 2e 31 30 36 2e    |  1=.....B.10.106.

34 39 2e 31 31 31 04 06 0a 6a 30 bf 1a 22 00 00    |  49.111...j0.."..

00 09 01 1c 69 70 3a 73 6f 75 72 63 65 2d 69 70    |  ....ip:source-ip

3d 31 30 2e 31 30 36 2e 34 39 2e 31 31 31 1a 1a    |  =10.106.49.111..

00 00 0c 04 92 14 41 4e 59 43 4f 4e 4e 45 43 54    |  ......ANYCONNECT

2d 50 52 4f 46 49 4c 45 1a 0c 00 00 0c 04 96 06    |  -PROFILE........

00 00 00 02                                        |  ....


Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 7 (0x07)

Radius: Length = 180 (0x00B4)

Radius: Vector: B6C2BF25CF8053A9A23DC8CA7405275C

Radius: Type = 1 (0x01) User-Name

Radius: Length = 7 (0x07)

Radius: Value (String) =

63 69 73 63 6f                                     |  cisco

Radius: Type = 2 (0x02) User-Password

Radius: Length = 18 (0x12)
```

```
Radius: Value (String) =

d7 99 45 6e 0f 46 71 bc 52 47 b0 81 b4 18 ae 34    |  ..En.Fq.RG.....4

Radius: Type = 5 (0x05) NAS-Port

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x4000

Radius: Type = 30 (0x1E) Called-Station-Id

Radius: Length = 15 (0x0F)

Radius: Value (String) =

31 30 2e 31 30 36 2e 34 38 2e 31 39 31             |  10.106.48.191

Radius: Type = 31 (0x1F) Calling-Station-Id

Radius: Length = 15 (0x0F)

Radius: Value (String) =

31 30 2e 31 30 36 2e 34 39 2e 31 31 31             |  10.106.49.111

Radius: Type = 61 (0x3D) NAS-Port-Type

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

Radius: Type = 66 (0x42) Tunnel-Client-Endpoint

Radius: Length = 15 (0x0F)

Radius: Value (String) =

31 30 2e 31 30 36 2e 34 39 2e 31 31 31             |  10.106.49.111

Radius: Type = 4 (0x04) NAS-IP-Address

Radius: Length = 6 (0x06)

Radius: Value (IP Address) = 10.106.48.191 (0x0A6A30BF)

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 34 (0x22)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 28 (0x1C)

Radius: Value (String) =

69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e    |  ip:source-ip=10.

31 30 36 2e 34 39 2e 31 31 31                      |  106.49.111

Radius: Type = 26 (0x1A) Vendor-Specific
```

```
Radius: Length = 26 (0x1A)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 20 (0x14)
Radius: Value (String) =
41 4e 59 43 4f 4e 4e 45 43 54 2d 50 52 4f 46 49    |  ANYCONNECT-PROFI
4c 45                                              |  LE
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
send pkt 10.106.50.20/1645
rip 0x74251058 state 7 id 7
rad_vrfy() : response message verified
rip 0x74251058
 : chall_state ''
 : state 0x7
 : reqauth:
    b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca 74 05 27 5c
 : info 0x74251190
    session_id 0x8
    request_id 0x7
   user 'cisco'
    response '***'
    app 0
    reason 0
    skey 'testing123'
    sip 10.106.50.20
    type 1
```

```
RADIUS packet decode (response)


--------------------------------------

Raw packet data (length = 80).....

0b 07 00 50 ed 7a 06 92 f7 18 16 6b 97 d4 83 5f    |  ...P.z.....k..._

be 9b d7 29 18 12 75 6b 35 36 58 49 4f 6e 35 31    |  ...)..uk56XIOn51

58 36 4b 75 4c 74 12 24 45 6e 74 65 72 20 79 6f    |  X6KuLt.$Enter yo

75 72 20 54 4f 4b 45 4e 20 6f 6e 65 2d 74 69 6d    |  ur TOKEN one-tim

65 20 70 61 73 73 77 6f 72 64 1b 06 00 00 00 5a    |  e password.....Z


Parsed packet data.....

Radius: Code = 11 (0x0B)

Radius: Identifier = 7 (0x07)

Radius: Length = 80 (0x0050)

Radius: Vector: ED7A0692F718166B97D4835FBE9BD729

Radius: Type = 24 (0x18) State

Radius: Length = 18 (0x12)

Radius: Value (String) =

75 6b 35 36 58 49 4f 6e 35 31 58 36 4b 75 4c 74    |  uk56XIOn51X6KuLt

Radius: Type = 18 (0x12) Reply-Message

Radius: Length = 36 (0x24)

Radius: Value (String) =

45 6e 74 65 72 20 79 6f 75 72 20 54 4f 4b 45 4e    |  Enter your TOKEN

20 6f 6e 65 2d 74 69 6d 65 20 70 61 73 73 77 6f    |   one-time passwo

72 64                                              |  rd

Radius: Type = 27 (0x1B) Session-Timeout

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5A

rad_procpkt: CHALLENGE

radius mkreq: 0x8

   old request 0x8 --> 8 (0x74251058), state 3

wait pass - pass '***'. make request
```

```
RADIUS_REQUEST

radius.c: rad_mkpkt

rad_mkpkt: ip:source-ip=10.106.49.111


RADIUS packet decode (authentication request)


--------------------------------------

Raw packet data (length = 198).....

01 08 00 c6 b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca    |  .......%..S..=..

74 05 27 5c 01 07 63 69 73 63 6f 02 12 83 c4 00    |  t.'\..cisco.....

3e 56 73 71 bc 52 47 b0 81 b4 18 ae 34 05 06 00    |  >Vsq.RG.....4...

00 40 00 1e 0f 31 30 2e 31 30 36 2e 34 38 2e 31    |  .@...10.106.48.1

39 31 1f 0f 31 30 2e 31 30 36 2e 34 39 2e 31 31    |  91..10.106.49.11

31 3d 06 00 00 00 05 42 0f 31 30 2e 31 30 36 2e    |  1=.....B.10.106.

34 39 2e 31 31 31 04 06 0a 6a 30 bf 18 12 75 6b    |  49.111...j0...uk

35 36 58 49 4f 6e 35 31 58 36 4b 75 4c 74 1a 22    |  56XIOn51X6KuLt."

00 00 00 09 01 1c 69 70 3a 73 6f 75 72 63 65 2d    |  ......ip:source-

69 70 3d 31 30 2e 31 30 36 2e 34 39 2e 31 31 31    |  ip=10.106.49.111

1a 1a 00 00 0c 04 92 14 41 4e 59 43 4f 4e 4e 45    |  ........ANYCONNE

43 54 2d 50 52 4f 46 49 4c 45 1a 0c 00 00 0c 04    |  CT-PROFILE......

96 06 00 00 00 02                                  |  ......


Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 8 (0x08)

Radius: Length = 198 (0x00C6)

Radius: Vector: B6C2BF25CF8053A9A23DC8CA7405275C

Radius: Type = 1 (0x01) User-Name

Radius: Length = 7 (0x07)

Radius: Value (String) =

63 69 73 63 6f                                     |  cisco

Radius: Type = 2 (0x02) User-Password
```

```
Radius: Length = 18 (0x12)

Radius: Value (String) =

83 c4 00 3e 56 73 71 bc 52 47 b0 81 b4 18 ae 34    |  ...>Vsq.RG.....4

Radius: Type = 5 (0x05) NAS-Port

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x4000

Radius: Type = 30 (0x1E) Called-Station-Id

Radius: Length = 15 (0x0F)

Radius: Value (String) =

31 30 2e 31 30 36 2e 34 38 2e 31 39 31             |  10.106.48.191

Radius: Type = 31 (0x1F) Calling-Station-Id

Radius: Length = 15 (0x0F)

Radius: Value (String) =

31 30 2e 31 30 36 2e 34 39 2e 31 31 31             |  10.106.49.111

Radius: Type = 61 (0x3D) NAS-Port-Type

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

Radius: Type = 66 (0x42) Tunnel-Client-Endpoint

Radius: Length = 15 (0x0F)

Radius: Value (String) =

31 30 2e 31 30 36 2e 34 39 2e 31 31 31             |  10.106.49.111

Radius: Type = 4 (0x04) NAS-IP-Address

Radius: Length = 6 (0x06)

Radius: Value (IP Address) = 10.106.48.191 (0x0A6A30BF)

Radius: Type = 24 (0x18) State

Radius: Length = 18 (0x12)

Radius: Value (String) =

75 6b 35 36 58 49 4f 6e 35 31 58 36 4b 75 4c 74    |  uk56XIOn51X6KuLt

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 34 (0x22)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair
```

```
Radius: Length = 28 (0x1C)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e    |  ip:source-ip=10.
31 30 36 2e 34 39 2e 31 31 31                      |  106.49.111
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 26 (0x1A)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 20 (0x14)
Radius: Value (String) =
41 4e 59 43 4f 4e 4e 45 43 54 2d 50 52 4f 46 49    |  ANYCONNECT-PROFI
4c 45                                              |  LE
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
send pkt 10.106.50.20/1645
rip 0x74251058 state 7 id 8
rad_vrfy() : response message verified
rip 0x74251058
 : chall_state 'uk56XIOn51X6KuLt'
 : state 0x7
 : reqauth:
    b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca 74 05 27 5c
 : info 0x74251190
    session_id 0x8
    request_id 0x8
    user 'cisco'
    response '***'
    app 0
```

```
    reason 0

    skey 'testing123'

    sip 10.106.50.20

    type 1


RADIUS packet decode (response)


--------------------------------------

Raw packet data (length = 44).....

02 08 00 2c c0 80 63 1c 3e 43 a4 bd 46 78 bd 68    |  ...,..c.>C..Fx.h

49 29 23 bd 12 18 41 75 74 68 65 6e 74 69 63 61    |  I)#...Authentica

74 69 6f 6e 20 73 75 63 63 65 73 73                |  tion success


Parsed packet data.....

Radius: Code = 2 (0x02)

Radius: Identifier = 8 (0x08)

Radius: Length = 44 (0x002C)

Radius: Vector: C080631C3E43A4BD4678BD68492923BD

Radius: Type = 18 (0x12) Reply-Message

Radius: Length = 24 (0x18)

Radius: Value (String) =

41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e 20 73    |  Authentication s

75 63 63 65 73 73                                  |  uccess

rad_procpkt: ACCEPT

RADIUS_ACCESS_ACCEPT: normal termination

RADIUS_DELETE

remove_req 0x74251058 session 0x8 id 8

free_rip 0x74251058

radius: send queue empty
```

Gerelateerde informatie

- AnyConnect Secure Mobility Client met split-tunneling op een ASA configureren
- RSA Secure ID-verificatie voor AnyConnect-clients op een Cisco IOS Head-end configuratie
- RSA Token Server en SDI-protocolgebruik voor ASA en ACS
- ASA AnyConnect dubbele verificatie met configuratiehandleiding voor certificaatvalidatie, -toewijzing en -voorvulling
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.