Configurazione di AnyConnect Secure Mobility Client con password temporanea

Sommario

Introduzione

Questo documento descrive un esempio di configurazione per l'accesso Cisco AnyConnect Secure Mobility Client di Adaptive Security Appliance (ASA).

Prerequisiti

Requisiti

In questo documento si presume che l'ASA sia completamente operativa e configurata per consentire a Cisco Adaptive Security Device Manager (ASDM) o all'interfaccia della riga di comando (CLI) di apportare modifiche alla configurazione.

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di CLI e ASDM di ASA
- Configurazione della VPN SSL sull'headend Cisco ASA
- Conoscenze base dell'autenticazione a due fattori

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Adaptive Security Appliance ASA5506
- Software Cisco Adaptive Security Appliance versione 9.6(1)
- Adaptive Security Device Manager versione 7.8(2)
- AnyConnect versione 4.5.0203

  Nota: scaricare il pacchetto AnyConnect VPN Client (anyconnect-win*.pkg) da Cisco Software Download (solo utenti registrati). Copiare il client VPN AnyConnect nella memoria flash dell'ASA, che viene scaricata sui computer degli utenti remoti per stabilire la connessione VPN SSL con l'ASA. Per ulteriori informazioni, consultare la sezione Installazione del client AnyConnect della guida alla configurazione delle appliance ASA.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Adaptive Security Appliance (ASA) L'accesso Cisco AnyConnect Secure Mobility Client utilizza l'autenticazione a due fattori con l'ausilio della password per una singola sessione (OTP). Per connettersi correttamente, è necessario fornire le credenziali e il token corretti per un utente AnyConnect.

L'autenticazione a due fattori utilizza due diversi metodi di autenticazione, che possono essere due di questi.

- Qualcosa che sai
- Qualcosa che hai
- Qualcosa che sei

In generale, comprende qualcosa che un utente sa (nome utente e password) e qualcosa che un utente ha (ad esempio, un'entità di informazioni che solo un individuo possiede come un token o un certificato). Questo metodo è più sicuro rispetto alle progettazioni di autenticazione tradizionali, in cui un utente esegue l'autenticazione tramite credenziali archiviate nel database locale dell'ASA o nel server Active Directory (AD) integrato con ASA. La password temporanea è una delle forme più semplici e diffuse di autenticazione a due fattori per la protezione dell'accesso alla rete. Nelle grandi aziende, ad esempio, l'accesso alla rete privata virtuale spesso richiede l'utilizzo di token One-Time Password per l'autenticazione degli utenti remoti.

In questo scenario, si utilizza il server di autenticazione OpenOTP come server AAA che utilizza il protocollo Radius per la comunicazione tra ASA e il server AAA. Le credenziali utente vengono configurate sul server OpenOTP associato all'applicazione Google Authenticator che funge da token soft per l'autenticazione a due fattori.

La configurazione OpenOTP non è trattata in questo documento poiché non rientra nell'ambito del presente documento. È possibile controllare questi collegamenti per ulteriori informazioni.

Impostazione di OpenOTP
https://www.rcdevs.com/docs/howtos/openotp_quick_start/openotp_quick_start/

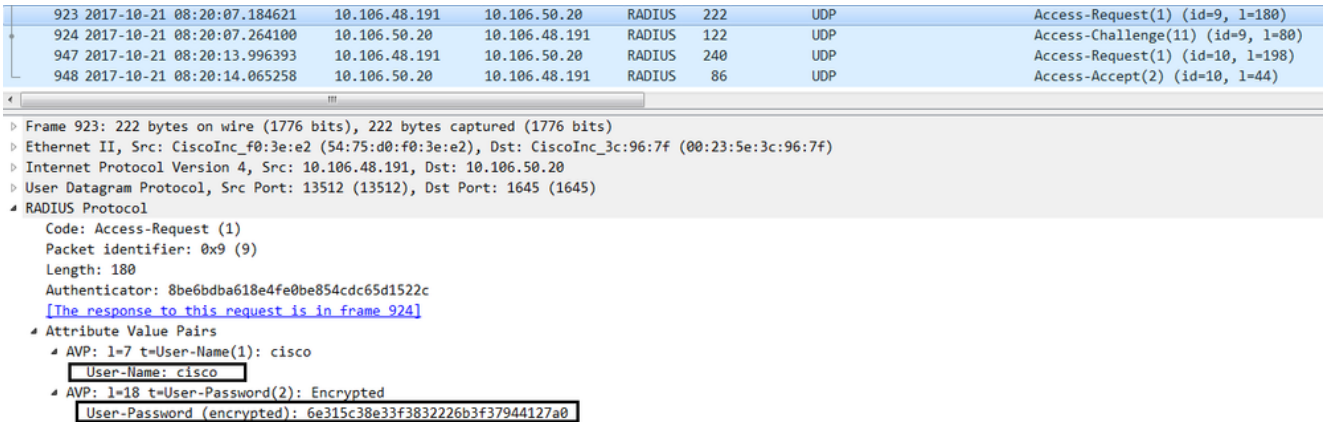
Configurazione dell'ASA per l'autenticazione OpenOTP
https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/

Flusso dei pacchetti

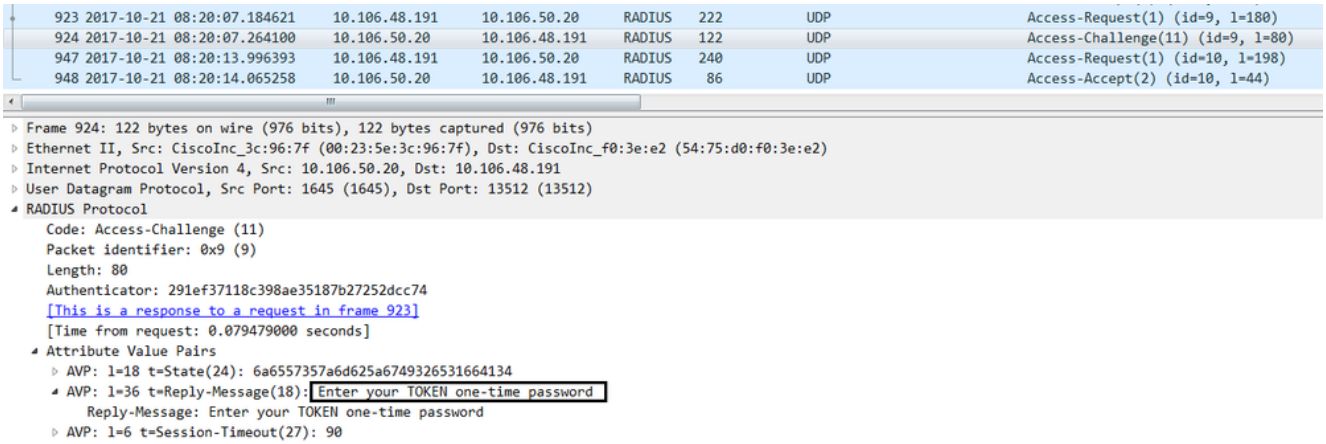
L'acquisizione è stata effettuata sull'interfaccia esterna dell'ASA collegata al server AAA alla versione 10.106.50.20.

1. L'utente AnyConnect avvia la connessione client verso l'appliance ASA e dipende dall'URL del gruppo e dall'alias del gruppo configurati, la connessione termina su un gruppo di tunnel (profilo di connessione) specifico. A questo punto, all'utente viene richiesto di immettere le credenziali.

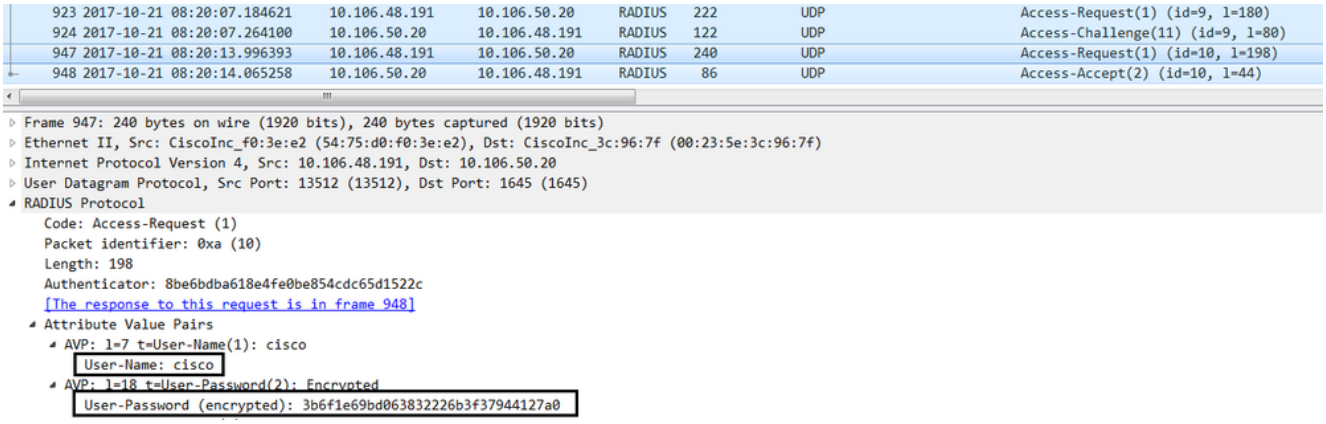
2. Dopo che l'utente ha immesso le credenziali, la richiesta di autenticazione (pacchetto Access-Request) viene inoltrata al server AAA dall'appliance ASA.



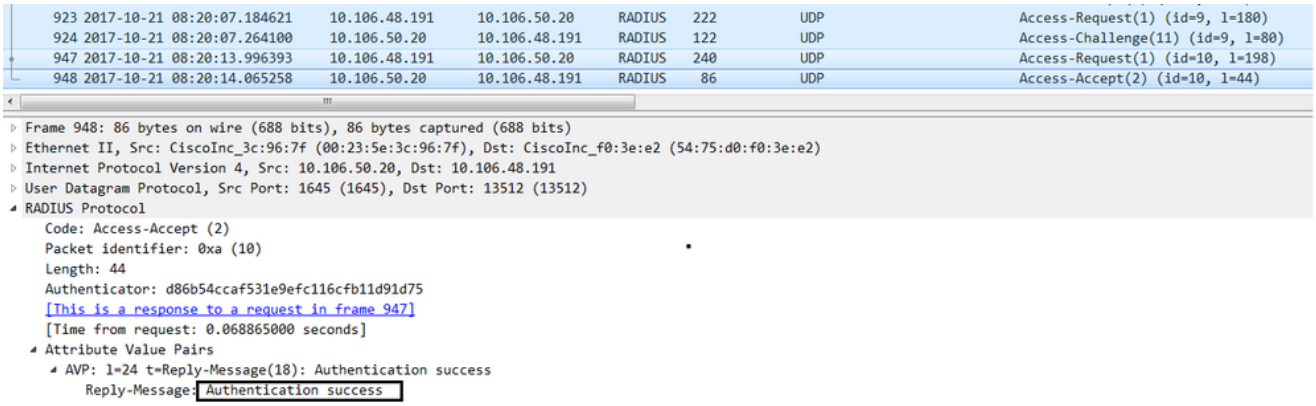
3. Dopo aver raggiunto il server AAA, la richiesta di autenticazione convalida le credenziali. Se sono corrette, il server AAA risponde con una richiesta di verifica di accesso in cui all'utente viene richiesto di immettere una password temporanea. In caso di credenziali errate, un pacchetto di rifiuto di accesso viene inviato all'appliance ASA.



4. Quando l'utente immette la password temporanea, la richiesta di autenticazione sotto forma di pacchetto Access-Request viene inviata dall'ASA al server AAA



5. Dopo aver convalidato la password temporanea sul server AAA, un pacchetto di accettazione dell'accesso viene inviato dal server all'appliance ASA, l'utente viene autenticato correttamente e il processo di autenticazione a due fattori viene completato.



Informazioni sulla licenza Anyconnect

Di seguito sono riportati alcuni collegamenti a informazioni utili sulle licenze Cisco AnyConnect Secure Mobility Client:

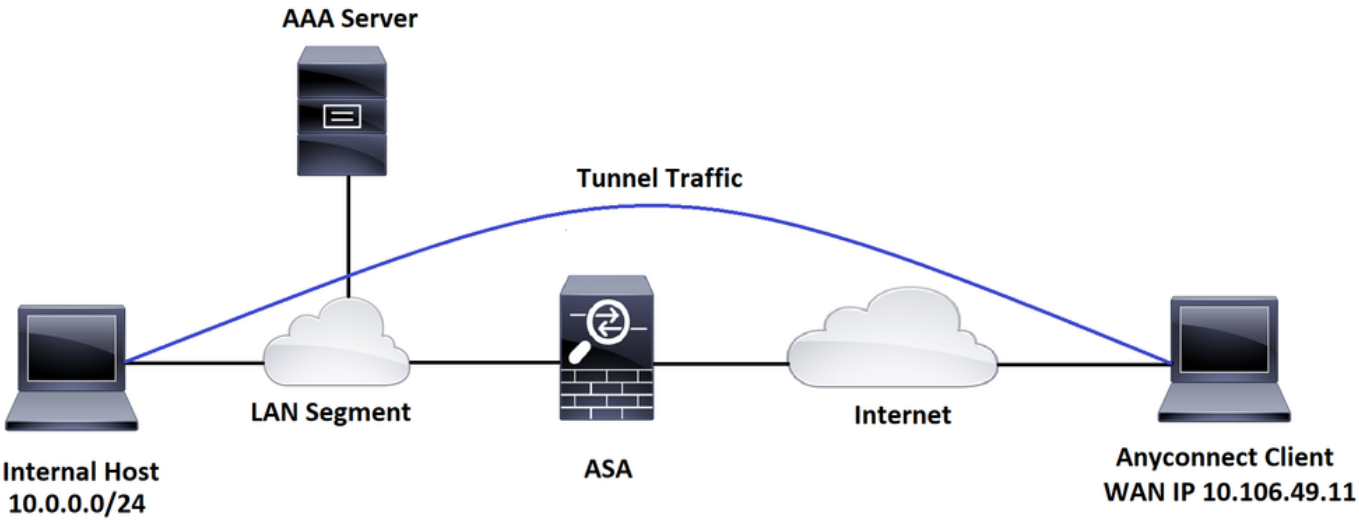
- Per le domande frequenti sulle licenze AnyConnect, consultare il presente documento.
- Per informazioni sulle licenze AnyConnect Apex e Plus, consultare la Guida agli ordini di Cisco AnyConnect.

Configurazione

In questa sezione viene descritto come configurare Cisco AnyConnect Secure Mobility Client sull'appliance ASA.

> **Nota**: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete



Configurazione guidata AnyConnect ASDM

La configurazione guidata AnyConnect può essere usata per configurare il client AnyConnect Secure Mobility. Prima di procedere, verificare che un pacchetto client AnyConnect sia stato caricato nella memoria flash/sul disco del firewall ASA.

Per configurare Anyconnect Secure Mobility Client con la Configurazione guidata, completare la procedura seguente:

Per la configurazione di uno split tunnel tramite ASDM, scaricare e installare AnyConnect, fare riferimento a questo documento.
AnyConnect Secure Mobility Client

Configurazione ASA CLI

In questa sezione viene fornita la configurazione CLI per Cisco AnyConnect Secure Mobility Client a scopo di riferimento.

```
!--------------------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
```

Per la configurazione e l'installazione di un certificato di terze parti sull'appliance ASA per le connessioni client AnyConnect, fare riferimento a questo documento.

Configurazione del certificato digitale SSL ASA

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

> **Nota**: lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show**. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

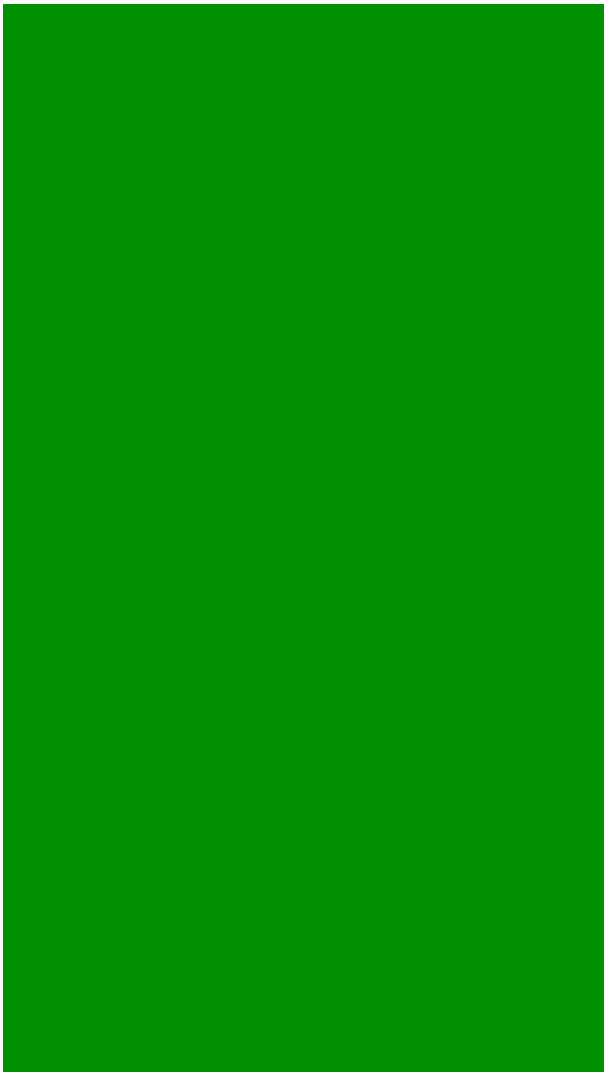
I comandi show possono essere eseguiti per confermare lo stato del client AnyConnect e le sue statistiche.

```
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
```

Esperienza utente



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

> **Nota**: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

> **Attenzione**: sull'appliance ASA, è possibile impostare vari livelli di debug; per impostazione predefinita, viene usato il livello 1. Se si modifica il livello di debug, il livello di dettaglio dei debug può aumentare. Procedere con cautela, soprattutto negli ambienti di produzione.

Per risolvere i problemi relativi all'intero processo di autenticazione per una connessione client AnyConnect in ingresso, è possibile utilizzare i seguenti debug:

- debug radius all
- debug autenticazione aaa
- debug wrbvpn anyconnect

Questi comandi confermano che le credenziali dell'utente sono corrette o meno.

test autenticazione aaa-server <gruppo_server_aaa> [<ip_host>] nome utente <utente> password

<password>

Se il nome utente e la password sono corretti,

```
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
```

L'ultimo errore si riferisce al fatto che, poiché il server AAA si aspetta che l'utente immetta una sola password dopo la riuscita dell'autenticazione del nome utente e della password e questo test non implica che l'utente entri attivamente in OTP, viene visualizzato il messaggio Access-Challenge inviato dal server AAA in risposta al quale non viene rilevato alcun errore sull'appliance ASA.

In caso di nome utente e/o password errati,

```
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
```

I debug da un'impostazione di lavoro hanno un aspetto simile al seguente:

Legenda

AnyConnect Client Real 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
```

Informazioni correlate

- Configurazione di AnyConnect Secure Mobility Client con split tunneling su una ASA
- Autenticazione RSA SecurID per client AnyConnect su una configurazione headend Cisco IOS
- Uso di RSA Token Server e del protocollo SDI per ASA e ACS
- ASA: doppia autenticazione AnyConnect con guida alla convalida, al mapping e alla configurazione pre-compilazione dei certificati
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).