# Configurer le client AnyConnect Secure Mobility avec un mot de passe à usage unique

## Table des matières



## Introduction

Ce document décrit un exemple de configuration pour l'accès au client Cisco AnyConnect Secure Mobility de l'appareil de sécurité adaptatif (ASA).

## Conditions préalables

### Exigences

Ce document suppose que l'ASA est entièrement opérationnel et configuré pour permettre à Cisco Adaptive Security Device Manager (ASDM) ou à l'interface de ligne de commande (CLI) d'apporter des modifications à la configuration.

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de l'interface CLI et de l'ASDM ASA
- Configuration SSLVPN sur la tête de réseau Cisco ASA
- Connaissance de base de l'authentification à deux facteurs

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles et matérielles suivantes :

- Appareil de sécurité adaptatif Cisco ASA5506
- Logiciel Cisco Adaptive Security Appliance Version 9.6(1)
- Adaptive Security Device Manager version 7.8(2)
- AnyConnect version 4.5.02033

---

> Remarque : téléchargez le package client VPN AnyConnect (anyconnect-win*.pkg) à partir du site de téléchargement de logiciels Cisco (clients enregistrés uniquement). Copiez le client VPN AnyConnect dans la mémoire flash de l'ASA, qui est téléchargée sur les ordinateurs des utilisateurs distants afin d'établir la connexion VPN SSL avec l'ASA. Référez-vous à la section Installer le client d'AnyConnect du guide de configuration d'ASA pour plus d'informations.

---

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Informations générales

ASA (Adaptive Security Appliance) L'accès client Cisco AnyConnect Secure Mobility utilise une authentification à deux facteurs à l'aide d'un mot de passe à usage unique (OTP). Il faut fournir les informations d’identification et le jeton corrects pour qu’un utilisateur AnyConnect puisse se connecter.

L'authentification à deux facteurs utilise deux méthodes d'authentification différentes, qui peuvent être n'importe laquelle de ces deux méthodes.

- Quelque chose que tu sais
- Quelque chose que vous avez
- Quelque chose que tu es

En général, il comprend quelque chose qu'un utilisateur connaît (nom d'utilisateur et mot de passe), et quelque chose qu'un utilisateur possède (par exemple, une entité d'information que seul un individu possède comme un jeton ou un certificat). Cette méthode est plus sécurisée que les conceptions d'authentification traditionnelles dans lesquelles un utilisateur s'authentifie via des informations d'identification stockées dans la base de données locale de l'ASA ou sur le serveur Active Directory (AD) intégré à l'ASA. Le mot de passe à usage unique est l'une des formes les plus simples et les plus répandues d'authentification à deux facteurs pour sécuriser l'accès au réseau. Par exemple, dans les grandes entreprises, l'accès au réseau privé virtuel nécessite souvent l'utilisation de jetons de mot de passe à usage unique pour l'authentification des utilisateurs distants.

Dans ce scénario, vous utilisez le serveur d'authentification OpenOTP comme serveur AAA qui utilise le protocole radius pour la communication entre ASA et le serveur AAA. Les informations

d'identification de l'utilisateur sont configurées sur le serveur OpenOTP qui est associé à la maintenance de l'application Google Authenticator en tant que jeton logiciel pour l'authentification à deux facteurs.

La configuration OpenOTP n'est pas traitée ici car elle sort du cadre de ce document. Vous pouvez consulter ces liens pour en savoir plus.

Configuration d'OpenOTP
https://www.rcdevs.com/docs/howtos/openotp_quick_start/openotp_quick_start/

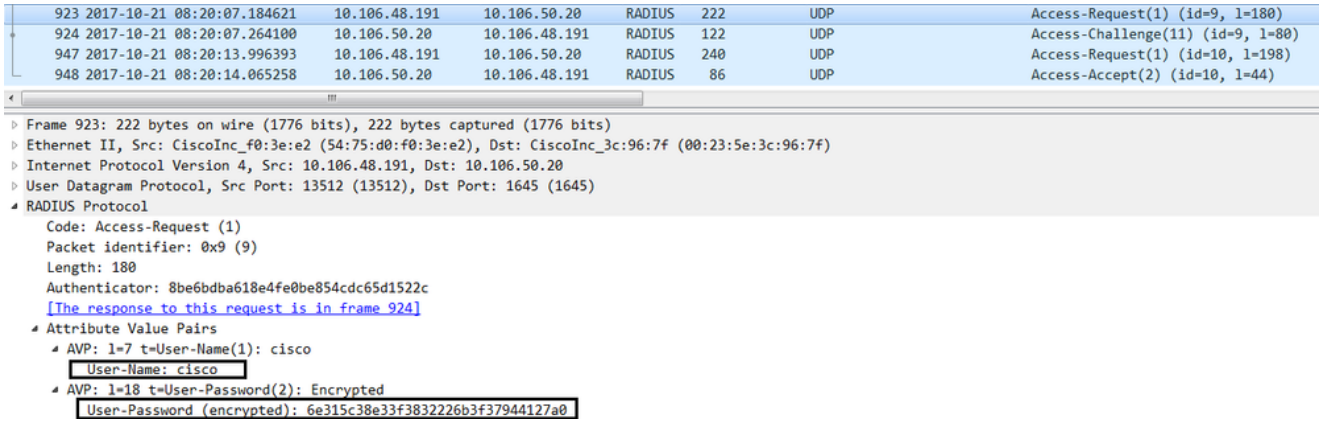
Configuration d'ASA pour l'authentification OpenOTP
https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/

## Flux des paquets

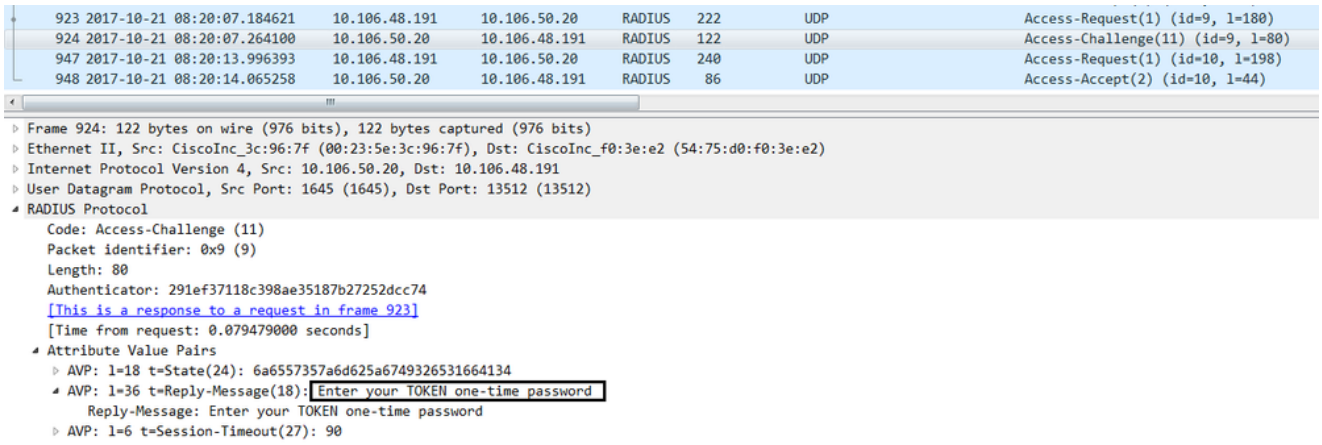
Cette capture de paquets a été effectuée sur l'interface externe de l'ASA connectée au serveur AAA à l'adresse 10.106.50.20.

1. Un utilisateur AnyConnect initie une connexion client vers ASA et dépend de l'url de groupe et de l'alias de groupe configurés, la connexion atterrit sur un groupe de tunnel spécifique (profil de connexion). À ce stade, l'utilisateur est invité à saisir les informations d'identification.

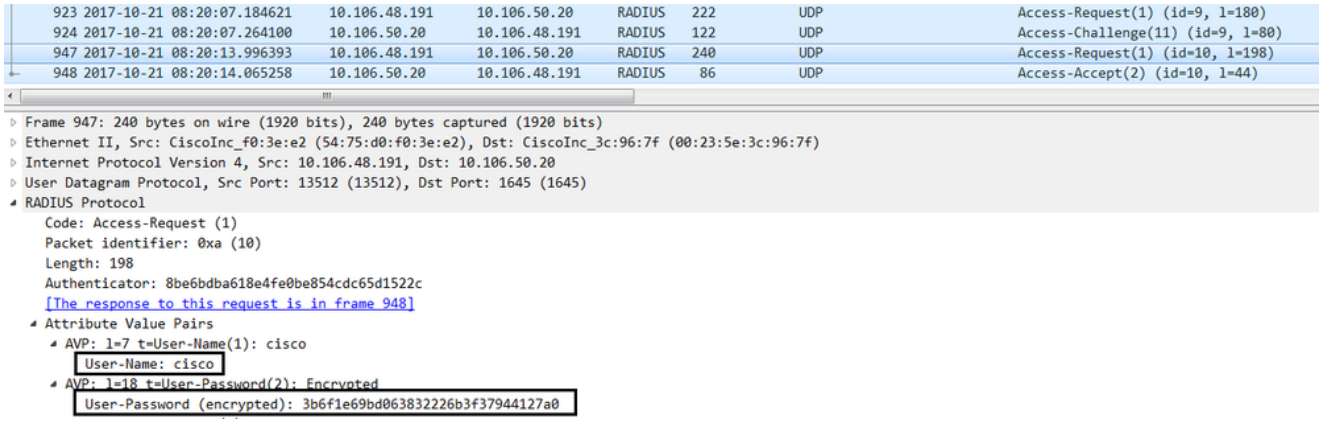
2. Une fois que l'utilisateur a saisi les informations d'identification, la demande d'authentification (paquet de demande d'accès) est transmise au serveur AAA à partir de l'ASA.



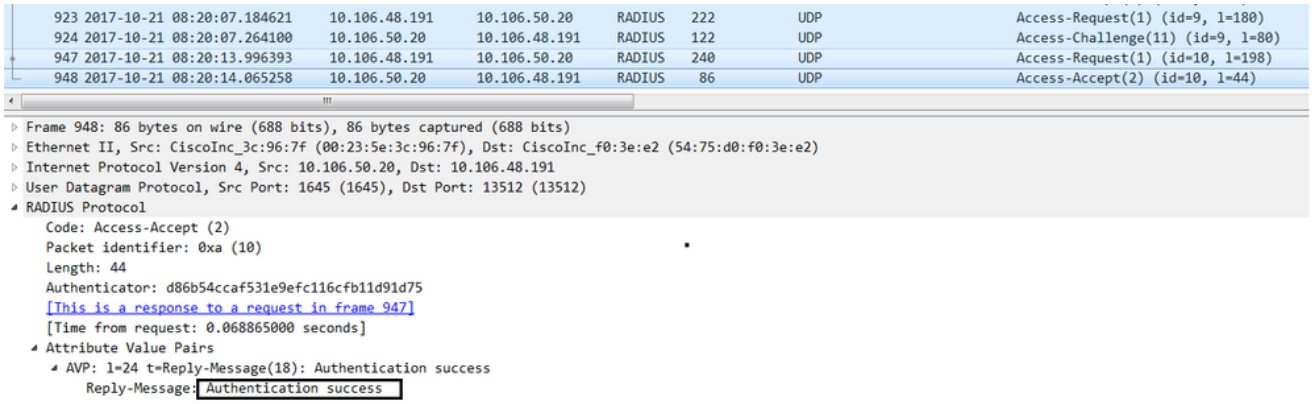

3. Une fois que la demande d'authentification atteint le serveur AAA, elle valide les informations d'identification. S'ils sont corrects, le serveur AAA répond avec un Access-Challenge où l'utilisateur est invité à entrer un mot de passe à usage unique. En cas d'informations d'identification incorrectes, un paquet Access-Reject est envoyé à l'ASA.




4. Lorsque l'utilisateur entre le mot de passe à usage unique, la demande d'authentification sous la forme d'un paquet de demande d'accès est envoyée de l'ASA au serveur AAA




5. Une fois que le mot de passe à usage unique a été validé sur le serveur AAA, un paquet d'acceptation d'accès est envoyé du serveur à l'ASA, l'utilisateur est authentifié et le processus d'authentification à deux facteurs est terminé.




### Renseignements sur la licence AnyConnect

Voici des liens vers des renseignements utiles sur les licences du client pour la mobilité sécurisée Cisco AnyConnect :

- Reportez-vous à ce document pour les questions fréquemment posées sur les licences AnyConnect.
- Consultez le guide de commande de Cisco AnyConnect pour obtenir des renseignements sur les licences AnyConnect Apex et Plus.

# Configurer

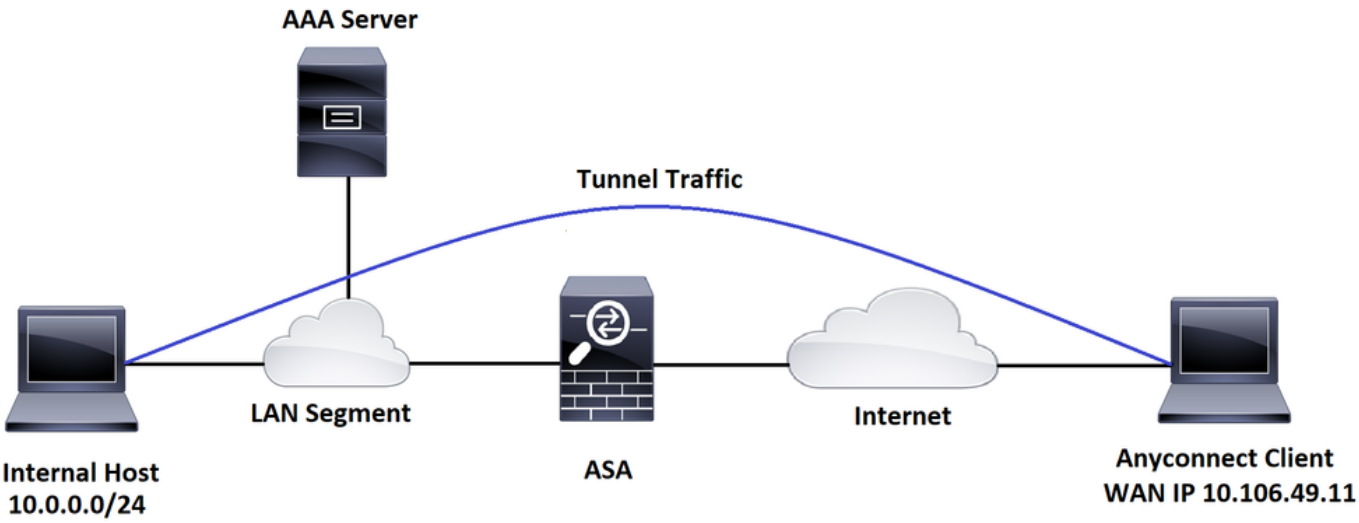
Cette section explique comment configurer le client pour la mobilité sécurisée Cisco AnyConnect sur l'ASA.

---

> Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

---

## Diagramme du réseau




### Assistant de configuration AnyConnect par ASDM

L'assistant de configuration AnyConnect peut être utilisé pour configurer le client pour la mobilité sécurisée Cisco AnyConnect. Assurez-vous qu'un paquet client AnyConnect a été chargé sur le disque ou la mémoire flash du pare-feu ASA avant de poursuivre.

Suivez ces étapes pour configurer le client pour la mobilité sécurisée AnyConnect avec l'aide de l'assistant de configuration :

Pour la configuration de tunnel partagé via ASDM, pour télécharger et installer AnyConnect, reportez-vous à ce document.

Client de mobilité sécurisée AnyConnect

Configuration de l'interface de ligne de commande ASA

Cette section fournit la configuration de la CLI affectée au client pour la mobilité sécurisée Cisco AnyConnect à des fins de référence.

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

Pour la configuration et l'installation d'un certificat tiers sur l'ASA pour les connexions client AnyConnect, référez-vous à ce document.

Configurer le certificat numérique SSL ASA

# Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Remarque : l'outil Output Interpreter Tool (clients enregistrés uniquement) prend en charge certaines commandes show. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Ces commandes show peuvent être exécutées pour confirmer l'état du client AnyConnect et ses statistiques.

```
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
  Ciphersuite  : 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
```

# Expérience utilisateur

: sur l'ASA, vous pouvez définir différents niveaux de débogage ; par défaut, le niveau 1 est utilisé. Si vous modifiez le niveau de débogage, le niveau de détail des débogages peut augmenter. Faites-le avec prudence, en particulier dans les environnements de production.

Pour dépanner le processus d'authentification complet d'une connexion client AnyConnect entrante, vous pouvez utiliser ces débogages :

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

Ces commandes confirment que les informations d'identification de l'utilisateur sont correctes ou non.

test aaa-server authentication <aaa_server_group> [<host_ip>] username <user> password <password>

En cas de nom d'utilisateur et de mot de passe corrects,

```
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
```

La dernière erreur se rapporte au fait que puisque le serveur AAA attend de l'utilisateur qu'il entre un mot de passe unique après l'authentification réussie du nom d'utilisateur et du mot de passe, et que ce test n'implique pas qu'un utilisateur entre activement OTP, vous voyez une demande d'accès envoyée par le serveur AAA en réponse à laquelle aucune erreur n'est vue sur l'ASA.

En cas de nom d'utilisateur et/ou de mot de passe incorrect,

```
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
```

Les débogages d'une configuration de travail ressemblent à ceci :

## Légende

Adresse IP réelle du client AnyConnect : 10.106.49.111

IP ASA : 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
```

# Informations connexes

- Configurer un client AnyConnect Secure Mobility avec la tunnellisation fractionnée sur un ASA
- Authentification RSA SecurID pour les clients AnyConnect sur une configuration de tête de réseau Cisco IOS

- Utilisation du serveur de jetons RSA et du protocole SDI pour ASA et ACS
- Guide de configuration de la double authentification ASA AnyConnect avec validation, mappage et pré-remplissage des certificats
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.