使用一次性密碼配置AnyConnect安全移動客戶端

目錄

簡介

本文檔介紹自適應安全裝置(ASA)Cisco AnyConnect安全移動客戶端訪問的配置示例。

必要條件

需求

本文檔假定ASA已完全正常運行並配置為允許Cisco Adaptive Security Device Manager(ASDM)或命令列介面(CLI)進行配置更改。

思科建議您瞭解以下主題：

- ASA CLI和ASDM的基本知識
- Cisco ASA頭端上的SSLVPN配置
- 雙因素認證的基本知識

採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- Cisco調適型安全裝置ASA5506
- 思科調適型安全裝置軟體版本9.6(1)
- 調適型安全裝置管理器版本7.8(2)
- AnyConnect版本4.5.02033

注意：從Cisco Software Download（僅限註冊客戶）下載AnyConnect VPN客戶端包(anyconnect-win*.pkg)。將AnyConnect VPN客戶端複製到ASA的快閃記憶體，該快閃記憶體下載到遠端使用者電腦，以便與ASA建立SSL VPN連線。有關詳細資訊，請參閱ASA配置指南的安裝AnyConnect客戶端部分。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

自適應安全裝置(ASA)Cisco AnyConnect安全移動客戶端訪問使用雙重身份驗證，輔以一次性密碼(OTP)。必須提供正確的憑據和令牌才能讓AnyConnect使用者成功連線。

雙因素身份驗證使用兩種不同的身份驗證方法，可以是其中任意兩種。

- 一些您知道的事情
- 你擁有的東西
- 有你這樣的東西

一般而言，它包含使用者知道的某物（使用者名稱和密碼），以及使用者所擁有某物（例如，只有個人擁有的資訊實體，如權杖或憑證）。這比傳統的身份驗證設計更安全，傳統的身份驗證設計使用者通過儲存在ASA本地資料庫或與ASA整合的Active Directory(AD)伺服器上的憑據進行身份驗證。一次性密碼是用於保護網路訪問的最簡單和最常用的雙因素身份驗證形式之一。例如，在大型企業中，虛擬專用網路訪問通常需要使用一次性密碼令牌進行遠端使用者身份驗證。

在此場景中，您使用OpenOTP身份驗證伺服器作為AAA伺服器，該伺服器使用radius協定在ASA和AAA伺服器之間進行通訊。在OpenOTP伺服器上配置使用者憑證，該伺服器與Google身份驗證器應用服務相關聯，作為用於雙因素身份驗證的軟令牌。

此處不涉及OpenOTP配置，因為它超出了本文檔的範圍。您可以檢查這些連結以備進一步閱讀。

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

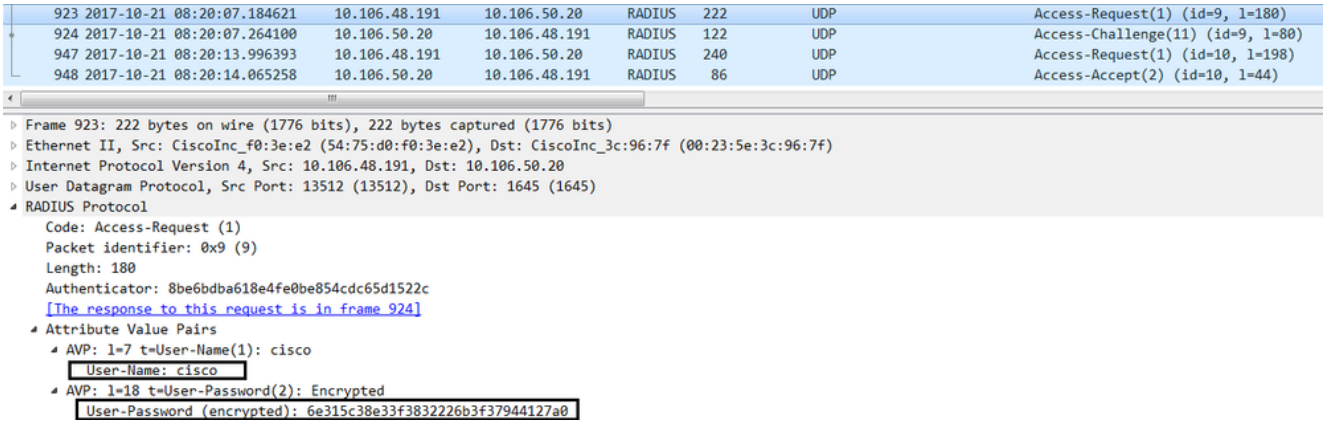
配置ASA以進行OpenOTP身份驗證
https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/

封包流量

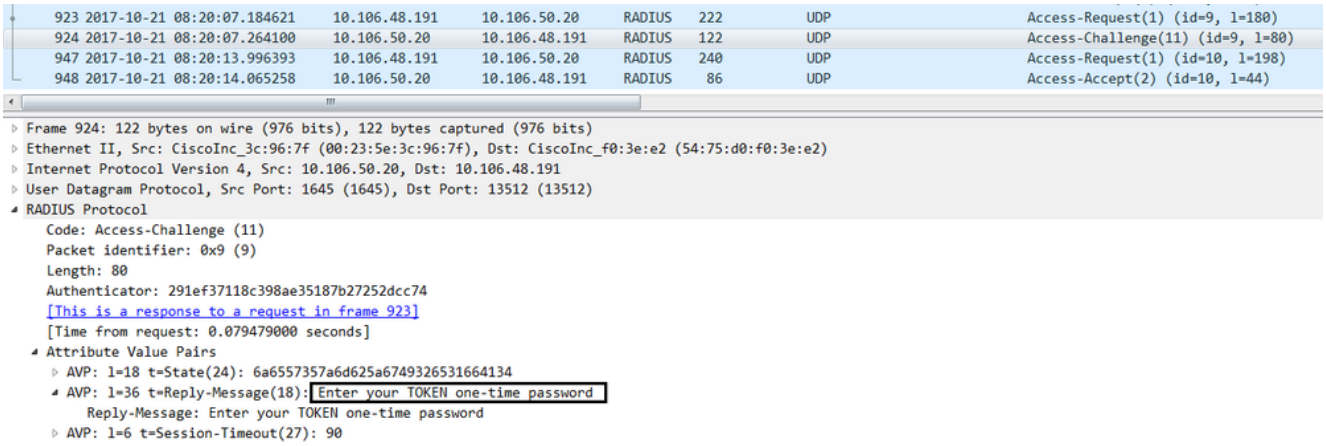
此資料包捕獲是在連線到AAA伺服器10.106.50.20的ASA外部介面上捕獲的。

1. AnyConnect使用者向ASA發起客戶端連線，並且取決於配置的group-url和group-alias，連線位於特定隧道組（連線配置檔案）上。此時，系統會提示使用者輸入憑證。

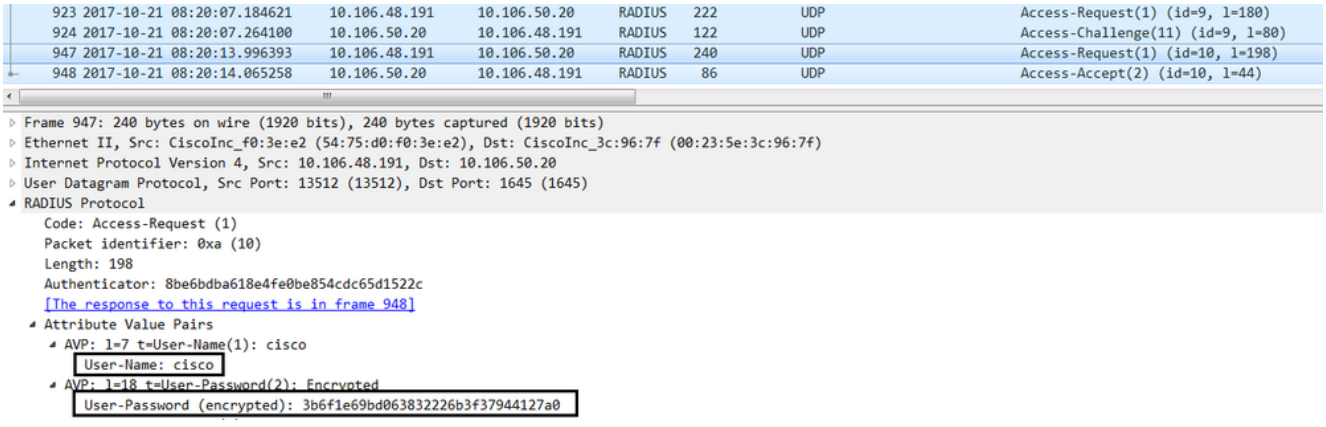
2. 使用者輸入憑證後，身份驗證請求（訪問請求資料包）將從ASA轉發到AAA伺服器。



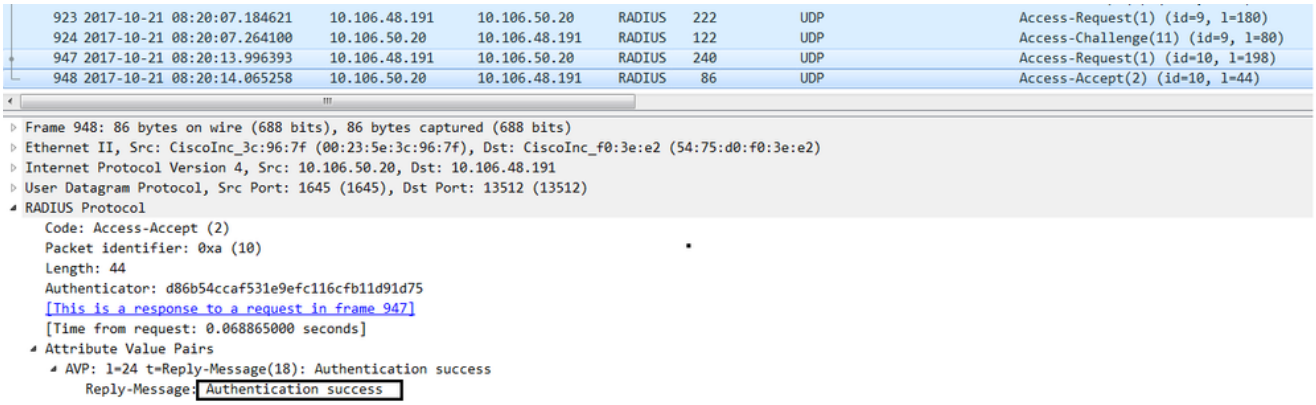
3. 身份驗證請求到達AAA伺服器後，將驗證憑證。如果密碼正確，AAA伺服器會使用Access-Challenge（訪問質詢）回覆，詢問使用者輸入一次性密碼。 如果憑證不正確，則會向ASA傳送Access-Reject資料包。



4. 當使用者輸入一次性密碼時，將以Access-Request資料包的形式向AAA伺服器傳送身份驗證請求



5. 在AAA伺服器上成功驗證一次性密碼後，從伺服器向ASA傳送Access-Accept資料包，使用者成功通過身份驗證，從而完成雙重身份驗證過程。



Anyconnect許可證資訊

以下連結指向有關Cisco AnyConnect安全移動客戶端許可證的有用資訊：

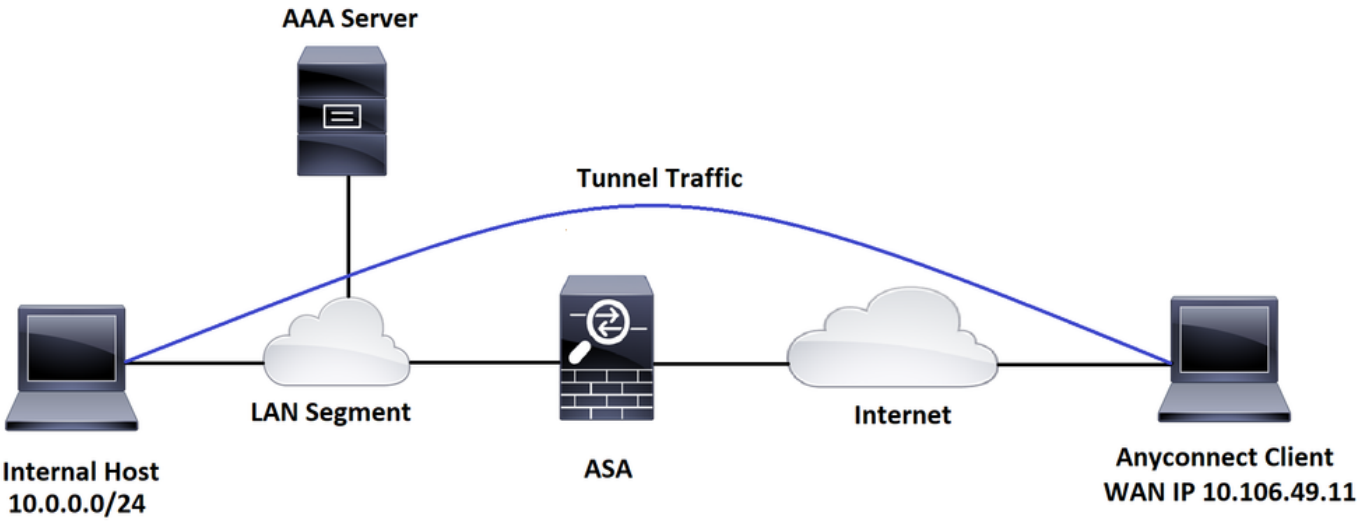
- 有關AnyConnect許可的常見問題，請參閱本文。
- 有關AnyConnect Apex和Plus許可證的資訊，請參閱《Cisco AnyConnect訂購指南》。

設定

本節介紹如何在ASA上配置Cisco AnyConnect安全移動客戶端。

註：使用命令查詢工具(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表



ASDM AnyConnect配置嚮導

AnyConnect配置嚮導可用於配置AnyConnect安全移動客戶端。繼續進行之前，請確保AnyConnect客戶端軟體包已上載到ASA防火牆的快閃記憶體/磁碟。

完成以下步驟，以便通過配置嚮導配置Anyconnect安全移動客戶端：

有關通過ASDM的拆分隧道配置，要下載和安裝AnyConnect，請參閱本文檔。
[AnyConnect安全行動化使用者端]

ASA CLI配置

本節提供Cisco AnyConnect安全移動客戶端的CLI配置以供參考。

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

有關在ASA上為AnyConnect客戶端連線配置和安裝第三方證書的資訊，請參閱本文檔。

配置ASA SSL數位證書

驗證

使用本節內容，確認您的組態是否正常運作。

> **註**:Output Interpreter Tool(僅供已註冊客戶)支援某些**show**命令。使用Output Interpreter工具檢視**show**指令輸出的分析。

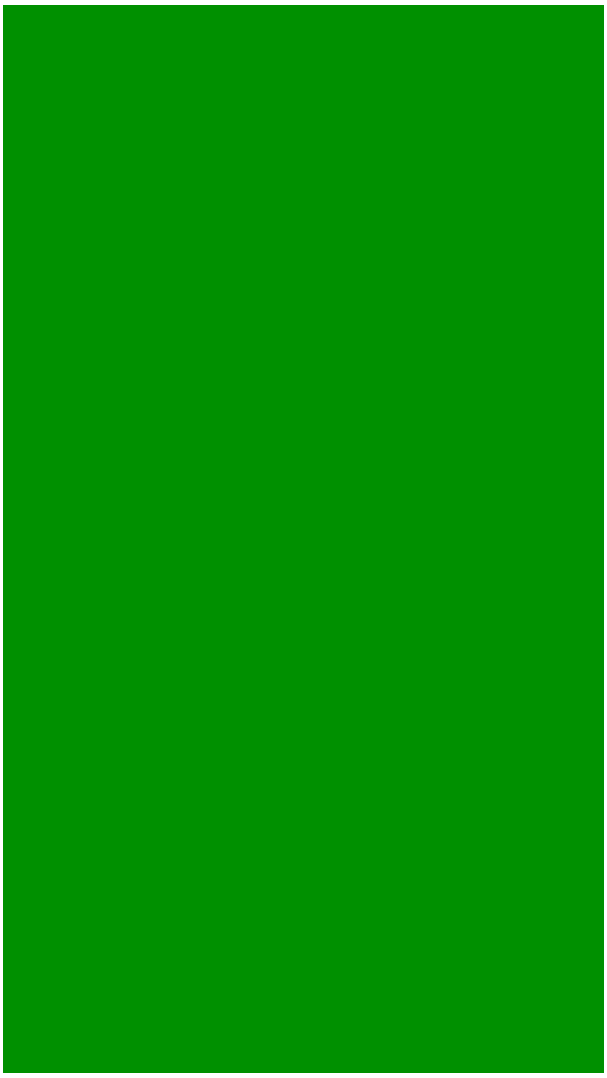
可以執行這些show命令以確認AnyConnect客戶端及其統計資訊的狀態。

```
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
```

使用者體驗



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

注意：在ASA上，您可以設定各種調試級別；預設情況下，使用級別1。如果更改調試級別，調試的詳細程度可能會增加。請謹慎執行此操作，尤其是在生產環境中。

要對傳入AnyConnect客戶端連線的完整身份驗證過程進行故障排除，可以使用以下調試：

- debug radius all
- 調試aaa身份驗證
- debug wrbvpn anyconnect

這些命令用於確認使用者憑證是否正確。

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

如果使用者名稱和密碼正確，

```
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
```

最後一個錯誤與以下事實有關：由於AAA伺服器要求使用者在成功驗證使用者名稱和密碼後輸入一次性密碼，並且此測試不涉及使用者主動輸入OTP，因此您會看到AAA伺服器傳送的訪問質詢響應，而ASA上未出現任何錯誤。

如果使用者名稱和/或密碼不正確，

```
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
```

工作設定中的調試如下所示：

圖例

AnyConnect Client Real IP:10.106.49.111

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
```

相關資訊

- 使用 ASA 上的分割通道設定 AnyConnect Secure Mobility 用戶端
- Cisco IOS頭端配置上AnyConnect客戶端的RSA SecurID身份驗證
- ASA和ACS的RSA令牌伺服器和SDI協定使用情況
- 《 ASA AnyConnect Double Authentication with Certificate Validation， Mapping， and Pre-Fill配置指南》
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。