AnyConnectセキュアモビリティクライアントをワンタイムパスワードで設定する

内容

概要

このドキュメントでは、適応型セキュリティアプライアンス(ASA)Cisco AnyConnectセキュアモビリティクライアントアクセスの設定例について説明します。

前提条件

要件

このドキュメントでは、ASAが完全に動作していて、Cisco Adaptive Security Device Manager(ASDM)またはコマンドラインインターフェイス(CLI)で設定を変更できるように設定されていることを前提としています。

次の項目に関する知識があることが推奨されます。

- ASAのCLIおよびASDMに関する基礎知識
- Cisco ASAヘッドエンドでのSSLVPNの設定
- 2要素認証の基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco適応型セキュリティアプライアンスASA5506
- Cisco 適応型セキュリティ アプライアンス ソフトウェア バージョン 9.6(1)
- Adaptive Security Device Manager(ASDM)バージョン7.8
- AnyConnect バージョン 4.5.02033

注:AnyConnect VPN Clientパッケージ(anyconnect-win*.pkg)をCisco Software Download(登録ユーザ専用)からダウンロードします。AnyConnect VPNクライアントをASAのフラッシュメモリにコピーします。このフラッシュメモリは、ASAとのSSL VPN接続を確立するためにリモートユーザコンピュータにダウンロードされます。詳細については、ASA コンフィギュレーション ガイドの「AnyConnect クライアントのインストール」を参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

適応型セキュリティアプライアンス(ASA)Cisco AnyConnectセキュアモビリティクライアントアクセスは、ワンタイムパスワード(OTP)を使用した2要素認証を使用します。AnyConnectユーザが正常に接続するには、正しいクレデンシャルとトークンを入力する必要があります。

2要素認証では、2つの異なる認証方式が使用されます。これらのうちどれでも使用できます。

- 知っているもの
- 持っているもの
- 自分が何者か

一般に、ユーザが知っていること（ユーザ名とパスワード）と、ユーザが持っているもの（たとえば、トークンや証明書のように個人だけが所有する情報の実体）で構成されます。これは、ASAのローカルデータベースまたはASAと統合されたActive Directory(AD)サーバに保存されたクレデンシャルを使用してユーザを認証する従来の認証設計よりも安全です。ワンタイムパスワードは、ネットワークアクセスを保護するための2要素認証の最も単純で最も一般的な形式の1つです。たとえば、大企業では、仮想プライベートネットワーク(VPN)アクセスで、リモートユーザ認証にワンタイムパスワード(OTP)トークンを使用する必要があります。

このシナリオでは、ASAとAAAサーバ間の通信にRADIUSプロトコルを使用するAAAサーバとしてOpenOTP認証サーバを使用します。ユーザクレデンシャルは、Google Authenticator Applicationサービスに関連付けられたOpenOTPサーバ上で、2要素認証用のソフトトークンとして設定されます。

OpenOTPの設定は、このドキュメントの範囲外であるため、ここでは説明しません。これらのリンクをチェックすると、さらに詳しい情報を得ることができます。

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

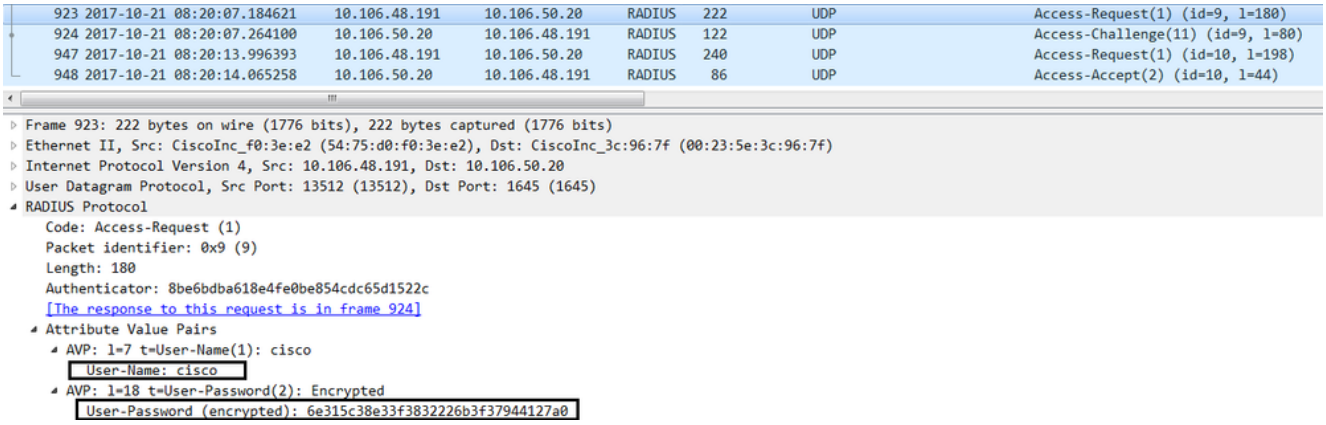
OpenOTP認証用のASAの設定
https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/

パケット フロー

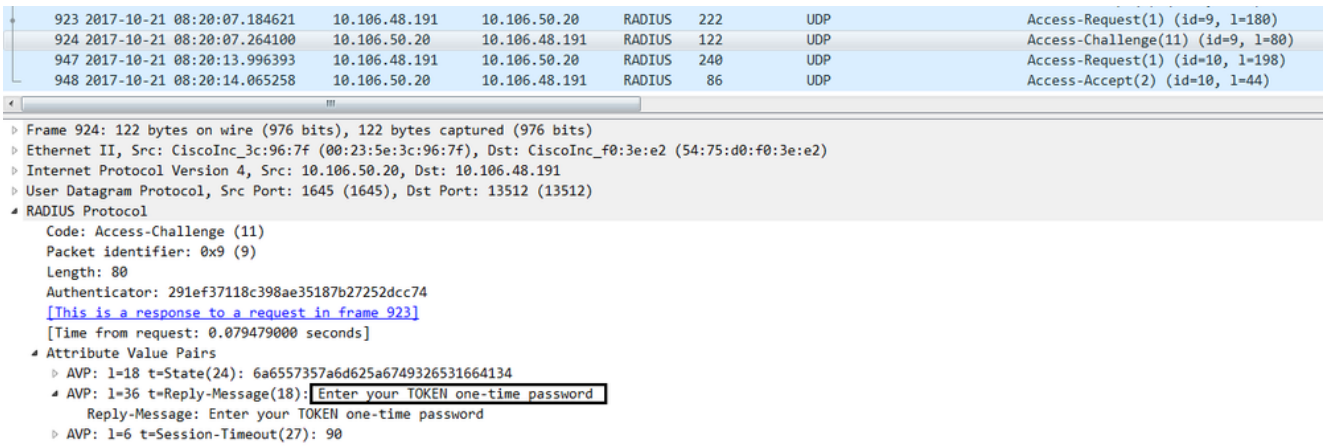
このパケットキャプチャは、10.106.50.20のAAAサーバに接続されたASAの外部インターフェイスで取得されました。

1. AnyConnectユーザがASAへのクライアント接続を開始し、設定されているグループURLとグループエイリアスに応じて、接続は特定のトンネルグループ（接続プロファイル）に到達します。この時点で、ユーザはクレデンシャルの入力を求められます。

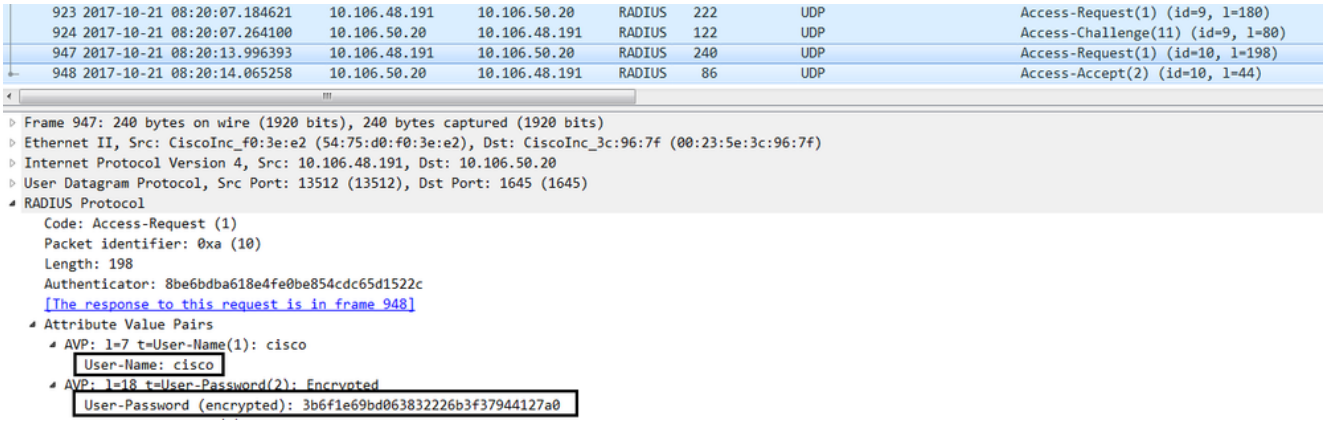
2. ユーザがクレデンシャルを入力すると、認証要求（Access-Requestパケット）がASAからAAAサーバに転送されます。



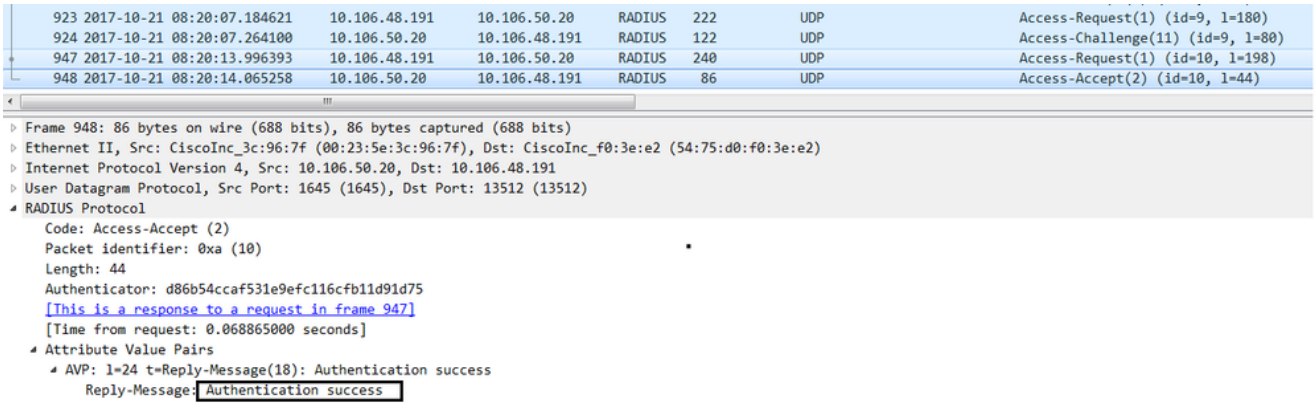
3. 認証要求がAAAサーバに到達すると、クレデンシャルが検証されます。正しい場合、AAAサーバはAccess-Challengeで応答し、ユーザにワンタイムパスワードの入力を求めます。 クレデンシャルが正しくない場合は、Access-RejectパケットがASAに送信されます。



4. ユーザがワンタイムパスワードを入力すると、Access-Requestパケットの形式の認証要求がASAからAAAサーバに送信されます



5. AAAサーバでワンタイムパスワードが正常に検証されると、サーバからASAにAccess-Acceptパケットが送信され、ユーザが正常に認証されて、2要素認証プロセスが完了します。



AnyConnect のライセンス情報

Cisco AnyConnect セキュア モビリティ クライアントのライセンスに関する役立つ情報へのリンクを次に示します。

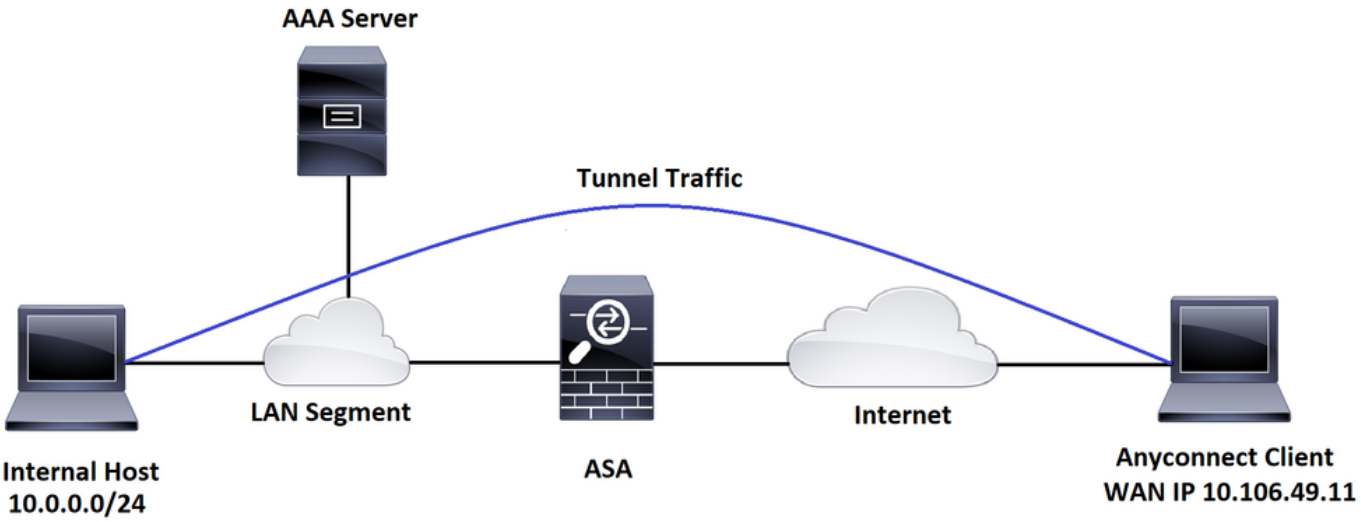
- AnyConnectのライセンスに関するFAQについては、このドキュメントを参照してください。
- AnyConnect Apex および Plus のライセンスの詳細については、『Cisco AnyConnect 発注ガイド』を参照してください。

設定

ここでは、ASA で Cisco AnyConnect セキュア モビリティ クライアントを設定する方法について説明します。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を使用してください。

ネットワーク図



ASDM AnyConnect 構成ウィザード

AnyConnect セキュア モビリティ クライアントの設定には、AnyConnect 設定ウィザードを使用できます。先に進む前に、AnyConnect クライアント パッケージが ASA ファイアウォールのフラッシュまたはディスクにアップロードされていることを確認します。

構成ウィザードを使用して AnyConnect セキュア モビリティ クライアントを設定するために、次の手順を実行します。

ASDMを使用したスプリットトンネルの設定で、AnyConnectをダウンロードしてインストールするには、このドキュメントを参照してください。
AnyConnect セキュア モビリティ クライアント

ASA CLI の設定

ここでは、参考までに Cisco AnyConnect セキュア モビリティ クライアントの CLI 設定の例を示します。

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

AnyConnectクライアント接続用にASAでサードパーティ証明書を設定およびインストールする方法については、このドキュメントを参照してください。

ASA SSLデジタル証明書の設定

確認

ここでは、設定が正常に機能しているかどうかを確認します。

> **注**：特定のshowコマンドは、Output Interpreter Tool(登録ユーザ専用)でサポートされています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

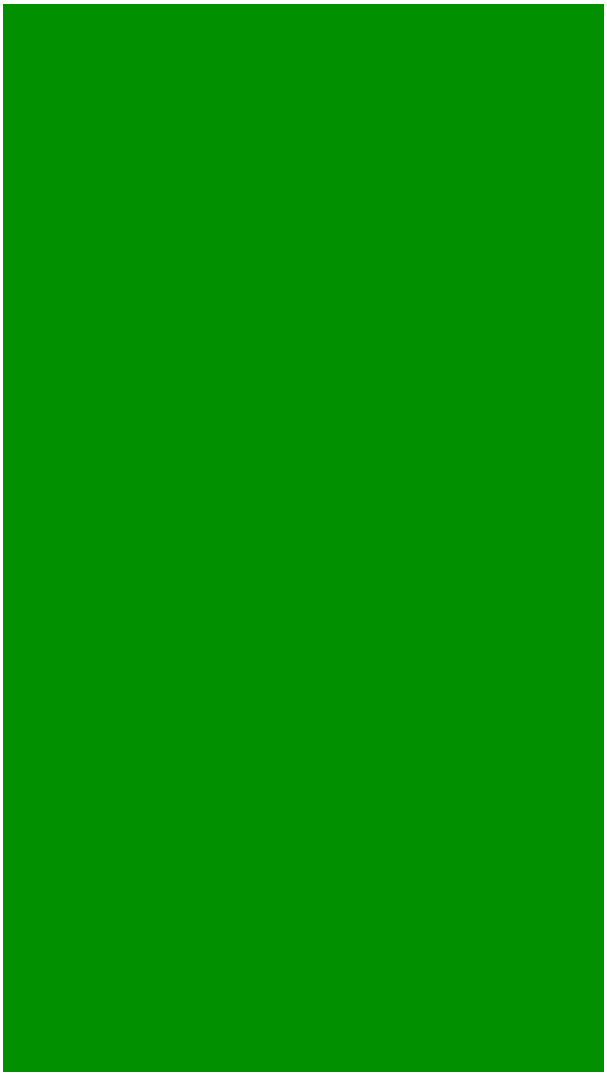
これらのshowコマンドを実行すると、AnyConnectクライアントのステータスとその統計情報を確認できます。

```
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 : 0000000000000100059f9de6d

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 : 0000000000000100059f9de6d

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
```

ユーザ エクスペリエンス



トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

> **注：debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。**

> **注意**:ASAでは、さまざまなデバッグレベルを設定できます。デフォルトでは、レベル1が使用されます。デバッグレベルを変更すると、デバッグの冗長性が高まる可能性があります。特に実稼働環境では、注意して実行してください。

着信AnyConnectクライアント接続の完全な認証プロセスをトラブルシューティングするには、次のデバッグを使用できます。

- debug radius all
- aaa 認証のデバッグ
- debug wrbvpn anyconnect

これらのコマンドは、ユーザクレデンシャルが正しいかどうかを確認します。

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

ユーザ名とパスワードが正しい場合は、

```
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
```

最後のエラーは、ユーザ名とパスワードの認証が成功した後にAAAサーバがユーザがワンタイムパスワードを入力することを想定しており、このテストではユーザがOTPにアクティブに入る必要がないため、ASAでエラーが発生しない応答としてAAAサーバから送信されたAccess-Challengeが表示されるという事実に関係しています。

ユーザ名やパスワードが正しくない場合は、

```
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
```

作業セットアップからのデバッグは次のようになります。

凡例

AnyConnectクライアントの実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
```

関連情報

- ASA でのスプリット トンネリングによる AnyConnect セキュア モビリティ クライアントの設定
- Cisco IOSヘッドエンドでの AnyConnectクライアント用のRSA SecurID認証の設定
- ASA および ACS における RSA トークン サーバおよび SDI プロトコルの使用
- 証明書の検証による ASA AnyConnect の二重認証、マッピング、およびプレフィル コンフィギュレーション ガイド
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。