Configure AnyConnect Secure Mobility Client with One-Time Password

Contents

Introduction

This document describes a configuration example for Adaptive Security Appliance (ASA) Cisco AnyConnect Secure Mobility Client access.

Prerequisites

Requirements

This document assumes that the ASA is fully operational and configured to allow the Cisco Adaptive Security Device Manager (ASDM) or Command Line Interface (CLI) to make configuration changes.

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of ASA's CLI and ASDM
- SSLVPN configuration on the Cisco ASA Head End
- Basic knowledge of Two Factor Authentication

Components Used

This information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance ASA5506
- Cisco Adaptive Security appliance Software Version 9.6(1)
- Adaptive Security Device Manager Version 7.8(2)
- AnyConnect Version 4.5.02033

> **Note**: Download the AnyConnect VPN Client package (anyconnect-win*.pkg) from the Cisco Software Download (registered customers only). Copy the AnyConnect VPN client to the ASA's flash memory, which is downloaded to the remote user computers in order to establish the SSL VPN connection with the ASA. Refer to the Installing the AnyConnect Client section of the ASA configuration guide for more information.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Adaptive Security Appliance (ASA) Cisco AnyConnect Secure Mobility Client access uses two-factor authentication with the help of One-Time Password (OTP). One must provide the correct credentials and token for an AnyConnect user to connect successfully.

Two-factor authentication utilizes two different authentication methods which can be any 2 of these.

- Something you know
- Something you have
- Something you are

In general, it comprises something a user knows (username and password), and something a user has (for example, an entity of information that only an individual owns like a token or certificate). This is more secure than traditional authenciation designs where a user authenticates via credentials stored either on ASA's local database or Active Directory (AD) Server integrated with ASA. One-Time Password is one of hte simplest and most popular forms of two-factor authentication for securing network access. For example, in large enterprises, Virtual Private Network access often requires the use of One-Time Passwrod tokens for remote user authentication.

In this scenario, you use OpenOTP authenication server as AAA server which uses radius protocol for communication between ASA and AAA server. User credentials are configures on the OpenOTP server which is associated with Google Authenticator Application servicing as a soft token for the two-factor authentication.

OpenOTP configuration is not covered here as it is outside the scope of this document. You can check these links for further reading.

Setting up OpenOTP
https://www.rcdevs.com/docs/howtos/openotp_quick_start/openotp_quick_start/

Configuring ASA for OpenOTP authentication
https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/

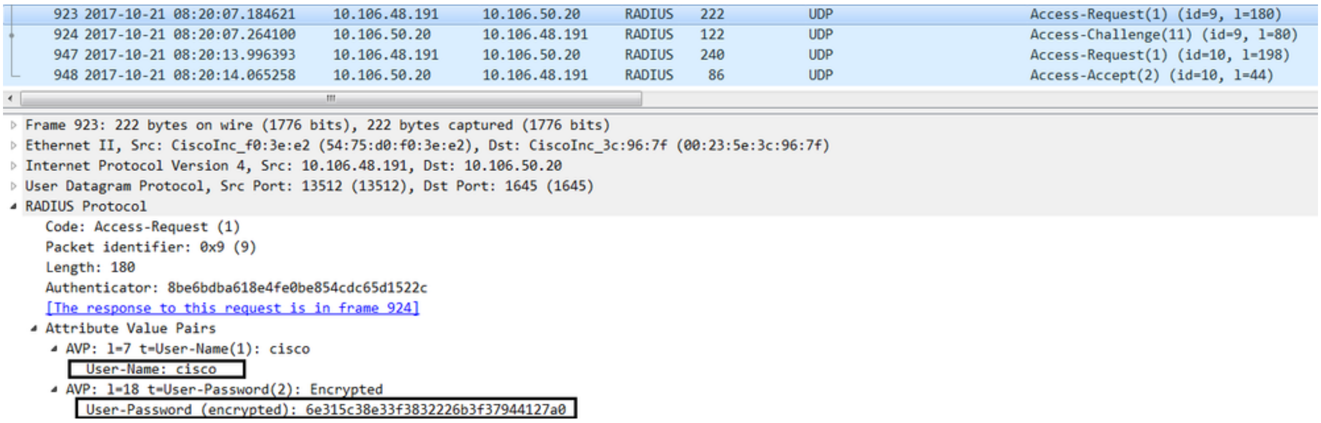
Packet Flow

This packet capture was taken on ASA's outside interface connected to AAA server at 10.106.50.20.

1. AnyConect user initiates client connection towards ASA and depends on the group-url and group-alias configured, the connection lands on a specific tunnel-group (connection profile). At this point, the

user is prompted to enter the credentials.

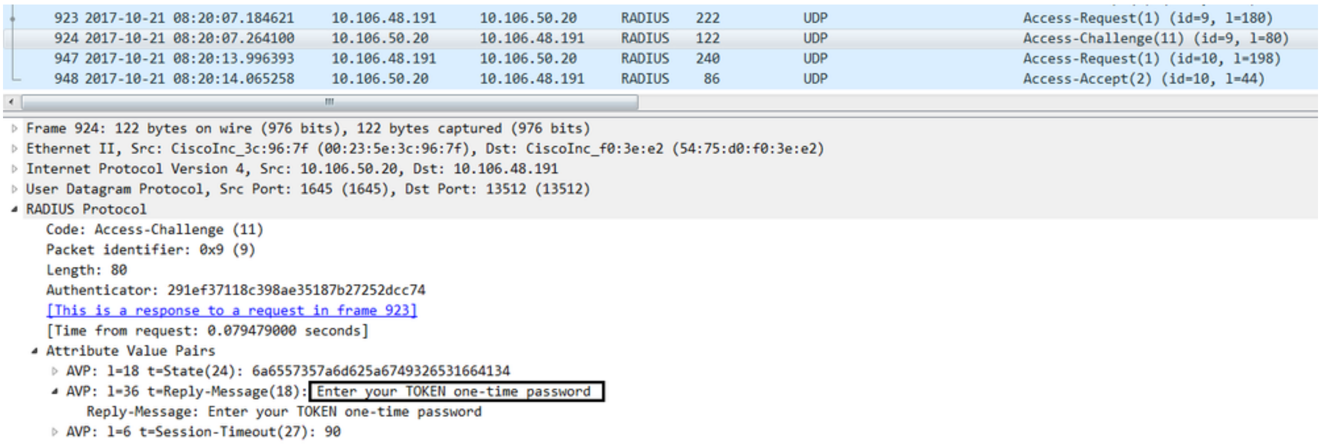
2. Once the user enters the credentials, the authentication request (Access-Request packet) is forwarded to AAA server from the ASA.



```
923 2017-10-21 08:20:07.184621   10.106.48.191   10.106.50.20    RADIUS  222   UDP   Access-Request(1) (id=9, l=180)
924 2017-10-21 08:20:07.264100   10.106.50.20    10.106.48.191   RADIUS  122   UDP   Access-Challenge(11) (id=9, l=80)
947 2017-10-21 08:20:13.996393   10.106.48.191   10.106.50.20    RADIUS  240   UDP   Access-Request(1) (id=10, l=198)
948 2017-10-21 08:20:14.065258   10.106.50.20    10.106.48.191   RADIUS   86   UDP   Access-Accept(2) (id=10, l=44)

▷ Frame 923: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits)
▷ Ethernet II, Src: CiscoInc_f0:3e:e2 (54:75:d0:f0:3e:e2), Dst: CiscoInc_3c:96:7f (00:23:5e:3c:96:7f)
▷ Internet Protocol Version 4, Src: 10.106.48.191, Dst: 10.106.50.20
▷ User Datagram Protocol, Src Port: 13512 (13512), Dst Port: 1645 (1645)
◢ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x9 (9)
    Length: 180
    Authenticator: 8be6bdba618e4fe0be854cdc65d1522c
    [The response to this request is in frame 924]
  ◢ Attribute Value Pairs
    ◢ AVP: l=7 t=User-Name(1): cisco
        User-Name: cisco
    ◢ AVP: l=18 t=User-Password(2): Encrypted
        User-Password (encrypted): 6e315c38e33f3832226b3f37944127a0
```

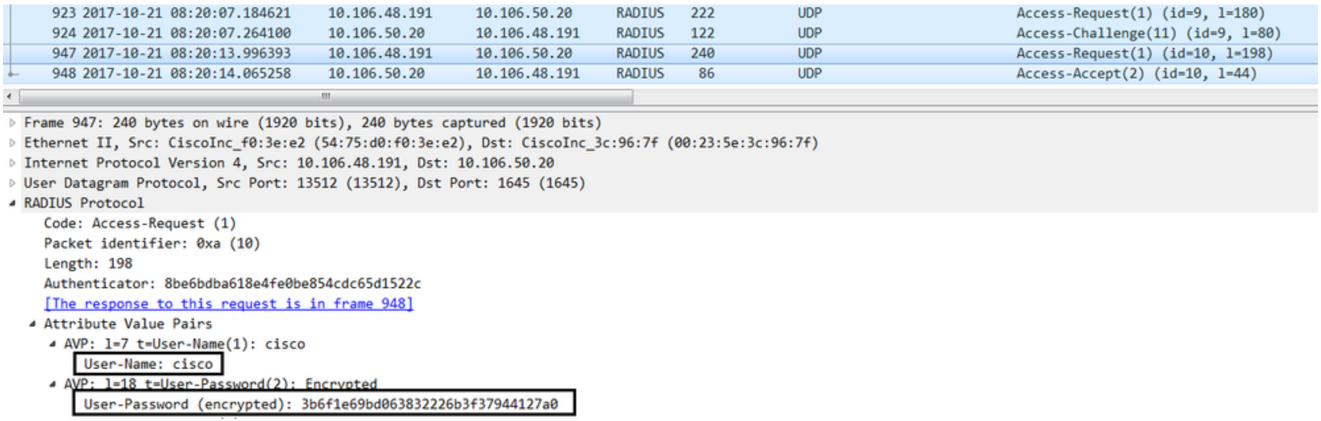
3. After the authentication request reaches AAA server, it validates the credentials. If they are correct, AAA server replies with an Access-Challenge where the user is asked to enter a one-time password. In case of incorrect credentials, an Access-Reject packet is sent to the ASA.



```
923 2017-10-21 08:20:07.184621   10.106.48.191   10.106.50.20    RADIUS  222   UDP   Access-Request(1) (id=9, l=180)
924 2017-10-21 08:20:07.264100   10.106.50.20    10.106.48.191   RADIUS  122   UDP   Access-Challenge(11) (id=9, l=80)
947 2017-10-21 08:20:13.996393   10.106.48.191   10.106.50.20    RADIUS  240   UDP   Access-Request(1) (id=10, l=198)
948 2017-10-21 08:20:14.065258   10.106.50.20    10.106.48.191   RADIUS   86   UDP   Access-Accept(2) (id=10, l=44)

▷ Frame 924: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
▷ Ethernet II, Src: CiscoInc_3c:96:7f (00:23:5e:3c:96:7f), Dst: CiscoInc_f0:3e:e2 (54:75:d0:f0:3e:e2)
▷ Internet Protocol Version 4, Src: 10.106.50.20, Dst: 10.106.48.191
▷ User Datagram Protocol, Src Port: 1645 (1645), Dst Port: 13512 (13512)
◢ RADIUS Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0x9 (9)
    Length: 80
    Authenticator: 291ef37118c398ae35187b27252dcc74
    [This is a response to a request in frame 923]
    [Time from request: 0.079479000 seconds]
  ◢ Attribute Value Pairs
    ▷ AVP: l=18 t=State(24): 6a6557357a6d625a6749326531664134
    ◢ AVP: l=36 t=Reply-Message(18): Enter your TOKEN one-time password
        Reply-Message: Enter your TOKEN one-time password
    ▷ AVP: l=6 t=Session-Timeout(27): 90
```

4. As the user enters the one-time password, the authentication request in the form of Access-Request packet is sent from the ASA to the AAA server

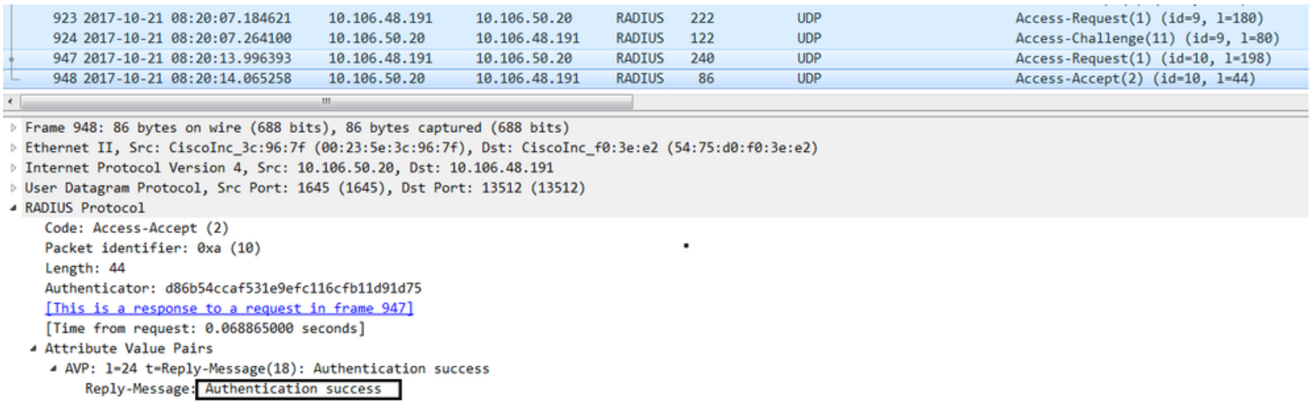


```
923 2017-10-21 08:20:07.184621   10.106.48.191   10.106.50.20    RADIUS  222   UDP   Access-Request(1) (id=9, l=180)
924 2017-10-21 08:20:07.264100   10.106.50.20    10.106.48.191   RADIUS  122   UDP   Access-Challenge(11) (id=9, l=80)
947 2017-10-21 08:20:13.996393   10.106.48.191   10.106.50.20    RADIUS  240   UDP   Access-Request(1) (id=10, l=198)
948 2017-10-21 08:20:14.065258   10.106.50.20    10.106.48.191   RADIUS   86   UDP   Access-Accept(2) (id=10, l=44)

▷ Frame 947: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits)
▷ Ethernet II, Src: CiscoInc_f0:3e:e2 (54:75:d0:f0:3e:e2), Dst: CiscoInc_3c:96:7f (00:23:5e:3c:96:7f)
▷ Internet Protocol Version 4, Src: 10.106.48.191, Dst: 10.106.50.20
▷ User Datagram Protocol, Src Port: 13512 (13512), Dst Port: 1645 (1645)
◢ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0xa (10)
    Length: 198
    Authenticator: 8be6bdba618e4fe0be854cdc65d1522c
    [The response to this request is in frame 948]
  ◢ Attribute Value Pairs
    ◢ AVP: l=7 t=User-Name(1): cisco
        User-Name: cisco
    ◢ AVP: l=18 t=User-Password(2): Encrypted
        User-Password (encrypted): 3b6f1e69bd063832226b3f37944127a0
```

5. Once the one-time password is successfully validated on the AAA server, an Access-Accept packet is

sent from the server to the ASA, the user is successfully authenticated and this completes the two-factor authentication process.



```
  923 2017-10-21 08:20:07.184621   10.106.48.191   10.106.50.20    RADIUS   222   UDP   Access-Request(1) (id=9, l=180)
  924 2017-10-21 08:20:07.264100   10.106.50.20    10.106.48.191   RADIUS   122   UDP   Access-Challenge(11) (id=9, l=80)
  947 2017-10-21 08:20:13.996393   10.106.48.191   10.106.50.20    RADIUS   240   UDP   Access-Request(1) (id=10, l=198)
  948 2017-10-21 08:20:14.065258   10.106.50.20    10.106.48.191   RADIUS    86   UDP   Access-Accept(2) (id=10, l=44)

▷ Frame 948: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▷ Ethernet II, Src: CiscoInc_3c:96:7f (00:23:5e:3c:96:7f), Dst: CiscoInc_f0:3e:e2 (54:75:d0:f0:3e:e2)
▷ Internet Protocol Version 4, Src: 10.106.50.20, Dst: 10.106.48.191
▷ User Datagram Protocol, Src Port: 1645 (1645), Dst Port: 13512 (13512)
◢ RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0xa (10)
    Length: 44
    Authenticator: d86b54ccaf531e9efc116cfb11d91d75
    [This is a response to a request in frame 947]
    [Time from request: 0.068865000 seconds]
  ◢ Attribute Value Pairs
    ◢ AVP: l=24 t=Reply-Message(18): Authentication success
        Reply-Message: Authentication success
```

Anyconnect License Information

Here are some links to useful information about the Cisco AnyConnect Secure Mobility Client licenses:

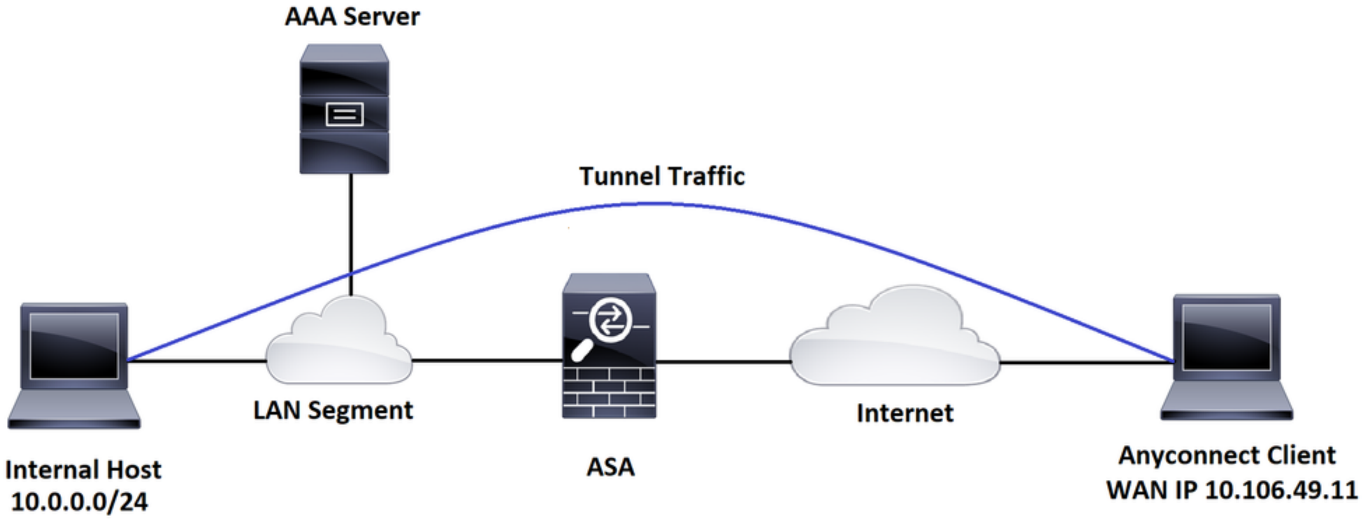
- Refer to this document for frequently asked AnyConnect licensing questions.
- Refer to the Cisco AnyConnect Ordering Guide for information about AnyConnect Apex and Plus licenses.

Configure

This section describes how to configure the Cisco AnyConnect Secure Mobility Client on the ASA.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram



ASDM AnyConnect Configuration Wizard

The AnyConnect Configuration Wizard can be used in order to configure the AnyConnect Secure Mobility Client. Ensure that an AnyConnect client package has been uploaded to the flash/disk of the ASA Firewall before you proceed.

Complete these steps in order to configure the Anyconnect Secure Mobility Client via the Configuration Wizard:

For split tunnel configuration via ASDM, to download and install AnyConnect, please refer to this document.

[AnyConnect Secure Mobility Client]

ASA CLI Configuration

This section provides the CLI configuration for the Cisco anyConnect Secure Mobility Client for reference purposes.

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

For configuring and installing a third-party certificate on the ASA for AnyConnect client connections, refer to this document.

Configure ASA SSL Digital Certificate

Verify

Use this section in order to confirm that your configuration works properly.

> **Note**: The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

These show commands can be executed to confirm the status of AnyConnect client and its statistics.

```
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
```

User Experience

> : On the ASA, you can set various debug levels; by default, level 1 is used. If you change the debug level, the verbosity of the debugs can increase. Do this with caution, especially in production environments.

To troubleshoot the complete authentication process for an incoming AnyConnect client connection, you can use these debugs:

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

These commands confirm the user credentials are correct or not.

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

In case of correct username and password,

```
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
```

The last error pertains to the fact that since the AAA server expects the user to enter one-time password post successful authentication of username and password, and this test does not involve a user actively entering OTP, you see Access-Challenge sent by AAA server in response to which no error is seen on the ASA.

In case of incorrect username and/or password,

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

Username: cisco

Password: ***

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

ERROR: Authentication Rejected: AAA failure
```

Debugs from a work setup look something like this:

Legend

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
```

Related Information

- Configure AnyConnect Secure Mobility Client with Split Tunneling on an ASA
- RSA SecurID Authentication for AnyConnect Clients on a Cisco IOS Headend Configuration
- RSA Token Server and SDI Protocol Usage for ASA and ACS
- ASA AnyConnect Double Authentication with Certificate Validation, Mapping, and Pre-Fill Configuration Guide
- Technical Support & Documentation - Cisco Systems