

Configure AnyConnect Secure Mobility Client mediante una contraseña única (OTP) para la autenticación de dos factores en un ASA

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo de paquetes](#)

[Configurar](#)

[Diagrama de la red](#)

[Verificación](#)

[Experiencia del usuario](#)

[Troubleshoot](#)

[Leyenda:](#)

[Información Relacionada](#)

Introducción

Este documento describe un ejemplo de configuración para el acceso Cisco AnyConnect Secure Mobility Client de Adaptive Security Appliance (ASA) que utiliza autenticación de dos factores con la ayuda de One-Time Password (OTP). Uno debe proporcionar las credenciales y el token correctos para que un usuario de AnyConnect se conecte correctamente.

Colaborado por Dinesh Moudgil, ingeniero de Cisco HTTS.

prerrequisitos

Requisitos

Este documento asume que el ASA está completamente operativo y configurado para permitir que el Cisco Adaptive Security Device Manager (ASDM) o la interfaz de línea de comandos (CLI) realice cambios en la configuración.

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de ASA CLI y ASDM
- Configuración de SSLVPN en el terminal Cisco ASA
- Conocimiento básico de la autenticación de dos factores

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

Dispositivo de seguridad adaptable Cisco ASA5506

Software Cisco Adaptive Security Appliance versión 9.6(1)

Adaptive Security Device Manager versión 7.8(2)

AnyConnect versión 4.5.02033

Nota: Descargue el paquete de AnyConnect VPN Client (anyconnect-win*.pkg) de Descarga de Cisco Software (sólo clientes registrados). Copie el AnyConnect VPN client en la memoria flash ASA, que será descargada a los equipos de los usuarios remotos para establecer la conexión SSL VPN con el ASA. Consulte la sección Instalación de AnyConnect Client de la guía de configuración ASA para obtener más información.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

La autenticación de dos factores utiliza dos métodos de autenticación diferentes que pueden ser cualquiera de los dos siguientes: "algo que usted sabe", "algo que usted tiene" y "algo que usted es".

En general, se compone de algo que un usuario conoce (nombre de usuario y contraseña) y algo que un usuario tiene (es decir, una entidad de información que sólo posee una persona, por ejemplo, un token o un certificado). Esto es más seguro que los diseños de autenticación tradicionales en los que un usuario se autentica mediante credenciales almacenadas en la base de datos local de ASA o en el servidor de Active Directory (AD) integrado con ASA. La contraseña de una sola vez es una de las formas más simples y populares de autenticación de dos factores para proteger el acceso a la red. Por ejemplo, en las grandes empresas, el acceso a la red privada virtual suele requerir el uso de tokens de contraseña única para la autenticación de usuarios remotos.

En esta situación, estamos utilizando el servidor de autenticación OpenOTP como servidor AAA que utiliza el protocolo RADIUS para la comunicación entre ASA y el servidor AAA. Las credenciales de usuario se configuran en el servidor OpenOTP que está asociado con el servicio de la aplicación Google Authenticator como un token de software para la autenticación de dos factores.

La configuración de OpenOTP no se trata aquí porque está fuera del alcance de este documento. Puede consultar los siguientes enlaces para obtener más información:-

Configuración de OpenOTP

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

Configuración de ASA para la autenticación OpenOTP

https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/

Flujo de paquetes

La siguiente captura de paquetes se realizó en la interfaz externa del ASA conectada al servidor AAA a 10.106.50.20.

1. El usuario de AnyConnect inicia la conexión del cliente hacia ASA y, en función de la dirección URL del grupo y el alias del grupo configurados, la conexión aterriza en un grupo de túnel específico (perfil de conexión). En este momento, se le solicita al usuario que introduzca las credenciales.
2. Una vez que el usuario ingresa las credenciales, la solicitud de autenticación (paquete de solicitud de acceso) se reenvía al servidor AAA desde el ASA.

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Details
923	2017-10-21 08:20:07.184621	10.106.48.191	10.106.50.20	RADIUS	222			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			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			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			Access-Accept(2) (id=10, l=44)


```
Frame 923: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface
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. Después de que la solicitud de autenticación llegue al servidor AAA, valida las credenciales. Si son correctos, el servidor AAA responde con un Desafío de acceso donde se le pide al usuario que introduzca una contraseña de una sola vez. En caso de credenciales incorrectas, se envía un paquete Access-Reject al ASA.

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Details
923	2017-10-21 08:20:07.184621	10.106.48.191	10.106.50.20	RADIUS	222			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			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			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			Access-Accept(2) (id=10, l=44)


```
Frame 924: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface
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. A medida que el usuario ingresa la contraseña de una sola vez, la solicitud de autenticación en forma de paquete Access-Request se envía desde el ASA al servidor AAA

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. Una vez que la contraseña de una sola vez se valida correctamente en el servidor AAA, se envía un paquete Access-Accept del servidor al ASA, el usuario se autentica correctamente y esto completa el proceso de autenticación de dos factores.

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: d86b54ccaf531e9efc116c11d91d75
  [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

```

Información de licencia de Anyconnect

Estos son algunos enlaces a información útil sobre las licencias de Cisco AnyConnect Secure Mobility Client:

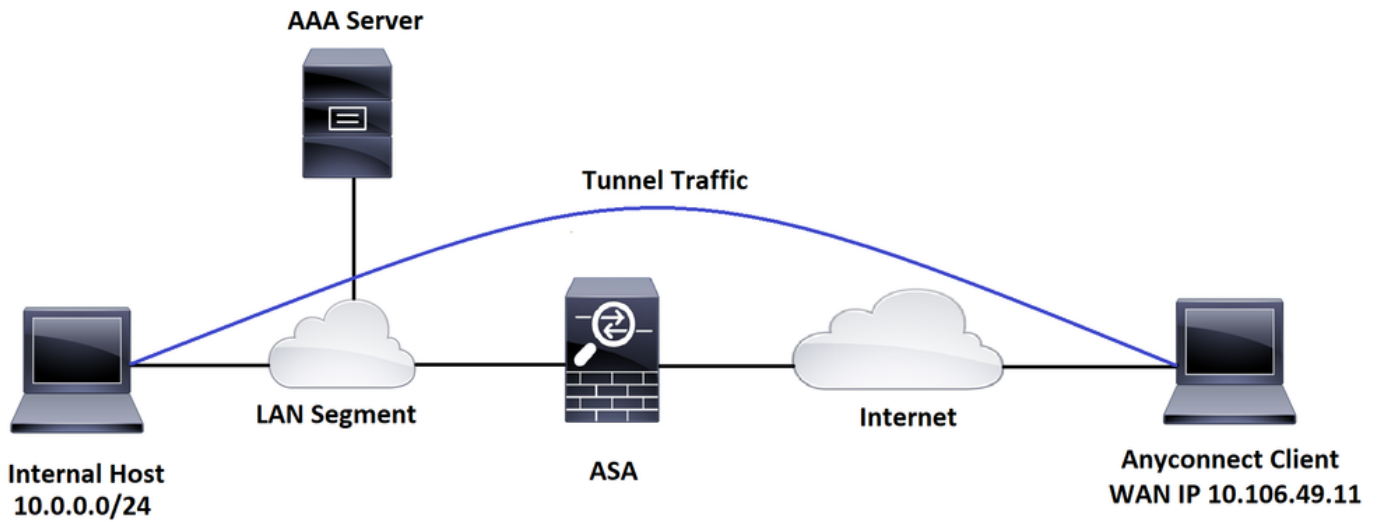
- Consulte [este documento](#) para ver las preguntas frecuentes sobre licencias de AnyConnect.
- Refiérase a la [Guía de Pedidos de Cisco AnyConnect](#) para obtener información sobre las licencias AnyConnect Apex y Plus.

Configurar

Esta sección describe cómo configurar Cisco AnyConnect Secure Mobility Client en ASA.

Nota: Use la Command Lookup Tool ([clientes registrados solamente](#)) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



Asistente para la configuración de ASDM AnyConnect

El Asistente para la configuración de AnyConnect se puede utilizar para configurar AnyConnect Secure Mobility Client. Asegúrese de que se ha cargado un paquete de cliente AnyConnect en la memoria flash/disco del firewall ASA antes de continuar.

Complete estos pasos para configurar AnyConnect Secure Mobility Client a través del asistente de configuración:

Para la configuración de túnel dividido a través de ASDM, la descarga e instalación de AnyConnect, consulte el siguiente documento:-

<https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/119006-configure-anyconnect-00.html#anc8>

Configuración CLI ASA

Esta sección proporciona la configuración CLI de Cisco AnyConnect Secure Mobility Client para fines de referencia.

```
!-----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) Configuraiton-----

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
```

Nota:

Para configurar e instalar un certificado de terceros en el ASA para las conexiones de cliente AnyConnect, consulte el siguiente documento:-

<https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-1.html>

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Nota:La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show.Utilice la herramienta para ver una análisis de información de salida del comando show.

Los siguientes comandos show se pueden ejecutar para confirmar el estado del cliente AnyConnect y sus estadísticas.

```
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

Experiencia del usuario



Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Nota: Consulte [Información Importante sobre Comandos de Debug antes de usar un comando debug.](#)

Precaución: En el ASA, puede establecer varios niveles de depuración; de forma predeterminada, se utiliza el nivel 1. Si cambia el nivel de depuración, la verbosidad de las depuraciones podría aumentar. Haga esto con precaución, especialmente en entornos de producción.

Para resolver problemas del proceso de autenticación completo para una conexión de cliente AnyConnect entrante, puede utilizar estos debugs:

- debug radius all

- debug aaa authentication
- debug webvpn anyconnect

El siguiente comando confirma que las credenciales del usuario son correctas o no.

```
test aaa-server authentication <aaa_server_group> [host <name>|<host_ip>] username <user> password <password>
```

En caso de que el nombre de usuario y la contraseña sean correctos

```
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
```

El último error se relaciona con el hecho de que puesto que el servidor AAA espera que un usuario introduzca una contraseña única después de la autenticación exitosa del nombre de usuario y la contraseña y esta prueba no implica que un usuario ingrese activamente a OTP, por lo tanto vemos el Access-Challenge enviado por el servidor AAA en respuesta al cual no se ve ningún error en el ASA.

En caso de que el nombre de usuario o la contraseña sean incorrectos

```
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
```

Las depuraciones de una configuración en funcionamiento tendrán un aspecto similar al siguiente:

Leyenda:

Anyconnect Client Real IP :10.106.49.111

IP de 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 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		...)..uk56XIO51
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		uk56XIO51X6KuLt
-------------------------------------------------	--	-----------------

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		>Vsqr.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 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	ANYCONN
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 | ...>Vsqr.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

Información Relacionada

- [Configuración de AnyConnect Secure Mobility Client con Tunelización Dividida en un ASA](#)
- [Autenticación SecurID RSA para Clientes AnyConnect en una Configuración de Cabecera de Cisco IOS](#)
- [Uso del Protocolo SDI y del Servidor Token RSA para ASA y ACS](#)
- [Guía de Configuración de Autenticación Doble ASA AnyConnect con Validación de Certificados, Mapping y Pre-Fill](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)