使用一次性密码配置AnyConnect安全移动客户端

目录

简介

本文档介绍自适应安全设备(ASA)Cisco AnyConnect安全移动客户端访问的配置示例。

先决条件

要求

本文档假设ASA完全运行且配置为允许思科自适应安全设备管理器(ASDM)或命令行界面(CLI)进行配置更改。

Cisco 建议您了解以下主题：

- ASA CLI和ASDM的基本知识
- Cisco ASA头端上的SSLVPN配置
- 双因素身份验证的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科自适应安全设备ASA5506
- Cisco 自适应安全设备软件版本 9.6(1)

- 自适应安全设备管理器版本7.8(2)
- AnyConnect版本4.5.02033

注意：从Cisco软件下载（仅限注册客户）下载AnyConnect VPN客户端包(anyconnect-win*.pkg)。将AnyConnect VPN客户端复制到ASA的闪存，该闪存下载到远程用户计算机，以便与ASA建立SSL VPN连接。有关 ASA 配置指南的详细信息，请参阅安装 AnyConnect 客户端部分。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

自适应安全设备(ASA)Cisco AnyConnect安全移动客户端访问在一次性密码(OTP)的帮助下使用双因素身份验证。必须提供正确的凭据和令牌，AnyConnect用户才能成功连接。

双因素身份验证使用两种不同的身份验证方法，可以是其中任意两种。

- 一些您知道的事情
- 您拥有的东西
- 有些东西你

一般而言，它包含用户知道的东西（用户名和密码），以及用户拥有的某种东西（例如，只有个人拥有的信息实体，如令牌或证书）。这比传统的身份验证设计更加安全，传统身份验证设计用户通过存储在ASA本地数据库或与ASA集成的Active Directory(AD)服务器上的凭证进行身份验证。一次性密码是一种最简单、最流行的双因素身份验证形式，用于保护网络访问。例如，在大型企业中，虚拟专用网络访问通常需要使用一次性密码令牌进行远程用户身份验证。

在此场景中，您使用OpenOTP身份验证服务器作为AAA服务器，该服务器使用radius协议进行ASA和AAA服务器之间的通信。用户凭证在OpenOTP服务器上配置，该服务器与Google Authenticator应用服务相关联，作为双因素身份验证的软令牌。

此处不介绍OpenOTP配置，因为它不在本文档的讨论范围之内。您可以查看这些链接进行进一步阅读。

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

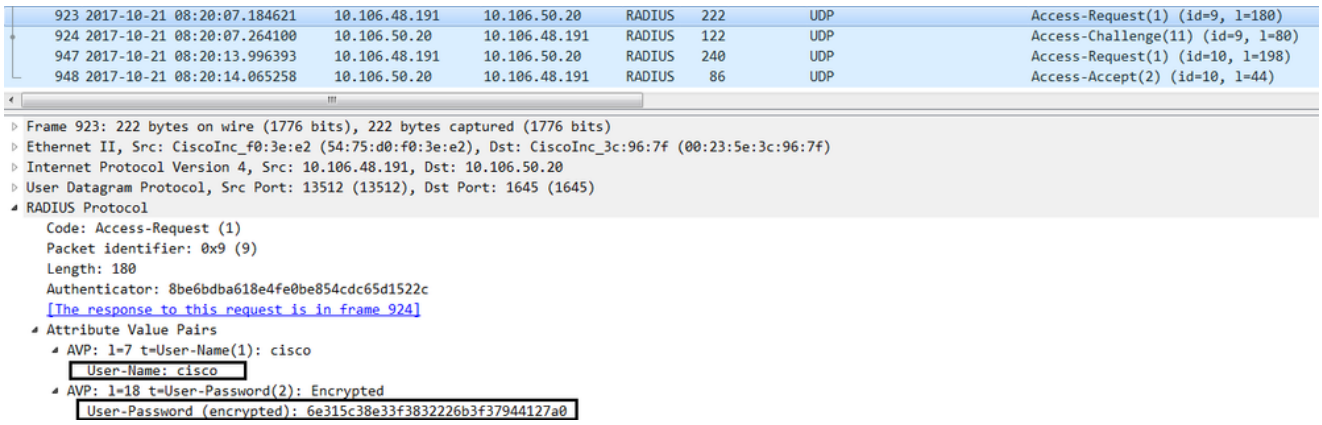
配置ASA进行OpenOTP身份验证
https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/

数据包流

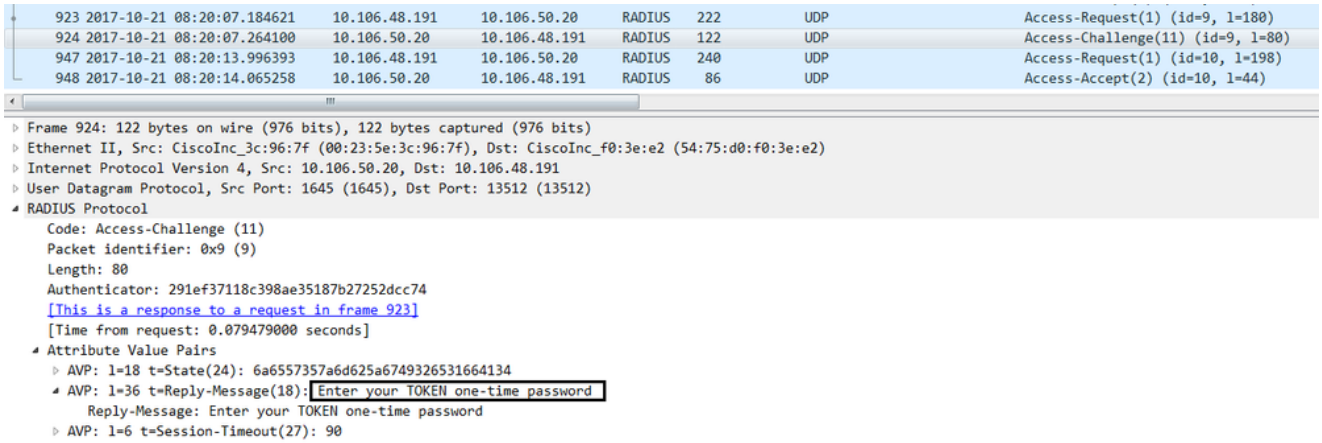
此数据包捕获是在连接到AAA服务器10.106.50.20的ASA的外部接口上进行的。

1. AnyConnect用户发起到ASA的客户端连接，并且取决于配置的group-url和group-alias，连接将位于特定隧道组（连接配置文件）上。此时，系统会提示用户输入凭证。

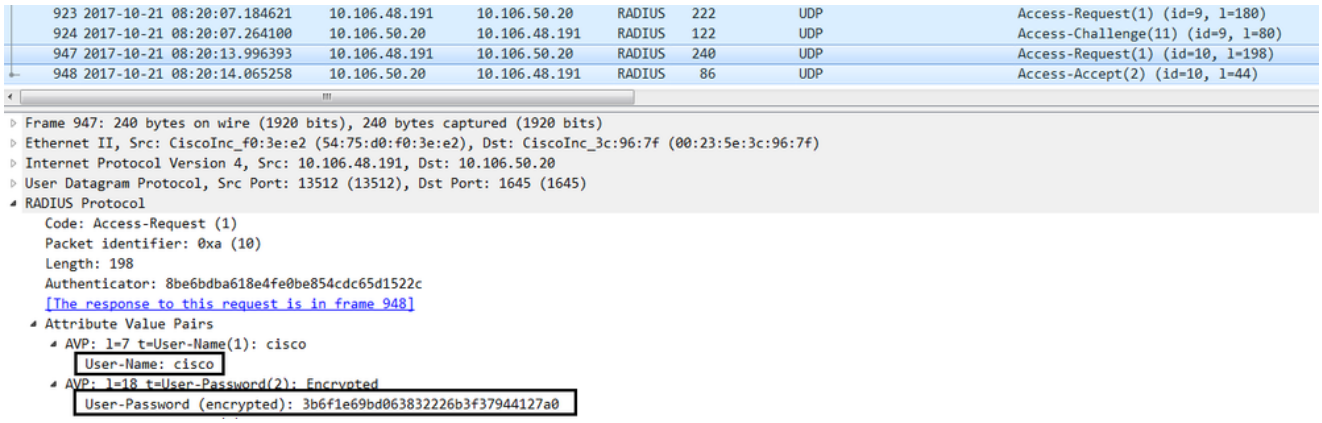
2. 用户输入凭证后，身份验证请求（访问请求数据包）将从ASA转发到AAA服务器。



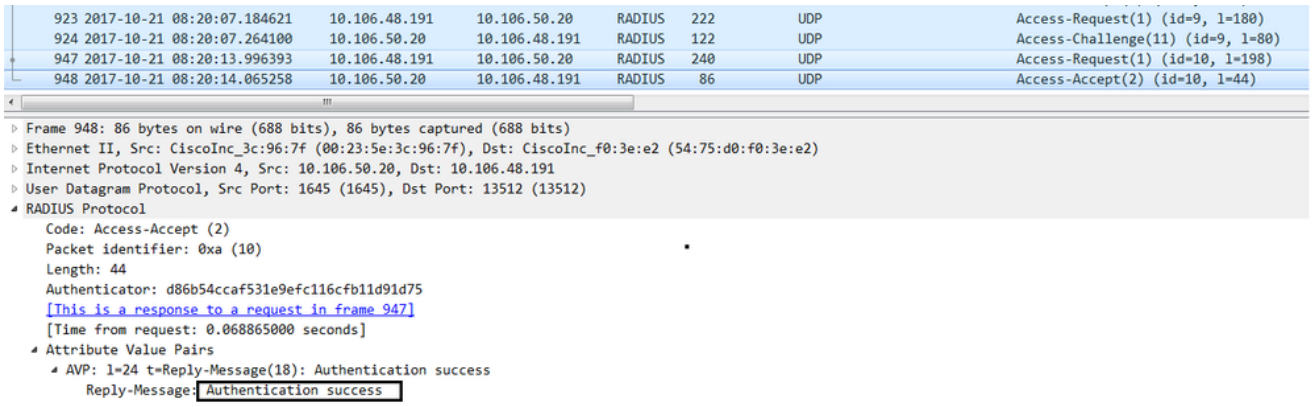
3. 身份验证请求到达AAA服务器后，将验证凭证。如果正确，则AAA服务器会回复访问质询，要求用户输入一次性密码。 如果凭证不正确，Access-Reject数据包将发送到ASA。



4. 当用户输入一次性密码时，将以Access-Request数据包的形式向AAA服务器发送身份验证请求



5. 在AAA服务器上成功验证一次性密码后，从服务器向ASA发送Access-Accept数据包，成功对用户进行身份验证，从而完成双因素身份验证过程。



AnyConnect 许可证信息

以下是一些指向有关 Cisco AnyConnect Secure Mobility Client 许可证的有用信息的链接：

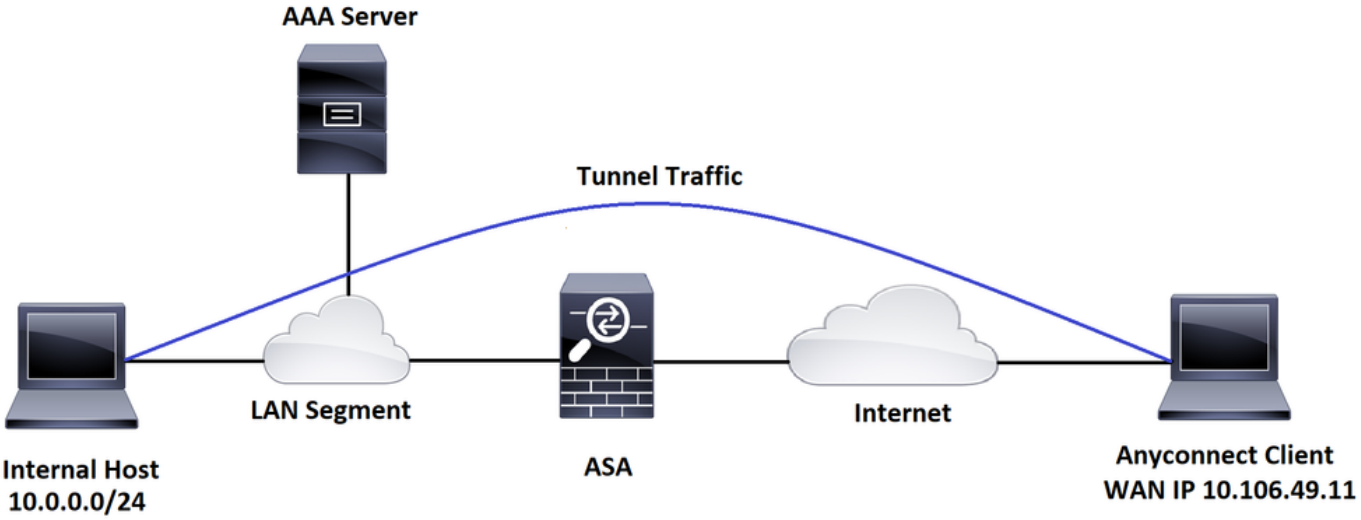
- 有关AnyConnect许可的常见问题，请参阅本文档。
- 有关 AnyConnect Apex 和 Plus 许可证的信息，请参阅《Cisco AnyConnect 订购指南》。

配置

本节介绍如何在ASA上配置Cisco AnyConnect安全移动客户端。

注意：要获取有关本部分中所使用命令的更多信息，可使用命令查找工具（仅限已注册客户）。

网络图



ASDM AnyConnect 配置向导

AnyConnect配置向导可用于配置AnyConnect安全移动客户端。在继续之前，请确保AnyConnect客户端软件包已上传到ASA防火墙的闪存/磁盘。

完成以下步骤，以通过配置向导配置 AnyConnect Secure Mobility Client。

有关通过ASDM的分割隧道配置，要下载和安装AnyConnect，请参阅本文档。

[AnyConnect 安全移动客户端]

ASA CLI 配置

本节介绍 Cisco AnyConnect Secure Mobility Client 的 CLI 配置，以供参考。

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

要在ASA上为AnyConnect客户端连接配置和安装第三方证书，请参阅本文档。

[配置ASA SSL数字证书]

验证

使用本部分可确认配置能否正常运行。

> 注意:Output Interpreter Tool(仅注册客户)支持某些show命令。使用输出解释器工具来查看 show 命令输出的分析。

可以执行这些show命令来确认AnyConnect客户端及其统计信息的状态。

```
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
```

用户体验

上，您可以设置各种调试级别；默认情况下，使用级别1。如果更改调试级别，调试的详细程度可能会增加。请谨慎执行此操作，尤其是在生产环境中。

要对传入AnyConnect客户端连接的完整身份验证过程进行故障排除，可以使用以下调试：

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

这些命令确认用户凭证是否正确。

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

如果用户名和密码正确，

```
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
```

最后一个错误与以下事实有关：由于AAA服务器预计用户在成功验证用户名和密码后输入一次性密码，并且此测试不涉及主动输入OTP的用户，因此您会看到AAA服务器发送的访问质询，以响应ASA上未出现任何错误。

如果用户名和/或密码不正确，

```
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
```

工作设置中的调试如下所示：

图例

AnyConnect客户端实际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
```

相关信息

- 在 ASA 上使用拆分隧道功能配置 AnyConnect Secure Mobility Client
- Cisco IOS头端配置上AnyConnect客户端的RSA SecurID身份验证
- ASA和ACS的RSA令牌服务器和SDI协议使用情况
- ASA AnyConnect Double Authentication with Certificate Validation， Mapping， and Pre-Fill配置指南
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。