Cisco IOS头端上AnyConnect客户端的RSA SecurID身份验证配置示例

目录

简介
先决条件
要求
使用的组件
背景信息
配置
网络图
验证
故障排除

简介

本文档介绍如何配置Cisco IOS®设备以使用一次性密码(OTP)对AnyConnect客户端进行身份验证，以及如何使用Rivest-Shamir-Addleman(RSA)SecurID服务器。

> **注意**：OTP身份验证在具有针对增强请求CSCsw95673和CSCue13902的修复的Cisco IOS版本上不起作用。

先决条件

要求

Cisco 建议您了解以下主题：

- RSA SecurID服务器设置
- Cisco IOS头端上的SSLVPN配置
- Web-VPN

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CISCO2951/K9
- 思科IOS软件，C2951软件(C2951-UNIVERSALK9-M)，版本15.2(4)M4，版本软件(fc1)

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

虽然AnyConnect客户端始终支持基于OTP的身份验证，但在修复Cisco Bug ID CSCsw95673之前，Cisco IOS头端未处理RADIUS访问质询消息。在初始登录提示（用户输入其“永久”用户名和密码）后，RADIUS发送“Cisco Bug ID”Cisco IOS网关的access-Challenge”消息，要求用户输入其OTP:

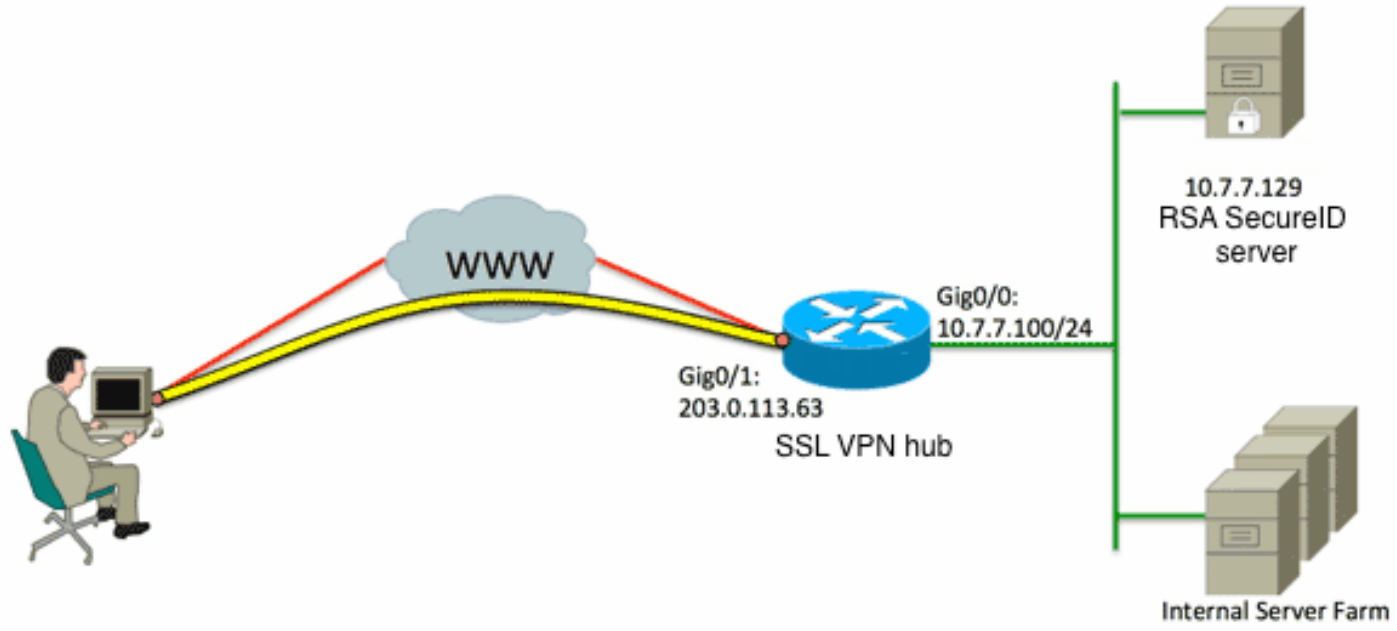
```
RADIUS/ENCODE: Best Local IP-Address 10.7.7.1 for Radius-Server 10.7.7.129
RADIUS(0000001A): Sending a IPv4 Radius Packet
RADIUS(0000001A): Send Access-Request to 10.7.7.129:1812 id 1645/17,len 78
RADIUS:  authenticator C3 A1 B9 E1 06 95 8C 65 - 7A C3 01 70 E1 E1 7A 3A
RADIUS:  User-Name           [1]   6   "atbasu"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   6
RADIUS:  NAS-Port-Id         [87]  16  "203.0.113.238"
RADIUS:  NAS-IP-Address      [4]   6   10.7.7.1
RADIUS(0000001A): Started 5 sec timeout
RADIUS: Received from id 1645/17 10.7.7.129:1812, Access-Challenge, len 65
RADIUS:  authenticator 5D A3 A6 9D 1A 38 E2 47 - 37 E8 EF A8 18 94 25 1C
RADIUS:  Reply-Message       [18]  37
RADIUS:   50 6C 65 61 73 65 20 65 6E 74 65 72 20 79 6F 75  [Please enter you]
RADIUS:   72 20 6F 6E 65 2D 74 69 6D 65 20 70 61 73 73 77  [r one-time passw]
RADIUS:   6F 72 64               [ ord]
RADIUS:  State               [24]  8
RADIUS:   49 68 36 76 38 7A           [ Ih6v8z]
```

此时，AnyConnect客户端应显示一个额外的弹出窗口，向用户请求其OTP，但由于Cisco IOS设备未处理Access-Challenge消息，因此这永远不会发生，并且客户端在连接超时之前处于空闲状态。

但是，从15.2(4)M4版开始，Cisco IOS设备应能处理基于质询的身份验证机制。

配置

网络图



自适应安全设备(ASA)和Cisco IOS头端之间的一个区别是，Cisco IOS路由器/交换机/接入点(AP)仅支持RADIUS和TACACS。它们不支持RSA专有协议SDI。但RSA服务器同时支持SDI和RADIUS。因此，要在Cisco IOS头端上使用OTP身份验证，必须将Cisco IOS设备配置为RADIUS协议和RSA服务器作为RADIUS令牌服务器。

注意：有关RADIUS和SDI之间差异的更多详细信息，请参阅RSA令牌服务器和ASA和ACS的SDI协议使用情况的理论部分。如果需要SDI，则必须使用ASA。

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

1. 配置身份验证方法和身份验证、授权和记帐(AAA)服务器组：

```
aaa new-model
!
!
aaa group server radius OTP-full
server 10.7.7.129
!
aaa group server radius OTP-split
server 10.7.7.129 auth-port 1812
!
aaa authentication login default local
aaa authentication login webvpn-auth group OTP-split
aaa authorization exec default local
aaa authorization network webvpn-auth local
```

2. 配置RADIUS服务器：

```
radius-server host 10.7.7.129 auth-port 1812
radius-server host 10.7.7.129
radius-server key Cisco12345
```

3. 将路由器配置为安全套接字层VPN(SSLVPN)服务器：

```
crypto pki trustpoint VPN-test2
enrollment selfsigned
revocation-check crl
rsakeypair VPN-test2
!
!
crypto pki certificate chain VPN-test2
certificate self-signed 02
3082021B 30820184 A0030201 02020102 300D0609 2A864886 F70D0101 05050030
29312730 2506092A 864886F7 0D010902 1618494E 4E424545 2D524F30 312E636F
7270726F 6F742E69 6E74301E 170D3133 30313134 31313434 32365A17 0D323030
31303130 30303030 305A3029 31273025 06092A86 4886F70D 01090216 18494E4E
4245452D 524F3031 2E636F72 70726F6F 742E696E 7430819F 300D0609 2A864886
F70D0101 01050003 818D0030 81890281 8100B03E D15F7D2C DF84855F B1055ACD
7BE43AAF EEB99472 50477348 45F641C6 5A244CEE 80B2A426 55CA223A 7F4F89DD
FA0BD882 7DAA24EF 9EA66772 2CC5A065 584B9866 2530B67E EBDE8F57 A5E0FF19
88C38FF2 D238A136 B32A114A 0187437C 488073E9 0E96FF75 F565D684 987F2CD1
8CC7F53C 2D419F90 EF4B9678 6BDFCD4B C7130203 010001A3 53305130 0F060355
1D130101 FF040530 030101FF 301F0603 551D2304 18301680 146B56E9 F770734C
B0AB7360 B806E9E1 E1E15921 B3301D06 03551D0E 04160414 6B56E9F7 70734CB0
AB7360B8 06E9E1E1 E15921B3 300D0609 2A864886 F70D0101 05050003 81810006
0D68B990 4F927897 AFE746D8 4C9A7374 3CA6016B EFFA1CA7 7AAD4E3A 2A0DE989
0BC09B17 5A4C75B6 D1F3AFDD F97DC74C D8834927 3F52A605 25518A42 9EA454AA
C5DCBA20 A5DA7C7A 7CEB7FF1 C35F422A 7F060556 647E74D6 BBFE116F 1BF04D0F
852768C3 2E972EEE DAD676F1 A3941BE6 99ECB9D0 F826C1F6 A944340D 14EA32
quit
ip cef
!
!
crypto vpn anyconnect flash0:/webvpn/anyconnect-win-3.1.02026-k9.pkg sequence 1
!
interface Loopback1
ip address 192.168.201.1 255.255.255.0
!
interface GigabitEthernet0/0
description WAN 0/0 VODAFONE WAN
ip address 203.0.113.63 255.255.255.240
no ip redirects
no ip unreachables
duplex auto
speed auto
!
!
interface Virtual-Template3
ip unnumbered Loopback1
!
ip local pool SSLVPN-pool 192.168.201.10 192.168.201.250
!
webvpn gateway gateway_1
hostname vpn.innervate.nl
ip address 203.0.113.63 port 443
http-redirect port 80
ssl trustpoint VPN-test2
inservice
!
webvpn context webvpn-context
secondary-color white
title-color #669999
text-color black
virtual-template 3
```

```
aaa authentication list webvpn-auth
gateway gateway_1
!
ssl authenticate verify all
inservice
!
policy group policy_1
functions svc-enabled
svc address-pool "SSLVPN-pool" netmask 255.255.255.0
svc keep-client-installed
svc split include 192.168.174.0 255.255.255.0
svc split include 192.168.91.0 255.255.255.0
default-group-policy policy_1
!
end
```

注意：有关如何在Cisco IOS设备上设置SSLVPN的详细配置指南，请参阅IOS路由器上AnyConnect VPN(SSL)客户端的CCP配置示例。

验证

当前没有可用于此配置的验证过程。

故障排除

为了对传入AnyConnect客户端连接的整个身份验证过程进行故障排除，可以使用以下调试：

- debug radius authentication
- debug aaa authentication
- debug webvpn authentication

命令输出解释程序工具（仅限注册用户）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。

注意：使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。