適用於Cisco IOS頭端上的AnyConnect客戶端的RSA SecurID身份驗證配置示例

目錄

簡介

本文說明如何配置Cisco IOS®裝置以使用一次性密碼(OTP)驗證AnyConnect客戶端，以及如何使用Rivest-Shamir-Addleman(RSA)SecurID伺服器。

> **附註**：OTP身份驗證不適用於修正了增強請求CSCsw95673和CSCue13902的Cisco IOS版本。

必要條件

需求

思科建議您瞭解以下主題：

- RSA SecurID伺服器設定
- Cisco IOS頭端上的SSLVPN配置
- Web-VPN

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CISCO2951/K9
- Cisco IOS軟體，C2951軟體(C2951-UNIVERSALK9-M)，版本15.2(4)M4，版本軟體(fc1)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

雖然AnyConnect客戶端始終支援基於OTP的身份驗證，但在修復思科錯誤ID CSCsw95673之前，Cisco IOS頭端不會處理RADIUS訪問質詢消息。在初始登入提示後（使用者輸入其「永久」使用者名稱和密碼），RADIUS會將「訪問質詢」消息傳送到Cisco IOS網關，該網關會要求使用者輸入其OTP:

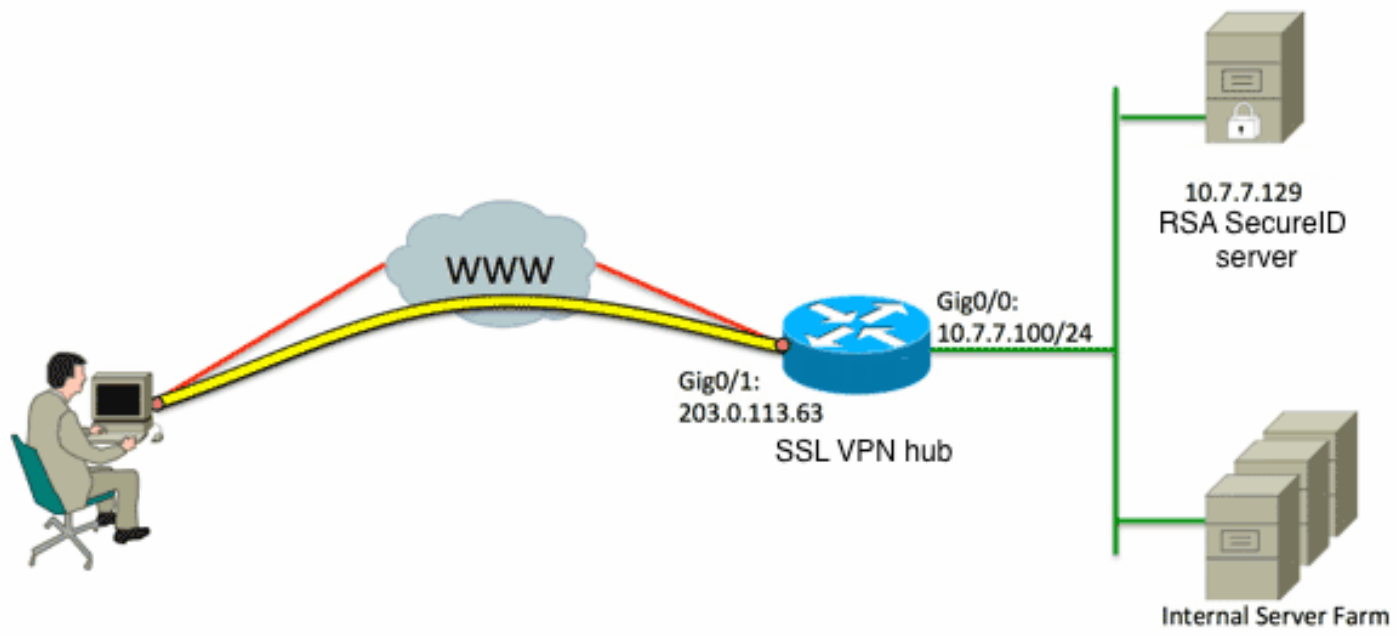
```
RADIUS/ENCODE: Best Local IP-Address 10.7.7.1 for Radius-Server 10.7.7.129
RADIUS(0000001A): Sending a IPv4 Radius Packet
RADIUS(0000001A): Send Access-Request to 10.7.7.129:1812 id 1645/17,len 78
RADIUS:  authenticator C3 A1 B9 E1 06 95 8C 65 - 7A C3 01 70 E1 E1 7A 3A
RADIUS:  User-Name           [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]
```

此時，AnyConnect客戶端應顯示一個額外的彈出視窗，請求使用者執行其OTP，但由於Cisco IOS裝置未處理訪問質詢消息，因此這種情況永遠不會發生，並且客戶端將處於空閒狀態，直到連線超時。

但是，自版本15.2(4)M4起，Cisco IOS裝置應該能夠處理基於質詢的驗證機制。

設定

網路圖表



自適應安全裝置(ASA)和Cisco IOS前端之間的一個區別是Cisco IOS路由器/交換機/接入點(AP)僅支援RADIUS和TACACS。它們不支援RSA專有協定SDI。但是，RSA伺服器同時支援SDI和RADIUS。因此，要在Cisco IOS頭端上使用OTP身份驗證，必須將Cisco IOS裝置配置為RADIUS協定，並將RSA伺服器配置為RADIUS令牌伺服器。

附註：有關RADIUS和SDI之間差異的詳細資訊，請參閱ASA和ACS的RSA令牌伺服器和SDI協定使用情況的理論部分。如果需要SDI，則必須使用ASA。

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

1. 設定驗證方法和驗證、授權和記帳(AAA)伺服器群組：

```
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. 設定RADIUS伺服器：

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

3. 將路由器配置為充當安全套接字層VPN(SSLVPN)伺服器：

```
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
```

附註：有關如何在Cisco IOS裝置上設定SSLVPN的詳細配置指南，請參閱使用CCP的IOS路由器上的AnyConnect VPN(SSL)客戶端配置示例。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

為了對傳入AnyConnect客戶端連線的整個身份驗證過程進行故障排除，可以使用以下調試：

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

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

附註：使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。