Cisco IOS Headend 컨피그레이션의 AnyConnect 클라이언트에 대한 RSA SecurID 인증 예

목차

소개

이 문서에서는 OTP(One Time Password)로 AnyConnect 클라이언트를 인증하도록 Cisco IOS® 디바이스를 구성하고 RSA(Rivest-Shamir-Addleman) SecurID 서버를 사용하는 방법에 대해 설명합니다.

> **참고:**OTP 인증은 개선 요청 CSCsw95673 및 CSCue13902에 대한 수정 사항이 있는 Cisco IOS 버전에서 작동하지 않습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RSA SecurID 서버 설정
- Cisco IOS 헤드엔드의 SSLVPN 컨피그레이션
- 웹-VPN

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CISCO2951/K9
- Cisco IOS 소프트웨어, C2951 소프트웨어(C2951-UNIVERSALK9-M), 버전 15.2(4)M4, 릴리스 소프트웨어(fc1)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

AnyConnect 클라이언트는 항상 OTP 기반 인증을 지원했지만 Cisco 버그 ID CSCsw95673을 수정하기 전에 Cisco IOS 헤드엔드는 RADIUS 액세스-챌린지 메시지를 처리하지 않았습니다. 초기 로그인 프롬프트(사용자가 "영구" 사용자 이름 및 비밀번호를 입력함) 후 RADIUS는 Cisco IOS 게이트웨이에 "액세스-챌린지" 메시지를 전송하며 사용자는 OTP를 입력합니다.:

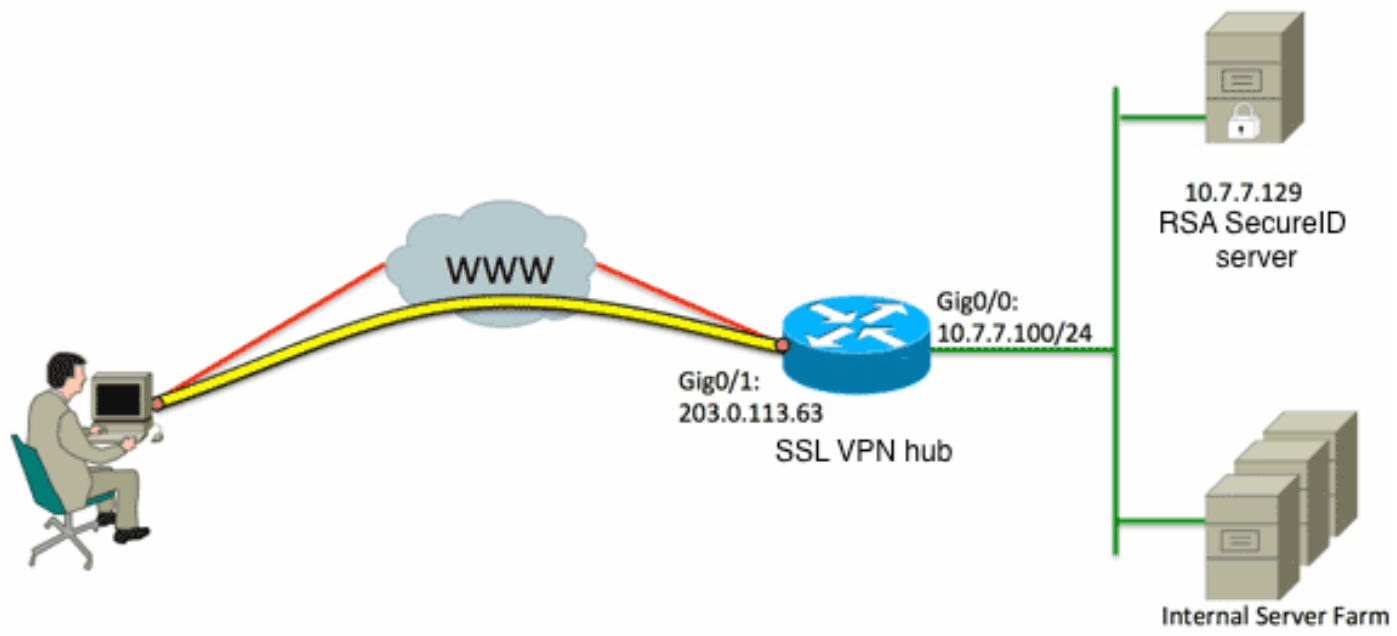
```
RADIUS/ENCODE: Best Local IP-Address 10.7.7.1 for Radius-Server 10.7.7.129
RADIUS(0000001A): Sending a IPv4 Radius Packet
RADIUS(0000001A): Send Access-Request to 10.7.7.129:1812 id 1645/17,len 78
RADIUS:  authenticator C3 A1 B9 E1 06 95 8C 65 - 7A C3 01 70 E1 E1 7A 3A
RADIUS:  User-Name        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

이 시점에서 AnyConnect 클라이언트는 사용자에게 OTP를 요청하는 추가 팝업 창을 표시할 것으로 예상되지만, Cisco IOS 디바이스에서 Access-Challenge 메시지를 처리하지 않았기 때문에 이 작업은 발생하지 않으며 연결 시간이 초과될 때까지 클라이언트가 유휴 상태로 유지됩니다.

그러나 Version15.2(4)M4부터 Cisco IOS 디바이스는 챌린지 기반 인증 메커니즘을 처리할 수 있어야 합니다.

구성

네트워크 다이어그램



ASA(Adaptive Security Appliance)와 Cisco IOS 헤드엔드의 차이점 중 하나는 Cisco IOS 라우터/스위치/액세스 포인트(AP)가 RADIUS와 TACACS만 지원한다는 것입니다.RSA 전용 프로토콜 SDI는 지원하지 않습니다.그러나 RSA 서버는 SDI 및 RADIUS를 모두 지원합니다.따라서 Cisco IOS 헤드엔드에서 OTP 인증을 사용하려면 RADIUS 프로토콜에 대해 Cisco IOS 디바이스를 구성하고 RSA 서버를 RADIUS 토큰 서버로 구성해야 합니다.

참고:RADIUS와 SDI의 차이점에 대한 자세한 내용은 RSA 토큰 서버의 이론 섹션 및 ASA 및 ACS의 SDI 프로토콜 사용을 참조하십시오.SDI가 필요한 경우 ASA를 사용해야 합니다.

참고:이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

1. 인증 방법 및 AAA(Authentication, Authorization, and Accounting) 서버 그룹을 구성합니다.

```
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. RADIUS 서버를 구성합니다.

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

3. SSLVPN(Secure Sockets Layer VPN) 서버 역할을 하도록 라우터를 구성합니다.

```
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
```

참고: Cisco IOS 디바이스에서 SSLVPN을 설정하는 방법에 대한 자세한 컨피그레이션 가이드는 CCP 컨피그레이션 예를 사용하여 IOS 라우터의 AnyConnect VPN(SSL) 클라이언트를 참조하십시오.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

수신 AnyConnect 클라이언트 연결에 대한 전체 인증 프로세스를 트러블슈팅하려면 다음 디버그를 사용할 수 있습니다.

- **디버그 radius 인증**
- **디버그 aaa 인증**
- **디버그 webvpn 인증**

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

참고:debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.