

Ejemplo de Configuración de Autenticación SecurID RSA para Clientes AnyConnect en una Cabecera de Cisco IOS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar un dispositivo Cisco IOS® para autenticar clientes AnyConnect con contraseñas de una sola vez (OTP) y el uso de un servidor SecurID de Rivest-Shamir-Adleman (RSA).

Nota: La autenticación OTP no funciona en las versiones de Cisco IOS que tienen la corrección para las solicitudes de mejora [CSCsw95673](#) y [CSCue13902](#).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración del servidor RSA SecurID
- Configuración de SSLVPN en la cabecera Cisco IOS
- Web-VPN

Componentes Utilizados

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

hardware.

- CISCO2951/K9
- Software Cisco IOS, C2951 Software (C2951-UNIVERSALK9-M), versión 15.2(4)M4, SOFTWARE DE VERSIÓN (fc1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Aunque el cliente AnyConnect siempre ha soportado la autenticación basada en OTP, antes de la corrección del Id. de bug Cisco [CSCsw95673](#), la cabecera de Cisco IOS no procesó los mensajes RADIUS Access-Challenge. Después del mensaje de inicio de sesión inicial (donde los usuarios ingresan sus nombres de usuario y contraseñas "permanentes"), RADIUS envía el mensaje "Access-Challenge" al gateway de Cisco IOS, que pide a los usuarios que ingresen su OTP:

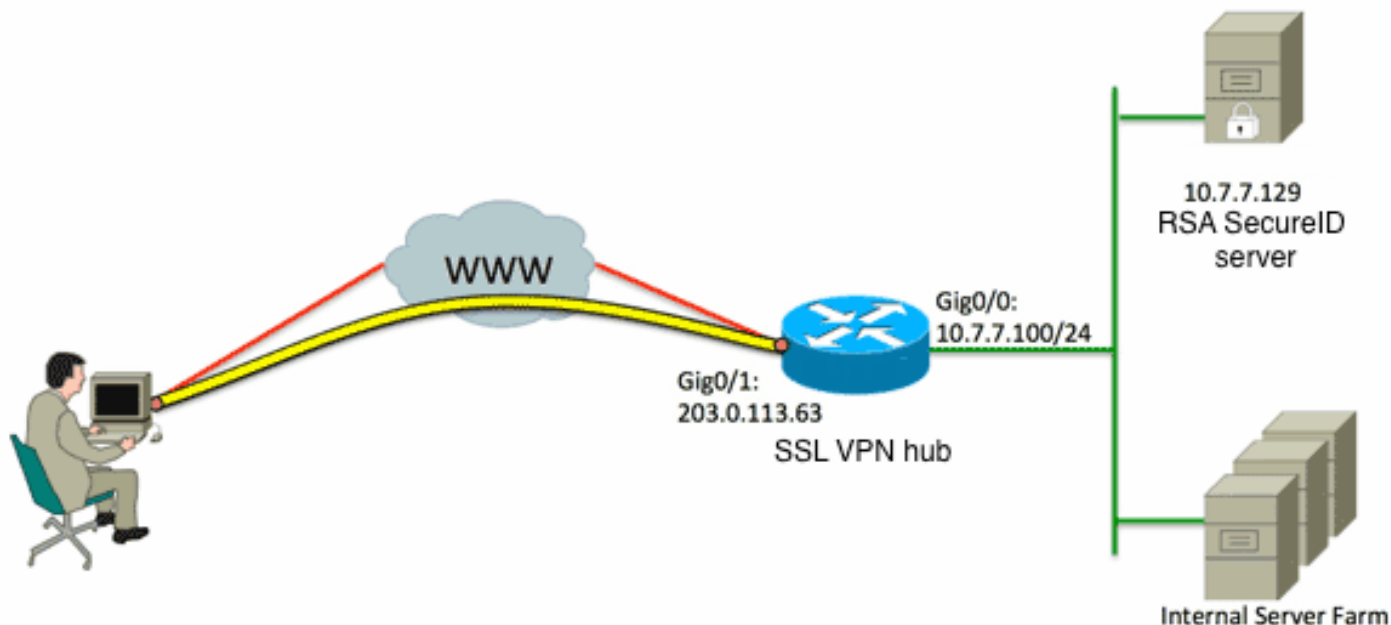
```
RADIUS/ENCODE: Best Local IP-Address 10.7.7.1 for Radius-Server 10.7.7.129
RADIUS(0000001A): Sending a IPv4 Radius Packet
RADIUS(0000001A): Send Access-Request to 10.7.7.129:1812 id 1645/17,len 78
RADIUS:  authenticator C3 A1 B9 E1 06 95 8C 65 - 7A C3 01 70 E1 E1 7A 3A
RADIUS:  User-Name      [1]  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]
```

En este momento, se espera que el cliente AnyConnect muestre una ventana emergente adicional que solicita a los usuarios su OTP, pero dado que el dispositivo Cisco IOS no procesó el mensaje Access-Challenge, esto nunca sucede y el cliente permanece inactivo hasta que se agota el tiempo de espera de la conexión.

Sin embargo, a partir de la versión 15.2(4)M4, los dispositivos Cisco IOS deben poder procesar el mecanismo de autenticación basado en desafío.

Configurar

Diagrama de la red



Una de las diferencias entre el dispositivo de seguridad adaptable (ASA) y las cabeceras de Cisco IOS es que los routers/switches/puntos de acceso (AP) Cisco IOS solo admiten RADIUS y TACACS. No soportan el protocolo SDI propiedad de RSA. Sin embargo, el servidor RSA soporta tanto SDI como RADIUS. Por lo tanto, para utilizar la autenticación OTP en una cabecera de Cisco IOS, el dispositivo Cisco IOS se debe configurar para el protocolo RADIUS y el servidor RSA como servidor de token RADIUS.

Nota: Para obtener más detalles sobre las diferencias entre RADIUS y SDI, refiérase a la sección [Teoría](#) del [Uso del Protocolo Token de RSA y el Uso del Protocolo SDI para ASA y ACS](#). Si se requiere SDI, se debe utilizar un ASA.

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

1. Configure el método de autenticación y el grupo de servidores Autenticación, Autorización y Contabilización (AAA):

```

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. Configure el servidor RADIUS:

```
radius-server host 10.7.7.129 auth-port 1812
radius-server host 10.7.7.129
radius-server key Cisc0l2345
```

3. Configure el router para que actúe como servidor VPN de capa de conexión segura (SSLVPN):

```
crypto pki trustpoint VPN-test2
enrollment selfsigned
revocation-check crl
rsa-keypair 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 unreachable
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
```

Nota: Para obtener más información sobre una guía de configuración detallada sobre cómo configurar SSLVPN en un dispositivo Cisco IOS, refiérase al [Ejemplo de Configuración de AnyConnect VPN \(SSL\) Client en el Router IOS con CCP](#).

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

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

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

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

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.