Índice

Introdução

Este documento descreve como configurar um dispositivo do ® do Cisco IOS para autenticar clientes de AnyConnect com senhas de uma vez (OTP) e o uso de um server do SecurID de Rivest-Shamir-Addleman (RSA).

> Nota: A autenticação OTP não trabalha nas versões do Cisco IOS que têm o reparo para as requisições de aprimoramento CSCsw95673 e CSCue13902.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Instalação do server do SecurID RSA
- Configuração SSLVPN no final do cabeçalho do Cisco IOS
- Web-VPN

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CISCO2951/K9
- Cisco IOS Software, software C2951 (C2951-UNIVERSALK9-M), versão 15.2(4)M4, SOFTWARE DE VERSÃO (fc1)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Informações de Apoio

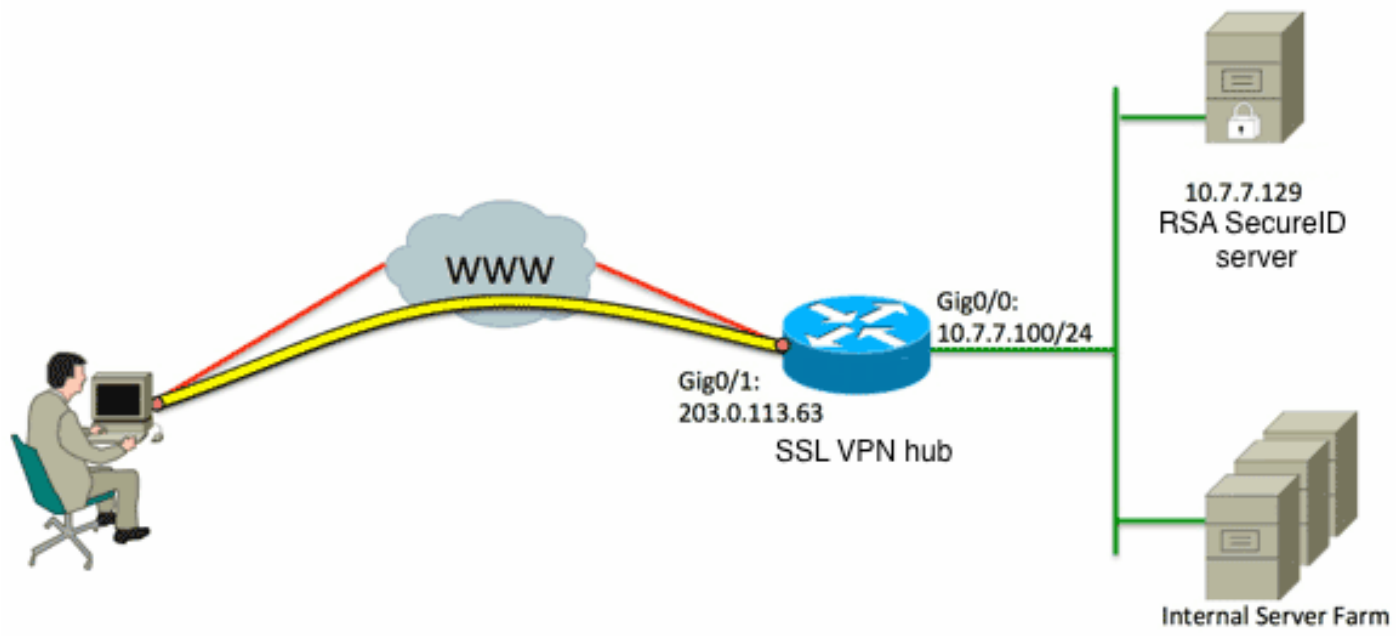
Embora o cliente de AnyConnect apoiasse sempre a autenticação OTP-baseada, antes do reparo para a identificação de bug Cisco CSCsw95673, o final do cabeçalho do Cisco IOS não processou mensagens do Acesso-desafio do RAIO. Depois que a alerta do login inicial (onde os usuários incorporam seu nomes de usuário e senha “permanentes”), RAIO envia a mensagem do “Acesso-desafio” ao Cisco IOS gateway, que pede que os usuários incorporem seu OTP:

Neste momento, o cliente de AnyConnect é esperado mostrar uma janela pop-up adicional que peça usuários para seu OTP, mas desde que o dispositivo IOS Cisco não processou a mensagem do Acesso-desafio, esta nunca acontece e o cliente senta a quietude até o tempo de conexão para fora.

Contudo, até à data de Version15.2(4)M4, os dispositivos IOS Cisco devem poder processar o mecanismo da autenticação desafio-baseado.

Configurar

Diagrama de Rede



Uma das diferenças entre os finais do cabeçalho adaptáveis da ferramenta de segurança (ASA) e do Cisco IOS é que o roteador/Switches/Access point do Cisco IOS (AP) apoiam somente o RAIO e o TACACS. Não apoiam o protocolo RSA-proprietário SDI. O server RSA contudo apoia o SDI e o RAIO. Consequentemente, a fim usar a autenticação OTP em um final do cabeçalho do Cisco IOS, o dispositivo IOS Cisco deve ser configurado para o protocolo de raio e o server RSA como um servidor de tokens do RAIO.

Nota: Para mais detalhes sobre as diferenças entre o RAIO e o SDI, refira a seção da teoria

do uso do servidor de tokens RSA e do protocolo SDI para o ASA e o ACS. Se o SDI é exigido, a seguir um ASA deve ser usado.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

1. Configurar o método de autenticação e o grupo de servidor do Authentication, Authorization, and Accounting (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. Configurar o servidor Radius:

```
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
```

3. Configurar o roteador para atuar como um server do secure sockets layer VPN (SSLVPN):

```
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
```

Nota: Para o mais um guia de configuração detalhada em como estabelecer SSLVPN em um dispositivo IOS Cisco, refere o cliente de AnyConnect VPN (SSL) no IOS Router com exemplo de configuração CCP.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

A fim pesquisar defeitos o processo de autenticação inteiro para uma conexão de cliente entrante de AnyConnect, você pode usar estes debuga:

- **debugar a autenticação RADIUS**
- **debug aaa authentication**
- **debugar a autenticação do webvpn**

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

> Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.