RSA SecurID Authentication for AnyConnect Clients on a Cisco IOS Headend Configuration Example

Document ID: 118778

Contributed by Atri Basu, Cisco TAC Engineer, and Vasavi Yellampalli, Cisco Engineering.

Mar 17, 2015

Contents

Introduction

This document describes how to configure a Cisco IOS® device to authenticate AnyConnect clients with One Time Passwords (OTPs) and the use of a Rivest-Shamir-Addleman (RSA) SecurID server.

Note: OTP authentication does not work on Cisco IOS versions that do not have the fix for the enhancement requests CSCsw95673 and CSCue13902.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- RSA SecurID server setup
- SSLVPN configuration on the Cisco IOS headend
- Web-VPN

Components Used

The information in this document is based on these software and hardware versions:

- CISCO2951/K9
- Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.2(4)M4, RELEASE SOFTWARE (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.

Background Information

Although the AnyConnect client has always supported OTP-based authentication, prior to the fix for Cisco bug ID CSCsw95673, the Cisco IOS headend did not process RADIUS Access-Challenge messages. After the initial login prompt (where users enter their "permanent" usernames and passwords), RADIUS sends the "Access-Challenge" message to the Cisco IOS gateway, which asks users to enter their OTP:

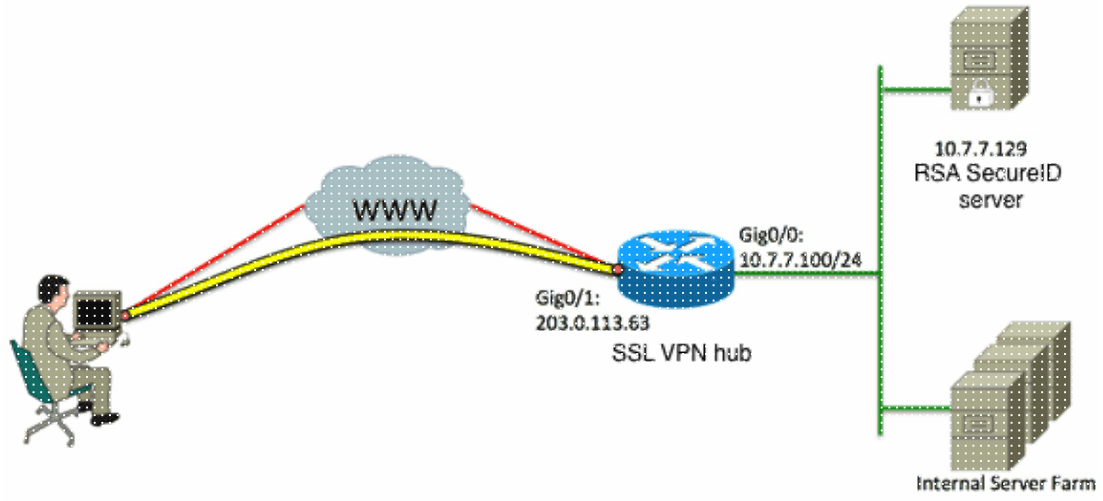
```
RADIUS/ENCODE: Best Local IP-Address 10.7.7.1 for Radius-Server 10.7.7.129
RADIUS(0000001A): Sending a IPv4 Radius Packet
RADIUS(0000001A): Send Access-Request to 10.7.7.129:1812 id 1645/17,len 78
RADIUS:  authenticator C3 A1 B9 E1 06 95 8C 65 - 7A C3 01 70 E1 E1 7A 3A
RADIUS:  User-Name        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

At this point, the AnyConnect client is expected to show an additional pop-up window that requests users for their OTP, but since the Cisco IOS device did not process the Access-Challenge message, this never happens and the client sits idle until the connection times out.

However, as of Version15.2(4)M4, Cisco IOS devices should be able to process the challenge-based authentication mechanism.

Configure

Network Diagram



One of the differences between the Adaptive Security Appliance (ASA) and Cisco IOS headends is that Cisco IOS Router/switches/Access Points (APs) only support RADIUS and TACACS. They do not support the RSA-proprietary protocol SDI. The RSA server however supports both SDI and RADIUS. Therefore, in order to use OTP authentication on a Cisco IOS headend, the Cisco IOS device must be configured for RADIUS protocol and the RSA server as a RADIUS token server.

Note: For more details about the differences between RADIUS and SDI, refer to the Theory section of RSA Token Server and SDI Protocol Usage for ASA and ACS. If SDI is required, then an ASA must be used.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

1. Configure the authentication method and the Authentication, Authorization, and Accounting (AAA) server group:

```
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 the RADIUS server:

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

3. Configure the router to act as an Secure Sockets Layer VPN (SSLVPN) server:

```
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.cisco.com
 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
```

Note: For more a detailed configuration guide on how to set up SSLVPN on a Cisco IOS device, refer to AnyConnect VPN (SSL) Client on IOS Router with CCP Configuration Example.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

In order to troubleshoot the entire authentication process for an incoming AnyConnect client connection, you can use these debugs:

- **debug radius authentication**

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

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Updated: Mar 17, 2015 Document ID: 118778