مصادقة RSA SecureID لعملاء AnyConnect على مثال تكوين وحدة الاستقبال والبث الخاصة ببرنامج Cisco IOS

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين جهاز Cisco IOS® لمصادقة عملاء AnyConnect باستخدام كلمات مرور المرة الواحدة (OTPs) واستخدام خادم Rivest-Shamir-Addleman SecureID (RSA).

ملاحظة: لا تعمل مصادقة OTP على إصدارات Cisco IOS التي تحتوي على الإصلاح لطلبات التحسين CSCsw95673 وCSCue13902.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إعداد خادم SecureID ل RSA
- تكوين SSLVPN على وحدة الاستقبال والبث من Cisco IOS
- ويب-VPN

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الطراز Cisco 2951/K9
- برنامج Cisco IOS، برنامج C2951-Universalk9-M) C2951)، الإصدار 15.2(4)M4، برنامج الإصدار (FC1)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

على الرغم من أن عميل AnyConnect دعم دائما المصادقة المستندة إلى OTP، قبل إصلاح معرف تصحيح الأخطاء من Cisco CSCsw95673، فإن وحدة الاستقبال والبث من Cisco IOS لم تعالج رسائل تحدي الوصول إلى RADIUS. بعد مطالبة تسجيل الدخول الأولية (حيث يقوم المستخدمون بإدخال أسماء المستخدمين وكلمات المرور "الدائمة")، يرسل RADIUS رسالة "تحدي الوصول" إلى بوابة Cisco IOS، التي تطلب من المستخدمين إدخال كلمة مرور المرة الواحدة:

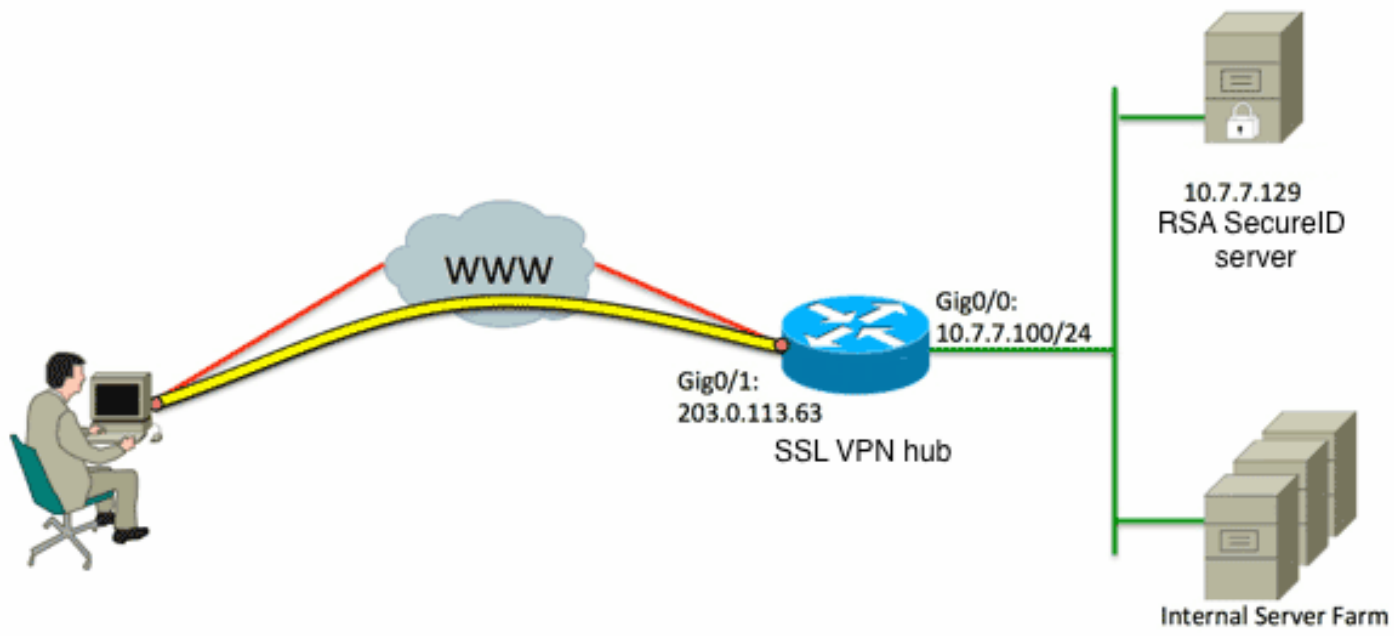
```
RADIUS/ENCODE: Best Local IP-Address 10.7.7.1 for Radius-Server 10.7.7.129
                            RADIUS(0000001A): Sending a IPv4 Radius Packet
RADIUS(0000001A): Send Access-Request to 10.7.7.129:1812 id 1645/17,len 78
  RADIUS:  authenticator C3 A1 B9 E1 06 95 8C 65 - 7A C3 01 70 E1 E1 7A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

عند هذه النقطة، من المتوقع أن يعرض عميل AnyConnect نافذة منبثقة إضافية تطلب من المستخدمين إجراء إختبار الاتصال البصري (OTP) الخاص بهم، ولكن نظرا لأن جهاز Cisco IOS لم يعالج رسالة "تحدي الوصول"، فلن يحدث ذلك أبدا ويجلس العميل في وضع الخمول حتى ينتهي الاتصال.

ومع ذلك، اعتبارا من الإصدار 15.2(4)M4، يجب أن تكون أجهزة Cisco IOS قادرة على معالجة آلية المصادقة المستندة إلى التحدي.

التكوين

الرسم التخطيطي للشبكة



أحد الفروق بين جهاز الأمان القابل للتكيف (ASA) والنهايات الرئيسية من Cisco IOS هو أن موجه/محولات/نقاط الوصول (AP) من Cisco IOS تدعم فقط RADIUS و TACACS. لا تدعم بروتوكول SDI الخاص ب RSA. ومع ذلك، يدعم خادم RSA كلا من SDI و RADIUS. لذلك، من أجل إستخدام مصادقة OTP على وحدة الاستقبال والبث من Cisco IOS، يجب تكوين جهاز Cisco IOS لبروتوكول RADIUS وخادم RSA كخادم رمز RADIUS.

ملاحظة: للحصول على مزيد من التفاصيل حول الفروق بين RADIUS و SDI، ارجع إلى قسم النظرية في خادم RSA المميز واستخدام بروتوكول SDI ل ASA و ACS. إذا كان SDI مطلوبا، فيجب إستخدام ASA.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

1. تكوين طريقة المصادقة ومجموعة خوادم المصادقة والتفويض والمحاسبة (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. تكوين خادم RADIUS:

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

3. قم بتكوين الموجه ليعمل كخادم طبقة مآخذ التوصيل الآمنة SSLVPN) VPN):

```
                                                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
        2506092A 864886F7 0D010902 1618494E 4E424545 2D524F30 312E636F 29312730
        7270726F 6F742E69 6E74301E 170D3133 30313134 31313434 32365A17 0D323030
        305A3029 31273025 06092A86 4886F70D 01090216 18494E4E 30303030 31303130
        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
```

ملاحظة: للحصول على مزيد من دليل التكوين التفصيلي حول كيفية إعداد SSLVPN على جهاز Cisco IOS، ارجع إلى عميل SSL VPN (AnyConnect) على موجه IOS باستخدام مثال تكوين CCP.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء عملية المصادقة بالكامل وإصلاحها لاتصال عميل AnyConnect الوارد، يمكنك إستخدام عمليات تصحيح الأخطاء التالية:

- **مصادقة نصف القطر debug**
- **تصحيح أخطاء مصادقة aaa (المصادقة والتفويض والمحاسبة)**
- **تصحيح أخطاء مصادقة WebVPN**

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).