تكوين AnyConnect SSL VPN ل ISR4k باستخدام المصادقة المحلية

المحتويات

المقدمة

يصف هذا المستند عينة تكوين من كيفية تكوين موجه خدمة مدمج (ISR) 4k وحدة الاستقبال والبث Cisco IOS® XE ل AnyConnect Secure Sockets Layer (SSL) VPN مع قاعدة بيانات مستخدم محلي.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- IOS XE (ISR 4K) من Cisco
- AnyConnect Secure Mobility Client
- عملية SSL العامة
- البنية الأساسية للمفتاح العام (PKI)

المكونات المستخدمة

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

- موجه Cisco ISR4451-X/K9 مع الإصدار 17.9.2a
- AnyConnect Secure Mobility Client 4.10.04065

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

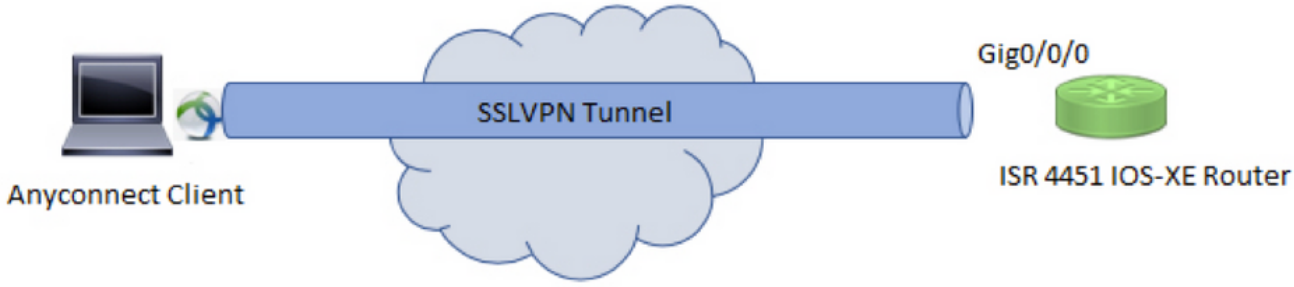
توفر ميزة الشبكة الخاصة الظاهرية (VPN) ل SSL الدعم في برنامج Cisco IOS XE للوصول عن بعد للمستخدم إلى شبكات المؤسسات من أي مكان على الإنترنت. يتم توفير الوصول عن بعد من خلال بوابة VPN ل SSL يتم تمكين طبقة مأخذ التوصيل الآمنة (SSL-enabled). تتيح بوابة SSL VPN للمستخدمين البعيدين إنشاء نفق VPN آمن. باستخدام شبكة VPN الخاصة بنظام Cisco IOS XE SSL، يمكن للمستخدمين النهائيين الوصول بشكل آمن من المنزل وأ أي موقع دعم الإنترنت مثل النقاط الفعالة اللاسلكية. كما تتيح الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول Cisco IOS XE SSL للشركات إمكانية الوصول إلى شبكات الشركات للشركاء والمستشاريين في الخارج، من أجل حماية بيانات الشركات.

هذه الميزة مدعومة على الأنظمة الأساسية المحددة:

المنصة	إصدار IOS XE المدعوم من Cisco
سلسلة موجه خدمات الشبكة السحابية 1000V من Cisco	Cisco IOS XE الإصدار 16.9
Cisco Catalyst 8000v	Cisco IOS XE Bengaluru، الإصدار 17.4.1
موجه الخدمات المدمجة Cisco 4461 Integrated Services Router موجه الخدمات المدمجة Cisco 4451 Integrated Services Router موجه الخدمات المدمجة Cisco 4431 Integrated Services Router	Cisco IOS XE Cuteno 17.7.1a

التكوين

الرسم التخطيطي للشبكة



التكوينات

1. تمكين المصادقة والتفويض والمحاسبة (AAA) وتكوين المصادقة وقوائم التخويل وإضافة اسم مستخدم إلى قاعدة البيانات المحلية.

```
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network default local
!
username test password cisco123
```

2. قم بإنشاء TrustPoint لتثبيت شهادة الهوية، إذا لم تكن موجودة بالفعل للمصادقة المحلية. يمكنك الرجوع إلى تسجيل الشهادة لـ PKI للحصول على مزيد من التفاصيل حول إنشاء الشهادة.

```
crypto pki trustpoint SSL
 enrollment mode ra
 enrollment url http://x.x.x.x:80/certsrv/mscep/mscep.dll
 subject-name cn=sslvpn.cisco.com
 revocation-check crl
 rsakeypair SSL-Keys
```

3. تكوين مقترح SSL.

```
crypto ssl proposal SSL_Proposal
 protection rsa-3des-ede-sha1 rsa-aes128-sha1
```

4. تكوين سياسة SSL واستدعاء مقترح SSL ونقطة ثقة PKI.

```
crypto ssl policy SSL_Policy
 ssl proposal SSL_Proposal
 pki trustpoint SSL sign
 ip address local y.y.y.y port 443
 no shut
```

Y.Y.Y هو عنوان IP لـ GigabitEthernet0/0/0.

5. (إختياري) قم بتكوين قائمة وصول قياسية ليتم إستخدامها للنفق المنقسم. تتكون قائمة الوصول هذه من الشبكات الوجهة التي يمكن الوصول إليها من خلال نفق VPN. بشكل افتراضي، تمر جميع حركة مرور البيانات عبر نفق VPN (النفق الكامل) إذا لم يتم تكوين النفق المقسم.

```
ip access-list standard split_tunnel_acl
 10 permit 192.168.10.0 0.0.0.255
```

6. إنشاء تجمع عناوين IPv4.

```
ip local pool SSLVPN_POOL 192.168.20.1 192.168.20.10
```

يعين تجمع عناوين IP الذي تم إنشاؤه عنوان IPv4 لعميل AnyConnect أثناء اتصال AnyConnect بنجاح.

7. قم بتحميل صورة وحدة الاستقبال والبث الخاصة بـ AnyConnect (WebDeployment) ضمن دليل WebVPN الخاص بذاكرة التمهيد وتحميل ملف تعريف العميل إلى ذاكرة التمهيد للموجه.

```
mkdir bootflash:webvpn
```

لحزمة AnyConnect :

```
copy tftp: bootflash:webvpn:
```

لملف تعريف العميل :

```
copy tftp: bootflash:
```

قم بتعريف صورة AnyConnect وملف تعريف العميل كما هو محدد:

```
crypto vpn anyconnect bootflash:/webvpn/anyconnect-win-4.10.04065-webdeploy-k9.pkg sequence 1
!
crypto vpn anyconnect profile sslvpn_client_profile bootflash:/sslvpn_client_profile.xml
```

8. تكوين نهج تخويل.

```
crypto ssl authorization policy SSL_Author_Policy
 rekey time 1110
 client profile sslvpn_client_profile
 mtu 1000
 keepalive 500
 dpd-interval client 1000
 netmask 255.255.255.0
 pool SSLVPN_POOL
 dns 8.8.8.8
 banner This is SSL VPN tunnel.
 route set access-list split_tunnel_acl
```

يتم تحديد تجمع IP و DNS وقائمة النفق المقسم، وما إلى ذلك ضمن نهج التخويل.

9. تكوين قالب ظاهري يتم من خلاله نسخ واجهات الوصول الظاهري.

```
interface Virtual-Template1 type vpn
 ip unnumbered GigabitEthernet0/0/0
 ip mtu 1400
 ip tcp adjust-mss 1300
```

يحصل الأمر غير المرقم على عنوان IP من الواجهة التي تم تكوينها (GigabitEthernet0/0/0) ويتم تمكين توجيه IPv4 على تلك الواجهة.

10. قم بتكوين ملف تعريف SSL ومطابقة نهج SSL الذي تم إنشاؤه بموجب مع معلمات المصادقة والتفويض والقالب الظاهري.

```
crypto ssl profile SSL_Profile
 match policy SSL_Policy
 aaa authentication user-pass list default
 aaa authorization group user-pass list default SSL_Author_Policy
 authentication remote user-pass
 virtual-template 1
```

إنشاء توصيف AnyConnect بمساعدة محرر توصيفات AnyConnect. يتم توفير قصاصة من ملف تعريف XML لمرجع الخاص بك.

```
!
!
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="false">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="true">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
```

```
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>SSLVPN</HostName>
<HostAddress>sslvpn.cisco.com</HostAddress>
</HostEntry>
</ServerList>
!
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

<#root>

1. Check the ssl connection parameters for your anyconnect connection

sslvpn# show crypto ssl session user test

```
Interface         : Virtual-Access1
Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 4.10.04065

Username      : test                  Num Connection : 1
Public IP     : 10.106.52.195
Profile       : SSL_Profile
Policy        : SSL_Policy
Last-Used     : 00:03:58              Created : *05:11:06.166 UTC Wed Feb 22 2023
Tunnel IP     : 192.168.20.10         Netmask : 255.255.255.0
Rx IP Packets : 174                   Tx IP Packets : 142
```

2. Verify the SSL session status

sslvpn# show crypto ssl session

```
SSL profile name: SSL_Profile
Client_Login_Name  Client_IP_Address    No_of_Connections   Created     Last_Used
test               10.106.52.195            1              00:03:32    00:03:32
```

3. Verify the tunnel statistics for the active connection

sslvpn# show crypto ssl stats tunnel

```
SSLVPN Profile name : SSL_Profile
Tunnel Statistics:
Active connections       : 1
Peak connections         : 1             Peak time : 5d12h
Connect succeed          : 10            Connect failed : 0
Reconnect succeed        : 38            Reconnect failed : 0
IP Addr Alloc Failed     : 0             VA creation failed : 0
DPD timeout              : 0
Client
in CSTP frames           : 129           in CSTP control : 129
in CSTP data             : 0             in CSTP bytes : 1516
out CSTP frames          : 122           out CSTP control : 122
out CSTP data            : 0             out CSTP bytes : 1057
cef in CSTP data frames  : 0             cef in CSTP data bytes : 0
cef out CSTP data frames : 0             cef out CSTP data bytes : 0
Server
In IP pkts               : 0             In IP bytes : 0
In IP6 pkts              : 0             In IP6 bytes : 0
Out IP pkts              : 0             Out IP bytes : 0
Out IP6 pkts             : 0             Out IP6 bytes : 0
```

4. Check the actual configuration applied for the Virtual-Acces interface associated with client

sslvpn# show derived-config interface virtual-access 1

```
Building configuration...

Derived configuration : 171 bytes
!
interface Virtual-Access1
description ***Internally created by SSLVPN context profile1***
ip unnumbered GigabitEthernet0/0/0
ip mtu 1400
ip tcp adjust-mss 1300
```

استكشاف الأخطاء وإصلاحها

يوفر هذه القسم المعلومات التي يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

1. تصحيح أخطاء SSL للتجميع من وحدة الاستقبال والبث:

```
debug crypto ssl condition client username <username>
debug crypto ssl aaa
debug crypto ssl aggr-auth message
debug crypto ssl aggr-auth packets
debug crypto ssl tunnel errors
debug crypto ssl tunnel events
debug crypto ssl tunnel packets
debug crypto ssl package
```

2. بعض الأوامر الإضافية لاستكشاف أخطاء اتصال SSL وإصلاحها:

```
# show crypto ssl authorization policy
# show crypto ssl diagnose error
# show crypto ssl policy
# show crypto ssl profile
# show crypto ssl proposal
# show crypto ssl session profile <profile_name>
# show crypto ssl session user <username> detail
# show crypto ssl session user <username> platform detail
```

3. DART من عميل AnyConnect.

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).