Configurazione di AnyConnect SSL VPN per ISR4k con autenticazione locale

Sommario

Introduzione

In questo documento viene descritta una configurazione di esempio di come configurare un headend ISR (Integrated Service Router) 4k Cisco IOS® XE per una VPN AnyConnect Secure Sockets Layer (SSL) con un database utenti locale.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco IOS XE (ISR 4K)
- AnyConnect Secure Mobility Client
- Operazione SSL generale
- PKI (Public Key Infrastructure)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISR 4451-X/K9 Router con versione 17.9.2a
- AnyConnect Secure Mobility Client 4.10.04065

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

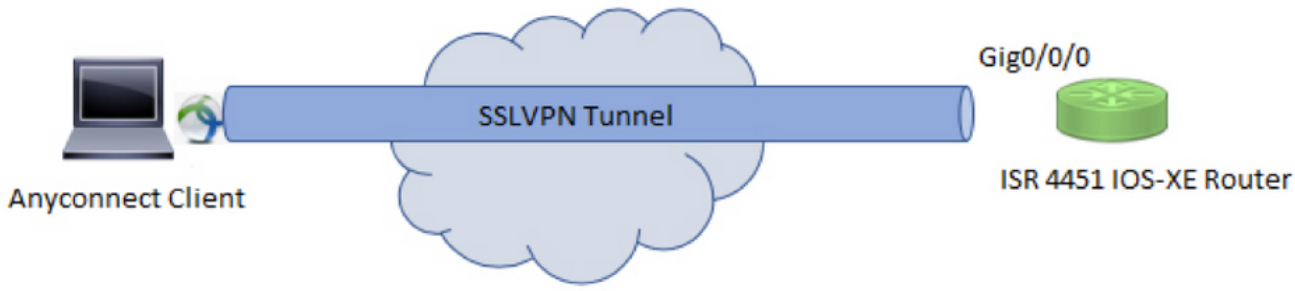
La funzionalità SSL Virtual Private Network (VPN) fornisce il supporto nel software Cisco IOS XE per l'accesso remoto degli utenti alle reti aziendali da qualsiasi punto di Internet. L'accesso remoto viene fornito tramite un gateway VPN SSL abilitato per SSL (Secure Socket Layer). Il gateway VPN SSL consente agli utenti remoti di stabilire un tunnel VPN sicuro. Con Cisco IOS XE SSL VPN, gli utenti finali ottengono l'accesso in modo sicuro da casa o da qualsiasi luogo abilitato per Internet, ad esempio gli hotspot wireless. Cisco IOS XE SSL VPN consente inoltre alle aziende di estendere l'accesso alla rete aziendale a partner e consulenti offshore, per la protezione dei dati aziendali.

Questa funzionalità è supportata sulle piattaforme specificate:

Piattaforma	Versione Cisco IOS XE supportata
Cisco Cloud Services Router serie 1000V	Cisco IOS XE release 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Cisco 4461 Integrated Services Router Cisco 4451 Integrated Services Router Cisco 4431 Integrated Services Router	Cisco IOS XE Cupertino 17.7.1a

Configurazione

Esempio di rete



Configurazioni

1. Abilitare l'autenticazione, l'autorizzazione e l'accounting (AAA), configurare l'autenticazione, gli elenchi di autorizzazioni e aggiungere un nome utente al database locale.

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

2. Creare un trust point per installare il certificato di identità, se non è già presente per l'autenticazione locale. È possibile fare riferimento a Registrazione certificato per una PKI per ulteriori dettagli sulla creazione del certificato.

```
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. Configurare una proposta SSL.

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

4. Configurare un criterio SSL e chiamare la proposta SSL e il trust point 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 è l'indirizzo IP di Gigabit Ethernet0/0/0.

5. (Facoltativo) Configurare un elenco degli accessi standard da utilizzare per il tunnel separato. Questo elenco degli accessi è composto dalle reti di destinazione a cui è possibile accedere tramite il tunnel VPN. Per impostazione predefinita, tutto il traffico passa attraverso il tunnel VPN (Full Tunnel) se il tunnel suddiviso non è configurato.

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

6. Creare un pool di indirizzi IPv4.

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

Il pool di indirizzi IP creato assegna un indirizzo IPv4 al client AnyConnect durante una connessione AnyConnect riuscita.

7. Caricare l'immagine headend AnyConnect (webdeploy) nella directory webvpn di bootflash e caricare il profilo del client sulla bootflash del router.

```
mkdir bootflash:webvpn
```

Per il pacchetto Anyconnect:

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

Per il profilo client:

```
copy tftp: bootflash:
```

Definire l'immagine AnyConnect e il profilo client come specificato:

```
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. Configurare un criterio di autorizzazione.

```
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
```

Il pool IP, il DNS, l'elenco dei tunnel suddivisi e così via sono specificati nei criteri di autorizzazione.

9. Configurare un modello virtuale da cui vengono clonate le interfacce di accesso virtuale.

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

Il comando senza numero ottiene l'indirizzo IP dall'interfaccia configurata (Gigabit Ethernet0/0/0) e il routing IPv4 è abilitato su tale interfaccia.

10. Configurare un profilo SSL e soddisfare i criteri SSL creati al suo interno insieme ai parametri di autenticazione e autorizzazione e al modello virtuale.

```
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
```

Creare un profilo AnyConnect con l'aiuto dell'Editor di profili AnyConnect. Viene fornito un frammento del profilo XML come riferimento.

```
!
!
<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>
!
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

<#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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

1. Debug SSL da raccogliere dall'headend:

```
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. Alcuni comandi aggiuntivi per risolvere i problemi di connessione SSL:

```
# 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 dal client AnyConnect.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).