AnyConnect: Configurazione della VPN SSL di base per l'headend del router Cisco IOS con CLI

Introduzione

Sommario

In questo documento viene descritta la configurazione base di un router Cisco IOS® come headend VPN (SSL) AnyConnect Secure Sockets Layer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco IOS
- AnyConnect Secure Mobility Client
- Operazione SSL generale

Componenti usati

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

- Router Cisco 892W con 15.3(3)M5
- AnyConnect Secure Mobility Client 3.1.0809

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

Informazioni sulle licenze per le diverse versioni di IOS

- Per utilizzare le funzionalità VPN SSL, è necessario il gruppo di funzionalità SecurityKey9, indipendentemente dalla versione di Cisco IOS in uso.
- Cisco IOS 12.x - la funzionalità VPN per SSL è integrata in tutte le immagini 12.x che iniziano con 12.4(6)T con almeno una licenza per la sicurezza (ad esempio advsecurityk9, adventerprisek9 e così via).
- Cisco IOS 15.0 - le versioni precedenti richiedono l'installazione di un file LIC sul router, che consente di effettuare 10, 25 o 100 connessioni utente. Le licenze Right to Use* sono state implementate in 15.0(1)M4
- Cisco IOS 15.1 - le versioni precedenti richiedono l'installazione di un file LIC sul router, che consente di effettuare 10, 25 o 100 connessioni utente. Le licenze Right to Use* sono state implementate nelle versioni 15.1(1)T2, 15.1(2)T2, 15.1(3)T e 15.1(4)M1
- Cisco IOS 15.2 - tutte le versioni 15.2 offrono licenze Right to Use* per VPN
- Cisco IOS versione 15.3 e successive - le versioni precedenti offrono le licenze Right to Use*. A partire dalla versione 15.3(3)M, la funzionalità SSLVPN è disponibile dopo l'avvio in un pacchetto con tecnologia SecurityK9

Per le licenze RTU, una licenza di valutazione verrà abilitata quando viene configurata la prima funzionalità webvpn (webvpn gateway GATEWAY1) e viene accettato il contratto di licenza con l'utente finale (EULA). Dopo 60 giorni, questa licenza di valutazione diventa una licenza permanente. Queste licenze sono basate sull'onore e richiedono una licenza cartacea per poter utilizzare la funzione. Inoltre, invece di essere limitata a un certo numero di utenti, l'RTU consente il numero massimo di connessioni simultanee che la piattaforma del router può supportare contemporaneamente.

Miglioramenti software significativi

Di seguito sono riportati gli ID dei bug che hanno portato a importanti funzionalità o correzioni per AnyConnect:

- CSCti8976: supporto aggiunto per AnyConnect 3.x a IOS
- CSCtx38806: correzione per vulnerabilità BESTIA, Microsoft KB2585542

Configurazione

Passaggio 1. Conferma abilitazione licenza

Il primo passaggio della configurazione di AnyConnect su un headend di router IOS è verificare che la licenza sia stata installata correttamente (se applicabile) e abilitata. Per le specifiche sulle licenze sulle diverse versioni, consultare le informazioni sulle licenze nella sezione precedente. A seconda della versione del codice e della piattaforma, il comando show license restituisce una licenza SSL_VPN o securityk9. Indipendentemente dalla versione e dalla licenza, il contratto di licenza dovrà essere accettato e la licenza verrà visualizzata come Attiva.

Passaggio 2. Caricare e installare il pacchetto AnyConnect Secure Mobility Client sul router

Per caricare un'immagine AnyConnect sulla VPN, l'headend ha due finalità. In primo luogo, solo i sistemi operativi che hanno immagini AnyConnect presenti sull'headend AnyConnect saranno autorizzati a connettersi. Ad esempio, i client Windows richiedono l'installazione di un pacchetto Windows sull'headend, i client Linux a 64 bit richiedono un pacchetto Linux a 64 bit e così via. In secondo luogo, al momento della connessione, l'immagine AnyConnect installata sull'headend viene automaticamente spostata sul computer client. Gli utenti che si connettono per la prima volta potranno scaricare il client dal portale Web e gli utenti che ritornano potranno eseguire l'aggiornamento, a condizione che il pacchetto AnyConnect sull'headend sia più recente di quello installato sul computer client.

I pacchetti AnyConnect sono disponibili nella sezione AnyConnect Secure Mobility Client del sito Web dei download di software Cisco. Sebbene siano disponibili molte opzioni, i pacchetti da installare sull'headend saranno etichettati con il sistema operativo e l'installazione headend (PKG). I pacchetti AnyConnect sono attualmente disponibili per le seguenti piattaforme di sistemi operativi: Windows, Mac OS X, Linux (32 bit) e Linux a 64 bit. Si noti che per Linux sono disponibili sia pacchetti a 32 che a 64 bit. Ogni sistema operativo richiede l'installazione del pacchetto appropriato sull'headend per consentire le connessioni.

Una volta scaricato, il pacchetto AnyConnect può essere caricato nella memoria flash del router con il comando **copy** tramite TFTP, FTP, SCP o altre opzioni. Di seguito è riportato un esempio:

```
copy tftp: flash:/webvpn/

Address or name of remote host []? 192.168.100.100
Source filename []? anyconnect-win-3.1.08009-k9.pkg
Destination filename [/webvpn/anyconnect-win-3.1.08009-k9.pkg]?
Accessing tftp://192.168.100.100/anyconnect-win-3.1.08009-k9.pkg...
Loading anyconnect-win-3.1.08009-k9.pkg from 192.168.100.100 (via GigabitEthernet0):
!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 37997096 bytes]

37997096 bytes copied in 117.644 secs (322984 bytes/sec)
```

Dopo aver copiato l'immagine AnyConnect nella memoria flash del router, occorre installarla dalla

riga di comando. Quando si specifica un numero di sequenza alla fine del comando di installazione, è possibile installare più pacchetti AnyConnect; in questo modo, il router potrà funzionare come headend per più sistemi operativi client. Quando si installa il pacchetto AnyConnect, lo si sposta anche nella **directory flash:/webvpn/,** se non è stato copiato inizialmente in questa posizione.

```
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1

SSLVPN Package SSL-VPN-Client (seq:1): installed successfully
```

Nelle versioni di codice rilasciate prima della 15.2(1)T, il comando per installare PKG è leggermente diverso.

```
webvpn install svc flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
```

Passaggio 3. Generare la coppia di chiavi RSA e il certificato autofirmato

Quando si configura SSL o una funzionalità che implementa l'infrastruttura a chiave pubblica (PKI) e i certificati digitali, per la firma del certificato è necessaria una coppia di chiavi Rivest-Shamir-Adleman (RSA). Questo comando genererà una coppia di chiavi RSA che verrà quindi utilizzata quando viene generato il certificato PKI autofirmato. Usare un modulo di 2048 bit non è un requisito, ma si consiglia di usare il modulo più grande disponibile per una maggiore sicurezza e compatibilità con i computer client AnyConnect. Si consiglia inoltre di utilizzare un'etichetta di chiave descrittiva da assegnare con la gestione delle chiavi. La generazione della chiave può essere confermata con il comando **show crypto key mypubkey rsa**.

> **Nota:** Poiché esistono molti rischi di sicurezza associati alla possibilità di esportare le chiavi RSA, la procedura consigliata consiste nel verificare che le chiavi siano configurate in modo da non essere esportabili, ovvero l'impostazione predefinita. I rischi che si corrono quando si rendono esportabili le chiavi RSA sono discussi in questo documento: Implementazione delle chiavi RSA in una PKI.

```
crypto key generate rsa label SSLVPN_KEYPAIR modulus 2048

The name for the keys will be: SSLVPN_KEYPAIR

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

show crypto key mypubkey rsa SSLVPN_KEYPAIR

% Key pair was generated at: 14:01:34 EDT May 21 2015
Key name: SSLVPN_KEYPAIR
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C4C7D6 F9533CD3 A5489D5A 4DC3BAE7 6831E832 7326E322 CBECC41C 8395A5F7
4613AF70 827F581E 57F72074 FD803EEA 693EBACC 0EE5CA65 5D1875C2 2F19A432
```

```
84188F61 4E282EC3 D30AE4C9 1F2766EF 48269FE2 0C1AECAA 81511386 1BA6709C
7C5A2A40 2FBB3035 04E3770B 01155368 C4A5B488 D38F425C 23E430ED 80A8E2BD
E713860E F654695B C1780ED6 398096BC 55D410DB ECC0E2D9 2621E1AB A418986D
39F241FE 798EF862 9D5EAEEB 5B06D73B E769F613 0FCE2585 E5E6DFF3 2E48D007
3443AD87 0E66C2B1 4E0CB6E9 81569DF2 DB0FE9F1 1A9E737F 617DC68B 42B78A8B
952CD997 78B96CE6 CB623328 C2C5FFD6 18C5DA2C 2EAFA936 5C866DE8 5184D2D3
6D020301 0001
```

Una volta generata correttamente la coppia di chiavi RSA, è necessario configurare un trust point PKI con le informazioni sul router e la coppia di chiavi RSA. Il nome comune (CN) nel nome soggetto deve essere configurato con l'indirizzo IP o il nome di dominio completo (FQDN) usato dagli utenti per connettersi al gateway AnyConnect; in questo esempio, i client utilizzano il nome di dominio completo (FQDN) di fdenofa-SSLVPN.cisco.com quando tentano di connettersi. Sebbene non sia obbligatorio, quando si immette correttamente nella CN, consente di ridurre il numero di errori di certificato che vengono visualizzati al momento dell'accesso.

> **Nota:** Anziché utilizzare un certificato autofirmato generato dal router, è possibile utilizzare un certificato rilasciato da una CA di terze parti. A tale scopo, è possibile utilizzare diversi metodi, come illustrato in questo documento: Configurazione della registrazione dei certificati per una PKI.

```
crypto pki trustpoint SSLVPN_CERT
 enrollment selfsigned
 subject-name CN=fdenofa-SSLVPN.cisco.com
 rsakeypair SSLVPN_KEYPAIR
```

Dopo aver definito correttamente il trust point, il router deve generare il certificato utilizzando il comando **crypto pki enroll**. Con questa procedura, è possibile specificare alcuni altri parametri, quali il numero di serie e l'indirizzo IP. Tuttavia, questa operazione non è necessaria. La generazione del certificato può essere confermata con il comando **show crypto pki certificates**.

```
crypto pki enroll SSLVPN_CERT

% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created

show crypto pki certificates SSLVPN_CERT

Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Subject:
    Name: fdenofa-892.fdenofa.lab
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Validity Date:
    start date: 18:54:04 EDT Mar 30 2015
    end   date: 20:00:00 EDT Dec 31 2019
  Associated Trustpoints: SSLVPN_CERT
```

Passaggio 4. Configurare gli account utente della VPN locale

Sebbene sia possibile utilizzare un server esterno di autenticazione, autorizzazione e accounting (AAA), per questo esempio viene utilizzata l'autenticazione locale. Questi comandi creano un nome utente VPNUSER e un elenco di autenticazione AAA denominato SSLVPN_AAA.

```
aaa new-model
aaa authentication login SSLVPN_AAA local
username VPNUSER password TACO
```

Passaggio 5. Definire il pool di indirizzi e l'elenco di accesso al tunnel suddiviso che i client devono utilizzare

Affinché le schede client AnyConnect possano ottenere un indirizzo IP, è necessario creare un pool di indirizzi IP locali. Accertarsi di configurare un pool abbastanza grande da supportare il numero massimo di connessioni client AnyConnect simultanee.

Per impostazione predefinita, AnyConnect funzionerà in modalità tunnel completo, ossia il traffico generato dal client verrà inviato attraverso il tunnel. Poiché questa operazione non è in genere consigliabile, è possibile configurare un Access Control List (ACL) che definisce quindi il traffico che deve o non deve essere inviato attraverso il tunnel. Come per altre implementazioni di ACL, il rifiuto implicito alla fine elimina la necessità di un rifiuto esplicito; pertanto, è necessario solo configurare le istruzioni di autorizzazione per il traffico che deve essere tunneling.

```
ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Passaggio 6. Configurazione dell'interfaccia VTI (Virtual-Template Interface)

VTI dinamici fornire un'interfaccia di accesso virtuale separata su richiesta per ciascuna sessione VPN che consenta una connettività altamente sicura e scalabile per le VPN ad accesso remoto. La tecnologia DVTI sostituisce le mappe crittografiche dinamiche e il metodo hub e spoke dinamico che aiuta a stabilire i tunnel. Poiché i servizi DVTI funzionano come qualsiasi altra interfaccia reale, consentono una distribuzione di Accesso remoto più complessa in quanto supportano QoS, firewall, attributi per utente e altri servizi di sicurezza non appena il tunnel è attivo.

```
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Virtual-Template 1
 ip unnumbered Loopback0
```

Passaggio 7. Configurare il gateway WebVPN

Il gateway WebVPN definisce l'indirizzo IP e le porte che verranno utilizzate dall'headend AnyConnect, nonché l'algoritmo di crittografia SSL e il certificato PKI che verranno presentati ai client. Per impostazione predefinita, il gateway supporta tutti i possibili algoritmi di crittografia, che variano a seconda della versione di Cisco IOS sul router.

```
webvpn gateway SSLVPN_GATEWAY
 ip address 209.165.201.1 port 443
```

```
 http-redirect port 80
 ssl trustpoint SSLVPN_CERT
 inservice
```

Passaggio 8. Configurare il contesto e i Criteri di gruppo di WebVPN

Il contesto e i Criteri di gruppo di WebVPN definiscono alcuni parametri aggiuntivi che verranno utilizzati per la connessione del client AnyConnect. Per una configurazione AnyConnect di base, il contesto funge semplicemente da meccanismo utilizzato per chiamare i Criteri di gruppo predefiniti che verranno utilizzati per AnyConnect. Tuttavia, il contesto può essere utilizzato per personalizzare ulteriormente la pagina iniziale WebVPN e l'operazione WebVPN. Nel gruppo di criteri definito, l'elenco SSLVPN_AAA è configurato come elenco di autenticazione AAA di cui gli utenti sono membri. Il comando **function svc-enabled** è l'elemento della configurazione che consente agli utenti di connettersi con il client VPN AnyConnect SSL anziché con la semplice VPN Web tramite un browser. Infine, i comandi SVC aggiuntivi definiscono i parametri relativi solo alle connessioni SVC: **svc address-pool** indica al gateway di distribuire gli indirizzi di SSLVPN_POOL ai client, **svc split include** definisce i criteri del tunnel suddiviso per ACL 1 definiti in precedenza e **svc dns-server** definisce il server DNS da utilizzare per la risoluzione dei nomi di dominio. Con questa configurazione, tutte le query DNS verranno inviate al server DNS specificato. L'indirizzo ricevuto nella risposta alla query determinerà se il traffico verrà inviato o meno attraverso il tunnel.

```
webvpn context SSLVPN_CONTEXT
virtual-template 1
 aaa authentication list SSLVPN_AAA
gateway SSLVPN_GATEWAY inservice
policy group SSLVPN_POLICY functions svc-enabled svc address-pool "SSLVPN_POOL" netmask
255.255.255.0 svc split include acl 1 svc dns-server primary 8.8.8.8
default-group-policy SSLVPN_POLICY
```

Passaggio 9 (Facoltativo) Configurazione di un profilo client

A differenza delle appliance ASA, Cisco IOS non dispone di un'interfaccia GUI integrata che possa aiutare gli amministratori a creare il profilo del client. Il profilo del client AnyConnect deve essere creato/modificato separatamente con l'Editor di profili autonomo.

> **Suggerimento**: Cercare anyconnect-profileeditor-win-3.1.03103-k9.exe.

Per fare in modo che il router distribuisca il profilo, attenersi alla procedura seguente:

- Caricarlo su IOS Flash con ftp/tftp.
- Utilizzare questo comando per identificare il profilo appena caricato:

```
crypto vpn annyconnect profile SSLVPN_PROFILE flash:test-profile.xml
```

> **Suggerimento**: Nelle versioni Cisco IOS precedenti alla 15.2(1)T, è necessario usare questo comando: **webvpn import svc profile <nome_profilo> flash:<profilo.xml>**

3. Nel contesto, utilizzare questo comando per collegare il profilo a tale contesto:

```
webvpn context SSLVPN_CONTEXT
 policy group SSLVPN_POLICY
```

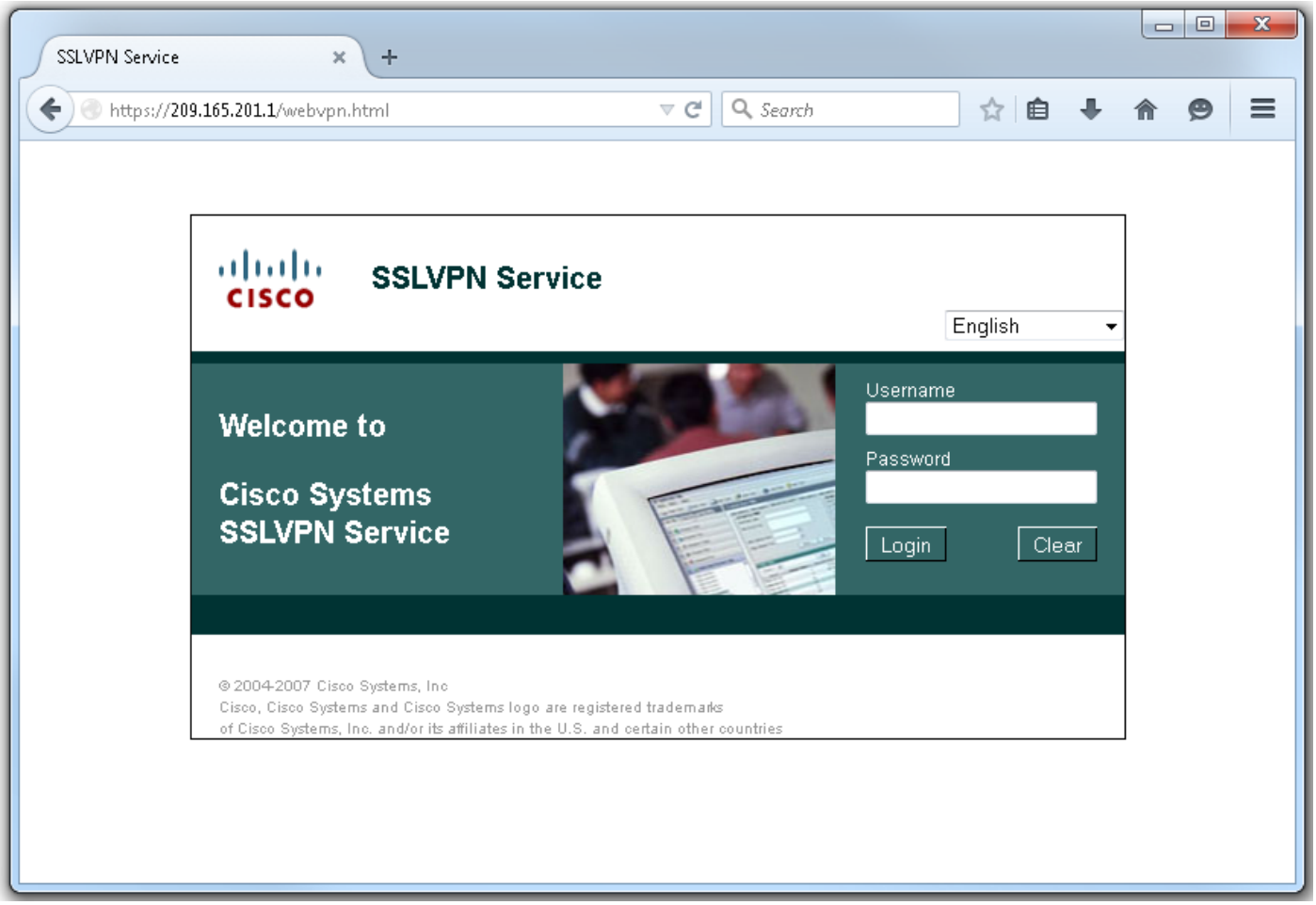
```
svc profile SSLVPN_PROFILE
```

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca dei comandi (solo utenti registrati).]

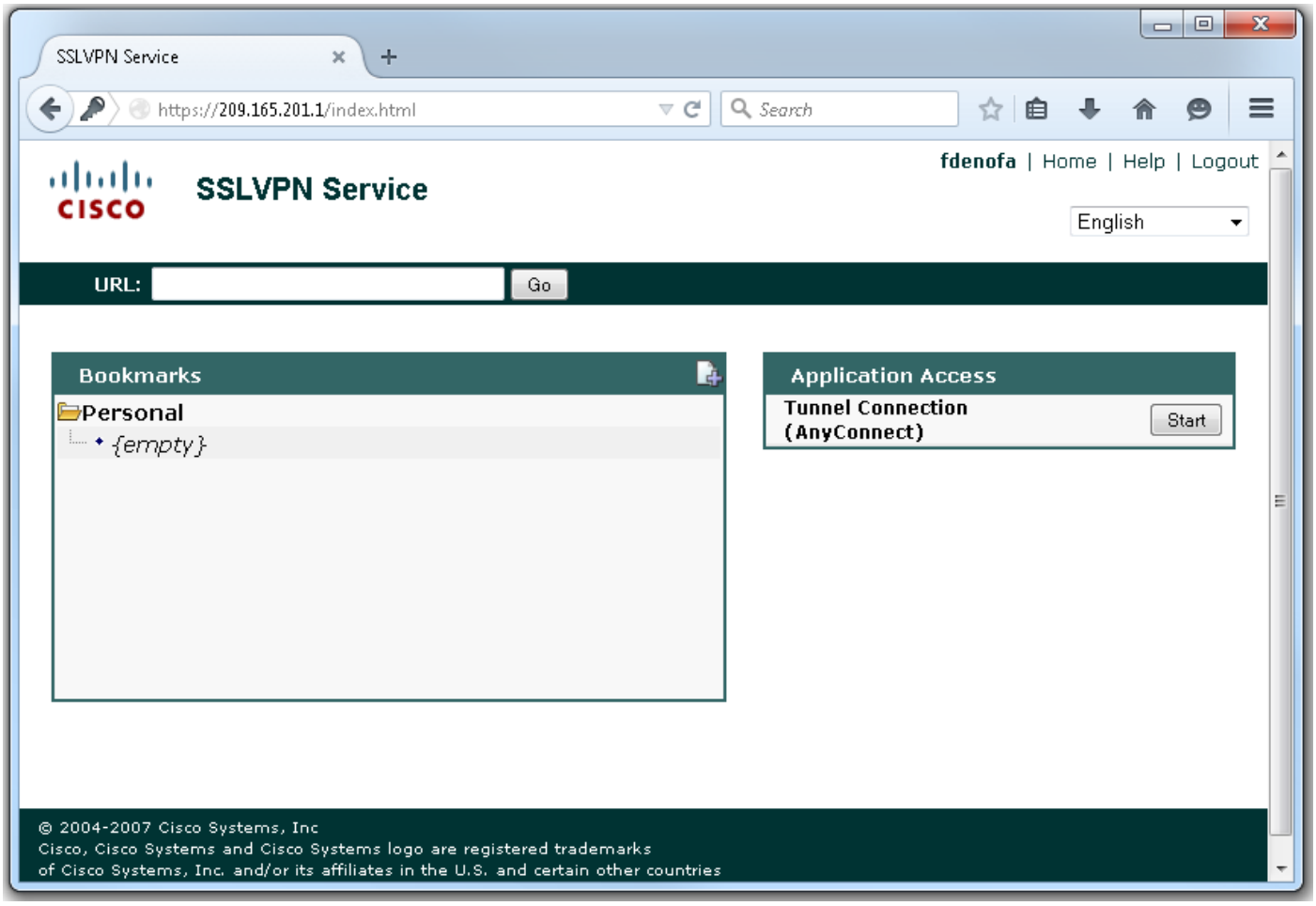
Verifica

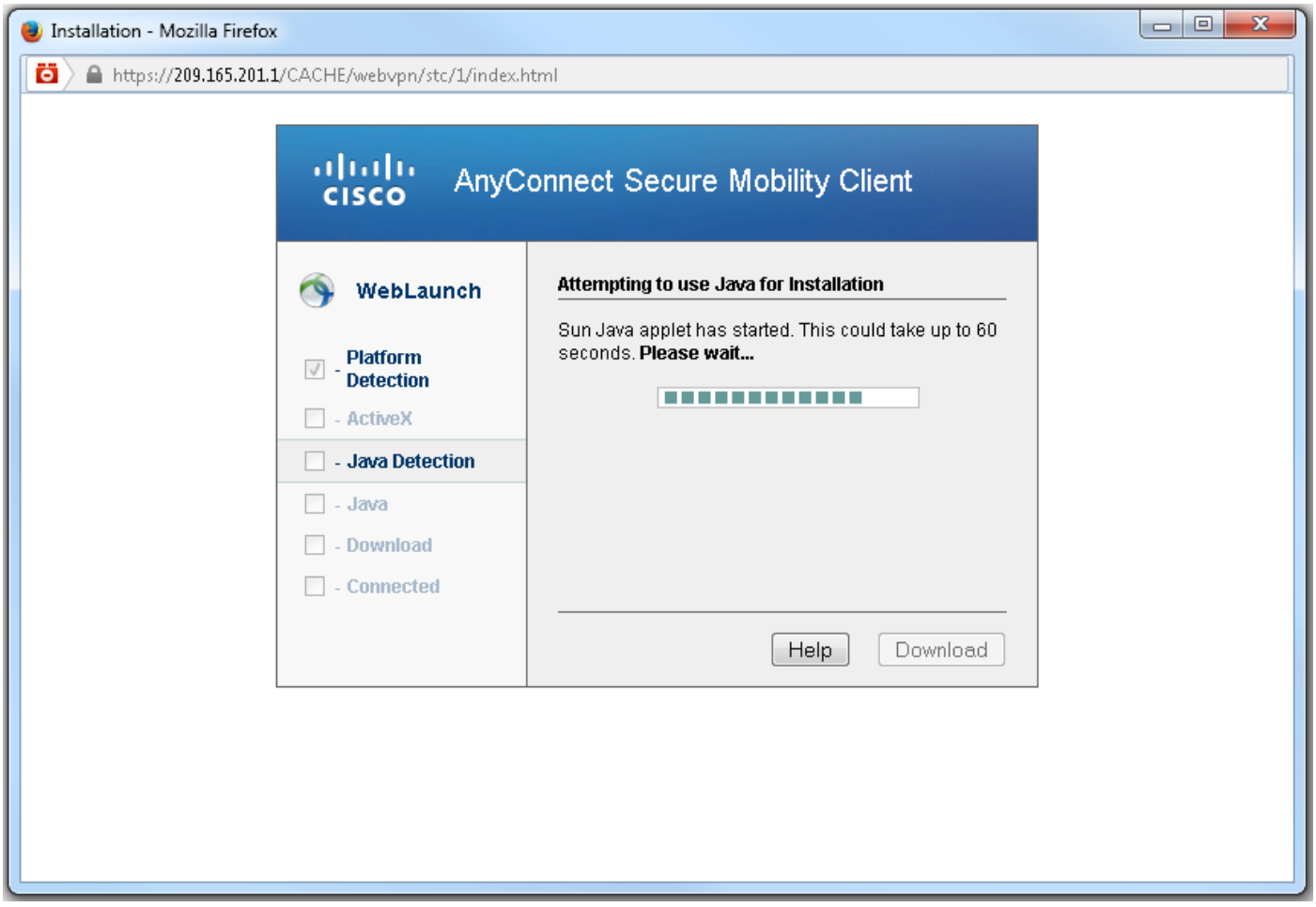
Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Al termine della configurazione, quando si accede all'indirizzo e alla porta del gateway tramite browser, viene visualizzata nuovamente la pagina WebVPN.



Dopo aver eseguito l'accesso, viene visualizzata la home page WebVPN. Da qui, fare clic su **Connessione tunnel (AnyConnect).** Quando si usa Internet Explorer, ActiveX viene usato per comprimere e installare il client AnyConnect. Se non viene rilevato, verrà utilizzato Java. Tutti gli altri browser utilizzano Java immediatamente.

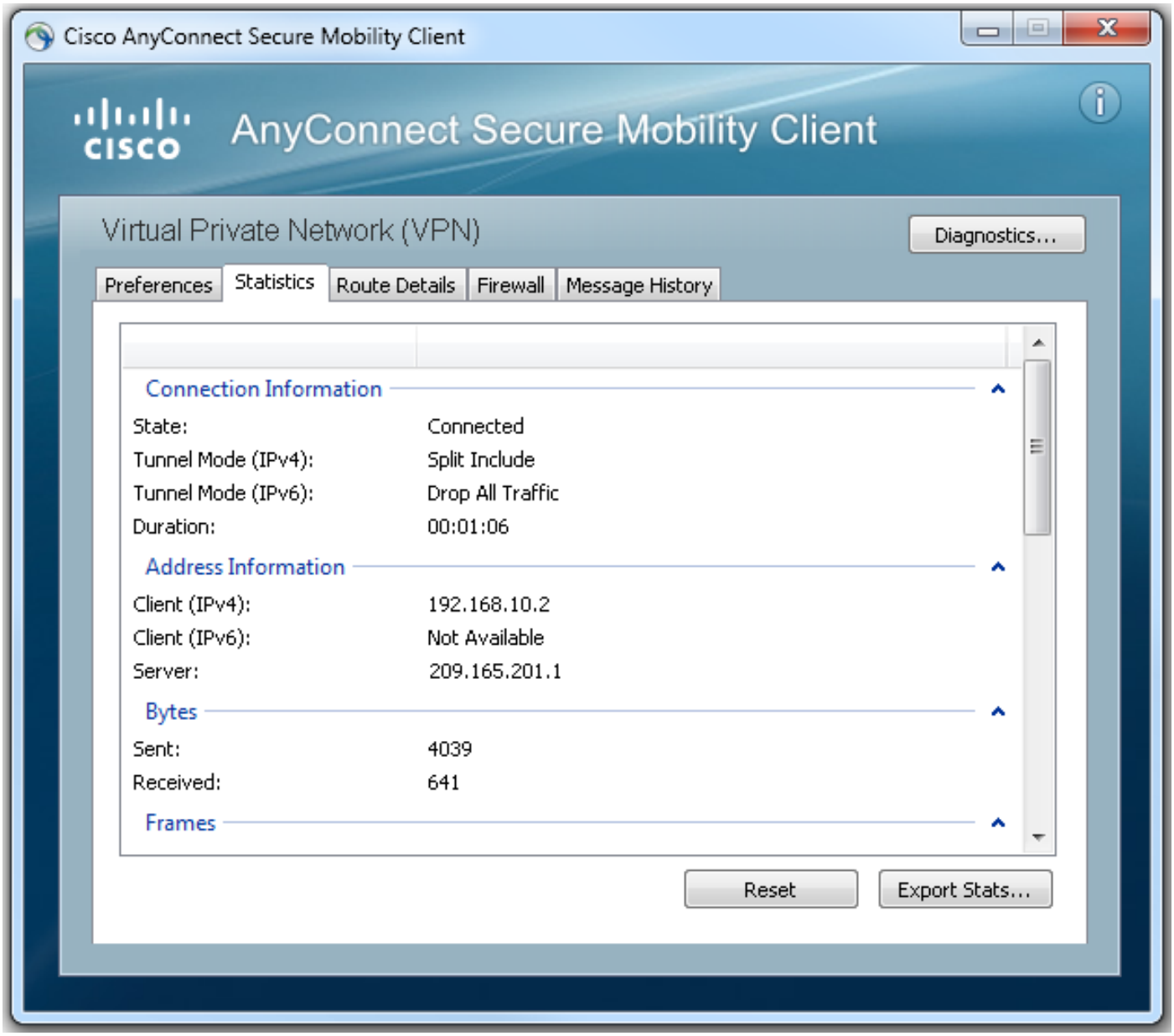


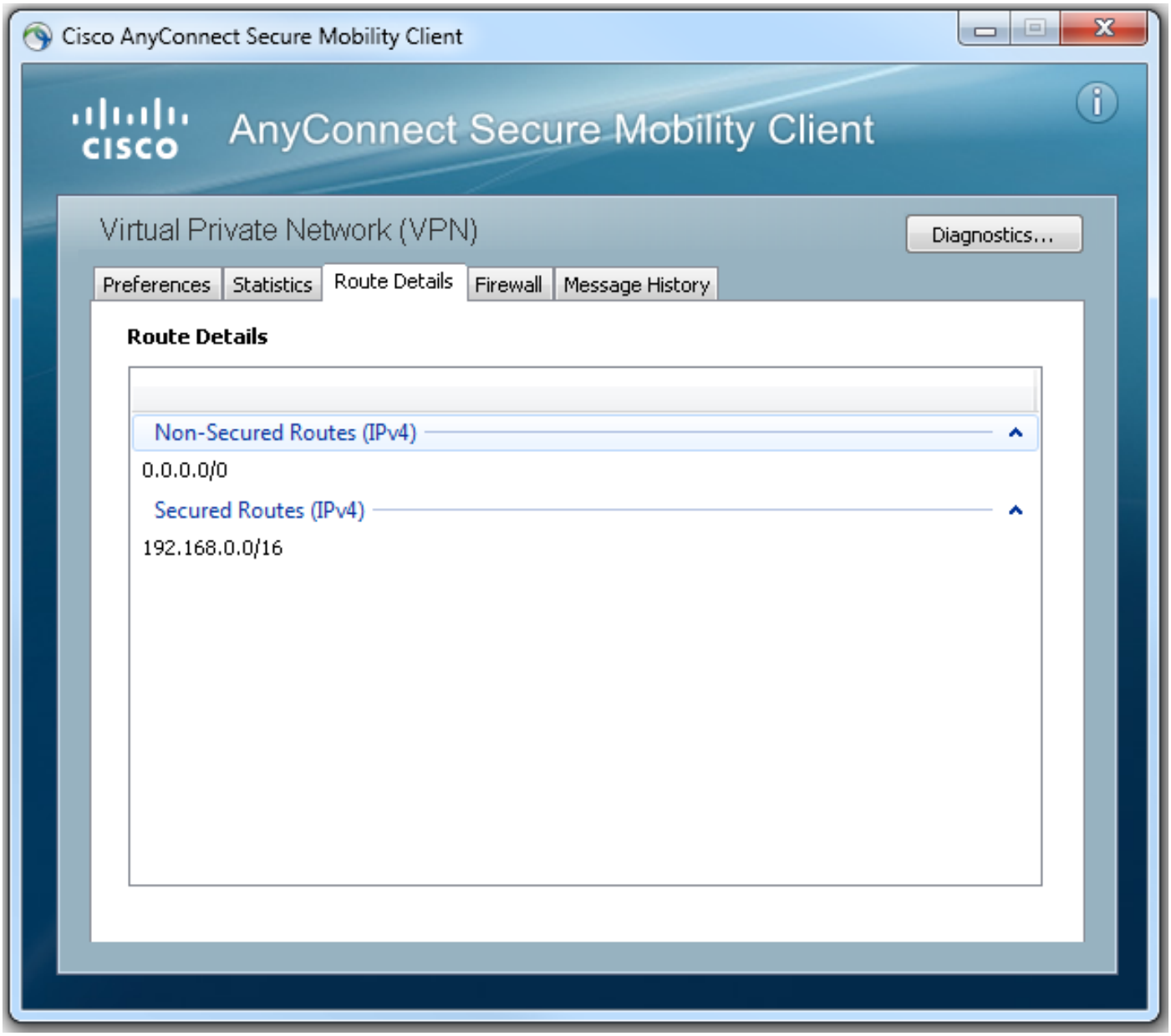


Al termine dell'installazione, AnyConnect tenterà automaticamente di connettersi al gateway WebVPN. Poiché per l'identificazione del gateway viene utilizzato un certificato autofirmato,

durante il tentativo di connessione verranno visualizzati più avvisi relativi ai certificati. Questi elementi sono previsti e devono essere accettati affinché la connessione possa continuare. Per evitare la visualizzazione di questi avvisi relativi ai certificati, è necessario che il certificato autofirmato presentato sia installato nell'archivio certificati attendibile del computer client oppure, se viene utilizzato un certificato di terze parti, il certificato dell'autorità di certificazione deve trovarsi nell'archivio certificati attendibile.

Quando la negoziazione viene completata, fare clic sull'icona **gear** in basso a sinistra in AnyConnect per visualizzare alcune informazioni avanzate sulla connessione. In questa pagina è possibile visualizzare alcune statistiche di connessione e i dettagli di route ottenuti dall'ACL del tunnel suddiviso nella configurazione di Criteri di gruppo.


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History
Connection Information
State: Connected
Tunnel Mode (IPv4): Split Include
Tunnel Mode (IPv6): Drop All Traffic
Duration: 00:01:06
Address Information
Client (IPv4): 192.168.10.2
Client (IPv6): Not Available
Server: 209.165.201.1
Bytes
Sent: 4039
Received: 641
Frames
Reset
Export Stats...



Di seguito è riportato il risultato finale della configurazione in esecuzione dalla procedura di configurazione:

```
crypto pki trustpoint SSLVPN_TP_SELFSIGNED
 enrollment selfsigned
 serial-number
 subject-name cn=892_SELF_SIGNED_CERT
 revocation-check none
 rsakeypair SELF_SIGNED_RSA
!
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
crypto vpn anyconnect profile SSLVPN_PROFILE flash:test-profile.xml ! access-list 1 permit
192.168.0.0 0.0.255.255 ! ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10 ! webvpn gateway
SSLVPN_GATEWAY ip address 209.165.201.1 port 443 ssl trustpoint SSLVPN_TP_SELFSIGNED inservice !
webvpn context SSLVPN_CONTEXT virtual-template 1
aaa authentication list SSLVPN_AAA
gateway SSLVPN_GATEWAY
! ssl authenticate verify all inservice ! policy group SSLVPN_POLICY functions svc-enabled svc
address-pool "SSLVPN_POOL" netmask 255.255.255.0 svc split include acl 1 svc dns-server primary
8.8.8.8
svc profile SSLVPN_PROFILE default-group-policy SSLVPN_POLICY
```

Risoluzione dei problemi

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

Quando si risolvono i problemi di connessione AnyConnect, è necessario verificare alcuni componenti comuni:

- Poiché il client deve presentare un certificato, è necessario che il certificato specificato nel gateway WebVPN sia valido. Per rilasciare un **certificato show crypto pki** verranno visualizzate le informazioni relative a tutti i certificati sul router.
- Ogni volta che viene apportata una modifica alla configurazione di WebVPN, è buona norma emettere un comando no inservice e inservice sia sul gateway che sul contesto. In questo modo le modifiche avranno effetto in modo corretto.
- Come accennato in precedenza, è necessario avere un PKG AnyConnect per ciascun sistema operativo client che si connetterà a questo gateway. Ad esempio, i client Windows richiedono un PKG Windows, i client Linux a 32 bit richiedono un PKG Linux a 32 bit e così via.
- Se si considera che sia il client AnyConnect che la WebVPN basata sul browser utilizzeranno il protocollo SSL, per poter accedere alla pagina WebVPN, in genere viene indicato che AnyConnect sarà in grado di connettersi (si supponga che la configurazione AnyConnect pertinente sia corretta).

Cisco IOS offre alcune opzioni di debug webvpn che possono essere utilizzate per risolvere i problemi di connessioni in errore. Questo è l'output generato dalla sessione debug webvpn aaa, debug wevpn tunnel e show webvpn su un tentativo di connessione riuscito:

```
fdenofa-892#show debugging


WebVPN Subsystem:
  WebVPN AAA debugging is on
  WebVPN tunnel debugging is on
  WebVPN Tunnel Events debugging is on
  WebVPN Tunnel Errors debugging is on


*May 26 20:11:06.381: WV-AAA: Nas Port ID set to 64.102.157.2.
*May 26 20:11:06.381: WV-AAA: AAA authentication request sent for user: "VPNUSER"AAA returned
status: 2 for session 37
*May 26 20:11:06.381: WV-AAA: AAA Authentication Passed!
*May 26 20:11:06.381: WV-AAA: User "VPNUSER" has logged in from "64.102.157.2" to gateway
"SSLVPN_GATEWAY"
             context "SSLVPN_CONTEXT"
*May 26 20:11:12.265:
*May 26 20:11:12.265:
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] CSTP Version recd , using 1
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Allocating IP 192.168.10.9 from address-pool
SSLVPN_POOL
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Using new allocated IP 192.168.10.9 255.255.255.0
*May 26 20:11:12.265:  Inserting static route: 192.168.10.9 255.255.255.255 Virtual-Access2 to
routing table
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Full Tunnel CONNECT request processed, HTTP reply
created
*May 26 20:11:12.265: HTTP/1.1 200 OK
```

```
*May 26 20:11:12.265: Server: Cisco IOS SSLVPN
*May 26 20:11:12.265: X-CSTP-Version: 1
*May 26 20:11:12.265: X-CSTP-Address: 192.168.10.9
*May 26 20:11:12.269: X-CSTP-Netmask: 255.255.255.0
*May 26 20:11:12.269: X-CSTP-Keep: false
*May 26 20:11:12.269: X-CSTP-DNS: 8.8.8.8
*May 26 20:11:12.269: X-CSTP-Lease-Duration: 43200
*May 26 20:11:12.269: X-CSTP-MTU: 1280
*May 26 20:11:12.269: X-CSTP-Split-Include: 192.168.0.0/255.255.0.0
*May 26 20:11:12.269: X-CSTP-DPD: 300
*May 26 20:11:12.269: X-CSTP-Disconnected-Timeout: 2100
*May 26 20:11:12.269: X-CSTP-Idle-Timeout: 2100
*May 26 20:11:12.269: X-CSTP-Session-Timeout: 0
*May 26 20:11:12.269: X-CSTP-Keepalive: 30
*May 26 20:11:12.269: X-DTLS-Session-ID:
85939A3FE33ABAE5F02F8594D56DEDE389F6FB3C9EEC4D211EB71C0820DF8DC8
*May 26 20:11:12.269: X-DTLS-Port: 443
*May 26 20:11:12.269: X-DTLS-Header-Pad-Length: 3
*May 26 20:11:12.269: X-DTLS-CipherSuite: AES256-SHA
*May 26 20:11:12.269: X-DTLS-DPD: 300
*May 26 20:11:12.269: X-DTLS-KeepAlive: 30
*May 26 20:11:12.269:
*May 26 20:11:12.269:
*May 26 20:11:12.269:
*May 26 20:11:12.269: [WV-TUNL-EVT]:[8A3AE410] For User VPNUSER, DPD timer started for 300
seconds
*May 26 20:11:12.273: [WV-TUNL-EVT]:[8A3AE410] CSTP Control, Recvd a Req Cntl Frame (User
VPNUSER, IP 192.168.10.9)
Severity ERROR, Type CLOSE_ERROR
Text: reinitiate tunnel to negotiate a different MTU
*May 26 20:11:12.273: [WV-TUNL-EVT]:[8A3AE410] CSTP Control, Recvd Close Error Frame
*May 26 20:11:14.105:
*May 26 20:11:14.105:
*May 26 20:11:14.105: [WV-TUNL-EVT]:[8A3AE690] CSTP Version recd , using 1
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Tunnel Client reconnecting removing existing tunl
ctx
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE410] Closing Tunnel Context 0x8A3AE410 for Session
0x8A3C2EF8 and User VPNUSER
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Reusing IP 192.168.10.9 255.255.255.0
*May 26 20:11:14.109:  Inserting static route: 192.168.10.9 255.255.255.255 Virtual-Access2 to
routing table
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Full Tunnel CONNECT request processed, HTTP reply
created
*May 26 20:11:14.109: HTTP/1.1 200 OK
*May 26 20:11:14.109: Server: Cisco IOS SSLVPN
*May 26 20:11:14.109: X-CSTP-Version: 1
*May 26 20:11:14.109: X-CSTP-Address: 192.168.10.9
*May 26 20:11:14.109: X-CSTP-Netmask: 255.255.255.0
*May 26 20:11:14.109: X-CSTP-Keep: false
*May 26 20:11:14.109: X-CSTP-DNS: 8.8.8.8
*May 26 20:11:14.113: X-CSTP-Lease-Duration: 43200
*May 26 20:11:14.113: X-CSTP-MTU: 1199
*May 26 20:11:14.113: X-CSTP-Split-Include: 192.168.0.0/255.255.0.0
*May 26 20:11:14.113: X-CSTP-DPD: 300
*May 26 20:11:14.113: X-CSTP-Disconnected-Timeout: 2100
*May 26 20:11:14.113: X-CSTP-Idle-Timeout: 2100
*May 26 20:11:14.113: X-CSTP-Session-Timeout: 0
*May 26 20:11:14.113: X-CSTP-Keepalive: 30
*May 26 20:11:14.113: X-DTLS-Session-ID:
22E54D9F1F6344BCB5BB30BC8BB3737907795E6F3C3665CDD294CBBA1DA4D0CF
*May 26 20:11:14.113: X-DTLS-Port: 443
*May 26 20:11:14.113: X-DTLS-Header-Pad-Length: 3
*May 26 20:11:14.113: X-DTLS-CipherSuite: AES256-SHA
*May 26 20:11:14.113: X-DTLS-DPD: 300
```

```
*May 26 20:11:14.113: X-DTLS-KeepAlive: 30
*May 26 20:11:14.113:
*May 26 20:11:14.113:
*May 26 20:11:14.113:
*May 26 20:11:14.113: [WV-TUNL-EVT]:[8A3AE690] For User VPNUSER, DPD timer started for 300
seconds
```

```
fdenofa-892#show webvpn session user VPNUSER context SSLVPN_CONTEXT

Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 3.1.08009

Username          : VPNUSER              Num Connection : 5
Public IP         : 64.102.157.2         VRF Name       : None
Context           : SSLVPN_CONTEXT       Policy Group   : SSLVPN_POLICY
Last-Used         : 00:00:00             Created        : *16:11:06.381 EDT Tue May 26 2015
Session Timeout   : Disabled             Idle Timeout   : 2100
DNS primary serve : 8.8.8.8
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : SSLVPN_POOL          MTU Size       : 1199
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 192.168.10.9         Netmask        : 255.255.255.0
Rx IP Packets     : 0                    Tx IP Packets  : 42
CSTP Started      : 00:00:13             Last-Received  : 00:00:00
CSTP DPD-Req sent : 0                    Virtual Access : 2
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : ACL 1
Client Ports      : 17462 17463 17464 17465 17471
```

Informazioni correlate

- Guida alla configurazione della VPN SSL, Cisco IOS release 15M&T
- Esempio di configurazione del client AnyConnect VPN (SSL) su router IOS con CCP
- Documentazione e supporto tecnico – Cisco Systems