# Esempio di configurazione di SSL VPN Client (SVC) su ASA con ASDM

## Sommario



## Introduzione

La tecnologia VPN (Virtual Private Network) SSL (Secure Sockets Layer) consente di connettersi in modo sicuro da qualsiasi luogo a una rete aziendale interna utilizzando uno dei metodi seguenti:

- VPN SSL senza client (WebVPN): fornisce un client remoto che richiede un browser Web

abilitato per SSL per accedere ai server Web HTTP o HTTPS su una rete LAN aziendale. Inoltre, la VPN SSL senza client fornisce l'accesso per l'esplorazione dei file di Windows tramite il protocollo CIFS (Common Internet File System). Outlook Web Access (OWA) è un esempio di accesso HTTP.

Per ulteriori informazioni sulla VPN SSL senza client, consultare l'esempio di configurazione di WebVPN (Client SSL VPN) sull'appliance ASA.

- Thin-Client SSL VPN (Port Forwarding): fornisce un client remoto che scarica una piccola applet basata su Java e consente l'accesso sicuro per le applicazioni TCP (Transmission Control Protocol) che utilizzano numeri di porta statici. Esempi di accesso protetto sono il protocollo POP3 (Post Office Protocol), il protocollo SMTP (Simple Mail Transfer Protocol), il protocollo IMAP (Internet Message Access Protocol), il protocollo ssh (Secure Shell) e Telnet. Poiché i file nel computer locale vengono modificati, per utilizzare questo metodo gli utenti devono disporre dei privilegi di amministrazione locali. Questo metodo di VPN SSL non funziona con le applicazioni che utilizzano assegnazioni dinamiche delle porte, ad esempio alcune applicazioni FTP (File Transfer Protocol).

  Per ulteriori informazioni sulla VPN SSL thin-client, consultare il documento di esempio della VPN SSL thin-client (WebVPN) sull'appliance ASA con configurazione ASDM.

  Nota: UDP (User Datagram Protocol) non è supportato.

- SSL VPN Client (modalità tunnel): scarica un client di piccole dimensioni sulla workstation remota e consente l'accesso sicuro alle risorse su una rete aziendale interna. È possibile scaricare il client VPN SSL (SVC) su una workstation remota in modo permanente oppure rimuovere il client dopo la chiusura della sessione protetta.

In questo documento viene descritto come configurare SVC su un'appliance ASA (Adaptive Security Appliance) utilizzando Adaptive Security Device Manager (ASDM). Le righe di comando risultanti da questa configurazione sono elencate nella sezione Risultati.

# Prerequisiti

## Requisiti

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- SVC avvia il supporto del software Cisco Adaptive Security Appliance versione 7.1 e successive
- Privilegi amministrativi locali su tutte le workstation remote
- Controlli Java e ActiveX sulla workstation remota
- La porta 443 non è bloccata in alcun punto del percorso di connessione

## Componenti usati

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

- Software Cisco Adaptive Security Appliance versione 7.2(1)
- Cisco Adaptive Security Device Manager 5.2(1)
- Cisco Adaptive Security Appliance serie 5510
- Microsoft Windows XP Professional SP 2

Le informazioni discusse in questo documento fanno parte di un ambiente di emulazione. Tutti i dispositivi utilizzati nel documento sono stati ripristinati alla configurazione predefinita. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi. Tutti gli indirizzi IP utilizzati in questa configurazione sono stati selezionati dagli indirizzi RFC 1918 in un ambiente lab. Questi indirizzi IP non sono instradabili su Internet e sono solo a scopo di test.

## Esempio di rete

Nel documento viene usata la configurazione di rete descritta in questa sezione.

Un utente remoto si connette all'indirizzo IP dell'appliance ASA con un browser Web abilitato per SSL. Una volta completata l'autenticazione, l'SVC viene scaricato nel computer client e l'utente può utilizzare una sessione protetta crittografata per l'accesso completo a tutte le risorse consentite sulla rete aziendale.

## Task di preconfigurazione

Prima di iniziare, eseguire le attività seguenti:

- Per configurare l'ASA con ASDM, consultare il documento sulla concessione dell'accesso HTTPS per ASDM.

  Per accedere all'applicazione ASDM, dalla stazione di gestione, usare un browser Web abilitato per SSL e immettere l'indirizzo IP del dispositivo ASA. Ad esempio: https://inside_ip_address, dove inside_ip_address è l'indirizzo dell'appliance ASA. Una volta caricato ASDM, è possibile iniziare la configurazione dell'SVC.

- Scaricare il pacchetto SSL VPN Client (sslclient-win*.pkg) dal sito Web Cisco Software Download (solo utenti registrati) sul disco rigido locale della stazione di gestione da cui si accede all'applicazione ASDM.

WebVPN e ASDM non possono essere abilitati sulla stessa interfaccia ASA a meno che non si modifichino i numeri di porta. Se si desidera che le due tecnologie utilizzino la stessa porta (porta 443) sullo stesso dispositivo, è possibile abilitare ASDM sull'interfaccia interna e abilitare WebVPN sull'interfaccia esterna.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

# Configurazione del client VPN SSL su un'appliance ASA

Per configurare il client VPN SSL su un'ASA, attenersi alla seguente procedura:

1. Abilitazione dell'accesso WebVPN sull'appliance ASA
2. Installare e abilitare il client VPN SSL sull'appliance ASA
3. Abilitazione dell'installazione di SVC sui client
4. Abilita parametri di reimpostazione chiavi

## Passaggio 1. Abilitazione dell'accesso WebVPN sull'appliance ASA

Per abilitare l'accesso WebVPN sull'appliance ASA, attenersi alla seguente procedura:

1. Nell'applicazione ASDM, fare clic su Configuration (Configurazione), quindi su VPN.
2. Espandere WebVPN e scegliere Accesso WebVPN.
3. Selezionare l'interfaccia per cui si desidera abilitare WebVPN e fare clic su Abilita.

## Passaggio 2. Installare e abilitare il client VPN SSL sull'appliance ASA

Per installare e abilitare il client VPN SSL sull'appliance ASA, attenersi alla seguente procedura:

1. Fare clic su Configurazione e quindi su VPN.
2. Nel riquadro di navigazione, espandere WebVPN e scegliere SSL VPN Client.
3. Fare clic su Add.

   Verrà visualizzata la finestra di dialogo Aggiungi immagine client VPN SSL.
4. Fare clic sul pulsante Upload.

   Viene visualizzata la finestra di dialogo Carica immagine.
5. Fare clic sul pulsante Sfoglia file locali per individuare un file nel computer locale oppure fare clic sul pulsante Sfoglia flash per individuare un file nel file system flash.
6. Individuare il file di immagine client da caricare e fare clic su OK.
7. Fare clic su Upload File, quindi su Close (Chiudi).
8. Una volta caricata l'immagine client per la memoria flash, selezionare la casella di controllo Abilita client VPN SSL e quindi fare clic su Applica.

Nota: se viene visualizzato un messaggio di errore, verificare che l'accesso a WebVPN sia abilitato. Nel riquadro di navigazione, espandere WebVPN e scegliere Accesso WebVPN. Selezionare l'interfaccia per la quale si desidera configurare l'accesso e fare clic su Abilita.

9. Fare clic su Salva e quindi su Sì per accettare le modifiche.

## Passaggio 3. Abilitazione dell'installazione di SVC sui client

Per abilitare l'installazione di SVC sui client, attenersi alla seguente procedura:

1. Nel riquadro di navigazione, espandere Gestione indirizzi IP, quindi selezionare Pool IP.
2. Fare clic su Aggiungi, immettere i valori nei campi Nome, Indirizzo IP iniziale, Indirizzo IP finale e Subnet mask. Gli indirizzi IP immessi nei campi Indirizzo IP iniziale e Indirizzo IP finale devono provenire da subnet della rete interna.
3. Fare clic su OK, quindi su Applica.
4. Fare clic su Salva e quindi su Sì per accettare le modifiche.
5. Nel riquadro di navigazione, espandere Gestione indirizzi IP, quindi selezionare Assegnazione.
6. Selezionare la casella di controllo Utilizza pool di indirizzi interni e quindi deselezionare le caselle di controllo Utilizza server di autenticazione e Usa DHCP.
7. Fare clic su Apply (Applica).
8. Fare clic su Salva e quindi su Sì per accettare le modifiche.
9. Nel riquadro di navigazione, espandere Generale, quindi scegliere Gruppo di tunnel.
10. Selezionare il gruppo di tunnel che si desidera gestire e fare clic su Modifica.
11. Fare clic sulla scheda Assegnazione indirizzo client e selezionare il pool di indirizzi IP appena creato dall'elenco Pool disponibili.
12. Fare clic su Add (Aggiungi), quindi su OK.
13. Nella finestra dell'applicazione ASDM, fare clic su Applica.
14. Fare clic su Salva e quindi su Sì per accettare le modifiche.

## Passaggio 4. Abilita parametro rekey

Per abilitare i parametri di reimpostazione chiavi:

1. Nel riquadro di spostamento espandere Generale e scegliere Criteri di gruppo.
2. Selezionare il criterio che si desidera applicare a questo gruppo di client e fare clic su

Modifica.

3. Nella scheda Generale deselezionare la casella di controllo Eredita protocolli di tunneling e selezionare la casella di controllo WebVPN.

4. Fare clic sulla scheda WebVPN, fare clic sulla scheda SSL VPN Client e scegliere le opzioni seguenti:

    a. Per l'opzione Usa client VPN SSL, deselezionare la casella di controllo Eredita e fare clic sul pulsante di opzione Facoltativo.

    Questa opzione consente al client remoto di scegliere se scaricare o meno l'SVC. L'opzione Always (Sempre) garantisce che l'SVC venga scaricato sulla workstation remota durante ciascuna connessione VPN SSL.

    b. Per l'opzione Mantieni programma di installazione sul sistema client, deselezionare la casella di controllo Eredita e fare clic sul pulsante di opzione Sì.

    Questa azione consente al software SVC di rimanere sul computer client; pertanto, l'ASA non deve scaricare il software SVC sul client ogni volta che viene stabilita una connessione. Questa opzione è ideale per gli utenti remoti che spesso accedono alla rete aziendale.

    c. Per l'opzione Intervallo rinegoziazione, deselezionare la casella di controllo Eredita, deselezionare la casella di controllo Illimitato e immettere il numero di minuti che devono trascorrere prima della reimpostazione della chiave.

    La protezione viene migliorata impostando limiti sulla durata di validità di una chiave.

    d. Per l'opzione Metodo rinegoziazione, deselezionare la casella di controllo Eredita e fare clic sul pulsante di opzione SSL. La rinegoziazione può utilizzare il tunnel SSL corrente o un nuovo tunnel creato espressamente per la rinegoziazione.

    Gli attributi del client VPN SSL devono essere configurati come mostrato in questa immagine:

5. Fare clic su OK, quindi su Applica.

6. Fare clic su Salva e quindi su Sì per accettare le modifiche.

## Risultati

ASDM crea le seguenti configurazioni della riga di comando:

| ciscoasa |
| --- |
| <#root><br>ciscoasa(config)# |

```
show run

ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
!

!--- Group Policy Statements

group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn

!--- Enable the SVC for WebVPN

 webvpn
  svc enable
  svc keep-installer installed
  svc rekey time 30
  svc rekey method ssl
!
username cisco password 53QNetqK.Kqqfshe encrypted privilege 15
!
http server enable
```

```
http 10.2.2.0 255.255.255.0 inside
!
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!--- Tunnel Group and Group Policy using the defaults here

tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool CorporateNet
 default-group-policy GroupPolicy1
!
no vpn-addr-assign aaa
no vpn-addr-assign dhcp
!
telnet timeout 5
ssh 172.22.1.0 255.255.255.0 outside
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global

!--- Enable webvpn and the select the SVC client

webvpn
 enable outside
 svc image disk0:/sslclient-win-1.1.1.164.pkg 1
 svc enable

!--- Provide list for access to resources

 url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
 url-list ServerList "BrowseServer" cifs://10.2.2.2 2
 tunnel-group-list enable

prompt hostname context
Cryptochecksum:80a1890a95580dca11e3aee200173f5f
: end
```

# Personalizzazione della configurazione

Le procedure descritte in Configurazione del client VPN SSL su un'appliance ASA utilizzano i nomi predefiniti ASA per Criteri di gruppo (GroupPolicy1) e per il gruppo di tunnel (DefaultWebVPNGroup), come mostrato nell'immagine:

In questa procedura viene descritto come creare criteri di gruppo e gruppi di tunnel personalizzati e collegarli in base ai criteri di sicurezza dell'organizzazione.

Per personalizzare la configurazione, attenersi alla seguente procedura:

1. Creare Criteri di gruppo personalizzati
2. Creazione di un gruppo di tunnel personalizzato
3. Creare un utente e aggiungerlo ai Criteri di gruppo personalizzati

## Passaggio 1. Creare Criteri di gruppo personalizzati

Per creare un criterio di gruppo personalizzato, eseguire la procedura seguente:

1. Fare clic su Configurazione e quindi su VPN.
2. Espandere Generale e scegliere Criteri di gruppo.
3. Fare clic su Aggiungi e scegliere Criteri di gruppo interni.
4. Nel campo Nome immettere un nome per il criterio di gruppo.

   In questo esempio il nome dei criteri di gruppo è stato modificato in SalesGroupPolicy.
5. Nella scheda Generale, deselezionare la casella di controllo Eredita protocolli di tunneling, quindi selezionare la casella di controllo WebVPN.
6. Fare clic sulla scheda WebVPN e quindi sulla scheda SSL VPN Client.

   In questa finestra di dialogo è inoltre possibile scegliere il comportamento del client VPN SSL.
7. Fare clic su OK, quindi su Applica.
8. Fare clic su Salva e quindi su Sì per accettare le modifiche.

## Passaggio 2. Creazione di un gruppo di tunnel personalizzato

Per creare un gruppo di tunnel personalizzato, attenersi alla seguente procedura:

1. Fare clic sul pulsante Configuration (Configurazione), quindi su VPN.

2. Espandere Generale e scegliere Gruppo tunnel.
3. Fare clic su Add (Aggiungi), quindi selezionare WebVPN Access (Accesso VPN Web).
4. Nel campo Nome, immettere un nome per il gruppo di tunnel.

   In questo esempio, il nome del gruppo di tunnel è stato modificato in SalesForceGroup.
5. Fare clic sulla freccia a discesa Criteri di gruppo e scegliere il criterio di gruppo appena creato.

   I Criteri di gruppo e il gruppo di tunnel sono ora collegati.
6. Fare clic sulla scheda Assegnazione indirizzo client e immettere le informazioni sul server DHCP o selezionare un pool IP creato localmente.
7. Fare clic su OK, quindi su Applica.
8. Fare clic su Salva e quindi su Sì per accettare le modifiche.

### Passaggio 3. Creare un utente e aggiungerlo ai Criteri di gruppo personalizzati

Per creare un utente e aggiungerlo ai Criteri di gruppo personalizzati, eseguire la procedura seguente:

1. Fare clic su Configurazione e quindi su VPN.
2. Espandere Generale e scegliere Utenti.
3. Fare clic su Add (Aggiungi), quindi immettere il nome utente e la password.
4. Fare clic sulla scheda Criteri VPN. Verificare che nel campo Criteri di gruppo sia visualizzato il criterio di gruppo appena creato.

   L'utente eredita tutte le caratteristiche del nuovo criterio di gruppo.
5. Fare clic su OK, quindi su Applica.
6. Fare clic su Salva e quindi su Sì per accettare le modifiche.

## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

### Autenticazione

L'autenticazione per i client VPN SSL viene eseguita utilizzando uno dei seguenti metodi:

- Cisco Secure ACS Server (Radius)

- Dominio NT
- Active Directory
- Password monouso
- Certificati digitali
- Smart card
- Autenticazione AAA locale

La presente documentazione utilizza un account locale creato sul dispositivo ASA.

Nota: se un'appliance Adaptive Security ha più trust point che condividono la stessa CA, per convalidare i certificati utente è possibile utilizzare solo uno di questi trust point che condividono la CA.

### Configurazione

Per connettersi all'appliance ASA con un client remoto, immettere https://ASA_outside_address nel campo dell'indirizzo di un browser Web abilitato per SSL. ASA_outside_address è l'indirizzo IP esterno dell'appliance ASA. Se la configurazione ha esito positivo, viene visualizzata la finestra Cisco Systems SSL VPN Client.

Nota: la finestra Cisco Systems SSL VPN Client viene visualizzata solo dopo aver accettato il certificato dell'ASA e dopo aver scaricato il client VPN SSL sulla stazione remota. Se la finestra non viene visualizzata, verificare che non sia ridotta a icona.

### Comandi

Diversi comandi show sono associati a WebVPN. È possibile eseguire questi comandi dall'interfaccia della riga di comando (CLI) per visualizzare le statistiche e altre informazioni. Per informazioni dettagliate sui comandi show, consultare il documento sulla verifica delle configurazioni WebVPN.

Nota: lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi show. Usare OIT per visualizzare un'analisi dell'output del comando show.

## Risoluzione dei problemi

Consultare questa sezione per risolvere i problemi di configurazione.

### Errore SVC

Problema

È possibile che venga visualizzato questo messaggio di errore durante l'autenticazione:

```
"The SSl VPN connection to the remote peer was disrupted
and could not be automatically re-estabilished. A new connection requires
re-authentication and must be restarted manually. Close all sensitive networked
applications."
```

Soluzione

Se sul PC è in esecuzione un servizio firewall, l'autenticazione può essere interrotta. Arrestare il servizio e riconnettere il client.

## L'SVC ha stabilito una sessione sicura con l'ASA?

Per verificare che il client VPN SSL abbia stabilito una sessione protetta con l'ASA:

1. Fare clic su Monitoraggio.
2. Espandere Statistiche VPN e scegliere Sessioni.
3. Dal menu a discesa Filtra per, scegliere SSL VPN Client, quindi fare clic sul pulsante Filtra.

   La configurazione dovrebbe essere visualizzata nell'elenco delle sessioni.

## Le sessioni sicure sono state stabilite e terminate correttamente?

È possibile visualizzare i log in tempo reale per verificare che le sessioni siano state stabilite e terminate correttamente. Per visualizzare i log delle sessioni:

1. Fare clic su Monitoraggio e quindi su Registrazione.
2. Scegliere il Visualizzatore log in tempo reale o Buffer log, quindi fare clic su Visualizza.

   Nota: per visualizzare solo le sessioni di un indirizzo specifico, filtrare in base all'indirizzo.

## Controllare il pool IP nel profilo WebVPN

```
%ASA-3-722020: Group group User user-name IP IP_address  No address
available for SVC connection
```

Nessun indirizzo disponibile da assegnare alla connessione SVC. Assegnare quindi l'indirizzo del pool IP nel profilo.

Se si crea il nuovo profilo di connessione, configurare un alias o un URL del gruppo per accedere a questo profilo di connessione. In caso contrario, tutti i tentativi SSL verranno eseguiti sul profilo di connessione WebVPN predefinito a cui non era associato un pool IP. Impostare questa opzione per utilizzare il profilo di connessione predefinito e inserirvi un pool IP.

### Suggerimenti

- Verificare che il routing funzioni correttamente con il pool di indirizzi IP assegnato ai client remoti. Questo pool di indirizzi IP deve provenire da una subnet della LAN. Per assegnare gli indirizzi IP, è inoltre possibile utilizzare un server DHCP o un server di autenticazione.
- L'appliance ASA crea un gruppo di tunnel predefinito (DefaultWebVPNGroup) e un criterio di gruppo predefinito (GroupPolicy1). Se si creano nuovi gruppi e criteri, assicurarsi di applicare i valori in conformità con i criteri di sicurezza della rete.
- Per abilitare l'esplorazione dei file di Windows tramite CIFS, immettere un server WINS (NBNS) in Configurazione > VPN > WebVPN > Server e URL. Questa tecnologia utilizza la selezione CIFS.

### Comandi

Diversi comandi debug sono associati a WebVPN. Per informazioni dettagliate su questi comandi, consultare il documento sull'uso dei comandi di debug di WebVPN.

Nota: l'uso dei comandi di debug può avere un impatto negativo sul dispositivo Cisco. Prima di usare i comandi di debug, consultare la sezione Informazioni importanti sui comandi di debug.

## Informazioni correlate

- Esempio di configurazione di una VPN SSL senza client (WebVPN) su ASA
- Esempio di configurazione di una VPN SSL thin-client (WebVPN) su un'appliance ASA con ASDM
- Esempio di configurazione di ASA con WebVPN e Single Sign-On con ASDM e NTLMv1
- Cisco ASA serie 5500 Adaptive Security Appliance
- Documentazione e supporto tecnico – Cisco Systems

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).