

Configurazione di una VPN SSL senza client (WebVPN) sull'appliance ASA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Procedure per la risoluzione dei problemi](#)

[Comandi utilizzati per la risoluzione dei problemi](#)

[Problemi comuni](#)

[L'utente non può accedere](#)

[Impossibile connettere più di tre utenti WebVPN all'appliance ASA](#)

[I client WebVPN non possono raggiungere i segnalibri ed è disattivato](#)

[Connessione Citrix tramite WebVPN](#)

[Come evitare la necessità di una seconda autenticazione per gli utenti](#)

[Informazioni correlate](#)

Introduzione

Questo documento offre una configurazione semplice per Cisco Adaptive Security Appliance (ASA) serie 5500 per consentire l'accesso VPN SSL (Secure Sockets Layer) senza client alle risorse della rete interna. Il protocollo WebVPN (Virtual Private Network) SSL senza client consente un accesso limitato, ma valido e sicuro alla rete aziendale da qualsiasi luogo. Gli utenti possono accedere in qualsiasi momento alle risorse aziendali tramite un browser protetto. Non sono necessari client aggiuntivi per accedere alle risorse interne. L'accesso viene fornito utilizzando un protocollo HTTP (Hypertext Transfer Protocol) su una connessione SSL.

La VPN SSL senza client consente di accedere in modo semplice e sicuro a un'ampia gamma di risorse Web e applicazioni legacy e abilitate per il Web da quasi tutti i computer in grado di raggiungere i siti HTTP (Hypertext Transfer Protocol Internet). Ciò include:

- Siti Web interni
- Microsoft SharePoint 2003, 2007 e 2010
- Microsoft Outlook Web Access 2003, 2007 e 2013

- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 e 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp versione 5-6.5
- Citrix XenDesktop versione 5-5.6 e 7.5
- VMware View 4

Un elenco di software supportati è disponibile nelle [piattaforme VPN supportate, Cisco ASA serie 5500](#).

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- browser abilitato per SSL
- ASA con versione 7.1 o successive
- Certificato X.509 rilasciato al nome di dominio ASA
- Porta TCP 443, che non deve essere bloccata sul percorso tra il client e l'appliance ASA

L'elenco completo dei requisiti è disponibile su [piattaforme VPN supportate, Cisco ASA serie 5500](#).

Componenti usati

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

- ASA versione 9.4(1)
- Adaptive Security Device Manager (ASDM) versione 7.4(2)
- ASA 5515-X

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.

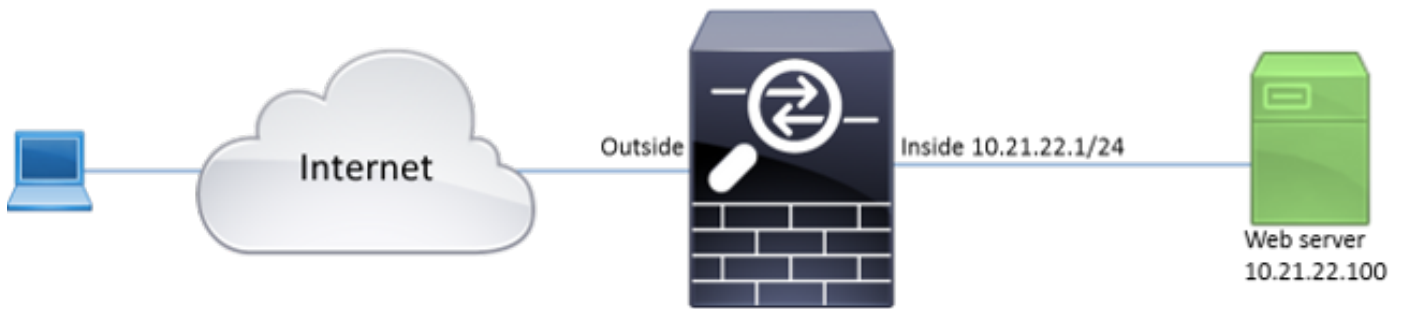
Configurazione

Questo articolo descrive il processo di configurazione per ASDM e CLI. È possibile scegliere di seguire uno degli strumenti per configurare la WebVPN, ma alcuni passaggi di configurazione possono essere eseguiti solo con ASDM.

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

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Premesse

WebVPN utilizza il protocollo SSL per proteggere i dati trasferiti tra il client e il server. Quando il browser avvia la connessione all'ASA, l'appliance presenta il proprio certificato per autenticarsi nel browser. Per garantire la sicurezza della connessione tra il client e l'ASA, è necessario fornire all'ASA il certificato firmato dall'autorità di certificazione che il client già considera attendibile. In caso contrario, il client non disporrà dei mezzi per verificare l'autenticità dell'ASA, il che comporta la possibilità di un attacco man-in-the-middle e una scarsa esperienza da parte dell'utente, perché il browser genera un avviso che la connessione non è attendibile.

Nota: Per impostazione predefinita, all'avvio l'ASA genera un certificato X.509 autofirmato. Questo certificato viene utilizzato per le connessioni client per impostazione predefinita. Non è consigliabile utilizzare questo certificato perché il browser non è in grado di verificarne l'autenticità. Inoltre, il certificato viene rigenerato a ogni riavvio in modo che cambi dopo ogni riavvio.

L'installazione del certificato non rientra nell'ambito di questo documento.

Configurazione

Configurare WebVPN sull'appliance ASA in cinque passaggi principali:

- Configurare il certificato che verrà utilizzato dall'appliance ASA.
- Abilitare WebVPN su un'interfaccia ASA.
- Creare un elenco di server e/o URL (Uniform Resource Locator) per l'accesso a WebVPN.
- Creare un criterio di gruppo per gli utenti WebVPN.
- Applicare il nuovo criterio di gruppo a un gruppo di tunnel.

Nota: Nelle versioni ASA successive alla release 9.4, l'algoritmo usato per scegliere i cifrari SSL è stato modificato (vedere le [note di rilascio per la serie Cisco ASA, 9.4\(x\)](#)). Se si usano solo client ellittici compatibili con le curve, è sicuro usare la chiave privata ellittica. In caso contrario, è necessario usare la suite di cifratura personalizzata per evitare che l'appliance ASA presenti un certificato temporaneo autofirmato. È possibile configurare l'ASA in modo che utilizzi solo cifrari basati su RSA con il comando "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-

SHA:RC4-MD5" personalizzato per la cifratura ssl.

1. **Opzione 1** - Importare il certificato con il file pkcs12. Scegliere **Configurazione > Firewall > Avanzate > Gestione certificati > Certificati di identità > Aggiungi**. È possibile installarlo con il file pkcs12 o incollarne il contenuto nel formato PEM (Privacy Enhanced Mail).

Trustpoint Name: ASDM_TrustPoint2

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From: Browse...

Add a new identity certificate:

Key Pair: <Default-RSA-Key> Show... New...

Certificate Subject DN: CN=ASA Select...

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Advanced...

Enable CA flag in basic constraints extension

Add Certificate Cancel Help

CLI:

```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"
```

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH  
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N  
+vkvjUgCaggAgIIFuHFrV6enVf1Nv3sBBYB/yZswHELY5KpeALbXhfrFDpLNncAB  
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x30zo0JJxSAafmTWqDOEOS/  
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbi1s1ioe4Dplx1b
```

--- output omitted ---

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
```

BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCaggAgIIFuHFrV6enVf1Nv3sBBYB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbi1s1ioe4Dplx1b

quit

INFO: Import PKCS12 operation completed successfully

Opzione 2: creare un certificato autofirmato. Scegliere **Configurazione > Firewall > Avanzate > Gestione certificati > Certificati di identità > Aggiungi**. Fare clic sul pulsante di opzione **Aggiungi nuovo certificato di identità**. Selezionare la **casella di controllo Genera certificato autofirmato**. Scegliere un nome comune (CN) che corrisponda al nome di dominio dell'appliance ASA.

Add Identity Certificate

Trustpoint Name:

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

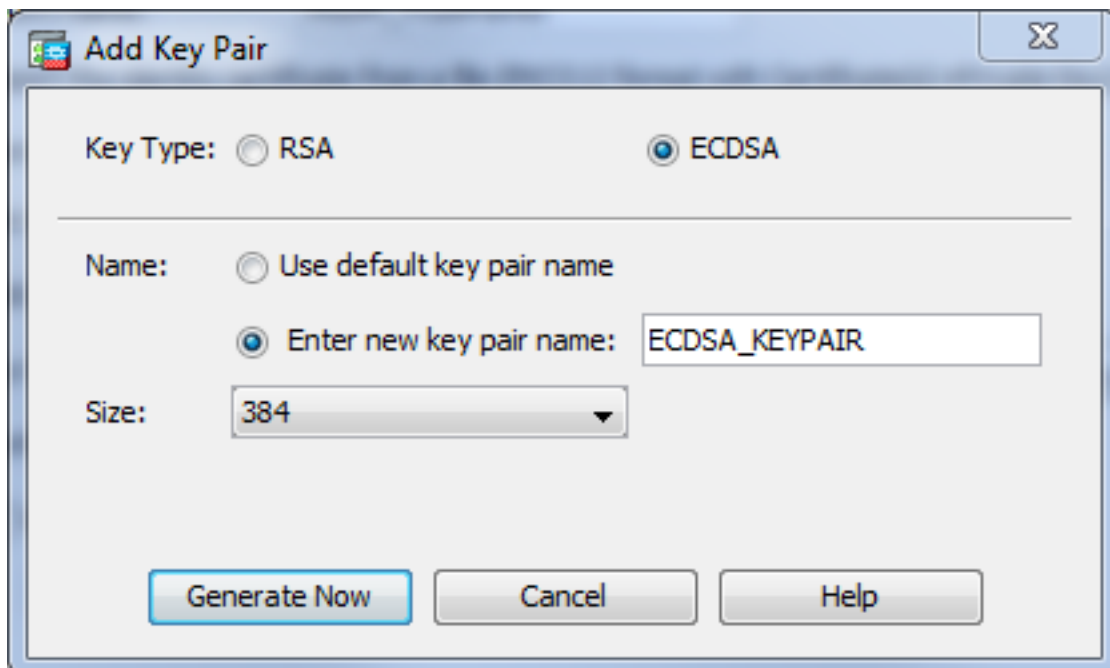
Certificate Subject DN:

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

Per creare la coppia di chiavi per il certificato, fare clic su **Nuovo**. Scegliere il tipo di chiave, il nome e la



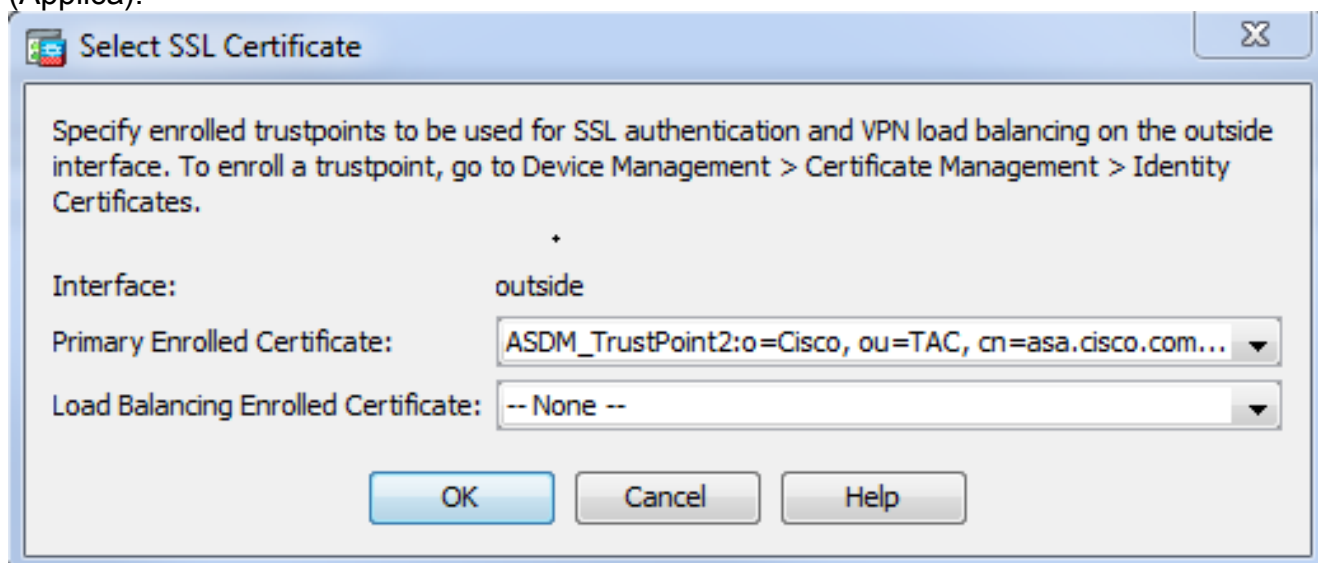
dimensione.

LI:

```
ASA(config)# crypto key generate ecdsa label ECDSA_KEYPAIR noconfirm
```

```
ASA(config)# crypto ca trustpoint TrustPoint1
ASA(config-ca-trustpoint)# revocation-check none
ASA(config-ca-trustpoint)# id-usage ssl-ipsec
ASA(config-ca-trustpoint)# no fqdn
ASA(config-ca-trustpoint)# subject-name CN=ASA
ASA(config-ca-trustpoint)# enrollment self
ASA(config-ca-trustpoint)# keypair ECDSA_KEYPAIR
ASA(config-ca-trustpoint)# exit
ASA(config)# crypto ca enroll TrustPoint1 noconfirm
```

2. Scegliere il certificato da utilizzare per le connessioni WebVPN. Scegliere **Configurazione > VPN ad accesso remoto > Avanzate > Impostazioni SSL**. Dal menu Certificati, scegliere il trust point associato al certificato desiderato per l'interfaccia esterna. Fare clic su **Apply** (Applica).



Configurazione CLI equivalente:

```
ASA(config)# ssl trust-point
```

3. (Facoltativo) Abilitare le ricerche DNS (Domain Name Server). Il server WebVPN funge da proxy per le connessioni client. Significa che l'ASA crea connessioni alle risorse per conto del client. Se i client richiedono connessioni alle risorse che utilizzano nomi di dominio, l'ASA deve eseguire la ricerca DNS. Scegliere **Configurazione > VPN ad accesso remoto > DNS**. Configurare almeno un server DNS e abilitare le ricerche DNS nell'interfaccia rivolta al server

Configuration > Remote Access VPN > DNS

Specify how to resolve DNS requests.

DNS Setup

Configure one DNS server group Configure multiple DNS server groups

Primary DNS Server:

Secondary Servers:

Domain Name:

DNS.

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
outside	False

DNS Guard

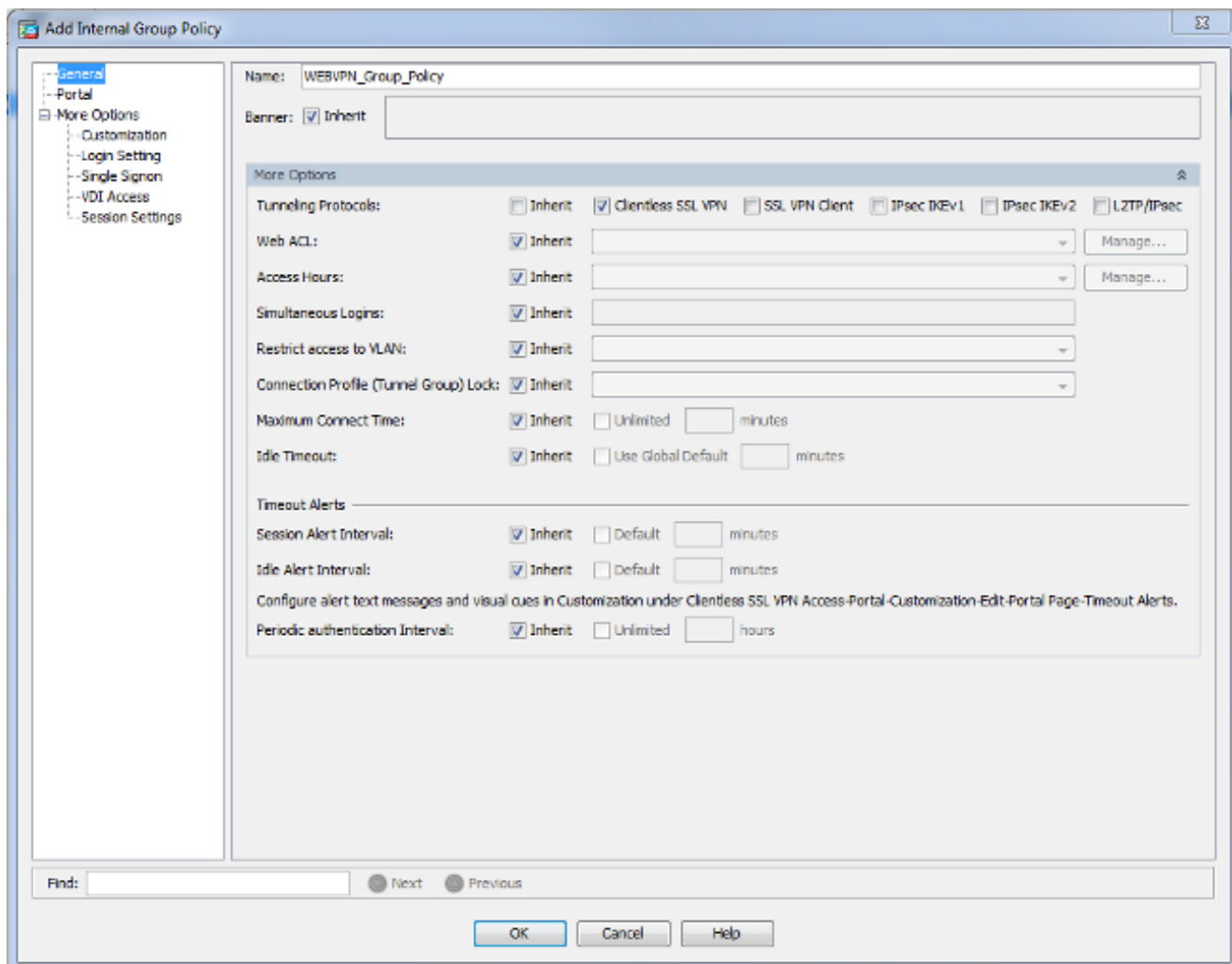
This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

Enable DNS Guard on all interfaces.

CLI:

```
ASA(config)# dns domain-lookup inside
ASA(config)# dns server-group DefaultDNS
ASA(config-dns-server-group)# name-server 10.11.12.101
```

4. (Facoltativo) Creare Criteri di gruppo per le connessioni WEBVPN. Scegliere **Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Criteri di gruppo > Aggiungi Criteri di gruppo interni**. In Opzioni generali modificare il valore di Protocolli di tunneling su "VPN SSL senza client".



CLI:

```
ASA(config)# group-policy WEBVPN_Group_Policy internal
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# vpn-tunnel-protocol ssl-clientless
```

5. Configurare il profilo di connessione. In ASDM, scegliere **Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Profili di connessione**.

Per una panoramica dei profili di connessione e dei criteri di gruppo, consultare la [guida alla configurazione della VPN CLI della serie Cisco ASA, 9.4 - Profili di connessione, Criteri di gruppo e Utenti](#). Per impostazione predefinita, le connessioni WebVPN utilizzano il profilo DefaultWEBVPNGroup. È possibile creare profili aggiuntivi. **Nota:** Esistono diversi modi per assegnare gli utenti ad altri profili.

- Gli utenti possono selezionare manualmente il profilo di connessione dall'elenco a discesa o con un URL specifico. Vedere [ASA 8.x: Consenti agli utenti di selezionare un gruppo all'accesso WebVPN tramite Group-Alias e Group-URL Method](#).

- Quando si utilizza un server LDAP, è possibile assegnare il profilo utente in base agli attributi ricevuti dal server LDAP. Vedere [Esempio di configurazione dell'uso delle mappe di attributi LDAP da parte dell'ASA](#).

- Quando si utilizza l'autenticazione basata sui certificati dei client, è possibile mappare l'utente ai profili basati sui campi contenuti nel certificato. Vedere [Cisco ASA Series VPN CLI Configuration Guide, 9.4 - Configure Certificate Group Matching for IKEv1](#).

- Per assegnare manualmente gli utenti ai Criteri di gruppo, vedere [Cisco ASA Series VPN CLI Configuration Guide, 9.4 - Configuring Attributes for Individual Users](#) Modificare il profilo DefaultWEBVPNGroup e scegliere WEBVPN_Group_Policy in Criteri di gruppo predefiniti.

The screenshot shows the configuration window for the DefaultWEBVPNGroup profile. The 'Advanced' tab is selected, and the configuration is as follows:

- Name:** DefaultWEBVPNGroup
- Aliases:** (empty)
- Authentication:**
 - Method: AAA Certificate Both
 - AAA Server Group: LOCAL (Manage...)
 - Use LOCAL if Server Group fails
- DNS:**
 - Server Group: DefaultDNS (Manage...)
 - (Following fields are attributes of the DNS server group selected above.)
 - Servers: 10.21.22.101
 - Domain Name: disco.com
- Default Group Policy:**
 - Group Policy: WEBVPN_Group_Policy (Manage...)
 - (Following field is an attribute of the group policy selected above.)
 - Enable clientless SSL VPN protocol

CLI:

```
ASA(config)# tunnel-group DefaultWEBVPNGroup general-attributes
ASA(config-tunnel-general)# default-group-policy WEBVPN_Group_Policy
```

6. Per abilitare WebVPN sull'interfaccia esterna, scegliere **Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Profili di connessione**. Selezionare la casella di controllo **Consenti accesso** accanto all'interfaccia esterna.

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Device Certificate ...

Port Setting ...

CLI:

```
ASA(config)# webvpn
```

```
ASA(config-webvpn)# enable outside
```

7. (Facoltativo) Creare segnalibri per il contenuto. I segnalibri consentono all'utente di sfogliare facilmente le risorse interne senza dover ricordare gli URL. Per creare un segnalibro, scegliere **Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Portale > Segnalibri > Aggiungi.**

Add Bookmark List

Bookmark List Name:

Bookmark Title	URL
----------------	-----

Add

Edit

Delete

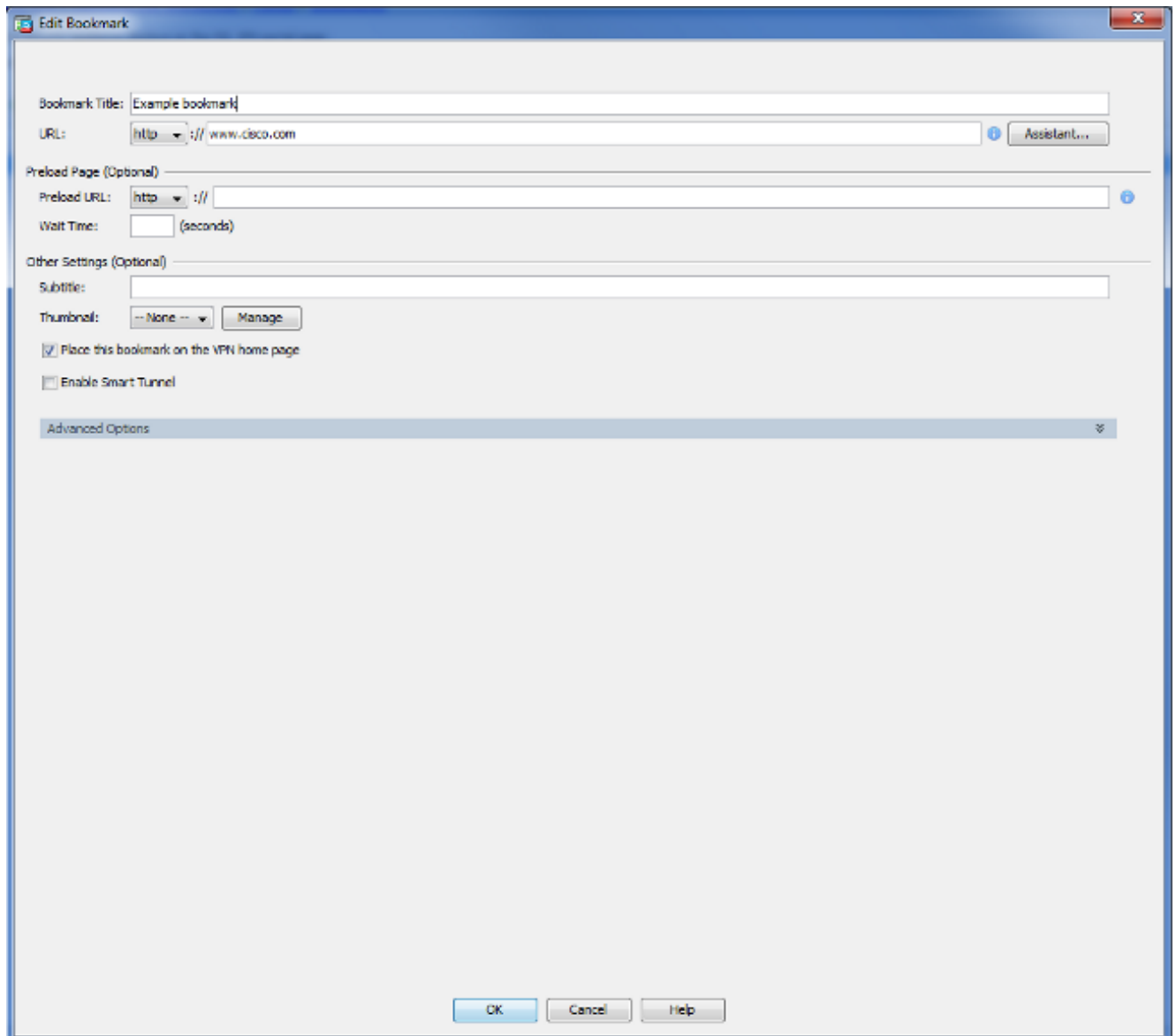
Move Up

Move Down

Find: Match Case

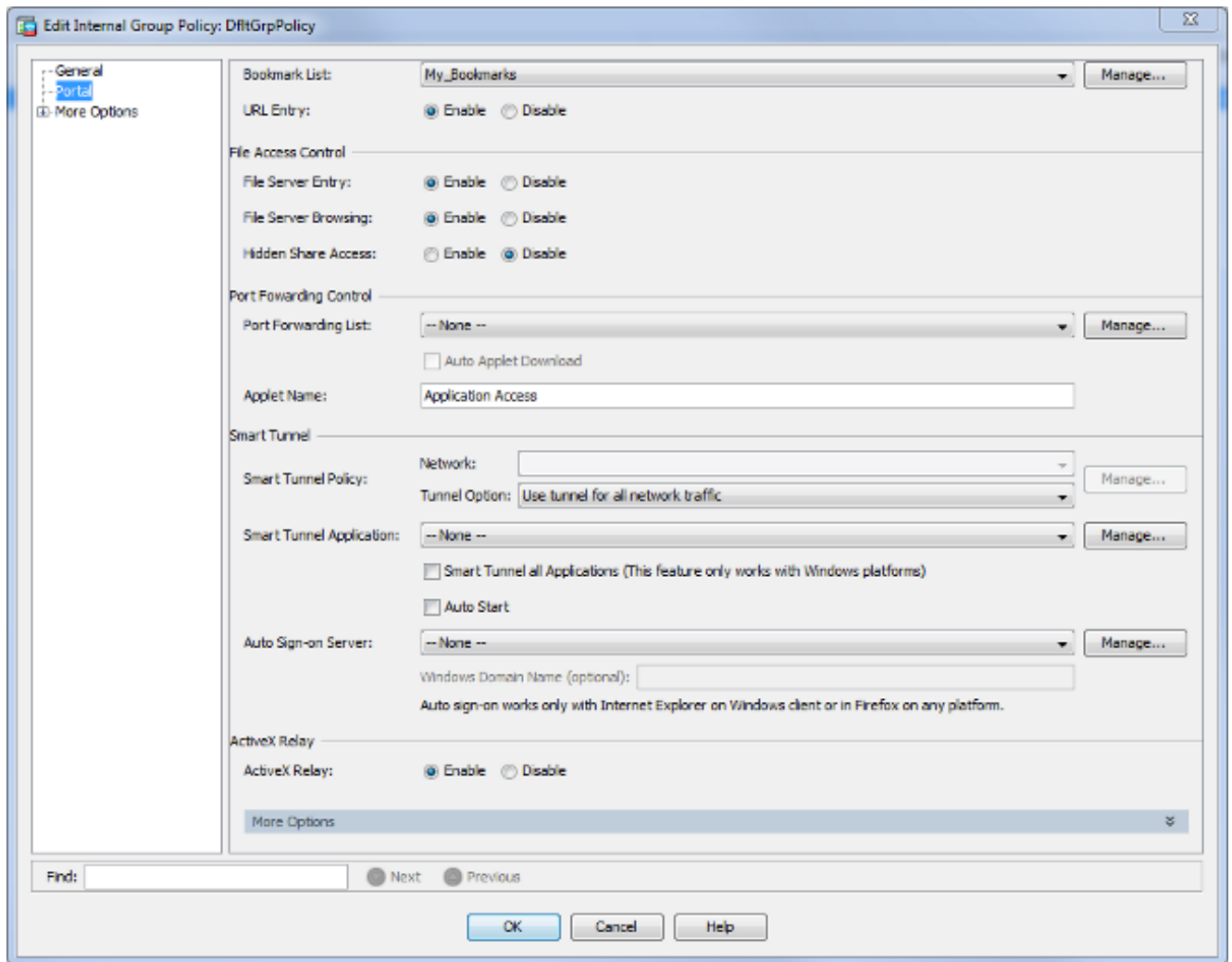
OK Cancel Help

Per aggiungere un segnalibro specifico, scegliere **Aggiungi.**



CLI: Non è possibile creare segnalibri tramite CLI perché vengono creati come file XML.

8. (Facoltativo) Assegnare segnalibri a criteri di gruppo specifici. Scegliere **Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Criteri di gruppo > Modifica > Portale > Elenco segnalibri**.

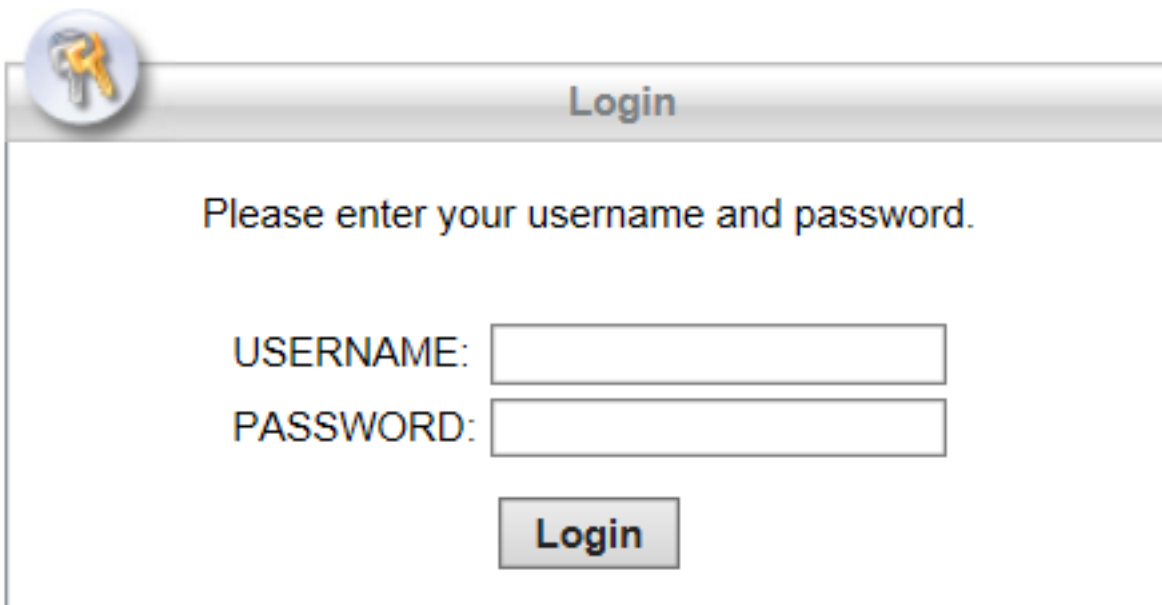


CLI:

```
ASA(config)# group-policy DfltGrpPolicy attributes  
ASA(config-group-policy)# webvpn  
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

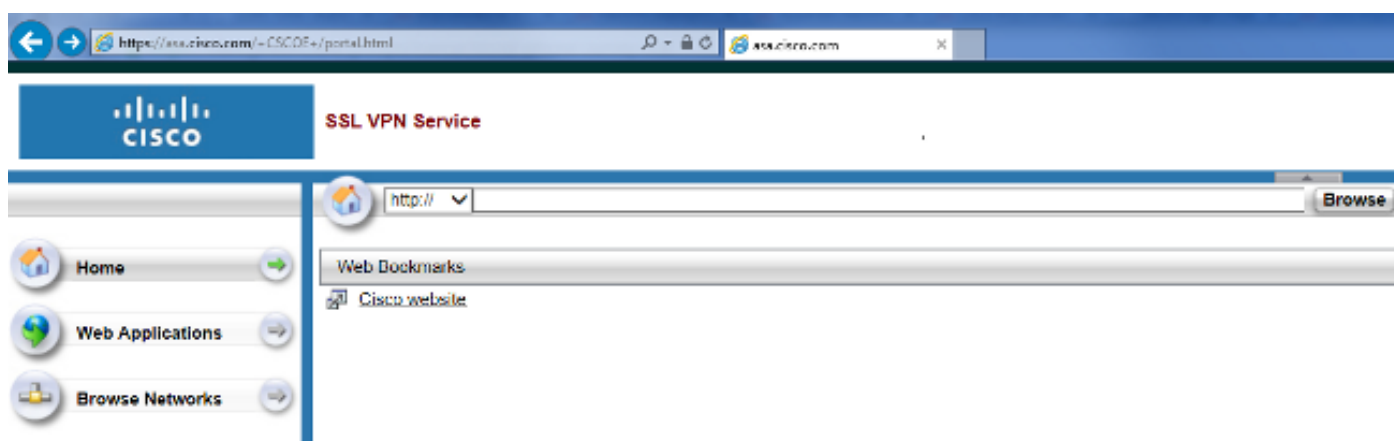
Verifica

Dopo aver configurato WebVPN, usare l'indirizzo `https://<FQDN dell'ASA>` nel browser.



A login dialog box with a title bar containing a key icon and the word "Login". The main area contains the text "Please enter your username and password." followed by two input fields labeled "USERNAME:" and "PASSWORD:". Below the fields is a "Login" button.

Dopo aver effettuato l'accesso, dovrebbe essere possibile visualizzare la barra degli indirizzi utilizzata per passare ai siti Web e ai segnalibri.



Risoluzione dei problemi

Procedure per la risoluzione dei problemi

Seguire queste istruzioni.

In ASDM, scegliere **Monitoraggio > Log > Real-time Log Viewer > Visualizza**. Quando un client si connette all'ASA, notare la creazione di una sessione TLS, la selezione di Criteri di gruppo e la riuscita dell'autenticazione dell'utente.

```

Device completed SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLSv1.2 session
SSL client outside:10.229.20.77/61307 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLS session
SSL client outside:10.229.20.77/61306 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLS session
Built inbound TCP connection 107 for outside:10.229.20.77/61307 (10.229.20.77/61307) to identity:10.48.66.179/443 (10.48.66.179/443)
Built inbound TCP connection 106 for outside:10.229.20.77/61306 (10.229.20.77/61306) to identity:10.48.66.179/443 (10.48.66.179/443)
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> Authentication: successful, Session Type: WebVPN.
Device selects trust-point ASA-self-signed for client outside:10.229.20.77/53047 to 10.48.66.179/443
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> WebVPN session started.
DAP: User admin, Addr 10.229.20.77, Connection Clientless: The following DAP records were selected for this connection: DfltAccessPolicy
AAA transaction status ACCEPT : user = admin
AAA retrieved default group policy (WEBVPN_Group_Policy) for user = admin
AAA user authentication Successful : local database : user = admin
Device completed SSL handshake with client outside:10.229.20.77/61304 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61303 to 10.48.66.179/443 for TLSv1.2 session

```

CLI:

```

ASA(config)# logging buffered debugging
ASA(config)# show logging

```

In ASDM, scegliere **Monitoraggio > VPN > Statistiche VPN > Sessioni > Filtra per: VPN SSL senza client**. Cercare la nuova sessione WebVPN. Assicurarsi di scegliere il filtro WebVPN e fare clic su **Filtro**. Se si verifica un problema, ignorare temporaneamente il dispositivo ASA per assicurarsi che i client possano accedere alle risorse di rete desiderate. Esaminare i passaggi di configurazione elencati in questo documento.

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left
admin 10.229.20.77	WEBVPN_Group_Policy DefaultWEBVPNGroup	Clientless Clientless: (1)AES128	10:40:04 UTC Tue May 26 2015 0h:02m:50s	63991 166375		

CLI:

```

ASA(config)# show vpn-sessiondb webvpn

Session Type: WebVPN

Username : admin Index : 3
Public IP : 10.229.20.77
Protocol : Clientless
License : AnyConnect Premium
Encryption : Clientless: (1)AES128 Hashing : Clientless: (1)SHA256
Bytes Tx : 72214 Bytes Rx : 270241
Group Policy : WEBVPN_Group_Policy Tunnel Group : DefaultWEBVPNGroup
Login Time : 10:40:04 UTC Tue May 26 2015
Duration : 0h:05m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a1516010000300055644d84
Security Grp : none

```

Comandi utilizzati per la risoluzione dei problemi

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le [informazioni importanti sui comandi di debug prima di usare i comandi di debug](#).

- **show webvpn** - Sono disponibili molti comandi **show** associati a WebVPN. Per informazioni dettagliate sull'utilizzo dei comandi **show**, vedere la sezione di [riferimento dei comandi](#) in Cisco Security Appliance.
- **debug webvpn**: l'uso dei comandi di **debug** può avere un impatto negativo sull'appliance ASA. Per informazioni più dettagliate sull'utilizzo dei comandi di **debug**, vedere la sezione di [riferimento dei comandi](#) in Cisco Security Appliance.

Problemi comuni

L'utente non può accedere

Problema

Viene visualizzato il messaggio "Accesso VPN SSL senza client (browser) non consentito." viene visualizzato nel browser dopo un tentativo di accesso non riuscito. La licenza AnyConnect Premium non è installata sull'appliance ASA o non è in uso, come mostrato nella sezione "La licenza AnyConnect Premium non è abilitata sull'appliance ASA".

Soluzione

Abilitare la licenza AnyConnect Premium con questi comandi:

```
ASA(config)# webvpn  
ASA(config-webvpn)# no anyconnect-essentials
```

Problema

Dopo un tentativo di accesso non riuscito, nel browser viene visualizzato il messaggio "Login failed" (Accesso non riuscito). Il limite di licenze AnyConnect è stato superato.

Soluzione

Cercare il messaggio nei registri:

```
%ASA-4-716023: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>  
Session could not be established: session limit of 2 reached.
```

Verificare inoltre il limite della licenza:

```
ASA(config)# show version | include Premium  
AnyConnect Premium Peers : 2 perpetual
```

Problema

Dopo un tentativo di accesso non riuscito, nel browser viene visualizzato il messaggio "AnyConnect is not enabled on the VPN server". Il protocollo VPN senza client non è abilitato nei Criteri di gruppo.

Soluzione

Cercare il messaggio nei registri:

```
%ASA-6-716002: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>  
WebVPN session terminated: Client type not supported.
```

Verificare che il protocollo VPN senza client sia abilitato per il criterio di gruppo desiderato:

```
ASA(config)# show run all group-policy | include vpn-tunnel-protocol  
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless
```

Impossibile connettere più di tre utenti WebVPN all'appliance ASA

Problema

Solo tre client WebVPN possono connettersi all'ASA. Connessione per il quarto client non riuscita.

Soluzione

Nella maggior parte dei casi, questo problema è correlato a un'impostazione di accesso simultaneo in Criteri di gruppo. Utilizzare questa illustrazione per configurare il numero desiderato di accessi simultanei. In questo esempio, il valore desiderato è 20.

```
ASA(config)# group-policy Cisco attributes  
ASA(config-group-policy)# vpn-simultaneous-logins 20
```

I client WebVPN non possono raggiungere i segnalibri ed è disattivato

Problema

Se questi segnalibri sono stati configurati per l'accesso degli utenti alla VPN senza client, ma nella schermata principale in "Web Applications" appaiono in grigio, come è possibile abilitare questi collegamenti HTTP in modo che gli utenti possano selezionarli e accedere all'URL specifico?

Soluzione

È necessario innanzitutto verificare che l'ASA sia in grado di risolvere i siti Web tramite DNS. Provare a eseguire il ping dei siti Web per nome. Se l'appliance ASA non è in grado di risolvere il nome, il collegamento è disattivato. Se i server DNS sono interni alla rete, configurare l'interfaccia privata di ricerca del dominio DNS.

Connessione Citrix tramite WebVPN

Problema

Viene visualizzato il messaggio di errore "il client ica ha ricevuto un file ica danneggiato." si verifica per Citrix su WebVPN.

Soluzione

Se si utilizza la modalità *gateway sicuro* per la connessione Citrix tramite WebVPN, il file ICA può essere danneggiato. Poiché l'appliance ASA non è compatibile con questa modalità operativa, creare un nuovo file ICA in modalità diretta (modalità non protetta).

Come evitare la necessità di una seconda autenticazione per gli utenti

Problema

Quando si accede ai collegamenti CIFS sul portale WebVPN senza client, dopo aver fatto clic sul segnalibro vengono richieste le credenziali. Il protocollo LDAP (Lightweight Directory Access Protocol) viene utilizzato per autenticare sia le risorse che gli utenti che hanno già immesso le credenziali LDAP per accedere alla sessione VPN.

Soluzione

In questo caso, è possibile utilizzare la funzione di firma automatica. In base ai criteri di gruppo specifici in uso e ai relativi attributi WebVPN, configurare quanto segue:

```
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri cifs://X.X.X.X/* auth-type all
```

dove X.X.X.X=IP del server CIFS e *=resto del percorso per raggiungere il file o la cartella condivisa in questione.

Di seguito è riportato un esempio di frammento di configurazione:

```
ASA(config)# group-policy ExamplePolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri
https://*.example.com/* auth-type all
```

Per ulteriori informazioni, vedere [Configurazione dell'SSO con l'autenticazione di base HTTP o l'autenticazione NTLM](#).

Informazioni correlate

- [ASA: Esempio di configurazione di Smart Tunnel con ASDM](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)