# Esempio di configurazione di ASA con WebVPN e Single Sign-On con ASDM e NTLMv1

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Configurazione Aggiungere un server AAA per l'autenticazione del dominio Windows Creare un certificato autofirmato Abilita WebVPN sull'interfaccia esterna Configurare un elenco di URL per i server interni Configurare Criteri di gruppo interni Configurare un gruppo di tunnel Configurare la firma automatica per un server Configurazione finale dell'ASA Verifica Verifica accesso WebVPN Sessioni di monitoraggio Debug di una sessione WebVPN Risoluzione dei problemi Informazioni correlate

# **Introduzione**

In questo documento viene descritto come configurare Cisco Adaptive Security Appliance (ASA) in modo che passi automaticamente le credenziali di accesso dell'utente WebVPN, nonché l'autenticazione secondaria, ai server che richiedono una convalida di accesso aggiuntiva in Windows Active Directory con NT LAN Manager versione 1 (NTLMv1). Questa funzionalità è nota come Single Sign-On (SSO). Fornisce ai collegamenti configurati per uno specifico gruppo WebVPN la possibilità di trasmettere queste informazioni di autenticazione utente, eliminando in tal modo più richieste di autenticazione. Questa funzione può essere utilizzata anche a livello di configurazione globale o utente.

# **Prerequisiti**

**Requisiti** 

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

• Verificare che le autorizzazioni NTLMv1 e Windows per gli utenti VPN di destinazione siano configurate. Per ulteriori informazioni sui diritti di accesso al dominio di Windows, consultare la documentazione di Microsoft.

#### Componenti usati

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

- Cisco ASA 7.1(1)
- Cisco Adaptive Security Device Manager (ASDM) 5.1(2)
- Microsoft Internet Information Services (IIS)

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.

#### **Convenzioni**

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

## **Configurazione**

In questa sezione vengono presentate le informazioni necessarie per configurare l'ASA come server WebVPN con SSO.

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

#### Aggiungere un server AAA per l'autenticazione del dominio Windows

Completare la procedura descritta di seguito per configurare l'appliance ASA in modo che utilizzi un controller di dominio per l'autenticazione.

 Selezionare Configurazione > Proprietà > Impostazione AAA > Server AAA e fare clic su Aggiungi. Fornire un nome per il gruppo di server, ad esempio Windows\_NT, e scegliere Dominio NT come protocollo.

Gaco ASDM 2	5.1 for ASA - 172.16.172.57	
Fie Rules Be	arch Options Tools Wizards	a Halp
- 🚯 🗌	🍫 😥	
Home 0	Configuration Monitoring	Back Forward Search Reflecth Save Help with a line at the
	Configuration • Properties • Av	AA Ostuo × AAA Gervers
Nertisses	全立平 町市市市	
24	Startup Wigard	AVA Servers
<b>1</b> 00,	AVA Servers	Sener Groups
Security Policy	SaAuth, Prompt	Server Group Protocol Accounting Node Reactivation Mode Add
64	- MATERIA AND UNS MAR	LOCAL LOCAL Edt.
NAT	₩- 🛃 ARF	Deels
- 25	- Auto Upcate R- D Certificate	
VI#1	🖶 🔐 Device Access	κ
<u> </u>	単部Device Administration 限部のLICE Services	
CSD Manugar	- BDNS Clent	Bevers in Selected Group
Q.	Falover	Server Name or IP Address Interface Timeout 200
PS	- RHistory Metrics	Edit .
123	- HTTP/HTTPS	Decle
Nouting	甲·哈川F Audit 回·司Longing	Minor as
8		70.48(20-0)
Global Gbjects	- 1883L	
5.	- TCP Options	🖬 dala data Sarawa Graum
Properties	-STImeoute	Contract Affection The tens when the set
	Cherry OHL Filtering	Apply Reset applicable for RACIUS and TACAGE+ protocols.
	4 <b>•</b>	
		oreco (NA (16) 😡 🎰 📋 Server Group: (Windows_N)
		Protocol UT Portain
		Azczuntag Koda 🔿 Smullaneuva 🛞 Single
		Reactivation Mode: <ul> <li>Depletion</li> <li>Timed</li> </ul>
		10
		Dead Time 10 minutes
		Nat Failed Aberrots: 3
		DV Concret Links
		OK Cantel Help

 Aggiungere un server Windows.Selezionare il gruppo appena creato e fare clic su Aggiungi. Selezionare l'interfaccia in cui si trova il server e immettere l'indirizzo IP e il nome del controller di dominio. Assicurarsi che il nome del controller di dominio sia scritto in maiuscolo. Al termine, fare clic su OK.

🖆 Cisco ASDM	5.1 for ASA -	172.16.172.5	2					<b>1</b>		
Fie Rulas Ga	anth <b>Options</b>	Tools Wizard	is Help							
i dia amin'ny fiana amin'ny fi	Configuration	[] Montoring	C Dack	O Forward	Q ( Search Re	💽 🔚 fresh Save	? Hela	Cisco Sr	allu.	
interfacese	Sentiputeter 9 (2) T - P Startu D AAA S - C Startu D AAA S - C Startu - C Startu	n - Properties - × I III   1   1   2   1 p Wizand stup A Carvers th. Prompt	AAA Setu AAAA S - Se S	pin AAA Berverie Re Kall © I Servers Inter Groups erver Groups	Protocol	Accounting Mod	ie Reactivation	Mode Add		
NAT SAT	- Seco -	MP Adribute Map poofing Jodate	UC [77]	CAL ndows_NT	LOCAL NT Domai		Depleti	nn Edit Delete		
VFN CSD Monager	E Certifi E Certifi E Societa E Conce E Conce	cate e Access e Administration ? Services Client	-Se	wers in Selector	d Group			>		
irs Racha	Failow FSFragm FSF FSFragm	er vent v Metrics HTTPS	8	erver Name or I	P Address	Interface	Timeout	Add Edit Delete		
Ginbal Objects	E Coggi F Priorit F SEL F SUNR	ng y Queue IPC Server						Move up biove down		
Properties	는 쇼라TCP C OTimed - 쨜URL P	Dations Inits Fitering				Apply	Rese Server	AA Server Group:	Windows_NT	X
	,				cisco	NA (15)	interfa Server	te Name: Name or IP Address:	inside 10.1.1.200	
							Timed NT Do Servi	ut: main Parameters er Port: en Dontraler.	10 139 Esc.e2200	seconds
								ок	Cancel	Help

Questa finestra mostra la configurazione AAA completata:



## Creare un certificato autofirmato

Completare la procedura seguente per configurare l'appliance ASA per l'utilizzo di un certificato autofirmato.

**Nota:** in questo esempio viene utilizzato un certificato autofirmato per semplificare la gestione. Per ulteriori opzioni di registrazione dei certificati, ad esempio la registrazione a un'Autorità di certificazione esterna, vedere <u>Configurazione dei certificati</u>.

- 1. Selezionare Configurazione > Proprietà > Certificato > Trustpoint > Configurazione e fare clic su Aggiungi.
- Nella finestra che viene visualizzata, immettere un nome di trust, ad esempio Local-TP, e selezionare Generate a self-signed certificate on enrollment (Genera certificato autofirmato all'iscrizione). È possibile lasciare invariate le altre opzioni con le relative impostazioni predefinite. Al termine, fare clic su OK.



In questa finestra viene visualizzata la configurazione di Trustpoint completata:



## Abilita WebVPN sull'interfaccia esterna

Completare questa procedura per consentire agli utenti esterni alla rete di connettersi utilizzando WebVPN.

- 1. Selezionare Configurazione > VPN > WebVPN > Accesso WebVPN.
- 2. Selezionare l'interfaccia desiderata, fare clic su Abilita e selezionare Abilita elenco a discesa Gruppo tunnel nella pagina di accesso a WebVPN.Nota: se si utilizza la stessa interfaccia per l'accesso WebVPN e ASDM, è necessario modificare la porta predefinita per l'accesso ASDM dalla porta 80 a una nuova porta, ad esempio 8080. Questa operazione viene eseguita in Configurazione > Proprietà > Accesso dispositivo > HTTPS/ASDM.Nota: è possibile reindirizzare automaticamente un utente alla porta 443 nel caso in cui un utente passi a http://<indirizzo\_ip> anziché a https://<indirizzo\_ip>. Selezionare Configurazione > Proprietà > HTTP/HTTPS, scegliere l'interfaccia desiderata, fare clic su Modifica e selezionare Reindirizza HTTP a HTTPS.

🖆 Cisco ASDM 5.1 for ASA - 172.16.171.51						
File Rules Se	arch Options Tools Wizards	Help				
in the second se	Configuration Monitoring	Sack Forward Search Refresh Save Help	STENS Allana			
	Configuration > VPN > WebVPN	> WebVPN Access				
Ξ,	●金革 ■ 前 炎暭	8. 免 筋 ( )				
Interfaces	(마젤E-mail Proxy 🔺	WebVPN Access				
<u>6</u>	General					
Security Policy	- B Client Update	Configure access parameters for WebVPN. (Note: The WebVPN features in this software release are currently provided as a free trial, and future major software releases will require the purchase and	6			
24	Group Policy	installation of a WebVPN feature license.)				
NAT	- 💭 Tunnel Group					
13	- SIVPN System Opt	Interface WebVPN Enabled Enable				
<u>88</u>	E Address Manager	outside Yes Disable				
VPN	🕀 🥵 IPSec		- 1			
<u> </u>						
CSD Manager						
۵.	-JAPCF					
IPS	- BCSD Setup	Port Number: 443				
4≩⊳	- Cache	Defaultiple Times de 1900				
Routing	- The Encoding	Default ldie Timeout: Tabu seconds				
(A)	- Sport Forwarding	Max. Sessions Limit: 2				
Clabel Objects	- Proxies	WebVPN Nemory Size: 50 % of Intel Integral memory				
Gibbal Objects	- 39 Proxy Bypass					
3	SSO Servers	Enable Tunnel Group Drop-down List on WebYPN Login Page				
Properties	Servers and URL					
	WebyPN Access	Apply Reset				
	<					
Configuration cha	anges saved successfully.	cisco 🛛 NA (15) 🛛 🛃 🖬 🔹 3/30/06 2:37:41 PM	UTC			

## Configurare un elenco di URL per i server interni

Completare questi passaggi per creare un elenco contenente i server per i quali si desidera concedere l'accesso agli utenti WebVPN.

- 1. Selezionare Configurazione > VPN > WebVPN > Server e URL e fare clic su Aggiungi.
- 2. Immettere un nome per l'elenco di URL. Questo nome non è visibile agli utenti finali. Fare clic su Add.
- 3. Immettere il nome visualizzato dell'URL da visualizzare agli utenti. Immettere le informazioni sull'URL del server. Questo dovrebbe essere il modo in cui si accede normalmente al server.



4. Fare clic su OK, OK e quindi su Applica.



## Configurare Criteri di gruppo interni

Completare la procedura seguente per configurare un criterio di gruppo per gli utenti WebVPN.

- 1. Selezionare Configurazione > VPN > Generale > Criteri di gruppo, fare clic su Aggiungi e selezionare Criteri di gruppo interni.
- Nella scheda Generale specificare un nome di criterio, ad esempio Gruppo interno\_POL\_WEBVPN. Quindi, deselezionare Inherit (Eredita) accanto a Tunneling Protocol (Protocolli di tunneling) e selezionare WebVPN (VPN Web).

🖆 Add Internal Group Policy							
Name: mal-GRP_POL_WEBVPN	4						
General IPSec Client Configuration	Client Firewall Hardware Client WebVPN						
Check an Inherit checkbox to let the	Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.						
Tunneling Protocols: 🗌 Inhe	rit 🔲 IPSec 🗹 WebVPN						
Filter: 🔽 Inhe	rit Manage						
Connection Settings							
Access Hours: 🗹 Inhe	rit New						
Simultaneous Logins: 🗹 Inhe	rit						
Maximum Connect Time: 🗹 Inhe	rit Unlimited minutes						
Idle Timeout: 🗹 Inhe	rit Unlimited minutes						
Servers							
DNS Servers: 🔽 Inhe	rit Primary; Secondary;						
WINS Servers: 🗹 Inhe	rit Primary: Secondary:						
DHCP Scope: 🗸 Inhe	rit						
OK	Cancel Help						

 Nella scheda WebVPN selezionare la scheda secondaria Altro. Deselezionare Inherit (Eredita) accanto a Server ed elenchi URL, quindi selezionare l'elenco di URL configurato dall'elenco a discesa. Al termine, fare clic su OK.

🖆 Add Internal Group Policy	
Name: mal-GRP_POL_WEBVPN	
General IPSec Client Configuration Client Firewall Hardware Client WebVPN	
Configure WebVPN attributes using the following tabs . Check an Inherit checkbox to let the corresponding setting take its value from the defa	ult group policy.
Functions Content Filtering Homepage Port Forwarding Other SSL VPN Clier	nt
Servers and URL Lists: 📃 Inherit 🛛 webserver	New
Web-Type ACL ID: 🔽 Inherit	Manage
SSO Server: 🔽 Inherit	New
HTTP Compression: VInherit O Enable O Disable	
Keepalive Ignore	
Specify upper limit of the HTTP/HTTPS traffic, per transaction to ignore. Transaction Size:  Inherit	
Deny Message	
	]
OK Cancel Help	

## Configurare un gruppo di tunnel

Completare questa procedura per configurare un gruppo di tunnel per gli utenti WebVPN.

 Selezionare Configurazione > VPN > Generale > Gruppo tunnel, fare clic su Aggiungi e selezionare Accesso WebVPN...



2. Immettere un nome per il gruppo di tunnel, ad esempio WEB\_VPN-GRP. Nella scheda Base selezionare i Criteri di gruppo creati e verificare che il tipo di gruppo sia **webvpn**.

📧 Edit Tunnel Group 🛛 🔀						
Name: WEB_VPN-GRP Type: webvpn						
General WebVPN						
Basic AAA Client Address Assignment Advensed						
AAA Client Address Assignment Advanced						
Group Policy: Internal-GRP_POL						
Internal-GRP_POL_WEBV DftGrpPolicy						
strip the realm from username before passing it on to the AAA server						
Strip the group from username before passing it on to the AAA server						
OK Cancel Help						

3. Selezionare la scheda AAA.In Gruppo server di autenticazione scegliere il gruppo configurato per abilitare l'autenticazione NTLMv1 con il controller di dominio.Facoltativo: Selezionare Utilizza LOCAL se il gruppo di server non riesce a abilitare l'uso del database locale nel caso in cui si verifichi un errore nel gruppo AAA configurato. Ciò consente di risolvere i problemi in un secondo momento.

🖆 Edit Tunnel Group						
Name: WEB_VPN-GRP Type: webvpn						
General WebVPN						
Configure general access attributes from the following sub-tabs.						
Basic AAA Client Address Assignment Advanced						
To set authentication server group per interface, go to the Advanced tab.						
Authentication Server Group: Windows_NT						
Use LOCAL if Server Ord Windows NT						
Authorization Server Group: LOCAL						
<ul> <li>Users must exist in the authorization database to connect</li> </ul>						
Accounting Server Group: None						
Authorization Settings						
◯ Use the entire DN as the username						
<ul> <li>Specify individual DN fields as the username</li> </ul>						
Primary DN Field: CN (Common Name)						
Secondary DN Field: OU (Organization Unit)						
Password Management						
Override account-disabled indication from AAA server						
Enable notification upon password expiration to allow user to change password						
Enable notification prior to expiration Notify days prior to expiration						
OK Cancel Help						

- 4. Andare alla scheda WebVPN e quindi alla scheda secondaria Alias e URL gruppo.
- 5. Immettere un alias in Alias gruppo e fare clic su **Aggiungi**. Questo alias viene visualizzato nell'elenco a discesa visualizzato agli utenti WebVPN al momento dell'accesso.

🖆 Edit Tunnel Group
Name: WEB_VPN-GRP Type: webvpn
General WebVPN
Configure WebVPN access attributes from the following sub-tabs.
Basic NetBIOS Servers Group Allases and ORLs Web Page
Group Aliases Status
Alias: Add >> Group-Selection enable
<< Remove
✓ Enable
Group URLs
URL (http or https): Add >>
<< Remove
✓ Enable
OK Cancel Help

6. Fare clic su **OK**, quindi su **Applica**.

#### Configurare la firma automatica per un server

Passare alla riga di comando per abilitare SSO per i server interni.

**Nota:** questo passaggio non può essere completato in ASDM e deve essere eseguito dalla riga di comando. Per ulteriori informazioni, fare riferimento a <u>Accesso all'interfaccia della riga di comando</u>.

Utilizzare il comando **auto-signon** per specificare la risorsa di rete, ad esempio un server, a cui si desidera consentire l'accesso agli utenti. In questa configurazione è configurato un singolo indirizzo IP del server, ma è possibile specificare un intervallo di rete, ad esempio **10.1.1.0** /24. Per ulteriori informazioni, fare riferimento al comando <u>auto-sign</u>.

```
ASA>enable
ASA#configure terminal
ASA(config)#webvpn
ASA(config-webpvn)#auto-signon allow ip 10.1.1.200 255.255.255.255 auth-type ntlm
ASA(config-webvpn)#quit
ASA(config)#exit
ASA(config)#exit
```

In questo output di esempio, il comando **auto-sign** è configurato globalmente per WebVPN. Questo comando può essere utilizzato anche in modalità di configurazione gruppo WebVPN o nome utente WebVPN. L'utilizzo di questo comando nella modalità di configurazione gruppo WebVPN lo limita a un gruppo particolare. Analogamente, l'utilizzo di questo comando nella modalità di configurazione del nome utente WebVPN lo limita a un singolo utente. Per ulteriori informazioni, fare riferimento al comando <u>auto-sign</u>.

#### Configurazione finale dell'ASA

Nel documento viene usata questa configurazione:

```
ASA versione 7.1(1)
ASA# show running-config
: Saved
ASA Version 7.1(1)
terminal width 200
hostname ASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.171.51 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
1
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
 shutdown
no nameif
no security-level
no ip address
```

passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name cisco.com pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm512.bin no asdm history enable arp timeout 14400 route outside 0.0.0.0 0.0.0.0 172.16.171.1 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip\_media 0:02:00 timeout uauth 0:05:00 absolute !--- AAA server configuration aaa-server Windows\_NT protocol nt aaa-server Windows\_NT host 10.1.1.200 ntauth-domain-controller ESC-SJ-7800 !--- Internal group policy configuration group-policy Internal-GRP\_POL\_WEBVPN internal group-policy Internal-GRP\_POL\_WEBVPN attributes vpn-tunnel-protocol webvpn webvpn url-list value webserver username cisco password Q/odgwmtmVIw4Dcm encrypted privilege 15 aaa authentication http console LOCAL aaa authentication ssh console LOCAL aaa authentication enable console LOCAL http server enable 8181 http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart !--- Trustpoint/certificate configuration crypto ca trustpoint Local-TP enrollment self crl configure crypto ca certificate chain Local-TP certificate 31 308201b0 30820119 a0030201 02020131 300d0609 2a864886 f70d0101 04050030 le311c30 la06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 1e170d30 36303333 30313334 3930345a 170d3136 30333237 31333439 30345a30 le311c30 la06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100 e47a29cd 56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6 58f3bec4 a60b2025 03748d5b 1226b434 561e5507 5b45f30e 9d65a03f 30add0b5 81f6801a 766c9404 9cabcbde 44b221f9 b6d6dc18 496fe5bb 4983927f adabfb17 68b4d22c cddfa6c3 d8802efc ec3af7c7 749f0aa2 3ea2c7e3 776d6d1d 6ce5f748 e4cda3b7 4f007d4f 02030100 01300d06 092a8648 86f70d01 01040500 03818100 c6f87c61 534bb544 59746bdb 4e01680f 06a88a15 e3ed8929 19c6c522 05ec273d 3e37f540 f433fb38 7f75928e 1b1b6300 940b8dff 69eac16b af551d7f 286bc79c e6944e21 49bf15f3 c4ec82d8 8811b6de 775b0c57 e60a2700 fd6acc16 a77abee6 34cb0cad 81dfaf5a f544258d cc74fe2d 4c298076 294f843a edda3a0a 6e7f5b3c quit !--- Tunnel group configuration tunnel-group WEB\_VPN-GRP type webvpn tunnel-group WEB\_VPN-GRP general-attributes authentication-server-group Windows\_NT default-grouppolicy Internal-GRP\_POL\_WEBVPN tunnel-group WEB\_VPN-GRP webvpn-attributes group-alias Group-Selection enable telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection\_default match default-inspectiontraffic ! ! policy-map global\_policy class inspection\_default inspect dns maximum-length 512

inspect ftp inspect h323 h225 inspect h323 ras inspect				
netbios inspect rsh inspect rtsp inspect skinny inspect				
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect				
<pre>sip inspect xdmcp ! service-policy global_policy global</pre>				
! WebVPN Configuration webvpn enable outside url-list				
webserver "Internal Server" https://10.1.1.200 1 tunnel-				
group-list enable auto-signon allow ip 10.1.1.200				
255.255.255.255 auth-type ntlm				
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6				
: end				

# **Verifica**

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

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

#### Verifica accesso WebVPN

Eseguire il login come utente per verificare la configurazione.

1. Tentare di accedere all'appliance ASA con le informazioni utente dal dominio NT. Selezionare l'alias del gruppo configurato nel passaggio 5 in <u>Configure a Tunnel</u>

<u>Group</u> .	
WebVPN Service - Microsoft Internet Explorer	
Ele Edit Wew Fgyorites Icols Help	a da katalah yang da 🖉 🖉
😋 Back 🔹 🐑 🕐 📓 🏠 🔎 Search 🤺 Favorites  🚱 - چ 🔂 🚳	
Address 🔊 https://172.16.171.51/+webvpr+/index.html	🗸 🋃 🚱 🛛 Unks 🎽
CISCO STRTEMS 	
Login	
Please enter your usemame and password.	1
USERNAME: test	
PASSWORD:	
GROUP: Group-Selection	
Login Clear	
	-
Done	🔒 🥶 Internet

2. Cercare i collegamenti configurati per i server interni. Fai clic sul link per verificare.

WebVPN Service - Microsoft Internet	et Explorer	
Elle Edit Yew Fevorites Icols Help		<b>R</b>
🌀 Back = 🛞 - 💌 🖻 🏠 🏓	🔎 Search 🧏 Favorites 🥝 🔗 🛁 🦝	
Address 🙋 https://172.16.171.51/+webvpn+/	e/portal.html 😒 🔂 Go	a Links 🌺
S Pop-up blocked. To see this pop-up or addition	onal options dick here	×
Cisco Systems additional WebVPN Servi	rice	
	Click here to open the Floating Toolbar 🖓 🖉 🙆	
WEB APPLICATIONS	Web Bookmarks	
Enter Web Address (URL)	Internal Server	
Go		
Web Bookmarks 👻		
		-
isusceptibles delilabilid@https://10.1.1.2005	n 🔂 🛆 internet	×
<ul> <li>Javaschpracopracowencing (https://10.111.2007</li> </ul>		

## Sessioni di monitoraggio

Selezionare **Monitoraggio > VPN > Statistiche VPN > Sessioni** e cercare una sessione WebVPN appartenente al gruppo configurato in questo documento.

🚰 Cisco ASDM 5.1 for ASA - 172	2.16.171.51			
File Rules Search Options To	'ools Wizards Help			
Home Configuration M	Ionitoring	Q @ Search Refresh	調 🦓 Save Halp	Cisco Systems
Image: Second system         Image: Second system	I > VPN Statistics > Sessions         nection Grapi         Tunnels         PNSVC         stics         or Loads         o Statistics         or Statistics         of Statistics         test         171.69.89.116         I < To sort VPN session         Logout By:         - All statistics	LAN WebVPN SSL VPN 0 1 N P - All Session Group Policy Tunnel Group Internal-ORP_POL WEB VPN-GRP Sessions -	I Client E-mail Proxy 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Total Total Cumulative 1 3 Filter Login Ti Details Duratior 03:36 UTC Thu t 01m:18s Ping Order from popup menu. t Sessions
Data Refreshed Successfully.		cisco NA	(15) 📑 🔂 🐼	🖄 3/30/06 3:05:21 PM UTC

#### Debug di una sessione WebVPN

Questo output è un esempio di debug di una sessione WebVPN riuscita.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

```
ASA#debug webvpn 255
INFO: debug webvpn enabled at level 255
ASA#
ASA# webvpn_portal.c:ewaFormServe_webvpn_login[1570]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286]
WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782]
!--- Begin AAA WebVPN: calling AAA with ewsContext (78986968) and nh (78960800)! WebVPN: started
user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422]
WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095]
WebVPN: user: (test) authenticated.
!--- End AAA webvpn_auth.c:http_webvpn_auth_accept[2093]
webvpn_session.c:http_webvpn_create_session[159] webvpn_session.c:http_webvpn_find_session[136]
```

#### WebVPN session created!

```
webvpn_session.c:http_webvpn_find_session[136]
webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202]
traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421]
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
!--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn auth.c:webvpn auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

## Risoluzione dei problemi

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

- Se la casella a discesa Gruppo non è presente nella pagina di accesso di WebVPN, accertarsi di aver completato il passaggio 2 in <u>Abilita WebVPN sull'interfaccia esterna</u> e il passaggio 5 in <u>Configura un gruppo di tunnel</u>. Se questi passaggi non vengono completati e l'elenco a discesa risulta mancante, l'autenticazione rientra nel gruppo predefinito e potrebbe non riuscire.
- Sebbene non sia possibile assegnare i diritti di accesso all'utente in ASDM o sull'appliance ASA, è possibile limitare gli utenti con diritti di accesso a Microsoft Windows sul controller di dominio. Aggiungere le autorizzazioni del gruppo NT necessarie per la pagina Web a cui l'utente esegue l'autenticazione. Una volta che l'utente accede a WebVPN con le autorizzazioni del gruppo, l'accesso alle pagine specificate viene concesso o negato di conseguenza. L'appliance ASA opera solo come host di autenticazione proxy per conto del controller di dominio e tutte le comunicazioni presenti sono NTLMv1.
- Impossibile configurare SSO per SharePoint su WebVPN. Il server SharePoint non supporta l'autenticazione basata su moduli. Di conseguenza, i segnalibri con post o la procedura di plug-in post non sono applicabili qui.

## Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- Documentazione e supporto tecnico Cisco Systems