ASA 8.x: Esempio di configurazione dell'appliance ASA che consente il tunneling ripartito per il client VPN AnyConnect

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Configurazione Esempio di rete Configurazione ASA con ASDM 6.0(2) Configurazione ASA CLI Stabilire la connessione VPN SSL con SVC Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento offre istruzioni dettagliate su come consentire ai client VPN Cisco AnyConnect di accedere a Internet mentre sono tunneling in una Cisco Adaptive Security Appliance (ASA) 8.0.2. Questa configurazione consente al client di accedere in modo sicuro alle risorse aziendali tramite SSL e allo stesso tempo di accedere a Internet in modo non protetto con il tunneling suddiviso.

Prerequisiti

Requisiti

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

- ASA Security Appliance deve eseguire la versione 8.x
- Cisco AnyConnect VPN Client 2.xNota: scaricare il pacchetto AnyConnect VPN Client (anyconnect-win*.pkg) da Cisco <u>Software Download</u> (solo utenti <u>registrati</u>). Copiare il client VPN AnyConnect nella memoria flash dell'ASA, da scaricare sui computer degli utenti remoti per stabilire la connessione VPN SSL con l'ASA. Per ulteriori informazioni, consultare la sezione <u>Installazione del client</u> AnyConnect della guida alla configurazione delle appliance

ASA.

Componenti usati

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

- Cisco serie 5500 ASA con software versione 8.0(2)
- Cisco AnyConnect SSL VPN Client versione per Windows 2.0.0343
- PC con Microsoft Vista, Windows XP SP2 o Windows 2000 Professional SP4 e Microsoft Installer versione 3.1
- Cisco Adaptive Security Device Manager (ASDM) versione 6.0(2)

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>

Premesse

Il client VPN Cisco AnyConnect fornisce connessioni SSL sicure all'appliance di sicurezza per gli utenti remoti. Senza un client installato in precedenza, gli utenti remoti immettono l'indirizzo IP nel browser di un'interfaccia configurata per accettare connessioni VPN SSL. A meno che l'appliance di sicurezza non sia configurata per reindirizzare le richieste http:// a https://, gli utenti devono immettere l'URL nel formato https://<indirizzo.

Dopo aver immesso l'URL, il browser si connette all'interfaccia e visualizza la schermata di accesso. Se l'utente soddisfa i requisiti di accesso e autenticazione e l'appliance di sicurezza identifica l'utente come utente che richiede il client, scarica il client corrispondente al sistema operativo del computer remoto. Al termine del download, il client si installa e si configura, stabilisce una connessione SSL protetta e rimane o si disinstalla (a seconda della configurazione dell'appliance di sicurezza) quando la connessione viene interrotta.

Nel caso di un client installato in precedenza, quando l'utente esegue l'autenticazione, l'appliance di sicurezza esamina la revisione del client e lo aggiorna in base alle esigenze.

Quando il client negozia una connessione VPN SSL con l'appliance di sicurezza, si connette utilizzando TLS (Transport Layer Security) e, facoltativamente, DTLS (Datagram Transport Layer Security). DTLS evita i problemi di latenza e larghezza di banda associati ad alcune connessioni SSL e migliora le prestazioni delle applicazioni in tempo reale che sono sensibili ai ritardi dei pacchetti.

Il client AnyConnect può essere scaricato dall'appliance di sicurezza o installato manualmente sul PC remoto dall'amministratore di sistema. Per ulteriori informazioni su come installare manualmente il client, consultare la <u>Cisco AnyConnect VPN Client Administrator Guide</u>.

L'accessorio di protezione scarica il client in base agli attributi dei criteri di gruppo o del nome utente dell'utente che stabilisce la connessione. È possibile configurare l'appliance di sicurezza in modo che il client venga scaricato automaticamente oppure in modo che venga richiesto all'utente remoto se scaricare il client. Nel secondo caso, se l'utente non risponde, è possibile configurare l'appliance di sicurezza in modo che scarichi il client dopo un periodo di timeout o presenti la pagina di accesso.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

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

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi <u>RFC 1918</u> utilizzati in un ambiente lab.

Configurazione ASA con ASDM 6.0(2)

in questo documento si presume che la configurazione di base, ad esempio la configurazione dell'interfaccia, sia già stata creata e funzioni correttamente.

Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'<u>autorizzazione</u> dell'<u>accesso HTTPS per ASDM</u>.

Nota: WebVPN e ASDM non possono essere abilitati sulla stessa interfaccia ASA a meno che non si modifichino i numeri di porta. Per ulteriori informazioni, fare riferimento a <u>ASDM e WebVPN</u> <u>abilitati sulla stessa interfaccia dell'ASA</u>.

Per configurare la VPN SSL sull'appliance ASA con tunneling suddiviso, completare la procedura seguente:

1. Per creare un pool di indirizzi IP, scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Gestione indirizzi > Pool di indirizzi > Aggiungi

	🚰 Add IP Pool			
	Name:		vpnpool	
	Starting IP Ad	dress:	192.168.10.1	
	Ending IP Add	ress:	192.168.10.2	254
	Subnet Mask:		255.255.255	.0
vpnpool.	ок		Cancel	Help

- 2. Fare clic su Apply (Applica). Configurazione CLI equivalente:
- 3. Abilita WebVPN.Scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione VPN SSL e in Interfacce di accesso, fare clic sulle caselle di controllo Consenti accesso e Abilita DTLS per l'interfaccia esterna. Inoltre, selezionare la casella di controllo Abilita accesso client VPN Cisco AnyConnect o client VPN SSL legacy sull'interfaccia selezionata nella tabella seguente per abilitare VPN SSL sull'interfaccia esterna.

Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles						
The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.						
(More client-related)	(More client-related parameters, such as client images and client profiles, can be found at <u>Client Settings</u>					
	Connect VPIN Client of 16	egacy SSL VPIN Client access on the I	Interraces selected in the			
Interface	Allow Access	Require Client Certificate	Enable DTLS			
outside	V					
inside						
Access Port: 443 DTLS Port: 443						
clicit horo to <u>Hosiqii (</u>	continued to interneted					

Fare clic su **Apply** (Applica).Per aggiungere l'immagine del client VPN Cisco AnyConnect dalla memoria flash dell'ASA, scegliere **Configurazione > VPN** ad **accesso remoto > Accesso** di **rete (client) > Avanzate > VPN SSL > Impostazioni client > Aggiungi**, come mostrato.

🕵 Add SSL VPN Client I	mage		SSL VPN > Cli	ent Settings
Flash SVC Image:		Browse Flash		
		Upload		ion sustem to the top of the
OK	Cancel	Help	puncereu opera	lion system to the top of the
🎼 Browse Flash				×
Folders	Files			
⊟- 🧼 disk0:		FileName 🔬	Size (bytes)	Date Modified
E-log	iua Cryp	to_archive		07/24/07 05:21:48
				07/24/07 05:21:36
	asdr	m-603.bin	6,851,212	01/04/08 18:07:02
	asat	303-k8.bin	14,635,008	01/04/08 17:49:50
	adm	in.cfg	1,220	09/20/07 09:51:38
	anyo	connect-win-2.0.03	, 2,635,734	08/13/07 04:14:50
	asdr	m-602.bin	6,889,764	01/03/08 21:38:26
	asa,	/22-K8.DIN	0,312,032	02/13/07 04:16:30
	asor	11-522.0IN	14 524 416	02/12/07 05:55:46
	asad	NUZ-KO, DITI	1 841	01/03/08 21:24:42
	oid_	iont-win-1 1 4 179	418 765	03/14/08 13:47:58
File	Name: anyconn	ect-win-2.0.0343-k9	.pkg	
i	dd SSL VPN C	ient Image		
		incine innoge		
Flas	h SVC Image:	ct-win-2.0.0343-k	9.pkg Browse Fl	ash
			Upload	1
	OK	Cancel	Halp	1
Fare clic su OK.				Fare clic su
Add.				
Configuration > Remote A	Access VPN > N	etwork (Client) Ac	cess > Advanced > S	SL VPN > Client Settings
Identify SSL VPN Client (S	5VC) related files.			
SSL VPN Client Images	time by movina l	the image used by the	e most commonly encou	ntered operation system to l
Add Replace	Delete	• Move UP	e Down	nered operation system to t
	0.0242 kg -kg			
disku:/anyconnect-win-2	.0.0343-K9.pkg			

Configurazione CLI equivalente:

4. Configurare Criteri di gruppo.Per creare un gruppo di client di Criteri di gruppo interno, scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo. Nella scheda Generale, selezionare la casella di controllo SSL VPN Client per abilitare WebVPN come protocollo di

tu	nneling. Add Internal Group Policy	
Genera Servers Advance JE B E-SSL E-SSL	General Servers Advanced Split Tunneling IE Browser Proxy	Name: clientgroup Banner: ☑ Inherit Address Pools: ☑ Inherit
		Mars Dellar a
		Tunneling Protocols:

Nella scheda **Avanzate > Tunneling ripartito**, deselezionare la casella di controllo **Eredita** per Criterio tunnel ripartito e scegliere **Elenco reti tunnel sotto** dall'elenco a discesa.

🚰 Add Internal Group Policy				X
General Servers -Advanced	Split tunneling network lists distinguish ne require tunneling. The security appliance ACL that consists of list of addresses on I	stworks that require traffic to go thro makes split tunneling decisions on th the private network.	ough the tunnel and t ne basis of a network	hose that do not list, which is an
	Policy: Inherit Tunnel Al Ne Network List: I Inherit Tunnel Al Ne Tunnel Al Ne Tunnel Network Exclude Netwo	etworks etworks ork List Belaw work List Belaw	T	Manage

Deselezionare la casella di controllo **Eredita** per **Elenco reti tunnel** e fare clic su **Gestisci** per avviare Gestione

ACL.	
💼 Edit Internal Group Policy:	hivalleyvpn
General Servers Advanced	Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.
SSL VPN Client	Policy: Inherit Tunnel Network List Below Network List: Inherit None
Hardware Client	

In Gestione ACL, selezionare Add > Add ACL... (Aggiungi ACL) per creare un nuovo elenco degli

accessi.

<u>1</u>	ACL Manager				
ſ	Standard ACL Extended	ACL			
	🔂 Add 🕞 📝 Edit 📋	Delete 🛧 🗲	* * * ®	*	
	🔂 Add ACL	dress	Action	Description	
	 Add ACL Add ACE 	dress	Action	Description	
	 Add ACL Add ACE Insert 	dress	Action	Description	

Specificare un nome per l'ACL e fare clic su

OK							
1	ACL Manag	er					
	Standard AC	L Extend	ed ACL				
	🔂 Add 👻	📑 Edit	<u>î</u> Delete 🔶	+ % h f	-		
	No		Address	Action		Description	
	🔂 Add A	CL			×		
	ACL Nar	me: split-tu	nnel				
			1	1	1		

Una volta creato il nome dell'ACL, scegliere **Aggiungi > Aggiungi ACE** per aggiungere una voce di controllo di accesso (ACE, Access Control Entry).Definire l'ACE che corrisponde alla LAN dietro l'ASA. In questo caso, la rete è 10.77.241.128/26 e selezionare **Permit** come azione.Per uscire da Gestione ACL, fare clic su **OK**.

No	Address	Action	Des	cription
split-tunnel				
🔄 Add ACE				
Host/Net	work			
IP Add	ress: 10.77.241.128			-
Netmas	sk: 255.255.255.192			T
Description	o.			

Verificare che l'ACL appena creato sia selezionato per l'elenco delle reti a tunnel separato. Per tornare alla configurazione di Criteri di gruppo, fare clic su **OK**

🔂 Add Internal Group Policy									×
General Servers Advanced <u>Splt Tunneling</u> IE Browser Proxy E-SSL VPN Client F-IPsec Client	Split tunneling require tunne ACL that cons DNS Names: Policy:	ing, The sect sists of list of Inherit	s distinguish nei urity appliance i addresses on t	tworks that re makes split tun he private net ork List Below	quire traffic to neling decision work.	go through is on the ba:	the tunnel and t sis of a network	hose that do list, which is a	not an
	Network List:	🕅 Inherit	split-tunnel					Manage	
	Intercept	DHCP Confi	guration Mes	sage from M	icosoft Clien	lts			¥

Nella pagina principale, fare clic su **Apply**, quindi su Send (se necessario) per inviare i comandi all'appliance ASA.Configurare le impostazioni della **VPN SSL** in modalità Criteri di gruppo.Per l'opzione Mantieni programma di installazione sul sistema client, deselezionare la casella di controllo **Eredita** e fare clic sul pulsante di opzione **S**ì.Questa azione consente al software SVC di rimanere sul computer client. Pertanto, ogni volta che si effettua una connessione, l'ASA non deve scaricare il software SVC sul client. Questa opzione è ideale per gli utenti remoti che spesso accedono alla rete aziendale.

🧱 Edit Internal Group Policy	r: clientgroup			
General	Keep Installer on Client System:	🔲 Inherit	• Yes	C No
E-Advanced	Compression:	🔽 Inherit	m C Enable	C Disab
	Datagram TLS:	🔽 Inherit	C Enable	C Disab
ECCEPTION Client	Keepalive Messages:	🔽 Inherit	🗖 Disable	Interval:

Fare clic su **Login Setting** (Impostazione accesso) per impostare **Post Login Setting** (Impostazione post accesso) e **Default Post Login Selection** (Selezione predefinita post accesso), come

mostrato

General	 After successfully logging in, user can have the choice to download the client software, or g portal page. The following settings decides what will happen.
-Advanced	Inherit
-Split Tunneling	
IE Browser Proxy	Post Login Setting —
-SSL VPN Client -Login Setting	Do not prompt user to choose
Key Regeneration	C Prompt user to choose
Dead Peer Detecti	
Customization	User has seconds to choose, or Default Post Login Selection below is take
i — IPsec Client	
	Default Post Login Selection
	C Go to Clientless SSL VPN portal
	Download SSL VPN Client

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.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.

-General	Renegotiation Interval:	🕅 Inherit	🔲 Unlimited	30	minutes
- Advanced	Renegotiation Method:	🔲 Inherit	🔿 None	⊙ SSL	🔿 New Tunnel
-Split Tunneling					
Eare clic su OK quindi su	,				

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

Co	nfiguration > Remote Access VPN	> Net	work (Client) Access >	Group Policies		
	Manage VPN group policies. A VPN grou externally on a RADIUS/LDAP server. T	p poli he gr	cy is a collection of user-c oup policy information is r	priented attribute/val eferenced by VPN tu	ue pairs that may be sto nnel groups and user acc	red inter counts.
	🛧 Add 👻 🗹 Edit 📋 Delete					
	Name		Туре	Tunneli	ng Protocol	
- (clientgroup)	Internal	svc		N/A -
	DfltGrpPolicy (System Default)		Internal	L2TP-IPSec, IPSec, w	ebvpn	N/A -

Configurazione CLI equivalente:

5. Per creare un nuovo account utente ssluser1, scegliere Configurazione > VPN ad accesso remoto > Impostazione AAA > Utenti locali > Aggiungi. Fare clic su OK e quindi su

Applica.	
🔄 Add User Account	
Identity ⊕-VPN Policy	Username: ssluser1
	Password: ******
	Confirm Password: ******
	User authenticated using MSCHAP
	Member-of
	Member-of: Add >> Delete
	Access Restriction
	Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
	Note: All users have network access, regardless of these settings.
	Full access(ASDM, SSH, Telnet and Console)
	Privilege level is used with command authorization.
	Privilege Level: 2
	CLI login prompt for SSH, Telnet and console (no ASDM access)
	This setting is effective only if AAA authenticate console command is configured.
	O No ASDM, SSH, Telnet or Console access
	This setting is effective only if AAA authenticate console command is configured.

Configurazione CLI equivalente:

 Scegliere Configurazione > VPN ad accesso remoto > Impostazione AAA > Gruppi di server AAA > Modifica per modificare il gruppo di server predefinito LOCAL selezionando la casella di controllo Abilita blocco utente locale con un valore massimo di tentativi pari a 16.

Configurat	ion > Remote	Access VPN > AA	A Setup > AAA Serve	r Groups	
AAA Serve	er Groups —				
Ser	ver Group	Protocol	Accounting Mode	Reactivation Mode	
LOCAL		LOCAL			
	Edit LOCA This feature before lockin when the loc Enable L Maximum	AL Server Group allows you to speci- ig out and denying al database is used ocal User Lockout Attempts: 16	fy the maximum number access to the user. This I for authentication.	of failed attempts to allow limit is applicable only Help	~
•		ОК	Cancel	Help	

- 7. Fare clic su OK, quindi su Applica.Configurazione CLI equivalente:
- 8. Configurare il gruppo di tunnel.Per creare un nuovo gruppo di tunnel, scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione VPN SSL > Aggiungi.Nella scheda Base è possibile eseguire l'elenco delle configurazioni come illustrato di seguito.Assegnare al gruppo di tunnel il nome sslgroup.In Assegnazione indirizzo client scegliere il pool di indirizzi vpnpool dall'elenco a discesa.In Criteri di gruppo predefiniti scegliere il gruppo client di Criteri di gruppo dall'elenco a discesa.

🚰 Add SSL ¥PN Connection	Profile		
<mark>(Basic)</mark> ⊛–Advanced	Name: Aliases:	ssigroup	
	Authentication		
	Method: AAA Server Group:	AAA C Certificate C Both	Manag
		Use LOCAL if Server Group fails	
	DHCP Servers:		
	Client Address Pools:	vpnpool	Select
	Group Policy:	clientgroup	Manag
	SSL VPN Client Protoco	Cancel Help	

Nella scheda SSL VPN > Alias connessione, specificare il nome alias del gruppo come sslgroup_users e fare clic su

Add 55L VPN Connection	Profile
Basic	Portal Page Customization: DfltCustomization
-Advanced	
General	CSD Alternate Group Policy: DfltGrpPolicy
-Client Addressing -Authentication	Enable the display of Radius Reject-Message on th
Authorization	Connection Aliases
SSL VPN	Add Delete
	🞼 Add Connection Alias
	Alias: sslgroup_users
	G OK Cancel Help
	🔂 Add 📝 Delete

clic su OK, quindi su Applica.Configurazione CLI equivalente:

9. Configurare NAT.Scegliere Configurazione > Firewall > Regole NAT > Aggiungi regola NAT dinamica in modo che il traffico proveniente dalla rete interna possa essere convertito con l'indirizzo IP esterno

72.16.1.5. 🚭 Add Dynamio	: NAT Rule	
Original	ide	
Source:	у	
Translated Select a global	pool for dynamic translation.	
Pool ID	Interface	Addresses Pool
0	(outbound)	Same as original address (identity)
-0	(inbound)	Same as original address (identity)
1	outside	🖳 172.16.1.5

clic su **OK**.Fare clic su **OK**.

Co	nfigura	tion > Firewall > NA	AT Rules				
4	🖡 Add	🝷 🗹 Edit ม De	lete 🛧 🗲 👗	🖻 💼 🗉 🔍	Find 🐏 Dia	gram 🛛 🥰 Packet Ti	race
Γ	#	Original					
	*	туре	Source	Destination	Service	Interface	
E	inside i	(1 Dynamic rules)					
	1	📊 Dynamic	🏈 any			outside	

Fare clic su Apply (Applica). Configurazione CLI equivalente:

10. Configurare l'esenzione nat per il traffico di ritorno dalla rete interna al client VPN. ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0 ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0 ciscoasa(config)#nat (inside) 0 access-list nonat

Configurazione ASA CLI

Cisco ASA 8.0(2) ciscoasa(config)#show running-config : Saved : ASA Version 8.0(2) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names Ţ interface Ethernet0/0 nameif inside security-level 100 ip address 10.77.241.142 255.255.255.192 ! interface Ethernet0/1 nameif outside security-level 0 ip address 172.16.1.1 255.255.255.0 ! interface Ethernet0/2 shutdown no nameif no security-level no ip address ! interface Ethernet0/3 shutdown no nameif no security-level no ip address 1 interface Management0/0 shutdown no nameif no security-level no ip address Ţ passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-k8.bin

ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid access-list split-tunnel standard permit 10.77.241.128 255.255.255.192 !--- ACL for Split Tunnel network list for encryption. access-list nonat permit ip 10.77.241.0 192.168.10.0 access-list nonat permit ip 192.168.10.0 10.77.241.0 !--- ACL to define the traffic to be exempted from NAT. pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0 !--- The address pool for the Cisco AnyConnect SSL VPN Clients no failover icmp unreachable rate-limit 1 burstsize 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 global (outside) 1 172.16.1.5 !--- The global address for Internet access used by VPN Clients. !--- Note: Uses an RFC 1918 range for lab setup. !--- Apply an address from your public range provided by your ISP. nat (inside) 0 access-list nonat !--- The traffic permitted in "nonat" ACL is exempted from NAT. nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 dynamic-access-policy-record DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list 1 class-map inspection_default match default-inspection-traffic 1 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 netbios

inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
webvpn
enable outside
<pre>! Enable WebVPN on the outside interface svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1</pre>
<pre>! Assign an order to the AnyConnect SSL VPN Client image svc enable</pre>
<pre>! Enable the security appliance to download SVC images to remote computers tunnel-group-list enable</pre>
! Enable the display of the tunnel-group list on the WebVPN Login page group-policy clientgroup internal
<pre>! Create an internal group policy "clientgroup" group-policy clientgroup attributes vpn-tunnel-protocol svc</pre>
<pre>! Specify SSL as a permitted VPN tunneling protocol split-tunnel-policy tunnelspecified</pre>
split-tunnel-network-list value split-tunnel
split-tunnel-network-list value split-tunnel
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the stort of the log security with the veloce to be </pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place from 1 to 10000 (1 week) are prime articled.</pre>
<pre>split-tunnel-network-list value split-tunnel ' Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ' When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ' Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted</pre>
<pre>split-tunnel-network-list value split-tunnel ' Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ' When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ' Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ' Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ' Create a user account "ssluser1" tunnel-group</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool ! Associate the address pool vpnpool created default- group-policy clientgroup</pre>
<pre>split-tunnel-network-list value split-tunnel ! Encrypt the traffic specified in the split tunnel ACL only webvpn svc keep-installer installed ! When the security appliance and the SVC perform a rekey, they renegotiate ! the crypto keys and initialization vectors, increasing the security of the connection. svc rekey time 30 ! Command that specifies the number of minutes from the start of the ! session until the rekey takes place, from 1 to 10080 (1 week). svc rekey method ssl ! Command that specifies that SSL renegotiation takes place during SVC rekey. svc ask none default svc username ssluser1 password ZRhW85jZqEaVd5P. encrypted ! Create a user account "ssluser1" tunnel-group sslgroup type remote-access ! Create a tunnel group "sslgroup" with type as remote access tunnel-group sslgroup general-attributes address-pool vpnpool ! Associate the address pool vpnpool created default- group-policy clientgroup</pre>

tunnel-group sslgroup webvpn-attributes



Stabilire la connessione VPN SSL con SVC

Per stabilire una connessione VPN SSL con ASA, completare la procedura seguente:

1. Immettere l'URL o l'indirizzo IP dell'interfaccia WebVPN dell'ASA nel browser Web nel formato mostrato.

https://url
0
https:// <ip address="" asa="" interface="" of="" the="" webvpn=""></ip>
File Edit View Favorites Tools Help
🌀 Back 🔹 🕥 - 📓 📓 🏠 🔎 Search 🤺 Favorites 🤣 🍙 - 🌺 🚍 🦓
Address an https://172.16.1.1/+webvpn+/index.html
utilities WebVPN Service
Login
Please enter your username and password.
USERNAME:
PASSWORD:
GROUP: sslgroup_users
Login Clear

2. Immettere il nome utente e la password. Inoltre, scegliere il proprio gruppo dall'elenco a discesa come



finestra viene visualizzata prima della connessione VPN



ota: il software ActiveX deve essere installato sul computer prima di scaricare SVC.Questa finestra viene visualizzata una volta stabilita la connessione.



3. Fare clic sul blocco visualizzato nella barra delle applicazioni del

Eisco AnyCo	nnect VPN Client		
K Connection	🚯 Statistics 릚 About		
	cisco		
Connect to:	172.16.1.1	~	
	Disconnect		

questa finestra che fornisce informazioni sulla connessione SSL. Ad esempio, **192.168.10.1** è l'indirizzo IP assegnato dall'ASA,

Cisco AnyConnect VPN C	lient 📃 🗖 🛽	
🗞 Connection 🕕 Statistics)	🙈 About	
cisc	0	
Tunnel State:	Connected	
Client Address: Server Address:	192.168.10.1 172.16.1.1	
Bytes Sent:	23461	
Bytes Received:	1111	
Time Connected:	00:04:51	
Details		
]
I session established.		In questa finestra v

visualizzate le informazioni sulla versione del client VPN Cisco



AnyConnect. WPN session established

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**.

• **show webvpn svc**: visualizza le immagini SVC memorizzate nella memoria flash ASA. ciscoasa#show webvpn svc

```
1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1
CISCO STC win2k+
2,0,0343
Mon 04/23/2007 4:16:34.63
```

- 1 SSL VPN Client(s) installed
- **show vpn-sessiondb svc**: visualizza le informazioni sulle connessioni SSL correnti. ciscoasa#**show vpn-sessiondb svc**

Session Type: SVC

```
Username : ssluser1
```

Assigned IP	:	192.168.10.1	Public IP	:	192.168.1.1
Protocol	:	Clientless SSL-Tunnel	DTLS-Tunnel		
Encryption	:	RC4 AES128	Hashing	:	SHA1
Bytes Tx	:	194118	Bytes Rx	:	197448
Group Policy	:	clientgroup	Tunnel Group	:	sslgroup
Login Time	:	17:12:23 IST Mon Mar 2	4 2008		
Duration	:	0h:12m:00s			
NAC Result	:	Unknown			
VLAN Mapping	:	N/A	VLAN	:	none
show webvpn group-alias: visualizza l'alias configurato per vari gruppi.					

ciscoasa#**show webvpn group-alias**

Tunnel Group: sslgroup Group Alias: sslgroup_users enabled

 In ASDM, scegliere Monitoraggio > VPN > Statistiche VPN > Sessioni per conoscere le sessioni WebVPN correnti nell'appliance

SA.								
lonitoring > VP	'N > VPN S	tatistic	s > Sessions)				
Sessions								
Remote	Site to	cito	SSL VPN			E-mail Drawy	UDM Load Palancia	_
Access	Site-to-	Sice	Clientless	With Client	Total	E-mail Proxy	VFN Load balancing	
0	0		0	0	0	0	0	
Filter By: SSL	VPN Client		All Sessions	- •		Fi	ter	
Username IP Address		0	Group Policy Connection	Proto Encryp	Protocol Encryption		Login Time Duration	
ssluser1 clienti 192.168.10.1 sslgro		clientg sslgrou	oup Clientless SSL-Tunnel DT p RC4 AES128		Tunnel DT	. 17:12:23 IST Mon Mar 24 2008 0h:03m:31s		194118 192474

Risoluzione dei problemi

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

1. vpn-sessiondb logoff name <nomeutente> —Comando per chiudere la sessione VPN SSL per il nome utente specifico.

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Do you want to logoff the VPN session(s)? [confirm] Y
INFO: Number of sessions with name "ssluser1" logged off : 1
ciscoasa#Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xB000)
```

Analogamente, è possibile utilizzare il comando **vpn-sessiondb logoff svc** per terminare tutte le sessioni SVC.

2. Nota: se il PC passa alla modalità standby o sospensione, la connessione VPN SSL può essere interrotta.

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e
tc)
Called vpn_remove_uauth: success!
```

webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xA000)

ciscoasa#**show vpn-sessiondb svc** INFO: There are presently no active sessions

3. debug webvpn svc <1-255> : fornisce gli eventi webvpn in tempo reale per stabilire la

sessione.

Ciscoasa#**debug webvpn svc 7**

```
webvpn_rx_data_tunnel_connect
CSTP state = HEADER PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B
7D75F4EDEF26'
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8
625B92C1338D631B08B7D75F4EDEF26'
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B
08B7D75F4EDEF26'
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7
5F4EDEF26'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
... input: 'X-CSTP-Accept-Encoding: deflate;g=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
... input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40
642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 '
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 '
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
-SHA:DES-CBC-SHA'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
```

No subnetmask must calculate it						
SVC: NP setup						
np_svc_create_session(0x3000, 0xD41611E8, TRUE)						
webvpn_svc_np_setup						
SVC ACL Name: NULL						
SVC ACL ID: -1						
SVC ACL ID: -1						
<pre>vpn_put_uauth success!</pre>						
SVC IPv6 ACL Name: NULL						
SVC IPv6 ACL ID: -1						
SVC: adding to sessmgmt						
SVC: Sending response						
Unable to initiate NAC, NAC might not be enabled or invalid policy						
CSTP state = CONNECTED						
webvpn_rx_data_cstp						
webvpn_rx_data_cstp: got internal message						
Unable to initiate NAC, NAC might not be enabled or invalid policy						

reale.

4. In ASDM, scegliere Monitoraggio > Log > Visualizzatore log in tempo reale > Visualizza per visualizzare gli eventi in tempo

🚰 Cisco ASDM 6.0 for ASA - 10.77.241.142								
File	<u>View T</u> ools Wi <u>z</u> ards <u>Wi</u> ndow <u>H</u> e	þ	Look For:					
Ċ	🚳 Home 🦓 Configuration 🔯 Monitoring 🔚 Save 💽 Refresh 🔇 Back 🕥 Forward 🦻 Help							
	Logging 라무×	Monitoring > Logging > Real-Time Log Viewer						
ce List	Real-Time Log Viewer	Real-Time Log Viewer						
Devi								
		Click the View button below to start displaying syslog messages in rea	al time. Select the					
		uestreu logging tever to see messages at that sevency of higher.						
		Logging Level: Debugging						
		Buffer Limit: 1000						
		View						

Nell'esempio viene mostrato come stabilire una sessione SSL con il dispositivo headend.

🙀 Real-Time Log Viewer - 10.77.241.142							
Ele Tools Window Help							
💷 Pause 🖹 Copy 🎧 Save 🌆 Clear 📅 Color Settings 🏠 Create Rule 式 Show Rule 🕲 Show Details 🤗 Help							
Fiker By: 💽 🐺 Fiker 📳 Show All Find:							
Severity	Date	Time	Syslog ID	Source IP	Destination IP		
<u>4</u> 6	Mar 21 2008	20:03:36	725007	10.77.233.74		SSL session with dient inside:10.77.233.74/1026 terminated.	
<u>4</u> 6	Mar 21 2008	20:03:35	106015	10.77.233.74	10.77.241.142	Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44	
<u>4</u> 6	Mar 21 2008	20:03:35	302014	10.77.233.74	10.77.241.142	Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identii	
<u>4</u> 6	Mar 21 2008	20:03:35	605005	0.0.0.0	0.0.0.0	Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enable	
A 6	Mar 21 2008	20:03:35	725002	10.77.233.74		Device completed SSL handshake with client inside:10.77.233.74/1026	
<u>4</u> 6	Mar 21 2008	20:03:35	725003	10.77.233.74		SSL client inside:10.77.233.74/1026 request to resume previous session.	
A 6	Mar 21 2008	20:03:35	725001	10.77.233.74		Starting SSL handshake with client inside: 10.77.233.74/1026 for TLSv1 se	
<u>4</u> 6	Mar 21 2008	20:03:35	302013	10.77.233.74	10.77.241.142	Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23	
■ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1							
%ASA-6-725002 Device completed SSL handshake with remote_device interface_name:IP_address/port The SSL handshake has completed successfully with the remote device.							

Informazioni correlate

- <u>Cisco serie 5500 Adaptive Security Appliance Pagina di supporto</u>
- Note sulla versione per AnyConnect VPN Client, versione 2.0
- ASA/PIX: Esempio di configurazione dell'appliance ASA che consente il tunneling ripartito per i client VPN
- Il router consente ai client VPN di connettersi a IPsec e a Internet utilizzando un esempio di configurazione del tunneling ripartito
- Esempio di configurazione di PIX/ASA 7.x e VPN Client per VPN Internet pubblica su Memory <u>Stick</u>
- Esempio di configurazione di SSL VPN Client (SVC) su ASA con ASDM
- Documentazione e supporto tecnico Cisco Systems