ASA 7.1/7.2: Esempio di configurazione dell'appliance ASA che consente il tunneling ripartito per SVC

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Configurazione Esempio di rete Configurazioni ASA con ASDM 5.2(2) Configurazione di ASA 7.2(2) con CLI Stabilire la connessione VPN SSL con SVC Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene spiegato dettagliatamente come consentire ai client VPN (SVC) Secure Socket Layer (SSL) di accedere a Internet mentre sono tunneling in una appliance Cisco Adaptive Security (ASA). Questa configurazione consente a SVC di accedere in modo sicuro alle risorse aziendali tramite SSL e fornisce accesso non protetto a Internet tramite l'utilizzo del tunneling ripartito.

La capacità di trasmettere il traffico protetto e non protetto sulla stessa interfaccia è nota come tunneling suddiviso. Il tunneling ripartito richiede che si specifichi esattamente quale traffico è protetto e quale sia la destinazione di tale traffico, in modo che solo il traffico specificato entri nel tunnel, mentre il resto viene trasmesso in modo non crittografato attraverso la rete pubblica (Internet).

Prerequisiti

Requisiti

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

- Privilegi amministrativi locali su tutte le workstation remote
- Controlli Java e ActiveX sulla workstation remota
- La porta 443 (SSL) non è bloccata in alcun punto del percorso di connessione

Componenti usati

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

- Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 7.2(2)
- Cisco SSL VPN Client versione per Windows 1.1.4.179Nota: scaricare il pacchetto SSL VPN Client (sslclient-win*.pkg) da <u>Cisco Software Download</u> (solo utenti <u>registrati</u>). Copiare lo SVC sulla memoria flash dell'ASA, che deve essere scaricata sui computer degli utenti remoti per stabilire la connessione VPN SSL con ASA. Per ulteriori informazioni, consultare la sezione <u>Installazione del software SVC</u> nella guida alla configurazione dell'ASA.
- PC con Windows 2000 Professional SP4 o Windows XP SP2
- Cisco Adaptive Security Device Manager (ASDM) versione 5.2(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

SSL VPN Client (SVC) è una tecnologia di tunneling VPN che offre agli utenti remoti i vantaggi di un client VPN IPsec senza la necessità per gli amministratori di rete di installare e configurare client VPN IPsec in computer remoti. SVC utilizza la crittografia SSL già presente nel computer remoto, nonché l'accesso e l'autenticazione WebVPN dell'appliance di sicurezza.

Per stabilire una sessione SVC, l'utente remoto immette nel browser l'indirizzo IP di un'interfaccia WebVPN dell'accessorio di protezione e il browser si connette a tale interfaccia e visualizza la schermata di accesso di WebVPN. Se il login e l'autenticazione sono soddisfacenti e l'appliance di sicurezza identifica l'utente come dispositivo che richiede l'SVC, l'appliance di sicurezza scarica l'SVC sul computer remoto. Se l'accessorio di protezione consente di utilizzare l'SVC, l'accessorio di protezione scaricherà l'SVC sul computer remoto mentre nella finestra viene visualizzato un collegamento che consente di ignorare l'installazione dell'SVC.

Una volta scaricato, l'SVC viene installato e configurato automaticamente e quindi rimane o si disinstalla automaticamente dal computer remoto, a seconda della configurazione, al termine della connessione.

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> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

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.

Configurazioni ASA con ASDM 5.2(2)

Completare questa procedura per configurare la VPN SSL sull'appliance ASA con tunneling ripartito come mostrato:

- Nel 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</u> per ASDM.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 abilitati sulla stessa interfaccia dell'ASA</u>.
- 2. Per creare un pool di indirizzi IP, scegliere **Configurazione > VPN > Gestione indirizzi IP > Pool** di indirizzi IP: **vpnpool** per client

Name:	vpnpool	-
Starting IP Address:	192.168.10.1	_
Ending IP Address:	192.168.10.254	
Subnet Mask:	255.255.255.0	•

Fare clic su **Apply** (Applica).

3. Abilita WebVPNScegliere Configurazione > VPN > WebVPN > Accesso WebVPN ed evidenziare l'interfaccia esterna con il mouse e fare clic su Abilita. Selezionare la casella di controllo Abilita elenco a discesa gruppi tunnel nella pagina di accesso WebVPN per abilitare la visualizzazione dell'elenco a discesa nella pagina di accesso per gli utenti, per scegliere i rispettivi

gruppi.

gruppi.		
Configuration > VPN > WebVPN	N > WebVPN Access	
VPN Wizard	-WebVPN Access	
🕀 🚰 General		
⊕–¶N KE	Configure access parameters for WebVPN.	
🕀 🃲 IPSec		
🖯 🎭 IP Address Management		
- Assignment		
- IP Pools	Interface Mahu/DN Enshied	Enchio
	Interface Veb VPN Linkber	Lensone
È-L K MebYPN	Inside No	
WebVPN Access	100.000 Yes	Disable
Proxies		
APCF		
Auto Signon		
Cache		
Content Rewrite		
Java Trustpoint	Dort Newbor	
Proxy Bypass	Por Mander.	
Ded Economics	Dataut Inia Timeout	
Port Forwarding		
ACL o	May Second Int: 2	
Encoding		
- SSL VPN Client	Web//PN Memory Size: 50 % of total physical memory	
SSO Servers	Preserve and physical memory	
E-mail Proxy	Enable Tunnel Group Drop-down List on WebVPN Login Page	
1		
	Apply Reset	
and a second		

Fare clic su **Apply** (Applica).Scegliere **Configurazione > VPN > WebVPN > SSL VPN Client > Aggiungi** per aggiungere l'immagine del client VPN SSL dalla memoria flash dell'ASA, come mostrato.

		Drowseria	sh.
		Upload	
ок	Cancel	Help	
owse Flash Dialog			
Folders	Files		
E- eisk0:	FileName 🔺	Size (bytes)	[
	asdm-603.bin	6,851,212	4
⊕-⊡ log ⊕-⊡ crypto_archive	asdm-603.bin asa803-k8.bin	6,851,212 14,635,008	
⊕-⊡ log ⊕-⊡ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg	6,851,212 14,635,008 1,220	
⊕-⊡ log ⊕-⊡ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0	6,851,212 14,635,008 1,220 2,635,734	
⊕⊡ log ⊕⊡ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin	6,851,212 14,635,008 1,220 2,635,734 6,889,764	
⊕-⊡ log ⊕-⊡ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin	6,851,212 14,635,008 1,220 2,635,734 6,889,764 8,312,832	
⊕-⊡ log ⊕-⊡ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin asdm-522.bin	6,851,212 14,635,008 1,220 2,635,734 6,889,764 8,312,832 5,623,108	
⊕-⊡ log ⊕-⊡ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin asadm-522.bin asa802-k8.bin	6,851,212 14,635,008 1,220 2,635,734 6,889,764 8,312,832 5,623,108 14,524,416	
⊕-⊡ log ⊕-⊡ crypto_archive	asdm-603.bin asa803-k8.bin admin.cfg anyconnect-win-2.0.0 asdm-602.bin asa722-k8.bin asa802-k8.bin old_running.cfg	6,851,212 14,635,008 1,220 2,635,734 6,889,764 8,312,832 5,623,108 14,524,416 1,841	

Fare clic su

Flash SVC Image:	disk0:/sslcl	ient-win-1.1.4.179.pk		Browse Fla
			[Upload.
	ок	Cancel	Hel	p

clic su OK.Selezionare la casella di controllo SSL VPN Client

Configuration > VPN > WebVP1	N > SSL VPN Client	
VPN Wizard General KE VPN Wizard General NAC VebVPN VebVPN VebVPN	-SSL VPN Client Configure SSL VPN Client parameters. ✓ Enable SSL VPN Client SSL VPN Client Images disk0:/sslclient-win-1.1.4.179.pkg	

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

4. Configura Criteri di gruppoPer creare un gruppo client di Criteri di gruppo interno, scegliere Configurazione > VPN > Generale > Criteri di gruppo > Aggiungi (Criteri di gruppo interni). In Generale, scegliere la casella di controllo WebVPN per abilitare WebVPN come protocollo di tunneling.

🚰 Add Internal Group Policy	and the second s	
Name: Clientgroup		
General IPSec Client Confi	guration Client Fir	ewall Hardware Client NAC WebVPN
Check an Inherit checkbox	to let the correspo	nding setting take its value from the default group policy.
Tunneling Protocols:	🗖 Inherit	IPSec WebVPN L2TP over IPSec
Filter:	🔽 Inherit	Manage

Nella scheda **Configurazione client >Parametri generali del client**, deselezionare la casella **Eredita** per Criterio tunnel diviso e scegliere **Elenco reti tunnel sotto** dall'elenco a discesa.Deselezionare la casella **Inherit** (Eredita) per **Split Tunnel Network List** (Elenco reti tunnel suddiviso) e fare clic su **Manage** (Gestisci) per avviare ACL

Manager.		
🚰 Edit Internal Group Policy: clientgroup		
Name: clientgroup		
General IPSec Client Configuration Client Firew	all Hardware Client	NAC VVebVPN
Check an Inherit checkbox to let the correspondin	g setting take its valu	e from the default group policy.
General Client Parameters Cisco Client Paramete	ers Microsoft Client I	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🗖 Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗆 Inherit	None Manage
⊢Address pools		
⊡ Inherit		
Available Pools		Assigned Pools (up to 6 entries)
	í sa l	
	Addee	
	< <remove< td=""><td></td></remove<>	
8		
ок	Cancel	Help

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

accessi.

CL Manager	d ACL		
🗣 Add 👻 📷 Edit 👩	🕽 Delete 🔶 🛧 🖣	• ۵ m m -	
🔂 Add ACL	dress	Action	Description
🔂 Add ACE			
🔹 insert 🐝 insert After			

Specificare un nome per l'ACL e fare clic su

ription

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** (Autorizza).Per uscire da Gestione ACL, fare clic su **OK**.

No	Address	Action	Description	
split-tunnel				
Add ACE				
Action				
Action:	✓ Permit ▼			
Host/Netv	vork			
IP Addr	ess: 10.77.241.128			*
Netmas	k: 255.255.255.192			•
Description	Ç.			

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

撞 Edit Internal Group Policy: clientgroup		
Name: clientgroup	. ((mark former and
General IPSec	ll Hardware Client	NAC WebVPN
Check an Inherit checkbox to let the corresponding	setting take its value	e from the default group policy.
General Client Parameters Cisco Client Paramete	rs Microsoft Client I	Parameters
Banner:	🔽 Inherit	Edit Banner
Default Domain:	🔽 Inherit	
Split Tunnel DNS Names (space delimited):	🔽 Inherit	
Split Tunnel Policy:	🔲 Inherit	Tunnel Network List Below
Split Tunnel Network List:	🗆 Inherit	split-tunnel Manage
⊢ Address pools		
Available Pools	Add>> < <remove< th=""><th>Assigned Pools (up to 6 entries)</th></remove<>	Assigned Pools (up to 6 entries)
ок	Cancel	Help

Nella pagina principale, fare clic su **Apply**, quindi su **Send** (se necessario) per inviare i comandi all'appliance ASA.Per l'opzione Usa client VPN SSL, deselezionare la casella di controllo **Eredita** e fare clic sul pulsante di opzione **Facoltativo**.Questa opzione consente al client remoto di scegliere se fare clic sulla scheda **WebVPN > SSL Client** e di scegliere le opzioni seguenti:Non scaricare SVC. L'opzione Always (Sempre) garantisce che l'SVC venga scaricato sulla workstation remota durante ogni connessione VPN SSL.Per l'opzione Mantieni programma di installazione sul sistema client, deselezionare la casella di controllo **Eredita** e fare clic sul pulsante di opzione **Sì**.Questa azione consente al software SVC di rimanere sul computer client; di conseguenza, non è necessario che l'ASA scarichi il software SVC sul client ogni volta che viene stabilita una connessione. Questa opzione è ideale per gli utenti remoti che spesso accedono alla rete aziendale.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 quando si impostano i limiti 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.Gli attributi del client VPN SSL devono essere configurati come mostrato in questa immagine:

Name: C	lientgroup				
eneral IPSec	Client Configuration C	lient Firewall Hard	ware Client NAC (NebVPN	
Configure Web	∨PN attributes using the f	ollowing tabs .			
Check an Inheri	it checkbox to let the corr	esponding setting ta	ake its value from the	default group polic	у.
Functions C	ontent Filtering Homepa	ge Port Forwardin	g Other SSL VPN	Client Auto Signo	n
Use SSL V	PN Client:	🗌 Inherit	C Always	• Optional	C Never
Keep Instal	ler on Client System:	🔲 Inherit	(Yes	C No	
Compressi	on:	🔽 Inherit	C Enable	$oldsymbol{C}$ Disable	
Keepalive 1	Messages:	🔽 Inherit	F Enable	Interval:	seco
Key Reneg	otiation Settings				
Renego	tiation Interval:	🗖 Inherit	🗌 Unlimited	30	minutes
Renego	tiation Method:	🔲 inherit	None	• 55L	C New tun
Dead Peer	Detection				
Gatewa	ay Side Detection:	🔽 Inherit	Enable	Interval:	seco
Client S	ide Detection:	🔽 Inherit	🗖 Enable	Interval:	seco

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



Configurazione CLI equivalente:

5. Per creare un nuovo account utente **ssluser1**, scegliere **Configurazione > VPN > Generale > Utenti > Aggiungi**. Fare clic su **OK** e quindi su

Username:	ssluser1	
Password:	*****	
Confirm Password:	*******	
🔲 User authentio	cated using MSCHAP	
Privilege level is used v	with command authorization.	
Privilege Level:	2	•

onfigurazione CLI equivalente:

 Scegliere Configurazione > Proprietà > Impostazione AAA > Gruppi di server AAA > Modifica per modificare il gruppo di server predefinito LOCAL e selezionare la casella di controllo Abilita blocco utente locale con un valore di tentativi massimo pari a 16.

Configuration > Properties > A	AA Setup > AAA Server Gro	ups			
Startup Wizard	AAA Server Groups	-			
🖯 🚽 AAA Setup	1				
AAA Server Groups	AAA server groups				
- Auth. Prompt	Samuel Comm	Destand	A new setting Marcle	Beautivelian Maria	
LDAP Attribute Map	Server Group	Protocol	Accounting Mode	Reactivation Mode	Add
Anti-Spoofing	LOCAL	LOCAL			Edit
E - B ARP	🗯 Edit LOCAL Server Gro	oup			×
- 🛃 Auto Update	Sector and the sector of the s				Delete
Gient Update	This facture allows to	onacity the maxim	um number of folloci offen	unto to ollow hotoro	-
Certificate	locking out a user and	I denu access to th	a user. This limit is anning	able only when local	
E Provice Access	database is used for	authentication.	e aser. The line is appro-	able only whethera	
AAA Access					
HTTPS/ASDM	Extended and the	d online t			
Secure Shell	Enduie Local Use	LOCKOUL:			-
Teinet			A		Add
Virtual Access	Maximum Attempt	s: (16)			-
Device Administration					Ealt
The purch services					Delete
Hab Availability and Sad					Deele
Fellower			12		Move I.
Exerment	OF	Ó Í Í	Cancel H	elp	
					Move Dry

Configurazione CLI equivalente:

7. Configura gruppo di tunnelScegliere Configurazione > VPN > Generale > Gruppo di tunnel > Aggiungi (accesso WebVPN) per creare un nuovo gruppo di tunnel.Nella scheda Generale > Generale scegliere Criteri di gruppo come gruppo client dall'elenco a discesa.

🚰 Add Tunnel (iroup	ana ana ang ang ang ang ang ang ang ang		_		
Name:	sslgroup)	-	туре:	vebvpn	
General V	VebVPN					
Configure	e general acc	ess attributes fro	om the followir	ng sub-ta	bs.	
Basic A	uthentication	Authorization	Accounting	Client Ac	ldress Assignme	nt Advanced
Group	Policy:	clientgroup	•]		
⊏ s	rip the realm	from username :	pefore passing	g it on to t	he AAA server	

In **Generale** > scheda **Assegnazione indirizzi client**, in Pool di indirizzi, fare clic su **Aggiungi** >> per assegnare il pool di indirizzi disponibile **vpnpool**.

rianic.	Jasigroup	k (rype. Jv	repupit	
General	WebVPN				
Configu	re general access attributes	s from the followir	ng sub-tai	os.	
Basic	Authentication Authorizati	on Accounting	Client Ac	ldress Assignment	Advanced
т	o specify whether to use D	HCP or address p	ools for a	address assignment	t, go to Configurati
2	IP Address Management >	Assignment.		-	
	DHCP Servers				
				14	
	IP Address:		Add >>		
	IP Address:		Add >> Delete		
	IP Address:		Add >> Delete		
	IP Address:		Add >> Delete		
	IP Address:		Add >> Delete		
	IP Address:	pecific address po	Add >> Delete	the Advanced tab.	
	IP Address: Address Pools To configure interface-sp Available Pools	pecific address po	Add >> Delete	the Advanced tab.	ools

Nella scheda **WebVPN > Alias gruppo e URL**, digitare il nome dell'alias nella casella del parametro e fare clic su **Aggiungi >>** per visualizzarlo nell'elenco dei nomi dei gruppi nella pagina di

accesso.

age	
	1
Alias	Statu
sslgroup_users	enable
0	slgroup_users

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

8. Configurazione NATScegliere Configurazione > NAT > Aggiungi > Aggiungi regola NAT

dinamica per il traffico proveniente dalla rete interna che può essere convertito con l'indirizzo

Real Address				
Interface:	inside			
IP Address:	0.0.0.0		•	· · · · ·
Netmask:	0.0.0.0			
Dynamic Tran	slation			
Interface:	outside			-
🔂 Add	🖌 Edit 👔 (Delete		
Select	Pool ID	Addro	esses Pool	
		172.16.1.5		
				1
NAT Options				
the second				

clic su OK, quindi su Applica nella pagina principale. Configurazione CLI equivalente:

9. 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 di ASA 7.2(2) con CLI

Cisco ASA 7.2(2)

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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
1
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
interface Ethernet0/3
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
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 mtu inside 1500 mtu outside 1500 ip local
pool vpnpool 192.168.10.1-192.168.10.254
!--- The address pool for the SSL VPN Clients no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.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
access-group 100 in interface outside
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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal
!--- Create an internal group policy "clientgroup".
group-policy clientgroup attributes
vpn-tunnel-protocol webvpn
!--- Enable webvpn as tunneling protocol. split-tunnel-
```

DOTICY LUIMETSDECTITED
anlit_tunnol_notwork_ligt walue anlit_tunnol
spiit-tunnei-network-fist value spiit-tunnei
<i>! Encrypt the traffic specified in the split tunnel</i>
ACL only. webvpn
svc required
510 10441104
! Activate the SVC under webvpn mode. svc keep-
installer installed
I then the convictor and the court of the court
! when the security appliance and the SVC perform a
rekey, ! they renegotiate the crypto keys and
initialization vectors, ! and increase the security
of the connection suc rekey time 30
<i>! Command that specifies the number of minutes !</i>
from the start of the session until the rekey takes
place, I from 1 to 10080 (1 week), svc rekey method
SSI
! Command that specifies that SSL renegotiation !
takes place during SVC rekey username ssluser1 password
eakes place during bye lekey. abelinane bblabeli pubbwela
ZRNW85jZqEavd5P. encrypted
! Create an user account "ssluser1". aaa local
authentication attempts max-fail 16
! Enable the AAA local authentication. http server
enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no compacerver contact compacerver enable trang
iocacion no simp-server concact simp-server enable craps
snmp authentication linkup linkdown coldstart tunnel-
group sslgroup type webvpn
I Croate a tunnel group "gglgroup" with tune ag
create a tunner group ssigroup with type as
WebVPN. tunnel-group sslgroup general-attributes
address-pool vpnpool
I Accoriate the address peel impreel created
: Associate the address poor vphpoor created.
default-group-policy clientgroup
default-group-policy clientgroup
default-group-policy clientgroup
default-group-policy clientgroup ! Associate the group policy "clientgroup" created.
default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes
default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable </pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection default match default-inspection-traffic ! !</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy map time inspect dng proget dng map parameters</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns map</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 rag inspect</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global policy global</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect 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</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect 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>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect 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>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect 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 ! Enable WebVPN op the outside interface. svc image</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect 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 ! Enable WebVPN on the outside interface. svc image disk0.(sslalient-vin-1 1 4 179 phz 1</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect 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 ! Enable WebVPN on the outside interface. svc image disk0:/sslclient-win-1.1.4.179.pkg 1</pre>
<pre>default-group-policy clientgroup ! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes group-alias sslgroup_users enable ! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect sip inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global webvpn enable outside ! Enable WebVPN on the outside interface. svc image disk0:/sslclient-win-1.1.4.179.pkg 1</pre>

-- Enable the security appliance to download !--- SVC



Stabilire la connessione VPN SSL con SVC

Completare questa procedura per stabilire una connessione VPN SSL con ASA.

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

nttps://uri
0
https:// <ip address="" asa="" interface="" of="" the="" webvpn=""></ip>
File Edit View Eavorites Tools Help
🔇 Back 🔹 🔘 🔄 🚺 🔎 Search 🦿 Favorites 🚱 🔗 🍓 🔜 🖓
Address Address https://172.16.1.1/+webvpn+/index.html
CISCO SYSTEMS
utility WebVPN Service
Webvr N Service
Login
Disass enter your yearname and password
Please enter your usemanie and password.
USERNAME:
PASSWORD:
GROUP: sslgroup_users
Login Clear

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



mostrato.

SSL

3. Prima di scaricare il software SVC, è necessario che nel computer sia installato il software



4. Queste finestre vengono visualizzate prima della connessione VPN

CISCO SYSTEMS SSLVPN CLIENT for WEBVPN
Please wait while the SSL VPN connection is established.

5. Èpossibile visualizzare queste finestre dopo aver stabilito la



connessione.

6. Fare clic sul tasto giallo visualizzato nella barra delle applicazioni del computer. Vengono visualizzate queste finestre che forniscono informazioni sulla connessione SSL. Ad esempio, 192.168.10.1 è l'indirizzo IP assegnato per l'indirizzo IP del client e del server è 172.16.1.1, il tunneling ripartito è abilitato e così

Statistics Route D	etails About		
Address Informa	tion	SSL Information	
Server:	172.16.1.1	Cipher:	3DES SHA-
Client:	192.168.10.1	Version:	TLSv1
Bytes		Transport Informat	ion
Sent:	2887	Local LAN:	Disable
Received:	940	Split Tunneling:	Enable
Frames		Connection Inform	ation
Sent:	35	Time:	00:00:2
Received:	12		

Inoltre, è

possibile controllare la rete protetta che deve essere crittografata con SSL. L'elenco delle reti viene scaricato dall'elenco degli accessi al tunnel separato configurato in ASA.Nell'esempio, il client VPN SSL protegge l'accesso a 10.77.241.128/24, mentre tutto il resto del traffico non viene crittografato e non inviato attraverso il

ð	Cisco Syste	ems SSL VPN Client	£	
	CISCO SYSTEMS	SLVPN CLIENT F	or WEBVPN	
	Statistics B	oute Details About		
	Local LAN	Routes	Secure Routes	
	Network	Subnet Mask	Network 10.77.241.128	Subnet Mask 255.255.255
unnel.		Close	Disconnect	
of Cisco	Systems SS	iL VPN Client		
Cisco Svstr	SSLV	PN CLIENT for WE	BVPN	
Statist	tics Route De	tails (About)		
Cisi 	CO SYSTEMS	SSL VPN CLIER for WEBVPN	NT Version	1.1.4.179
(.		Create a fully anywhere an SECURE REM	v secure conne ytime IOTE ACCESS.	ction
© Cop and th its affi	pyright 2004-200 he Cisco System iliates in the Unit	6 Cisco Systems, Inc. All s Logo are registered trac ed States and certain othe	rights reserved. Cisco, Cis lemarks of Cisco Systems, er countries.	co Systems Inc. and/or
		Close	Disconnect	

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:/sslclient-win-1.1.4.179.pkg 1
CISCO STC win2k+ 1.0.0
1,1,4,179
Fri 01/18/2008 15:19:49.43
```

- 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
```

```
: ssluser1
Username
Index
              : 1

      Assigned IP
      : 192.168.10.1
      Public IP
      : 192.168.1.1

      Protocol
      : SVC
      Encryption
      : 3DES

Hashing
              : SHA1
Bytes Tx : 131813
                                          Bytes Rx : 5082
Client Type : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy : clientgroup
Tunnel Group : sslgroup
Login Time : 12:38:47 UTC Mon Mar 17 2008
Duration : 0h:00m:53s
Filter Name :
```

- **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

VPN Connection Graphs	Sessions						
PSec Turnels	Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
Crypto Statistics	0 Filter By: VVeb	O VPN	1 Al Sessions	0	. 0	1 Fiter	12
NAC Session Summe Protocol Statistics	Usernam IP.Addres	e Gr IS Tu	oup Policy nnel Group	Protocol Encryption	n	Login Time Duration	Detail
Sessions	ssluser1	clientara	up	WebVPN	08 49 52	UTC Thu Mar 20	2 Loool

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 Called vpn_remove_uauIth: success! webvpn_svc_np_tear_down: no ACL NFO: Number of sessions with name "ssluser1" logged off : 1

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

 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, etc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
```

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

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

Ciscoasa#debug webvpn svc 7

```
ATTR_CISCO_AV_PAIR: got SVC ACL: -1
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 Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
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;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2 '
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
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
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED
```

4. In ASDM, scegliere Monitoraggio > Log > Visualizzatore log in tempo reale > Visualizza per visualizzare gli eventi in tempo reale. Nell'esempio vengono mostrate le informazioni sulla sessione tra SVC 192.168.10.1 e Webserver 10.2.2.2 in Internet tramite ASA

Lescription	abon P. I	Constructions (C)	Concernent 10	100
	THE PROPERTY OF TOWN	Descriation P	Source IP	
38 dst inside:192.168.10.255/138	No trainslation group found		192.168.10.255	
027. dst inside:10.77.244.193/53	Notranslation group found		10.77.244,193	
028 dst indide:10.77.244.193/53	No transistion group tound		10.77.244;193	
00 (172.16.1.5/1025) to outside:10.2.2.260 (10.2.2.260) (ssluser1)	Built inbound TCP connecti	10.2.2.2	192.168.10.1	
o outside:172.16.1.5/1025	5 Built dynamic TCP translati	172.16.1.5	192.168.10.1	
38 dist inside:192.168.10.255//38	No translation group Yound		192.168.10.255	_
027 dist-inside:10.77.244.190/53	No translation group found		10.77.244.193	
328 dst-inside:10.77.244.193/53	No transition group found		10:77.244.193	
027 det inside:10.77.244.193/53	No translation group found		10:77 244 193	
				9
	to see the emispation	ing entry to see	ase select a sus	Ple
	to see the explanation	and they to see	ase serece a sys	- DCI
328 dst inside:10.77.244.193/53 027 dst inside:10.77.244.193/53	No transistion group found No transistion group found to see the exclanation	log entry to see	10.77.244.193 10.77.244.193 ase select a sys	∎ Pie

Informazioni correlate

- Cisco serie 5500 Adaptive Security Appliance Supporto dei prodotti
- ASA/PIX: Esempio di configurazione dell'appliance ASA che consente il tunneling ripartito per <u>i client VPN</u>
- 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
 Stick
- Esempio di configurazione di SSL VPN Client (SVC) su ASA con ASDM
- Documentazione e supporto tecnico Cisco Systems