Configurazione del traffico di inversione del client VPN AnyConnect su ASA 9.X

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Premesse Configura inversione traffico di accesso remoto Esempio di configurazione di AnyConnect VPN Client per VPN Internet pubblica su Memory Stick Esempio di rete Configurazioni ASA release 9.1(2) con ASDM release 7.1(6) Configurazione di ASA release 9.1(2) nella CLI Consenti la comunicazione tra i client VPN AnyConnect con la configurazione TunnelAll in uso Esempio di rete Configurazioni ASA release 9.1(2) con ASDM release 7.1(6) Configurazione di ASA release 9.1(2) nella CLI Consenti la comunicazione tra client VPN AnyConnect con split-tunnel Esempio di rete Configurazioni ASA release 9.1(2) con ASDM release 7.1(6) Configurazione di ASA release 9.1(2) nella CLI Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritto come configurare una Cisco Adaptive Security Appliance (ASA) versione 9.X in modo da poter invertire il traffico VPN. Viene illustrato questo scenario di configurazione: Inversione del traffico proveniente dai client di accesso remoto.

Nota: Per evitare una sovrapposizione di indirizzi IP nella rete, assegnare un pool di indirizzi IP completamente diverso al client VPN (ad esempio, 10.x.x.x, 172.16.x.x e 192.168.x.x). Questo schema di indirizzi IP è utile per risolvere i problemi relativi alla rete.

Puntina o inversione a U

Questa funzionalità è utile per il traffico VPN che entra in un'interfaccia, ma che viene quindi instradato all'esterno della stessa interfaccia. Ad esempio, se si dispone di una rete VPN hub e spoke in cui l'appliance di sicurezza è l'hub e le reti VPN remote sono spoke, affinché uno spoke comunichi con un altro traffico spoke, è necessario andare all'appliance di sicurezza e quindi uscire di nuovo dall'altro spoke.

ciscoasa(config)#same-security-traffic permit intra-interface

Prerequisiti

Requisiti

Cisco consiglia di soddisfare i seguenti requisiti prima di provare la configurazione:

- Hub ASA Security Appliance deve eseguire la release 9.x.
- Cisco AnyConnect VPN Client 3.xNota: Scarica il pacchetto client VPN AnyConnect (anyconnectwin*.pkg) da Cisco Software Download (solo utenti registrati). Copiare il client VPN AnyConnect nella memoria flash Cisco ASA, da scaricare sui computer degli utenti remoti per stabilire la connessione VPN SSL con l'ASA. Per ulteriori informazioni, consultare la sezione <u>AnyConnect</u> <u>VPN Client Connections</u> della guida alla configurazione dell'ASA.

Componenti usati

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

- Cisco serie 5500 ASA con software versione 9.1(2)
- Cisco AnyConnect SSL VPN Client versione per Windows 3.1.05152
- PC con un sistema operativo supportato sulle piattaforme VPN supportate, serie Cisco ASA.
- Cisco Adaptive Security Device Manager (ASDM) versione 7.1(6)

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.

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 il reindirizzamento http:// richieste a https://, gli utenti devono immettere l'URL nel modulo https://

.Una volta immesso l'URL, il browser si connette a tale 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 necessario per 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 a TLS (Transport Layer Security) e utilizza anche 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>Guida dell'amministratore di</u> <u>Cisco AnyConnect Secure Mobility</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.**Nota:** Negli esempi riportati in questo documento viene utilizzato il protocollo IPv4. Per il traffico di inversione IPv6, i passaggi sono gli

stessi ma vengono utilizzati gli indirizzi IPv6 anziché IPv4. Configura inversione

traffico di accesso remotoIn 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 le guide di <u>riferimento</u> ai comandi.Esempio di configurazione di AnyConnect VPN Client per VPN Internet pubblica su Memory StickEsempio di reteNel documento viene usata questa impostazione di rete:



Configurazioni ASA release 9.1(2) con ASDM release 7.1(6)in questo documento si presume che la configurazione di base, ad esempio la configurazione dell'interfaccia, sia già stata completata e funzioni correttamente.Nota: Per configurare l'ASA con ASDM, consultare il documento sulla <u>configurazione dell'accesso alla gestione</u>.Nota: Nella versione 8.0(2) e successive, l'ASA supporta contemporaneamente sia le sessioni SSL VPN (WebVPN) senza client che le sessioni amministrative ASDM sulla porta 443 dell'interfaccia esterna. Nelle versioni precedenti alla release 8.0(2), 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 su uno stick nell'appliance ASA, completare la procedura seguente:

1. Scegli Configuration > Device Setup > Interfaces *e controllare la* Enable traffic between two or more hosts connected to the same interface *per consentire al traffico VPN SSL di entrare e uscire dalla stessa interfaccia. Clic* Apply.

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Туре	Add 🔫
SigabitEthemet0/0	outside	Enabled	0	172.16.1.1	255.255.255.0		Hardware	Edit
igabitEthernet0/1	inside	Enabled	100	10.77.241.142	255.255.255.192		Hardware	
igabitEthernet0/2		Disabled					Hardware	Delete
igabitEthernet0/3		Disabled					Hardware	
anagement0/0	mgmt	Disabled	0				Hardware/Ma	
<	m						Þ	
Enable traffic between	m n two or more inte	rfaces which a	are configure	d with same security	levels		5	

Configurazione CLI equivalente:

ciscoasa(config)#same-security-traffic permit intra-interface

2. Scegli Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add per creare un pool di indirizzi IP vpnpool.

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

3. Clic Apply. Configurazione CLI equivalente:

ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0

4. Abilita WebVPN. Scegli Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles *e inferiore* Access Interfaces, *Selezionare le caselle di controllo* Allow Access *e* Enable DTLS *per l'interfaccia esterna*. *Inoltre, controllare la* Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below *per abilitare la VPN SSL sull'interfaccia esterna*.

edministrative r options. East Interfaces	prance automaticary dep ights. The Gisco AnyCon	Noys the Cisco AnyCom nect VPN Client support	es selected in the table t	e users upon connection. The initia s well as SSL tunnel with Datagram	I dient deployment requires end-user Transport Layer Security (DTLS) tunneling
SL access mus	t be enabled if you allow	AnyConnect client to b	e launched from a brows	er (Web Launch) .	
SL access mus	SSL Access	AnyConnect client to b	IPsec (IKEv2) Acce	ser (Web Launch) . 1955	
SL access mus Interface	SSL Access Allow Access	Enable DTLS	e launched from a brows IPsec (IKEv2) Acco Allow Access	Enable Client Services	Device Certificate
SL access mus Interface outside	SSL Access Allow Access	Enable DTLS	e launched from a brows IPsec (IKEv2) Acco Allow Access	Enable Client Services	Device Certificate

Clic Apply.*Scegli* Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add per aggiungere l'immagine del client VPN Cisco AnyConnect dalla memoria flash dell'ASA, come mostrato.

Local File Path:	C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg	Browse Local Files
Flash File System Path:	disk0:/anyconnect-win-3.1.05152-k9.pkg	Browse Flash
🝯 Add AnyConne	ct Client Image	×
AnyConnect Image	: anyconnect-win-3.1.05152-k9.pkg	Browse Flash
AnyConnect Image	: anyconnect-win-3.1.05152-k9.pkg	Browse Flash

Configurazione CLI equivalente:

ciscoasa(config)#**webvpn**

ciscoasa(config-webvpn)#enable outside

ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable

5. Configurare Criteri di gruppo. Scegli Configuration > Remote Access VPN > Network (Client) Access > Group Policies per creare una politica di gruppo interna clientgroup. Sotto la General selezionare la scheda SSL VPN Client per abilitare WebVPN come protocollo del tunnel.

1	10.	. 1		9 11
Jarvara	Farm:	yatorb _		
Advance:	Advance: Barrer:	nher:		
	SCEP forwarding URL	inte-it		
	Activess Pools	nhe-t		Ereck
	3Pv6 Address Pools	mer:	1	Seet
	More Options			*
	Tunneling Protocols	📃 Sherik 🔄 Clenifess SS, WPV 📝 SS, WPA C and 📄 (Psec SIEV). 🔄 (Psec Si	EV2 🔲 L2754Fsec	

Nella Advanced > Split Tunneling, scegliere Tunnel All Networks dall'elenco a discesa Criterio del Criterio per creare tutti i pacchetti dal PC remoto attraverso un tunnel protetto.

anaral	The VEN plant makes split humaing decisions on the basis of a network list how can be specified below by providing the purper parameters for Thinly and Telefond List' Reids.	
desired	CMS Nances (V) Inform	
Browser Typey	Palay: Internet [Jurnel All Networks]	1.

Configurazione CLI equivalente:

ciscoasa(config)#group-policy clientgroup internal ciscoasa(config)#group-policyclientgroup attributes ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client ciscoasa(config-group-policy)#split-tunnel-policy tunnelall

6. Scegli Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add per creare un nuovo

account utente ssluser1. Clic OK e poi Apply.

VPN Policy	liseraras cdusri
Presswort Confirm Pose IF User aut Auros Road	Parmare management
	Confine Research (*******)
	F Oxy adjustated any VOCHY
	Rucco Residual Sectors of the options below to redshift XSIN, 531, Tablet and Console arrays.
	Patter Allesers have indexed success, reportless of these settings.
	Differences/STIN, 731, Telefand Conscie)
	Philese levels used with command extinction.
	Privilege Level: 2
	CLTogin prompt for 55H, Tehret and romsslevino AGDPI accessi
	This setting is effective only #"ase subtentication http://consule.LOCIA_"command is configured.
	C No ADDM, 3394, Telesto or Coreade accesso
	This satisfy is effective only 6" and authentication http: conside LOCA," and "and authentication exec" commands are configured.

Configurazione CLI equivalente:

ciscoasa(config)#username ssluser1 password asdmASA@

7. Configurare il gruppo di tunnel. Scegli Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add per creare un nuovo gruppo di tunnel ssigroup.Nella Basic è possibile eseguire l'elenco delle configurazioni come illustrato di seguito: Assegna al gruppo di tunnel il nome ssigroup.Sotto Client Address Assignment, scegliere il pool di indirizzi vpnpool dal Client Address Pools elenco a discesa.Sotto Default Group Policy, scegliere i Criteri di gruppo clientgroup dal Group Policy elenco a discesa.

Basic	Name:	ssigroup					
Advanced	Aliases:						
	Authentication	Authentication					
	Method:	💿 AAA 💿 Certificate 💿 Both					
	AAA Server Group:	LOCAL	▼ Manage				
		Use LOCAL if Server Group fails					
	Client Address Assignment						
	DHCP Servers:						
		None DHCP Link DHCP Subnet					
	Client Address Pools:	vpnpool	Select				
	Client IPv6 Address Pool	s:	Select				
		IPv6 address pool is only supported for SSL.					
	Default Group Policy						
	Group Policy:	clientgroup	← Manage				
	(Eollowing field is an attr	in the of the group policy selected above)					

Sotto la Advanced > Group Alias/Group URL, specificare il nome alias del gruppo come ssIgroup_users e fare clic su OK. Configurazione CLI equivalente:

ciscoasa (config) #tunnel-group sslgroup type remote-access ciscoasa (config) #tunnel-group sslgroup general-attributes ciscoasa (config-tunnel-general) #address-pool vpnpool ciscoasa (config-tunnel-general) #default-group-policy clientgroup ciscoasa (config-tunnel-general) #exit ciscoasa (config-tunnel-general) #exit ciscoasa (config) #tunnel-group sslgroup webvpn-attributes ciscoasa (config-tunnel-webvpn) #group-alias sslgroup_users enable

8. Configurazione NAT Scegli Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule quindi il traffico che proviene dalla rete interna può essere tradotto con l'indirizzo IP esterno 172.16.1.1.

File View Tools Wizards Wind	low Help								
Home 🗞 Configuration 🔯 Mo	nitaring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 He	de l							
Device List di 4 X	Configuration > Firewall > NAT Rules				D				
🗣 Add 📋 Delete 🚿 Connect	🙅 Add 🚽 🖉 Edit 👔 Delete 🖈 🗳 👗 📴 🏬 - 🔍 Find 🔛 Diagram 🥰 Padiet Trace								
Find: Go	Add NAT Rule Before "Network Object" NAT Rules		Action: Transla	ted Packet					
localhost:55000	Add "Network Object" NAT Rule	Service	Source	Destination	Service				
		Stany	Original (5)	Original	Original				
	👲 Insert	i any	Original (5)	Original	Original				
firewall ਰ P	🐺 Insert After	-							
Control of the second s									

lame:	obj-inside
Гуре:	Network 👻
P Address:	10.77.241.128
Vetmask:	255.255.255.192 👻
Description:	
NAT	۸
NAT Add Auto Type:	omatic Address Translation Rules
NAT Add Auto Type: Translated	omatic Address Translation Rules Dynamic Addr: outside

Scegli Configuration >

Firewall > NAT Rules > Add "Network Object" NAT Rule in modo che il traffico VPN che proviene dalla rete esterna possa essere convertito con l'indirizzo IP esterno 172.16.1.1.

Vame:	obj-AnyconnectPool	
Гуре:	Network	•
P Address:	192.168.10.0	
letmask:	255.255.255.0	-
Description:		
NAT		٨
NAT Add Auto Type:	omatic Address Translation Rules	*
NAT Add Auto Type: Translated	omatic Address Translation Rules Dynamic PAT (Hide) 👻 Addr: outside	*

equivalente:

```
ciscoasa(config)# object network obj-inside
ciscoasa(config-network-object)# subnet 10.77.241.128 255.255.255.192
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config)# object network obj-AnyconnectPool
ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)# nat (outside,outside) dynamic interface
```

Configurazione di ASA release 9.1(2) nella CLI

```
ciscoasa(config)#show running-config
```

```
: Saved
.
ASA Version 9.1(2)
1
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
1
interface GigabitEthernet0/1
nameif inside
```

security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address

!

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 same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool subnet 192.168.10.0 255.255.255.0 object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated when going to the Anyconnect Pool.

object network obj-AnyconnectPool nat (outside,outside) dynamic interface object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and Anyconnect Clients. !--- Note: Uses an RFC 1918 range for lab setup.

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 class-map inspection_default match default-inspection-traffic 1 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

!--- Enable WebVPN on the outside interface

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect enable

!--- Enable the security appliance to download SVC images to remote computers

tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients.

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

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#

Consenti la comunicazione tra i client VPN AnyConnect con la configurazione TunnelAll in usoEsempio di rete



Se è richiesta la comunicazione tra i client Anyconnect e è installato il NAT for Public Internet su Memory Stick; è inoltre necessario un NAT manuale per consentire la comunicazione bidirezionale.Si tratta di uno scenario comune quando i client Anyconnect utilizzano i servizi telefonici e devono essere in grado di comunicare tra loro.Configurazioni ASA release 9.1(2) con ASDM release 7.1(6)Scegli Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules pertanto, il traffico proveniente dalla rete esterna (pool Anyconnect) e destinato a un altro client Anyconnect dello stesso pool non viene convertito con l'indirizzo IP esterno 172.16.1.1.

File View Tools Wizards Winds	ow Help Starting Discuss On Patients Of Back Of Security 9 Hel	e î			
Device List D 9 ×	[Configuration > Firewall > NAT Rules]	r			0
Add 👔 Delete 🚿 Connect	🗣 Add 🔹 💽 Edit 🗻 Delete 🌩 🗲 👗 🖏 🌉 - 🔍 Find	📴 Disgram 🗠	Packet Trace		
	Add NAT Rule Before "Network Object" NAT Rules Action: Translated Packet				
localhost:55000	Add "Network Object" NAT Rule	Service	Source	Destination	Service
	Add NAT Rule After "Network Object" NAT Rules	any any	Original (5)	Original	Original
	👷 Insert	🏟 any	Original (S)	Original	Original
Firewall 🗗 A	🐺 Insert After	. 🏟 any	- Original (5)	- Original	- Original

Source Interface:	outside	Destination Interface:	outside	-
Source Address:	obj-AnyconnectPool (Destination Address:	obj-AnyconnectPool	[
		Service:	any	
Action: Translated	Packet			
Source NAT Type:	Static	•		
Source Address:	obj-AnyconnectPool (obj-AnyconnectPool	
Fall through to	interface PAT	Service:	Original	
Options				
📝 Enable rule				
Translate DNS	replies that match this rule			
)irection: Both				

Configurazione CLI equivalente:

```
nat (outside, outside) source static obj-AnyconnectPool obj-AnyconnectPool destination
static obj-AnyconnectPool obj-AnyconnectPool
Configurazione di ASA release 9.1(2) nella CLI
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
```

```
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
interface Management0/0
shutdown
no nameif
no security-level
```

no ip address

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 same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool subnet 192.168.10.0 255.255.255.0 object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

nat (inside,outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT statements used so that traffic from the inside network destined to the Anyconnect Pool and traffic from the Anyconnect Pool destined to another Client within the same pool does not get translated.

object network obj-AnyconnectPool nat (outside,outside) dynamic interface object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and Anyconnect Clients. !--- Note: Uses an RFC 1918 range for lab setup.

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
1
service-policy global_policy global
webvpn
enable outside
```

```
!--- Enable WebVPN on the outside interface
```

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect enable

!--- Enable the security appliance to download SVC images to remote computers

tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page

```
group-policy clientgroup internal
```

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients. 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

!--- Associate the group policy "clientgroup" created

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users

prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
Conceptible communications trachient\/DA

Consenti la comunicazione tra client VPN AnyConnect con split-tunnelEsempio di rete



Se è richiesta la comunicazione tra i client Anyconnect e viene usato lo split-tunnel; non è richiesto alcun NAT manuale per consentire la comunicazione bidirezionale a meno che non ci sia una regola NAT che influisce sul traffico configurato. Tuttavia, il pool VPN Anyconnect deve essere incluso nell'ACL dello split tunnel.Si tratta di uno scenario comune quando i client Anyconnect utilizzano i servizi telefonici e devono essere in grado di comunicare tra loro.Configurazioni ASA release 9.1(2) con ASDM release 7.1(6)

1. Scegli Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add per creare un pool di indirizzi IP vpnpool.

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

- 2. Clic Apply. Configurazione CLI equivalente:
- ciscoasa (config) #ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0 3. Abilita WebVPN. Scegli Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles e inferiore Access Interfaces, Selezionare le caselle di controllo Allow Access e Enable DTLS per l'interfaccia esterna. Inoltre, controllare la Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below per abilitare la VPN SSL sull'interfaccia esterna.

The security ap administrative r options. cess Interfaces Denable Osc SSL access mus	plance automatically dep ights. The Cisco AnyCon : o AnyConnect VPN Client t be enabled if you allow	loys the Cisco AnyCon nect VPN Client support access on the interfac	es selected in the table t e launched from a brows	e users upon connection. The initial s well as SSL tunnel with Datagram selow ser (Web Launch) .	dient deployment requires end-user Transport Layer Security (DTLS) tunneling
	SSL Access		IPsec (IKEv2) Acco	955	
Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate
Interface outside	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Port Settings

Clic Apply.*Scegli* Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add per aggiungere l'immagine del client VPN Cisco AnyConnect dalla memoria flash dell'ASA, come mostrato.

Upload a file from local (computer to flash file system on the device. The upload process mig	ght take a few minutes.
Local File Path:	C:\Users\iosemed\Desktop\anvconnect-win-3.1.05152-k9.pkg	Browse Local Files
Flash File System Path:	disk0:/anyconnect-win-3.1.05152-k9.pkg	Browse Flash

AnyConnect Image:	anyconnect-win	-3.1.05152-k9.pk	Browse Flash
			Upload
Regular express	ion to match u	ser-agent	*

Configurazione CLI equivalente:

ciscoasa(config)#webvpn ciscoasa(config-webvpn)#enable outside ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1 ciscoasa(config-webvpn)#tunnel-group-list enable ciscoasa(config-webvpn)#anyconnect enable

4. Configurare Criteri di gruppo. Scegli Configuration > Remote Access VPN > Network (Client) Access > Group Policies per creare una politica di gruppo interna clientgroup. Sotto la General selezionare la scheda SSL VPN Client per abilitare WebVPN come protocollo tunnel consentito.

THE	Lore:	ntgroup		
Advanced	Barrer:	Drheit		
	SCEP forwarding URL)	Pres:		
	Address Pools	liter:	Et	ert.
	3PV6 Address Pools	Inst	- Se	25

Nella Advanced > Split Tunneling, scegliere Tunnel Network List Below dall'elenco a discesa Criterio per creare tutti i pacchetti dal PC remoto attraverso un tunnel sicuro.

e e	McCharace III Intent		1
Broweser Provy	Foloyi Elitterit Tunna hasaara	. Let Defon	1
>*-yConnect Client Disco(DEvt.) Client	Network Liste 🗐 Inner 🛛 SPUD-Ara		Hanage
	Pressing this batter to set up split of Law	🖬 ADI Manager	.22
	Set up Split Curlie on the Web Security	Standard Acc. Textended et al	
	Intercept DHCP Configuration Mes	♥ Add = 2 tok 1 toktu + 4 S % 2 1 1	
		No Address Action Description	
		[] [] [] [] [] [] [] [] [] []	
		2 4 57.107.10.024 VI.tonk	

Configurazione CLI equivalente:

ciscoasa(config)#access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0 ciscoasa(config)#access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

ciscoasa(config)#group-policy clientgroup internal ciscoasa(config)#group-policy clientgroup attributes ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified ciscoasa(config-group-policy)#split-tunnel-network-list SPLIt-ACL

5. Scegli Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add per creare un nuovo

account utente ssluser1. Clic OK e poi Apply.

Identity						
VPN Policy	Bearrance eckeet					
	Pressuret					
	Confine Posseed.					
	IF User automitated using PSUHP					
	Augo Rotellen					
	Select one of the optimor below to reduct ACIN, 721, Teinet and Conselectnees.					
	Note: Alloses have not a see of these actings.					
	In Dialecters/STIN, SSI, Telbel and Console)					
	Rivilage level is used with command extractation.					
	Pridage Lavel: 2 👻					
	O Libridin prompt for SSH, Telnet and console (no ASDM access)					
	This setting is effective only it "are authentication http:console.LOCAL" command is configured.					
	(*) No ASDA, 32H, Tainst or Cornela access					
	This setting is effective only if "ass authentication http://orgade.LOCAL" and "assa authentication exect commands are configured.					

Configurazione CLI equivalente:

ciscoasa(config)#username ssluser1 password asdmASA@

6. Configurare il gruppo di tunnel. Scegli Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add per creare un nuovo gruppo di tunnel ssigroup.Nella Basic è possibile eseguire l'elenco delle configurazioni come illustrato di seguito: Assegna al gruppo di tunnel il nome ssigroup.Sotto Client Address Assignment, scegliere il pool di indirizzi vpnpool dal Client Address Pools elenco a discesa.Sotto Default Group Policy, scegliere i Criteri di gruppo clientgroup dal Group Policy elenco a discesa.

Basic	Name:	ssigroup	
Advanced	Aliases:		Ì
	Authentication		59
	Method:	💿 AAA 💿 Certificate 💿 Both	
	AAA Server Group:	LOCAL	Manage
		Use LOCAL if Server Group fails	
	Client Address Assignment		2
	DHCP Servers:		
		None O DHCP Link O DHCP Subnet	
	Client Address Pools:	vpnpcol	Select
	Client IPv6 Address Pool	s:	Select
		IPv6 address pool is only supported for SSL.	
	Default Group Policy		
	Crown Dollary	[clieptoroup]	Manage

Sotto la Advanced > Group Alias/Group URL , specificare il nome alias del gruppo come ssigroup_users e fare clic su ok. Configurazione CLI equivalente:

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

Configurazione di ASA release 9.1(2) nella CLI ciscoasa (config) #show running-config

```
: Saved
ASA Version 9.1(2)
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
interface Management0/0
shutdown
no nameif
no security-level
no ip address
```

```
!
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 same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-inside subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0 access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

!--- Standard Split-Tunnel ACL that determines the networks that should travel the Anyconnect tunnel.

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 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400

nat (inside, outside) source static obj-inside obj-inside destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated when going to the Anyconnect Pool

object network obj-inside nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users.
!--- Note: Uses an RFC 1918 range for lab setup.

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 ! ! 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

anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client image

anyconnect enable

!--- Enable the security appliance to download SVC images to remote computers

tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the WebVPN Login page

group-policy clientgroup internal

!--- Create an internal group policy "clientgroup"

group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

!--- Encrypt only traffic specified on the split-tunnel ACL coming from the SSL VPN Clients.

split-tunnel-network-list value SPLIt-ACL

!--- Defines the previosly configured ACL to the split-tunnel policy.

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

Session Type: SVC

```
!--- Associate the group policy "clientgroup" created
```

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users

```
prompt hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9
: end
ciscoasa(config)#
```

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

• show vpn-sessiondb svc - Visualizza le informazioni sulle connessioni SSL correnti. ciscoasa#show vpn-sessiondb anyconnect

Username : ssluser1 Index : 12 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 24 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 Monitoring > VPN > VPN Statistics > Sessions per conoscere le sessioni correnti nell'appliance ASA.

p Save Refresh Back of oring > VPN > VPN Statistics > Sessions e Active
Save Refresh Back of oring > VPN > VPN Statistics > Sessions e Active
e Active
e Active
e Active
r By: AnyConnect Client A rname Group Policy Connection Profile ser1 clientgroup 168.10.1 sslgroup

Risoluzione dei problemiLe informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

• vpn-sessiondb logoff name - Comando per disconnettersi dalla 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 vpn-sessiondb logoff anyconnect per terminare tutte le sessioni di AnyConnect.

• debug webvpn anyconnect <1-255> - Fornisce gli eventi webvpn in tempo reale per stabilire la sessione.

Ciscoasa#debug webvpn anyconnect 7

CSTP state = HEADER_PROCESSING http_parse_cstp_method() ...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' webvpn_cstp_parse_request_field() ...input: 'Host: 10.198.16.132' Processing CSTP header line: 'Host: 10.198.16.132' webvpn_cstp_parse_request_field() ...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152' Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152' Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.05152' webvpn_cstp_parse_request_field() ...input: 'Cookie: webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60' Processing CSTP header line: 'Cookie: webvpn= 146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60' Found WebVPN cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60' WebVPN Cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60' 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: WCRSJOW7Pnbc038' Processing CSTP header line: 'X-CSTP-Hostname: WCRSJOW7Pnbc038' Setting hostname to: 'WCRSJOW7Pnbc038' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-MTU: 1280' Processing CSTP header line: 'X-CSTP-MTU: 1280' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Address-Type: IPv6, IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv6, IPv4' webvpn_cstp_parse_request_field() webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Base-MTU: 1300' Processing CSTP header line: 'X-CSTP-Base-MTU: 1300' webvpn_cstp_parse_request_field() webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Full-IPv6-Capability: true' Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true' webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0A602CF075972F91EAD1 9BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D' Processing CSTP header line: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0 A602CF075972F91EAD19BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D' 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' webvpn_cstp_parse_request_field() ... input: 'X-DTLS-Accept-Encoding: lzs' Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs' webvpn_cstp_parse_request_field()

```
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
... input: 'X-CSTP-Accept-Encoding: lzs, deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/255.255.255.0
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
SVC: Sent gratuitous ARP for 192.168.10.1.
SVC: NP setup
np_svc_create_session(0x5000, 0xa930a180, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.1!
NO SVC ACL
Iphdr=20 base-mtu=1300 def-mtu=1500 conf-mtu=1406
tcp-mss = 1260
path-mtu = 1260 (mss)
mtu = 1260(path-mtu) - 0(opts) - 5(ssl) - 8(cstp) = 1247
tls-mtu = 1247(mtu) - 20(mac) = 1227
DTLS Block size = 16
mtu = 1300(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1243
mod-mtu = 1243(mtu) & 0xfff0(complement) = 1232
dtls-mtu = 1232(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1210
computed tls-mtu=1227 dtls-mtu=1210 conf-mtu=1406
DTLS enabled for intf=2 (outside)
tls-mtu=1227 dtls-mtu=1210
SVC: adding to sessmgmt
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
```

• In ASDM, scegliere Monitoring > Logging > Real-time Log Viewer > View per vedere gli eventi in tempo reale. Nell'esempio vengono mostrate le informazioni sulla sessione tra AnyConnect 192.168.10.1 e Telnet Server 10.2.2.2 su Internet tramite ASA

172.16.1.1.

Real-T	ime Log View	ecr-					200 J
Lie 10	ols <u>W</u> indow	a <u>Help</u>					
þ. Sægr	· Rt Copy	See Or a	lover 🚰 Calor S	ierzings 👔 Com	rie Rule 📓 Show Ru	Rule 🔯 Show Betala 🔅 Eulo	
Hillas Byo	AUG. 2.8		2008/020	- Spritz	Resultation 111 : 11	Stow All mot	
Time	Syring ID	Source IP	Source Port	Destination IP	Destination Port	t Decaption	
22:03:02	302013	292.368.30.1	6/1050	30.2.2.2	60	Balk researd TCP connection 403 for outside: 592.388.12.1/54050 (1/2.18.1.1/54050)(1/CAL/solase 1) to outside: 10.2.2.2(80) (allose 1)	
22:03:02	305011	:92.368.30.3	64059	172.35.1.1	64059	Built dynamic TCP branslation from outsides IS2, ISB, ID, US40393, OC44, (soluser () to outside: 172, 35, 1, 1/64259	

Informazioni correlate

- <u>Cisco ASA serie 5500-X Firewall</u>
- <u>Esempio di configurazione di PIX/ASA e VPN Client per VPN Internet pubblica su Memory</u>
 <u>Stick</u>
- Esempio di configurazione di SSL VPN Client (SVC) su ASA con ASDM
- <u>Documentazione e supporto tecnico Cisco Systems</u>

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).