Configurazione di AnyConnect Secure Mobility Client con split tunneling su una ASA

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Premesse Informazioni sulla licenza AnyConnect Configurazione Esempio di rete Configurazione guidata AnyConnect ASDM Configurazione tunnel suddiviso Scarica e installa il client AnyConnect **Distribuzione Web** Distribuzione autonoma **Configurazione CLI** Verifica Risoluzione dei problemi Installare DART **Eseguire il DART** Informazioni correlate

Introduzione

In questo documento viene descritto come configurare Cisco AnyConnect Secure Mobility Client tramite Cisco Adaptive Security Device Manager (ASDM) su una appliance Cisco Adaptive Security (ASA) con software versione 9.3(2).

Prerequisiti

Requisiti

Il pacchetto di distribuzione Web di Cisco AnyConnect Secure Mobility Client deve essere scaricato sul desktop locale da cui è presente l'accesso ASDM all'appliance ASA. Per scaricare il pacchetto client, consultare la pagina Web <u>Cisco AnyConnect Secure Mobility Client</u>. I pacchetti di distribuzione Web per vari sistemi operativi (OS) possono essere caricati sull'ASA contemporaneamente.

Questi sono i nomi dei file di distribuzione Web per i vari sistemi operativi:

Sistemi operativi Microsoft Windows - AnyConnect-win-<versione>-k9.pkg

- Sistemi operativi Macintosh (MAC) AnyConnect-macosx-i386-<versione>-k9.pkg
- Sistemi operativi Linux AnyConnect-linux-<versione>-k9.pkg

Componenti usati

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

- ASA versione 9.3(2)
- ASDM versione 7.3(1)101
- AnyConnect versione 3.1

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

In questo documento viene illustrato come usare la Configurazione guidata Cisco AnyConnect tramite ASDM per configurare il client AnyConnect e abilitare il tunneling suddiviso.

Il tunneling ripartito è usato negli scenari in cui solo il traffico specifico deve essere tunneling, al contrario degli scenari in cui tutto il traffico generato dal client passa attraverso la VPN quando connesso. Per impostazione predefinita, l'uso della Configurazione guidata AnyConnect determina una configurazione *completa* dell'appliance ASA. Il tunneling ripartito deve essere configurato separatamente, come spiegato più in dettaglio nella sezione di questo documento.

Nell'esempio di configurazione, l'intenzione è inviare il traffico per la subnet 10.10.10.0/24, che è la subnet LAN dietro l'ASA, attraverso il tunnel VPN e tutto il resto del traffico proveniente dal computer client viene inoltrato attraverso il proprio circuito Internet.

Informazioni sulla licenza AnyConnect

Di seguito sono riportati alcuni collegamenti a informazioni utili sulle licenze Cisco AnyConnect Secure Mobility Client:

- Per determinare le licenze necessarie per AnyConnect Secure Mobility Client e le funzionalità correlate, consultare il documento <u>AnyConnect Secure Mobility Client Features, Licenze e sistemi operativi</u> versione <u>3.1</u>.
- Per informazioni sulle licenze AnyConnect Apex e Plus, consultare la <u>Guida agli ordini di</u> <u>Cisco AnyConnect</u>.
- Per ulteriori informazioni, consultare il documento sulla <u>licenza ASA richiesta per le</u> <u>connessioni IP Phone e VPN per dispositivi mobili?</u> nel presente documento vengono fornite

informazioni sui requisiti di licenza aggiuntivi per le connessioni telefoniche e mobili IP.

Configurazione

In questa sezione viene descritto come configurare Cisco AnyConnect Secure Mobility Client sull'appliance ASA.

Esempio di rete

Questa è la topologia utilizzata per gli esempi riportati nel presente documento:



Configurazione guidata AnyConnect ASDM

La configurazione guidata AnyConnect può essere usata per configurare il client AnyConnect Secure Mobility. Prima di procedere, verificare che un pacchetto client AnyConnect sia stato caricato nella memoria flash/sul disco del firewall ASA.

Per configurare AnyConnect Secure Mobility Client tramite la Configurazione guidata, completare la procedura seguente:

1. Accedere ad ASDM, avviare la Configurazione guidata e fare clic su Avanti:

E Cisco ASDM 7.3 for ASA - 10.106.44.21							
<u>File View T</u> ools	Wigards Window Help						
🕝 Hame 🍕 ConFig	Startup Wizard. Draward ? Help						
Device List	VPN Wizards Site-to-site VPN V	/izerd					
🗣 Add 📋 Delete 👙	High Availability and Scalability Wizard AnyConnect VPN V	Mizard hboard					
Find: 一型 10.106.44.3 一题 10.106.44.21	Unified Communication Wizard Clientless SSL VPN ASDM Identity Certificate Wizard IPsec (KEv1) Rem.	Wizard ote Access VPN Wizard					
	Packet Capture Wizard. Host ASA ASD Firev Envir	Name: EdgeASA-4 Version: 9.3(2) Device Uptime: 0d 16h 15m 5s A Version: 7.3(1)101 Device Type: ASA 5525 val Mode: Routed Context Mode: Single onment Status: � OK Total Flash: 8192 MB					

2. Immettere il *nome* del *profilo di connessione*, scegliere l'interfaccia su cui terminare la VPN dal menu a discesa *VPN Access Interface* (Interfaccia di accesso VPN) e fare clic su **Avanti**:

AnyConnect VPN Connection Setup Wizard				X
Steps	Connection Profile Identific	ation		
1. Introduction	This step allows you to cor	nfigure a Connection Profile Na	ame and the Interf	face the remote access users will
2. Connection Profile Identification	access for VPN connection	s.		
3. VPN Protocols	Connection Profile Name:	SSLClient		
4. Client Images	VPN Access Interface:	outside	•	
5. Authentication Meth				

3. Per abilitare SSL (Secure Sockets Layer), selezionare la casella di controllo SSL. Il certificato del dispositivo può essere un certificato rilasciato da un'Autorità di certificazione (CA) di terze parti attendibile, ad esempio Verisign o Entrust, oppure un certificato autofirmato. Se il certificato è già installato sull'appliance ASA, può essere scelto dal menu a discesa. Nota: Questo certificato è il certificato lato server che verrà fornito. Se sull'appliance ASA non è installato alcun certificato ed è necessario generare un certificato autofirmato, fare clic su Gestisci. Per installare un certificato di terze parti, completare la procedura descritta nell'ASA 8.x Installazione manuale dei certificati dei fornitori di terze parti da utilizzare con la configurazione di WebVPN nel documento Cisco.

	AnyConnect VPN Conn	ection Setup Wizard
ſ	Steps	VPN Protocols
l	1. Introduction	AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol
	2. Connection Profile Identification	or protocols you would like this connection profile to support.
	3. VPN Protocols	SSL SSL
	4. Client Images	IPsec
	5. Authentication Meth	Device Certificate
	6. Client Address Assignment	Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.
	7. Network Name Resolution Servers	Device Certificate: None Manage
	8. NAT Exempt	
I	0 AnyConnect Client	

4. Fare clic su Aggiungi:

fanage Ider	ntity Certificat	tes				
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
						Delete
						Export
						Install

5. Digitare un nome appropriato nel campo Nome trust e fare clic sul pulsante di opzione Aggiungi nuovo certificato di identità. Se sul dispositivo non sono presenti coppie di chiavi Rivest-Shamir-Addleman (RSA), fare clic su New (Nuovo) per generarne una:

🔄 Add Identity Certificate		X					
Trustpoint Name:	SelfsignedCert						
Import the identity certific	Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):						
Decryption Passphrase:							
File to Import From:		Browse					
Add a new identity certific	cate:						
Key Pair:	<default-rsa-key></default-rsa-key>	Show New					
Certificate Subject DN:	CN=anyconnect.cisco.com	Select					
Generate self-signed	certificate						
🗌 Act as local certif	ficate authority and issue dynamic certifica	ates to TLS-Proxy					
		Advanced					
Add Cert	tificate Cancel H	lelp					

6. Fare clic sul pulsante di scelta **Usa nome coppia di chiavi predefinita** oppure sul pulsante di scelta **Immettere il nuovo nome della coppia di chiavi** e immettere un nuovo nome. Selezionare le dimensioni delle chiavi e quindi fare clic su **Genera ora**:

E	Add Key F	Pair	X
	Кеу Туре:	RSA	C ECDSA
	Name:	🔘 Use default key pair name	
		Enter new key pair name:	sslcert
	Size:	2048 🗸	
	Usage:	 General purpose 	🔘 Special
	_		
		Generate Now Cancel	Help

7. Dopo aver generato la coppia di chiavi RSA, scegliere la chiave e selezionare la casella di controllo **Generate self-signed certificate** (Genera certificato autofirmato). Immettere il nome di dominio (DN) del soggetto desiderato nel campo *DN soggetto certificato*, quindi fare clic su **Aggiungi certificato**:

Add Identity Certificate	×
Trustpoint Name:	SelfsignedCert
O Import the identity certific	cate from a file (PKCS12 format with Certificate(s)+Private Key):
Decryption Passphrase:	
File to Import From:	Browse
Add a new identity certific	cate:
Key Pair:	ssicert Show New
Certificate Subject DN:	CN=anyconnect.cisco.com Select
Generate self-signed	certificate
Act as local certi	ficate authority and issue dynamic certificates to TLS-Proxy
	Advanced
Add Cer	tificate Cancel Help

8. Al termine dell'iscrizione, fare clic su OK, OK e quindi su Avanti:

AnyConnect VPN Connection Setup Wizard							B-10-10
Ste	[Manage Ide	ntity Certificat	es				X
1. 2.	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
3	hostname	. hostname	16:39:40 M	SelfsignedCert	Gener	RSA (2048 bits)	Show Details
4.							Delete
5.							Export
6.				E Marth Care			Install
7.	End:	Ut		Match Case			
8.	Get your Cis	illment ico ASA secur	ity appliance up	and running quickly with	an SSL A	dvantage digital cert	tificate from
9.	Entrust. Ent	rust oners CIS	E CUSUMERS a	nroll ASA SSL certificate v	vith Entru	st	ncates for testing.
10	Using a pre	viously saved	certificate sign	inq request, <u>enroll with Er</u>	ntrust.		
			Ok	Cancel		lelp	

9. Per aggiungere l'immagine del client AnyConnect (il file .pkg) dal PC o dalla memoria flash, fare clic su Add (Aggiungi). Fare clic su Browse Flash (Sfoglia flash) per aggiungere l'immagine dall'unità flash oppure fare clic su Upload per aggiungere l'immagine direttamente dal computer host:

5. Authentication Meth	Add Replace To Delete 🕈 🗲
6. Client Address Assignment	Add AnyConnect Client Image
7. Network Name Resolution Servers	AnyConnect Image: Browse Flash
8. NAT Exempt	Upload
 AnyConnect Client Deployment 	Regular expression to match user-agent
10. Summary	OK Cancel Help
Browse Flash	

Folders	Files		
land disk0: ⊕ • <mark>⊆ → log</mark>	FileName	Size (Date	
🖶 🛄 crypto_archive	anyconnect-win-3.1.05152-k9.pkg	35,167, 12/17/	
eredumpinto	anyconnect-win-3.1.06073-k9.pkg	38,048, 01/02/	
🖬 🛄 tmp	asa932-smp-k8.bin	63,479, 01/02/	
		10.004 11.007	

10. Una volta aggiunta l'immagine, fare clic su Avanti:

🛧 Add 🗹 Replace 📋 Delete 🛧 🗲					
Image	Regular expression to match user-agent				
disk0:/anyconnect-win-3.1.06073-k9.pkg					
You can download AnyConnect Client packages from <u>Cisco</u> by searching 'AnyConnect VPN Client' or <u>click</u> <u>here</u> ,					
< Back Next >	Cancel Help				

11. L'autenticazione utente può essere completata tramite i gruppi di server Autenticazione, Autorizzazione e Accounting (AAA). Se gli utenti sono già configurati, scegliere CA locale e fare clic su Avanti. Nota: In questo esempio, è configurata l'autenticazione LOCAL, ossia il database utenti locale sull'appliance ASA verrà usato per l'autenticazione.

AnyConnect VPN Co	onnection Setup Wizard	×
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols	Authentication Methods This step lets you specify the location of the authentication server. You can click on the "New" button to create a new server group. AAA Server Group: LOCAL New	
 Client Images Authentication Methods 	Local User Database Details	
 Client Address Assignment Network Name Resolution Servers NAT Exempt AnyConnect Client Deployment Summary 	User to be Added Username: User1 Add >> Password: •••• Delete Confirm Password: ••••	
	< Back Next > Cance	I Help

12. Ènecessario configurare il pool di indirizzi per il client VPN. Se ne è già stato configurato uno, selezionarlo dal menu a discesa. In caso contrario, fare clic su **Nuovo** per configurarne uno nuovo. Al termine, fare clic su **Avanti**:

4. Client Images	IP v4 Ad	IP v4 Address Pool IP v6 Address Pool						
5. Authentication Methi	Address Pool	Address Pool: Select New						
6. Client Address Assignment	Details of	Add IPv4 Pool		×				
7. Network Name Resolution Servers		Name:	SSL-Pool					
3. NAT Exempt		Starting IP Address:	10.10.11.1					
 AnyConnect Client Deployment 		Ending IP Address:	10.10.11.20					
10. Summary		Subnet Mask:	255.255.255.0	•				
		ОК	Cancel	Help				

13. Immettere i server DNS (Domain Name System) e i DN nei campi *DNS* e *Nome dominio* in modo appropriato e quindi fare clic su **Avanti**:

Steps	Network Name R	Network Name Resolution Servers				
1. Introduction	This step lets you	This step lets you specify how domain names are resolved for the remote user when accessing the internal				
2. Connection Profile Identification	network.					
3. MPN Protocols	DNS Servers: 10.10.10.23					
4. Client Images WINS Servers:						
5. Authentication Meth	Domain Name: Cisco.com					

14. In questo scenario, l'obiettivo è limitare l'accesso sulla VPN alla rete **10.10.10.0/24** configurata come subnet *interna* (o LAN) dietro l'ASA. Il traffico tra il client e la subnet interna deve essere esentato da qualsiasi NAT (Network Address Translation) dinamico.

Selezionare la casella di controllo **Esenzione traffico VPN da conversione indirizzi di rete** e configurare le interfacce LAN e WAN da utilizzare per l'esenzione:

2. Connection Profile Identification	🗸 Exempt VPN traffi	c from network address translation
3. VPN Protocols	Inside Interface is	the interface directly connected to your internal network.
4. Client Images	Inside Interface:	[Inside -
5. Authentication Metho	Local Network is t	the network address(es) of the internal network that client
6. Client Address	can access.	
Assignment	Local Network:	any 🔤
7. Network Name Resolution Servers	_	
8. NAT Exempt	The traffic betwee from network add	en AnyConnect client and internal network will be exempt Iress translation.
9. AnyConnect Client		

15. Scegliere le reti locali a cui applicare l'esenzione:

÷.

					Filter C	Clea
Name 1	IP Address	Netmask	Description	Obje	ect NAT Add	::::
⊡·IPv4 Network C	bjects					
- 🏈 any	-					
📑 🚅 Inside	10.10.10.0	255.255.255.0				
- 📲 outsid	10.106.44.0	255.255.255.0				
- 🚅 10.0.0.0	10.0.0.0	255.0.0.0				
- 🛃 10.1.2	10.1.232.192	255.255.255				
FIPv4 Network C	bject Groups					
🕀 🎆 ANY						
🕀 🧱 OBJ_L						
🗄 🎆 OBJ_S						
Interfaces						
- Maride						
🏧 🏧 outside						
Selected Local Net	work					
Selected Local Net	work	etwork/24				
Selected Local Net Local Networl	work < -> Inside-n	etwork/24		OK	Ca	ance

16. Fare clic su Avanti, Avanti e quindi su Fine.

La configurazione del client AnyConnect è ora completata. Tuttavia, quando si configura AnyConnect tramite la Configurazione guidata, i criteri del tunnel *suddiviso* vengono configurati come **tunnel** per impostazione predefinita. Per effettuare solo il tunnel del traffico specifico, occorre implementare il *split-tunneling*. **Nota:** Se non è configurato il tunneling ripartito, il criterio verrà ereditato dal criterio di gruppo predefinito (DfltGrpPolicy), che per impostazione predefinita è **Tunnel** tutto. Ciò significa che quando il client è connesso tramite VPN, tutto il traffico (per includere il traffico verso il Web) viene inviato tramite il tunnel.

Solo il traffico destinato all'indirizzo IP WAN ASA (o *esterno*) ignorerà il tunneling sul computer client. Questa condizione può essere rilevata nell'output del comando **route print** nei computer Microsoft Windows.

Configurazione tunnel suddiviso

Il tunneling ripartito è una funzione che può essere utilizzata per definire il traffico delle subnet o degli host che devono essere crittografati. Questa operazione richiede la configurazione di un Access Control List (ACL) che verrà associato a questa funzione. Il traffico per le subnet o gli host definiti in questo ACL verrà crittografato sul tunnel dal client-end e le route per queste subnet verranno installate nella tabella di routing del PC.

Completare questa procedura per passare dalla configurazione *Tunnel-all* alla configurazione *Split-tunnel*:

1. Selezionare Configurazione > VPN ad accesso remoto > Criteri di gruppo:



2. Fare clic su **Modifica** e utilizzare la struttura di navigazione per passare a **Avanzate** > **Tunneling ripartito**. Deselezionare la casella di controllo **Eredita** nella sezione *Criteri* e selezionare **Elenco reti tunnel sottostante** dal menu a discesa:

1	Edit Internal Group Polic	y: GroupPolicy_SSLClient	7-	
	General	The VPN client makes split tunneling de	cisions on the	basis of a network list that can be specifie
	Advanced	DNS Names:	🗸 Inherit	
	Browser Proxy AnyConnect Client IPsec(IKEv1) Client	Send All DNS Lookups Through Tunnel	: 📝 Inherit	O Yes O No
		Policy:	📃 Inherit	Tunnel Network List Below
		Network List:	🗸 Inherit	

3. Deselezionare la casella di controllo Inherit nella sezione Network List, quindi fare clic su

Manage per selezionare l'ACL che specifica le reti LAN a cui il client deve accedere:

Network List:	🔲 Inherit	inside_access_in	•	Manage
Pressing this button to set up split extu Set up Split Exclusion for Web Secu	sion for Web S rity	curity proxies.		

4. Fare clic su ACL standard, Aggiungi, Aggiungi ACL, quindi su ACL name:

General	The VPN	client makes split tunneling decisions on the basis of a network list that can be specif				
Servers		ACL Manager				
Solit Tuppeling	DNS N	and the second sec				
Browser Proxy	Send	Standard ACL Extended ACL				
⊕ AnyConnect Client ⊕ IPsec(IKEv1) Client	 AnyConnect Client IPsec(IKEv1) Client ▲ Add ▲ Edit 					
	Policy	No Address Action Description				
	Netwo					
		Add ACL				
	Pressi					
	Set	ACL Name: Split-ACL				
		OK Cancel Help				
	Inte					

5. Per aggiungere la regola, fare clic su Add ACE:

ACL Man	ager						
Standard ACL Extended ACL							
💠 Add 🗸 📷 Edit 💼 Delete 🛧 🗲 👗 ங 🏨 🖉							
No	Address	Action	Description				
Split-A	CL						
🔄 Add A	ACE						
Action: Permit Deny							
Description	tion:						

6. Fare clic su OK.

📵 Edit Internal Group Policy	GroupPolicy_S9_Client	7-		×
-Ceneral -Cervers	The VPN client makes split to reling det	istorie on the	deals of a network iso fraction be specified below by providing the proper parameters to YokγY and Network test' fac	bs.
i≟-Advanced Split Tunne Ing	DNE Names:	🔽 Inherit		
→Browser Provy →AnyConnect Client →Psec(KBy1) Client	Send All DNS Loci ups Through Tunnel:	🔽 liiherit	⊙ wes ⊙No	
	Policy:	 Inherit 	Turnel Network List Selow 🔻	
	Network List:	🔲 Inherit	(Bolt-ACL 🔹	Manage
	Pressing this button to set up cold extus Extup Split Ectlusion for Web Securi Intercept DHCP Configuration Mes	on for Web S ly	iecurity provies ficrosoft Clients	8

7. Fare clic su Apply (Applica).

Una volta connessi, i percorsi per le subnet o gli host sull'ACL suddiviso vengono aggiunti alla tabella di routing del client. Nei computer con sistema operativo Microsoft Windows, è possibile visualizzare questa informazione nell'output del comando **route print**. L'hop successivo per queste route sarà un indirizzo IP dalla subnet del pool IP del client (in genere il primo indirizzo IP della subnet):

10.106.44.0 255.255.255.0 On-link 10.106.44.243 261 172.16.21.1 255.255.255 On-link 10.106.44.243 6

II This is the route for the ASA Public IP Address. Sui computer MAC OS, immettere il comando **netstat -r** per visualizzare la tabella di routing del PC:

\$ netstat -r Routing tables Internet: Destination Gateway Flags Refs Use Netif Expire default hsrp-64-103-236-1. UGSc 34 0 en1 10.10.10/24 10.10.11.2 UGSc 0 44 utun1 !! This is the split tunnel route. 10.10.11.2/32 localhost UGSc 1 0 lo0 172.16.21.1/32 hsrp-64-103-236-1. UGSc 1 0 en1 !! This is the route for the ASA Public IP Address.

Scarica e installa il client AnyConnect

Per distribuire Cisco AnyConnect Secure Mobility Client sul computer dell'utente, è possibile procedere in due modi:

- Distribuzione Web
- Distribuzione autonoma

Entrambi i metodi vengono illustrati in modo più dettagliato nelle sezioni seguenti.

Distribuzione Web

Per utilizzare il metodo di distribuzione Web, immettere l'URL https://<FQDN dell'ASA>o <IP dell'ASA> in un browser sul computer client, in modo da visualizzare la pagina del portale *WebVPN*.

Nota: Se si utilizza Internet Explorer (IE), l'installazione viene completata principalmente tramite ActiveX, a meno che non si sia costretti a utilizzare Java. Tutti gli altri browser utilizzano Java.

Dopo aver effettuato l'accesso alla pagina, l'installazione deve iniziare sul computer client e, al termine, il client deve connettersi all'appliance ASA.

Nota: È possibile che venga richiesta l'autorizzazione per l'esecuzione di ActiveX o Java. Per procedere con l'installazione, è necessario consentire tale operazione.

Logon					
Group	SSLClient	¥			
Username					
Password					
	Logon				

- -> C Attor: 172.16.21.1/CACHE/stc/1/index.html

AnyConnect Secure Mobility Client					
🔦 WebLaunch	Attempting to use Java for Installation				
 Platform Detection - ActiveX 	Sun Java applet has started. This could take up to 60 seconds. Please wait				
Java Detection					
🗌 - Java					
Download					
Connected					
	Help Download				

Distribuzione autonoma

Per utilizzare il metodo di distribuzione standalone, completare i seguenti passaggi:

- Scaricare l'immagine del client AnyConnect dal sito Web Cisco. Per scegliere l'immagine corretta da scaricare, consultare la pagina Web <u>Cisco AnyConnect Secure Mobility Client</u>. In questa pagina è disponibile un collegamento per il download. Passare alla pagina di download e selezionare la versione appropriata. Eseguire una ricerca del pacchetto di installazione completa - Windows / Programma di installazione autonomo (ISO). Nota: Viene quindi scaricata un'immagine del programma di installazione ISO (ad esempio, *anyconnectwin-3.1.06073-pre-deploy-k9.iso*).
- 2. Usare WinRar o 7-Zip per estrarre il contenuto del pacchetto ISO:

appropriation-21.070				
anyconnect-win-5.1.070	1	Burn disc image		1
		7-Zip	×	Open archive
	2	Edit with Notepad++		Open archive
		Open with	•	Extract files
		Share with	•	Extract Here
				Extract to "anyconnect-win-3.1.07021-pre-deploy-k9\"

3. Una volta estratto il contenuto, eseguire il file **Setup.exe** e scegliere i moduli da installare con Cisco AnyConnect Secure Mobility Client.

Suggerimento: Per configurare impostazioni aggiuntive per la VPN, fare riferimento alla sezione <u>Configurazione delle connessioni client VPN</u> di <u>AnyConnect</u> della *guida alla configurazione di Cisco ASA serie 5500 dalla CLI, versione 8.4 e 8.6*.

Configurazione CLI

In questa sezione viene fornita la configurazione CLI per Cisco AnyConnect Secure Mobility Client a scopo di riferimento.

```
ASA Version 9.3(2)
!
hostname PeerASA-29
enable password 8Ry2YjIyt7RRXU24 encrypted
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
1
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
1
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
1
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224
access-list all extended permit ip any any
```

!*********Split ACL configuration*********

access-list Split-ACL standard permit 10.10.10.0 255.255.255.0

no pager logging enable logging buffered debugging mtu outside 1500 mtu inside 1500 mtu dmz 1500 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-721.bin no asdm history enable arp timeout 14400 no arp permit-nonconnected

nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24 destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp route-lookup

access-group all in interface outside route outside 0.0.0.0 0.0.0.0 172.16.21.2 1 timeout xlate 3:00:00 timeout pat-xlate 0:00:30 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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:01:00 timeout floating-conn 0:00:00 dynamic-access-policy-record DfltAccessPolicy user-identity default-domain LOCAL aaa authentication ssh console LOCAL http server enable http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact

!******* Trustpoint for Selfsigned certificate*********
!Genarate the key pair and then configure the trustpoint
!Enroll the trustpoint genarate the self-signed certificate

```
crypto ca trustpoint SelfsignedCert
enrollment self
subject-name CN=anyconnect.cisco.com
keypair sslcert
crl configure
crypto ca trustpool policy
crypto ca certificate chain SelfsignedCert
certificate 4748e654
308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105
0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e
636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e
170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a
311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31
19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d
06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0
55a975ec alf2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4
ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0
7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c
75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93
```

5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7 53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34 03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36 19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001 300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296 c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1 64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41 daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928 f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9 4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833 900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206 3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8 quit telnet timeout 5 ssh timeout 5 ssh key-exchange group dh-group1-shal console timeout 0 management-access inside threat-detection basic-threat threat-detection statistics access-list no threat-detection statistics tcp-intercept ssl server-version tlsv1-only ssl encryption des-shal 3des-shal aes128-shal aes256-shal !******* Bind the certificate to the outside interface******* ssl trust-point SelfsignedCert outside !*******Configure the Anyconnect Image and enable Anyconnect*** webvpn enable outside anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1 anyconnect enable tunnel-group-list enable !*****Group Policy configuration******* !Tunnel protocol, Spit tunnel policy, Split !ACL, etc. can be configured. group-policy GroupPolicy_SSLClient internal group-policy GroupPolicy_SSLClient attributes wins-server none dns-server value 10.10.10.23 vpn-tunnel-protocol ikev2 ssl-client split-tunnel-policy tunnelspecified split-tunnel-network-list value Split-ACL default-domain value Cisco.com username User1 password PfeNk7qp9b4LbLV5 encrypted username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15 !*****Tunnel-Group (Connection Profile) Configuration**** tunnel-group SSLClient type remote-access tunnel-group SSLClient general-attributes address-pool SSL-Pool default-group-policy GroupPolicy_SSLClient tunnel-group SSLClient webvpn-attributes group-alias SSLClient enable class-map inspection_default match default-inspection-traffic 1 1 policy-map type inspect dns preset_dns_map

```
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect sip
isspect xdmcp
!
service-policy global_policy global
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0
: end
```

Verifica

Completare questi passaggi per verificare la connessione client e i vari parametri associati a tale connessione:

1. Selezionare Monitoraggio > VPN su ASDM:



2. Per filtrare il tipo di VPN, è possibile utilizzare l'opzione **Filter By**. Selezionare **AnyConnect Client** dal menu a discesa e tutte le sessioni del client AnyConnect. **Suggerimento**: Le sessioni possono essere ulteriormente filtrate in base ad altri criteri, ad esempio *Nome utente* e *indirizzo*

IP.							
VPN 27 0	Elter By: AnyCon-	nact Cliant 🔹 💌	Al Sessions	•	Eltar		
	Usemane	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes TX Bytes RX	Inactivity
- Compression Statistics - Encryption Statistics - Clobal D(E/IPsec Statistics	cisco.	CroupPolicy_SSUCIER SSUCIENT	(F.16.11.1 17215/21	AnyConnect-Parent SSL-Tunnel AnyConnect-Parent (I)none S.	16 58:56 UTC Dr: 12m:55a	11472 22738	01.00m:00s
Clentless SSL VPN VPN Connection Graphs WSA Sessions							
🖳 Interfaces							
MAN VEN							

3. Fare doppio clic su una sessione per ottenere ulteriori dettagli su quella particolare sessione:

assio	on Details —								
Username		Group Palicy Connection Profile	Assigned IP Address Public IP Address	Protocol Login Time Encryption Duration		Login Time Duration	Bytes Tx Bytes Rx	Tx Rx Inactivity	
sco GroupPolicy_SSLClien 10.10.11.1 SSLClient 172.16.21.1		AnyConnect-Parent SSL-Tunnel . 16:58:56 UTC 1147 AnyConnect-Parent: (1)none S., Oh:21m:09s 2665			1472 26653	Oh:ODm:ODs			
leta D	alls ACL	Local Addr. / Subnet N	Ask / Protocol / Port	Encryption	Other		Bytes Tx Bytes Tx		Mon
	AnyConn		none Tunnel ID: 14.1 Public IP: 172.16.21.1 Hashing: none TCP Src Port 57828 TCP Dst Port 443 Authentication Mode: userPassword Idle Time Out: 30 Minutes Idle TO Left: 9 Minutes Client Oc Type: Windows Client Type: AnyConnect Client Ver: Clico AnyConnect VFN Agent		5954 1046	* III			

4. Per ottenere i dettagli della sessione, immettere il comando **show vpn-sessiondb anyconnect** nella CLI:

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1 Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. Per perfezionare i risultati, è possibile utilizzare le altre opzioni di filtro:

show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

Username : cisco Index : 19 Assigned IP : 10.10.11.1 Public IP : 10.106.44.243 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 11036 Bytes Rx : 4977 Pkts Tx : 8 Pkts Rx : 60 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GroupPolicy_SSLClient Tunnel Group : SSLClient Login Time : 20:33:34 UTC Mon Apr 6 2015 Duration : 0h:01m:19s

```
AnyConnect-Parent Tunnels: 1
```

SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 19.1 Public IP : 10.106.44.243 Encryption : none Hashing : none TCP Src Port : 58311 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073 Bytes Tx : 5518 Bytes Rx : 772 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel TD : 19.2 Assigned IP : 10.10.11.1 Public IP : 10.106.44.243 Encryption : 3DES Hashing : SHA1 Encapsulation: TLSv1.0 TCP Src Port : 58315 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073 Bytes Tx : 5518 Bytes Rx : 190 Pkts Tx : 4 Pkts Rx : 2 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 19.3 Assigned IP : 10.10.11.1 Public IP : 10.106.44.243 Encryption : DES Hashing : SHA1 Encapsulation: DTLSv1.0 UDP Src Port : 58269 UDP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073

Pkts Tx : O Pkts Rx : 59 Pkts **Tx Drop** : O Pkts **Rx Drop** : O

Bytes Tx : 0 Bytes Rx : 4150

Risoluzione dei problemi

Èpossibile usare lo strumento di diagnostica e segnalazione di AnyConnect (DART) per raccogliere i dati utili per la risoluzione dei problemi di installazione e connessione di AnyConnect. La procedura guidata DART viene usata sul computer su cui è in esecuzione AnyConnect. DART raggruppa i registri, lo stato e le informazioni di diagnostica per l'analisi di Cisco Technical Assistance Center (TAC) e non richiede privilegi di amministratore per l'esecuzione sul computer client.

Installare DART

Per installare DART, completare i seguenti passaggi:

1. Scaricare l'immagine del client AnyConnect dal sito Web Cisco. Per scegliere l'immagine

corretta da scaricare, consultare la pagina Web <u>Cisco AnyConnect Secure Mobility Client</u>. In questa pagina è disponibile un collegamento per il download. Passare alla pagina di download e selezionare la versione appropriata. Eseguire una ricerca del **pacchetto di installazione completa - Windows / Programma di installazione autonomo (ISO)**. Nota: Viene quindi scaricata un'immagine del programma di installazione ISO (ad esempio, *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).

2. Usare WinRar o 7-Zip per estrarre il contenuto del pacchetto ISO:



- 3. Selezionare la cartella in cui è stato estratto il contenuto.
- 4. Eseguire il file Setup.exe e selezionare solo lo strumento di diagnostica e report Anyconnect:



Eseguire il DART

Di seguito sono riportate alcune importanti informazioni da considerare prima di eseguire DART:

- Il problema deve essere ricreato almeno una volta prima di eseguire DART.
- La data e l'ora sul computer dell'utente devono essere annotate quando il problema viene ricreato.

Eseguire il comando DART dal menu Start sul computer client:



Èpossibile selezionare la modalità *predefinita* o *personalizzata*. Cisco consiglia di eseguire il comando DART nella modalità predefinita in modo che tutte le informazioni possano essere acquisite in una singola ripresa.

Cisco DART 3.1.05170	X					
Bundle Creation Option	ili.ili. cisco					
Select "Default" to include the typical log files and diagnostic informative the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.	ation in ostic					
 Default (Bundle will be saved to Desktop) 						
Custom						
Clear logs after DART finshes						
Back Next	Cancel					

Al termine, lo strumento salva il file DART bundle *.zip* sul desktop del client. Il bundle può quindi essere inviato al TAC (dopo aver aperto una richiesta TAC) per ulteriori analisi.

Informazioni correlate

- Guida alla risoluzione dei problemi dei client VPN AnyConnect Problemi comuni
- Java 7 Guida alla risoluzione dei problemi di AnyConnect, CSD/Hostscan e WebVPN
- Documentazione e supporto tecnico Cisco Systems

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).