Configurazione del tunnel VPN di gestione di AnyConnect sull'ASA

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Funzionamento del tunnel di gestione
Limitazioni
Configurazione
Configurazione su ASA tramite ASDM/CLI
Creazione del profilo VPN di gestione di AnyConnect
Metodi di distribuzione per il profilo VPN di gestione di AnyConnect
(Facoltativo) Configurare un attributo personalizzato per supportare la configurazione tunnel-tutto
Verifica
Risoluzione dei problemi
Informazioni correlate

Introduzione

In questo documento viene descritto come configurare l'ASA in modo che il gateway VPN accetti le connessioni da AnyConnect Secure Mobility Client tramite il tunnel VPN di gestione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione VPN tramite Adaptive Security Device Manager (ASDM)
- Configurazione CLI ASA (Basic Adaptive Security Appliance)
- Certificati X509

Componenti usati

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

• Software Cisco ASA versione 9.12(3)9

- Software Cisco ASDM versione 7.12.2
- Windows 10 con Cisco AnyConnect Secure Mobility Client versione 4.8.03036

Nota: scaricare il pacchetto AnyConnect VPN Web Deployment (anyconnect-win*.pkg or anyconnectmacos*.pkg) dal sito Cisco <u>Software Download</u> (solo utenti registrati). Copiare il client VPN AnyConnect nella memoria flash dell'ASA da scaricare sui computer degli utenti remoti per stabilire la connessione VPN SSL con l'ASA. Per ulteriori informazioni, consultare la sezione <u>Installazione del client AnyConnect</u> della guida alla configurazione delle appliance ASA.

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

Un tunnel VPN di gestione assicura la connettività alla rete aziendale ogni volta che il sistema client viene acceso, non solo quando l'utente finale stabilisce una connessione VPN. È possibile eseguire la gestione delle patch sugli endpoint fuori sede, in particolare sui dispositivi che l'utente raramente connette alla rete aziendale tramite VPN. Questa funzionalità offre inoltre vantaggi agli script di accesso al sistema operativo degli endpoint che richiedono la connettività di rete aziendale.

AnyConnect Management Tunnel consente agli amministratori di connettere AnyConnect senza l'intervento dell'utente prima del momento in cui l'utente esegue l'accesso. Il tunnel di gestione di AnyConnect può funzionare insieme al rilevamento di reti attendibili e quindi viene attivato solo quando l'endpoint è fuori sede e disconnesso da una VPN avviata dall'utente. Il tunnel di gestione di AnyConnect è trasparente per l'utente finale e si disconnette automaticamente quando l'utente avvia la VPN.

SO/applicazione	Requisiti minimi di versione
ASA	9.0.1
ASDM	7.10.1
Versione di Windows AnyConnect	4.7.00136
Versione macOS AnyConnect	4.7.01076
Linux	Non supportato

Funzionamento del tunnel di gestione

Il servizio agente VPN AnyConnect viene avviato automaticamente all'avvio del sistema. Rileva che la funzionalità tunnel di gestione è abilitata (tramite il profilo VPN di gestione), quindi avvia l'applicazione client di gestione per avviare una connessione tunnel di gestione. L'applicazione client di gestione utilizza la voce host del profilo VPN di gestione per avviare la connessione. Il

tunnel VPN viene quindi stabilito come di consueto, con una sola eccezione: non viene eseguito alcun aggiornamento software durante una connessione al tunnel di gestione, in quanto il tunnel di gestione deve essere trasparente per l'utente.

L'utente avvia un tunnel VPN tramite l'interfaccia utente di AnyConnect, che attiva la terminazione del tunnel di gestione. Dopo l'interruzione del tunnel di gestione, l'impostazione del tunnel utente continua normalmente.

L'utente disconnette il tunnel VPN, che attiva il ripristino automatico del tunnel di gestione.

Limitazioni

- Interazione utente non supportata
- L'autenticazione basata su certificati tramite l'archivio certificati del computer (Windows) è supportata solo
- · La verifica rigorosa dei certificati del server è applicata
- Un proxy privato non è supportato
- Un proxy pubblico non è supportato (il valore ProxyNative è supportato sulle piattaforme in cui le impostazioni Proxy nativo non vengono recuperate dal browser)
- Script di personalizzazione AnyConnect non supportati

Nota: per ulteriori informazioni, fare riferimento a Informazioni sul tunnel VPN di gestione.

Configurazione

In questa sezione viene descritto come configurare Cisco ASA come gateway VPN per accettare le connessioni dai client AnyConnect tramite il tunnel VPN di gestione.

Configurazione su ASA tramite ASDM/CLI

Passaggio 1. Creare i Criteri di gruppo AnyConnect. Passare aConfiguration > Remote Access VPN > Network (Client) Access > Group Policies. Fare clic su .Add

Nota: si consiglia di creare un nuovo criterio di gruppo AnyConnect che venga utilizzato solo per il tunnel di gestione di AnyConnect.



Passaggio 2. Fornire unNamenome per i Criteri di gruppo. Assegnare/creare unAddress Poologgetto. ScegliereTunneling ProtocolsComeSSL VPN Cliente/OIPsec IKEv2, come illustrato nell'immagine.

General Servers ▶ Advanced	Name: AnyConnect_MGMT_ Banner: Z Inherit	unnel	
	Address Pools: Inherit VPN_Po	l	Select
	IPv6 Address Pools: 🗹 Inherit		Select
	More Options		*
	Tunneling Protocols:	Inherit Clientless SSL VPN SSL VPN Process Process Client	V IPsec IKEv2 L2TP/IPsec
	Priter.		Manage
	Access Hours:		- Manage
	Simultaneous Logins:		^
	Compaction Parfile (Turnel Crewn) Look		
	Connection Profile (Tunnel Group) Lock:		
	Idle Timeout		
		innert None minutes	
	Security Group Tag (SGT):	✓ Inherit None (2 – 65519)	
	On smart card removal:	V Inherit Disconnect Keep the connection	
	Maximum Connect Time Alert Interval:	Inherit Default minutes	
	Periodic Certificate Authentication Interval	✓ Inherit Unlimited hours	
Find:	Next	Previous	

Passaggio 3. Passare aAdvanced > Split Tunneling. Configurare ilPolicyComeTunnel Network List Belowe scegliere ilNetwork List, come mostrato nell'immagine.

• • •		Edit Internal G	roup Policy: AnyConnect_MGMT_Tunnel	
General Servers V Advanced <u>Split Tunneling</u> Browser Proxy AnyConnect Client > IPsec(IKEv1) Client	The VPN client makes split tunneling dee fields. DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List: Pressing this button to set up split exlus Set up Split Exclusion for Web Securit	Edit Internal G isions on the Inherit Inherit Inherit Inherit ion for Web S iy	iroup Policy: AnyConnect_MGMT_Tunnel t basis of a network list that can be specified below by providing the proper parameters to 'Policy' an Yes No Tunnel Network List Below VPN-Split C Upon	nd 'Networl Manag
•	Set up Split Exclusion for Web Securi	from Microso	oft Clients	-
Find:	Next 🔵	Previous Help	Cancel OK	

Nota: se non viene eseguito il push di un indirizzo client per entrambi i protocolli IP (IPv4 e IPv6), l'impostazione deve essere taleclient Bypass Protocolenabledche il traffico corrispondente non venga interrotto dal tunnel di gestione. Per configurare, fare riferimento al <u>passo 4</u>.

Passaggio 4. Passare aAdvanced > AnyConnect Client. ImpostareClient Bypass ProtocolSUEnable. Fare clicoKper salvare, come mostrato nell'immagine.

		Add Internal Group Policy	
General	Keep Installer on Client System:	V Inherit Yes No	
Servers Advanced	Datagram Transport Layer Security (DTLS):	Inherit Enable Disable	
Split Tunneling	DTLS Compression:	Inherit Enable Disable	
AnyConnect Client	SSL Compression:	✓ Inherit O Deflate O LZS O Disable	
IPsec(IKEv1) Client	Ignore Don't Fragment(DF) Bit:	Inherit Enable Disable	
	Client Bypass Protocol:	Inherit O Enable Disable	
	FQDN of This Device:	V FQDN	
	MTU:	✓ Inherit	
	Keepalive Messages:	✓ Inherit Disable Interval: seconds	
	Optional Client Modules to Download:	☑ Inherit	٥
•	Always-On VPN:	✓ Inherit O Disable O Use AnyConnect Profile setting 0	
	Client Profiles to Download:	Inherit	
		Add 1 Delete	
		Profile Name Profile Usage/Type	
Find:	🔘 Next 🔘	Previous	
		Help Cancel OK	

Passaggio 5. Come mostrato nell'immagine, fare clic su_{Apply}per inviare la configurazione all'appliance ASA.

ổ Home 🔧 Configuration 📝 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forw	vard 💡 Help Type topic Go			dialo
000 Remote Access VPN	O Configuration > Remote Acc	cess VPN > Network (Client) Acces	s > Group Policies		
Introduction Introduction Phetwork (Clent) Access Phetwork (Clent) Access Phetwork (Clent) Access PhyConnect Connection Profiles AnyConnect Clent Profile AnyConnect Clent Profile AnyConnect Clent Software	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes Add C C Edit Delete A As	roup is a collection of user-oriente VPN connection profiles and user ac from an LDAP server you must use a sign	J authorization attribute/value pairs that may be stored i counts. In <u>LDAP attribute map</u> .	nternally on the device or externally on a RADIUS/LDAP server. The grou	p
S Dynamic Access Policies	Name	Туре	Tunneling Protocol	Connection Profiles/Users Assigned To	
Croup Policies	AnyConnect	internal	ssl-client	AnyConnect	
IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Defa	ultWE
IPsec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel	
 Berlin Statution Berlin Statution					
Contraction of the second seco					
Site-to-Site VPN	Find:	Match Case			
Device Management			Reset Apply		

Configurazione CLI per Criteri di gruppo:

<#root>

ip local pool

VPN_Pool

192.168.10.1-192.168.10.100 mask 255.255.255.0

! access-list

VPN-Split

standard permit 172.16.0.0 255.255.0.0
!
group-policy

AnyConnect_MGMT_Tunnel

internal group-policy

AnyConnect_MGMT_Tunnel

attributes vpn-tunnel-protocol

ikev2 ssl-client

split-tunnel-network-list value

```
VPN-Split
```

client-bypass-protocol enable address-pools value VPN_Pool

Passaggio 6. Creare il profilo di connessione AnyConnect. Passare aConfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Fare clic su .Add

Nota: si consiglia di creare un nuovo profilo di connessione AnyConnect che venga usato solo per il tunnel di gestione di AnyConnect.



Passaggio 7. Fornire unNameprofilo per il profilo di connessione e impostareAuthentication MethodComeCertificate only. Scegliete comeGroup Policyquella creata nel <u>passo 1</u>.

Advanced	Aliases: Authentication Method: AAA Server Group:	Certificate only		
	Authentication Method: AAA Server Group:	Certificate only		
	Method: AAA Server Group:	Certificate only		
	AAA Server Group:			
		LOCAL	٥	Manage
		Use LOCAL if Server Group fails		
	SAML Identity Provider			
	SAML Server :	None	0	Manage
	Client Address Assignment	t		
	e	• None OHCP Link OHCP Subnet		
	Client Address Pools:			Select
	Client IPv6 Address Pool	s:		Select
	Default Group Policy			
	Group Policy:	AnyConnect_MGMT_Tunnel	٥	Manage
	(Following fields are link	ed to attribute of the group policy selected above.)		
	✓ Enable SSL VPN cli	ient protocol		
	Enable IPsec(IKEv2	?) client protocol		
	DNS Servers:			
	WINS Servers:			
	Domain Name:			
Find:		Next OPrevious		

Nota: verificare che il certificato radice della CA locale sia presente sull'appliance ASA. Passare aConfiguration > Remote Access VPN > Certificate Management > CA Certificatesper aggiungere/visualizzare il certificato.

Nota: verificare che un certificato di identità rilasciato dalla stessa CA locale sia presente nell'archivio certificati del computer (per Windows) e/o nella catena di chiavi di sistema (per macOS).

Passaggio 8. Passare aAdvanced > Group Alias/Group URL. Fare clic suAddsottoGroup URLse aggiungere un'URLicona. Accertarsi che siaEnabledselezionata. Fare clicokper salvare, come mostrato nell'immagine.

Add AnyConnect Connection Profile

Basic Advanced General Client Addressing Authentication Secondary Authentication Authorization Accounting	 Enable the display of Radius Reject-Message on the login screen when authentication is rejected Enable the display of Securid messages on the login screen Connection Aliases This SSL VPN access method will present a list of aliases configured for all connection profiles. You r the Login Page Setting in the main panel to complete the configuration. Add Delete (The table is in-line editable.) ¹
	Alias Enabled Group URLs This SSL VPN access method will automatically select the connection profile, without the need for use Add Delete (The table is in-line editable.) URL Enabled URL: https://asa.example.com/AnyConnect_MGMT_Tunnel C Enabled Help Cancel OK
Find:	Next Previous Help Cancel OK

Se si usa IKEv2, verificare cheIPsec (IKEv2) Accesssia abilitato sull'interfaccia usata per AnyConnect.

O O Remote Access VPN	Config	uration > Remot	e Access VPN > N	Vetwork (Client) A	Access > AnyConnect Co	nnection Profiles			
Introduction	The security	appliance automa	tically deploys the	e Cisco AnvConne	rt VPN Client to remote u	ers upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN			
Network (Client) Access	Client sunno	rts IPcor (IKEv2) to	innel as well as SS	I tunnel with Dat	aram Transport Laver Se	(TTS) transling options			
AnyConnect Connection Profiles	Cheffe Juppo	103 11 300 (10242) 0	anner as wen as so		agram mansport cayer se	anty (or to) taimining options.			
S AnyConnect Customization/Local	Access Interfac	es							
T AnyConnect Client Profile	Z Enable C	Inable Cisco AnyConnect VPN Client access on the interfaces selected in the table below							
AnyConnect Client Software									
Compare Access Policies	SSL access m	lust be enabled if	you allow AnyCon	pect client to be I	aunched from a browser (ved Launch) .			
US Course Ballalas	transfer a	SSL Access		IPsec (IKEv2) Acc	855				
Group Policies	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Dealer Continue			
IPsec(IKEv1) Connection Profiles	outrida					Device Certificate			
IPsec(IKEv2) Connection Profiles	ousine		· · · · · ·		<u> </u>				
Secure Mehility Colution	inside					Port Settings			
Secure mooning solution									
Sp Address Assignment									

Passaggio 9. Fare clicApplysu questa opzione per inviare la configurazione all'appliance ASA.



Configurazione CLI per il profilo di connessione (gruppo di tunnel):

```
<#root>
tunnel-group
AnyConnect_MGMT_Tunnel
type remote-access
tunnel-group
AnyConnect_MGMT_Tunnel
general-attributes
default-group-policy AnyConnect_MGMT_Tunnel
tunnel-group AnyConnect_MGMT_Tunnel
authentication certificate
group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

Passaggio 10. Verificare che sull'appliance ASA sia installato un certificato protetto e che il certificato sia associato all'interfaccia usata per le connessioni AnyConnect. PassareConfiguration > Remote Access VPN > Advanced > SSL Settingsa per aggiungere/visualizzare questa impostazione.

Nota: per ulteriori informazioni, consultare il documento sull'<u>installazione del certificato di</u> <u>identità sull'appliance ASA</u>.

C Remote Access VPN	O O Configuration > Remote Acces	ss VPN > Advanced > SSL Settings			
Introduction					
Network (Client) Access	Configure SSL parameters. These para	meters affect both ASDM and SSL VPN acc	ess.		
AnyConnect Connection Pr					
AnyConnect Customization	The minimum SSI version for the sec	urity appliance to peopliate as a "server":	TISVI		6V1 2
AnyConnect Client Profile	The minimum 35c version for the sec	arity appliance to negotiate as a server .	1011		341-2
AnyConnect Client Softwar	The minimum SSL version for the sec	urity appliance to negotiate as a "client":	TLS V1	۵	
🍄 Dynamic Access Policies					
Group Policies	Diffie-Hellman group to be used with	i SSL:	Group2 - 1024-bit modulus	S	
IPsec(IKEv1) Connection P	ECDH group to be used with SSI		Group19 - 256-bit EC		
IPsec(IKEv2) Connection P	con group to be used min sse.			•	
Secure Mobility Solution	Encryption				
Sp Address Assignment	Cichardian	Cinhas Consults Lovel		Cicker Manalikers / Custom Steine	
Advanced	Cipher version Default	Cipher Security Level		Cipher Algorithms/ Custom String	Edit
Clientless SSL VPN Access	Default	Medium		DES-CBC3-SHA AES128-SHA DHE-KSA-F	AES128-SHA AES256-SHA DHE-RSA
AAA/Local Users	TISVI	Medium		DHE-KSA-AES256-SHA AES256-SHA DH	E-KSA-AESI28-SHA AESI28-SHA
AAA Server Groups	11591.1	Medium		DHE-KSA-AES250-SHA AES250-SHA DH	E-KSA-AESIZ8-SHA AESIZ8-SHA
Se I DAP Attribute Map	11391.2	Medium		ECDHE-ECDSA-AES250-GCM-SHA384 E	CDHE-KSA-AES250-GCM-SHA384 D
local lisers	DIGV1	Medium		UHE-KSA-AES256-SHA AES256-SHA UH	E-KSA-AESIZ8-SHA AESIZ8-SHA
Secure Deckton Manager	DIGVI.2	Medium		ECDHE-ECDSA-AES256-GCM-SHA384 E	CDHE-RSA-AES256-GCM-SHA384 D
Castificate Management					
Certificate Management					
Language Localization					
Load balancing	Server Name Indication (SNI)				
DHCP Server	Domain		Certificate		
UNS	Coman		Certificate		Add
Advanced					Edia
Connection Gateway					CON
SSL Settings					Delete
E Reference Identity					
Certificate to AnyConnect					
HTTP Redirect					
Maximum VPN Sessions					
Crypto Engine					
	Certificates				
	Specify which certificates, if any, s	hould be used for SSL authentication on ea	ch interface. The fallback certificate	will be used on interfaces not associated with	a certificate of their own.
	Interface	Brimany Castificate	Lond Polyaging Castificate	Key Tope	
evice Setup	iorida	rimary cerolicate	coad searcing Certificate	Key-Type	Edit
	management				
rewall	loutside	ROOT - CAthostname - ASA example	0	Primane PSA (2048	hits) Load Balancing: none
emote Access VPN		proor-occussmame=xsx.example		Primary, KSA (2046	onar, coad balancing, none
emote Access VPN					
ite-to-Site VPN					
evice Management					

Configurazione CLI per Trustpoint SSL:

<#root>

ssl trust-point ROOT-CA outside

Creazione del profilo VPN di gestione di AnyConnect

Passaggio 1. Creare il profilo del client AnyConnect. Passare aConfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Fare clic suAdd, come mostrato nell'immagine.

🚭 Home 🦓 Configuration 📴 Monitorin	g 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward	? Help Type topic Go			cisco
OOO Remote Access VPN	○ ○ ○ Configuration > Remote Access VPN >	Network (Client) Access > AnyConnect Clie	nt Profile		
Pinroduction Pinroduction Pin Network (Client) Access Pin/Connect Connection Profil Pin/Connect Customization/Lc An/Connect Customization/Lc An/Connect Client Software Dinamic Access Policies Pinroduction Pinroduction	This panel is used to manage AnyConnect Clier button to add a new profile. Pressing the Impor The profile Usage field is introduced with the S HostScan configuration can be performed by gr	nt Profiles and perform group assignment for / t or Export button is for upload and download ecure Mobility Solution. This field contains dif oing to Secure Desktop Manager/HostScan. If '	AnyConnect version 2.5 or later.You can select a profile of client profiles between local machine and device. ferent profile usage in AnyConnect version 3.0 and later HostScan' is not visible under 'Secure Desktop Manager	to edit, change group or to delete. You can select the 'Add' , you will need to restart ASDM.	
IPsec(IKEv1) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	
Prectificity) Connection Profil Address Assignment Address Assignment Address SSL VPN Access Advanced Clentiess SSL VPN Access AAA Server Corups LOAP Attribute Map Cleat Users AAA Server Corups Load Balancing POHCP Server DoK SL Connection Cateway SSL Settings					
Certificate to AnyConnect and Certificate to AnyConnect and HTTP Redirect Cal Maximum VPN Sessions Crypto Engine					
Device Setup					
Remote Access VPN					
Site-to-Site VPN					
Device Management			Reset Apply		

Passaggio 2. Fornire unaProfile Namerisposta. Scegliere ilProfile UsageComeAnyConnect Management VPN profile. Scegliere il fileGroup PolicyCreato nel passo 1. Fare clic suok, come mostrato nell'immagine.

Profile Name		Profile Usage	Group Policy	Profile Location
	• • •	Add AnyConnect Client P	rofile	
	Profile Name	AnyConnect_MGMT_Profile		
	Profile Usage	AnyConnect Management VPN Profile	C	
	Enter a device f created if it doe	ile path for an xml file, ie. disk0:/ac_profile. The file v es not exist.	will be automatically	
	Profile Location	disk0:/anyconnect_mgmt_profile.vpnm	Browse Flash	
			Upload	
	Group Policy	AnyConnect_MGMT_Tunnel		
		Enable 'Always On VPN' for selected group		
		Help Cancel	ОК	
			Reset Anniv	

Passaggio 3. Scegliere il profilo creato e fare clic su Modifica, come mostrato nell'immagine.

file Name	Profile Usage	Group Policy	Profile Location
Connect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm

Passaggio 4. Passare a Server List. Fare clic suAdd per aggiungere una nuova voce all'elenco dei server, come illustrato nell'immagine.

	Anyo	Connect Client Profile Ed	itor - AnyConnect_MG	MT_Profile						
Profile: AnyConnect_MG	MT_Profile				At	bout				
VPN Preferences (Part 1) Preferences (Part 2)	Server List									
 Backup Servers ☑ Certificate Pinning ☑ Certificate Matching ☑ Server List 	Hostname	Host Address	User Group	Backup Server List	Certificate Pins					
	Note: at most o	ne server can be defined	l in a management VPI	N profile. Add Edit	Delete Details					
		Help C	ancel OK]						

Passaggio 5. Fornire unaDisplay Namerisposta. Aggiungere il valoreFQDN/IP addressdell'appliance ASA. Fornire come nome delUser Groupgruppo di tunnel.Group URLviene popolato automaticamente conFQDNeUser Group. Fare clic su .OK

Server	Certificate Pinning
Primary Server Display Name (required) AnyConnect_MGMT_Tunnel FQDN or IP Addr User Group (required) asa.example.com / AnyConnect_MGMT_ Group URL asa.example.com/AnyConnect_MGMT_Tunnel Backup Servers	Connection Information Primary Protocol SSL ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only)
Host Address	Add Move Up Move Down Delete
ОК	Cancel

Nota: I'FQDN/indirizzo IP + gruppo di utenti deve corrispondere all'URL del gruppo indicato durante la configurazione del profilo di connessione AnyConnect al <u>passaggio 8</u>.

Nota: AnyConnect con IKEv2 come protocollo può essere utilizzato anche per stabilire una VPN di gestione per l'appliance ASA. Accertarsi chePrimary Protocolsia impostatoIPsecsu Passo 5.

Passaggio 6. Come mostrato nell'immagine, fare clic suokper salvare.

AnyCo	onnect Client Profile Edi	tor - AnyConnect_MGM	T_Profile		
MT_Profile					About
Server List					
Hostname	Host Address	User Group	Backup Server List	Certificate Pins	
AnyConnect_MGMT_	T asa.example.com	AnyConnect_MGMT_	T Inherited		
Note: at most on	e server can be defined	in a management VPN	profile. Add	Delete	
			Edit	Details	
2					
	MT_Profile Server List Hostname AnyConnect_MGMT	MT_Profile Server List Hostname Host Address AnyConnect_MGMT_T asa.example.com Note: at most one server can be defined	MT_Profile Server List Hostname Host Address AnyConnect_MGMT_T asa.example.com AnyConnect_MGMT_ Note: at most one server can be defined in a management VPN	MT_Profile Server List Hostname HostAddress User Group Backup Server List AnyConnect_MGMT_T asa.example.com AnyConnect_MGMT_T asa.example.com Note: at most one server can be defined in a management VPN profile. Add Edit Edit	MT_Profile Server List Hostname Host Address User Group Backup Server List Certificate Pins InvyConnect_MGMT_T asa.example.com AnyConnect_MGMT_T Inherited Note: at most one server can be defined in a management VPN profile. Add Delete Edit Details

Passaggio 7. Fare clic_{Apply}per spostare la configurazione sull'appliance ASA, come mostrato nell'immagine.



Configurazione CLI dopo l'aggiunta del profilo VPN di gestione di AnyConnect.

<#root>

```
webvpn
```

```
enable outside
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
ļ
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
```

webvpn

Profilo VPN di gestione di AnyConnect sul computer client AnyConnect:

<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc
<ClientInitialization>
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>
```

true

<ShowPreConnectMessage>false</ShowPreConnectMessage>

Machine

System

true

<ProxySettings>IgnoreProxy</ProxySettings> <AllowLocalProxyConnections>true</AllowLocalProxyConnections> <AuthenticationTimeout>30</AuthenticationTimeout>

--- Output Omitted ---

<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover> <AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>

AnyConnect_MGMT_Tunnel

asa.example.com

</AnyConnectProfile>

Nota: se si usa TND (Trusted Network Detection) nel profilo VPN AnyConnect dell'utente, si consiglia di usare le stesse impostazioni nel profilo VPN di gestione per garantire un'esperienza utente coerente. Il tunnel VPN di gestione viene attivato in base alle impostazioni TND applicate al profilo del tunnel VPN utente. Inoltre, l'azione TND Connect nel profilo VPN di gestione (applicata solo quando il tunnel VPN di gestione è attivo), si applica sempre al tunnel VPN dell'utente, per garantire che il tunnel VPN di gestione sia trasparente per l'utente finale.

Nota: su qualsiasi PC dell'utente finale, se le impostazioni TND sono abilitate nel profilo VPN di gestione e il profilo VPN dell'utente è mancante, vengono prese in considerazione le impostazioni delle preferenze predefinite per il TND (disabilitato nelle preferenze predefinite nell'applicazione client AC) anziché il profilo VPN dell'utente mancante. Questa mancata corrispondenza può causare un comportamento imprevisto/non definito. Per impostazione predefinita, le impostazioni TND sono disattivate nelle preferenze predefinite.

Per superare le impostazioni hardcoded delle preferenze predefinite nell'applicazione Client AnyConnect, il PC dell'utente finale deve avere due profili VPN, un profilo VPN utente e un profilo VPN di gestione CA, ed entrambi devono avere le stesse impostazioni TND. La logica alla base della connessione e della disconnessione del tunnel VPN di gestione è che per stabilire un tunnel VPN di gestione, l'agente AC utilizza le impostazioni TND del profilo VPN dell'utente e, per la disconnessione del tunnel VPN di gestione, controlla le impostazioni TND del profilo VPN di gestione.

Metodi di distribuzione per il profilo VPN di gestione di AnyConnect

 Una connessione VPN dell'utente è stata completata con il profilo di connessione ASA per scaricare il profilo VPN di gestione di AnyConnect dal gateway VPN.

💊 Nota: se il protocollo usato per il tunnel VPN di gestione è IKEv2, è necessario stabilire la prima connessione tramite SSL (per scaricare il profilo AnyConnect Management VPN



• Il profilo VPN di gestione di AnyConnect può essere caricato manualmente sui computer client tramite un push di oggetti Criteri di gruppo o tramite installazione manuale (verificare che il nome del profilo siavpnMgmtTunProfile.xml).

Percorso della cartella in cui aggiungere il profilo: Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun Mac OS: /opt/cisco/anyconnect/profile/mgmttun/

(Facoltativo) Configurare un attributo personalizzato per supportare la configurazione tunnel-tutto

Il tunnel VPN di gestione richiede una divisione che include la configurazione del tunneling per impostazione predefinita, per evitare un impatto sulla comunicazione di rete avviata dall'utente. È possibile ignorare questa impostazione quando si configura l'attributo personalizzato nei Criteri di gruppo utilizzati dalla connessione del tunnel di gestione.

Passaggio 1. PassareConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributesa. Fare clic su, come mostrato nell'immagine.



Passaggio 2. Impostare l'attributo personalizzato Tipo su_{Management}TunnelAllAllowed e fornire un Description. Fare clic su_{OK}, come mostrato nell'immagine.

O O O Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes

	Description
	Create Custom Attribute Type
• •	Create Custom Attribute Type
Туре	Create Custom Attribute Type ManagementTunnelAllAllowed ManagementTunnelAllAllowed
Type	Create Custom Attribute Type ManagementTunnelAllAllowed ManagementTunnelAllAllowed
• • • Type Desc	Create Custom Attribute Type ManagementTunnelAllAllowed ription:
Type Desc	Create Custom Attribute Type ManagementTunnelAllAllowed ription:
Type Desc	Create Custom Attribute Type ManagementTunnelAllAllowed ription: Help Cancel OK

Passaggio 3. Passare a Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Fare clic su, come mostrato nell'immagine.



Passaggio 4. Scegliete il Tipo (Type) come ManagementTunnelAllAllowed. Impostare il nome cometrue. Fare clic suAddper fornire un valore di attributo personalizzato, come mostrato nell'immagine.

○ ○ ○ <u>Configuration > Rem</u>	ote Access VPN > Network (Client) Access > A	dvanced > AnyConnect Custon	n Attribute Names
Declarations of custom attrib	oute names and these attributes are enforced in ,	AnyConnect group policy and Any	Connect dynamic access policy
🕈 Add 🗹 Edit 📋 Delete			
Type Name Values			
	Oranto Oustana Attributa	News	
	Create Custom Attribute	Name	
Type:	ManagementTunnelAllAllowed		Manage
Name:	true		
	Value	Add	
		Edit	
		Delete	
Configure Values:			
	Help Cancel	OK	

Passaggio 5. Impostare il valore cometrue. Fare clic suok, come mostrato nell'immagine.

	Management runner	AnAnowed	~	manage
Name:	true			
	Value		Add	
		Add Value	e 19	
		Add Value		
true				
ue:				
ue:				
lue:				
ue:				
ue:				
ue:				

Passaggio 6. Passare aConfiguration > Remote Access VPN > Network (Client) Access > Group Policies. Scegliere Criteri di gruppo. Fare clic su Edit , come illustrato nell'immagine.

1	Home 🔏 Configuration 📴 Monitoring 冒	🕽 Save 🔇 Refresh 🔇 Back 🔘 Fo	orward 💡 Help Type topic G	0		cisco
	O O Remote Access VPN	O Configuration > Remote A	Access VPN > Network (Client)	Access > Group Policies		
marks	? Introduction ▶ Network (Client) Access ▶ AnyConnect Connection Profiles ▷ GaryConnect Customization/Localization ☑ AnyConnect Client Profile ☑ AnyConnect Client Software ▷ Description Access in the second s	Manage VPN group policies.A VPN server. The group policy informat To enforce authorization attribute Add C Edit Delete	I group is a collection of user-o ion is referenced by VPN connec es from an LDAP server you mus Assign	riented authorization attribute/value pairs that ma tion profiles and user accounts. t use an <u>LDAP attribute map</u> .	ay be stored internally on the device or externally on a RADIUS/	LDAP
ooki	W Crown Policies	Name	Туре	Tunneling Protocol	Assigned To	
	Psec(KEv1) Connection Profiles	AnyConnect	Internal	ssl-client	AnyConnect	
-	IPsec(IKEv2) Connection Profiles	Amconnect MGMT Tunnel	Internal	ikev2;iztp=ipsec	AnyConnect_MGMT_Tunnel	Jp;Det
	Secure Mobility Solution	Party-connect_mainin_i conner	THE COMPANY	INCY6, 331-CIICIIL	herberginger Turgur Tranner	
	Address Assignment Address Assignment Address Assignment Advanced AnyConnect Essentials AnyConnect Custom Attributes AnyConnect Custom Attributes AnyConnect Custom Attribute Names Advanced Advanced Advanced Advanced Advanced Advanced Advanced					
	Bevice Setup					
	Firewall					
	Site-to-Site VPN	Find:	Match Case			
	Device Management			Reset Apply		

Passaggio 7. Come mostrato nell'immagine, passare aAdvanced > Split Tunneling. Configurare il criterio comeTunnel All Networks.

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers	The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network fields.	i:
▼ Advanced Split Tunneling Browser Proxy AnyConnect Client IPsec(IKEv1) Client	DNS Names: Inherit Inherit Yes No Policy: Inherit Tunnel All Networks S IPv6 Policy: Inherit Inherit Tunnel All Networks I Network List: Inherit Inher	
Find:	Next O Previous	
	Help Cancel OK	

Passaggio 8. Passare aAdvanced > Anyconnect Client > Custom Attributes. Fare clic suAdd, come mostrato

nell'immagine.

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers Y Advanced Split Tunneling Browser Proxy Y AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Customization Custom Attributes > IPsec(IKEv1) Client	Configuration of custom policy attributes. Image: Configuration of custom policy attributes. Type Name of Value Image: Configuration of custom policy attributes. Type Name of Value Image: Configuration of custom policy attributes. Type Image: Configuration of custom policy attributes. Type Image: Configuration of custom policy attributes. Type Image: Configuration of custom policy attributes. Image: Configuration of custom policy attributes.	
Find:	Next Previous	
	Help Cancel OK	

Passaggio 9. Scegliere il tipo di attributo comeManagementTunnelAllAllowed e il valore come true. Fare clic OKSU, come mostrato nell'immagine.

	Name of Value	
	Create Custom Attribute	
Attribute type:	ManagementTunnelAllAllowed	age
Omit the value		
Select Value:	true ᅌ Mana	age

Passaggio 10. Fare clic su_{Apply}per trasferire la configurazione sull'appliance ASA, come mostrato nell'immagine.



Configurazione CLI dopo l'aggiunta dellManagementTunnelAllAllowed'attributo personalizzato:

<#root>

```
webvpn
```

```
enable outside
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
 disable
 error-recovery disable
I
anyconnect-custom-data ManagementTunnelAllAllowed true true
I
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
```

```
vpn-tunnel-protocol ikev2 ssl-client
```

```
split-tunnel-policy tunnelall
client-bypass-protocol enable
address-pools value VPN_Pool
anyconnect-custom ManagementTunnelAllAllowed value true
webvpn
anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Verifica

Verificare la connessione del tunnel VPN di gestione sulla CLI dell'ASA con ilshow vpn-sessiondb detail anyconnect comando.

```
<#root>
ASA#
show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username
           :
vpnuser
               Index
                           : 10
Assigned IP :
192.168.10.1
Public IP : 10.65.84.175
Protocol
            :
AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
            : AnyConnect Premium
License
Encryption
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
            : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Hashing
            : 17238
                                                 : 1988
Bytes Tx
                                     Bytes Rx
                                                  : 13
            : 12
                                     Pkts Rx
Pkts Tx
Pkts Tx Drop : 0
                                     Pkts Rx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time : 01:23:55 UTC Tue Apr 14 2020
Duration
            : 0h:11m:36s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                     VLAN
                                                  : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
DTLS-Tunnel:
  Tunnel ID : 10.3

        Assigned IP
        : 192.168.10.1
        Public IP
        : 10.65.84.175

        Encryption
        : AES-GCM-256
        Hashing
        : SHA384

  Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
  Encapsulation: DTLSv1.2
                                               UDP Src Port : 57053
  UDP Dst Port : 443
Auth Mode : Certificate
  Idle Time Out: 30 Minutes
                                    Idle TO Left : 18 Minutes
  Client OS : Windows
  Client Type : DTLS VPN Client
  Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03036
  Bytes Tx : 17238
Pkts Tx : 12
                                                     Bytes Rx : 1988
Pkts Rx : 13
  Pkts Tx Drop : 0
                                                     Pkts Rx Drop : 0
```

--- Output Omitted ---

Verificare la connessione del tunnel VPN di gestione su ASDM.

Selezionare Monitoraggio > VPN > Statistiche VPN > Sessioni. Filtra per client AnyConnect per visualizzare la sessione client.

ổ Home 🦓 Configuration [M	onitoring 📊 Save (🔇 Refresh 🔇 Ba	ck 🔘 Forward 💡	Help Type topic	io				cisco
Device List Bookmarks	OOO Monitoring	> VPN > VPN Stati	stics > Sessions						
O O O Device List									
🕈 Add 📋 Delete 🚿 Connect	Туре	Active		Cumulative	Peak Concu	rrent	Inactiv	e	
Find: Go	AnyConnect Client		1		19		1		0
A 10.106.39.196	SSL/TLS/DTLS		1		19		1		0
₫ 10.106.64.230									
10.197.227.47									
10.106.51.99:444									
O O O VPN									
VPN Statistics	Filter By AnyCo	nnect Client	All S	essions ᅌ		Filter			
VPN Cluster Loads	Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Inactivity	Audit !	Details
Crypto Statistics	vpnuser	AnyConnect_MGMT.	192.168.10.1	AnyConnect-Parent	10:52:25 0	TC 34688	0h:00m:00s	c0a80	Logout
Encryption Statistics		AnyConnect_MGM1.		AnyConnect-Parent:	(1)none [0n:01m:31	5 33954			Logout
Global IKE/IPsec Statistics									Ping
Protocol Statistics									
VLAN Mapping Sessions									
E Clientless SSL VPN									
Shared SSL VPN									
VPN Connection Graphs									
SA Sessions									
interfaces									
₩ VP <u>N</u>						-			
4 Routing	To sort VPN session	ns, right-click on th	ne above table and s	elect Table Sort Order	from popup menu.				
	Logout By: A	II Sessio		Logout Sessions					
🔏 Properties	Logour by:								

Verifica della connessione del tunnel VPN di gestione sul computer client:

Sisco AnyConnect Secure Mobil	ity Client	- 🗆 X	
cisco AnyCon	nect Secure Mobility Clie	ent (i)	
Virtual Private Network (VPN)		Diagnostics	
Preferences Statistics Route Details Firewall Message History			
Connection Information State: Tunnel Mode (IPv4):	Disconnected Not Available	Cisco AnyConnect Secure Mobility Client –	
Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Not Available Not Available 00:00:00 None Connected (asa.example.com)	VPN: Ready to connect.	nnect
Address Information			
Client (IPv4): Client (IPv6): Server:	Not Available Not Available Not Available	\$ ()	alialia cisco
Bytes		• •	
	Reset	Export Stats	

Risoluzione dei problemi

La nuova riga Statistiche interfaccia utente (Stato connessione di gestione) può essere utilizzata per risolvere i problemi di connettività del tunnel di gestione. Di seguito sono riportati gli stati di errore più comuni:

Disconnesso (disabilitato):

- La funzione è disattivata.
- Verificare che il profilo VPN di gestione sia stato distribuito nel client tramite la connessione al tunnel utente (è necessario aggiungere il profilo VPN di gestione ai criteri di gruppo del tunnel utente) o fuori banda tramite il caricamento manuale del profilo.
- Verificare che il profilo VPN di gestione sia configurato con una singola voce host che includa un gruppo di tunnel.

Disconnesso (rete attendibile):

• TND ha rilevato una rete attendibile, quindi il tunnel di gestione non è stato stabilito.

Disconnesso (tunnel utente attivo):

• Tunnel VPN utente attualmente attivo.

Disconnesso (avvio del processo non riuscito):

• Errore di avvio del processo durante il tentativo di connessione al tunnel di gestione.

Disconnesso (connessione non riuscita):

- Errore di connessione durante la definizione del tunnel di gestione.
- Verificare che l'autenticazione del certificato sia configurata nel gruppo del tunnel, che non sia presente alcun banner nei Criteri di gruppo e che il certificato del server sia attendibile.

Disconnesso (configurazione VPN non valida):

- Configurazione non valida del tunneling suddiviso o del protocollo client da ignorare ricevuta dal server VPN.
- Controllare la configurazione nei criteri di gruppo del tunnel di gestione in base alla documentazione.

Disconnesso (aggiornamento software in sospeso):

• Un aggiornamento software AnyConnect è attualmente in sospeso.

Disconnesso:

• Il tunnel di gestione sta per essere stabilito o non può essere stabilito per altri motivi.

Raccogli DART per ulteriore risoluzione dei problemi.

Informazioni correlate

- Configurazione del tunnel VPN di gestione
- Risoluzione dei problemi del tunnel VPN di gestione
- <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).