Konfigurieren des AnyConnect Management-VPN-Tunnel auf der ASA

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen **Betrieb eines Management-Tunnels** Einschränkungen Konfigurieren Konfiguration auf der ASA über ASDM/CLI Erstellung des AnyConnect-Management-VPN-Profils Bereitstellungsmethoden für das AnyConnect-Management-VPN-Profil (Optional) Konfigurieren eines benutzerdefinierten Attributs zur Unterstützung der Tunnel-All-Konfiguration Überprüfung Fehlerbehebung Zugehörige Informationen Einleitung

In diesem Dokument wird beschrieben, wie eine ASA konfiguriert wird, wenn das VPN-Gateway Verbindungen vom Cisco AnyConnect Secure Mobility Client über den Management-VPN-Tunnel akzeptiert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- VPN-Konfiguration durch Adaptive Security Device Manager (ASDM)
- Grundlegende CLI-Konfiguration der Adaptive Security Appliance (ASA)
- X509-Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ASA Software Version 9.12(3)9
- Cisco ASDM Software Version 7.12.2

• Windows 10 mit Cisco AnyConnect Secure Mobility Client der Version 4.8.03036

Hinweis: Laden Sie das AnyConnect VPN Web Deployment-Paket herunter (anyconnect-win*.pkg or anyconnect-macos*.pkg) aus dem Cisco <u>Software Download</u> (nur registrierte Kunden). Kopieren Sie den AnyConnect VPN-Client in den Flash-Speicher der ASA, die auf die Computer der Remote-Benutzer heruntergeladen werden soll, um die SSL VPN-Verbindung mit der ASA herzustellen. Weitere Informationen finden Sie im Abschnitt <u>Installing the AnyConnect</u> <u>Client</u> (Installieren des AnyConnect-Clients) im ASA-Konfigurationsleitfaden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Ein Management-VPN-Tunnel stellt die Verbindung zum Unternehmensnetzwerk sicher, wenn das Client-System hochgefahren wird, nicht nur, wenn der Endbenutzer eine VPN-Verbindung herstellt. Sie können das Patch-Management auf Endgeräten außerhalb des Büros durchführen, insbesondere auf Geräten, die vom Benutzer nur selten über VPN mit dem Büronetzwerk verbunden werden. Auch Betriebssystem-Anmeldeskripts für Endgeräte, die eine Verbindung mit dem Unternehmensnetzwerk benötigen, profitieren von dieser Funktion.

AnyConnect Management Tunnel ermöglicht es Administratoren, AnyConnect ohne Benutzereingriff anzuschließen, bevor sich der Benutzer anmeldet. Der AnyConnect Management-Tunnel kann zusammen mit der Erkennung vertrauenswürdiger Netzwerke eingesetzt werden und wird daher nur ausgelöst, wenn das Endgerät extern installiert und von einem benutzerinitiierten VPN getrennt ist. Der AnyConnect Management-Tunnel ist für den Endbenutzer transparent und trennt die Verbindung automatisch, wenn der Benutzer das VPN initiiert.

Betriebssystem/Anwendung

ASA ASDM Windows AnyConnect-Version macOS AnyConnect-Version Linux Mindestversionsanforderungen 9.0.1 7.10.1 4.7.00136 4.7.01076 Nicht unterstützt

Betrieb eines Management-Tunnels

Der AnyConnect VPN-Agentendienst wird beim Systemstart automatisch gestartet. Es erkennt, dass die Management-Tunnel-Funktion aktiviert ist (über das Management-VPN-Profil), und startet daher die Management-Client-Anwendung, um eine Management-Tunnel-Verbindung zu initiieren. Die Management-Client-Anwendung verwendet den Hosteintrag aus dem Management-VPN-Profil, um die Verbindung zu initiieren. Dann wird wie üblich der VPN-Tunnel aufgebaut, mit einer Ausnahme: Während einer Management-Tunnel-Verbindung wird kein Software-Update durchgeführt, da der Management-Tunnel für den Benutzer transparent sein soll.

Der Benutzer initiiert über die AnyConnect-Benutzeroberfläche einen VPN-Tunnel, der die Beendigung des Management-Tunnels auslöst. Nach der Beendigung des Management-Tunnels wird die Einrichtung des Benutzertunnels wie gewohnt fortgesetzt. Der Benutzer trennt den VPN-Tunnel, wodurch die automatische Wiederherstellung des Management-Tunnels ausgelöst wird.

Einschränkungen

- Es wird keine Benutzerinteraktion unterstützt
- Es wird nur die zertifikatbasierte Authentifizierung über den Machine Certificate Store (Windows) unterstützt
- Die strenge Überprüfung des Serverzertifikats wird erzwungen
- Ein privater Proxy wird nicht unterstützt.
- Ein öffentlicher Proxy wird nicht unterstützt (ProxyNative-Wert wird auf Plattformen unterstützt, auf denen die Einstellungen des systemeigenen Proxys nicht vom Browser abgerufen werden)
- AnyConnect-Anpassungsskripte werden nicht unterstützt

Hinweis: Weitere Informationen finden Sie unter <u>Informationen zum Management-VPN-</u><u>Tunnel.</u>

Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie Cisco ASA als VPN-Gateway konfigurieren, um Verbindungen von AnyConnect-Clients über den Management-VPN-Tunnel zu akzeptieren.

Konfiguration auf der ASA über ASDM/CLI

Schritt 1: Erstellen Sie die AnyConnect-Gruppenrichtlinie. Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Klicken Sie auf Add.

Hinweis: Es wird empfohlen, eine neue AnyConnect-Gruppenrichtlinie zu erstellen, die nur für den AnyConnect-Management-Tunnel verwendet wird.



Schritt 2: Bieten Sie Name für die Gruppenrichtlinie. Zuweisen/Erstellen eines Address Pool. Auswählen Tunneling Protocols als SSL VPN Client und/oder IPsec IKEv2, wie im Bild dargestellt.

General	Name: AnvConnect MGMT	Tunnel		-
Servers	Rappor			
Auvanceu	Banner:			
	SCEP forwarding URL: 🗹 Inherit			
	Address Pools: Inherit VPN_Po	ool		Select
	IPv6 Address Pools: 🔽 Inherit			Select
	More Options			
	Tunneling Protocols:	Inherit	Clientless SSL VPN 🗹 SSL VPN Client 🛛 IPsec IKEv1 🔽 IPsec IKEv2 🗌 L2TP/	IPsec
	Filter:	🗹 Inherit	•	Manage
	Access Hours:	🗹 Inherit	•	Manage
	• Simultaneous Logins:	🗹 Inherit		
	Restrict access to VLAN:	🗹 Inherit	○	
	Connection Profile (Tunnel Group) Lock:	🗹 Inherit	≎	
	Maximum Connect Time:	🗹 Inherit	Unlimited minutes	
	Idle Timeout:	🗹 Inherit	None minutes	
	Security Group Tag (SGT):	🗹 Inherit	None (2 – 65519)	
	On smart card removal:	🗹 Inherit	O Disconnect O Keep the connection	
	Timeout Alerts			
	Maximum Connect Time Alert Interval:	🗹 Inherit	Default minutes	
	Periodic Certificate Authentication Interval	: 🗹 Inherit	Unlimited hours	
ind:	Next	Previous		

Schritt 3: Navigieren Sie zu Advanced > Split Tunneling. Konfigurieren Sie Policy als Tunnel Network List Below und wählen Sie Network List, wie im Bild dargestellt.

		Edit Internal G	Group Policy: AnyConnect_MGMT_	Tunnel	
General Servers	The VPN client makes split tunneling dee fields.	cisions on the	e basis of a network list that can	be specified below by providing the proper parameters to 'Policy' a	nd 'Networl
Split Tunneling	DNS Names:	🗹 Inherit			
Browser Proxy ► AnyConnect Client	Send All DNS Lookups Through Tunnel:	Inherit	🗌 Yes 💿 No		
IPSec(IKEV1) Client	Policy:	🗌 Inherit	Tunnel Network List Below	3	
	IPv6 Policy:	🗹 Inherit		0	
	Network List:	Inherit	VPN-Split	•	Manag
	Pressing this button to set up split exlus Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	ion for Web S	Security proxies. sft Clients		
Find:	🔘 Next 🔮	Previous			
		Help	Cancel OK		

Hinweis: Wenn für beide IP-Protokolle (IPv4 und IPv6) keine Client-Adresse angefordert wird, Client Bypass Protocol Einstellung muss enabled sodass der entsprechende Datenverkehr nicht durch den Management-Tunnel unterbrochen wird. Weitere Informationen zur Konfiguration finden Sie in <u>Schritt 4</u>.

Schritt 4: Navigieren Sie zu Advanced > AnyConnect Client. Festlegen Client Bypass Protocol zu Enable. Klicken Sie auf OK um zu speichern, wie im Bild gezeigt.

		Add Internal Group Policy	
General Servers ▼ Advanced Split Tunneling Browser Proxv ► AnyConnect Client ► IPsec(IKEv1) Client	Keep Installer on Client System: Datagram Transport Layer Security (DTLS): DTLS Compression: SSL Compression: Ignore Don't Fragment(DF) Bit:	Inherit Yes No Inherit Enable Disable Inherit Enable Disable Inherit Deflate LZS Inherit Enable Disable	
	Client Bypass Protocol: FQDN of This Device: MTU: Keepalive Messages:	Inherit Enable Ø FQDN Ø Inherit Ø Inherit Disable Inherit seconds	
۰	Optional Client Modules to Download: Always-On VPN: Client Profiles to Download:	 ✓ Inherit ✓ Inherit ✓ Inherit ✓ Inherit ✓ And ● potend 	٢
		Profile Name Profile Usage/Type	
Find:	Next 🕥 I	Previous Help Cancel OK	

Schritt 5: Klicken Sie wie in dieser Abbildung dargestellt auf Apply um die Konfiguration an die ASA weiterzuleiten.

🚳 Home 🗞 Configuration 📴 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forw	rard 💡 Help Type topic Go		cisco
COO Remote Access VPN	○ ○ ○ Configuration > Remote Acc	cess VPN > Network (Client) Acces	s > Group Policies	
Introduction I	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes Add C Edit Delete & As	roup is a collection of user-oriented VPN connection profiles and user ac from an LDAP server you must use a sign	i authorization attribute/value pairs that may be stored i counts. n LDAP attribute map.	nternally on the device or externally on a RADIUS/LDAP server. The group
E Dynamic Access Policies	Name	Type	Tunneling Protocol	Connection Profiles/Users
Group Policies	AmConnect	Internal	est_client	Assigned To Am/Connect
Psec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	internal	ikev1:ikev2:l2tp-ipsec	DefaultRAGroup:DefaultL2LGroup:DefaultADMINGroup:DefaultWE
Psec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MCMT_Tunnel
 Address Assignment Address St. VPN Access AAJLocal Users AAJLocal Users DAP Antibute Map Scure Desktop Manager Certificate Management Certificate Management Certificate Management Certificate Management Der Stever DNS Advanced 				
Bevice Setup				
Device setup				
👯 Firewall				
Remote Access VPN				
Site-to-Site VPN	Find:	Match Case		
Device Management			Reset Apply	

CLI-Konfiguration für die Gruppenrichtlinie:

```
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
```

Schritt 6: Erstellen Sie das AnyConnect-Verbindungsprofil. Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Klicken Sie auf Add.

Hinweis: Es wird empfohlen, ein neues AnyConnect-Verbindungsprofil zu erstellen, das nur für den AnyConnect-Management-Tunnel verwendet wird.

🚯 Home 🔧 Configuration 📴 Monitoring 🔓	🚽 Save 🔇 Refresh 🔇 Back 🌘	Derward 🦻 He	Ip Type topic Go				cis	
COO Remote Access VPN	Configuration > Rem	ote Access VPN > I	Network (Client) Acc	cess > AnyConnect Co	nnection Profiles			
Introduction Metwork (Client) Access AryConnect Connection Profiles Fig AnyConnect Customization/Localizati	The security appliance autor VPN Client supports IPsec (II Access Interfaces	natically deploys th (Ev2) tunnel as well	e Cisco AnyConnect as SSL tunnel with D	VPN Client to remote us atagram Transport Laye	ers upon connection. The initia r Security (DTLS) tunneling opti	l client deployment requires end-use ons.	er administrative rights. The Cisco AnyConnect	t
AnyConnect Client Profile	C Enable Cisco AnyConnec	t VPN Client access	on the interfaces se	lected in the table below	/			
Dynamic Access Policies	SSL access must be enabled	IT you allow AnyCor	Prec (KEv2) Access	nched from a browser (v	veb Launch) .			
Group Policies Psec(IKEv1) Connection Profiles	Interface Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate			
IPsec(IKEv2) Connection Profiles	inside			0	Port Settings			
Secure Mobility Solution Address Assignment								
G Advanced Gardess SS VPN Access	Bypass interface access	lists for inbound VP	'N sessions					
T 🖬 AAA/Local Users	Access lists from group poli	cy and user policy a	lways apply to the tr	affic.				
AAA Server Groups	Login Page Setting							
Cocal Users	Allow user to select con	nection profile on t	he login page. 💿					
A Secure Desktop Manager	Shutdown portal login p	age.						
Language Localization	Connection Profiles							
Se Load Balancing	Connection profile (tunnel g	roup) specifies how	user is authenticated	d and other parameters.	You can configure the mapping	from certificate to connection profi	le <u>here</u> .	
DHCP Server	🕈 Add 🗹 Edit 📋 Delete	Find:	0	Match Case				
Advanced	Name	SSL Enabled	IPsec	Enabled	Aliases	Authentication Method	Group Policy	٦.
	DefaultRAGroup			<u> </u>		AAA(LOCAL)	DfltGrpPolicy	
	Am Connect				AmConnect	AAA((OCAL)	AmConnect	
	Myconnect	<u>∞</u>			Anyconnect	poor(cocac)	surgeonneer	٩.
Device Setup								
Remote Access VPN								
Site-to-Site VPN	Let group LIRL take prez	edence if group LIRI	and certificate man	match different connect	ion profiles. Otherwise, the cor	maction profile that matches the car	tificate man will be used	1
Device Management	Let group the take preci	evence il group uni	and certificate map	materr unresent connect	Reset Apoly	mection prome that matches the cer	uncare map win oe used.	
:					HERE Apply			

Schritt 7. Bieten Sie Name für das Verbindungsprofil, und legen Sie Authentication Method als Certificate only. Wählen Sie Group Policy wie in <u>Schritt 1</u> erstellt.

Basic Industrial	Name:	AnyConnect_MGMT_Tunnel		
Advanced	Aliases:			
	Authentication			
	Method:	Certificate only		
	AAA Server Group:	LOCAL	0	Manage
		Use LOCAL if Server Group fails		
	SAML Identity Provider			
	SAML Server :	None	0	Manage
	Client Address Assignment			
	DHCP Servers:			
		None OHCP Link OHCP Subnet		
	Client Address Pools:			Select
	Client IPv6 Address Pools:			Select
	Default Group Policy			
	Group Policy:	AnyConnect_MGMT_Tunnel	٥	Manage
	(Following fields are linked	t to attribute of the group policy selected above.)		
	🗹 Enable SSL VPN clien	nt protocol		
	✓ Enable IPsec(IKEv2) of	client protocol		
	DNS Servers:			
	WINS Servers:			
	Domain Name:			
Find:		Next Previous		

Hinweis: Stellen Sie sicher, dass das Stammzertifikat der lokalen Zertifizierungsstelle (Certificate Authority, kurz "CA") auf der ASA vorhanden ist. Navigieren Sie zu Configuration > Remote Access VPN > Certificate Management > CA Certificates um das Zertifikat hinzuzufügen/anzuzeigen.

Hinweis: Stellen Sie sicher, dass ein Identitätszertifikat, das von derselben lokalen CA ausgestellt wurde, im Machine Certificate Store (unter Windows) und/oder in der Keychain-Verwaltung des Systems (unter macOS) vorhanden ist.

Schritt 8: Navigieren Sie zu Advanced > Group Alias/Group URL. Klicken Sie auf Add unter Group URLs und eine URL. Sicher Enabled ist aktiviert. Klicken Sie auf OK um zu speichern, wie im Bild gezeigt.

Add AnyConnect Connection Profile

Basic V Advanced General Client Addressing Authentication Secondary Authentication Authorization Accounting Group Alias/Group URL	 Enable the display of Radius Reject-Message on the login screen when authentication is rejected Enable the display of Securld 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.) Alias
	Croup 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 © Enabled Help Cancel OK

Wenn IKEv2 verwendet wird, stellen Sie sicher, IPsec (IKEv2) Access ist auf der für AnyConnect verwendeten Schnittstelle aktiviert.

O O Remote Access VPN	● ● ● ● Config	uration > Remote	e Access VPN > N	letwork (Client) A	Access > AnyConnect Co	inection Profiles			
Introduction Network (Client) Access AnyConnect Connection Profiles	The security Client suppo	security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN nt supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.							
S AnyConnect Customization/Local	Access Interfa	ces							
AnyConnect Client Profile	Second Cisco AnyConnect VPN Client access on the interfaces selected in the table below SSL access must be enabled if you allow AnyCongect client to be launched from a browser (Web Launch) .								
Group Policies	Interface	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Acce Allow Access	Enable Client Services	Device Certificate			
Psec(IEEv2) Connection Profiles Secure Mobility Solution Addrags Argingment	outside inside			0	Ø	Port Settings			

Schritt 9. Klicken Sie auf Apply um die Konfiguration an die ASA weiterzuleiten.



CLI-Konfiguration für das Verbindungsprofil (tunnel-group):

```
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 webvpn-attributes
authentication certificate
group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

Schritt 10. Stellen Sie sicher, dass ein vertrauenswürdiges Zertifikat auf der ASA installiert und an die für AnyConnect-Verbindungen verwendete Schnittstelle gebunden ist. Navigieren Sie zu Configuration > Remote Access VPN > Advanced > SSL Settings um diese Einstellung hinzuzufügen/anzuzeigen.

Hinweis: Weitere Informationen finden Sie unter <u>Installation des Identitätszertifikats auf der</u> <u>ASA</u>.

Remote Access VPN	○ ○ ○ Configuration > Remote Acces	s VPN > Advanced > SSL Settings				
Introduction	r					
Network (Client) Access	Configure SSL parameters. These para	meters affect both ASDM and SSL VPN acc	ess.			
AnyConnect Customization AnyConnect Client Profile	The minimum SSL version for the second	urity appliance to negotiate as a "server":	TLS V1	0	O DTLSV1 O DTLSV1.2	
AnyConnect Client Softwar	The minimum SSL version for the second	urity appliance to negotiate as a "client":	TLS V1	0		
Group Policies	Diffie-Hellman group to be used with	SSL:	Group2 - 1024-bit modulus	0		
IPsec(IKEv1) Connection P IPsec(IKEv2) Connection P	ECDH group to be used with SSL:		Group19 - 256-bit EC	0		
Secure Mobility Solution	Encountion					
Sp Address Assignment	cheryption				10.00.001	
Advanced	Cipher version	Cipher Security Level		Cipher Algorithm	s/ custom string	Edit
Clientless SSL VPN Access	Default	Medium		DES-CBC3-SHA	AES128-SHA DHE-KSA-AES128-SHA AES256-SHA DHE-KSA	
AAA/Local Users	TLSV1	Medium		DHE-RSA-AESZS	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
AAA Server Grouns	TLSV1.1	Medium		DHE-RSA-AESZ	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
Se LDAR Ancibude Man	TLSV1.2	Medium		ECDHE-ECDSA-	AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
	DTLSV1	Medium		DHE-RSA-AES2	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
I Local Users	DTLSV1.2	Medium		ECDHE-ECDSA-	AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
Secure Desktop Manager						
Certificate Management						
Language Localization						
Load Balancing						
DHCP Server	Server Name Indication (SNI)					
DNS	Domain		Certificate			Add
Advanced						
Connection Gateway						Edit
Reference Identity						Delete
Certificate to AnyConnect						
HTTP Redirect						
Maximum VPN Sessions						
Crypto Engine						
	Certificates					
	Specify which contificator if any of	ould be used for SSL authentication on ea	ch interface. The fallback contificate u	uill be used on interfs	car not prescipted with a cartificate of their own	
	specify which certificates, if any, si	iouid be used for SSL authentication on ea	ich interface. The fanback certificate v	vill be used on interra	ces not associated with a certificate of their own.	
under Cature	Interface	Primary Certificate	Load Balancing Certificate		Key-Type	Edit
evice Setup	inside					
innuall	management					
ineman.	outside	ROOT-CA:hostname=ASA.example	.co		Primary: RSA (2048 bits), Load Balancing: none	
emote Access VPN						
ite-to-Site VPN						
Device Management						
			(Charles) (Charles			

CLI-Konfiguration für SSL-Trustpoint:

ssl trust-point ROOT-CA outside

Erstellung des AnyConnect-Management-VPN-Profils

Schritt 1: Erstellen Sie das AnyConnect-Client-Profil. Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Klicken Sie auf Add, wie im Bild dargestellt.

	Home 🔏 Configuration 📴 Monitor	ing 🔚 Save 🔇 Refresh 🔇 Back 🕻	Forward 💡 Help Type topic Go			cisco
	O O Remote Access VPN	0 0 0 Configuration > Remote Acc	ess VPN > Network (Client) Access > AnyCon	nect Client Profile		
Bookmarks	Introduction ▼ IN Network (Client) Access ■ AnyConnect Connection Profil ■ AnyConnect Customization/LC ■ AnyConnect Client Software ■ AnyConnect Client Software ■ Dynamic Access Policies ■ Opmaric Access Policies	This panel is used to manage AnyCo button to add a new profile. Pressing The profile Usage field is introduced HostScan configuration can be perfo	nnect Client Profiles and perform group assignn the Import or Export button is for upload and with the Secure Mobility Solution. This field co rmed by going to Secure Desktop Manager/Hos Solicy	nent for AnyConnect version 2.5 or later.You can select fownload of client profiles between local machine and ntains different profile usage in AnyConnect version 3.0 tScan. If 'HostScan' is not visible under 'Secure Desktop e	a profile to edit, change group or to delete. You can select the 'Add' levice. • and later. Manager', you will need to restart ASDM.	
	Psec(IKEv1) Connection Profil	Profile Name	Profile IIrane	- Croup Policy	Brofile Location	
	Psec(KEv2) Connection Profil Secure Mobility Solution Ps. Address Assignment Standards Assignment Standards Assignment Add/tacsd Users Add/Local Users Standards Assever Groups Scure Desktop Manager DicCal Users Secure Desktop Manager DicCal Users Desktop Manager DicC Balancing DicC Server Standards DicS Settings	Profile Name	Prome usage	Liroup Policy	PTOINE LOCATION	
	Reference Wentity Certificate to AnyConnect and HTP Redirect Maximum VPN Sessions Crypto Engine Crypto Engine Remote Access VPN Firewall Certificate Sector VPN					
	Device Management			Reset Apply		

Schritt 2: Bieten Sie Profile Name. Wählen Sie Profile Usage als AnyConnect Management VPN profile. Wählen Sie Group Policy in <u>Schritt 1</u> erstellt. Klicken Sie auf OK, wie im Bild dargestellt.

ofile Name		Profile Usage	Group Policy		Profile Location
	• • •	Add AnyConnect Client P	Profile		
	Profile Name	AnyConnect_MGMT_Profile			
	Profile Usage	AnyConnect Management VPN Profile			
	Enter a device f created if it do	ile path for an xml file, ie. disk0:/ac_profile. The file es not exist.	will be automatically		
	Profile Location	disk0:/anyconnect_mgmt_profile.vpnm	Bro	vse Flash	
				Ipload	
	Group Policy	AnyConnect_MGMT_Tunnel	0		
		Enable 'Always On VPN' for selected group			
				_	
		Help Cancel	ОК		
			Reset Apply		

Schritt 3: Wählen Sie das erstellte Profil aus, und klicken Sie auf Edit, wie im Bild dargestellt.

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

Schritt 4: Navigieren Sie zu Server List. Klicken Sie auf Add um einen neuen Server-Listeneintrag hinzuzufügen, wie im Bild gezeigt.

* Someral	ict			
erences (Part 1)	IST			
Hostname Hostname Hostname Hostname	Host Address	User Group	Backup Server List	Certificate Pins
Note: at	most one server can be define	ed in a management VPI	N profile. Add Edit	Delete Details
•				

Schritt 5: Bieten Sie Display Name. Fügen Sie FQDN/IP address der ASA. Stellen Sie die User Group als Name der Tunnelgruppe. Group URL wird automatisch mit dem FQDN und User Group. Klicken Sie auf 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	Connection Information Primary Protocol SSL ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect KE Identity (IOS gateway only)
Backup Servers	
Host Address	Add
	Move Up Move Down Delete
ОК	Cancel

Hinweis: Die FQDN/IP-Adresse + Benutzergruppe muss mit der Gruppen-URL übereinstimmen, die bei der Konfiguration des AnyConnect-Verbindungsprofils in <u>Schritt 8</u> erwähnt wird.

Hinweis: AnyConnect mit IKEv2 als Protokoll kann auch zum Einrichten eines Management-VPNs zur ASA verwendet werden. Sicher Primary Protocol ist auf IPsec in <u>Schritt 5</u>.

Schritt 6: Klicken Sie wie in der Abbildung dargestellt auf OK zum Speichern.

🕘 🖶 Profile: AnyConnect MG	Any(Connect Client Profile Edit	or - AnyConnect_MGM	Γ_Profile	Abo
VPN	Server List				
Backup Servers Certificate Pinning Gertificate Matching Berver List	Hostname AnyConnect_MGMT	Host Address	User Group AnyConnect_MGMT_	Backup Server List	Certificate Pins
	Note: at most of	ne server can be defined	in a management VPN	profile. Add Edit	Delete Details
c					
		Help Ca	ncel OK		

Schritt 7. Klicken Sie auf Apply to Übertragen Sie die Konfiguration an die ASA, wie im Abbild dargestellt.

-	Home 🍫 Configuration 📴 Monitorin	g 🔚 Save 🔇 Refresh 🔇 Back 🔘	Forward 🖓 Help Type topic Go			CISCO
	O O O Remote Access VPN	○ ○ ○ Configuration > Remote Acces	s VPN > Network (Client) Access > AnyConnect Client	Profile		
ookmarks	Introduction Introduction Party Retwork (Client) Access AnyConnect Connection Profil MayConnect Clustomization/Lc AnyConnect Client Profile AnyConnect Client Software Dynamic Access Policies Dynamic Access Policies	This panel is used to manage AnyConn button to add a new profile. Pressing th The profile Usage field is introduced w HostScan configuration can be perform	Lect Client Profiles and perform group assignment for Any he Import or Export button is for upload and download of ith the Secure Mobility Solution. This field contains differ ed by going to Secure Desktop Manager/HostScan. If 'Ho	Connect version 2.5 or later.You can select a proi client profiles between local machine and device ent profile usage in AnyConnect version 3.0 and l stScan' is not visible under 'Secure Desktop Mana	ile to edit, change group or to delete. You can select the 'Add' ater. ger', you will need to restart ASDM.	
8	Group Policies IPser(IKEv1) Connection Profil	· Add S con 25 change Group For	cy Delete Miniport & Export & Vandate			
	IPsec(KEv2) Connection Profil IPsec(KEv2) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	_
	Secure Mobility Solution	AnyConnect_MGMT_Prohie	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0;/anyconnect_mgmt_profile.vpnm	
	Address Assignment					
	Advanced					
	Clientless SSL VPN Access					
	V Carl Users					
	AAA Server Groups					
	CDAP Attribute Map					
	Secure Deskton Manager					
	Certificate Management					
	B Language Localization					
	Sea Load Balancing					
	DHCP Server					
	and DNS					
	* Downeed					
	SSL Settings					
	Reference Identity					
	Certificate to AnyConnect and					
	HTTP Redirect					
	Maximum VPN Sessions					
	Su Crypto Engine					
	💑 Device Setup					
	🗊 Firewall					
	Remote Access VPN					
	Site-to-Site VPN					
	Device Management					
	ŝ			Reset Apply		

CLI-Konfiguration nach dem Hinzufügen des AnyConnect-Management-VPN-Profils.

```
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
1
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
 anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

AnyConnect-Management-VPN-Profil auf dem AnyConnect-Client-Computer:

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

<ShowPreConnectMessage>false</ShowPreConnectMessage>

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

--- Output Omitted ---

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

Hinweis: Wenn Trusted Network Detection (TND) im AnyConnect VPN-Benutzerprofil verwendet wird, ist es ratsam, die gleichen Einstellungen im VPN-Verwaltungsprofil vorzunehmen, um eine einheitliche Benutzererfahrung zu gewährleisten. Der Management-VPN-Tunnel wird auf Basis der TND-Einstellungen ausgelöst, die auf das Profil des Benutzer-VPN-Tunnels angewendet werden. Außerdem gilt die TND Connect-Aktion im Management-VPN-Profil (wird nur durchgesetzt, wenn der Management-VPN-Tunnel aktiv ist) immer für den Benutzer-VPN-Tunnel, um sicherzustellen, dass der Management-VPN-Tunnel für den Endbenutzer transparent ist.

Hinweis: Wenn auf einem Endbenutzer-PC im Management-VPN-Profil die TND-Einstellungen aktiviert sind und das Benutzer-VPN-Profil fehlt, werden die Standard-Voreinstellungseinstellungen für den TND (diese sind in den Standardeinstellungen in der AC-Client-Anwendung deaktiviert) anstelle des fehlenden Benutzer-VPN-Profils berücksichtigt. Diese Diskrepanz kann zu unerwartetem/undefiniertem Verhalten führen. Standardmäßig sind die TND-Einstellungen in den Standardeinstellungen deaktiviert. Um die hardcodierten Standardeinstellungen in der AnyConnect Client-Anwendung zu überwinden, müssen auf dem Endbenutzer-PC zwei VPN-Profile, ein Benutzer-VPN-Profil und ein AC-Management-VPN-Profil vorhanden sein. Beide müssen die gleichen TND-Einstellungen aufweisen.

Die Logik hinter der Verbindung und Trennung des Management-VPN-Tunnels besteht darin, dass der AC-Agent zum Einrichten eines Management-VPN-Tunnels die TND-Einstellungen für das Benutzer-VPN-Profil verwendet und zum Trennen der Verbindung zum Management-VPN-Tunnel nach TND-Einstellungen für das Management-VPN-Profil sucht.

Bereitstellungsmethoden für das AnyConnect-Management-VPN-Profil

• Eine erfolgreiche Benutzer-VPN-Verbindung wird mit dem ASA-Verbindungsprofil hergestellt, um das AnyConnect-Management-VPN-Profil vom VPN-Gateway herunterzuladen.

Hinweis: Wenn das Protokoll für den Management-VPN-Tunnel IKEv2 ist, muss die erste Verbindung über SSL hergestellt werden (um das AnyConnect-Management-VPN-Profil von der ASA herunterzuladen).

• Das AnyConnect Management VPN-Profil kann manuell auf die Client-Computer hochgeladen werden, entweder durch GPO-Push oder durch manuelle Installation (Stellen Sie sicher, dass der Name des Profils VpnMgmtTunProfile.xml).

Speicherort des Ordners, in dem das Profil hinzugefügt werden muss: Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun MacOS: /opt/cisco/anyconnect/profile/mgmttun/

(Optional) Konfigurieren eines benutzerdefinierten Attributs zur Unterstützung der Tunnel-All-Konfiguration

Management-VPN-Tunnel erfordern einen Split, der standardmäßig eine Tunneling-Konfiguration umfasst, um Auswirkungen auf die vom Benutzer initiierte Netzwerkkommunikation zu vermeiden. Dies kann überschrieben werden, wenn Sie das benutzerdefinierte Attribut in der Gruppenrichtlinie

konfigurieren, die von der Verwaltungstunnelverbindung verwendet wird.

Schritt 1: Navigieren Sie zuConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Klicken Sie auf Add, wie im Bild dargestellt.

	Home 🍓 Configuration 📴 Monitoring	Save 🗞 Refresh 🔇 Back 💭 Forward 🦻 Help Type topic Go	isco
	O O O Remote Access VPN	Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes	
5	2 Introduction	Declarations of custom attribute types and these attributes are enforced in ApyConnect group policy. ApyConnect dynamic access policy and ApyConnect custom attribute names	
š	🔻 💭 Network (Client) Access	becausions of earon activate types and and a activates we enforce in an experiment group party and experiment activate number number	
å	AnyConnect Connection Profiles		
	AnyConnect Customization/Localizati		
	AnyConnect Client Profile	Type Description	
arks	AnyConnect Client Software		
- s	Dynamic Access Policies		
8 B	Group Policies		
	IPsec(IKEv1) Connection Profiles		
	IPsec(IKEv2) Connection Profiles		
	Secure Mobility Solution		
	Address Assignment		
	Advanced		
	AnyConnect Essentials		
	AnyConnect Custom Attributes		
	AnyConnect Custom Attribute Nar	u.	
	▶ IB IPsec		
	23 ACL Manager		
	Clientless SSL VPN Access		
	AAA/Local Users		
	AAA Server Groups		
	CDAP Attribute Map		
	B Sarura Darkton Managar		
	Gartificate Manager		
	Language Localization		
	B Load Palancing		
	Courd balancing		
	B DNS		
	Advanced		
	- Contained		
	9 Durley Colum		
	Device Setup		
	📆 Firewall		
	Remote Access VPN		
	Site-to-Site VPN		
	Device Management		
	>	Reset Apply	
	•		

Schritt 2: Legen Sie das benutzerdefinierte Attribut Type auf ManagementTunnelAllAllowed und bieten eine Description. Klicken Sie auf OK, wie im Bild dargestellt.

			escription		
		De	escription		
•••	Create Custom /	Attribute Type			
• •	Create Custom /	Attribute Type			
• • • Type:	Create Custom / ManagementTunnelAllAllowed	Attribute Type			
Type:	Create Custom , ManagementTunnelAllAllowed ManagementTunnelAllAllowed	Attribute Type			
Type: Description:	Create Custom . ManagementTunnelAllAllowed ManagementTunnelAllAllowed	Attribute Type			
Type: Description:	Create Custom , ManagementTunnelAllAllowed ManagementTunnelAllAllowed	Attribute Type			

Schritt 3: Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Klicken Sie auf Add, wie im Bild dargestellt.



Schritt 4: Wählen Sie den Typ ManagementTunnelAllAllowed . Legen Sie den Namen fest als true. Klicken Sie auf Addum einen benutzerdefinierten Attributwert bereitzustellen, wie im Bild dargestellt.

Name Values		
• • •	Create Custom Attribute N	lame
Type: Name: Configure Values:	ManagementTunnelAllAllowed true Value	Contraction Manage
	Help Cancel	ОК

Schritt 5: Wert festlegen als true. Klicken Sie auf ok, wie im Bild dargestellt.

Type:	ManagementTunnelAllAll	lowed	0	Manage
Type.			•	
Name:	true			
	Value		Add	
•		Add Value	- P.	
true				
alua				
alue:				

Schritt 6: Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Wählen Sie die Gruppenrichtlinie aus. Klicken Sie auf Edit , wie im Bild dargestellt.

< Home 🦓 Configuration 📴 Monitoring 🔓	🕽 Save 🔇 Refresh 🔇 Back 🔘 Fo	rward 🂡 Help Type topic G	0	diala
COO Remote Access VPN	O O Configuration > Remote A	ccess VPN > Network (Client)	Access > Group Policies	
Introduction Network (Client) Access Network (Client) Access Access AnyConnect Connection Profiles AnyConnect Client Profile AnyConnect Client Profile	Manage VPN group policies.A VPN server. The group policy informati To enforce authorization attribute Add C Edit Delete 2	group is a collection of user-or ion is referenced by VPN connect is from an LDAP server you must Assign	iented authorization attribute/value pairs that ma ion profiles and user accounts. use an LDAP attribute map.	y be stored internally on the device or externally on a RADIUS/LDAP
Dynamic Access Policies	Name	Туре	Tunneling Protocol	Connection Profiles/Users
Search Group Policies	AnyConnect	Internal	ssl-client	AnyConnect
IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;DefaultADMINGroup;Def
IPsec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2;ssl-client	AnyConnect_MGMT_Tunnel
Secure Mobility Solution				
 Advanced AnyConnect Essentials AnyConnect Custom Attributes AnyConnect Custom Attributes AnyConnect Custom Attribute Names AnyConnect Custom Attributes AnyConnect Custom AnyConnect Custom Contribute Map Cond Users Contribute Map Advanced 				
Device Setup				
Firewall				
Remote Access VPN				
Site-to-Site VPN	Find:	Match Case		
Device Management			Reset Apply	

Schritt 7. Navigieren Sie, wie in dieser Abbildung dargestellt, zu Advanced > Split Tunneling. Konfigurieren Sie die Richtlinie als Tunnel All Networks.

• •		Edit Intern	nal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers	The VPN client makes split tunneling de fields.	cisions on the	e basis of a network list that can be specified below by providing the proper parameters to 'Policy' and	'Network Li:
Split Tunneling	DNS Names:	🗹 Inherit		
Browser Proxy ► AnyConnect Client ► IBcoc(KEul) Client	Send All DNS Lookups Through Tunnel:	Inherit	Yes ONO	
P IPSec(IKEV1) Client	Policy:	Inherit	Tunnel All Networks	
	IPv6 Policy:	🗹 Inherit	0	
	Network List:	🗹 Inherit	0	Manage
	Pressing this button to set up split exlu	sion for Web S	Security proxies.	
	Set up Split Exclusion for Web Securi	ty		
•	Intercept DHCP Configuration Message	from Microso	oft Clients	
Find:	🔘 Next	Previous		
			Help Cancel OK	

Schritt 8: Navigieren Sie zu Advanced > Anyconnect Client > Custom Attributes. Klicken Sie auf Add, wie im Bild dargestellt.

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers * Advanced Split Tunneling Browser Proxy * AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Customization Customization * IPsec(IKEv1) Client	Configuration of custom policy attributes. Ype Name of Value	
Find:	Next Previous	

Schritt 9. Wählen Sie den Attributtyp ManagementTunnelAllAllowed und wählen Sie den Wert als true. Klicken Sie auf OK, wie im Bild dargestellt.

De		Name of Va	lue
	Attribute type:	Create Custom Attribute ManagementTunnelAllAllowed	Manage
	Omit the value Oselect Value:	true	Manage
		Help Cancel OK	

Schritt 10. Klicken Sie auf Apply um die Konfiguration an die ASA weiterzuleiten (siehe Abbildung).

< Home 🗞 Configuration 📴 Mon	itoring 🔚 Save 🔇 Refresh 🔇 Back	Sorward ? Help Type topic Go			cisco			
000 Remote Access VPN	○ ○ ○ Configuration > Rep	mote Access VPN > Network (Client) Acc	ess > Group Policies					
Introduction Phetwork Client Access AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile AnyConnect Client Software AnyConnect Client Software	Manage VPN group policies policy information is refere localization to enforce authorization at Add C C Edit Dele	Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts. To enforce authorization attributes from an LDAP server you must use an LDAP attribute map. Add C C Edit Delete Assign						
2 By Group Policies	Name	Туре	Tunneling Protocol	Assigned To				
Psec(IKEv1) Connection Pro	AnyConnect offles Differentiate (functions Default	Internal	ssl-client	AnyConnect	our Defecter			
IPsec(IKEv2) Connection Pro	ofiles) Internal	ikev2;iztp-ipsec	Default/AGroup;Default/2EGroup;DefaultADMINGR	sup;DefaultwE			
 Address Assignment Advanced Cliendess SSL VPN Access Advanced LDP Artibute Map (LDP Artibute Map (LD								
S. Connell								
Firewall								
Remote Access VPN								
Site-to-Site VPN	Find:	Match Case						
Device Management	*		Reset Apply					

CLI-Konfiguration nach dem ManagementTunnelAllAllowed Benutzerdefiniertes Attribut wird hinzugefügt:

```
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
1
anyconnect-custom-data ManagementTunnelAllAllowed true true
1
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
```

Überprüfung

ASA# show vpn-sessiondb detail anyconnect

Überprüfen Sie die Management-VPN-Tunnelverbindung auf der ASA CLI mit dem show vpnsessiondb detail anyconnect aus.

```
Session Type: AnyConnect Detailed
Username
           : vpnuser
                                    Index
                                               : 10
Assigned IP : 192.168.10.1
                                    Public IP : 10.65.84.175
           : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
          : AnyConnect Premium
License
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-
256
Hashing
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx
           : 17238
                                    Bytes Rx : 1988
Pkts Tx
           : 12
                                    Pkts Rx
                                                : 13
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
           : 0h:11m:36s
Duration
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
--- Output Omitted ---
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	Bytes Rx	: 1988
Pkts Tx :	12	Pkts Rx	: 13
Pkts Tx Drop :	0	Pkts Rx Dro	p : 0

Überprüfen Sie die Management-VPN-Tunnelverbindung in ASDM.

Navigieren Sie zu Monitoring > VPN > VPN Statistics > Sessions (Überwachung > VPN > VPN-Statistik > Sitzungen). Filtern Sie nach AnyConnect-Client, um die Client-Sitzung anzuzeigen.

I Home 🦓 Configuration [I Mo	onitoring 📊 Save (ि Refresh 🔇 Bao	ck 🔘 Forward 💡	Help Type topic Go					cisco
Device List Bookmarks	000 Monitoring	> VPN > VPN Statis	stics > Sessions						
OOO Device List									
Add 🚺 Delete 🔊 Connect	Туре	Active		Cumulative	Peak Concurrent	t	Inactive		
ind: 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									
A O O VPN									
VPN Statistics	Filter By AnyCo	nnect Client	🗧 All S	essions ᅌ	Filte	er			
Sessions		Group Policy	Assigned IP Address	Protocol	Login Time	Bytes Tx	to a still day.	Audio	Details
	Username	Connection Profile	Public IP Address	Encryption	Duration	Bytes Rx	Inactivity	Audit :	Details
Compression Statistics	vpnuser	AnyConnect_MGMT	. 192.168.10.1	AnyConnect-Parent AnyConnect-Parent: (1)r	10:52:25 UTC .	34688	0h:00m:00s	c0a80	Logout
Encryption Statistics		phyconnece_monnt.		panyconnect rurent. (2)	1011C 1011.0 2111.3 23	00004			
Global IKE/IPsec Statistics									Ping
Protocol Statistics									
VLAN Mapping Sessions									
Clientless SSL VPN									
Shared SSL VPN									
VPN Connection Graphs									
SA Sessions									
Interfaces									
₩ VP <u>N</u>									
A Routing	To sort VPN sessio	ns, right-click on th	e above table and s	elect Table Sort Order fro	m popup menu.				
Sa Properties	Logout By: A	II Sessio ᅌ		Logout Sessions					

Überprüfen der Management-VPN-Tunnelverbindung auf dem Client-Computer:

Sisco AnyConnect Secure Mobil	ity Client	- 🗆 X	
cisco AnyCon	nect Secure Mobility Cl	ient	
Virtual Private Network (VPI	۷)	Diagnostics	
Preferences Statistics Route Detail	ls Firewall Message History		
Connection Information State: Tunnel Mode (IPv4): Tunnel Mode (IPv6): Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Disconnected Not Available Not Available Not Available Not Available 00:00:00 None Connected (asa.example.com)	Cisco AnyConnect Secure Mobility Client –	×
Address Information		-	
Client (IPv6): Client (IPv6): Server:	Not Available Not Available Not Available	\$ ()	alialia cisco
Bytes		• •	
	Rese	et Export Stats	

Fehlerbehebung

Die neue Statistikzeile Management Connection State (Management-Verbindungsstatus) in der Benutzeroberfläche kann verwendet werden, um Probleme mit der Management-Tunnelverbindung zu beheben. Die häufigsten Fehlerzustände sind:

Disconnected (disabled) (Verbindung getrennt (deaktiviert)):

- Die Funktion ist deaktiviert.
- Stellen Sie sicher, dass das Management-VPN-Profil auf dem Client über eine Benutzer-Tunnel-Verbindung (Sie müssen das Management-VPN-Profil der Benutzer-Tunnel-Gruppenrichtlinie hinzufügen) oder Out-of-Band über den manuellen Upload des Profils bereitgestellt wurde.
- Stellen Sie sicher, dass das Management-VPN-Profil mit einem einzelnen Hosteintrag konfiguriert ist, der eine Tunnelgruppe enthält.

Disconnected (trusted network) (Verbindung getrennt (vertrauenswürdiges Netzwerk)):

• TND hat ein vertrauenswürdiges Netzwerk erkannt, sodass der Management-Tunnel nicht eingerichtet wird.

Disconnected (user tunnel active) (Verbindung getrennt (Benutzertunnel aktiv)):

• Ein Benutzer-VPN-Tunnel ist derzeit aktiv.

Disconnected (process launch failed) (Verbindung getrennt (Prozess konnte nicht gestartet werden)):

• Fehler beim Starten des Prozesses beim Versuch, eine Management-Tunnelverbindung herzustellen.

Disconnected (connect failed) (Verbindung getrennt (Verbindung fehlgeschlagen)):

- Beim Herstellen des Verwaltungstunnels ist ein Verbindungsfehler aufgetreten.
- Stellen Sie sicher, dass die Zertifikatauthentifizierung in der Tunnelgruppe konfiguriert ist, kein Banner in der Gruppenrichtlinie vorhanden ist und das Serverzertifikat vertrauenswürdig sein muss.

Disconnected (invalid VPN configuration) (Verbindung getrennt (ungültige VPN-Konfiguration)):

- Eine ungültige Split-Tunneling-Konfiguration wurde vom VPN-Server empfangen.
- Überprüfen Sie die Split-Tunneling-Konfiguration in der Management-Tunnelgruppenrichtlinie.

Disconnected (software update pending) (Verbindung getrennt (Software-Updates ausstehend)):

• Ein AnyConnect-Software-Update steht derzeit aus.

Disconnected (Verbindung getrennt):

• Der Verwaltungstunnel steht kurz vor der Einrichtung oder kann aus anderen Gründen nicht eingerichtet werden.

Sammeln Sie DART zur weiteren Fehlerbehebung.

Zugehörige Informationen

- Konfiguration des Management-VPN-Tunnels
- Fehlerbehebung beim Management-VPN-Tunnel
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.