Konfigurieren von AnyConnect Secure Mobility Client mit Split-Tunneling auf einer ASA

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen AnyConnect-Lizenzinformationen Konfigurieren Netzwerkdiagramm ASDM AnyConnect-Konfigurationsassistent Split-Tunnel-Konfiguration Herunterladen und Installieren von AnyConnect Client Webbereitstellung Standalone-Bereitstellung **CLI-Konfiguration** Überprüfung Fehlerbehebung Installieren von DART Ausführen von DART Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie der Cisco AnyConnect Secure Mobility Client über Cisco Adaptive Security Device Manager (ASDM) auf einer Cisco Adaptive Security Appliance (ASA) konfiguriert wird, auf der die Softwareversion 9.3(2) ausgeführt wird.

Voraussetzungen

Anforderungen

Das Web-Bereitstellungspaket für Cisco AnyConnect Secure Mobility Client sollte auf den lokalen Desktop heruntergeladen werden, auf dem ASDM-Zugriff auf die ASA besteht. Wie Sie das richtige Client-Image für den Download auswählen, erfahren Sie auf der Webseite zu <u>Cisco</u> <u>AnyConnect Secure Mobility Client</u>. Die Web-Bereitstellungspakete können für verschiedene Betriebssysteme gleichzeitig auf die ASA hochgeladen werden.

Dies sind die Dateinamen für die Web-Bereitstellung bei den verschiedenen Betriebssystemen:

• Microsoft Windows-Betriebssysteme: AnyConnect-win-<version>-k9.pkg

- Macintosh-Betriebssysteme: AnyConnect-macosx-i386-<version>-k9.pkg
- Linux-Betriebssysteme: AnyConnect-linux-<version>-k9.pkg

Verwendete Komponenten

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

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

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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Dieses Dokument enthält schrittweise Anweisungen zur Verwendung des Cisco AnyConnect-Konfigurationsassistenten über ASDM, um den AnyConnect-Client zu konfigurieren und Split-Tunneling zu aktivieren.

Split-Tunneling wird in Szenarien verwendet, in denen nur bestimmter Datenverkehr getunnelt werden muss, im Gegensatz zu Szenarien, in denen der gesamte vom Client generierte Datenverkehr über das VPN fließt, wenn eine Verbindung besteht. Die Verwendung des AnyConnect-Konfigurationsassistenten führt standardmäßig zu einer *tunnel-all*-Konfiguration auf der ASA. Split-Tunneling muss separat konfiguriert werden, was im entsprechenden Abschnitt dieses Dokuments ausführlicher erläutert wird.

In diesem Konfigurationsbeispiel soll der Datenverkehr für das Subnetz 10.10.10.0/24 (das LAN-Subnetz hinter der ASA) über den VPN-Tunnel gesendet werden. Der gesamte übrige Datenverkehr vom Client-Computer wird über seine eigene Internetverbindung weitergeleitet.

AnyConnect-Lizenzinformationen

Hier finden Sie Links zu hilfreichen Informationen über die Cisco AnyConnect Secure Mobility Client-Lizenzen:

- Im Dokument <u>AnyConnect Secure Mobility Client Funktionen, Lizenzen und</u> <u>Betriebssysteme, Version 3.1</u> erfahren Sie, wie Sie die erforderlichen Lizenzen für AnyConnect Secure Mobility Client und die zugehörigen Funktionen ermitteln.
- Weitere Informationen zu AnyConnect Apex- und Plus-Lizenzen finden Sie in der Bestellanleitung für Cisco AnyConnect.

 Im Dokument <u>What ASA License Is Needed for IP Phone and Mobile VPN Connections?</u> (Welche ASA-Lizenz wird f
ür IP-Telefon- und mobile VPN-Verbindungen benötigt?) finden Sie Informationen
über die zusätzlichen Lizenzanforderungen f
ür IP-Telefon- und Mobilfunkverbindungen.

Konfigurieren

In diesem Abschnitt wird die Konfiguration von Cisco AnyConnect Secure Mobility Client auf der ASA beschrieben.

Netzwerkdiagramm

Dies ist die Topologie, die für die Beispiele in diesem Dokument verwendet wird:



ASDM AnyConnect-Konfigurationsassistent

Der AnyConnect-Konfigurationsassistent kann verwendet werden, um AnyConnect Secure Mobility Client zu konfigurieren. Stellen Sie sicher, dass ein AnyConnect-Client-Paket in den Flash-Speicher oder auf die Festplatte der ASA-Firewall hochgeladen wurde, bevor Sie fortfahren.

Führen Sie die folgenden Schritte aus, um AnyConnect Secure Mobility Client über den Konfigurationsassistenten zu konfigurieren:

1. Melden Sie sich bei ASDM an, starten Sie den Konfigurationsassistenten (**Configuration Wizard**), und klicken Sie dann auf **Next** (Weiter):

Cisco ASDM 7.3 fr	for ASA - 10.106.44.21	NUMBER OF TAXABLE
<u>File View T</u> ools	Wizards Window Help	
🌀 Home 🗞 ConFig	, Startup Wizard	
Device List	VPN Wizards Site-to-site VPN Wizard	
🔹 Add 📋 Delete 🔮	High Availability and Scalability Wizard	iboard
Find:	Unified Communication Wizard	
- 월 10,106,44.3 - 월 10,106,44.21	ASDM Identity Certificate Wizard [Psec (KEvd) Remote Access VPN Wizard	
_	Packet Capiture Wizard EdgeASA-4	
	ASA Version: 9.3(2) (ASDM Version: 7.3(1)101 (Firewall Mode: Routed (Cevice Uptime: 0d 16h 15m 5s Cevice Type: ASA 5525 Context Mode: Single
	Environment Status : 🗣 OK 🔅	Total Flash: 8192 MB

2. Geben Sie unter *Connection Profile Name* (Verbindungsprofilname) den Namen ein, wählen Sie im Dropdown-Menü *VPN Access Interface* (VPN-Zugriffsschnittstelle) die Schnittstelle aus, an der das VPN terminiert wird, und klicken Sie dann auf **Next** (Weiter):

1	AnyConnect VPN Connect	ection Setup Wizard				X	
	Steps	Connection Profile Identific	ation				
l	1. Introduction	This step allows you to configure a Connection Profile Name and the Interface the remote access users will					
	2. Connection Profile	access for VPN connections.					
I	Identification	Connection Profile Name:	SSLClient				
I.	3. VPN Protocols						
l	Client Images	VPN Access Interface:	outside	•			
	5. Authentication Methr						

3. Aktivieren Sie das Kontrollkästchen SSL, um SSL (Secure Sockets Layer) zu aktivieren. Unter *Device Certificate* (Gerätezertifikat) können Sie ein von einer vertrauenswürdigen Zertifizierungsstelle (z. B. Verisign oder Entrust) ausgestelltes Zertifikat oder ein selbstsigniertes Zertifikat angeben. Wenn das Zertifikat bereits auf der ASA installiert ist, kann es über das Dropdown-Menü ausgewählt werden. Anmerkung: Dieses Zertifikat ist das serverseitige Zertifikat, das bereitgestellt wird. Wenn derzeit keine Zertifikate auf der ASA installiert sind und ein selbstsigniertes Zertifikat generiert werden muss, klicken Sie auf Manage (Verwalten).Um ein Drittanbieterzertifikat zu installieren, führen Sie die Schritte aus, die im Dokument ASA 8.x Manually Install 3rd Party Vendor Certificates for use with WebVPN Configuration Example (ASA 8.x – manuelle Installation von Drittanbieterzertifikaten zur Verwendung mit dem WebVPN-Konfigurationsbeispiel) von Cisco beschrieben sind.

	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.					
l	3. VPN Protocols	SSL					
	4. Client Images	IPsec					
	5. Authentication Meth	Device Certificate					
	 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					
	8. NAT Exempt						
1	0 in Connect Client						

4. Klicken Sie auf Add (Hinzufügen):

🔁 Any	Connect VPN C	onnection Set	tup Wizard				B-20	Х
Ste	🔄 Manage Ider	ntity Certificat	tes				X	
1. 2.	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add	icol
3.							Show Details	
4.							Delete	
5.							Export	
6.							Install	
7.	Eind:		00	Match Case				

5. Geben Sie im Feld *Trustpoint Name* (Trustpoint-Name) einen geeigneten Namen ein, und klicken Sie dann auf die Optionsschaltfläche Add a new identity certificate (Neues Identitätszertifikat hinzufügen). Wenn auf dem Gerät keine RSA-Schlüsselpaare (Rivest-Shamir-Addleman) vorhanden sind, klicken Sie auf New (Neu), um eines zu generieren:

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 certification	cate:
Key Pair:	<default-rsa-key> ▼ Show New</default-rsa-key>
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

6. Klicken Sie auf die Optionsschaltfläche Use default key pair name (Standard-Schlüsselpaarnamen verwenden), oder klicken Sie auf die Optionsschaltfläche Enter new key pair name (Neuen Schlüsselpaarnamen eingeben), und geben Sie einen neuen Namen ein. Wählen Sie die Größe für die Schlüssel aus, und klicken Sie dann auf Generate Now (Jetzt generieren):

5	Add Key F	Pair
	Кеу Туре:	RSA CDSA
	Name:	 Ose default key pair name Enter new key pair name: sslcert
	Size:	2048
	Usage:	General purpose Special
		Generate Now Cancel Help

7. Nachdem das RSA-Schlüsselpaar generiert wurde, wählen Sie den Schlüssel aus, und aktivieren Sie das Kontrollkästchen Generate self-signed certificate (Selbstsigniertes Zertifikat generieren). Geben Sie im Feld *Certificate Subject DN* (Subject-DN des Zertifikats) den gewünschten Subject-Domänennamen (DN) ein, und klicken Sie dann auf Add Certificate (Zertifikat hinzufügen):

Add Identity Certificate		×
Trustpoint Name:	SelfsignedCert	
O Import the identity certific	cate from a file (PKCS12 format with Cer	tificate(s)+Private Key):
Decryption Passphrase:		
File to Import From:		Browse
Add a new identity certification	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 certifi	cates to TLS-Proxy
		Advanced
Add Cer	tificate	Help

8. Sobald die Registrierung abgeschlossen ist, klicken Sie auf **OK**, erneut auf **OK** und dann auf **Next** (Weiter):

🔄 An	yConnect VPN Co	nnection Set	up Wizard				
Ste	🛐 Manage Iden	tity Certificat	es				X
1. 2.	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
з.	hostname	hostname	16:39:40 M	SelfsignedCert	Gener	RSA (2048 bits)	Show Details
4.							Delete
5.							Export
6.							Install
7	Eind:		00	Match Case			
	Public CA Enrol	lment —					
8.	Get your Cisc Entrust, Entru	o ASA secur Jst offers Cis	ity appliance up co customers a	and running quickly with special promotional price	an SSL A for certif	dvantage digital cer îcates and trial certi	tificate from ificates for testing.
9.			E	nroll ASA SSL certificate v	vith Entru	st	
10	Using a prev	iously saved	certificate sign	ing request, <u>enroll with En</u>	itrust.		
			Ok	Cancel		lelp	

9. Klicken Sie auf Add (Hinzufügen), um das AnyConnect Client-Image (die PKG-Datei) vom PC oder aus dem Flash-Speicher hinzuzufügen. Klicken Sie auf Browse Flash (Flash durchsuchen), um das Image vom Flash-Laufwerk hinzuzufügen, oder klicken Sie auf Upload (Hochladen), um das Image direkt vom Host-Computer hinzuzufügen:

5. Authentication Methr	🗣 Add 📝 Rep	lace 📋 Delete 🗲 🗲			
6. Client Address Assignment	Add AnyConne	ct Client Image			x
7. Network Name Resolution Servers	AnyConnect Imag	e:	E	Prowse Flas	n
8. NAT Exempt				Upload	
9. AnyConnect Client Deployment	Regular expre	ssion to match user-agent			۲
10. Summary		OK Cancel He	lp		
					Y
Browse Flash					~
Folders		Files			
l ⊡		FileName	Size (Date	
 iog crypto_archive coredumpinfo snmp tmp 					
		anyconnect-win-3.1.05152-k9.pkg	35,167,	12/17/	
		anyconnect-win-3.1.06073-k9.pkg	38,048,	01/02/	
		asa932-smp-k8.bin	63,479,	01/02/	
in a cub			10.004	11/00/	

10. Sobald das Image hinzugefügt wurde, klicken Sie auf Next (Weiter):

🕈 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>Cisc</u> <u>here</u> .	o by searching 'AnyConnect VPN Client' or <u>click</u>			
< Back Next >	Cancel Help			

 Die Benutzerauthentifizierung kann über die AAA-Servergruppen (Authentication, Authorization, and Accounting) abgeschlossen werden. Wenn die Benutzer bereits konfiguriert sind, wählen Sie LOCAL (LOKAL) aus, und klicken Sie dann auf Next (Weiter). Anmerkung: In diesem Beispiel ist LOCAL (LOKAL) für die Authentifizierung konfiguriert. Das bedeutet, dass die lokale Benutzerdatenbank auf der ASA für die Authentifizierung verwendet

wird.	×					
AnyConnect VPN Connection Setup Wizard						
AnyConnect VPN Co Steps I. Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods Client Address Assignment Network Name	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 Local User Database Details User to be Added Username: User1 Add >>					
Resolution Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	Confirm Password:					
	< Back Next > Cancel Help					

12. Der Adresspool f
ür den VPN-Client muss konfiguriert werden. Wenn er bereits konfiguriert ist, w
ählen Sie ihn aus dem Dropdown-Men
ü aus. Wenn nicht, klicken Sie auf New (Neu), um einen neuen zu konfigurieren. Klicken Sie anschlie
ßend auf Next (Weiter):

D. VENTEROUCOIS		
4. Client Images	IP v4 Address Pool IP v6 Address Pool	
5. Authentication Meth	Address Pool: Select 🔻 New	
6. Client Address Assignment	Details of 🔁 Add IPv4 Pool	X
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: 255.255.25.0	•
	OK Cancel Help	

13. Geben Sie in den Feldern *DNS* und *Domain Name* (Domännename) die DNS-Server und DNs ein, und klicken Sie dann auf **Next** (Weiter):

Steps	Network Name R	lesolution Servers	
1. Introduction	This step lets yo	u specify how domain names are resolved for the remote user wh	en accessing the internal
2. Connection Profile Identification	network.		
3 VPN Protocols	DNS Servers:	10.10.10.23	
4. Climb Images	WINS Servers:		
4. Client Images			
5. Authentication Metho	Domain Name:	Cisco.com	

14. In diesem Szenario soll der Zugriff über das VPN auf das Netzwerk **10.10.10.0/24** beschränkt werden, das als *internes* (oder LAN-)Subnetz hinter der ASA konfiguriert ist. Der Datenverkehr zwischen dem Client und dem internen Subnetz muss von jeglicher dynamischer NAT (Network Address Translation) ausgenommen sein.

Aktivieren Sie das Kontrollkästchen **Exempt VPN traffic from network address translation** (VPN-Datenverkehr von NAT ausnehmen), und konfigurieren Sie die LAN- und WAN-Schnittstellen, die für die Ausnahme verwendet werden sollen:

2. Connection Profile Identification	Exempt VPN traffic 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 Meth	Local Network is the network address(es) of the internal network that client
6. Client Address Assignment	Local Network: any
7. Network Name Resolution Servers	
8. NAT Exempt	The traffic between AnyConnect client and internal network will be exempt from network address translation.
9. AnyConnect Client	

15. Wählen Sie die lokalen Netzwerke aus, die ausgenommen sein sollen:

A						Filteric	lea
Name	1	IP Address	Netmask	Description	Obje	ct NAT Add	łr
E-IPv4 Ne	etwork O	bjects					
- 🏈 a	any	,					
je je	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				
E IPv4 Ne	etwork O	bject Groups					
E 📰 /	ANY						
🕀 🔛	OBJ_L						
🕀 🔛 🔁	OBJ_S						
🖻 Interfa	ices						
	Inside						
	outside						
Selected L	outside .ocal Net	work	-notwork /24				
Selected L	outside .ocal Net	work	-network/24				
Selected L Loca	outside .ocal Net I Network	work <-> Inside	-network/24		OK	Ca	ince
Selected L Loca	outside .ocal Net I Network	work Inside	-network/24			Ca	ince
Selected L Loca	outside .ocal Net I Network	work <-> Inside	-network/24 vork is the network addr	ess(es) of the internal net	OK work that client	Ca	ince
Selected L Loca Authenticati	outside .ocal Net I Network	work <-> Inside Local Netw can access Local Netw	r-network/24 vork is the network addr vork: 10.10.10.0/24	ess(es) of the internal net	OK work that client		ince
Authenticati Client Addres Assignment Network Na Resolution S	outside .ocal Net I Network I Network	work <-> Inside Local Network Local Network Local Network	r-network/24	ess(es) of the internal net	OK work that client		ince
Authenticati Client Addre Assignment Network Na Resolution S NAT Exempt	ion Metho ion Metho Servers pt	work <-> Inside Local Netw can access Local Netw The traffic from netw	-network/24 vork is the network addr vork: 10.10.10.0/24 between AnyConnect cl ork address translation.	ess(es) of the internal net	OK work that client		ince

16. Klicken Sie auf **Next** (Weiter), erneut auf **Next** (Weiter) und dann auf **Finish** (Fertigstellen). Die AnyConnect-Client-Konfiguration ist jetzt abgeschlossen. Wenn Sie AnyConnect jedoch über den Konfigurationsassistenten konfigurieren, wird die *Split-Tunnel*-Richtlinie standardmäßig als **Tunnelall** konfiguriert. Um nur bestimmten Datenverkehr zu tunneln, muss *Split-Tunneling* implementiert werden.

Anmerkung: Wenn Split-Tunneling nicht konfiguriert ist, wird die Split-Tunnel-Richtlinie von der Standardgruppenrichtlinie (DfltGrpPolicy) übernommen, die standardmäßig auf **Tunnelall** festgelegt ist. Das heißt, sobald der Client über VPN verbunden ist, wird der gesamte Datenverkehr (einschließlich des Datenverkehrs zum Web) über den Tunnel gesendet.

Nur der Datenverkehr, der für die ASA-WAN-IP-Adresse (*extern*) bestimmt ist, umgeht das Tunneling auf dem Client-Computer. Dies ist der Ausgabe des Befehls **route print** auf Microsoft Windows-Computern zu entnehmen.

Split-Tunnel-Konfiguration

Split-Tunneling ist eine Funktion, die Sie verwenden können, um den Datenverkehr für die zu verschlüsselnden Subnetze oder Hosts zu definieren. Dies umfasst die Konfiguration einer Zugriffskontrollliste (Access Control List, ACL), die dieser Funktion zugeordnet werden soll. Der in dieser ACL definierte Datenverkehr für die Subnetze oder Hosts wird vom Client-Ende über den Tunnel verschlüsselt, und die Routen für diese Subnetze werden in der PC-Routing-Tabelle eingetragen.

Führen Sie die folgenden Schritte aus, um von der *Tunnel-all*-Konfiguration zur *Split-Tunnel*-Konfiguration zu wechseln:

Navigieren Sie zu Configuration > Remote Access VPN > Group Policies (Konfiguration > RAS-VPN > Gruppenrichtlinien):



2. Klicken Sie auf Edit (Bearbeiten), und verwenden Sie die Navigationsstruktur, um zu Advanced > Split Tunneling (Erweitert > Split-Tunneling) zu navigieren. Deaktivieren Sie im Abschnitt *Policy* (Richtlinie) das Kontrollkästchen Inherit (Übernehmen), und wählen Sie im Dropdown-Menü die Option Tunnel Network List Below (Tunnel-Netzwerkliste unten) aus:



3. Deaktivieren Sie im Abschnitt Network List (Netzwerkliste) das Kontrollkästchen Inherit (Übernehmen), und klicken Sie auf Manage (Verwalten), um die ACL auszuwählen, die die LAN-Netzwerke angibt, auf die der Client zugreifen können muss:

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. Klicken Sie auf **Standard ACL > Add > Add ACL > ACL name** (Standard-ACL > Hinzufügen > ACL hinzufügen > ACL-Name):

General Servers Advanced	The VPN	Client m	nakes solit tunneling decisions on the basis of a network list that can b Manager	e specif
Split Tunneling	DIVS IN			
Browser Proxy	Send	Stand	dard ACL Extended ACL	
IPsec(IKEv1) Client		🗣 Ac	dd 🕶 🗃 Edit 📋 Delete 🛧 🎸 👗 ங 🛍 -	
	Policy	No	Address Action Description	
	Netwo		Add ACL	
	Pressi Set		ACL Name: Split-ACL	
	Inte		OK Cancel Help	

5. Klicken Sie auf Add ACE (ACE hinzufügen), um die Regel hinzuzufügen:

ACL Man	lager			
Standard	ACL Extended ACL			
🗣 Add 🚽	🗹 Edit 前 Delete 🛛 🛧 🦂	f % 🖻 🛍	1 -	
No	Address	Action	Description	
Split-A	CL			
🔤 Add A	ACE			
Action:	💿 Permit 🛛 🔘 Deny			
Address	s: <u>10.10.10.0/24</u>			
Descrip	tion:			

6. Klicken Sie auf OK.

📵 Edit Internal Group Policy	: GroupPolicy_SSLClient	7-		X			
-Ceneral -Eervers	The VIN cleant makes split tometing decisions on the base of a network ust that can be specified below by providing the proper parameters to "toticy" and "Network test" fa						
i⊒>dranced Solt Turne Ing	DNE Names:	🛛 Inherit					
—Browser Proxy H-AnyConnect Client H-IPsec(KByt) Client	Send All DRS Loci ups Through Tunnel:	🔽 Interit	© YES ⊙No				
	Poloyi	🗌 Inherit	Turnel Network List Selow 👻				
	Network List:	🗐 Inherit	9515-401 · · · · · · · · · · · · · · · · · · ·	Manage			
	Pressing this butch to set up colities/us Extup Spirit Est Asian for Web Baruri Intercept CHCP Configuration Mes	on for Web S V	iecurty protes ficrosoft Clients	8			

7. Klicken Sie auf Apply (Anwenden).

Sobald die Verbindung hergestellt ist, werden die Routen für die Subnetze oder Hosts in der geteilten ACL zur Routing-Tabelle des Client-Computers hinzugefügt. Auf Microsoft Windows-Computern ist dies der Ausgabe des Befehls **route print** zu entnehmen. Der nächste Hop für diese Routen ist eine IP-Adresse aus dem Client-IP-Pool-Subnetz (normalerweise die erste IP-Adresse des Subnetzes):

C:\Users\admin>route print IPv4 Route Table Active Routes: Network Destination Netmask Gateway Interface Metric 0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261 10.10.10.0 255.255.255.0 10.10.11.2 10.10.11.1 2 *!! This is the split tunnel route*. 10.106.44.0 255.255.255.0 on-link 10.106.44.243 261 172.16.21.1 255.255.255.0 on-link 10.106.44.243 6

!! This is the route for the ASA Public IP Address. Geben Sie auf Computern mit macOS den Befehl **netstat -r** ein, um die PC-Routing-Tabelle anzuzeigen: 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.

Herunterladen und Installieren von AnyConnect Client

Es gibt zwei Methoden, um Cisco AnyConnect Secure Mobility Client auf dem Benutzercomputer bereitzustellen:

- Webbereitstellung
- Standalone-Bereitstellung

Beide Methoden werden in den folgenden Abschnitten ausführlicher erläutert.

Webbereitstellung

Um die Webbereitstellungsmethode zu verwenden, geben Sie auf dem Client-Computer in einem Browser die URL https://<ASA's FQDN>or<ASA's IP> ein. So gelangen Sie zur *WebVPN*-Portalseite.

Anmerkung: Wenn Sie Internet Explorer (IE) verwenden, erfolgt die Installation hauptsächlich über ActiveX, es sei denn, Sie sind gezwungen, Java zu verwenden. Bei allen anderen Browsern wird Java genutzt.

Nach der Anmeldung auf der Seite sollte die Installation auf dem Client-Computer beginnen, und der Client sollte sich nach Abschluss der Installation mit der ASA verbinden.

Anmerkung: Möglicherweise werden Sie aufgefordert, die Berechtigung zur Ausführung von ActiveX oder Java zu erteilen. Diese Berechtigung ist erforderlich, um die Installation fortzusetzen.

	Logon
Group	SSLClient 🔻
Username	
Password	
	Logon

C States: 172.16.21.1/CACHE/stc/1/index.html

cisco AnyC	onnect Secure Mobility Client
WebLaunch Platform Detection ActiveX	Attempting to use Java for Installation Sun Java applet has started. This could take up to 60 seconds. Please wait
Java Detection Java Jownload Connected	Help Download

Standalone-Bereitstellung

Führen Sie die folgenden Schritte aus, um die Standalone-Bereitstellungsmethode zu verwenden:

- Laden Sie das AnyConnect Client-Image von der Cisco Website herunter. Wie Sie das richtige Image für den Download auswählen, erfahren Sie auf der Webseite zu <u>Cisco</u> <u>AnyConnect Secure Mobility Client</u>. Auf dieser Seite wird ein Download-Link bereitgestellt. Navigieren Sie zur Download-Seite, und wählen Sie die entsprechende Version aus. Führen Sie eine Suche nach dem vollständigen Installationspaket - Windows/Standalone installer (ISO) durch. Anmerkung: Anschließend wird ein ISO-Installations-Image heruntergeladen (z. B. anyconnect-win-3.1.06073-pre-deploy-k9.iso).
- 2. Verwenden Sie WinRar oder 7-Zip, um den Inhalt des ISO-Pakets zu extrahieren:

anyconnect-win-31.070	-			
anjconnect win-5.1.070		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. Sobald der Inhalt extrahiert wurde, führen Sie die Datei **Setup.exe** aus, und wählen Sie die Module aus, die zusammen mit Cisco AnyConnect Secure Mobility Client installiert werden müssen.

Tipp: Wenn Sie zusätzliche Einstellungen für das VPN konfigurieren möchten, lesen Sie den Abschnitt zum <u>Konfigurieren von AnyConnect VPN-Client-Verbindungen</u> im *Konfigurationsleitfaden für die Cisco ASA 5500-Serie mit CLI, 8.4 und 8.6.*

CLI-Konfiguration

Dieser Abschnitt enthält die CLI-Konfiguration für Cisco AnyConnect Secure Mobility Client zu Referenzzwecken.

```
ASA Version 9.3(2)
1
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
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
!
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-sha1 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 1 class-map inspection_default match default-inspection-traffic 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 xdmcp 1 service-policy global_policy global

```
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0 : end
```

Überprüfung

Führen Sie diese Schritte aus, um die Client-Verbindung und die verschiedenen Parameter zu überprüfen, die dieser Verbindung zugeordnet sind:

1. Navigieren Sie in ASDM zu Monitoring > VPN (Überwachung > VPN):



 Sie können die Option Filter by (Filtern nach) verwenden, um den VPN-Typ zu filtern. Wählen Sie im Dropdown-Menü AnyConnect Client und alle AnyConnect Client-Sitzungen aus. Tipp: Die Sitzungen können mit den anderen Kriterien wie Username (Benutzername) und IP address (IP-Adresse) weiter gefiltert werden

werden.							
VPN 27 4	Filter By: AnyO	ennact Cliant 🔹 🔻	Al Sessions	•	Eltar		
- VPN Cluster Loads	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 DE/IPsec Statistics NAC Session Summary	cisco	CroupPolicy_SSUCtion SSUCtions	16,16,11,1 172,15,21	AnyConnect-Farent SSI-Tunnel AnyConnect-Farent (I)none S.	. 16 58:56 UTC . Dh. 12m:55a	. 11472 22738	01.00m:00s
Protocol Statistics VLAN Mapping Sessions Clambers SSL VFN							
WSA Sessions							
A VEN							

3. Doppelklicken Sie auf eine Sitzung, um weitere Details zu dieser Sitzung abzurufen:

lana		Group Policy	Assigned IP Address	Protocol		Login Time	Bytes Tx	Terre	45
,68	name	Connection Profile Public IP Address		Encryption		Duration	Bytes Rx	Inac	unity
900	co GroupPolicy_SSLClien 10.10.11.1 SSLClient 172.16.21.1		AnyConnect-Parent SEL-Tunnel . 16:58:56 UTC 1147 AnyConnect-Parent: (1)none S., Oh:21m:09s 2665			11472 26653	0h:0	Dm:0Ds	
eta	ails ACL	Local Addr. / Subnet N Remote Addr. / Schnet	Ask / Protocol / Port Mask / Protocol / Port	Encryption	Other		Bytes Tx Bytes Ry		More
	AnyConn			none	Tunnel ID: 14.1 Public IP: 172.16.2 Hashing: none TCP Src Port 5782 TCP Dst Port 443 Authentication Mo Idle Time Out: 30 Idle TO Left: 9 Mil Client OS Type: W	21.1 29 de: userPassword Minutes nutes Vindows	5954 1046	• 11	

 Geben Sie in die CLI den Befehl show vpn-sessiondb anyconnect ein, um die Sitzungsdetails abzurufen:

```
# 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. Sie können die anderen Filteroptionen verwenden, um die Ergebnisse zu verfeinern:

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 ID : 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 Bytes Tx : 0 Bytes Rx : 4150 Pkts Tx : 0 Pkts Rx : 59 Pkts Tx Drop : 0 Pkts Rx Drop : 0

Fehlerbehebung

Sie können das AnyConnect-Diagnose- und Reporting-Tool (DART) verwenden, um die Daten zu erfassen, die zur Behebung von AnyConnect-Installations- und Verbindungsproblemen nützlich sind. Der DART-Assistent wird auf dem Computer verwendet, auf dem AnyConnect ausgeführt wird. DART stellt die Protokolle, Status und Diagnoseinformationen für die Analyse durch das Cisco Technical Assistance Center (TAC) zusammen. Für die Ausführung von DART auf dem Client-Computer sind keine Administratorrechte erforderlich.

Installieren von DART

Führen Sie diese Schritte aus, um DART zu installieren:

- Laden Sie das AnyConnect Client-Image von der Cisco Website herunter. Wie Sie das richtige Image für den Download auswählen, erfahren Sie auf der Webseite zu <u>Cisco</u> <u>AnyConnect Secure Mobility Client</u>. Auf dieser Seite wird ein Download-Link bereitgestellt. Navigieren Sie zur Download-Seite, und wählen Sie die entsprechende Version aus. Führen Sie eine Suche nach dem vollständigen Installationspaket - Windows/Standalone installer (ISO) durch. Anmerkung: Anschließend wird ein ISO-Installations-Image heruntergeladen (z. B. anyconnect-win-3.1.06073-pre-deploy-k9.iso).
- 2. Verwenden Sie WinRar oder 7-Zip, um den Inhalt des ISO-Pakets zu extrahieren:

Burn disc image 7-Zip Open archive Edit with Notepad++ Open archive Open with Extract files	(a)			
7-Zip Open archive Edit with Notepad++ Open archive Open with Extract files	anyconnect-win-3.1.070.	Burn disc image		1
Edit with Notepad++ Open archive Open with Extract files		7-Zip	×	Open archive
Open with Extract files		Edit with Notepad++		Open archive
		Open with	•	Extract files
Share with Extract Here		Share with		Extract Here
Extract to "anyconnect-win-3.1.07021-pre-deploy-k9\"				Extract to "anyconnect-win-3.1.07021-pre-deploy-k9\"

- 3. Navigieren Sie zu dem Ordner, in den der Inhalt extrahiert wurde.
- 4. Führen Sie die Datei **Setup.exe** aus, und wählen Sie nur **AnyConnect Diagnostic And Reporting Tool** aus:



Ausführen von DART

Hier einige wichtige Informationen, die Sie vor der Ausführung von DART beachten sollten:

- Das Problem muss mindestens einmal reproduziert werden, bevor Sie DART ausführen.
- Das Datum und die Uhrzeit auf dem Benutzercomputer müssen notiert werden, wenn das Problem erneut auftritt.

Führen Sie DART über das Startmenü auf dem Client-Computer aus:



Sie können als Modus entweder *Default* (Standard) oder *Custom* (Benutzerdefiniert) auswählen. Cisco empfiehlt, DART im Standardmodus auszuführen, damit alle Informationen auf einmal erfasst werden können.

Cisco DART 3.1.05170	X			
Bundle Creation Option	0			
Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.	1			
 Default (Bundle will be saved to Desktop) 				
Custom				
Clear logs after DART finshes				
Back Next Ca	ancel			

Nach Abschluss des Vorgangs speichert das Tool die *ZIP*-Datei mit dem DART-Paket auf dem Client-Desktop. Das Paket kann dann zur weiteren Analyse per E-Mail an das TAC gesendet werden (nachdem Sie einen TAC-Fall erstellt haben).

Zugehörige Informationen

- <u>Fehlerbehebungsleitfaden für AnyConnect VPN-Client häufige Probleme</u>
- Java 7 Probleme mit AnyConnect, CSD/Hostscan und WebVPN Leitfaden zur Fehlerbehebung
- 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.