ASA でのスプリット トンネリングによる AnyConnect セキュア モビリティ クライアント の設定

内容

概要 前提条件 要件 使用するコンポーネント 背景説明 AnyConnect のライセンス情報 設定 ネットワーク図 ASDM AnyConnect 構成ウィザード Split-tunnel 設定 AnyConnect クライアントのダウンロードとインストール <u>Web</u> 展開 スタンドアロンでの導入 CLI での設定 確認 トラブルシュート DART のインストール DART の実行 関連情報

概要

このドキュメントでは、ソフトウェア バージョン 9.3(2) を実行する Cisco 適応型セキュリティ アプライアンス(ASA)の Cisco Adaptive Security Device Manager(ASDM)で Cisco AnyConnect セキュア モビリティ クライアントを設定する方法について説明します。

前提条件

要件

Cisco AnyConnect セキュア モビリティ クライアントの Web 展開パッケージは、ASA への ASDM アクセスが可能なローカルデスクトップにダウンロードする必要があります。クライアン トパッケージをダウンロードするには、<u>Cisco AnyConnect セキュア モビリティ クライアントの</u> <u>Web ページを参照してください。</u>さまざまなオペレーティングシステム(OS)用の Web 展開パ ッケージを ASA に同時にアップロードできます。

各種 OS 用の Web 展開ファイルの名前は次のとおりです。

- Microsoft Windows OS : AnyConnect-win-<version>-k9.pkg
- Macintosh (MAC) OS : AnyConnect-macosx-i386-<version>-k9.pkg
- Linux OS : AnyConnect-linux-<version>-k9.pkg

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA バージョン 9.3(2)
- ASDM バージョン 7.3(1)101

• AnyConnect バージョン 3.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

背景説明

このドキュメントでは、AnyConnect クライアントを設定し、スプリットトンネリングを有効に するために、ASDM を介して Cisco AnyConnect 設定ウィザードを使用する方法を、順を追って 詳しく説明します。

スプリットトンネリングは、特定のトラフィックのみをトンネリングする必要があるシナリオで 使用されます。これは、接続時にクライアントマシンで生成されるすべてのトラフィックが VPN を介して転送されるシナリオとは異なります。AnyConnect 設定ウィザードを使用すると、デフ ォルトでは ASA で *Tunnel-all が設定されます。*スプリットトンネリングは個別に設定する必要が あります。これについては、このドキュメントの該当するセクションで詳しく説明します。

この設定例は、10.10.10.0/24 サブネット(ASA の背後にある LAN サブネット)のトラフィック を VPN トンネル経由で送信し、クライアントマシンからの他のトラフィックはすべて独自のイ ンターネット回線経由で転送することを目的としています。

AnyConnect のライセンス情報

Cisco AnyConnect セキュア モビリティ クライアントのライセンスに関する役立つ情報へのリン クを次に示します。

- AnyConnect セキュア モビリティ クライアントおよび関連機能に必要なライセンスを確認するには、『AnyConnect セキュア モビリティ クライアントの機能、ライセンス、および OS -リリース 3.1』を参照してください。
- AnyConnect Apex および Plus のライセンスの詳細については、『<u>Cisco AnyConnect 発注ガ</u> <u>イド』を参照してください。</u>
- IP フォンおよびモバイル接続の追加のライセンス要件については、「<u>IP Phone およびモバイ</u>

<u>ル VPN 接続に ASA ライセンスが必要な理由」</u>を参照してください。

設定

ここでは、ASA で Cisco AnyConnect セキュア モビリティ クライアントを設定する方法につい て説明します。

ネットワーク図

次の図は、このドキュメントの例で使用されるトポロジを示しています。



ASDM AnyConnect 構成ウィザード

AnyConnect セキュア モビリティ クライアントの設定には、AnyConnect 設定ウィザードを使用 できます。先に進む前に、AnyConnect クライアント パッケージが ASA ファイアウォールのフラ ッシュまたはディスクにアップロードされていることを確認します。

構成ウィザードを使用して AnyConnect セキュア モビリティ クライアントを設定するために、次の手順を実行します。

1. ASDM にログインし、設定ウィザードを起動して、[次へ(Next)]をクリックします。

Cisco ASDM 7.3 fr	r ASA - 10.106.44.21	CONTRACTOR OF MALE OF MALE OF	No. of Concession, Name
<u>File View T</u> ools	Wizards Window Help		
🌀 Home 🗞 ConFig	Startup Wizsrd	C Forward 🦓 Help	
Device List	VPN Wizards	Site-to-site VPN Wizard	
🏶 Add 📋 Delete 💡	High Availability and Scalability Wizard	AnyConnect VPN Wizard 1	board
End: Unified Communication Wizard 전체 10:106-94.3 ASDM Identity Certificate Wizard		<u>C</u> lientless SSL VPN Wizard IPsec (IKEv1) Remote Access VPN Wizard	
	Packet Capture Wizard	Host Name: EdgeASA-4 ASA Version: 9.3(2) ASDM Version: 7.3(1)101 Firewall Mode: Routed Environment Status: © OK	Device Uptime: Od 16h 15m 5s Device Type: ASA 5525 Context Mode: Single Total Flash: 8192 MB

2. [接続プロファイル名(Connection Profile Name)] に接続プロファイル名を入力し、 [VPNアクセスインターフェイス(VPN Access Interface)] ドロップダウンメニューから VPN を終了するインターフェイスを選択して、[次へ(Next)] をクリックします。

AnyConnect VPN Conn	ection Setup Wizard		X		
Steps	Connection Profile Identific	ation			
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.				
2 VRN Protocole	Connection Profile Name:	SSLClient			
4. Client Images					
5. Authentication Meth	VPN Access Interface;	outside	•		

3. セキュア ソケット レイヤ (SSL)を有効にするために、[SSL] チェックボックスにチェック を入れます。 デバイス証明書は、信頼できるサードパーティの認証局 (CA)によって発行 された証明書 (Verisign、Entrust など)や自己署名証明書にすることができます。証明書が すでに ASA にインストールされている場合、ドロップダウン メニューから選択できます。 注:この証明書は、提供されるサーバ側の証明書です。ASA に現在インストールされてい る証明書がなく、自己署名証明書を生成する必要がある場合は、[管理 (Manage)]をクリ ックします。サードパーティの証明書をインストールするために、シスコの <u>ASA 8.x</u> <u>WebVPN で使用するサードパーティ ベンダーの証明書を手動でインストールする設定例の</u> 資料で説明されている手順を実行します。

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

4. [追加(Add)] をクリックします。

AnyCo	onnect VPN Co	onnection Set	tup Wizard				
•	Manage Ider	ntity Certificat	tes				23
	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
							Show Details
							Delete
							Export
							Install
	Eind:		00	Match Case			

5. [トラストポイント名(Trustpoint Name)] フィールドに適切な名前を入力し、[新しいアイ デンティティ証明書の追加(Add a new identity certificate)] オプションボタンをクリック します。デバイスに Rivest-Shamir-Addleman(RSA)キーペアが存在しない場合は、[新規 (New)] をクリックしてキーペアを生成します。

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

[デフォルトのキーペア名を使用(Use default key pair name)] オプションボタンをクリックするか、[新しいキーペア名を入力(Enter new key pair name)] オプションボタンをクリックして新しい名前を入力します。キーのサイズを選択し、[今すぐ生成(Generate Now)] をクリックします。

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

- 7. RSA キーペアが生成されたら、そのキーを選択し、[自己署名証明書の生成(Generate selfsigned certificate)] チェックボックスをオンにします。[証明書サブジェクト
 - DN(Certificate Subject DN)] フィールドに目的のサブジェクトドメイン名(DN)を入力 し、[証明書の追加(Add Certificate)] をクリックします。

Add Identity Certificate	
Trustpoint Name:	SelfsignedCert
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:	ssicert Show New
Certificate Subject DN:	CN=anyconnect.cisco.com Select
Generate self-signed	certificate
📃 Act as local certi	ficate authority and issue dynamic certificates to TLS-Proxy
	Advanced
Add Cer	tificate Cancel Help

8. 登録が完了したら、[OK]、[OK]、[次へ(Next)] の順にクリックします。

🔄 An	yConnect VPN Co	onnection Set	tup Wizard				
Ste	👩 Manage Ider	ntity Certificat	ies				X
1.						-]
2.	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
	hostname	hostname	. 16:39:40 M	SelfsignedCert	Gener	RSA (2048 bits)	Show Details
3.							Delete
4.							
5.							Export
6.							Install
	Eind:		00	Match Case			
7.							
	Public CA Enro	liment —					
0.	Entrust. Entr	ust offers Cis	ico customers a	a special promotional price	for certif	icates and trial certi	ificates for testing.
9.			E	nroll ASA SSL certificate v	vith Entru	st	-
10	Using a prev	viously saved	certificate sign	ing request, enroll with En	drust.		
	cound or birds			and redeeed on on white			
			Ok	Cancel	ŀ	Help	

9. PC またはフラッシュから AnyConnect クライアントイメージ(*.pkg ファイル*)を追加する ために、[追加(Add)]をクリックします。[フラッシュの参照(Browse Flash)]をクリッ クしてフラッシュドライブからイメージを追加するか、[アップロード(Upload)]をクリッ クしてホストマシンから直接イメージを追加します。

n onene milagea			
5. Authentication Meth	Add 🗹 Rep	lace 📋 Delete 🛧 🗲	
6. Client Address Assignment	Add AnyConne	ct Client Image	X
7. Network Name Resolution Servers	AnyConnect Imag	e:	Browse Flash
8. NAT Exempt			Upload
9. AnyConnect Client Deployment	Regular expre	ssion to match user-agent	*
10. Summary		OK Cancel	Help
Browse Flash		Nagala suprement &	X
Folders		Files	
disk0: disk0: disk0: disk0: corport disk0: disk0		FileName	Size (Date
		anyconnect-win-3.1.05152-k9.pkg	35,167, 12/17/ 🔺
		anyconnect-win-3.1.06073-k9.pkg	38,048, 01/02/
🗄 🛄 tmp		asa932-smp-k8.bin	63,479, 01/02/

10. イメージが追加されたら、[次へ(Next)]をクリックします。

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

11. ユーザ認証は認証、許可、およびアカウンティング(AAA)サーバ グループを介して実行 できます。ユーザーがすでに設定されている場合は、[ローカル(LOCAL)]を選択し、[次 へ(Next)]をクリックします。 注:この例では、ローカル認証が設定されています。こ れは、ASA のローカル ユーザ データベースが認証に使用されることを示します。

AnyConnect VPN Co	nnection Setup Wizard
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Officient Methods	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 Local User Database Details
 Client Address Assignment Network Name Resolution Servers NAT Exempt AnyConnect Client Deployment Summary 	User to be Added Username: User1 Add >> Password: •••• Delete Confirm Password: ••••
	< Back Next > Cancel Help

12. VPN クライアントのアドレスプールが設定されている必要があります。すでに設定されて いる場合は、それをドロップダウンメニューから選択します。まだ設定されていない場合 は、[新規(New)] をクリックして新しく設定します。 完了したら、[OK] をクリックしま す。

5. 4114110000018							
Client Images	IP v4 Address Pool IP v6 Address Pool						
5. Authentication Meth	Address Pool:	Select 🔻 Nev	H				
6. Client Address Assignment	Details of	🖬 Add IPv4 Pool		×			
7. Network Name Resolution Servers		Name:	SSL-Pool				
3. NAT Exempt		Starting IP Address:	10.10.11.1	-			
 AnyConnect Client Deployment 		Ending IP Address:	10.10.11.20				
10. Summary		Subnet Mask:	255.255.255.0	•			
		ОК	Cancel Help				

13. ドメインネームシステム(DNS)サーバと DN を [DNS] フィールドと [ドメイン名 (Domain Name)] フィールドに適切に入力し、[次へ(Next)] をクリックします。

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

14. このシナリオの目的は、ASA の背後にある*内部(または LAN)サブネットとして設定され ている* 10.10.10.0/24 ネットワークへの VPN 経由のアクセスを制限することです。 クライ アントと内部サブネットの間のトラフィックは、動的なネットワークアドレス変換 (NAT)から除外する必要があります。

[ネットワークアドレス変換からVPNトラフィックを除外(Exempt VPN traffic from network address translation)] チェックボックスをオンにして、除外に使用される LAN および WAN インターフェイスを設定します。

2. Connection Profile Identification	🔽 Exempt VPN traffic f	from network address translation					
3. VPN Protocols	Inside Interface is t	he interface directly connected to your internal network.					
4. Client Images	Inside Interface: Ir	nside 🔹 🔻					
5. Authentication Metho	Local Network is the	e network address(es) of the internal network that client					
Client Address	can access.						
Assignment	Local Network: a	ny 👘					
7. Network Name Resolution Servers							
8. NAT Exempt	from network addre	The traffic between AnyConnect client and internal network will be exempt from network address translation.					
9. AnyConnect Client							

15. 除外する必要があるローカルネットワークを選択します。

					1 11001 [0101
Name ^ 1		IP Address	Netmask	Description	Object NAT Addr
-IPv4 Netw	ork Ob	jects			
- 🏈 any		-			
📑 🛃 Insi	de :	10.10.10.0	255.255.255.0		
- 📲 outs	sid :	10.106.44.0	255.255.255.0		
्रम् १०.0	0.0.0	10.0.0.0	255.0.0.0		
🚽 📲 10.1	1.2 :	10.1.232.192	255.255.255		
- IPv4 Netw	ork Ob	ject Groups			
🗈 🞆 ANY	1				
🕀 🎆 OBJ	_L				
🕀 🎆 OBJ	_S				
Interfaces					
The state	de				
Insi	ae				
outs	de side				
Selected Loca	al Netw	vork			
Selected Local Ne	al Netw stwork	vork -> Inside-r	network/24		
Selected Loca Local Ne	al Netw stwork	vork -> Inside-r	network/24		
Selected Local Ne	al Netw stwork	/ork -> Inside-r	network/24		OK Canc
Selected Loca	al Netw stwork	/ork -> Inside-r	network/24		OK Canc
Selected Local Ne	al Netw stwork	/ork -> Inside-r	network/24		OK Canc
Selected Local Ne	al Netw side al Netw stwork	/ork -> Inside-r	network/24		OK Canc
Selected Loca Local Ne	al Netw side al Network	/ork -> Inside-r	network/24 rk is the network addr	ess(es) of the internal net	OK Canc work that client
Selected Loca Local Ne Authentication N	al Netw al Netw stwork	/ork -> Inside-r Local Networ can access. Local Networ	network/24 rk is the network addr	ess(es) of the internal net	OK Canc
Selected Loca Local Ne Authentication N Client Address Assignment Network Name	al Netw stwork	/ork -> Inside-r Local Networ can access. Local Networ	network/24 rk is the network addr rk: 10.10.10.0/24	ess(es) of the internal net	OK Canc work that client
Authentication N Client Address Assignment Network Name Resolution Servi	al Network	/ork -> Inside-r Local Networ can access. Local Networ	network/24 rk is the network addre rk: 10.10.10.0/24	ess(es) of the internal net	OK Canc
Authentication N Client Address Assignment Network Name Resolution Serve NAT Exempt	al Netw al Netw atwork	/ork -> Inside-r Local Networ can access. Local Networ The traffic b from petwor	network/24 rk is the network addr rk: 10.10.10.0/24 etween AnyConnect cl	ess(es) of the internal network v	OK Canc work that client

16. [次へ(Next)]、[次へ(Next)]、[完了(Finish)] の順にクリックします。

これで、AnyConnect クライアントの設定が完了しました。ただし、設定ウィザードを使用して AnyConnect を設定すると、スプリットトンネルポリシーがデフォルトで「**Tunnel-all**」に設定さ れます。特定のトラフィックだけをトンネリングするには、スプリットトンネリングを実装する 必要があります。 注:スプリットトンネリングが設定されていない場合、スプリットトンネルポリシーはデフ ォルトのグループポリシー(DfltGrpPolicy)から継承されます(デフォルトでは Tunnelall に設定される)。これは、クライアントが VPN を介して接続されるとすべてのトラフィッ ク(Web へのトラフィックを含む)がトンネルを介して送信されることを意味します。

ASA WAN(または*外部*)IP アドレス宛てのトラフィックのみがクライアントマシンでのトンネリングをバイパスします。これは、Microsoft Windowsマシンでの **route print コマンドの出力で確** 認**できます。**

Split-tunnel 設定

スプリットトンネリングは、暗号化する必要があるサブネットまたはホストのトラフィックを定 義するために使用できる機能です。これには、この機能に関連付けられるアクセスコントロール リスト(ACL)の設定が含まれます。この ACL で定義されたサブネットまたはホストのトラフィ ックは、クライアント側からのトンネルを介して暗号化され、これらのサブネットのルートは PC ルーティングテーブルにインストールされます。

Tunnel-all 設定から Split-tunnel 設定に移行するには、次の手順に従います。

1. [設定(Configuration)] > [リモートアクセスVPN(Remote Access VPN)] > [グループポリ シー(Group Policies)] に移動します。

🚳 Home 🦓 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🕓 Back 🔘 Forward 💡 Help								
Device List	2 P	×	Configuration > Remote Access VE	N > Network (Client) Access >	Group Policies			
Add Delets S Connect Find: Go	t	• =	Managa VPN group policies A VPN g information is referenced by VPN co To enforce authorization attributes f Add V C CdR Delete As	oup is a collection of user-oriented medicin profiles and user accounts, form an LDAP server you must use a lign	authorization attribute/value pairs that may be stored internal n <u>LDAP attribute map</u> .			
Remote Access VPN	ð	ę.	Name	Туре	Tunneling Protocol			
🖓 🥐 Introduction			GroupPolicy_SSLElient	internal	ssHoliant			
Network (Client) Access AnyConnect Connection Customizet AnyConnect Client Profi AnyConnect Client Soft AnyConnect Client Soft Opnamic Access Policies	i Profiles tion/Locali la ware 8	2	DfittGrpPolicy (System Default)	Internal	kev1;/kev2;ssHclientless;l2tp-ipsec			

2. [編集(Edit)] をクリックし、ナビゲーションツリーを使用して [詳細(Advanced)] > [ス プリットトンネリング(Split Tunneling)] に移動します。[ポリシー(Policy)] セクション の [継承(Inherit)] チェックボックスをオフにして、ドロップダウンメニューから [以下の ネットワークリストをトンネリング(Tunnel Network List Below)] を選択します。

Edit Internal Group Pol	licy: GroupPolicy_SSLClient	7	
General	The VPN client makes split tunn	eling decisions on the	basis of a network list that can be specifie
Advanced	DNS Names:	📝 Inherit	
Browser Proxy	Send All DNS Lookups Through	Tunnel: 📝 Inherit	O Yes O No
	Policy:	📃 Inherit	Tunnel Network List Below
	Network List:	📝 Inherit	

3. [ネットワークリスト (Network List)] セクションの [継承 (Inherit)] チェックボックスをオ フにして、[管理 (Manage)] をクリックし、クライアントがアクセスする必要のある LAN ネットワークを指定する ACL を選択します。

Network List:	🔲 Inherit	nside_access_in	•	Manage			
Pressing this button to set up split extusion for Web Security proxies.							
- Set up Bplit Exclusion for Web	b Security						

4. [標準ACL(Standard ACL)]、[追加(Add)]、[ACLの追加(Add ACL)]、[ACL名(ACL Name)] の順にクリックします。

General	The VPN	client n	nakes split tunneling deci	isions on the basis o	of a network list that can be spec
-Servers -Advanced		ACL	Manager	-	
Split Tunneling Browser Proxy	Send	Stand	ard ACL Extended ACL		
AnyConnect Client	Jenu	🗣 Ad	dd 🔹 🛒 Edit 📋 Delete	÷ + λ m m	<u>n</u> *
	Policy	No	Address	Action	Description
	Netwo		Add ACL		
	Pressi		ACL Name: Split-AC	1	
	Set		Acchanie, opie Ac	~	
	Inte			Cancel	Help

5. [追加(Add)]をクリックしてルールを追加します。

ACL Man	ager						
Standard ACL Extended ACL							
💠 Add 🕶 🗹 Edit 📋 Delete 🎓 🗲 👗 🐚 🏙 📲							
No	Address	Action	Description				
Split-A	CL						
Add ACE							
Action:) Permit 💿 Deny						
Address: 10.10.10.0/24							
Descrip	tion:						

6. [OK] をクリックします。

General Eerkens	The VPN client makes split to an eling der	oisions on the	base of a network, iso had can be specified below by providing the proper carameters to "Folicy" and "Network too" fe	e de .	
-Advanced Solit Tunna Ing	DNE Names:	😨 Inherit			
−Browser Froxy →AryConnect Client →Psec(R(8yt)) Client	Send All DRS Loci ups Through Tunnel:	🔽 Inherit	⊙ YES ⊙No		
	Poloy:	🔲 Inherit	Turnel Network List Selow 🔻		
	Network List:	🔲 Inherit	9515-401 · · · · · · · · · · · · · · · · · · ·	E	Manag
	Pressing this button to set up to it eaks Estup Split Ecolusion for Web Estua Internet 1941 8 Conferencies New	ion for Web S iy	iecunty provies.		

7. [Apply] をクリックします。

接続されると、Split-ACL に含まれるサブネットまたはホストのルートがクライアントマシンのル ーティングテーブルに追加されます。Microsoft Windowsマシンでは、これを route print コマンド の出力で確認できます。これらのルートのネクストホップは、クライアント IP プールサブネット からの IP アドレス(通常、サブネットの最初の IP アドレス)です。

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 10.10.10.0 255.255.0 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 On-link 10.106.44.243 6

!! This is the route for the ASA Public IP Address. MAC OS マシンでは、netstat -r コマンドを入力して PC ルーティングテーブルを表示します。

\$ netstat -r
Routing tables
Internet:
Destination Gateway Flags Refs Use Netif Expire
default hsrp-64-103-236-1. UGSc 34 0 en1
10.10.10/24 10.10.11.2 UGSc 0 44 utun1

!! This is the split tunnel route.

10.10.11.2/32 localhost UGSc 1 0 lo0 172.16.21.1/32 hsrp-64-103-236-1. UGSc 1 0 en1

!! This is the route for the ASA Public IP Address.

AnyConnect クライアントのダウンロードとインストール

Cisco AnyConnect セキュア モビリティ クライアントは次の 2 つの方法でユーザマシンに展開で きます。

• Web 展開

スタンドアロン展開

これらの方法の両方について、以下のセクションで詳しく説明します。

Web 展開

Web 展開方式を使用するには、クライアントマシンのブラウザに https://<ASA's FQDN> または <ASA's IP>URL を入力して *WebVPN* ポータルページを表示します。

注:Internet Explorer(IE)を使用する場合は、Java を強制的に使用する設定になっていな ければ、インストールのほとんどが ActiveX を介して完了します。他のすべてのブラウザで は Java が使用されます。

ページにログインすると、クライアントマシンへのインストールが開始され、インストールの完 了後にクライアントが ASA に接続します。

注:ActiveX または Java を実行する権限を求められる場合があります。インストールを続行するには、これを許可する必要があります。

Logon						
Group SSLClient 🔻						
Username						
Password						
Logon						



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

スタンドアロンでの導入

スタンドアロン展開の方法を使用するには、次の手順に従います。

- 1. シスコの Web サイトから AnyConnect クライアントのイメージをダウンロードします。ダ ウンロードするイメージを正しく選択するには、<u>Cisco AnyConnect セキュア モビリティ ク</u> <u>ライアントの Web ページを参照してください。</u>このページにダウンロードリンクがありま す。ダウンロードページに移動し、適切なバージョンを選択します。「Full installation package - Windows / Standalone installer (ISO)」を検索してください。 注: ISO インスト ーライメージ (*anyconnect-win-3.1.06073-pre-deploy-k9.iso* など)がダウンロードされます
- 2. WinRar または 7-Zip を使用して ISO パッケージの内容を抽出します。

anyconnect-win-3.1.070	Rurn dis simpas		
	burn use image		L
	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. 内容が抽出されたら、Setup.exe ファイルを実行し、Cisco AnyConnect セキュア モビリテ ィ クライアントと同時にインストールする必要があるモジュールを選択します。

ヒント: VPN の追加設定を指定するには、『*Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*』の「<u>Configuring AnyConnect VPN Client Connections」を参照してください。</u>

CLI での設定

```
ここでは、参考までに Cisco AnyConnect セキュア モビリティ クライアントの CLI 設定の例を示します。
```

```
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
1
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
1
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
1
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224
access-list all extended permit ip any any
!********Split ACL configuration*********
access-list Split-ACL standard permit 10.10.10.0 255.255.255.0
no pager
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-721.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!This will exempt traffic from Local LAN(s) to the
!Remote LAN(s) from getting NATted on any dynamic NAT rule.
nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24
destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp
route-lookup
access-group all in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.21.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

timeout tcp-proxy-reassembly 0:01:00 timeout floating-conn 0:00:00 dynamic-access-policy-record DfltAccessPolicy user-identity default-domain LOCAL aaa authentication ssh console LOCAL http server enable http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact !******** Trustpoint for Selfsigned certificate********* !Genarate the key pair and then configure the trustpoint !Enroll the trustpoint genarate the self-signed certificate crypto ca trustpoint SelfsignedCert enrollment self subject-name CN=anyconnect.cisco.com keypair sslcert crl configure crypto ca trustpool policy crypto ca certificate chain SelfsignedCert certificate 4748e654 308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105 0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e 170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d 06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0 55a975ec alf2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4 ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0 7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c 75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93 5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7 53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34 03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36 19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001 300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296 c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1 64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41 daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928 f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9 4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833 900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206 3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8 quit telnet timeout 5 ssh timeout 5 ssh key-exchange group dh-group1-shal console timeout 0 management-access inside threat-detection basic-threat threat-detection statistics access-list no threat-detection statistics tcp-intercept ssl server-version tlsv1-only ssl encryption des-shal 3des-shal aes128-shal aes256-shal !******* Bind the certificate to the outside interface******* ssl trust-point SelfsignedCert outside

!*******Configure the Anyconnect Image and enable Anyconnect***

webvpn

```
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) Configuraiton****
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
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
```

確認

クライアント接続とその接続に関連付けられているさまざまなパラメータを確認するには、次の 手順に従います。

1. ASDMで [モニタリング(Monitoring)] > [VPN] に移動します。

Cisco ASDM 7.2 for ASA - 10.106.44.	162
<u>File View T</u> ools Wizards <u>W</u> indov	v <u>H</u> elp
Home 🦓 Configuration [Monitorin	g 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🢡 Help
Device List 과 무 ×	Monitoring > VPN > VPN Statistics > Sessions
🕈 Add 📋 Delete 🚿 Connect	

[次でフィルタ処理(Filter By)] オプションを使用すると VPN のタイプをフィルタ処理できます。ドロップダウンメニューから [AnyConnectクライアント(AnyConnect Client)] を選択し、すべての AnyConnect クライアントセッションを選択します。 ヒント:セッションは、ユーザ名や IP アドレスなどの他の条件でさらにフィルタ処理できます。

VPN 3.4	Eliter By: Arealogs	act Client 🔹	Al Societa	•	Eltar		
I Statistics	T IG UST MADE	Second -	THE OBJOINT OF		1.46		
- 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	cism.	 GroupPolicy_SSUCIIer SSUCIIent 	10.10.11.1 172.15.21	AnyConnect-Farent SSL-Tunnel . AnyConnect-Farent (1)none S.	16 58:56 UTC Dr: 12m:55a	11472 22738	01.00m:00s
Clobal UE; (Psec Statistics I RAC Sessian Burmary I Protocol Statistics VLAN Megoing Sessions Clentiless Set VFN Clentiless Set VFN WFN Connection Graphs WFA Censions							
Length John Harden							

3. 特定のセッションの詳細情報を取得するには、そのセッションをダブルクリックします。

) Se: iessio	ssion Detail: on Details	5							2
User	name	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption AnyConnect-Parent SSL-Tunnel AnyConnect-Parent: (1)none S.		Login Time B Duration B	Bytes Tx Bytes Rx	Inactivity	
isco		GroupPolicy_SSLClien SSLClient	10.10.11.1 172.16.21.1			Tunnel . 16:58:56 UTC 11472 Oh:00m:00 none S Oh:21m:09s 26653			
Deta	ails ACL	Local Addr. / Subnet N Remote Addr. / Subnet	Nask / Protocol / Port Mask / Protocol / Port	Encryption	Other		Bytes Tx Bytes Rx		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 Client OS Type: W Client Ver: Cisco /	21.1 28 Minutes nutes Vindows onnect AnyConnect VPN Ag	5954 1046	-	

4. CLI に show vpn-sessiondb anyconnect コマンドを入力してセッションの詳細情報を取得します。

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. 他のフィルタオプションを使用して結果を絞り込むことができます。

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

トラブルシュート

AnyConnect Diagnostics and Reporting Tool (DART)を使用すると、AnyConnect のインストー ルと接続に関する問題のトラブルシューティングに役立つデータを収集できます。 DART ウィザ ードは、AnyConnect が稼働するコンピュータで使用します。DART によってログ、ステータス 、および診断情報が収集され、それを Cisco Technical Assistance Center (TAC)での分析に使 用できます。クライアントマシンで実行するために管理者権限は不要です。

DART のインストール

DART をインストールするには、次の手順に従います。

- 1. シスコの Web サイトから AnyConnect クライアントのイメージをダウンロードします。ダ ウンロードするイメージを正しく選択するには、<u>Cisco AnyConnect セキュア モビリティ ク</u> <u>ライアントの Web ページを参照してください。</u>このページにダウンロードリンクがありま す。ダウンロードページに移動し、適切なバージョンを選択します。「Full installation package - Windows / Standalone installer (ISO)」を検索してください。注:ISO インスト ーライメージ(*anyconnect-win-3.1.06073-pre-deploy-k9.iso* など)がダウンロードされます
- 2. WinRar または 7-Zip を使用して ISO パッケージの内容を抽出します。

				· · · · ·
i anyconnect-win-3.1.070	-	Burn disc image		
		7-Zip	×	Open archive
		Edit with Notepad++		Open archive
		Open with	•	Extract files
		Share with	,	Extract Here
				Extract to "anyconnect-win-3.1.07021-pre-deploy-k9\"

- 3. 内容が抽出されたフォルダを参照します。
- 4. Setup.exe ファイルを実行し、[Anyconnect Diagnostic And Reporting Tool] のみを選択します。



DART の実行

DART を実行する前に考慮する必要がある重要な情報は、次のとおりです。

• DART を実行する前に、少なくとも1回は問題を再現する必要があります。

•問題が再現されたときに、ユーザマシンの日付と時刻を記録する必要があります。 クライアントマシンの [スタート(Start)]メニューから DART を実行します。



[デフォルト(Default)] モードまたは [カスタム(Custom)] モードを選択できます。DART をデ フォルトモードで実行することをお勧めします。これにより、すべての情報を 1 回のスクリーン ショットでキャプチャできます。

Cisco DART 3.1.05170						
Bundle Creation Option						
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.						
 Default (Bundle will be saved to Desktop) 						
Custom						
Clear logs after DART finshes						
Back Next Cancel						

完了すると、DART バンドルの *.zip ファイルがクライアントデスクトップに保存されます。*この バンドルを、さらなる分析のために TAC に電子メールで送信できます(TAC のケースをオープ ンした後)。

関連情報

- AnyConnect VPN クライアントのトラブルシューティング ガイド 一般的な問題
- <u>AnyConnect、CSD/Hostscan、および WebVPN による Java 7 の問題 トブルシューティン</u> <u>グガイド</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。