Cisco Start Firewall

Cisco ASA 5506-X AnyConnect VPN の設定

2016年2月16日 第1.0版



www.networld.co.jp







改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016年2月16日	ネットワールド	● 新規
			•
			•
			•





免責事項

- 本書のご利用は、お客様ご自身の責任において行われるものとします。本書に記載する情報については、株式会社ネットワールド(以下弊社)が慎重に作成および管理いたしますが、弊社がすべての情報の正確性および完全性を保証するものではございません。
- 弊社は、お客様が本書からご入手された情報により発生したあらゆる損害に関して、一切の責任を 負いません。また、本書および本書にリンクが設定されている他の情報元から取得された各種情報 のご利用によって生じたあらゆる損害に関しても、一切の責任を負いません。
- 弊社は、本書に記載する内容の全部または一部を、お客様への事前の告知なしに変更または廃 止する場合がございます。なお、弊社が本書を更新することをお約束するものではございません。





表記規則

表記	表記の意味
「」(括弧記号)	キー、テキストボックス、ラジオボタンなどのオブジェクト
bold (ボールド文字)	入力または選択するシステム定義値
<italic>(イタリック文字)</italic>	入力または選択するユーザー定義値
─── □ (囲み線)	入力または選択するオブジェクト
""(二重引用符記号)	表示されるメッセージ
(蛍光マーカー)	確認するメッセージ
表記の例) (1) Exec」ラジオボタンを選 (2) テキストボックスに以下の → copy running-config	択します。 コマンドを入力します。 <file name=""></file>
(3)「コマンドを実行」ボタンを Destination filename [s Building configuration…) (OK]	クリックします。正常に実行されれば、画面に"[OK]"が表示されます。 startup-config]?
CLIIこよる設定 CLi機能はルータのコマンドブロンプトで実行可能な認 ・ Exec ・ Configure copy running-config startup-config コマンドを実行 クリア Destination filename [startup-config]? Building configuration [OK]	1定や、全ての105 CLIコマンドを入力できます
	~





<u>目次</u>

1. はじめに	1
1.1 対象機器	1
1.2 AnyConnect VPN について	1
1.3 事前に用意するもの	1
2. システム構成	2
2.1 システム構成	2
3. AnyConnect VPNの設定	3
3.1 AnyConnect VPN のポリシー設定	3
3.2 クライアント PC の AnyConnect VPN 設定	17
3.2.1 AnyConnect Secure Mobility Clientのインストール	17
3.2.2 AnyConnect VPNの接続	21





1. はじめに

本書は Cisco ASA 5506-X における AnyConnect VPN の設定手順について説明しています。

1.1 対象機器

本書で対象としている機器は以下になります。

表1 本書の対象機器

ASA 5506-X	ASA 5506W-X	
(ASA5506-K9)	(ASA5506W-Q-K9)	
Ø	V	

1.2 AnyConnect VPN について

AnyConnect VPNとは、Cisco ASA 5500シリーズ等を終端装置として、PCなどのリモート端末から VPN 接続を行う際にクライアントとなるソフトウェアおよび機能の名称です。

AnyConnect VPNを行うためには、AnyConnect Plus ライセンスまたは AnyConnect Apex ラ イセンスを購入し、ASA 本体でアクティベーション(有効化)する必要があります。 ライセンスのアクティベーシ ョン手順については別紙「Cisco ASA 5506-X AnyConnect ライセンスアクティベーション」を参照し て下さい。

1.3 事前に実施しておく事

- AnyConnect Plus ライセンスまたは AnyConnect Apex ライセンスのアクティベーション
- AnyConnect Secure Mobility Client のイメージファイル (Windows 用、Web depl oy)をCisco.comよりダウンロードし、ASAのFlashへのコピーしておきます。ダウンロード時にはC isco.com IDにAnyConnect Plus ライセンスまたはAnyConnect Apex ライセンスの契約番 号が紐づいている必要があります

Cisco Start Firewall Cisco ASA 5506-X AnyConnect VPNの設定

-thatheisco

2. システム構成

2.1 システム構成

本書での AnyConnect VPN 設定手順は以下のシステム構成に基づいて行われます。設定状態 は別紙「Cisco ASA 5506-X クイックスタートガイド」の設定完了後となり、管理 PC の ASDM から A SA に接続でき、インターネットへもアクセスできる状態を想定しています。また、ASA の outside のインタ フェース(GE1/1)に対してクライアント PC からインターネット越しにアクセスできることが前提となります。



図1 システム構成図

表 2 本書で使用した機材およびそれらのシステム環境

機器	機器名	OS およびアプリケーション	ネットワーク設定
Firewall	ASA 5506W-	OS Version 9.5(2)	GE1/1
	х	ASDM Version 7.5(2)153	nameif:outside (デフォルト)
		AnyConnect Secure Mobility Clie	IP アドレス:DHCP(デフォルト)
		nt Version 4.2.01035 ※	security level:0(デフォルト)
		AnyConnect Plus ライセンス	GE1/2
			nameif:inside (デフォルト)
			IP アドレス:172.16.1.254/24
			Security level:100(デフォルト)
管理用 PC		OS: Windows 7	インタフェース IP アドレス:172.16.1.1/24
		ターミナルアプリケーション (Tera Term)	
		Web ブラウザ(Internet Explorer11)	
クライアント PC		OS : Windows 7	インタフェース IP アドレス:DHCP
		Web ブラウザ(Internet Explorer11)	

※AnyConnect Secure Mobility Client のイメージファイルはデフォルトでは ASA の Flash に入っていないため、事前に Cisco.com よりダウンロードして Flash に入れておく必要があります

表 3 ASA 5506-X のネットワーク設定

ルーティング	・インターネット側ヘデフォルトルートを DHCP により取得
NAT	・any→outside への PAT (デフォルト)

表 4 AnyConnect VPN のポリシー

VPN アクセス	VPN プロトコル	AnyConnect クライア	IP Address プール (プ	NAT 除外ルール	スプリットトンネリン
インタフェース		ントイメージ	ール名)		グ(ACL 名)
outside	SSL	anyconnect-win-4.	192.168.1.1-250/24	inside,	172.16.1.0/24
		2.01035-k9.pkg	(Pool)	172.16.1.0/24	(split)





3. AnyConnect VPN の設定

3.1 AnyConnect VPN のポリシー設定

本節では、AnyConnect VPN のポリシー設定手順を説明します。

1) 管理 PC から ASDM により ASA にアクセスし、「Wizards」>「VPN Wizards」>「AnyCon nect VPN Wizard」を開きます。

Cisco ASDM 7.5(2	2)153 for ASA - 17	72.16.3	1.254								- 0	×
File View Tools	Wizards Windo	w He	elp					Type top	pic to search	Go		.1.
🚮 Home 🔩 Cor	Startup Wize	ard		Back 🙆	Forward	Help					CIS	sco
Device List	VPN Wizards	5	•	Sit	e-to-site VPN	Wizard						
Device List	High Availab	ility ar	nd Scalability Wizard	An	yConnect VPN	V Wizard						
🕈 Add 📋 Delete 🎙	Onlined Com	munica	auon wizaro	Clie	entiess SSL V	PN Wizard						
Find	ASDM Ident	ity Cer	tificate Wizard	IPs	ec (IKEv1) Re	emote Acces	ss VPN	Wizard	Address (Mask	Line	Liek	Khno
172.16.1.254	Packet Capt	ure Wi	zard	IPs	ec (IKEv2) Re	emote Acces	ss VPN	Wizard	2.16.1.254/24	O up	Unk O UD	4
		ASA	Version: 95(2) De	vice Hotim	~ 3d 13h 45m	. 220	00	utside	10.870	Oup	🕒 up	17
		ASDI	M Version: 7.5(2)153 De	rice Type:	ASA 5506V	v	99	ifi	192.168.10.1/24	😧 up	😌 up	0
		Firew	vall Mode: Routed Co	ntext Mode	Single							
		Envir	onment Status: 🗣 OK 🛛 To	al Flash:	8192 MB							
							Se	elect an interface	e to view input and o	utput Kbps		
	1	/PN Set	ssions				Fa	ilover Status				
		IPsec:	0 Clientless SSL VPN: 0	AnyConnec	t Client: 🛚 👘	Details_	F.	ailover not confi	gured. Click the link	to configure	it.	Configu
	s	ystem	Resources Status				Tra	affic Status				
		Total M	emory Usage Total CPU Usag	e Core U	sage Details		ГC	Connections Per	Second Usage			
	м	emory l	Usage (MB)					4				
								2 00000		-		
			3000					06:50	06:51 0 TCP: 0 Total	06:52 0	06:53	06:54
			2000				E.	outside' Interface	e Traffic Usage (Kbp	(s)		
		772MB	2000					2000				
			1000					1000				
								06:50	06:51 0	16:52 I	06:53	06:54
	0	65432	06:50 06:51	06:52	06:53	06:54		a por rope		~~ 0		
	< [III						۱. F
	Late	est ASI	DM Syslog Messages									р ф ×
			ASDM logg	ng is disab	led.To enable A	SDM logging	with in	formational leve	L click the button be	low.		
						Enable Lo	eeine					
L					ŀ	(admin)	15			A	16/02/01 6	354:32 JST

図 2 AnyConnect VPN Wizard を開く

2) AnyConnect VPN Connection Setup Wizard が開始されます。「Next」をクリックします。



図 3 AnyConnect VPN Connection setup Wizard の開始





3) 「Connection Profile Name」および「VPN Access Interface」を設定して「Next」をクリックします。

TanyConnect VPN Conne	ction Setup Wizard
AnyConnect VPN Connect Steps I. Introduction Connection Profile Identification VPN Protocols Client Images Activent Images Content Images Content Address Assignment Network Name Resolut Servers	connection Profile Mentification This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections. Connection Profile Name SSL-VPN Connection Profile Name SSL-VPN (アPN Access Interface)に「outside」を選択します
8. NA1 Exempt 9. AnyConnect Client Deployment 10. Summary	③「Next」をクリックします
	<back< td=""> 取消 Help</back<>

図 4 Connection Profile の作成

4) 使用する VPN を選択し、「Next」をクリックします。

AnyConnect VPN Conne	ection Setup Wizard			
AnyConnect VPN Conne Steps I. Introduction Connection Profile Identification VPN Protocols Client Images Cultent darkens Assignment	ection Setup Witard VPN Protocols AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support. SSL ①SSL ①SSL ②SSL ②SSL ③Psec Device Certificate Device Certificate 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.			
 Network Name Resolut Servers NAT Exempt AnyConnect Client Deployment Summary 	be available on the ASA. Device Certificate: None Manage_			
	(2)1 Next」をクリックします			
	< <u>Back</u> Next> 取消 Help			

図 5 VPN の選択





5) 「Add」をクリックして Client Image の指定に進みます。

📑 AnyConnect VPN Conne	ction Setup Wizard	×
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Olient Images 5. Authentication Methods	Client Images ASA can automatically upload the latest AnyConnect package to network. A regular expression can be used to match the user-agent of a bi You can also minimize connection setup time by moving the image system to the top of the list.	the client device when it accesses the enterprise rowser to an image. e used by the most commonly encountered operation
 Client Address Assignment Network Name Resolut Servers NAT Exempt AnyConnect Client Deployment Summary 	Image You can download AnyConnect Client packages from Cisco by se	Regular expression to match user-agent
	< <u>B</u> ack <u>N</u> ext >	取消 Help

図 6 Client Image の指定(1)

6) 「Browse Flash」をクリックします。

Add AnyConnect Client Image	×
AnyConnect Image:	Browse Flash
	Upload
Regular expression to match user-agent	*
OK Cancel Help	

図7 Client Imageの指定(2)

7) AnyConnect Client Image を指定し、「OK」をクリックします。

⊐~ <mark>- → disk0:</mark>	FileName ^ 1	Size (bytes)	Date Modified
🗄 🛄 log		0120 (8)(03)	Date Moanica
⊕~ crypto_archive ⊕~ coredumpinfo	□ crypto_archive ①Any(□ log	Connect Clier	nt Imageを選択
	anvconnect-win-4201	19 183 882	1 4.2.01035 KJ
	anyconnect-win-4.2.01	28,381,184	
	asa951-lfbff-k8.spa	74,369,568	
	asa952-Ifbff-k8.SPA	82,335,584	
	asdm-751bin	25,025,404	
	asdm-752-153bin	25,629,676	
	fr_customization.po	2,686	
	fr_PortForwarder.po	4,149	
	fr_webvpn.po	34,638	
	ja_customization.po	2,927	
	ja_PortForwarder.po	4,481	
	ia webyon oo	0.90 3.9	

図 8 Client Image の指定(3)





8) 「OK」をクリックして Client Image の指定を完了します。



図9 Client Image の指定(4)

9) 「Next」をクリックして先に進みます。



図 10 Client Image の指定(5)

10) AnyConnect VPN で接続するクライアントを認証するためのユーザアカウントを追加し、「Next」をク

リックします。

Steps	Authentication Methods
Introduction Connection Profile Jentification VPN Protocols VPN Protocols Ven Vrotocols A client Images Authentication Methods Collent Address Assignment Network Name Resolut Servers NAT Exempt AngConnect Client Deployment Io. Summary	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: LOC. New. Local User Database Details User to be Adde Username: Password Confirm Password ① ユーザ名およびパスワードを入力します ④ クリックします

図 11 AnyConnect VPN ユーザアカウントの追加



す。



- 11) VPN で接続するクライアント端末に割り当てる IP アドレスプールを作成するため、「New」をクリックしま
 - × AnyConnect VPN Connection Setup Wizard Steps Client Address Assignment 1. Introduction This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect. 2. Connection Profile Identification IPv6 address pool is only supported for SSL connection. 3. VPN Protocols IP v4 Address Pool IP v6 Address Pool Address Pool --- Select -_ Vew... 4. Client Images 5. Authentication Methods Client Address Assignment Details of the selected address pool -7. Network Name Resolut Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary < <u>B</u>ack Next > 取消 Help

図 12 IP Address Poolの作成(1)

12) IP アドレスプールの設定を入力し、「OK」をクリックします。

Add IPv4 Pool	
Name:	Pool ①プール名を入力します
Starting IP Address:	192.168.1.1 ②アドレス範囲の開始アドレスを入力します(例:192.168.1.1)
Ending IP Address:	192.168.1.250 ③アドレス範囲の最終アドレスを入力します(例:192.168.1.250)
Subnet Mask:	255.255.255.0 ④サブネットマスクを入力します(例:255.255.255.0)
ОК	Sylvy/0-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1

図 13 IP Address Poolの作成(2)

13) 先ほど作成した Pool を選択し、「Next」をクリックします。

anyConnect VPN Connect	ection Setup Wizard	×
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignment 7. Network Name Resolut Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	Client Address Assignment This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AryConnect clients will be assigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool Address Pool Details of the selected address pool Starting IP Address: 192.168.1.1 Ending IP Address: 192.168.1.250 Subnet Mask: 255.255.255.0	
	< Next > 2) グリゾグしま 9 取消 He	:lp

図 14 IP Address Poolの作成(3)





14) クライアント端末が使用する DNS サーバのアドレスを入力し、「Next」をクリックします。

anyConnect VPN Conne	ction Setup Wizard
Steps	Network Name Resolution Servers
1. Introduction	This step lets you specify how domain names are resolved for the remote user when accessing the internal network.
2. Connection Profile Identification	DNS Servers: 192.168.1.251 1DNS サーバアドレスを入力します(例:192.168.1.251
3. VPN Protocols	WINS Servers:
4. Client Images	Domain Name:
5. Authentication Methods	
6. Client Address Assignment	
7. Network Name Resolution Servers	
8. NAT Exempt	
9. AnyConnect Client Deployment	
10. Summary	
	②クリックします

図 15 DNS サーバアドレスの設定

15) NAT 除外のルールを作成します。

AnyConnect VPN Connect	ection Setup Wizard
AnyConnect VPN Connect Steps Introduction Connection Profile Identification VPN Protocols Client Images	ction Setup Wizard NAT Exempt If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation. I Exempt VPN traffic from network address translation ①チェックします Inside Interface is the interface directly connected to your internal network. Interface is the interface directly connected to your internal network. Interface is the interface directly connected to your internal
 Authentication Methods Client Address Assignment Network Name Resolut Servers NAT Exempt 	Inside Interfac: inside
9. AnyConnect Client Deployment 10. Summary	The traffic between AnyConnect client and internal network will be exempt from network address translation.
	〈Back Next 〉 預防満 Help

図 16 NAT 除外ルールの設定(1)





16) NAT の除外となる Local Network を選択し、「OK」をクリックします。

A 1	ID Address	Maturali	Deservintion	Object NOT Addre
-Network Objects	I Houless		notwork」を遅ま	
- @		E I III SILLE-I	network」で送	(02.9
- 🚔 inside-n	172.16.1.0	255.255.255.0		
📑 📑 obj_any	0.0.0.0	0.0.0.0		outside (P)
🔤 🚮 wifi-net	192.168.10.0	255.255.255.0		
Interfaces				
- 🔤 inside				
🔤 outside				
- 🔤 wifi				

図 17 NAT 除外ルールの設定(2)

17)「Next」をクリックして先に進みます。

AnyConnect VPN Connection Setup Wizard			
Steps	NAT Exempt		
1. Introduction 2. Connection Profile	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.		
Identification	V Exempt VPN traffic from network address translation		
3. VPN Protocols	Inside Interface is the interface directly connected to your internal network.		
5. Authentication Methods	Inside Interface: inside		
6. Client Address Assignment	Local Network is the network address(es) of the internal network that		
7. Network Name Resolut Servers	Local Network: 172.16.1.0/24		
8. NAT Exempt			
9. AnyConnect Client Deployment	The traffic between AnyConnect client and internal network will be exempt from network address translation.		
10. Summary			
	、 《Back Next> 現決論 Help		

図 18 NAT 除外ルールの設定(3)





18) 「Next」をクリックして先に進みます。

AnyConnect VPN Connection Setup Wizard				
Steps	AnyConnect Client Deployment			
1. Introduction	AnyConnect client program can be installed to a client device by one of the following two methods:			
2. Connection Profile Identification	 Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed; 			
3. VPN Protocols	Pre-deployment - Manually install the AnyConnect client package.			
4. Client Images				
5. Authentication Methods				
 Client Address Assignment 				
 Network Name Resolut Servers 				
8. NAT Exempt				
9. AnyConnect Client Deployment				
10. Summary				
< <u>Back</u> Next> 取消 Hep				

図 19 AnyConnect VPN Client のインストール方法

19) 「Finish」をクリックして Wizard を完了します。

Branch Summary Here is the summary of the configuration.	
Name	Value
Summary	
Name/Alias of the Connection Profile	SSL-VPN
Home VPN Access Interface	outside
Device Digital Certificate	none
VPN Protocols Enabled	SSL only
AnyConnect Client Images	1 package
Authentication Server Group	LOCAL
Address Pool for the Client	192.168.1.1 - 192.168.1.250
DNS	Server: Domain Name:
Network Address Translation	The protected traffic is not subjected to network address translation

図 20 Wizard の完了





20) ASA に実行されるコマンドのプレビューが表示されるので、「Send」をクリックして実行します。



図 21 コマンドのプレビュー

21)「Configuration」>「Remote Access VPN」>「Network (Client) Access」>Group Policies」を開き、「GroupPolicy_SSL-VPN」を選択し、「Edit」をクリックします。

Cisco ASDM 7.5(2)153 for ASA - 172.16.1.254					
File View Tools Wizards W	indow Help Configurat fonitoring Save (フします アレます ck の Forward ? Help	to search Go	uluulu cisco
Device List Bookmarks Device List 교무 × 화 Add 한 Delote 에 Connect	Configuration > Re	policies A VPN group	Network (Client) Access is a collection of user-oriented BADTUC (DAD	> Group Policies authorization attribute/value	pairs that may
Find: Go	by VPN connection	ation attributes from a	n LDAP server you must use a	n LDAP attribute map.	n is reierenceu
Durate Acces (ACDM Accie)	Add - d Edit	Delete Assie 5 Edit 4 Type	n クリックします Tunneling Protocol	Connection Profiles/Use Assigned To	rs
Remote Acces ASDM Assis. Remote Access VPN 🗗 म	GroupPolicy_SSL-V	Internal	ssi-client	SSL-VPN	/Usroup:Letau
Metwork (Client) Access AryCornect Connection Pr AryCornect Quartering AryConnect Olient Stream AryConnect Olient Profile AryConnect Olient Stream AryConnect Olient Stream	emote Acc	.ess VPN]	SroupPolicy_SS	5L-VPN」を選折	します
Bemote Access VPN	Remote A	CCESS VPI	N」をクリックします		
Device Management	Eind	00	Match Case		
×			Apply Reset		
		<admin></admin>	15 😡 📑	🔂 🛛 🔒 🕅	i/02/02 16:08:40 JST

図 22 Group Policyの設定





22) スプリットトンネリングの設定を行います。スプリットトンネリングにより、VPN クライアントは VPN へ接続または切断することなく、セキュリティ保護されたサイトおよび保護されていないサイトの両方に接続するこ



図 23 スプリットトンネリングの設定(1)

23) 右にスクロールし、「Manage」をクリックします。

Edit Internal Group Poli	y: GroupPolicy_SSL-VPN	
- General - Servers - Advanced	basis of a network list that can be specified below by providing the proper par-	ameters to 'Policy' and 'Network List' fields.
Browser Proxy	🗇 Yes 🔿 No	
IPsec(IKEv1) Client	Turnel Network List Below	•
	None	• Manace
	ecurity proxies.	
	ft Clients	¥
		E
		m >
Find	Next Previous	
	OK Cancel	Heb

図 24 スプリットトンネリングの設定(2)





24)「Add」>「Add ACL」を開きます。

[ACL	Manager							×	
	Stan	dard ACL Ex	tended ACL							
	e /	Ndd 🕶 🗹 Ed	🍿 Delete	↑	አ 🖻 🛍	1 -				
	4	Add ACL			Action	Description				
	+	Add ACE								
	2	Insert								
	Ŧ	Insert After	r							

図 25 ACLの設定(1)

25) 「ACL Name」を入力し、「OK」をクリックします。

Add ACL	L Name」を	、 入力します(例:split	t)
ACL Name split			
ОК	Cancel	Help	
<u>②</u> クリ	ックします		

図 26 ACLの設定(2)

26)「Add」>「Add ACE」を開きます。

AC	CL Manager		×
Sta	andard ACL Extended ACL	1	
4	🛚 Add 👻 🛒 Edit 🛅 Delete	ナ チ ぷ ℡ 咄 ~	
4	Add ACL	Action Description	
4	Add ACE		
1	Insert		
1	Insert After		

図 27 ACEの設定(1)





27) ACE の設定をします。

Add ACE	x
1) Permit」を選択します Action:	
Address: ②クリックします	
Description	
OK Cancel Help	

図 28 ACEの設定(2)

28) 「inside-network」を選択し、「OK」をクリックします。

Filter:				Filter Clear
Name	IP Address	Netmask	Description	Object NAT Addre
- Network Obj	^{ects} ①Γins	side-netw	ork」を選択します	-
🚽 🚅 🔤 inside	e-n 172.16.1.0	255.255.255.0		
The will be	IBL 132.100.10.0	200.200.200.0		
1				
Selected Addres	8			

図 29 ACE の設定(3)

29)「OK」をクリックして先に進みます。

🔤 Add AC	CE
Action:	Permit O Deny
Address:	172.16.1.0/24
Descriptio	on:
	OK Cancel Help

図 30 ACE の設定の完了





30)「OK」をクリックして ACL の設定を完了します。

ACL Manager				×
Standard ACL Extend	ed ACL			
🖶 Add 🕶 🗹 Edit 📋	Delete 🛧 🗲 👗 🗈 💼	*		
No Address	Action	Description		
split 1 split 1	10/24 🖌 Permit			
and the second second	- Conne			
		OK Cancel H	łelp	

図 31 ACL の設定の完了

31)「OK」をクリックし、スプリットトンネリングの設定を完了します。

Edit Internal Group Polic	y: GroupPolicy_SSL-\	/PN			_
General	The VPN client make	s split tunneling decisions on th	e basis of a network	list that can be specified below by providing the proper parameters to '	Policy and 🔺
-Servers -Advanced	DNS Names:	📝 Inherit			_
Browser Proxy	Send All DNS Lookup	is Through Tunnel: 📝 Inherit	🔿 Yes 🔘 No	Space, comma, or semicolon delimited entries.	
IPsec(IKEv 1) Client	Policy:	🕅 Inherit	Tunnel Network List	Below	
	IPv6 Policy	🔽 Inherit			
	Network List:	🕅 Inherit	split		_
	Pressing this button Set up Split Exclu	to set up split exlusion for Web sion for Web Security	Security proxies.		
	Intercept DHCP Cor	figuration Message from Micros	oft Clients		
					=
	1				*
Find		Next Previous			
		OK	Cancel	Help	

図 32 スプリットトンネリングの設定の完了





32)「Apply」をクリックして ASA に設定を反映します。

E Cisco ASDM 7.5(2)153 for ASA - 1	.72.16.1.254				
File View Tools Wizards Windo	ow <u>H</u> elp		Type topic	to search Go	ahaha
🚮 Home 🦓 Configuration 🔯 Monit	toring 🔚 Save 🔇	Refresh 🔇 Bac	k 🔘 Forward 🤗 Help		CISCO
Device List Bookmarks	onfiguration > Remo	ote Access VPN	Network (Client) Acces	s > Group Policies	
Device List □ □ × ◆ Add ① Delete Ø Connect Find Go Go ● 172.16.1.254 Go ■ 192.168.1.1 Go	Manage VPN group poi be stored internally on by VPN connection pro To enforce authorization Add • 2	licies A VPN group the device or exter ofiles and user acco on attributes from a Delete X Assign	is a collection of user-oriente nally on a RADIUS/LDAP serv unts. n LDAP server you must use a n	d authorization attribute/value ver. The group policy informatio an LDAP attribute map.	pairs that may n is referenced
	Name	Туре	Tunneling Protocol	Connection Profiles/Use Assigned To	rs
Remote Acces. VPN I P Periode Connect Connection P Production AnyConnect Customication AnyConnect Customication Particulations AnyConnect Client Porfile = Particulations Provide Connect Connection P Presettick's) Connection P Presettick's Connection P P	GroupPolicy CSL-V. 1 DflfGrpPolicy (Syst 1	internal	ssi-client Rev Likev2ssi-clientless;I2tp	SSL-VPN ;p DefaultRAGroup,DefaultL	2LGroup;Defaul
Site-to-Site VPN	Eind		Match Case		
» *		l	Apply Reset	t	
		<admin></admin>	15 🗔 📑	10	3/02/02 17:06:30 JST

図 33 Group Policyの設定完了と設定の反映

33) ASA に実行されるコマンドのプレビューが表示されるので、「Send」をクリックして実行します。



図 34 コマンドのプレビュー

Cisco Start Firewall Cisco ASA 5506-X AnyConnect VPNの設定



3.2 クライアント PC の AnyConnect VPN 設定

本節ではクライアント PC で AnyConnect VPN を設定する手順について説明します。

3.2.1 AnyConnect Secure Mobility Client のインストール

1) クライアント PC で WEB ブラウザを起動し、URL に「http://<ASA の outside の IP アドレス>」を 入力し、ASA にアクセスします。図 35 のように表示されるので、「このサイトの閲覧を続行する」をクリッ クして先に進みます。



図 35 クライアント PC から ASA へのアクセス

2) ASA で設定した VPN クライアントのユーザ名とパスワードを入力してログインします。

	Login				
Please enter you	r username and	passwo	rd.		
GROUP: USERNAME: PASSWORD	SSL-VPN - user01	①グル-	ープを選択しま ②ユーザ名と	す パスワードを入力	っします
[Login ③ク!	トックします	F		
GROUP: USERNAME: PASSWORD	SSL-VPN ▼ user01 Login ③ク! 図 36 ロクイン	 ①グル- 」 」<!--</th--><th>ープを選択しま ②ユーザ名と 5</th><th>す :パスワードを入力</th><th>します</th>	ープを選択しま ②ユーザ名と 5	す :パスワードを入力	します





3) AnyConnect Secure Mobility Clientのインストールを行います。図 37 の画面で「skip」をクリックします。



図 37 AnyConnect Secure Mobility Client のインストール(1)

4) 図 38 の画面が表示されますが、しばらく待ち、「Manual Installation」に進みます。



図 38 AnyConnect Secure Mobility Client のインストール(2)





5) 「AnyConnect VPN」をクリックします。

🖉 Installation - Windows Internet Explorer		
🚱 🕞 🗢 🖻 https:// 🛯 📔 💌 😵 🏭	明 🗟 😽 🗙 🔁 Bing	+ م
🖕 お気に入り 🛛 🏫 🔁 おすすめサイト 🔻	🥭 Web スライス ギャラ 🔻	
6 Installation	🛐 ▼ 🛐 ▼ 🖃 🖶 ▼ ページ(P) ▼ セーフティ(S) ▼	ツール(0) - 🔞 -
 ごの Web サイトは、'Cisco Systems, Inc. す。Web サイトとアドオンを信頼し、アド: 	' からの 'AnyConnect Secure Mobility Client' アドオンを実行(オンの実行を許可するには、ここをクリックしてください	しようとしていま 🗙
cisco AnyC	Connect Secure Mobility Client	_
 WebLaunch Platform Detection - ActiveX - Java Detection - Java - Download - Connected 	Manual Installation Web-based installation was unsuccessful. If you wish to install the Cisco AnyConnect Secure Mobility Client, you may download an installer package. Install module(s) below in the listed sequence. Platforms supported: Windows Desktop AnyConnect VPN ①クリックします Alternatively, refry the automatic installation.	E
	● インターネット 保護モード: 無効 🌾 🔹	• 🔍 100% 👻

図 39 AnyConnect Secure Mobility Client のインストール(3)

6) 「実行」をクリックします。

ファイルのち	プウンロード - セキュリティの警告
このファイル	を実行または保存しますか?
	名前: anyconnect-win-4.2.01035-web-deploy-k9.exe 種類: アプリケーション, 3.46 MB 発信元: 『『【【【TL】
	実行(<u>B</u>) 保存(<u>S</u>) キャンセル
	インターネットのファイルは役に立ちますが、このファイルの種類はコンピューターに問題を起こす可能性があります。発信元が信頼できない場合は、このソフトウェアを 実行したり保存したりしないでください。 <u>危険性の説明</u>

図 40 AnyConnect Secure Mobility Client のインストール(4)

7) 「実行する」をクリックします。



図 41 AnyConnect Secure Mobility Client のインストール(5)





8) End-User License Agreement において「I accept the terms in the License Agree ment」にチェックを要れ、「Next」をクリックします。

방 Cisco AnyConnect Secure Mobility Client Setup
End-User License Agreement Please read the following license agreement carefully
Supplemental End User License Agreement for AnyConnect® Secure Mobility Client v4.x and other VPN-related Software
IMPORTANT: READ CAREFULLY
This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the
◎ I accept the terms in the License Agreement ①チェックします
I do not accept the terms in the License Agreement
Advanced Installer ②クリックします < Back Next > Cancel

図 42 AnyConnect Secure Mobility Client のインストール(6)

9) 「Install」をクリックします。

Cisco AnyConnect Secure Mo	obility Client Setup	X
Ready to Install	1ª	1
The Setup Wizard is ready to be	gin the Typical installation	2
Click "Install" to begin the installa installation settings, click "Back".	ation. If you want to review or change any of your Click "Cancel" to exit the wizard.	
dvanced Installer		
	< Back Install Cancel	

図 43 AnyConnect Secure Mobility Client のインストール(7)





10)「Finish」をクリックしてインストールを完了します。



図 44 AnyConnect Secure Mobility Client のインストールの完了

3.2.2 AnyConnect VPN の接続

1) Windowsのスタートメニューから「Cisco AnyConnect Secure Mobility Client」を起動しま



図 45 Cisco AnyConnect Secure Mobility Clientの起動





2) Cisco AnyConnect Secure Mobility Client が起動したら、VPN の接続先である ASA の ou tside の IP アドレスを入力し、「Cinnect」をクリックします。



図 46 VPN の接続

3) セキュリティ警告のメッセージが表示されますが、「Connect Anyway」をクリックします。



4) ASA で設定した VPN クライアントのユーザ名とパスワードを入力して VPN に接続します。

🕙 Cisco	AnyConne	ct 📭 📲	5 .1		x	
Ω	Please ente	r your userna	me and pass	word.		
	Group:	SSL-VPN			• ①	ブループを選択します
	Username:	user01			2	ユーザ名とパスワードを入力します
	Password:					
			③クリックしま	ます		
			OK	Cance		







5) VPN に接続できると、右下のアイコンに鍵マークが表示され、これをクリックすると Cisco AnyConnec t Secure Mobility Client が起動します。次に「VPN」またはをクリックします。左下のアイコンをクリ



図 49 VPN 接続の完了

6) 統計情報などのステータスが確認できます。

ックします。

/irtual Priv	vate Net	vork (VPN)					
references	Statistics	Route Details	Firewall	Message Hi	story		
-		20				 _	
Connect	tion Inform	ation				~	-
State:		Connect	ed				
Tunnel Mod	de (IPv4):	Split Ind	ude				11
Tunnel Mod	de (IPv6):	Drop All	Traffic				
Duration:	187 B)	00:04:1	7				
Address	Informati	on				~	
Client (IPv	4):	192.168	.1.1				
Client (IPvi	6):	Not Ava	lable				
Server:		13,15.0	.: 22				
Bytes -						~	
Sent:		29956					
Received:		54334					
Framos							-

図 50 VPN クライアントの統計情報





7) ASDM で「Monitoring」>「VPN」>「VPN Statistics」>「Sessions」を開き、VPN クライアントのセッションを確認します。

Cisco ASDM 7.5(2)153 for ASA	- 172.16.1.254	1
File View Tools Wizards W	ndow Hele(1) [Monitoring をクリックレ業等pic to search Go	
onfiguration 🚱 M	onitorine Save 🔇 Refresh 🔾 Back 🔘 Forward 🦓 Help CISCO	
Device List Bookmarks	Monitoring > VPN > VPN Statistics > Sessions	
Device List ☐ ₽ ×		
🕈 Add 📋 Delete 🚿 Connect	Type ④IAnyConnect Client」を確認します Inactive	
Find: Go	AnyConnect Client 1 2 1	
172.16.1.254	SSL/TLS/DTLS 1 2 1	
	Browser 1 1 1	
3 FVPN Statistics	」>「Sessions」をクリックします	
VPN 07 F	Filter By AnyConnect Client - 54 AnyConnect - Client を選択します	
VPN Statistics	Group Policy Assigned IP Address Protocol Details	
Sessions	Ilsername Contoctor Fronto Pablic & Hourses Encryption	Decails JODOD
	user01 GroupPolicy_SSL-VPN 192.168.1.1 AnyConnect-Parent SSL-Tunne Logout	ます
Encryption Statistics Global IKE (IPsec Statist -	Ping	
Protocol Statistics	⑥接続中のユーザのセッションをクリックします	
VLAN Mapping Sessions		
MDM Proxy Statistics		
Clientless SSL VPN		
Easy VPN Client VPN Connection Graphs		
< <u> </u>		
Therfaces		
	127597029 	
Par Bouting	To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.	
State Properties	Logout By: [All Sessions	
Lossing	Refresh	
*	Last Updated: 16/02/02 17:42:14	
Data Refreshed Successfully.	Kadmin> 15 😡 🛃 🔒 16/02/02 17:48:10 JST	

図 51 VPN クライアントセッションの確認

8) 接続中のユーザーのセッションの詳細情報が確認できます。

Group Policy Connection Profile Public IP Address		s Protocol Login Time Encryption Duration			Bytes Tx Bytes Rx		Inactiv	
GroupPolicy_SSL-VPN SSL-VPN	192.168.1.1 10.1.1.1	AnyConn AnyConn	ect-Parent SSL-Tunnel DTL 17: ect-Parent: (1)none SSL-T. 0h:	32:53 JST Tue 10m:46s	26348 45749		0h:00m	
							,	
Local Addr. / Subnet Mask Remote Addr. / Subnet Mas	< / Protocol / Port sk / Protocol / Port	Encryption	Other		Bytes Tx Bytes Rx		More	
		none	Tunnel ID: 3.1 Public IP: 10.1.1 Hashing: none TOP Sic Port 49207 TOP Diet Port 443 Authentication Mode: userPass Idle Time Out: 30 Minutes Client 0S Type: win Client 0S Type: win Client OS Type: win Client Type: AngConnect Client Type: AngConnect Client Type: Clico AngConnect Packets Tx: 10 Packets Tx: 0 Packets Tx: 0 Pac	word Pack 1 /PN Agent for	13174 0	Ш		
		AES-GCM-2.	Turnel ID: 34 Assigned IP: 192.168.1.1 Public IP: 10.1.1.1 Hashing: SHA984 Ciphersuite: ECDHE-ECDSA-A Encapsulation: TLSV12 TOP Src Port 44211 TOP Dst Port 443 Authentication Mode: userPass Ital Time Out: 30 Ministes	ES256-GCM word	6587 61	Ŧ		
	Local Addr. / Subnet Masl	Connection Profile Public IP Address GroupPolicySSL-VPN 192168.1.1 SSL-VPN 19.168.1.1 III.1.1 Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Su	Connection Profile Produces Encryption D D D D D D D D D D D D D D D D D D D	Connection Profile Public IP Address Protocol Durant Time GroupPolicy_SSL-VPN 192.168.1.1 AngConnect-Parent SSL-Tunnel DT1173258.3.ST Tue AngConnect-Parent SSL-Tunnel DT1173258.3.ST Tue AngConnect-Parent (None SSL-T. In Him 46s III Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Connection Profile Provide Profile Provide Profile Duration GroupPolicy_SSL-VPN 192.168.11 AnyConnect-Parent SSL-Tunel DT1732583 UST Ue _28348 SSL-VPN 192.168.11 AnyConnect-Parent SSL-Tunel DT1732583 UST Ue _28348 Umain Umain 45749 Umain Umain Umain Umain Umain Umain	Connect-Pretile Protection During Direction During Direction GroupPolicy_SSL-VPN 192.188.1.1 AnyConnect-Parent SSL-Turnel DTL 173253 JST Tue _ 28348 SSL-VPN 10.1.1 AnyConnect-Parent SSL-Turnel DTL 173253 JST Tue _ 28348 Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Strength Direction Image: Stre	

図 52 VPN セッションの詳細情報

お問い合わせ

Q 製品のご購入に関するお問い合わせ

https://info-networld.smartseminar.jp/public/application/add/152

Q ご購入後の製品導入に関するお問い合わせ

弊社担当営業にご連絡ください。

Q 製品の保守に関するお問い合わせ

保守開始案内に記載されている連絡先にご連絡ください。

本書に記載されているロゴ、会社名、製品名、サービ ス名は、一般に各社の登録商標または商標です。 本書では、®、™、©マークを省略しています。

www.networld.co.jp

