Cisco Start Firewall

Cisco ASA 5506-X サイト間 VPN の設定

2016年3月3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3月3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) ExecJラジオボタンを選 (2) テキストボックスに以下の copy running-config < (3) 「コマンドを実行」ボタンを Destination filename Building configuratio	沢します。 コマンドを入力します。 file name> 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]? n
CLIIこよる設定 CL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 つ Configure つ Configure コマンドを実行 クリア Destination filename [startup-config]? Building configuration [OK]	差や、全てのIOS CU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 サイト間 VPN について	1
2. システム構成	2
2.1 システム構成	2
3. サイト間 VPN の設定およびセッションの確認	4
3.1 サイト間 VPN の設定	4
3.2 サイト間 VPN セッションの確認	10





1. はじめに

本書では Cisco ASA 5506-X におけるサイト間 VPN の設定手順について説明します。

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		

1.2 サイト間 VPN について

サイト間 VPN(Virtual Private Network)とは、IPSec による暗号化および認証を使用し、Cisco ASA 5500 シリーズ等を終端装置としたトンネル技術の名称です。サイト間 VPN により、インターネットを 介してオフィスネットワーク間にセキュアな通信を提供する事ができます。



aladia cisco

2. システム構成

2.1 システム構成

本書でのサイト間 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。ASA-1および AS A-2 は別紙「Cisco ASA 5506-X クイックスタートガイド」の内容に基づいて初期設定を行っており、各 管理 PC から ASDM により ASA にアクセスできる状態および、VPN を終端する両端の ASA が互いに インターネットを介して GE1/1(outside)にアクセスできる状態を前提としています。



凶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- X	OS Version 9.5(2)2 ASDM Version 7.5(2)153	ASA-1 GE1/1 nameif:outside(デフォルト) IP アドレス:DHCP(デフォルト) security level:0(デフォルト) 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) ASA-2 GE1/1 nameif:outside(デフォルト) IP アドレス:DHCP(デフォルト) security level:0(デフォルト) GE1/2 nameif:inside(デフォルト) IP アドレス:172.16.2.254/24 Security level:100(デフォルト)
クライアント PC 兼 管理用 PC		OS : Windows 7 ターミナルアプリケーション (Tera Term) Cisco ASDM-IDM Launcher v1.7 (0)	クライアント PC-1 インタフェース IP アドレス:172.16.1.1/24 クライアント PC-2 インタフェース IP アドレス:172.16.2.1/24





表 3 ASA 5506-X のネットワーク設定

ルーティング	DHCP によりインターネット側へのデフォルトルートを取得
NAT	inside(すべてのトラフィック)→outside への PAT

表 4 VPN のポリシー

設定機器	ピア IP アドレス	ローカルネットワーク	リモートネットワーク	Pre-shared Key	NAT 除外
ASA-1	ASA-2のoutside	172.16.1.0/24	172.16.2.0/24	cisco	inside
ASA-2	ASA-1のoutside	172.16.2.0/24	172.16.1.0/24	cisco	inside



3. サイト間 VPN の設定およびセッションの確認

3.1 サイト間 VPN の設定

本節ではサイト間 VPN の設定手順について説明します。

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



図 2 Site-to-Site VPN Wizardを開く

2) Site-to-Site VPN Wizard が開始されます。「Next」をクリックして先に進みます。



図 3 Site-to-Site VPN Wizard の開始



す。



3) 「Peer IP Address」に VPN ピアとなる IP アドレス(ここでは ASA-2 の ouside)を入力し、「VPN Access Interface」は「Outside」を選択し、「Next」をクリックします。

🔂 Site-to-site VPN Conne	ection Setup Wizard	
Steps	Peer Device Identification	
1. Introduction	This step lets you identify the peer VPN device by its IP address and the interface	ce used to access the peer.
2. Peer Device Identification	Peer IP Address:	①VPN ピアの IP アドレスを入力します
 Traffic to protect 		
4. Security	VPN Access Interface outside	・ ②I OUTSIGE」を選択しま9
5. NAT Exempt		
6. Summary		
	≪ Back Next > 3クリックします	取消 Help

図 4 VPN ピアの設定

4) 「Local Network」にローカルのネットワークセグメント(ここでは ASA-1 の LAN)を、「Remote Net work」に対向側のネットワークセグメント(ここでは ASA-2 の LAN)を入力し、「Next」をクリックしま



図 5 ローカル・リモートネットワークの設定





5) Pre-shared Key (事前共有鍵)を入力し、「Next」をクリックします。

Site-to-site VPN Conne	ection Setup Wizard
Steps	Security
1. Introduction	This step lets you secure the selected traffic.
2. Peer Device Identification	Simple Configuration
3. Traffic to protect	ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security
4. Security	parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.
5. NAT Exempt	Pre-shared Key ●●●●●
6. Summary	
	Customized Configuration
	You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

図 6 Pre-shared Keyの設定

6) NAT 除外の設定を入力し、「Next」をクリックします。

Site-to-site VPN Cor	nnection Setup Wizard	×
Steps	NAT Exempt	
1. Introduction	This step allows you to exempt the local network addresses from network translation.	
2. Peer Device Identification	▼ Exempt ASA side host/network from address translation inside - ②inside を選択します	
3. Traffic to protect		
4. Security	①チェックを入れます	
5. NAT Exempt		
6. Summary		
	Gack Mext> ③クリックします G	取消 Help

図 7 NAT 除外の設定





7)「Finish」をクリックし、設定を完了します。

🔄 Site-to-site VPN Connection Setup Wizard				
VPN Wizard	Summary			
Branch	Here is the summary of the configuration.			
- Ton I	Name	Value		
ISP ISP	Summary Peer Device IP Address			
Home	VPN Access Interface	outside		
Corporate	Protected Traffic	Local Network: 172.16.1.0/24 Remote Network: 172.16.2.0/24		
Network	IKE Version Allowed	IKE version 1 and IKE version 2		
Train .	Authentication Method			
State State	IKE v1	Use pre-shared key		
	IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device =		
SUITING SU	Encryption Policy			
	Perfect Forward Secrecy (PFS)	Disabled		
TITUT	E IKE v1			
TTTT	IKE Policy	rsa-sig-aes-256-sha, pre-share-aes-256-sha, rsa-sig-aes-192-sha, pre-share-aes-192-sha, rsa-sig-aes-sha, pre-share-aes-sha, rsa-sig-3des-sha, pre-share-3des-sha, rsa-sig-des-sha, pre-share-des-sha		
	IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5		
	□ IKE v2			
	IKE Policy	aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha		
< Back Enish 即流 Help				

図8設定の完了

8) 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。

Preview CLI Commands	
The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the ASA, click Send. To not send the commands and continue making changes in ASDM, click Cancel.	
object network. NETWO RK_OBJ_172.16.2.0_24 subnet 172.16.2.0_255.255.05 object network. NETWO RK_OBJ_172.16.1.0_24 subnet 172.16.1.0_256.255.255.0	
access-list outside cryptomap line 1 extended permit ip 172.16.1.0 255.255.255.0 172.16.2.0 255.255.255.0 group-policy GroupPolicy 1 I I I internal group-policy GroupPolicy 1 II I internal ypn-tunnel-protocol ikev2 ikev1 evit	
tunnel-group :],]::; type ipsec=121 tunnel-group :], general-attributes default-group-policy GroupPolicy." I [: 153 : tunnel-group],], [: 1-2] ipsec-attributes ikev1 pre-shared-key *********** ikev2 local-authentication pre-shared-key ************************************	
crypto ikev1 policy 70 encryptoin aes authentication crack crypto ikev1 policy 80 encryptoin aes authentication rsa-sig	
Send Cancel Save To File	

図 9 コマンドのプレビュー





9) 既にサポートされていないコマンドに対するエラーが表示される場合があり、「Close」をクリックします。

Error in sending command	x					
ASDM received messages below when one or more of the commands below were sent to the ASA [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning message received.	۹.					
[OK] ikev2 remote-authentication pre-shared-key ********* [OK] isakmp keepalive threshold 10 retry 2 [OK] crybto ikev1 policy 70 [OK] encrybtion aes [ERROR] authentication crack	* III					
EKRUPS ILEVI policy authentication method crack is no longer supported. Removing ikev1 policy 70 [OK] crypto ikev1 policy 80 [OK] encryption aes [OK] authentication rsa-sig [OK] crypto ikev1 policy 90 crypto ikev1 policy 90 [OK] encryption aes [OK] encryption aes [OK] encryption aes [OK] crypto ikev1 policy 40 crypto ikev1 policy 40 [OK] encryption aes-192 [ERROR] authentication crack						
ERROR IKEV1 policy authentication method crack is no	-					
Close						
図 10 エラーコマンドの表示						

(C) 2016 Networld Corporation





10) 再度コマンドの実行を求められる場合があります。

Site-to-site VPN Connec	tion Setup Wizard	
VPN Wizard	Summary	
Branch	Here is the summary of the configuration.	
CEN T	Name	Value
ISP ISP	Summary	A
	Peer Device IP Address	10.10.153.2
Home	VPN Access Interface	outside
(Corporate)	Protected Traffic	Local Network: 172.16.1.0/24 Remote Network: 172.16.2.0/24
Network	IKE Version Allowed	IKE version 1 and IKE version 2
- Ar	Authentication Method	
and the second	IKE v1	Use pre-shared key
	IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device
	Encryption Policy	
	Perfect Forward Secrecy (PFS)	Disabled
TTUI	E IKE v1	
	IKE Policy	crack-eesersha ras-sig-ases-sha, pre-share-ase-sha, crack-eese-192-sha, rsa-sig-aser12-sha, pre-share-ases-192-sha, crack-ase-256-sha, rsa-sig-ades-z56-sha, pre-share-ase-256-sha, crack-ades-sha, rsa-sig-ades-sha pre-share-3des-sha, crack-des-sha, rsa-sig-des-sha, pre-share-des-sha
	IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD6, ESP-AES-122-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
	□ IKE ∨2	•
	K Back	[ЩС:) Нер



図 11 コマンドの再実行

11) 同様の設定を ASA-2 でも行い、PC-1 と PC-2 の間で通信が成功したら設定完了となります。





3.2 サイト間 VPN セッションの確認

本節ではサイト間 VPN のセッション情報の確認方法について説明します。

 ASDM で「Monitoring」>「VPN」>「VPN Statistics」>「Sessions」を開き、VPN セッションの 詳細情報を確認します。(PC 間で通信を発生させないとセッションは表示されません)

Cisco ASDM 7.5(2)153 for ASA -	172.16.1.254			and a second a			
File View Tools Wizards Wir	nitorine 🔚 Save 🔇	Refresh 🔇 Back	をクリックします O Forward ? Help	Type topic to sea	ch G	olialia cisco	
Device List Bookmarks	Monitoring > VPN > V	/PN Statistics > Se	<u>ssions</u>				
Device List ☐ ₽ × ♣ Add							
Find: Go	Type Site-to-Site VPN	Active	Cumulative	Peak Concurrent 4	Inactive 1		
	IKEv2 IPsec		1	4	1]	
	4VPN t	マション情報	が表示されている	事を確認します			
VPN 0 4							
VPN Statistics 31 V	PN Statisti	cs]> Ses	sions」をクリックし	UET Filter			·
Crypto Statistics	Connection Profile	Protocol	Login Time	Bytes Tx	Cer Auth Int	Ce	⑥クリックします
Compression Statistics	11812. 11812	IKEv2 IPsec IKEv2: (1)AES256 II	06:46:45 UTC Wed Mar 2 20 Psec (0h:00m:20s	016 180 180		Logout	
Okodi Ik.J. Psec. statistics Okodi Ik.J. Psec. statistics VLAN Mapping Sessions MOM Proxy Statistics MOM Proxy Sessions Ocienties SSL VPN Essy VPN Client VR Correction Graphs WSA Sessions	⑤現在張	5れている V	PN セッションを選	択します		Prig	
m	いをクリックし	ます	m			,	
Routing	To sort VPN sessions, i	ight-click on the above	e table and select Table Sort Order	from popup menu.			
Reporties	Logout By All Ses	sions 👻	Logout Ses	sions			
Lossing Lossing			Refre	ish			
» *					Last Update	ed: 16/03/02 18:36:09	
Data Refreshed Successfully.			<admin></admin>	15 💽 🛃 🔂		16/03/02 6:52:42 UTC	

図 12 サイト間 VPN セッション情報の表示

2) セッションの詳細情報が表示されます。

🔁 Se	ssion Details		and N Real	-					— X
Session Details									
Cor	Connection Profile Protocol Login Time IP Address Encryption Duration		Bytes Tx Bytes Rx		Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left		
-31	17 - 513 10. 251	IKEv2 IPsec IKEv2: (1)AES256 IPsec: (.	23:01:53 UTC \ 0h:00m:27s	Wed Mar 2 20	16	780 780			
Det	tails act								
Dei	Idiis AUL								
ID	Туре	Local Addr. / Subnet Mask / Pr Remote Addr. / Subnet Mask / P	otacol / Port rotocol / Port	Encryption	Other		Bytes Tx Bytes Rx		More
	IKEv2			AES-256	Tunnel ID: 5 Loc Auth M Rem Auth N UDP Source UDP Destin Hashing: SH PRF: SHA1 Authenticat UDP Source UDP Destin IKE Negotia Hashing: SH Diffie-Hellm Rekey Time Rekey Lett(1 dote preSharedKeys Mode preSharedKeys Port 500 antion Port 500 on Mode preSharedKeys Port 500 taion Port 500 taion Port 500 taion Port 500 taion Mode: none A1 an Group: 5 Interval 80400 Seconds		E	
	IPsec	172.16.10/2552552550/0/0 172.16.2.0/2552552550/0/0		AES-256	Tunnel ID: 5 Hashing: SH Encapsulatii Rekey Time Rekey Left(Rekey Data Rekey Left(Idle Time O	2 A1 Interval: 28800 Seconds TJ: 28773 Seconds Interval: 4608000 K-Bytes D): 4608000 K-Bytes ut: 30 Minutes	780 780	•	
			Refres	sh Clo	se Hel	q	Last Update	d: 16/0	3/03 10:51:20

図 13 セッション情報の詳細

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

