ASA 間、動的静的間 IKEv1/IPsec の設定例

内容

概要 前提条件 要件 使用するコンポーネント 設定 ネットワーク図 ASDM の設定 中央 ASA (スタテ<u>ィック ピア)</u> リモート ASA(ダイナミック ピア) CLI での設定 <u>中央ASA(スタティックピア)の設定</u> リモート ASA (ダイナミック ピア) 確認 中央 ASA リモート ASA トラブルシュート リモート ASA(イニシエータ) 中央 ASA(レスポンダ) 関連情報

概要

このドキュメントでは、適応型セキュリティ アプライアンス(ASA)が任意のダイナミック ピア (このケースでは ASA)からのダイナミック IPsec サイト間 VPN 接続を受け入れるようにする 方法について説明します。 このドキュメントのネットワーク図に示されているように、IPsec ト ンネルは、トンネルがリモート ASA 側から開始される場合にのみ確立されます。中央 ASA は、 ダイナミック IPsec 設定のために VPN トンネルを開始できません。リモート ASA の IP アドレ スは不明です。

ワイルドカード IP アドレス(0.0.0.0/0)とワイルドカード事前共有キーからの接続をダイナミックに受け入れるように中央 ASA を設定します。その後、リモート ASA は、暗号アクセスリストでの指定に従ってローカル サブネットから中央 ASA サブネットへのトラフィックを暗号化するように設定されます。どちら側でも、IPsec トラフィックのネットワーク アドレス変換(NAT)をバイパスするために NAT 除外が実行されます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco ASA(5510 および 5520)ファイアウォール ソフトウェア リ リース 9.x 以降に基づくものです。

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。

設定

注:このセクションで使用されるコマンドの詳細については、<u>Command Lookup Tool(登</u> <u>録ユーザ専用)を使用してください。</u>

ネットワーク図



ASDM の設定

中央 ASA (スタティック ピア)

スタティック IP アドレスを持つ ASA で、不明なピアからのダイナミック接続を受け入れる一方 で IKEv1 事前共有キーを使用してピアを認証するように VPN をセットアップします。

 [Configuration] > [Site-to-Site VPN] > [Advanced] > [Crypto Maps] の順に選択します。この ウィンドウには、すでに存在する暗号マップ エントリのリストが表示されます(存在する 場合)。 ASA にはピアの IP アドレスが不明であるため、ASA が接続を受け入れるために 、一致するトランスフォームセット(IPsec プロポーザル)を使用してダイナミック マップ を設定します。 [Add] をクリックします。

File View Tools Wizards Window Help						Туре	topic to search	h
🔥 Home 🔥 Configuration 📄 Monitoring 🔚 Save 🔇	Refresh 🕝 Back (🔵 Forward 🧳 Help						
Site-to-Site WPN 0 9	Configuration > 5	te-to-Site VPN > Advi	nced > Crypto Map	x				
Connection Profiles	🔶 Add + 🎬 E.R.	- 🏦 Delete 🛧 🗲	美物園・国	Find 🔠 Diagram				
Gertificate Management Advanced Tunnel Groups	Type:Priority	Traffic Selection Source	Destination	Service Action	Transform Set (IXEv1)	3Psec Proposal (IKEv2)	Peer	PPS P
- REPERT								
Prec Prefragmentation Policies Certificate to Connection Profile Maps								
Crypto Engine								
- B. Device Setup								
Frend								
Remote Access VPN								
G Ste-to-Ste VPN	E foshie letione	las adadas sitas dit	-					
Device Management	Colore works	aly menutive size: 04	•					
				Ap	ply Reset			

 [Create IPsec Rule] ウィンドウの [Tunnel Policy (Crypto Map) - Basic] タブで、[Interface] ドロップダウンリストから [outside] を選択し、[Policy Type] ドロップダウンリストから [dynamic] を選択します。[Priority] フィールドで、ダイナミック マップに複数のエントリが ある場合のこのエントリの優先順位を割り当てます。次に、[IKE v1 IPsec Proposal] フィー ルドの横にある [Select] をクリックして、IPsec プロポーザルを選択します。

	/pto Map) - Basi	Tunnel Policy (Crypto	Map) - Advanced	Traffic Select	ion
Interface:	outside	▼ Policy 1	Type: dynamic	. •	Priority: 1
IPsec Propo	sals (Transform	Sets)			
IKE v1 IPse	: Proposal:				Select
IKE v2 IPse	: Proposal:				Select
-Peer Settin	ns Ontional fo	r Dynamic Crypto Man P	otries		
Peer Settin The Conne for LAN-to- redundant	gs - Optional fo ction Type is app LAN redundancy peers.	r Dynamic Crypto Map B Dicable to static tunnel p V. Tunnel policies of the b	intries olicies only. Uni-di Originate Only' co	rectional conne nnection type r	ction type policies are used nay specify up to 10
Peer Settin The Conne for LAN-to- redundant IP Address	gs - Optional fo ction Type is app LAN redundancy peers. of Peer to Be Ad	r Dynamic Crypto Map B Dicable to static tunnel p V. Tunnel policies of the dded:	intries olicies only. Uni-di Originate Only' co	rectional conne nnection type r	ction type policies are used nay specify up to 10
Peer Settin The Conne for LAN-to- redundant IP Address	gs - Optional fo ction Type is app LAN redundancy peers. of Peer to Be Ar	r Dynamic Crypto Map E Dicable to static tunnel p V. Tunnel policies of the dded:	intries olicies only. Uni-di Originate Only' co	rectional conne nnection type r	ction type policies are used nay specify up to 10 Move Up

3. [Select IPsec Proposals (Transform Sets)] ダイアログボックスが開いたら、現在の IPsec プロポーザルの中から選択するか、[Add] をクリックし、新しいプロポーザルを作成して使用します。完了したら、[OK] をクリックします。

	••••••	rowsy	ayname +	110167.	
sec Propos	als (Transform Sets)				-
V1 IPsec P	Proposal: tset			Select	
V2 IPs	Select IPsec Prop	osals (Transfo	rm Sets)		23
	🗣 Add 📝 Edit	Delete			
		- Contro			
	Name	Mode	ESP Encryption	ESP Authentication	
er Setti	ESP-3DES-SHA	Transport	3DE5	SHA	
Cr Dotta	ESP-3DES-MDS	Transport	3DES	MDS	
e Conne	ESP-DES-SHA	Tunnel	DES	SHA	
dundani	ESP-DES-MD5	Tunnel	DES	MD5	
Jundan	ESP-DES-SHA-T	Transport	DES	SHA	
	ESP-DES-MDS-T	Transport	DES	MD5	E
	tset	Tunnel	AES-256	SHA	-
	Assigned IPsec Pro	posals —			
Addres	Assigned IPsec Pro	posals			
Addres	Assigned IPsec Pro Assign-> ts	posals et			

4. [Tunnel Policy (Crypto Map)-Advanced] タブで、[Enable NAT-T] **チェックボックス(ピアが** NAT デバイスの背後にある場合に必要)と [Enable Reverse Route Injection] チェックボッ クスをオンにします。ダイナミック ピアに対して VPN トンネルが稼働状態になると、ASA は、VPN インターフェイスを指すネゴシエートされたリモート VPN ネットワークのダイナ ミック ルートをインストールします。

Create IPsec Rule	25
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
☑ Enable Reverse Route Injection	
Security Association Lifetime Settings	
Time: 8:0:0 hh:mm:ss	
Traffic Volume: 🔲 unlimited 4608000 KBytes	
ESP v3	
Validate incoming ICMP error messages	
Enable Do Not Fragment (DF) policy	
Enable Traffic Flow Confidentiality (TFC) packets. This is unavailable if IKEv1 is enabled.	
OK Cancel Help	

必要に応じて、[Traffic Selection] タブで、ダイナミック ピアの関心のある VPN トラフィッ クを定義し、[OK] をクリックすることもできます。

Create IPsec	Rule	Σ
Tunnel Policy ((Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
Action: 💿 F	Protect 💿 Do not Protect	
Source Criter	ia	
Source:	any4	
Destination C	Iriteria	
Destination:	any4	
Service:	ip	
Description:		
More Opti	ons	۲
📝 Enable	Rule	
Source Ser	vice: (TCP or UDP service only) 😗	
Time Range	e:	
	OK Cancel Help	

Configuration > Site-	to-Sil	te VPN > Advance	<u>d > Crypto Maps</u>			
🖶 Add 🝷 📝 Edit 👻	<u>î</u> De	elete 🛧 🗲 👗	🗈 💼 - 🛛 🔍 Fir	nd 👥 Diag	ram	
	Traff	ic Selection				
Type:Priority	#	Source	Destination	Service	Action	Transform Set (IKEV1)
🖃 interface: outside						
dynamic: 65535.1	1	🌍 any4	🌍 any4	IP ip	🖌 Protect	tset
•						
📝 Enable Anti-replay	windov	v size: 64 👻				
					Apply	Reset
前述のように、AS	Aに	はリモート ダ	イナミック ピア	の IP ア	ドレスに関	する情報がないた

め、不明な接続要求は、デフォルトで、ASA 上に存在する DefaultL2LGroup に到達します 。認証に成功するには、リモート ピアで設定された事前共有キー(この例では cisco123)が DefaultL2LGroup にあるものと一致する必要があります。

5. [Configuration] > [Site-to-Site VPN] > [Advanced] > [Tunnel Groups] の順に選択して、 [DefaultL2LGroup] を選択し、[Edit] をクリックして必要な事前共有キーを設定します。完了 したら、[OK] をクリックします。

Configure IPsec site-to-site tun Add 🗹 Edit 🏢 Delete	inel groups.		
Name	Group Policy	IKEv1 Enabled	IKEv2 Enabled
DefaultL2LGroup	DfltGrpPolicy		
		Edit IPsec Site-to-site Tunnel Group: DefaultL2LG	iroup
		Name: DefaultL2LGroup	
		IPsec Enabling	
		Group Policy Name: DfltGrpPolicy	✓ Manage
		(Following two fields are attrib	utes of the group policy selected above.)
		V Enable IKE v1 Enable	IKE v2
		IPsec Settings	
		IKE v1 Settings	
		Authentication	
		Pre-shared Key:	
		Device Certificate: None	✓ Manage
		IKE Peer ID Validation: Required	•
		IKE Keepalive	
		Disable keepalives	
		Monitor keepalives	
		Confidence Interval: 10 seconds	
		Retry Interval: 2 seconds	
		OK Cancel	Help

infiguration > Site-to-Site VPN > Advanced > Tunn

- 注:これにより、スタティックピア(中央-ASA)にワイルドカード事前共有キーが作成されます。 この事前共有キーおよびその一致するプロポーザルを認識しているデバイス/ピア は、VPN トンネルを確立し、VPN 経由でリソースにアクセスすることができます。この事 前共有キーが不明なエンティティと共有されていないことと容易に推測できないことを確認 してください。
- 6. [Configuration] > [Site-to-Site VPN] > [Group Policies]を選択し、選択したグループポリシー (この場合はデフォルトのグループポリシー)を選択します。[Edit] をクリックし、[Edit Internal Group Policy]ダイアログボックスでグループポリシーを編集します。完了したら、 [OK] をクリックします。

	Туре	Tunneling Protocol	Connection Profiles/Users Assigned To
irpPolicy (System Default)	Internal	kev1;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultWEBVPI
	Edit Internal Group Pol	icy: DfltGrpPolicy	2
	Name:	DfltGrpPolicy	
	Tunneling Protocols:	Clientless SSL VPN 📄 SSL VPN Client 🕑 IPser	c IKEv1 🔄 IPsec IKEv2 📝 L2TP/IPsec
	Filter:	None	▼ Manage
	Idle Timeout:	Unlimited 30 minutes	
	Maximum Connect Time:	V Linimited minutes	
	PidAmuni Comico, milo,	• or minored	
	Prevention Competer Inter		
	PROVINGIN CONNECC. HINES		
	PROVINGIN CONNECC. HINES	OK Cancel Help	

7. [Configuration] > [Firewall] > [NAT Rules] の順に選択し、[Add Nat Rule] ウィンドウで VPN トラフィックの no nat(NAT-EXEMPT)ルールを設定します。完了したら、[OK] をクリッ クします。

Confi	iguration	> Firewall > NAT Rules					
e 4	Add 🗸 📝	🔤 Add NAT Rule	6 4 million	e		23	
#	Match (Match Criteria: Original Packet					
_	Source Ir	Source Interface:	inside 🔹 👻	Destination Interface:	outside	•	
۷.	Jetwork Ol	Source Address:	10.1.2.0-inside_network	Destination Address:	10.1.1.0-remote_netwo	or	
				Service:	any		
		Action: Translated Packet					
		Source NAT Type:	Static 🔹				
		Source Address:	10.1.2.0-inside_network	Destination Address:	10.1.1.0-remote_netwo	or	
		Use one-to-one address transla	tion				
	- 1	PAT Pool Translated Address:		Service:	Original		
		Round Robin					
		Extend PAT uniqueness to pe	er destination instead of per int	erface			
		Translate TCP and UDP ports	into flat range 1024-65535	Include range 1-1023	3		
		Fall through to interface PAT					
		Use IPv6 for source interface PAT Use IPv6 for destination interface PAT					
		Options				_	
		📝 Enable rule					
		Translate DNS replies that mate	h this rule				
L		Disable Proxy ARP on egress in	terface				
		Lookup route table to locate eg	ress interface				
		Direction: Both 👻					
			OK Cancel	Help			

リモート ASA(ダイナミック ピア)

1. ASDM アプリケーションが ASA に接続したら、[Wizards] > [VPN Wizards] > [Site-to-site VPN Wizard] の順に選択します。

Cisco ASDM 7.1 fo	or ASA - 10.105.130.220
File View Tools	Wizards Window Help
Home 🖓 Conf	Startup Wizard Back C Forward 2 Help
Device List	VPN Wizards Site-to-site VPN Wizard
Add 👔 Delete	High Availability and Scalability Wizard AnyConnect VPN Wizard Unified Communication Wizard Clientlass SSL VPN Wizard
Find:	Packet Capture Wizard IPsec (IKEv1) Remote Access VPN Wizard
- = 10.105.130.51 - = 10.105.130.51 - = 10.105.130.54 - = 10.105.130.72 - = 10.105.130.89	General License Host Name: 121-peer ASA Version: 9.1(3) Device Uptime: 2d 1h 42m 50 ASDM Version: 7.1(4) Device Type: ASA 5520

2. [next] をクリックします。



 [VPN Access Interface] ドロップダウンリストから [outside] を選択し、リモート ピアの外部 IP アドレスを指定します。暗号マップを適用するインターフェイス(WAN)を選択してく ださい。[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 used to access the peer.
2. Peer Device Identification	Peer IP Address: 172.16.2.1
3. Traffic to protect	
4. Security	VPN Access Interface: outside
5. NAT Exempt	
6. Summary	
	< Back Next >

VPN トンネルの通過を許可する必要のあるホスト/ネットワークを指定します。このステップでは、VPN トンネルの [Local Networks] と [Remote Networks] を指定します。必要に応じて、[Local Network] フィールドと [Remote Network] フィールドの横にあるボタンをクリックしてアドレスを選択します。完了したら、[Next] をクリックします。

Site-to-site VPN Connection	on Setup Wizard
Steps	Traffic to protect
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption. IP Address Type: IPV4 IPV6 Local Network: I0.1.1.0/24 IPV6 IPV6 IPV6 IPV6 IPV6 IPV6 IPV6 IPV6
	<back next=""></back>

5. 使用する認証情報(この例では事前共有キー)を入力します。この例で使用する事前共有キーはcisco123です。LAN-to-LAN(L2L)VPNを設定する場合、トンネルグループ名はデフォルトでリモートピアのIPアドレスです。

Site-to-site VPN Connect	ion Setup Wizard
Steps 1. Introduction 2. Peer Device Identificatio 3. Traffic to protect 4. Security 5. NAT Exempt 6. Summary	Security This step lets you secure the selected traffic. Simple Configuration ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IRE and ISARMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer. Pre-shared Key: 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.
	< Back Next > Cancel Help

または任意の IKE および IPsec ポリシーを含むように設定をカスタマイズできます。ピア間 には少なくとも 1 つの一致するポリシーがある必要があります。[Authentication Methods] タブで、[Pre-shared Key] フィールドに IKE バージョン 1 の事前共有キーを入力します。こ の例では、cisco123 です。

		and the local data					
teps	Security						
I. Introduction	This step lets you secure the selected traffic.						
2. Peer Device Identificatio							
Traffic to protect	Simple Configuration						
. Security	ASA uses the pre-shared key entered here that will allow tunnel establishment. It is rec	to authenticate this device commended that this option	with the peer. ASDM will sele is also selected when configu	ct co ring	mmon IKE and ISAKMP the remote peer.	security parameter	rs for
. NAT Exempt							
	 Customized Configuration You can use pre-shared key or digital certific selected for you. 	icate for authentication with	the peer device. You can als	io fin	e tune the data encryp	tion algorithms ASI	DM
	IKE Version Authentication Method	s Encryption Algorithms	Perfect Forward Secrecy				
	IKE version 1						
	Pre-shared Key:	•••••					
	Device Certificate:	None		•	Manage		
	IXE version 2						
	Local Pre-shared Key:						
	Local Device Certificate:	None		Ţ	Manage		
	Demote Deer Dreich wed Verin	·					
	Remote Peer Pre-snared Key.			۰,			
	Barrish Barrish Market A. Market Market	and a second second			Adverse and the second se		

[Encryption Algorithms] タブをクリックします。

6. [IKE Policy] フィールドの横にある [Manage] をクリックし、[Add] をクリックして、カスタム IKE ポリシー(フェーズ 1)を設定します。 完了したら、[OK] をクリックします。

Site-to-site VPN Connects	on Setup Wizard	An Incise of the later of the l	L. L.		
Steps	Security				
1. Introduction 2. Peer Device Identificatio	This step lets you see	ure the selected traffic.			
3. Traffic to protect	Simple Configuration				
4. Security	ASA uses the pre-s that will allow tunn	hared key entered here to authenticate this device with the peer. ASDM will select common IRE and ISAKMP security el establishment. It is recommended that this option is also selected when configuring the remote peer.	/ parameters for		
6. Summary					
	Customized Configuration				
	You can use pre-sh selected for you.	ared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption aig	orithms ASDM		
	IKE Version	Authentication Methods Encryption Algorithms Perfect Forward Secrecy			
	IKE version 1				
	IKE Policy:	crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-192-	Manage		
	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-M	Select		
	IKE version 2				
	IKE Policy:	aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha	Manage		
	IPsec Proposal:	AES256, AES192, AES, 3DES, DES	Select		
	< Back Next	>	ncel Hel		

7. [IPsec Proposal] フィールドの横にある [Select] をクリックして、必要な IPsec プロポーザ ルを選択します。完了したら、[Next] をクリックします。

Steps	Security			
Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary	Simple Configurat ASA uses the pre-s ISAKMP security pa when configuring th Customized Config You can use pre-sh data encryption alg	ture the selected traffic. tion shared key entered here to authenticate this device of arameters for that will allow tunnel establishment. It i he remote peer. iguration hared key or digital certificate for authentication with gorithms ASDM selected for you.	with the peer. ASDM will selec s recommended that this opti the peer device. You can also	t common IKE and on is also selected o fine tune the
	IKE Version	Authentication Methods Encryption Algorithms	Perfect Forward Secrecy	
	IKE version 1			
	IKE Policy:	pre-share-aes-256-sha		Manage
	IPsec Proposal:	ESP-AES-256-SHA		Select
	IKE version 2			
	nor a t	aes-256-sha-sha		Manage
	IKE Policy:			
	IKE Policy: IPsec Proposal:	AES256, AES192, AES, 3DES, DES		Select

必要に応じて、[Perfect Forward Secrecy] タブに移動し、[Enable Perfect Forward Secrecy (PFS)] **チェックボックスをオンにすることができます。**完了したら、[Next] をクリックしま

Steps	Security
Steps I. Introduction 2. Peer Device Identificatio 3. Traffic to protect 4. Security 5. NAT Exempt 6. Summary	Security This step lets you secure the selected traffic. Simple Configuration ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer. 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 ASD selected for you. INE Version Authentication Methods Encryption Algorithms Perfect Forward Secrecy Enable Perfect Forward Secrecy (PFS). If PFS is used, a new Diffie-Heliman exchange is performed for each phase-2 negotiation. It ensures compromised in the future Diffie-Heliman Group:

8. [Exempt ASA side host/network from address translation] チェックボックスをオンにして、 トンネル トラフィックのネットワーク アドレス変換が開始されないようにします。ドロッ プダウンリストから [local] または [inside] を選択してローカル ネットワークに到達可能なイ

ンターフェイスを設定します。[next] をクリックします。

Site-to-site VPN Connection Setup Wizard

Steps	NAT Exempt
1. Introduction	This step allows you to exempt the local network addresses from network translation.
 Peer Device Identificatio Traffic to protect 	Exempt ASA side host/network from address translation inside -
4. Security	
5. NAT Exempt	
6. Summary	
	< back Next >

9. 設定した VPN の概要が表示されます。確認して、[Finish] をクリックします。 Site-to-site VPN Connection Setup Wizard

Branch	Here is the summary of the configuration.			
	Name	Value		
T ISP	Summary			
	Peer Device IP Address	172.16.2.1		
Corporate Network	VPN Access Interface	outside		
	Protected Traffic	Local Network: 10.1.1.0/24 Remote Network: 10.1.2.0/24		
	IKE Version Allowed	IKE version 1 and IKE version 2		
	Authentication Method			
-I the	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		
THINK	Encryption Policy			
HIII	Perfect Forward Secrecy (PFS)	Disabled		
TTT	IKE v1			
- The	IKE Policy	pre-share-aes-256-sha		
_ Tot	IPsec Proposal	ESP-AES-256-SHA		
- NT	□ IKE v2			
100 A 21	IKE Policy aes-256-sha-sha			
	IPsec Proposal	AES256, AES192, AES, 3DES, DES		
	Network Address Translation	The protected traffic is not subjected to network address translation		

ΣZ

CLI での設定

中央 ASA (スタティック ピア)の設定

次の例のように、VPN トラフィックのNO-NAT/NAT-EXEMPT ルールを設定します。
 object network 10.1.1.0-remote_network
 subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-inside_network subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup

2. 任意のリモート ダイナミック L2L ピアを認証するために、DefaultL2LGroup で事前共有キ ーを設定します。

tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123

3. フェーズ 2/ISAKMP ポリシーを定義します。

crypto ikev1 policy 10 authentication pre-share encryption aes-256 hash sha group 2 lifetime 86400

- 4. フェーズ 2 トランスフォーム セット/IPsec ポリシーを定義します。 crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
- 5. 次のパラメータを使用してダイナミック マップを設定します。 必要なトランスフォーム セットリバース ルート インジェクションの有効化:接続されたクライアントのルーティング 情報をセキュリティ アプライアンスが学習することを可能にする(任意) crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset crypto dynamic-map outside_dyn_map 1 set reverse-route
- 6. ダイナミック マップを暗号マップにバインドし、暗号マップを適用して、外部インターフ ェイスで ISAKMP/IKEv1 を有効にします。

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside crypto ikev1 enable outside

リモート ASA(ダイナミック ピア)

1. VPN トラフィックの NAT 除外ルールを設定します。

object network 10.1.1.0-inside_network subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-remote_network subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup

2. スタティック VPN ピアおよび事前共有キーのトンネル グループを設定します。 tunnel-group 172.16.2.1 type ipsec-121 tunnel-group 172.16.2.1 ipsec-attributes ikev1 pre-shared-key cisco123

3. フェーズ 1/ISAKMP ポリシーを定義します。

```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

- 4. フェーズ 2 トランスフォーム セット/IPsec ポリシーを定義します。 crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
- 5. 関心のある VPN トラフィック/ネットワークを定義するアクセス リストを設定します。 access-list outside_cryptomap extended permit ip object 10.1.1.0-inside_network object 10.1.2.0-remote_network
- 6. 次のパラメータを使用してスタティック暗号マップを設定します。 暗号/VPN アクセス リス トリモート IPsec ピアの IP アドレス必要なトランスフォーム セット crypto map outside_map 1 match address outside_cryptomap crypto map outside_map 1 set peer 172.16.2.1 crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
- 7. 暗号マップを適用して、外部インターフェイスで ISAKMP/IKEv1 を有効にします。 crypto map outside_map interface outside crypto ikev1 enable outside

確認

ここでは、設定が正常に動作することを検証します。

アウトプット インタープリタ ツール(登録ユーザ専用)は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

 show crypto isakmp sa: ピアにおける現在の IKE セキュリティ アソシエーション(SA)を すべて表示します。

• show crypto ipsec sa:現在の IPsec SA をすべて表示します。

ここでは、2 つの ASA の検証出力の例を示します。

中央 ASA

Central-ASA#show crypto isakmp sa

IKEv1 SAs:

Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 172.16.1.1 Type : L2L Role : responder Rekey : no State : MM_ACTIVE Central-ASA# show crypto ipsec sa interface: outside Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1 local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) current_peer: 172.16.1.1

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
 #TFC rcvd: 0, #TFC sent: 0
 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
 #send errors: 0, #recv errors: 0
   local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
 path mtu 1500, ipsec overhead 74(44), media mtu 1500
 PMTU time remaining (sec): 0, DF policy: copy-df
 ICMP error validation: disabled, TFC packets: disabled
 current outbound spi: 30D071C0
 current inbound spi : 38DA6E51
 inbound esp sas:
 spi: 0x38DA6E51 (953839185)
     transform: esp-aes-256 esp-sha-hmac no compression
     in use settings ={L2L, Tunnel, IKEv1, }
    slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
    sa timing: remaining key lifetime (kB/sec): (3914999/28588)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
     0x0000000 0x000001F
outbound esp sas:
 spi: 0x30D071C0 (818966976)
    transform: esp-aes-256 esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, IKEv1, }
    slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
    sa timing: remaining key lifetime (kB/sec): (3914999/28588)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
     0x0000000 0x0000001
```

リモート ASA

Remote-ASA#show crypto isakmp sa

IKEv1 SAs: Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 IKE Peer: 172.16.2.1 1 Type : L2L Role : initiator State : MM_ACTIVE Rekey : no Remote-ASA#show crypto ipsec sa interface: outside Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1 access-list outside_cryptomap extended permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0 local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)

current_peer: 172.16.2.1

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frqs needing reassembly: 0
 #TFC rcvd: 0, #TFC sent: 0
 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
 #send errors: 0, #recv errors: 0
   local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
 path mtu 1500, ipsec overhead 74(44), media mtu 1500
 PMTU time remaining (sec): 0, DF policy: copy-df
 ICMP error validation: disabled, TFC packets: disabled
 current outbound spi: 38DA6E51
 current inbound spi : 30D071C0
 inbound esp sas:
 spi: 0x30D071C0 (818966976)
     transform: esp-aes-256 esp-sha-hmac no compression
     in use settings ={L2L, Tunnel, IKEv1, }
    slot: 0, conn_id: 8192, crypto-map: outside_map
    sa timing: remaining key lifetime (kB/sec): (4373999/28676)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
     0x0000000 0x000001F
outbound esp sas:
 spi: 0x38DA6E51 (953839185)
    transform: esp-aes-256 esp-sha-hmac no compression
    in use settings ={L2L, Tunnel, IKEv1, }
    slot: 0, conn_id: 8192, crypto-map: outside_map
    sa timing: remaining key lifetime (kB/sec): (4373999/28676)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
     0x0000000 0x0000001
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

アウトプット インタープリタ ツール(登録ユーザ専用)は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

注:debug コマンドを使用する前に、「デバッグ コマンドの重要な情報」を参照してください。

次のようなコマンドを使用します。

clear crypto ikev1 sa <peer IP address> Clears the Phase 1 SA for a specific peer.

> 注意:clear crypto isakmp sa コマンドは、アクティブな VPN トンネルをすべてクリアする ため、動作の中断をともないます。

PIX/ASA ソフトウェア リリース 8.0(3) 以降では、clear crypto isakmp sa <peer ip address> コマ

ンドを使用して IKE SA を個別にクリアできます。8.0(3) より前のソフトウェア リリースでは、 <u>vpn-sessiondb logoff tunnel-group <tunnel-group-name> コマンドを使用して、1 つのトンネルの</u> <u>IKE および IPsec SA をクリアします。</u>

Remote-ASA#**vpn-sessiondb logoff tunnel-group 172.16.2.1** Do you want to logoff the VPN session(s)? [confirm] INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1

clear crypto ipsec sa peer <peer IP address> !!! Clears the required Phase 2 SA for specific peer. debug crypto condition peer < Peer address> !!! Set IPsec/ISAKMP debug filters. debug crypto isakmp sa <debug level> !!! Provides debug details of ISAKMP SA negotiation. debug crypto ipsec sa <debug level> !!! Provides debug details of IPsec SA negotiations undebug all !!! To stop the debugs デバッグの使用:

debug cry condition peer <remote peer public IP> debug cry ikev1 127 debug cry ipsec 127

リモート ASA (イニシエータ)

次の packet-tracer コマンドを入力してトンネルを開始します。

Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched. Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0 IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0 IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched. Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address 10.1.2.0, Crypto map (outside_map) :

Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +

```
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONCE (13) + VENDOR (13) +
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
.
```

Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1

```
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR ID received 172.16.2.1
:
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin guick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID IPV4 ADDR SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

```
中央 ASA (レスポンダ)
```

```
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
:
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group
DefaultL2LGroup
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED
:
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, IKE Responder starting QM:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Received remote
IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0:
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, Received local
IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,
Protocol 0, Port 0Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
```

with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE

(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52: . Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder, Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0: . Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 2 COMPLETED (msgid=c45c7b30) Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static

route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0

関連情報

- Cisco ASA シリーズ コマンド リファレンス
- ・<u>IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ</u>
- Requests for Comments (RFCs)
- ・テクニカル サポートとドキュメント Cisco Systems