# ASA/PIX:Cisco IOSルータのLAN-to-LAN IPsecトンネルの設定

## 内容

 概要

 前提条件

 要件

 使用するコンポーネント

 表記法

 背景説明

 設定

 ネットワーク図

 設定

 ASDM を使用した設定

 確認

 トラブルシュート

 トラブルシューティングのためのコマンド

<u>関連情報</u>

## <u>概要</u>

このドキュメントでは、内部ネットワークが 1 つである PIX セキュリティ アプライアンス 7.x 以 降または Adaptive Security Appliance(ASA)から、暗号イメージを実行する 2611 ルータへの IPSsec トンネルの設定方法を示します。話を簡単にするため、スタティック ルートを使用しま す。

ルータと PIX の間の LAN-to-LAN トンネル設定の詳細については、『<u>ルータから PIX へ間の</u> IPSec の設定』を参照してください。

PIX ファイアウォールと Cisco VPN 3000 コンセントレータの間の LAN-to-LAN トンネル設定の 詳細については、『<u>Cisco VPN 3000 コンセントレータと PIX ファイアウォール間の LAN-to-LAN</u> IPSec トンネルの設定例』を参照してください。

LAN-to-LAN トンネルが PIX と VPN コンセントレータの間に存在するシナリオの詳細については 、『<u>PIX 7.x および VPN 3000 コンセントレータ間の IPSec トンネルの設定例』を参照してくだ</u> <u>さい。</u>

複数の PIX 間の LAN-to-LAN トンネルが、VPN クライアントがハブ PIX を介してスポーク PIX にアクセスすることを許可するシナリオの詳細については、『<u>TACACS+ 認証を使用した</u> <u>PIX/ASA 7.x 拡張 Spoke-to-Client VPN の設定例』を参照してください。</u>

PIX/ASA セキュリティ アプライアンスでソフトウェア バージョン 8.x が稼働している場合の同 様のシナリオについては、『<u>SDM:ASA/PIX および IOS ルータ間の Site-to-Site IPsec VPN の設定</u> ASA 関連の設定が ASDM GUI を使用して表示され、ルータ関連の設定が Cisco CP GUI を使用して表示される同様のシナリオについては、『<u>Configuration Professional:ASA/PIX および IOS ルー</u> <u>夕間の Site-to-Site IPsec VPN の設定例』を参照してください。</u>

# 前提条件

### <u>要件</u>

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、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。

- PIX ソフトウェア バージョン 7.0 が稼働する PIX-525
- Cisco IOS(R) ソフトウェア リリース 12.2(15)T13 が稼働する Cisco 2611 ルータ

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。

### <u>表記法</u>

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

# <u>背景説明</u>

PIX では、access-list および nat 0 コマンドが連携して機能します。10.1.1.0 ネットワーク上のユ ーザが 10.2.2.0 ネットワークにアクセスする際には、10.1.1.0 ネットワークのトラフィックを Network Address Translation (NAT; ネットワーク アドレス変換)を行わずに暗号化することを 許可するために、アクセス リストが使用されます。 ルータでは、10.2.2.0 ネットワークのトラフ ィックを NAT 変換せずに暗号化することを許可するために、route-map コマンドと access-list コマンドが使用されます。しかし、同じユーザが他の場所にアクセスする際には、Port Address Translation (PAT; ポート アドレス変換)によりアドレス 172.17.63.230 に変換されます。

トラフィックがトンネルでは PAT を通過しないようにし、インターネットへのトラフィックは PAT を通過するようにするためには、PIX セキュリティ アプライアンスで次の設定コマンドが必 要です。

access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0



このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して います。

**注:このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(**登録ユーザ専用)を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

### <u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



### <u>設定</u>

これらの設定例は、コマンドライン インターフェイス用のものです。ASDM を使用して設定する 場合は、このドキュメントの「<u>Adaptive Security Device Manager(ASDM)を使用した設定」を</u> <u>参照してください。</u>

- <u>本社の PIX</u>
- <u>ブランチ ルータ</u>

#### 本社の PIX

HQPIX(config)#**show run** PIX Version 7.0(0)102 names

interface Ethernet0 description WAN interface nameif outside

```
security-level 0
ip address 172.17.63.229 255.255.255.240
1
interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname HQPIX
domain-name cisco.com
ftp mode passive
clock timezone AEST 10
access-list Ipsec-conn extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
access-list nonat extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
pager lines 24
logging enable
logging buffered debugging
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0
access-group 100 in interface inside
route outside 0.0.0.0 0.0.0.0 172.17.63.230 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
```

```
mgcp-pat 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partner protocol tacacs+
username cisco password 3USUcOPFUiMCO4Jk encrypted
http server enable
http 10.1.1.2 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
crypto ipsec transform-set avalanche esp-des esp-md5-
hmac
crypto ipsec security-association lifetime seconds 3600
crypto ipsec df-bit clear-df outside
crypto map forsberg 21 match address Ipsec-conn
crypto map forsberg 21 set peer 172.17.63.230
crypto map forsberg 21 set transform-set avalanche
crypto map forsberg interface outside
isakmp identity address
isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
tunnel-group 172.17.63.230 type ipsec-121
tunnel-group 172.17.63.230 ipsec-attributes
pre-shared-key *
class-map inspection_default
match default-inspection-traffic
1
policy-map asa_global_fw_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect http
1
service-policy asa_global_fw_policy global
Cryptochecksum: 3a5851f7310d14e82bdf17e64d638738
```

: end SV-2-8# ブランチ ルータ BranchRouter#**show run** Building configuration... Current configuration : 1719 bytes 1 ! Last configuration change at 13:03:25 AEST Tue Apr 5 2005 ! NVRAM config last updated at 13:03:44 AEST Tue Apr 5 2005 Ţ version 12.2 service timestamps debug datetime msec service timestamps log uptime no service password-encryption ! hostname BranchRouter 1 logging queue-limit 100 logging buffered 4096 debugging ! username cisco privilege 15 password 0 cisco memory-size iomem 15 clock timezone AEST 10 ip subnet-zero 1 1 1 ip audit notify log ip audit po max-events 100 ! ! crypto isakmp policy 11 encr 3des authentication pre-share group 2 crypto isakmp key cisco123 address 172.17.63.229 crypto ipsec transform-set sharks esp-des esp-md5-hmac 1 crypto map nolan 11 ipsec-isakmp set peer 172.17.63.229 set transform-set sharks match address 120 ! 1 no voice hpi capture buffer no voice hpi capture destination !

```
mta receive maximum-recipients 0
!
!
!
interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan
interface Ethernet0/1
ip address 10.2.2.1 255.255.255.0
ip nat inside
half-duplex
ip nat pool branch 172.17.63.230 172.17.63.230 netmask
255.255.255.0
ip nat inside source route-map nonat pool branch
overload
no ip http server
no ip http secure-server
ip classless
ip route 10.1.1.0 255.255.255.0 172.17.63.229
access-list 120 permit ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 130
!
call rsvp-sync
1
1
mgcp profile default
1
dial-peer cor custom
!
!
!
1
!
line con 0
line aux 0
line vty 0 4
login
!
1
end
```

# <u>ASDM を使用した設定</u>

この例では、ASDM GUI を使用した PIX の設定方法を示します。ブラウザを搭載し、IP アドレ

スが 10.1.1.2 である PC が、PIX の内部インターフェイス e1 に接続されています。PIX で http が有効であることを確認します。

この手順は、本社の PIX の ASDM 設定を示しています。

1. PC を PIX に接続し、ダウンロード方式を選択します。



ASDM は、PIX から既存の設定をロードします。

Device Information				Interface Stat	us			
General License				Interface	IP Address/Mas	k Line	Link	Current Kbps
Host Name:								
PDC Version:	Device	Uptime:						
Firewall Mode:	Device	туре.						
Total Flash:	Status:	-	_			<u>×</u>		
VPN Status	50	Please wai	while ASOM is li	ading the curren	t configuration from	white		
IKE Tunnels:	- <b>*</b>	device.	C THING PLOCHING IN	and a second	comparator for	- Jour -		
	P.	Initializing	62 Monitor modules	9 <b>4</b>	J		Total:	
Memory Memory Usa								
				input Kbp	e	Output Kbp	r.	
Latest ASDM Syslog Mes	sages							

次のウィンドウでは、監視ツールとメニューが示されます。

1 Cisco ASDM 5.0 for PIX - 10.1.1.1	
File Rules Search Options Tools Wizards Help	
Home Configuration Monitoring Back Forward Search	Refresh Save Help
Device Information	Interface Status
General License	Interface IP Address/Mask Line Link Current Kbps
Host Name: SV-2.8 cisco.com	inside 10.1.1.1/24 O up O up 1
PIX Version: 7.0(0)102 Device Uptime: 0d 0h 24m 50s	
ASDM Version: 5.0(0)73 Device Type: PIX 525	
Firewall Mode: Routed Context Mode: Single	
Total Flash: 16 MB Total Memory: 256 MB	Collect as interface to view insult and autout Views
VPN Status	Traffic Status
IKE Tunnels: 0 IPSec Tunnels: 0	Connections Per Second Usage
System Resources Status CPU CPU Usage (percent) 01 04:57:48 Memory 61 62 63 64 92 04:55:48 Memory Usage (MB) 128 04:55:48 CPU Usage (MB) 128 CPU Usage (MB) CPU Usage (MB) 128 CPU Usage (MB) CPU Usage (MB) 128 CPU Usage (MB) CPU Usage	0.5 0.5 0.5 0.5 0.5 0.5 0.5 0.5
Syslog Disabled Device configuration loaded successfully.	≤admin> NA (15)

2. [Configuration] > [Features] > [Interfaces] の順に選択して、新しいインターフェイスの場合 は [Add] を、既存の設定の場合は [Edit] **を選択します。** 

s Conf	Iguration + Features + Im	erfaces					-	-	_	-
	Same II v	V 85 57 8	5.01							
	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU		D
icy E	themeti	inside	Yes	100	10.1.1.1	255.255.255.0	No.	1500		
E	themet0	outside	Yes	0	172.17.63.229	255 255 255 240	No	1500	WAN interface	
e	themet2		No				No			
E	themet3		No				No			
E	theme14		No.				No			
	themet5		No				No			
						1		-		-
cks on						3				3

3. 内部インターフェイスのセキュリティ オプションを選択します。

File Rules Search								-1910
Home Conf	Guration Monitoring	ands Help	Q Refresh	Save Help			Cis	CO SYSTEMS
Features	infiguration > Features >	Security Policy > Access 8	Rules					
Piterfaces		AR Underfaces	s C Service Policy Ru Show Alt	es				
Security Policy	# Rule Enabled Action	Source Host/Network	Destination HostNetwork	Rule Applied	Interface	Service	Log Level Interval	Add
品	1 🗷 🧭	🔹 any	🔹 any	al incoming in	iside	<b>₽</b> ₽		Edit
VPN VPN Rouling Building Blocks								Delete
Device Administration Properties	< ✓ Allow traffic (	3 Deny traffic	Dent			F Show Summary	C Show Detail	
Wizards 🕗		лару	Heset	Advanc	eg			

4. NAT 設定では、暗号化されたトラフィックは NAT の対象外になり、それ以外のすべてのト

#### ラフィックは外部インターフェイスに対しては NAT/PAT の対象です。

	2		0 0 1	0 0	0 9		Cis
one Con	figuration	Monitoring	Back Forward	Search Refresh	Save Help		
atures G	ortiguration +	Features > NA	T = Translation Rules				-
- 1	<ul> <li></li></ul>	3 🔒 🕺					
arlaces	Enable to	raffic through th	e firewall without addres	s translation			
3	(* Translati	ion Rules	C Translation Exer	ption Rules			
ntry Policy	Show Rule	s for Interface:	All Interfaces	Show All			
NAT	Rule		Original			Translated	
3	Туре	Interface	Source Network	Destination Network	Interface	Address	DNS Rewrite
VPN	L in	nside	c 10.1.1.0/24	🤹 any	outside	172 17.63.2290nterface PAT)	No
0140							
perties							
nistration	-						x
perties	+ I √+ Static N	4AT 411 C	lynamic NAT 🔒 St	affic Policy NAT .D D	ymamic Policy N#	NT	Manago Pools
nitration D perties		4AT 웹 C	lynamic NAT 👍 St	NTIC Policy NAT . D	ynamic Policy № Reset	ат 	Manage Pools
reithation Egenties zands //	Static N	WT HI C	lynamic NAT 4 35	atic Policy NAT . D D	ynamic Policy N/ Reset	ят 	Manage Pools
zards ×	्। चं- Static N	4AT 쉡 C	lynamic NAT 👍 St	Nic Policy NAT . D Asply	J ynamic Policy № Reset cisco	NA (2)	Manage Pools
Izards /	eneral]	₩T ∰10	hmamic NAT 🔔 St	ntic Policy NAT ゆロ 	」 Reset cisco て、トン	xī   	▲ Manage Pools ▲ 45/05 3 26 2 名効にしま
zards VI > [G	• Static N • Static N eneral]	₩T ∰ 0	hmamic NAT 🖓 St	Mic Policy NAT ゆロ <u>Asply</u> D順に選択し	」 Reset cisco て、トン	™ ™ (2) <b>₽ ₽</b> *ネル グループを	▲ <u>Manage Pools</u> ▲ 4/6/05 3 26 2 名 対にしま



6. [VPN] > [IKE] > [Global Parameters] の順に選択して、外部インターフェイス上で IKE を有

#### 効にします。



7. [VPN] > [IKE] > [Policies] の順に選択して、IKE ポリシーを選択します。



8. [VPN] > [IPsec] > [IPsec Rules] の順に選択して、ローカル トンネルとリモート アドレッシ

## ング用の [IPsec] を選択します。

Home	Configuration Monitoring Back	Forward	Search	Refresh Save	? Help		and how of the
Features	Configuration + Features + VPN + IPSet	> IPSec Ri	iles				
Interfaces interf	A Client Update     Clien	IPSec R Use the	ules a Rules menu, Action protect P	he toolbar, or the right r PDC Side HostiNotwork	mouse button to add, edit or Remote Side HostNetwork C <sup>2</sup> 10.2.2.0/24	felete rules.	Turmel Po Add Delete

9. [VPN] > [IPsec] > [Tunnel Policy] を選択して、トンネル ポリシーを選択します。

File Roles E	Rearch Options Tools Wizards Help						
Home	Configuration Montoring Back	Porward Search	Retresh	Save Help			Casco Systems
Features	Configuration > Features > VPN > IPSec >	<ul> <li>Turinel Policy</li> </ul>					
Interfaces	General     G	Turnel Policy Specify Turnel Policy Interface outside	Type & Priority Static - 21	Transform Set avalanche	Peer 172 17 63 230	Connection Type Bisirectional 01	SA Add
VPN 425 Routing Duilding Diocks Device Administration Device Administration	Okobal Parameters     Policies     Policy     Policy     Policy     Policy     Prese     Policy     Prese     Policy     Prese     Policy	*					Delete
Wizards			Acp		Reset		

10. [VPN] > [IPsec] > [Transform Sets] の順に選択して、トランスフォーム セットを選択しま

す。							
Cisco ASDM	5.0 for PIX - 10.1.1.1		100		1		_10 ×
File Hotes I	Control Oppons Tobis Wizards Hep	O Q	a	2			Cosco Systems
Home	Configuration Montoring Back	Forward Search	Retreath	Save Help			all mailton
Features	Configuration > Features > VPN > IPSec	> Transform Sets					
Interfaces Security Policy NAT NAT Security Policy NAT Security Po	Client Update  Client Update  Client Update  Client Update  Client Update  Control and Coup  Control	Transform Sets Specify Transform Sets System ESP-DES-SHA ESP-DES-MD5 ESP-AES-128-SHA ESP-AES-128-SHA ESP-AES-128-SHA ESP-AES-128-SHA ESP-AES-256-SHA ESP-AES-256-SHA ESP-AES-256-MD5	Node Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel Tunnel	ESP Encryption DES DES 3DES AES-128 AES-128 AES-128 AES-192 AES-192 AES-256 AES-256	ESP Authentication MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5 SHA MD5	AH Authentication None None None None None None None No	Add Edt Delete
Wizards		1		/dphy	Reset	]	

11. [Routing] > [Routing] > [Static Route] **の順に選択して、ゲートウェイ ルータへのスタティ ック ルートを選択します。**この例では、簡単にするため、スタティック ルートはリモート VPN ピアを指します。

Cisco ASDM 5.	0 for PIX - 10.1.1.1	ete Holo					
Home C	Configuration Montoring	Back Forward 1	Q Q Retresh	Save Help			Cisco Systems
Features	Configuration > Features > P	louting + Routing + Static Re	oute				
Electric ces Security Policy Security Policy Security Policy Security Policy Security Policy NAT Security Policy NAT Security Policy NAT Security Policy NAT Security Policy Security Policy Securi	GRUING     GRUING     GRIP     GOSPF     GOSPF     GOSPF     GOSPF     GMULICASI     GMP     GMP     GMROUTE	Static Route Specify static routes.	Address Netro	ask Oateway IP 172.17.63.230	Metric 1	Tunneled No	Add Edit Delete
				Apply	Reset		
Wizards /	1		-	cisco NA	(7) <b>D</b>		05 3 39 36 PM AEST

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

- show crypto ipsec sa:フェーズ2のセキュリティ アソシエーションを表示します。
- show crypto isakmp sa:フェーズ1のセキュリティ アソシエーションを表示します。

# <u>トラブルシュート</u>

ASDM を使用すると、ロギングを有効にしてログを表示できます。

- [Configuration] > [Properties] > [Logging] > [Logging Setup]の順に選択して、[Enable Logging] を選択し、[Apply] をクリックしてロギングを有効にします。
- [Monitoring] > [Logging] > [Log Buffer] > [On Logging Level] の順に選択して、[Logging Buffer] を選択し、[View] をクリックしてログを表示します。

### <u>トラブルシューティングのためのコマンド</u>

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。 注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

- debug crypto ipsec:フェーズ2の IPSec ネゴシエーションを表示します。
- debug crypto isakmp:フェーズ1の ISAKMP ネゴシエーションを表示します。
- debug crypto engine:暗号化されたトラフィックを表示します。
- clear crypto isakmp:フェーズ1に関連したセキュリティアソシエーションをクリアします。
- clear crypto sa:フェーズ2に関連したセキュリティ アソシエーションをクリアします。
- debug icmp trace:ホストからの ICMP 要求が PIX に到達するかどうかを表示します。この デバッグを実行するには、access-list コマンドを設定に追加して、ICMP を許可する必要が あります。
- logging buffer debugging: PIX を通過する、ホストへの確立された接続と拒否された接続を 表示します。情報は PIX ログ バッファに保存され、show log コマンドを使用して出力を確認 できます。

# 関連情報

- <u>一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について</u>
- <u>Cisco PIX Firewall ソフトウェア</u>
- <u>Cisco Secure PIX ファイアウォール コマンド リファレンス</u>
- セキュリティ製品に関する Field Notice (PIX を含む)
- <u>Requests for Comments (RFCs)</u>