PIX/ASA(バージョン 7.x 以降)ネットワーク アドレス変換を使用した IPSec VPN トンネルの 設定例

目次

概要 前提条件 要件 使用するコンポーネント 表記法 関連製品 設定 ネットワーク図 設定 PIX セキュリティ アプライアンスとアクセス リストの設定 PIX セキュリティ アプライアンスおよび MPF(モジュラ ポリシー フレームワーク)の設定 確認 トラブルシューティング <u>ルータ IPsec のトラブルシュー</u>ティング コマンド セキュリティ アソシエーションのクリア PIX のトラブルシューティング コマンド 関連情報

<u>概要</u>

この設定例では、ネットワーク アドレス変換(NAT)を実行するファイアウォール経由の IPSec VPN トンネルを示します。 Cisco IOS® ソフトウェアの 12.2(13)T より前のリリースを使用して いる場合、この設定はポート アドレス変換(PAT)では動作しません。 この種の設定は、IP ト ラフィックのトンネル伝送に使用できます。 IPX やルーティング アップデートなど、ファイアウ ォールを経由しないトラフィックの暗号化には、この設定は使用できません。 総称ルーティング カプセル化(GRE)トンネリングの方が適しています。 この例で、Cisco 2621 ルータおよび 3660 ルータは 2 つのプライベート ネットワークを結合する IPsec トンネル エンドポイントで、 中間の PIX に IPsec トラフィックを許可するためのコンジットまたはアクセス コントロール リ スト(ACL)があります。

注: NAT は 1 対 1 のアドレス変換です。多(ファイアウォールの Inside)対 1 の変換である PAT と混同しないでください。 NAT の動作と設定についての詳細は、『<u>NAT オペレーションの検証</u> <u>と NAT の基本的なトラブルシューティング</u>』または『<u>NAT の動作</u>』を参照してください。

注: PAT を使用する IPsec は、トンネル外部のエンドポイントのデバイスが1つの IP アドレスか らの複数のトンネルを処理できないために、正しく動作しない場合があります。 トンネルのエン ドポイント デバイスが PAT で動作するかどうかを判断するには、ベンダーにお問い合わせくだ さい。また、Cisco IOS ソフトウェア リリース 12.2(13)T 以降では、PAT に対して NAT 透過機 能を使用できます。詳細については、『<u>IPSec NAT 透過</u>』を参照してください。 Cisco IOS ソフ トウェア リリース 12.2(13)T 以降のこれらの機能についての詳細は、『<u>NAT を使用した IPSec</u> <u>ESP のサポート</u>』を参照してください。

注: Cisco テクニカル サポートでサービス リクエストをオープンする前に、『<u>NAT に関する</u> FAQ』を参照してください。よくある質問に対する多くの回答があります。

PIX バージョン 6.x 以前の NAT を使用したファイアウォール経由の IPsec トンネルを設定する方 法の詳細については、『<u>NAT を使用したファイアウォール経由の IPSec トンネルの設定</u>』を参照 してください。

<u>前提条件</u>

要件

このドキュメントに関しては個別の要件はありません。

<u>使用するコンポーネント</u>

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くものです。

- Cisco IOS ソフトウェア リリース 12.0.7 T (Cisco IOS ソフトウェア リリース 12.2(13)T より前)最新のバージョンについては、『IPSec NAT 透過』を参照してください。
- Cisco 2621 ルータ
- Cisco 3660 ルータ
- •7.x 以降が稼働する Cisco PIX 500 シリーズ セキュリティ アプライアンス

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中 のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してくだ さい。

表記法

ドキュメント表記の詳細は、『<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。

関連製品

このドキュメントは、ソフトウェア バージョン 7.x 以降を実行する Cisco 5500 シリーズ適応型 セキュリティ アプライアンス(ASA)でも使用できます。

<u>設定</u>

このセクションでは、このドキュメントで説明している機能の設定に使用するための情報を説明 します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、<u>コマンド検索ツール(登録</u>

<u>ユーザ専用</u>)を使用してください。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク構成を使用しています。



10.3.3.2

<u>設定</u>

このドキュメントでは、次の設定を使用します。

- ・<u>Cisco 2621 の設定</u>
- Cisco 3660の設定
- PIX セキュリティ アプライアンスとアクセス リストの設定Advanced Security Device Manager GUI (ASDM)の設定コマンド ライン インターフェイス (CLI)の設定
- PIX セキュリティ アプライアンスおよび MPF(モジュラ ポリシー フレームワーク)の設定

Cisco 2621

```
Current configuration:
1
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
 !
hostname goss-2621
 1
ip subnet-zero
 !
ip audit notify log
ip audit po max-events 100
isdn voice-call-failure 0
cns event-service server
 1
!--- The IKE policy. crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
crypto ipsec transform-set myset esp-des esp-md5-hmac
 1
crypto map mymap local-address FastEthernet0/1
!--- IPsec policy. crypto map mymap 10 ipsec-isakmp
 set peer 99.99.99.2
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
1
controller T1 1/0
 1
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 1
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
!--- Apply to the interface. crypto map mymap
1
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
no ip http server
```

```
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
line con 0
 transport input none
line aux 0
line vty 0 4
 !
no scheduler allocate
end
Cisco 3660
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
 1
hostname goss-3660
 1
ip subnet-zero
 1
cns event-service server
 1
!--- The IKE policy. crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.12
crypto ipsec transform-set myset esp-des esp-md5-hmac
 crypto map mymap local-address FastEthernet0/0
!--- The IPsec policy. crypto map mymap 10 ipsec-isakmp
 set peer 99.99.99.12
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
interface FastEthernet0/0
 ip address 99.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
!--- Apply to the interface. crypto map mymap
 1
interface FastEthernet0/1
 ip address 10.3.3.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 duplex auto
 speed auto
 Т
 interface Ethernet3/0
 no ip address
 no ip directed-broadcast
 shutdown
 !
```

```
interface Serial3/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 Т
interface Ethernet3/1
 no ip address
 no ip directed-broadcast
 interface Ethernet4/0
 no ip address
 no ip directed-broadcast
 shutdown
 !
interface TokenRing4/0
 no ip address
 no ip directed-broadcast
 shutdown
 ring-speed 16
 !
!--- The pool from which inside hosts translate to !---
the globally unique 99.99.99.0/24 network. ip nat pool
OUTSIDE 99.99.99.70 99.99.99.80 netmask 255.255.255.0
!--- Except the private network from the NAT process. ip
nat inside source route-map nonat pool OUTSIDE
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.1
no ip http server
 1
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 101 deny ip 10.3.3.0 0.0.0.255 any
!--- Except the private network from the NAT process.
access-list 110 deny ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
access-list 110 permit ip 10.3.3.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
1
line con 0
 transport input none
line aux 0
line vty 0 4
 1
 end
```

<u>PIX セキュリティ アプライアンスとアクセス リストの設定</u>

<u>ASDM 5.0 の設定</u>

ASDM を使用して PIX Firewall バージョン 7.0 を設定するには、次の手順を実行します。

1. PIX にコンソール接続します。 クリアな設定から、インタラクティブなプロンプトを使用して、Workstation 10.1.1.3 から Advanced Security Device Manager GUI(ASDM)で PIX を 管理できるようにします。

- 2. Workstation 10.1.1.3 から、Web ブラウザを開いて、ADSM を使用します(この例では https://10.1.1.1)。
- 3. 認証のプロンプトで [Yes] を選択し、<u>PIX Firewall ASDM のブートストラップ構成</u>で設定さ れているイネーブル パスワードでログインします。
- 4. PC 上で初めて ASDM を実行する場合は、ASDM Launcher を使用するのか、それとも Java App として ASDM を使用するのかを尋ねるプロンプトが出ます。この例では、ASDM Launcher が選択され、インストールされます。
- 5. [ASDM Home] ウィンドウに移動して、[Configuration] タブを選択します。

Home Configuration M	onitoring Back Forward Se	arch Refresh	Save Help		
Device Information		Interface Sta	tus		
General License		Interface	IP Address/Mask	Line Link	Current Kops
Host Name: pixfirewall.c	isco.com	inside	10.1.1.1/24	onb onb	1
P0(Version: 7.0(0)102	Device Uptime: Od Oh 3m 53s				
ASDM Version: 5.0(0)73	Device Type: PIX 515E				
Firewall Mode: Routed	Context Mode: Single				
Total Flash: 16 MB	Total Memory: 64 MB	Select so inter	face to view input and	output Khns	
VPN Status		- Traffic Statu	s	ouputrops	
IKE Tunnels: 0	IPSec Tunnels: 0	Connections	Per Second Usage		
CPU CPU Usage (perc 07 10:20:28 Memoty 10:20:28 CPU Usage (perc 10:20:18 Memoty 10:20:18 CPU Usage (perc 10:20:18 Memoty Usage (perc	sent)	0.5 10.20:18 UDP: 0 'inside' Inter 1.5 1.5 10.20:18 Input Ka	TCP: 0 lace Tramo Usage (Kbps) ps: 0	Total: 0 Output Kbps: 1	
-Latest ASDM Syslog Messag	es Syslog Disabled			Contigues A	

6. **イーサネット 0 インターフェイス**を強調表示し、[Edit] をクリックして外部インターフェイ スを設定します。

Eisco ASDM 5. File Rulas Be	.0 for and	PTX - 10.1 Options	.1.1 Tools Wizard	s Help						_ 🗆 🗙
👘 Ноте	Confi	Guration	Monitoring	O Back F	orward	Q Search	Refresh S	Savve Help		CISCO SYSTEMS
Features	Co	nfiguration	> Features > Int	erfaces	21.001					
Interfaces	35	.H. ¥			31991					
<u>,</u>			Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only MTU	Add
Security Policy		Ethernet1		inside	Yes	100	10.1.1.1	255.255.255.0	No 1500	Edit
NAT		Ethernetü			No				No	Delete
SS VPN										
AZA Routing										
Building Blocks										
Device Administration										
D		•							•	
Properties		Enable	traffic between t	we or more inf	lerfaces w	hich are co	onfigured with sam	me security levels		
Wizards - 4						Apply	Re	set		
						ŀ	admin> NA	(15)	🔒 3/1 6/03	5 4:26:48 PM UTC

7. <u>インターフェイス編集のプロンプトで、[OK] をクリックします。</u>



8. インターフェイスの詳細を入力し、完了したら [OK] をクリックします。

🔂 Edit Interface		x
Hardware Port:	Ethernet0	Configure Hardware Properties
🔽 Enable Interface	Dedicate this interface to mana	gement only
	F	
Interface Name:	outside	
Security Level:	0	
- IP Address		
 Use Static IP 	O Obtain Address via DHCP	
IP Address:	99.99.99.1	
Subnet Mask:	255.255.255.0	
MTU:	1500	
Description:		
	OK Cancel	Help
 インターフェイス変更の	プロンプトで、[OK] をクリック	します。



10. [Apply] をクリックして、インターフェイス設定を承認します。 設定内容は PIX にもプッ シュされます。 この例ではスタティック ルートを使用します。

Eisco ASDM 5. File Rules Be	.0 foi iarch	PTX - 10.1 Options	 Tools Wizards	Help								_ 🗆 X
G Home	Conf	of the second se	Monitoring	O Back F	C) prward	Q Search	Q Refresh	Save	? Help			Casco Systems
Features	Co	nfiguration	> Features > Interfa → 2 L ↔ 1 B → 3b	ices m o 2	5 L-Q L							
Interfaces		. X ¥ I			51001							
<u>è</u> ,			Interface	Name	Enabled	Security Level	IP Address	Sub	onet Mask	Management Only	MTU	Add
Security Policy		Ethernet1		inside	Yes	100	10.1.1.1	255.2	55.255.0	No	1500	Edit
AL NOT		Ethernet0		outside	Yes	0	99.99.99.1	265.2	55.255.0	No	1500	Deleta
A Routing												
Building Blocks												
Device Administration												
5.		•									•	
Properties		Enable	traffic between two	or more inf	erfaces wi	hich are co	onfigured with sa	ame sec	urity levels			
Wizards /						Apply	R	eset				
						-	admin> N	A (15)			3/16/05	4:28:18 PM UTC

11. [Features] タブの下で [Routing] をクリックし、[Static Route] を強調表示し、[Add] をクリ ックします。

🔨 Cisco ASDM 5.0) for PIX - 10.1.1.1		_ D X
File Rules Bea	arch Options Tools Wizari	is Help	
Home C	onfiguration Monitoring	O O O O O O O O O O O O O O O O O O O	CISCO SYSTEMS
Features	Configuration > Features > R	outing > Routing > Static Route	
Hterfaces Security Policy NAT		Static Route Specify static routes. Interface IP Address Netmask Gateway IP Metric Tunneled	Add
VPN	4截MRouts		Delete
Properties Wizards /		Asply Reset	
	,	admin> 🛛 🗛 (15) 🛛 🚔 👧 👘 👔	16/05 4:44:48 PM UTC

12. <u>デフォルト ゲートウェイを設定し、[OK] をクリックします。</u>

🔂 Add Static Route	×
Interface Name:	outside
IP Address:	0.0.0.0
Mask:	0.0.0.0
Gateway IP:	99.99.99.2
Metric	1
C Tunneled (Used of	nly for default route)
ок	Cancel Help

13. [Add] をクリックして、inside ネットワークにルートを追加します。

	📬 Add St	atic Route	×	
	Int	erface Name:	inside	
	IP	Address:	10.2.2.0	
	Ma	ask:	255.255.255.0	
	Ga	ateway IP:	10.1.1.2	
	۰ ۱	Aetric .	1	
	ΓO	funneled (Used	only for default route)	
	(ок	Cancel Help	
14.	LLLL 正しいルー	· トが設定されて ^い	ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー	
	File Rules Bea) for PTX - 10.1.1.1 arch: Options Tools Wizar	ds Help	
	Home C	antiquiration Maximiza	Basis Enroyand Search Seve Halo	Cisco S
	Features	Configuration = Features = F	Routing > Routing > Static Route	
		● £ ● I ■ I Ⅲ I A ■ ARouting	사 Kill Koute	
	internaces		Specify static routes.	
	Security Policy	⊕ Multicast	Interface IP Address Netmask Gateway IP Metric Tunneled	Add
	NAT	E B IGMP	inside 10.2.2.0 255.255.2 10.1.1.2 1 N/A	Edit
	VPN VPN	%截MRoute		Delete
	423			
	Rectang			
	Building Blocks			
	Device Administration			
	Properties			
			Apply Reset	
	Wizards 🗠			

_OX

ISCO SYSTEMS

🛃 🔜 🕴 📋 3/16/05 4:46:48 PM UTC

15. この例では、NAT を使用します。 [Enable traffic through the firewall without address

NA (15)

<admin>

translation	<u>」 </u>	/ 人をオノ	にし、[Add] を	クリックして「	NAT IL-	ルを設定します	0
🔨 Cisco ASDM :	5.0 for PIX - 10	.1.1.1					
File Rules S	earch Option	is Tools Wizar	ds Help				
ổ Ноте	orgeneration	Monitoring	Back Forward	Q Q Search Refresh	Save Help		Casco Systems
Features	Configuration	on > Features > N	AT = Translation Rules				
_		111118	科 🗈 🔒 🏹 🕼 🕯				
Interfaces	🗆 Enat)le traffic through	the firewall without addres	ss translation			
<u>6</u> .	🖲 Tran	slation Rules	C Translation Exer	nption Rules			
Security Policy	Show F	luies for interface	All Interfaces	Show All			
24			- par interiaces				
NAT	Rule		Original			Translated	Add
<u>8</u>	Type	Interface	Source Network	Destination Network	Interface	Address	Edit
VPN							Delete
425 Routing							
8							
Building Blocks							
Device Administration							
5							
Properties							
						<u>.</u>	
	in Sta	00 1441	Dynamic NAT 42 8	aac Holicy NAT 430 C	Amarnic Policy N	Manage Pools]
				Apply	Reset		
Wizards <							
				<admin> N/</admin>	A (15)	🍰 🔂 📔 🗎 👌 3/1 6/05 4	4:31:48 PM UTC

L · · ·

16. 送信元ネットワーク(この例のみで使用)を設定します。 次に、PAT を定義するため、 [Manage Pools] をクリックします。

🕵 Add Address T	ranslation R	ule						x
O Use NAT	. OU	se Policy NAT						
- Source Ho	st/Network-							
		Interface:	inside		•			
		IP Address:	0.0.0.0		_			
		Mask:	0.0.0.0		-			
			10.0.0					
			Browse					
							NAT Options	
Translate Ade	dress on Inte	rface: outsid	le 💌			_		_
-Translate A	Address To —							
0.1	Static	IP Address:		-	1			
	🗖 Redirect p	ort	'		1			
	C UDP	Original port:	Т	ranslated p	ort:			
• ¶	Dynamic	Address Pool:	same addres	s 💌	Managel	Pools		
	Pool ID		Addr	ess				
	N/A	No address poo	ol defined					
	1							
	Г	014			Liela	1		
	_	UK	Cancel		нер			

17. outside インターフェイスを選択し、[Add] をクリックします。

🕵 Manage	Global Add	ress Pools								×
Global	Address Po	ols								
Clabal	Address Do		to configu		ic blobs	ork Addr	Trong	lation /		
addres	ses.	ois are used	to conligu	re Dynam	IC NEW	ork Addr	ess mans	nation (i	NAT)	
Int	orfaco	Pool ID		ID A	ddraee	(00)		Т		
inside	enace	FUULD		IF A	uuress	(85)			Add	1
outsid	e							-	Auu]
									Edit	
									Delete	1
								-		1
		OK	. 1	Con		1	Holp	1		
		06	·	Can	Cel		нер			
この例では	は、インタ	ーフェイス	スの IP フ	^ドレス	を使用	する P	AT を使	用しま	き。	
🔂 Add G	lobal Pool	Item								x
Interf	ace:	outside		•	Po	ol ID:	1			
							·			
0	Range									
0	Port Addre	ss Transla	ition (PA	T)						
۲	Port Addre	ss Transla	ition (PA	T) using	the IP	addres	s of the i	interfa	ce	
			Ì	·						_
	IP Addre	ess:				— Г				
		1				L				
	Network	Mask (ont	ionally							
	14667011	emaione (ope	iorrony.	1						
		ок		Can	cel		Help			

18. <u>PAT が設定されたら、</u>	[OK] をクリックします。
-------------------------	----------------

Interface	Pool ID	IP Ad	dress(es)	
side tside	1 9	9 99 99 1 (interface 8	PATI	A
10100		5.55.55.1 (Interface)	,	
				E
				De
				De

19. スタティック変換を設定するため、[Add] をクリックします。

🔁 Add Address 1	ranslation R	ule				x
Use NAT	. CU	se Policy NAT				
Source Ho	st/Network—					1
		Interface:	inside	•		
		IP Address:	0.0.0.0			
		Mask	0.0.0.0	T		
			·			
			Browse			
					NAT Options	
Translate Ad	dress on Inte	face: outsic	ie 💌			
Translate /	Address To —					
0.11	Static	IP Address:		-		
	🗖 Redirect p	ort			_	
	C UDP	Original port:	Translate	ed port		
e 📲	Dynamic	Address Pool:	same address 💌	Manage Pools	s	
	Pool ID		Address			
	1	99.99.99.1 (inter	face PAT)		-	
	1					
		OK	Cancel	Help		
	_	UK		Tiolp		

20. [Interface] ドロップダウンで [inside] を選択した後、IP アドレス 10.1.1.2 とサブネット マ スク 255.255.255.255 を入力してから、[Static] を選択し、[IP Address] フィールドに外部 アドレス 99.99.99.12 を入力します。 完了したら、[OK] をクリックします。

📬 Add Address Transla	tion Rule			x
• Use NAT	C Use Policy NAT			
- Source Host/Netw	ork			
	Interface: IP Address:	inside 10.1.1.2	<u> </u>	
	Mask:	255.255.255.255	¥	
		Browse		
				NAT Options
Translate Address o	n Interface: outsi	de 💌		
Translate Address	з То			
⊙ י י Static	IP Address:	99.99.99.12	~	
E Red	lirect port			_
e C	TCP Original port: UDP	Translated	d port:	
C 🚻 Dynam	nic Address Pool:	same address 💌	Manage Pool	s
Poo	ID	Address		
	ОК	Cancel	Help	

21. [Apply] をクリックして、インターフェイスの設定を承認します。 設定内容は PIX にもプ ッシュされます。



22. [Features] タブの [Security Policy] を選択して、セキュリティ ポリシー ルールを設定します。



23. [Add] をクリックして esp トラフィックを許可し、[OK] をクリックして続行します。

Add Access Rule	
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range Time Range: Not Applied New
Source Host/Network	Destination Host/Network
	C IP Address C Name C Group
Interface: outside	Interface: inside
IP address: 99.99.99.2	IP address: 99.99.99.12
Mask: 255.255.255.265 💌	Mask: 255.255.255.255
99.99.99.2	99.99.99.12
Protocol and Service	
C TCP C UDP C ICMP C IP	Manage Service Groups
Please enter the description below (optional):	
Access Rule to Allow ESP traffic	*
ОК Са	ancel Help

24. ISAKMP トラフィックを許可するため、[Add] をクリックした後、[OK] をクリックして続 行します。

🖆 Edit Access Rule	×
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range Time Range: Not Applied New
Source Host/Network	Destination Host/Network
Interface: outside	Interface: Inside 💌
IP address: 99.99.99.2	IP address: 99.99.99.12
Mask: 255.255.255.265 💌	Mask: 255.255.255.255 💌
99.99.99.2 outside	99.99.99.12
Protocol and Service	
CITCP © UDP CICMP CIP	Manage Service Groups
Service =isakmp	Service = _ any
C Service Group	C Service Group
Please enter the description below (optional):	
Access Rule to allow ISAKMP to host 99.99.99.12	
OK Car	ncel Help

25. [Add] をクリックして NAT-T のための UDP ポート 4500 トラフィックを許可し、[OK] を クリックして続行します。

🚰 Edit Access Rule	×
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range Time Range: Not Applied New
Source Host/Network	Destination Host/Network
	IP Address C Name C Group
Interface: outside	Interface: inside 💌
IP address: 99.99.99.2	IP address: 99.99.99.12
Mask: 255.255.255	Mask: 255.255.255.255
99.99.99.2	affic
Protocol and Service	
C TCP © UDP C ICMP C IP Source Port © Service = • 4500 © Service Group	Manage Service Groups Destination Port Service = any Service Group
Please enter the description below (optional):	
Access Rule to allow 4500 to host 99.99.99.12	A 7
OK Can	Help

26. [Apply] をクリックして、インターフェイス設定を承認します。 設定内容は PIX にもプッ シュされます。

File Rules Search Options Tools Wizards Help									
Home C	anfigura	tion Mo	itioring	Back Forward	Q Q Search Refresh	Save He	(Ces 1	CO SYSTEMS
Features	Configu	ration > Fe	atures >	Security Policy > Access F	Rules				
			iles						
	Show	Rules for I	interíace	: All Interfaces 🔄	Show All				
Security Policy	ŧ	Rule Enabled	Action	Source HostNetwork	Destination Host/Network	Rule Applied To Traffic	Interface	Service	Add
NAT		V	¥	🍅 any	🧼 any		inside (outbound)	💌 ip	Edit
100	1	¥	*	8 99.99.99.2	a 99.99.99.12	🔊 incoming	outside	ı™ esp	Delete
VPN	2		1	89.99.99.2	A 99.99.99.12	🚰 incoming	outside	Brc: isakmp	
Routing Building Blocks Device Administration Froperties	*								
	×	Allow traffi	c	O Deny traffic		⊛ st	iow Summary	C. Show Detail	
Wizards - A				Apply	Reset	Adva	nced		
					<admin></admin>	NA (15)	😹 🔂 🔢	🔁 3/1 6/05 4:54	4:58 PM UTC

27. 設定はこれで完了しました。[File] > [Show Running Configuration in New Windows] の順に 選択し、CLI 設定を確認します。



PIX ファイアウォール

```
pixfirewall# show run
: Saved
PIX Version 7.0(0)102
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 99.99.99.1 255.255.255.0
1
interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
1
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
ftp mode passive
access-list outside_access_in remark Access Rule to
Allow ESP traffic
access-list outside_access_in
            extended permit esp host 99.99.99.2 host
99.99.99.12
access-list outside_access_in
            remark Access Rule to allow ISAKMP to host
99.99.99.12
access-list outside_access_in
            extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12
access-list outside_access_in
            remark Access Rule to allow port 4500 (NAT-
T) to host 99.99.99.12
access-list outside_access_in
                    extended permit udp host 99.99.99.2
eq 4500 host 99.99.99.12
pager lines 24
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 0.0.0.0 0.0.0.0
static (inside, outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255
access-group outside_access_in in interface outside
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 99.99.99.2 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
mqcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.3 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
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
1
service-policy asa_global_fw_policy global
Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e
: end
```

<u>PIX セキュリティ アプライアンスおよび MPF(モジュラ ポリシー フレームワーク</u> <u>)の設定</u>

アクセス リストの代わりに、MPF(モジュラ ポリシー フレームワーク)でコマンド inspect ipsec-pass-thru を使用し、PIX/ASA セキュリティ アプライアンス経由で IPsec トラフィックを 渡します。

この検査は ESP トラフィックのピンホールを開くように設定されています。転送フローが存在 していて、かつ許容できる最大接続数に制限がない場合、ESP データ フローのすべてが許可され ます。AH は許可されません。ESP データ フローのデフォルト アイドル タイムアウトは、デフ ォルトで 10 分に設定されています。この検査は、クラスおよび一致コマンド モードを含め、他 の検査を適用できるすべての場所に適用可能です。IPSec パススルー アプリケーション インス ペクションは、IKE UDP ポート 500 接続に関連付けられた ESP (IP プロトコル 50) トラフィッ クを簡単に横断できます。このインスペクションは、冗長なアクセス リスト コンフィギュレー ションを回避して ESP トラフィックを許可し、タイムアウトと最大接続数によりセキュリティも 確保します。 class-map、policy-map、および service-policy の各コマンドを使用してトラフィッ クのクラスを定義し、inspect コマンドをクラスに適用して、ポリシーを1 つまたは複数のインタ ーフェイスに適用します。有効にした場合、inspect IPSec-pass-thru コマンドでは、タイムアウ ト 10 分の無制限 ESP トラフィックが可能になります。これは設定不可能です。 NAT および非 NAT トラフィックは許可されます。

```
hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class
hostname(config)#policy-map test-udp-policy
hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru
hostname(config)#service-policy test-udp-policy interface outside
```

<u>確認</u>

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示してい ます。

特定の show コマンドは、<u>Output Interpreter Tool</u>(<u>登録</u>ユーザ専用)によってサポートされてい ます。このツールを使用すると、show コマンド出力の分析を表示できます。

- 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。
- show crypto engine connections active 暗号化パケットおよび復号化パケットを表示します。

<u>トラブルシューティング</u>

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

ルータ IPsec のトラブルシューティング コマンド

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 engine:暗号化されたトラフィックを表示します。
- 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 Internet Security Association and Key Management Protocol (ISAKMP) ネゴシエーションを表示します。

<u>セキュリティ アソシエーションのクリア</u>

- clear crypto isakmp インターネット キー交換(IKE)のセキュリティ アソシエーションをクリアします。
- clear crypto ipsec sa IPSec のセキュリティ アソシエーションをクリアします。

<u>PIX のトラブルシューティング コマンド</u>

特定の show コマンドは、<u>Output Interpreter Tool</u>(<u>登録</u>ユーザ専用)によってサポートされてい ます。このツールを使用すると、show コマンド出力の分析を表示できます。

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。

• 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。 この情報は PIX ログ バッファに保存されており、出力は show log コマンドを 使用して表示できます。

- ASDM を使用してロギングを有効にし、以下の手順で示されているようにログを表示できます。
- 1. [Configuration] > [Properties] > [Logging] > [Logging Setup] > [Enable Logging] を選択した後 、[Apply] をクリックします。

🔨 Cisco ASDM 5.1	0 for PIX - 10.1.1.1	
File Rules Se	arch Options Tools Wizards H	elp
<u> </u>		
Home	Configuration Monitoring Bi	ck Forward Search Refresh Save Holp
Features	Configuration > Features > Propert	ies > Logging > Logging Setup
	4 4 3 2 1 1 1 1 K 1 K	
	1 2 Seauch Promot	
Interfaces	E-BActvanced	igging Setup
a	- BAnti-Speefing	Enable logging on the failurer standby unit
1 3	- 😻 Fragment	Sand debus messenes as systems Sand sustains in EVBLEN format
Security Policy	TCP Options	Toend devog meesages as systege in the existinge in the transmission
24	- O Timeouts	Logging to Internal Buffer
NAT	- Auto Lindate	Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will
100	DHCP Services	be overwritten.
<u>88</u>	- PDHCP Server	Buffer Size: 4096 bytes
VHN	- POHCP Relay	
A	- BDNS Client	You can choose to save the buffer contents before the buffer is overwritten.
Routing	Failover	Save Buffer To: FTP Server Configure FTP Settings
<u>e</u> s	P- IP Audit	
Diddex Diseas	- 18 IP Audit Policy	Flash Configure Flash Usage
A A A A A A A A A A A A A A A A A A A	- In Audit Signatur	
<u></u>	🕀 🔚 Logging	ASDM Logging
Administration	Logging Setup	Specify the size of the queue for syslogs intended for viewing in ASDM.
B		Owene Size: 100
Properties	Syslog Setup	
	- EgSyslog Servers	
	- 🦓 E-Mail Setup	
	Priority Queue	
	RUNPPC Server	Apply Reset
Wizards 🗠		
		«admin» 🛛 NA (15) 👘 🛃 🔤 🔂 3/16/05 5:03:38 PM UTC

2. [Monitoring] > [Logging] > [Log Buffer] > [On Logging Level] > [Logging Buffer] を選択してか ら、[View] をクリックします。



ログ バッファの例を次に示します。

	🔂 Log Buf	fer	
	This scre	en shows syslog mess	ages in ASDM logging buffer as of now.
	Find text	in messages below:	Find Next
	Severity	Time	<u>.</u>
l	<u> </u>	Mar 16 2005 17:06:11	605005: Login permitted from 10.1.1.3/1247 to inside:10.1.1.1/https for user "enable
I	<u>i</u> 6	Mar 16 2005 17:05:47	609001: Built local-host inside:10.1.1.2
l	▲ 6	Mar 16 2005 17:05:47	609001: Built local-host outside:99.99.99.2
l	🔺 6	Mar 16 2005 17:05:47	605005: Login permitted from 10.1.1.3/1220 to inside:10.1.1.1/https for user "enable
l	▲ 6	Mar 16 2005 17:05:47	302013: Built inbound TCP connection 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t
l	<u>∔</u> 6	Mar 16 2005 17:05:47	302014: Teardown TCP connection 47 for inside:10.1.1.3/1219 to NP Identity Ifc:10.
l	<u> </u>	Mar 16 2005 17:05:47	605005: Login permitted from 10.1.1.3/1221 to inside:10.1.1.1/https for user "enabl
l	▲ 6	Mar 16 2005 17:05:47	302013: Built inbound TCP connection 50 for inside:10.1.1.3/1221 (10.1.1.3/1221) t
l	<u>1</u> 6	Mar 16 2005 17:05:47	302014: Teardown TCP connection 48 for inside:10.1.1.3/1220 to NP Identity Ifc:10.
l	<u>A</u> 4	Mar 16 2005 17:05:47	106023: Deny udp src outside:99.99.99.2/4500 dst inside:99.99.99.12/4500 by acce
l	<u>∔</u> 6	Mar 16 2005 17:05:47	302015: Built inbound UDP connection 49 for outside:99.99.99.2/500 (99.99.99.2/5)
l	<u> </u>	Mar 16 2005 17:05:47	609001: Built local-host inside:10.1.1.2
l	<u>∔</u> 6	Mar 16 2005 17:05:47	609001: Built local-host outside:99.99.99.2
l	<u> </u>	Mar 16 2005 17:05:47	605005: Login permitted from 10.1.1.3/1220 to inside:10.1.1.1/https for user "enable
l	▲ 6	Mar 16 2005 17:05:47	302013: Built inbound TCP connection 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t
I	<u>∔</u> 6	Mar 16 2005 17:05:47	302014: Teardown TCP connection 47 for inside:10.1.1.3/1219 to NP Identity Ifc:10.
I	▲ 6	Mar 16 2005 17:05:46	605005: Login permitted from 10.1.1.3/1219 to inside:10.1.1.1/https for user "enable
	▲ 6	Mar 16 2005 17:05:46	302013: Built inbound TCP connection 47 for inside:10.1.1.3/1219 (10.1.1.3/1219) t
	<u>i</u> 6	Mar 16 2005 17:05:46	302014: Teardown TCP connection 46 for inside:10.1.1.3/1218 to NP Identity Ifc:10.
1	1.6	Mar 16 2005 17:05:46	605005: Login permitted from 10.1.1.3/1218 to inside:10.1.1.1/https for user "enable

Mar 16 2005 17:05:46 302013: Built inbound TCP connection 46 for inside:10.1.1.3/1218 (10.1.1.3/1218) t

Mar 16 2005 17:05:46 302014: Teardown TCP connection 45 for inside:10.1.1.3/1217 to NP Identity Ifc:10.

Mar 16 2005 17:05:46 605005: Login permitted from 10.1.1.3/1217 to inside:10.1.1.1/https for user "enable

Mar 16 2005 17:05:46 302013: Built inbound TCP connection 45 for inside:10.1.1.3/1217 (10.1.1.3/1217) t

Mar 16 2005 17:05:46 302014: Teardown TCP connection 44 for inside:10.1.1.3/1216 to NP Identity Ifc:10.

Clear

Mar 16 2005 17:05:46 605005: Login permitted from 10.1.1.3/1219 to inside:10.1.1.1/https for user "enable"

Close

F.

Help

<u>関連情報</u>

<u>i</u> 6

46 46

<u>i</u> 6

16

6 🔥

• 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

Save Log As...

• <u>PIX に関するサポート ページ</u>

Refresh

- <u>PIX コマンド リファレンス</u>
- <u>NAT に関するサポートページ</u>
- Requests for Comments (RFC)
- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>