L2L IPsec トンネルで接続されたリモート ネットワーク上のインバウンド ホスト変換のための PIX ファイアウォールの設定例

目次

概要

このドキュメントでは、2 つの Cisco Secure PIX Firewall 間にある LAN-to-LAN IPSec トンネルを通過するホストの発信元 IP の変換に使用される手順について説明します。 各 PIX Firewall には、その背後に保護されたプライベート ネットワークがあります。 この概念は、個々のホストの代わりにサブネットを変換する場合にも適用されます。

注: PIX/ASA 7.x の同じシナリオを設定するためにこれらのステップを使用して下さい:

- PIX/ASA 7.x のためのサイト間VPN トンネルを設定するために、PIX/ASA 7.x を参照して下さい: 簡単なPIX-to-PIX VPNトンネル 設定例。
- 受信コミュニケーションに使用する **static コマンドは**これに記述されているように 6.x および 7.x 両方のために類似した 資料です。
- この資料で使用される**提示**、**クリア**および **debug コマンドは** PIX 6.x および 7.x で類似したです。

前提条件

要件

この設定例を続行する前にインターフェイスの IP アドレスで PIXファイアウォールを設定したし、基本的な接続をように持って下さい。

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くものです。

- Cisco PIX 506E ファイアウォール
- Cisco Secure PIX Firewall ソフトウェア バージョン 6.3(3)

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

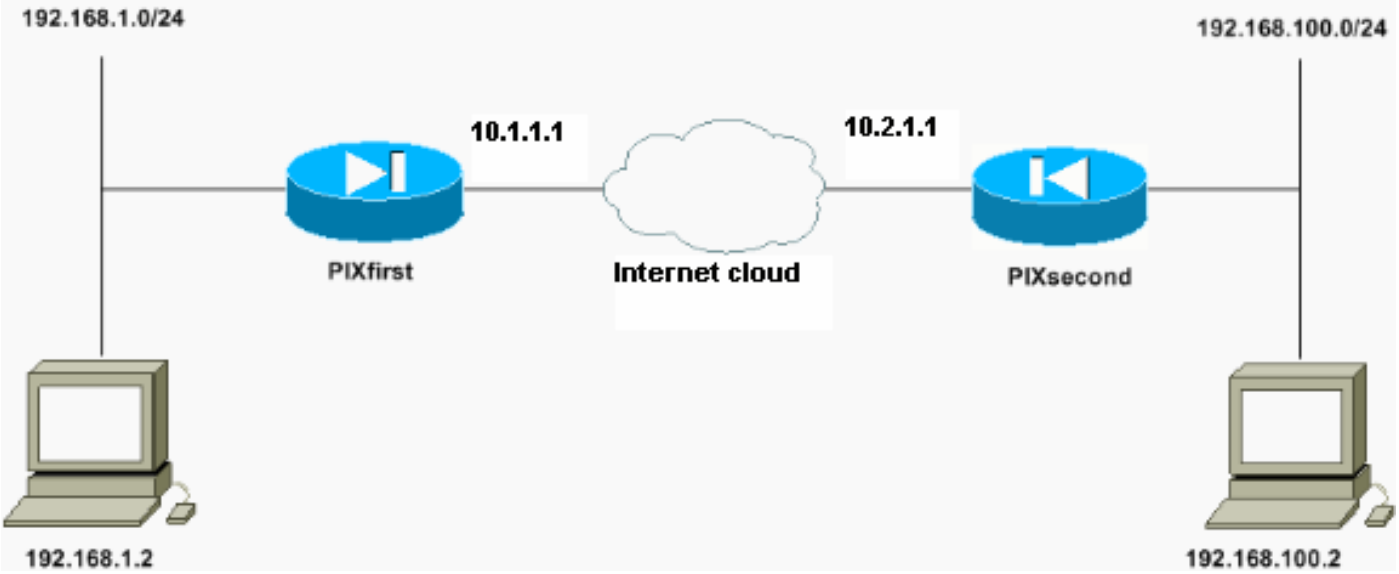
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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）を使用してください。

ネットワーク図

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。



192.168.100.2 の IP アドレスのホストは PIXfirst のホスト名と PIXファイアウォールの 192.168.50.2 に変換されます。 この変換はホストおよび宛先に対して透過的です。

注: そのアプリケーションのためのフィックスアップが有効に ならなければどの組み込み IP アドレスでもデフォルトで変換されません。 組み込みIPアドレスはアプリケーションは IPパケットの

データペイロード部分の内で含まれている 1 です。 ネットワーク アドレス変換（NAT）は IPパケットの外 IP ヘッダーだけ修正します。 それは IP がある特定のアプリケーションによって組み込むことができるオリジナルパケットのデータペイロードを修正しません。 これにより時々それらのアプリケーションは適切に機能します。

設定

このドキュメントでは、次の設定を使用します。

- PIXfirst 設定
- PIXsecond 設定

PIXfirst 設定

```
PIXfirst(config)#write terminal Building
configuration... : Saved : PIX Version 6.3(3) interface
ethernet0 auto interface ethernet1 auto nameif ethernet0
outside security0 nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted passwd
2KFQnbNIdI.2KYOU encrypted hostname PIXfirst fixup
protocol dns maximum-length 512 fixup protocol ftp 21
fixup protocol h323 h225 1720 fixup protocol h323 ras
1718-1719 fixup protocol http 80 fixup protocol rsh 514
fixup protocol rtsp 554 fixup protocol sip 5060 fixup
protocol sip udp 5060 fixup protocol skinny 2000 fixup
protocol smtp 25 fixup protocol sqlnet 1521 fixup
protocol tftp 69 names !--- Define encryption domain
(interesting traffic) !--- for the IPsec tunnel. access-
list 110 permit ip host 192.168.1.2 host 192.168.100.2
!--- Accept the private network traffic from the NAT
process. access-list 120 permit ip host 192.168.1.2 host
192.168.50.2 pager lines 24 mtu outside 1500 mtu inside
1500 ip address outside 10.1.1.1 255.255.255.0 ip
address inside 192.168.1.1 255.255.255.0 ip audit info
action alarm ip audit attack action alarm pdm history
enable arp timeout 14400 !--- Bypass translation for
traffic that goes over the IPsec tunnel. nat (inside) 0
access-list 120 !--- Inbound translation for the host
located on the remote network. static (outside,inside)
192.168.50.2 192.168.100.2 netmask 255.255.255.255 0 0
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
mgcp 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 LOCAL
protocol local no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable !--- Accept traffic that
comes over the IPsec tunnel from !--- Adaptive Security
Algorithm (ASA) rules and !--- access control lists
(ACLs) configured on the outside interface. sysopt
connection permit-ipsec !--- Create the Phase 2 policy
for actual data encryption. crypto ipsec transform-set
chevelle esp-des esp-md5-hmac crypto map transam 1
ipsec-isakmp crypto map transam 1 match address 110
crypto map transam 1 set peer 10.2.1.1 crypto map
transam 1 set transform-set chevelle crypto map transam
interface outside isakmp enable outside !--- Pre-shared
key for the IPsec peer. isakmp key ******** address
10.2.1.1 netmask 255.255.255.255 !--- Create the Phase 1
```

```
policy. isakmp identity address isakmp policy 1
authentication pre-share isakmp policy 1 encryption des
isakmp policy 1 hash md5 isakmp policy 1 group 1 isakmp
policy 1 lifetime 1000 telnet timeout 5 ssh timeout 5
console timeout 0 terminal width 80
Cryptochecksum:778f934d42c037a978b8b5236a93b5f4 : end
[OK] PIXfirst(config)#
```

PIXsecond 設定

```
PIXsecond(config)#write terminal Building
configuration... : Saved : PIX Version 6.3(3) interface
ethernet0 auto interface ethernet1 auto nameif ethernet0
outside security0 nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted passwd
2KFQnbNIdI.2KYOU encrypted hostname PIXsecond fixup
protocol dns maximum-length 512 fixup protocol ftp 21
fixup protocol h323 h225 1720 fixup protocol h323 ras
1718-1719 fixup protocol http 80 fixup protocol rsh 514
fixup protocol rtsp 554 fixup protocol sip 5060 fixup
protocol sip udp 5060 fixup protocol skinny 2000 fixup
protocol smtp 25 fixup protocol sqlnet 1521 fixup
protocol tftp 69 names !--- Accept the private network
traffic from the NAT process. access-list nonat permit
ip host 192.168.100.2 host 192.168.1.2 !--- Define
encryption domain (interesting traffic) for the IPsec
tunnel. access-list 110 permit ip host 192.168.100.2
host 192.168.1.2 pager lines 24 mtu outside 1500 mtu
inside 1500 ip address outside 10.2.1.1 255.255.255.0 ip
address inside 192.168.100.1 255.255.255.0 ip audit info
action alarm ip audit attack action alarm pdm history
enable arp timeout 14400 !--- Bypass translation for
traffic that goes over the IPsec tunnel. nat (inside) 0
access-list nonat route outside 0.0.0.0 0.0.0.0 10.2.1.2
1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00 timeout
h323 0:05:00 mgcp 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 LOCAL protocol local no snmp-server location no
snmp-server contact snmp-server community public no
snmp-server enable traps floodguard enable !--- Accept
traffic that comes over the IPsec tunnel from ASA rules
and !--- ACLs configured on the outside interface.
sysopt connection permit-ipsec !--- Create the Phase 2
policy for actual data encryption. crypto ipsec
transform-set chevelle esp-des esp-md5-hmac crypto map
transam 1 ipsec-isakmp crypto map transam 1 match
address 110 crypto map transam 1 set peer 10.1.1.1
crypto map transam 1 set transform-set chevelle crypto
map transam interface outside isakmp enable outside !---
Pre-shared key for the IPsec peer. isakmp key ********
address 10.1.1.1 netmask 255.255.255.255 !--- Create the
Phase 1 policy. isakmp identity address isakmp policy 1
authentication pre-share isakmp policy 1 encryption des
isakmp policy 1 hash md5 isakmp policy 1 group 1 isakmp
policy 1 lifetime 1000 telnet timeout 5 ssh timeout 5
console timeout 0 terminal width 80
Cryptochecksum:a686f71a023d1cd7078728a38acf529e : end
[OK] PIXsecond(config)#
```

所定のインターフェイスのための複数の暗号マップエントリを作成する場合、それをランク付けするのに各エントリのシーケンス番号を使用する必要があります。 下部のはシーケンス番号、より高いです優先順位は。 設定 される クリプト マップがあるインターフェイスでセキュリティ ア

プライアンス モデルは高優先順位マップのエントリに対してトラフィックを最初に評価します。

異なるトラフィック の 種類に別の IPsec セキュリティを適用したいと思う場合所定のインターフェイスのための複数の暗号マップエントリを別の同位ハンドル異なるデータフローまたは作成して下さい（同じにまたは同位を分けるため）。 サブネットの別のセット間のたとえば 1 組のサブネット間のトラフィックに認証されてほしければおよびトラフィック認証され、暗号化されるため。 この場合、2 つの別々のアクセス リストの異なるトラフィック の 種類を定義し、各々の暗号 アクセス リストのための別途の暗号マップエントリを作成して下さい。

セキュリティ アソシエーション（SA）の消去

PIX の特権 モードでは、これらのコマンドを使用して下さい:

- **clear [crypto] ipsec sa**：アクティブな IPSec SA を削除します。 crypto キーワードはオプションです。
- **clear [crypto] ipsec sa**：アクティブな IKE SA を削除します。 crypto キーワードはオプションです。

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show crypto isakmp sa** —フェーズ 1 Security Association （SA）を示します。
- **show crypto ipsec sa** —フェーズに 2 SA を示します。
- **ping** - 基本ネットワークの接続を診断します。 1 PIX からの他への PING は 2 つの PIX 間の接続を確認します。 PING はまた PIXfirst の後ろでホストからホストへの PIXsecond の後ろで IPSecトンネルを呼び出すために実行することができます。
- **show local-host <IP_address>** —規定 される IP アドレスがあったローカル ホストのための変換および接続スロットを表示する。
- **show xlate は detail** — 変換 スロットのコンテンツを表示する。 これがホストが変換されることを確認するのに使用されています。

PIXfirst を確認して下さい

これは **ping コマンド**の出力です。

```
PIXfirst(config)#ping 10.2.1.1 !--- PIX pings the outside interface of the peer. !--- This
implies that connectivity between peers is available. 10.2.1.1 response received -- 0ms 10.2.1.1
response received -- 0ms 10.2.1.1 response received -- 0ms PIXfirst(config)#
```

これは **show crypto isakmp sa コマンド**の出力です。

```
PIXfirst(config)#show crypto isakmp sa Total : 1 Embryonic : 0 !--- Phase 1 SA is authenticated
and established. dst src state pending created 10.1.1.1 10.2.1.1 QM_IDLE 0 1
```

以下は、**show crypto ipsec sa** コマンドの出力です。

```
!--- Shows Phase 2 SAs. PIXfirst(config)#show crypto ipsec sa interface: outside Crypto map tag:
```

transam, local addr. 10.1.1.1 *!--- Shows addresses of hosts that !--- communicate over this tunnel.* **local ident (addr/mask/prot/port): (192.168.1.2/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (192.168.100.2/255.255.255.255/0/0)** current_peer: 10.2.1.1:500 PERMIT, flags={origin_is_acl,} *!--- Shows if traffic passes over the tunnel or not. !--- Encapsulated packets translate to packets that are sent. !--- Decapsulated packets translate to packets that are received.* **#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21 #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 21** #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.1.1 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 6ef53756 *!--- If an inbound Encapsulating Security Payload (ESP) !--- SA and outbound ESP SA exists with a !--- security parameter index (SPI) !--- number, it implies that the Phase 2 SAs !--- are established successfully.* **inbound esp sas: spi: 0x1cf45b9f(485776287) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2, crypto map: transam sa timing: remaining key lifetime (k/sec): (4607998/28756) IV size: 8 bytes replay detection support: Y** inbound ah sas: inbound pcp sas: **outbound esp sas: spi: 0x6ef53756(1861564246) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 1, crypto map: transam sa timing: remaining key lifetime (k/sec): (4607998/28756) IV size: 8 bytes replay detection support: Y** outbound ah sas: outbound pcp sas:

これは show local-host コマンドの出力です。

!--- Shows translation for the host on a remote network. PIXfirst(config)#**show local-host 192.168.100.2** Interface outside: 1 active, 1 maximum active, 0 denied local host: <192.168.100.2>, TCP connection count/limit = 0/unlimited TCP embryonic count = 0 TCP intercept watermark = unlimited UDP connection count/limit = 0/unlimited AAA: Xlate(s): **Global 192.168.50.2 Local 192.168.100.2** Conn(s):

これは show xlate detail コマンドの出力です。

!--- Shows translation for the host on a remote network. PIXfirst(config)#**show xlate detail** 1 in use, 1 most used Flags: D - DNS, d - dump, I - identity, i - inside, n - no random, o - outside, r - portmap, s - static **NAT from outside:192.168.100.2 to inside:192.168.50.2 flags s** PIXfirst(config)#

PIXsecond を確認して下さい

これは ping コマンドの出力です。

PIXsecond(config)#**ping 10.1.1.1** *!--- PIX can ping the outside interface of the peer. !--- This implies that connectivity between peers is available.* **10.1.1.1 response received -- 0ms 10.1.1.1 response received -- 0ms 10.1.1.1 response received -- 0ms** PIXsecond(config)#

これは show crypto isakmp sa コマンドの出力です。

PIXsecond(config)#**show crypto isakmp sa** Total : 1 Embryonic : 0 *!--- Phase 1 SA is authenticated and established.* dst src state pending created **10.1.1.1 10.2.1.1 QM_IDLE 0 1**

以下は、show crypto ipsec sa コマンドの出力です。

!--- Shows Phase 2 SAs. PIXsecond(config)#**show crypto ipsec sa** interface: outside Crypto map tag: transam, local addr. 10.2.1.1 *!--- Shows addresses of hosts that communicate !--- over this tunnel.* **local ident (addr/mask/prot/port): (192.168.100.2/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (192.168.1.2/255.255.255.255/0/0)** current_peer: 10.1.1.1:500 PERMIT, flags={origin_is_acl,} *!--- Shows if traffic passes over the tunnel or not. !--- Encapsulated packets translate to packets that are sent. !--- Decapsulated packets translate to packets that are received.* **#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21 #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 21** #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 10.2.1.1, remote crypto endpt.: 10.1.1.1 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 1cf45b9f *!--- If an inbound ESP SA and outbound ESP SA exists with an SPI !--- number, it implies that the Phase 2 SAs are established successfully.* **inbound esp sas: spi: 0x6ef53756(1861564246) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:**

```
0, conn id: 2, crypto map: transam sa timing: remaining key lifetime (k/sec): (4607990/28646) IV
size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas:
spi: 0x1cf45b9f(485776287) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 1, crypto map: transam sa timing: remaining key lifetime (k/sec): (4607993/28645) IV
size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: PIXsecond(config)#
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングを行うための情報について説明します。

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

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。

- **debug crypto ipsec** - IPsec イベントに関する情報を表示します。
- **debug crypto isakmp**：インターネット キー エクスチェンジ（IKE）イベントに関するメッセージを表示します。
- **パケット if_name [ソース source_ip [netmask mask]] [dst dest_ip [netmask mask]] [デバッグして下さい[原始 icmp] | [原始 TCP [スポーツ src_port] [dport dest_port]] | [原始 UDP（ユーザ・データグラム・プロトコル）[スポーツ src_port] [dport dest_port]] [rx | tx | 両方]** —特定 のインターフェイスを押すパケットを表示する。 このコマンドは PIXfirst の内部インターフェイスのトラフィック の 種類を判別するとき役立ちます。 このコマンドも意図されている変換が行われることを確認するのに使用されています。
- **logging buffered は水平になります**— **show logging コマンド**で表示される内部バッファに syslog メッセージを送信 します。 メッセージ バッファをクリアする **clear logging コマンドを**使用して下さい。 バッファの終わりへの新しいメッセージ アペンド。 このコマンドが構築される変換を表示するのに使用されています。 バッファへの記録は必要な場合につける必要があります。 **ロギングバッファ レベル**無しでバッファリングするべき記録および/または**ログオンを**オフにしないで下さい。
- **debug icmp trace** —着き、から出発し、PIXファイアウォールを横断しなさいパケットのインターネット制御メッセージ プロトコル（ICMP）パケット情報、ソース IP アドレスおよび宛先アドレスを示します。 これには PIXファイアウォール ユニットの自身のインターフェイスに ping が含まれています。 **debug icmp trace を**消すのに **debug icmp trace を**使用しないで下さい。

これは **debug crypto isakmp** および **debug crypto ipsec コマンド**の出力です。

```
PIXfirst(config)#debug crypto isakmp PIXfirst(config)#debug crypto ipsec PIXfirst(config)#debug
crypto engine PIXfirst(config)#show debug debug crypto ipsec 1 debug crypto isakmp 1 debug
crypto engine PIXfirst(config)# PIXfirst(config)# crypto_isakmp_process_block:src:10.2.1.1,
dest:10.1.1.1 spt:500 dpt:500 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0):
processing SA payload. message ID = 137660894 ISAKMP : Checking IPSec proposal 1 ISAKMP:
transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type
in seconds ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP:
SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-MD5 !--- Phase 1
policy accepted. ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal
part #1, (key eng. msg.) dest= 10.1.1.1, src= 10.2.1.1, !--- Encryption domain (interesting
traffic) that invokes the tunnel. dest_proxy= 192.168.1.2/255.255.255.255/0/0 (type=1),
src_proxy= 192.168.100.2/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-
md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0):
processing NONCE payload. message ID = 137660894 ISAKMP (0): processing ID payload. message ID =
```

```
137660894 ISAKMP (0): ID_IPV4_ADDR src 192.168.100.2 prot 0 port 0 ISAKMP (0): processing ID
payload. message ID = 137660894 ISAKMP (0): ID_IPV4_ADDR dst 192.168.1.2 prot 0 port
0IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi 0x15ee92d9(367956697)
for SA from 10.2.1.1 to 10.1.1.1 for prot 3 return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:10.2.1.1, dest:10.1.1.1 spt:500 dpt:500 OAK_QM exchange
oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 2 map_alloc_entry:
allocating entry 1 ISAKMP (0): Creating IPSec SAs inbound SA from 10.2.1.1 to 10.1.1.1 (proxy
192.168.100.2 to 192.168.1.2) has spi 367956697 and conn_id 2 and flags 4 lifetime of 28800
seconds lifetime of 4608000 kilobytes outbound SA from 10.1.1.1 to 10.2.1.1 (proxy 192.168.1.2
to 192.168.100.2) has spi 1056204195 and conn_id 1 and flags 4 lifetime of 28800 seconds
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): ,
(key eng. msg.) dest= 10.1.1.1, src= 10.2.1.1, dest_proxy= 192.168.1.2/0.0.0.0/0/0 (type=1),
src_proxy= 192.168.100.2/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb, spi= 0x15ee92d9(367956697), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): , (key eng. msg.) src= 10.1.1.1, dest= 10.2.1.1, src_proxy=
192.168.1.2/0.0.0.0/0/0 (type=1), dest_proxy= 192.168.100.2/0.0.0.0/0/0 (type=1), protocol= ESP,
transform= esp-des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0x3ef465a3(1056204195),
conn_id= 1, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:10.2.1.1/500 Ref cnt incremented
to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:10.2.1.1/500 Ref cnt incremented to:3 Total VPN
Peers:1 return status is IKMP_NO_ERROR PIXfirst(config)#
```

これはソース コマンドの中のデバッグ パケットの出力です。

```
!--- Shows that the remote host packet is translated. PIXfirst(config)#debug packet inside src
192.168.50.2 dst 192.168.1.2 PIXfirst(config)# show debug debug packet inside src 192.168.50.2
dst 192.168.1.2 both --------- PACKET --------- -- IP -- !--- Source IP is translated to
192.168.50.2. 192.168.50.2 ==> 192.168.1.2 ver = 0x4 hlen = 0x5 tos = 0x0 tlen = 0x3c id = 0x82
flags = 0x0 frag off=0x0 ttl = 0x80 proto=0x1 chksum = 0x85ea !--- ICMP echo packet, as
expected. -- ICMP -- type = 0x8 code = 0x0 checksum=0x425c identifier = 0x200 seq = 0x900 --
DATA -- 0000001c: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 | abcdefghijklmnop 0000002c:
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 | qrstuvwabcdefghi 0000003c: 01 | . ---------
END OF PACKET --------- --------- PACKET --------- -- IP -- 192.168.50.2 ==> 192.168.1.2 ver =
0x4 hlen = 0x5 tos = 0x0 tlen = 0x3c id = 0x83 flags = 0x0 frag off=0x0 ttl = 0x80 proto=0x1
chksum = 0x85e9 -- ICMP -- type = 0x8 code = 0x0 checksum=0x415c identifier = 0x200 seq = 0xa00
-- DATA -- 0000001c: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 | abcdefghijklmnop
0000002c: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 | qrstuvwabcdefghi 0000003c: 01 | . --
------- END OF PACKET --------- --------- PACKET --------- -- IP -- 192.168.50.2 ==> 192.168.1.2
ver = 0x4 hlen = 0x5 tos = 0x0 tlen = 0x3c id = 0x84 flags = 0x0 frag off=0x0 ttl = 0x80
proto=0x1 chksum = 0x85e8 -- ICMP -- type = 0x8 code = 0x0 checksum=0x405c identifier = 0x200
seq = 0xb00 -- DATA -- 0000001c: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 |
abcdefghijklmnop 0000002c: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 | qrstuvwabcdefghi
0000003c: 01 | . --------- END OF PACKET --------- --------- PACKET --------- -- IP --
192.168.50.2 ==> 192.168.1.2 ver = 0x4 hlen = 0x5 tos = 0x0 tlen = 0x3c id = 0x85 flags = 0x0
frag off=0x0 ttl = 0x80 proto=0x1 chksum = 0x85e7 -- ICMP -- type = 0x8 code = 0x0
checksum=0x3f5c identifier = 0x200 seq = 0xc00 -- DATA -- 0000001c: 61 62 63 64 65 66 67 68 69
6a 6b 6c 6d 6e 6f 70 | abcdefghijklmnop 0000002c: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68
69 | qrstuvwabcdefghi 0000003c: 01 | . --------- END OF PACKET --------- PIXfirst(config)#
```

これは logging buffer コマンドの出力です。

```
!--- Logs show translation is built. PIXfirst(config)#logging buffer 7 PIXfirst(config)#logging
on PIXfirst(config)#show logging Syslog logging: enabled Facility: 20 Timestamp logging:
disabled Standby logging: disabled Console logging: disabled Monitor logging: disabled Buffer
logging: level debugging, 53 messages logged Trap logging: disabled History logging: disabled
Device ID: disabled 111009: User 'enable_15' executed cmd: show logging 602301: sa created, (sa)
sa_dest= 10.1.1.1, sa_prot= 50, sa_spi= 0xb1274c19(2972142617), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 2 602301: sa created, (sa) sa_dest= 10.2.1.1, sa_prot= 50, sa_spi=
0x892de1df(2301485535), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 1 !--- Translation is
built. 609001: Built local-host outside:192.168.100.2 305009: Built static translation from
outside:192.168.100.2 to inside:192.168.50.2 PIXfirst(config)#
```

これは debug icmp trace コマンドの出力です。

```
!--- Shows ICMP echo and echo-reply with translations !--- that take place.
PIXfirst(config)#debug icmp trace ICMP trace on Warning: this may cause problems on busy
networks PIXfirst(config)# 5: ICMP echo-request from outside:192.168.100.2 to 192.168.1.2
ID=1024 seq=1280 length=40 6: ICMP echo-request: translating outside:192.168.100.2 to
inside:192.168.50.2 7: ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=1280
length=40 8: ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2 9: ICMP
echo-request from outside:192.168.100.2 to 192.168.1.2 ID=1024 seq=1536 length=40 10: ICMP echo-
request: translating outside:192.168.100.2 to inside:192.168.50.2 11: ICMP echo-reply from
inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=1536 length=40 12: ICMP echo-reply: untranslating
inside:192.168.50.2 to outside:192.168.100.2 13: ICMP echo-request from outside:192.168.100.2 to
192.168.1.2 ID=1024 seq=1792 length=40 14: ICMP echo-request: translating outside:192.168.100.2
to inside:192.168.50.2 15: ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024
seq=1792 length=40 16: ICMP echo-reply: untranslating inside:192.168.50.2 to
outside:192.168.100.2 17: ICMP echo-request from outside:192.168.100.2 to 192.168.1.2 ID=1024
seq=2048 length=40 18: ICMP echo-request: translating outside:192.168.100.2 to
inside:192.168.50.2 19: ICMP echo-reply from inside:192.168.1.2 to 192.168.50.2 ID=1024 seq=2048
length=40 20: ICMP echo-reply: untranslating inside:192.168.50.2 to outside:192.168.100.2
PIXfirst(config)#
```

関連情報

- PIX 500 シリーズ セキュリティ アプライアンス サポート ページ
- PIX コマンド リファレンス
- Requests for Comments (RFC)
- 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
- テクニカルサポートとドキュメント - Cisco Systems