PIX/ASA/FWSM を介した PPTP/L2TP の接続許可

目次

概要

この資料がポイントツーポイント トンネリング プロトコル（PPTP）/Layer 2 トンネリング プロトコル（L2TP）クライアントをネットワーク アドレス変換（NAT）によって PPTP サーバに接続することを許可するように Ciscoセキュリティ Appliance/FWSM で必要な設定を説明します。

FWSM 3.1.x およびそれ以降は PAT の PPTP パススルーをサポートします。 この機能性を有効に するために PPTP インスペクションを使用して下さい。

注: FWSM のために PIX の同じ 設定を使用して下さい。

PPTP 接続を受容するようにセキュリティ アプライアンスを設定するには、『PPTP を使用するための Cisco Secure PIX Firewall の設定方法』を参照してください。

Microsoft Windows 2003 Internet の事前共有鍵を使用して、リモートの Microsoft Windows 2000/2003 および Windows XP のクライアントから PIX/ASA セキュリティ アプライアンス企業オフィスへの L2TP over IP Security（IPsec）を設定するには、『事前共有鍵を使用した Windows 2000/XP PC と PIX/ASA 7.2 の間の L2TP Over IPsec 設定例』を参照してください。

前提条件

要件

この設定を試みるために、PIX/ASA/FWSM を含む前にはたらく PPTP サーバおよびクライアントがなければなりません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco PIX Firewall バージョン 6.x 以降
- バージョン 7.x または それ 以上を実行する Cisco ASA 5500 シリーズ セキュリティ アプライアンス モデル
- バージョン 3.1.x または それ 以上を実行する FWSM

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。

背景理論

PPTP については、RFC 2637sで説明されています。 このプロトコルは、実際のデータ（PPP フレーム）を伝送するために、ポート 1723 を使用する TCP 接続、および Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）（プロトコル 47）の拡張機能を使用します。 TCP 接続はクライアントにより開始され、これにサーバによって開始される GRE 接続が続きます。

バージョン 6.2 以前の情報

PPTP 接続は一方のポートで TCP として開始され、GRE プロトコルによって応答されます。このため、両トラフィック フローが関連していることは、PIX の Adaptive Security Algorithm（ASA; アダプティブ セキュリティ アルゴリズム）では認識されていません。 その結果、PIX へのリターン トラフィックを許可するための ACL を設定する必要があります。 NAT（1 対 1 のアドレス マッピング）機能を持つ PIX を経由した PPTP が正しく動作するのは、PIX が TCP または User Datagram Protocol（UDP）ヘッダーのポート情報を使用して変換を追跡管理するためです。 Port Address Translation（PAT; ポート アドレス変換）機能を持つ PIX を経由した PPTP が動作しないのは、GRE にポートの概念がないためです。

バージョン 6.3 の情報

バージョン 6.3 での PPTP フィックスアップ機能により、PAT に設定されている場合に、PPTP トラフィックが PIX を通過できます。 さらに、このプロセスでは、ステートフルな PPTP パケット検査が実施されます。 fixup protocol pptp コマンドでは、PPTP パケットが検査され、さらに、GRE 接続がダイナミックに作成されて、PPTP トラフィックの許可に必要な変換が行われます。 特に、ファイアウォールでは、PPTP バージョンのアナウンスメントと、発信コールの要求/応答シーケンスが検査されます。 RFC 2637 で定義されているように、検査が行われるのは PPTP バージョン 1 だけです。 いずれかの側からアナウンスされたバージョンがバージョン 1 ではない場合は、TCP コントロール チャネル上の詳細検査はディセーブルにされます。さらに、発信コール要求と応答のシーケンスがトラッキングされます。 接続あるいは変換、またはその両方は、後続のセカンダリ GRE データ トラフィックを許可するために、必要に応じてダイナミックに割り当てられます。 PAT で PPTP トラフィックが変換されるためには、PPTP フィックスアップ機能をイネーブルにしておく必要があります。

バージョン 7.x の情報

バージョン 7.x の PPTP アプリケーション インスペクション エンジンは、バージョン 6.3 で **fixup protocol pptp** が動作するのと同じように動作します。

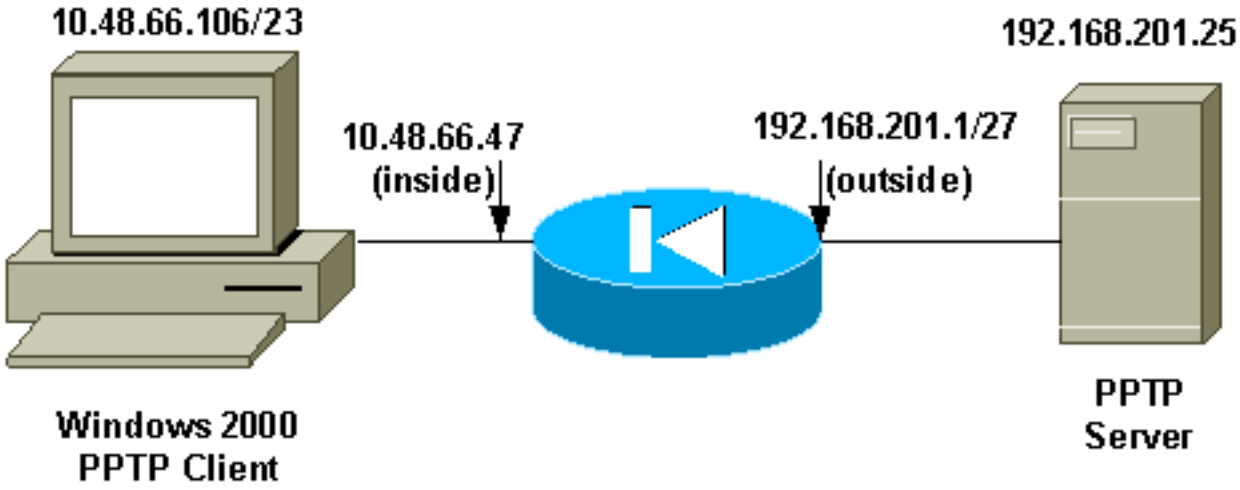
表記法

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。

クライアントが内部、サーバが外部の PPTP

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。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

6.2 以前のバージョン用の追加コマンド

バージョン 6.2 用のコマンドを追加するには、次のステップを実行します。

1. Inside PC に対してスタティック マッピングを定義します。 Outside で見えるアドレスは

192.168.201.5 です。pixfirewall(config)#**static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0**

2. PPTP サーバから PPTP クライアントへの GRE リターン トラフィックを許可するための ACL を設定します。pixfirewall(config)#**access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5**
3. ACL を適用します。pixfirewall(config)#**access-group acl-out in interface outside**

バージョン 6.3 用の追加コマンド

バージョン 6.3 用のコマンドを追加するには、次のステップを実行します。

1. 次のコマンドを使用して、フィックスアップ プロトコル PPTP 1723 をイネーブルにします。pixfirewall(config)#**fixup protocol pptp 1723**
2. PPTP フィックスアップ プロトコルがイネーブルになっているので、スタティック マッピングの定義は不要です。 PAT が使用できます。pixfirewall(config)#**nat (inside) 1 0.0.0.0 0.0.0.0 0 0** pixfirewall(config)#**global (outside) 1 interface**

inspection を使用した 7.x および 8.0 のバージョン用の追加コマンド

inspect コマンドを使用してバージョン 7.x と 8.0 用のコマンドを追加するには、次の手順を実行します。

1. デフォルトのクラスマップを使用するデフォルトのポリシーマップに、PPTP 検査を追加します。pixfirewall(config)#**policy-map global_policy** pixfirewall(config-pmap)#**class inspection_default** pixfirewall(config-pmap-c)#**inspect pptp**
2. PIX が PPTP トラフィックの検査を行っているので、スタティック マッピングの定義は不要です。 PAT が使用できます。pixfirewall(config)#**nat (inside) 1 0.0.0.0 0.0.0.0 0 0** pixfirewall(config)#**global (outside) 1 interface** **または**

ACL を使用した 7.x および 8.0 のバージョン用の追加コマンド

ACL を使用してバージョン 7.x と 8.0 用のコマンドを追加するには、次の手順を実行します。

1. Inside PC に対してスタティック マッピングを定義します。 Outside で見えるアドレスは 192.168.201.5 です。pixfirewall(config)#**static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0**
2. PPTP サーバから PPTP クライアントへの GRE リターン トラフィックを許可するための ACL を設定します。pixfirewall(config)#**access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5** pixfirewall(config)#**access-list acl-out permit tcp host 192.168.201.25 host 192.168.201.5 eq 1723**
3. ACL を適用します。pixfirewall(config)#**access-group acl-out in interface outside**

6.2 以前のバージョンでのコンフィギュレーション

PIX のコンフィギュレーション：クライアントが Inside、サーバが Outside
pixfirewall(config)#**write terminal** Building configuration... : Saved : PIX Version 6.2(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 intf2 security10 enable password Ujkil6aDv2yp6suI encrypted passwd

```
OnTrBUG1Tp0edmkr encrypted hostname pixfirewall domain-
name cisco.com fixup protocol ftp 21 fixup protocol http
80 fixup protocol h323 h225 1720 fixup protocol h323 ras
1718-1719 fixup protocol ils 389 fixup protocol rsh 514
fixup protocol rtsp 554 fixup protocol smtp 25 fixup
protocol sqlnet 1521 fixup protocol sip 5060 fixup
protocol skinny 2000 no names !--- This line allows GRE
traffic from the !--- PPTP server to the client. access-
list acl-out permit gre host 192.168.201.25 host
192.168.201.5 pager lines 24 logging on logging console
debugging logging trap debugging interface ethernet0
auto interface ethernet1 auto interface ethernet2 auto
shutdown mtu outside 1500 mtu inside 1500 mtu intf2 1500
ip address outside 209.165.201.1 255.255.255.224 ip
address inside 10.48.66.47 255.255.254.0 ip address
intf2 127.0.0.1 255.255.255.255 ip audit info action
alarm ip audit attack action alarm no failover failover
timeout 0:00:00 failover poll 15 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0 pdm history enable arp
timeout 14400 !--- This allows traffic from a low
security interface to !--- a high security interface.
static (inside,outside) 192.168.201.5 10.48.66.106
netmask 255.255.255.255 0 0 !--- This applies the ACL to
the outside interface. access-group acl-out in interface
outside timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
uauth 0:04:00 inactivity 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 snmp-server
enable traps no floodguard enable no sysopt route dnat
telnet timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:18bdf8e21bd72ec0533795549165ecf5 : end
[OK]
```

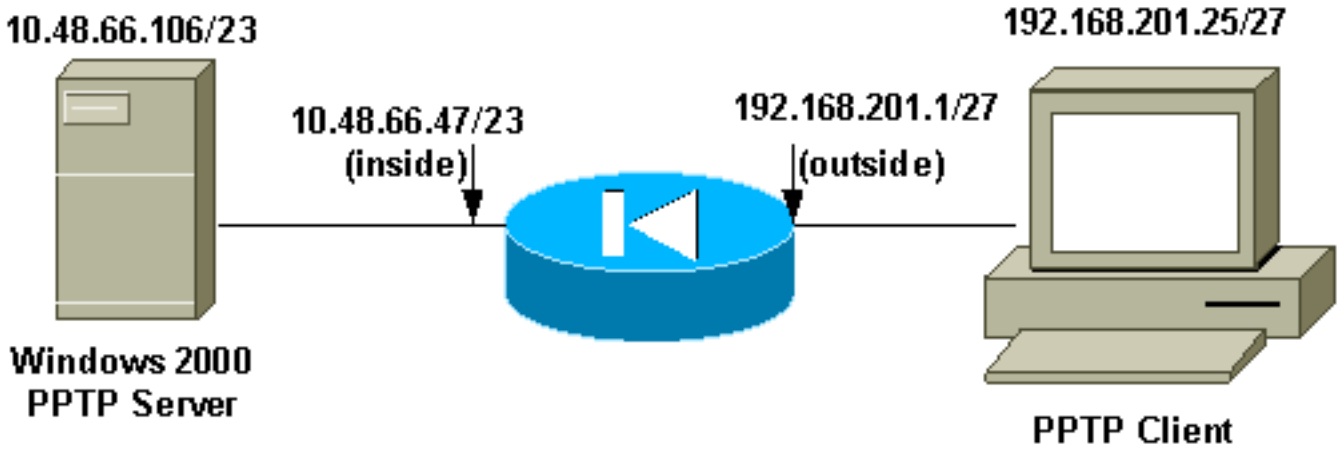
クライアントが Inside、サーバが Outside の L2TP

ACL を使用してバージョン 7.x と 8.x 用のコマンドを追加するには、次の手順を実行します（このコンフィギュレーションでは、PPTP クライアントとサーバの IP アドレスが L2TP クライアントとサーバの IP アドレスと同じであることを前提にしています）。

1. Inside PC に対してスタティック マッピングを定義します。 Outside で見えるアドレスは 192.168.201.5 です。`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**
2. L2TP サーバから L2TP クライアントへの L2TP リターン トラフィックを許可するための ACL を設定して適用します。`pixfirewall(config)#`
`pixfirewall(config)#`**`access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701`**
3. ACL を適用します。`pixfirewall(config)#`**`access-group acl-out in interface outside`**

外部クライアントと内部サーバを使用するPPTP

ネットワーク図



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

すべてのバージョン用の追加コマンド

このコンフィギュレーション例では、PPTP サーバが 192.168.201.5 (Inside アドレス 10.48.66.106 に対してスタティック) 、PPTP クライアントが 192.168.201.25 に存在します。

```
access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5 access-list acl-out permit
tcp host 192.168.201.25 host 192.168.201.5 eq 1723 static (inside,outside) 192.168.201.5
10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in interface outside
```

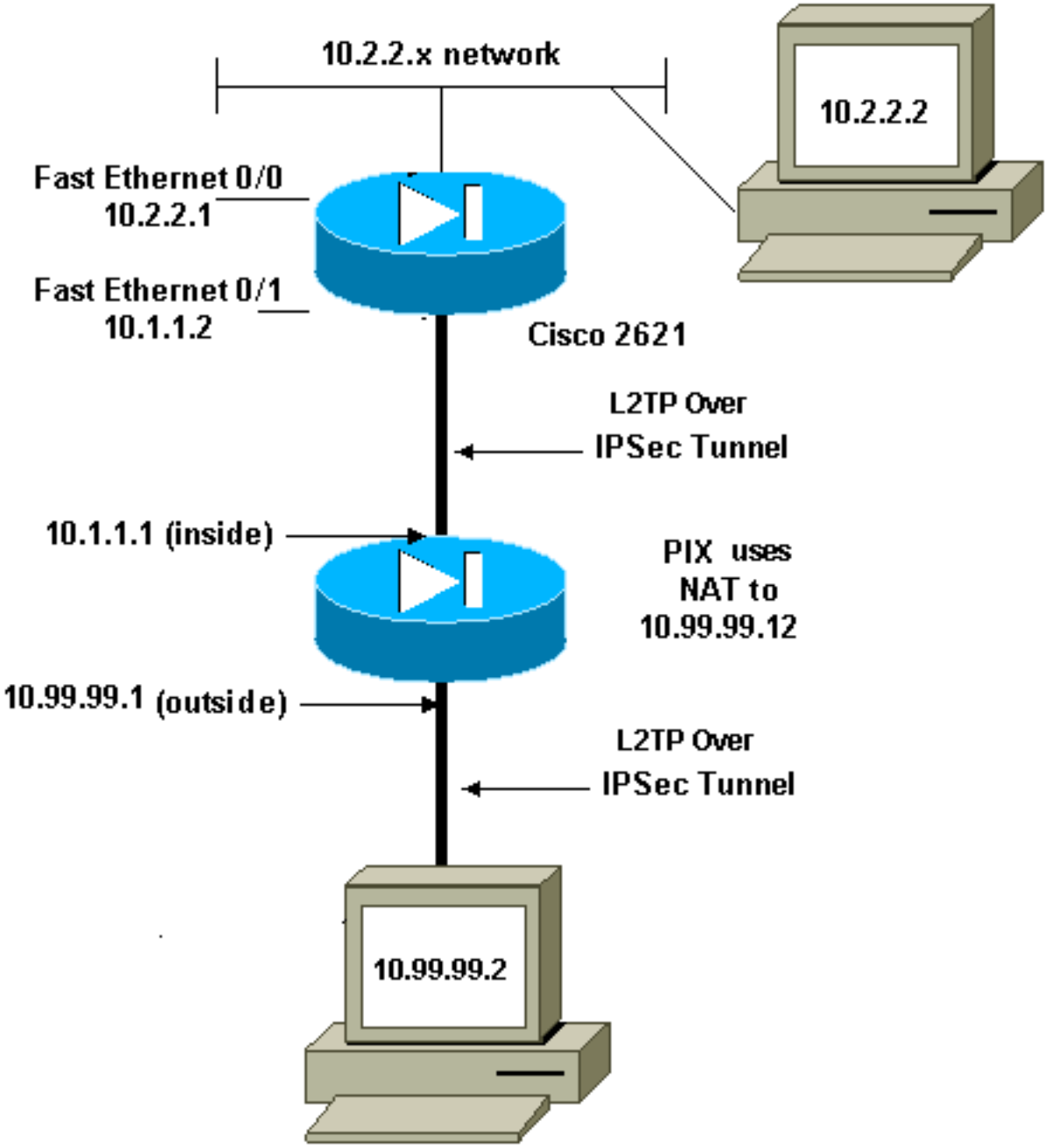
クライアントが Outside、サーバが Inside の L2TP

このコンフィギュレーション例では、L2TP サーバが 192.168.201.5 (Inside アドレス 10.48.66.106 に対してスタティック) 、L2TP クライアントが 192.168.201.25 に存在します。 (このコンフィギュレーションでは、PPTP クライアントとサーバの IP アドレスが L2TP クライアントとサーバの IP アドレスと同じであることを前提にしています) 。

```
access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701 static
(inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in
interface outside
```

PIX/ASA 7.x 以降による L2TP Over IPsec の許可

Outside の L2TP クライアントが、Inside の L2TP サーバと L2TP over IPsec VPN 接続を確立しようとします。 L2TP over IPsec パケットによる中間 PIX/ASA の通過を許可するには、ESP、ISAKMP (500) 、NAT-T、および L2TP ポート 1701 によるトンネルの確立を許可する必要があります。 L2TP パケットは PIX で変換され、VPN トンネルを介して送信されます。




```
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 10.99.99.12 10.1.1.2 netmask 255.255.255.255
access-group outside_access_in in interface outside

access-list outside_access_in remark Access Rule to Allow ESP traffic
access-list outside_access_in extended permit esp host 10.99.99.2
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow ISAKMP to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq isakmp
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 4500 (NAT-T) to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq 4500
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 1701 (L2TP) to
            host 10.99.99.12
```

```
access-list outside_access_in extended permit udp host 10.99.99.2 eq 1701
            host 10.99.99.12
```

確認

現在のところ、このドキュメントに関して、確認手順はありません。

トラブルシューティング

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。

PAT を使用している際の複数の PPTP/L2TP 接続での障害

PAT を使用している際に、PIX セキュリティ アプライアンスを介して維持できる PPTP/L2TP 接続は 1 つだけです。 この理由は、必要な GRE 接続はポート 0 で確立され、PIX セキュリティ アプライアンスでは、単一のホストへのポート 0 のマッピングだけを行うためです。 回避策はセキュリティ アプライアンス モデルの PPTP インスペクションを有効に することです。

受信 PPTP VPN に接続することを試みた場合エラー 800

受信 PPTP VPN に接続することを試みるときこのエラーメッセージが現れます:

```
Error 800: The remote connection was not made because the attempted VPN tunnels failed. The VPN
server might be unreachable. If this connection is attempting to use an L2TP/IPsec tunnel, the
security parameters required for IPsec negotiation might not be configured properly.
```

この問題は通常 PPTP または L2TP パススルーがクライアントとヘッドエンド デバイス間の中間 ASA で有効に ならないとき発生します。 PPTP または L2TP パススルーを有効に し、問題を解決するために設定をチェックして下さい。

debug 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。

次の例では、PIX の Inside の PPTP クライアントが PIX の Outside の PPTP サーバへの接続を開始していますが、この際に、GRE トラフィックを許可する ACL 設定はありません。 PIX でデバッグを口ギングすると、クライアントからの TCP ポート 1723 のトラフィックが開始され、GRE プロトコル 47 のリターン トラフィックが拒否されていることがわかります。

```
pixfirewall(config)#loggin on pixfirewall(config)#loggin console 7 pixfirewall(config)#302013:
Built outbound TCP connection 4 for outside: 192.168.201.25 /1723 (192.168.201.25 /1723) to
inside:10.48.66.106/4644 (192.168.201.5 /4644) 106010: Deny inbound protocol 47 src
outside:192.168.201.25 dst inside:192.168.201.5 106010: Deny inbound protocol 47 src
outside:192.168.201.25 dst inside:192.168.201.5
```

TAC のサービスリクエストをオープンする場合に収集すべき情報

上記のトラブルシューティング手順を実施した上で、さ

らにサポートが必要で、Cisco TAC でサービスリクエストをオープンする場合は、必ず次の情報を提供してください。
• 問題の説明と関連するトポロジの詳細 • サービスリクエストをオープンする前に実施したトラブルシューティング • show tech-support コマンドの出力 • logging buffered debugging コマンドを実行した後の show log コマンドの出力、または問題を示すコンソール キャプチャ（利用可能な場合） 収集したデータは、圧縮しないプレーン テキスト形式（.txt）でサービス リクエストに添付してください。Service Request Query Tool（登録ユーザ専用）を使用してアップロードすることで、サービス リクエストに情報を添付できます。 Service Request Query Tool にアクセスできない場合は、attach@cisco.com への電子メールに情報を添付して送信できます。この場合は、メッセージの件名（Subject）行にサービス リクエスト番号を記入してください。

関連情報

- PPTP に関するサポート ページ
- PIX/ASA 7.x 以降でのアクセス リストと MPF を使用した NAT を使用するセキュリティ アプライアンスをパススルーする IPSec トンネルの設定例
- 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
- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems