PPTP、MPPE、および IPSec を使用した PIX Firewall と VPN Client の設定

目次

概要

この設定例では、Cisco Secure PIX Firewall をトンネル エンドポイントとして、次の 4 種類のクライアントが接続とトラフィックの暗号化を行っています。

- Microsoft Windows 95 /98/NT の Cisco Secure VPN Client 1.1 を実行するユーザ
- Windows 95 /98/NT の CiscoセキュアVPN 3000 クライアント 2.5.x を実行するユーザ
- ネイティブ Windows 98 /2000/XP ポイントツーポイント トンネリング プロトコル（PPTP）クライアントを実行するユーザ
- Windows 95 /98/NT/2000/XP の Cisco VPN Client 3.x/4.x を実行するユーザ

この例では、IPsec のための単一 プー ルおよび PPTP は設定されます。 ただし、プールはまた別途に作ることができます。

前提条件

要件

このドキュメントに関する固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くものです。

- PIX ソフトウェア リリース 6.1.1
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client バージョン 2.5
- Cisco VPN Client 3.x and 4.x
- Microsoft Windows 2000 および Windows 98 クライアント

注: これは PIXソフトウェアリリース 6.3.3 テストされましたりリリース 5.2.x でおよび 5.3.1 で動作する必要があります。 Cisco VPN Client 3.x および 4.x に PIXソフトウェアリリース 6.x が必要となります。 （Cisco VPN 3000 Client 2.5 のためのサポートは PIXソフトウェアリリース 5.2.x に追加されます。 設定はまた Cisco VPN 3000 Client 部品。）IPsec を除いて PIXソフトウェアリリース 5.1.x のために、機能し、PPTP/Microsoft ポイント ツー ポイント暗号化（MPPE）は最初は別々に機能するように設計する必要があります。 別々にはたらかない場合、協力しません。

注: PIX 7.0 は RPC パケットを処理するのに **Inspect RPC** コマンドを使用します。 Inspect sunrpc コマンドは Sun RPC プロトコルのためのアプリケーション インスペクションを有効に するか、またはディセーブルにします。 Sun RPC サービスはシステムのあらゆるポートで動作できます。 クライアントがサーバの RPC サービスにアクセスするように試みるとき特定のサービスが実行するポート調べる必要があります。 それはよく知られたポート番号 111 のポートマッパプロセスの問い合わせによってこれをします。 クライアントはサービスの RPC プログラム数を送信 し、gets はポート番号を支持します。 ここから先は、クライアント プログラムはその新しいポートに RPC クエリを送ります。

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。

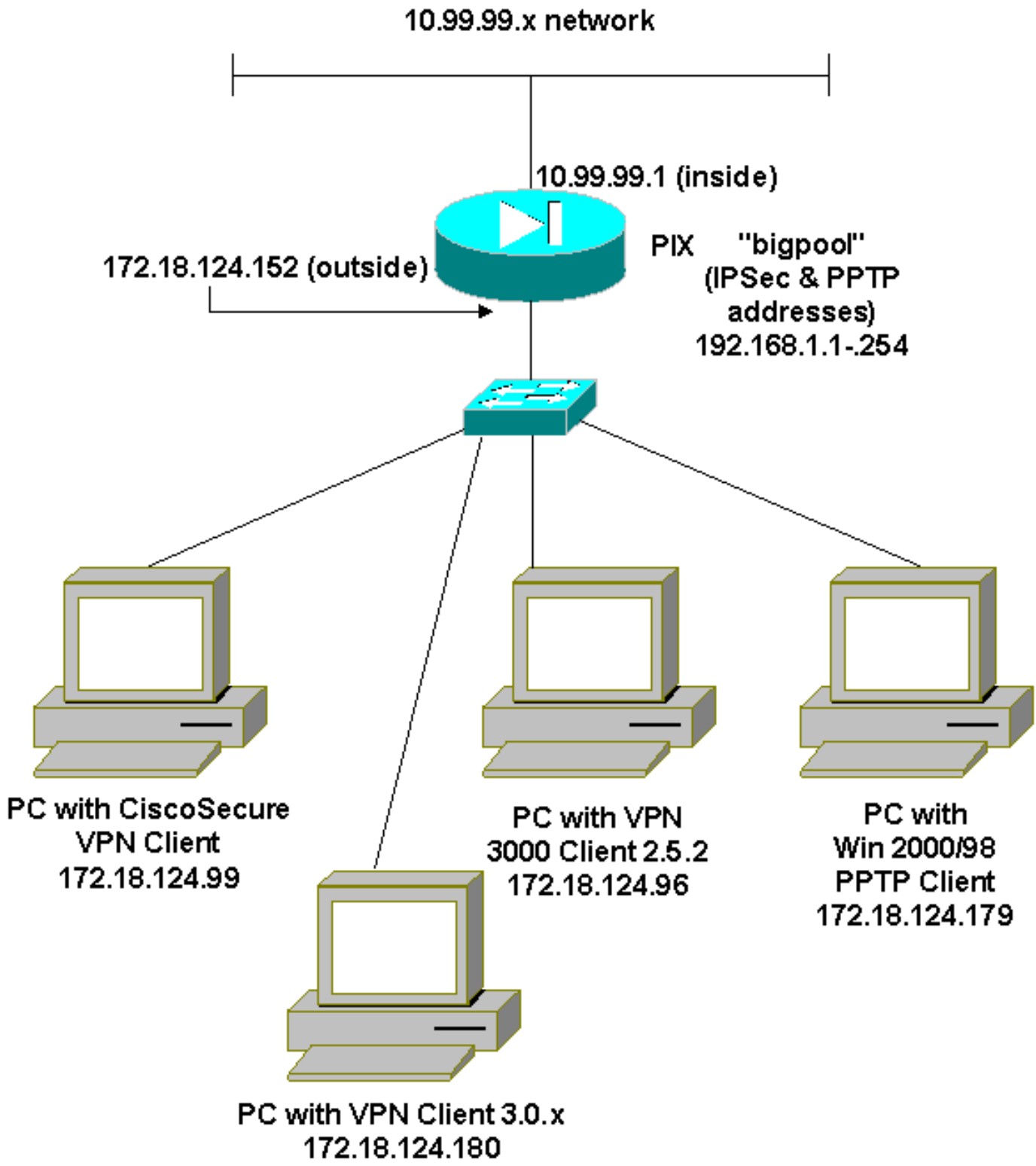
設定

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、次の図で示されるネットワーク構成を使用しています。



設定

このドキュメントでは、次の設定を使用します。

- Cisco Secure PIX Firewall
- Cisco Secure VPN Client 1.1

Cisco Secure PIX Firewall

`PIX Version 6.3(3)`
`interface ethernet0 auto`
`interface ethernet1 100full`

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname goss-515A
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
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
names
access-list 101 permit ip 10.99.99.0 255.255.255.0
192.168.1.0 255.255.255.0 pager lines 24 mtu outside
1500 mtu inside 1500 ip address outside 172.18.124.152
255.255.255.0 ip address inside 10.99.99.1 255.255.255.0
ip audit info action alarm ip audit attack action alarm
ip local pool bigpool 192.168.1.1-192.168.1.254 pdm
history enable arp timeout 14400 nat (inside) 0 access-
list 101 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
sysopt connection permit-ipsec sysopt connection permit-
pptp crypto ipsec transform-set myset esp-des esp-md5-
hmac crypto dynamic-map dynmap 10 set transform-set
myset crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside isakmp enable outside
!--- Cisco Secure_VPNClient_key. isakmp key ********
address 0.0.0.0 netmask 0.0.0.0 isakmp identity address
isakmp client configuration address-pool local bigpool
outside !--- ISAKMP Policy for Cisco VPN Client 2.5 or
!--- Cisco Secure VPN Client 1.1. isakmp policy 10
authentication pre-share isakmp policy 10 encryption des
isakmp policy 10 hash md5 !--- The 1.1 and 2.5 VPN
Clients use Diffie-Hellman (D-H) !--- group 1 policy
(PIX default). isakmp policy 10 group 1 isakmp policy 10
lifetime 86400 !--- ISAKMP Policy for VPN Client 3.0 and
4.0. isakmp policy 20 authentication pre-share isakmp
policy 20 encryption des isakmp policy 20 hash md5 !---
The 3.0/4.0 VPN Clients use D-H group 2 policy !--- and
PIX 6.0 code. isakmp policy 20 group 2 isakmp policy 20
lifetime 86400 vpngroup vpn3000-all address-pool bigpool
vpngroup vpn3000-all dns-server 10.99.99.99 vpngroup
vpn3000-all wins-server 10.99.99.99 vpngroup vpn3000-all
default-domain password vpngroup vpn3000-all idle-time
1800 !--- VPN 3000 group_name and group_password.
vpngroup vpn3000-all password ******** telnet timeout 5
ssh timeout 5 console timeout 0 vpdn group 1 accept
dialin pptp vpdn group 1 ppp authentication pap vpdn
group 1 ppp authentication chap vpdn group 1 ppp
authentication mschap vpdn group 1 ppp encryption mppe
```

```
auto vpdn group 1 client configuration address local
bigpool vpdn group 1 pptp echo 60 vpdn group 1 client
authentication local !--- PPTP username and password.
vpdn username cisco password ********* vpdn enable
outside terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
goss-515A#
```

Cisco Secure VPN Client 1.1

```
1- TACconn
      My Identity
           Connection security: Secure
           Remote Party Identity and addressing
           ID Type: IP subnet
           10.99.99.0
            255.255.255.0
           Port all Protocol all

      Connect using secure tunnel
           ID Type: IP address
           172.18.124.152

      Pre-shared Key=CiscoSecure_VPNClient_key

      Authentication (Phase 1)
      Proposal 1
          Authentication method: pre-shared key
          Encryp Alg: DES
          Hash Alg: MD5
          SA life: Unspecified
          Key Group: DH 1

      Key exchange (Phase 2)
      Proposal 1
          Encapsulation ESP
          Encrypt Alg: DES
          Hash Alg: MD5
          Encap: tunnel
          SA life: Unspecified
          no AH

  2- Other Connections
         Connection security: Non-secure
         Local Network Interface
           Name: Any
           IP Addr: Any
           Port: All
```

Cisco VPN 3000 Client 2.5.x または Cisco VPN Client 3.0

Options > Properties > Authentication の順に選択します。 次のように、group_name および group_password が PIX 上の group_name および group_password と照合されます。

```
vpngroup vpn3000-all password ********
Host-name = 172.18.124.152
```

Windows 2000 または Win 98 PPTP クライアントのセットアップ

PPTP クライアントを作るベンダーに連絡できます。 これをセットする方法の情報に関しては PPTP を使用するためのCisco Secure PIX Firewall の設定方法を参照して下さい。

確認

現在、この設定に使用できる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。

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。

PIX IPSec デバッグ

- **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。
- **debug crypto engine**：暗号化されたトラフィックを表示します。

PIX PPTP のデバッグ

- debug ppp io - PPTP PPP 仮想インターフェイスのパケット情報を表示します。
- **debug ppp error** — PPTP PPP バーチャルインターフェイスエラーメッセージを表示する。
- **debug vpdn error** — PPTP プロトコルエラーメッセージを表示する。
- **debug vpdn packets** — PPTP トラフィックについての PPTP パケット情報を表示する。
- **debug vpdn events** — PPTP トンネルイベント変更の情報を表示する。
- debug ppp uauth - PPTP PPP 仮想インターフェイスの AAA ユーザ認証デバッグ メッセージを表示します。

Microsoft関連の問題

- **RAS 接続をログオフの後でアクティブ保持する方法** — Windows Remote Access Service（RAS）クライアントからログオフする時、どの RAS 接続でも自動切断されます。 ログオフした後接続されたままになるために、RAS クライアントのレジストリの KeepRasConnections キーを有効に して下さい。
- **ユーザは**- Windowsベース の ワークステーション からのドメインにログオンするように試みるか、またはメンバーサーバおよびドメインコントローラが見つけることができないとき**キャッシュされた クレデンシャルとログオンするとき**—徴候 No エラーメッセージは表示する**警告されません**。 その代わり、キャッシュされたクレデンシャルを使用してローカル コンピュータにログインされます。
- **ドメイン バリデーションおよび他の名前解決問題のために LMHOST をファイル書く方法** —時直面する TCP/IP ネットワークの名前解決問題に例がある場合もあり、NetBIOS 名を変換するのに Lmhost ファイルを使用する必要があります。 この技術情報は名前解決およびド

メイン バリデーションを援助するために Lmhost ファイルを作成する適切な方式を論議します。

関連情報

- IPSec ネゴシエーション/IKE プロトコル サポートページ
- PIX コマンド リファレンス
- Cisco 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
- Requests for Comments (RFC)
- IPsec ネットワーク セキュリティの設定
- インターネット キー交換セキュリティ プロトコルの設定
- テクニカルサポートとドキュメント - シスコシステムズ