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

内容

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でCisco Secure VPN Client 1.1を実行するユーザ
- Windows 95/98/NTでCisco Secure VPN 3000 Client 2.5.xを実行するユーザ
- ネイティブWindows 98/2000/XP Point-to-Point Tunneling Protocol(PPTP)クライアントを実行するユーザ
- Windows 95/98/NT/2000/XPでCisco VPN Client 3.x/4.xを実行するユーザ

この例では、IPsecとPPTPの単一プールが設定されています。ただし、プールを分離することもできます。

前提条件

要件

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 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でテストされましたが、リリース5.2.x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にはPIXソフトウェアリリース6.xが必要です。(Cisco VPN 3000 Client 2.5のサポートは、PIXソフトウェアリリース5.2.xで追加されました。この設定は、Cisco VPN 3000 Clientの部分を除き、PIXソフトウェアリリース5.1.xでも動作します)。 IPSec と PPTP/Microsoft Point-to-Point Encryption（MPPE）は、最初に個別に動作するよう準備する必要があります。別々に作業しないと、一緒に作業できません。

注：PIX 7.0では、**inspect rpc**コマンドを使用して**RPC/**パケットを処理します。inspect sunrpcコマンドは、Sun RPCプロトコルのアプリケーション検査を有効または無効にします。Sun RPCサービスは、システム上の任意のポートで実行できます。クライアントがサーバ上のRPCサービスにアクセスしようとすると、特定のサービスが実行されているポートを見つける必要があります。これは、既知のポート番号111でportmapperプロセスを照会することによって行われます。クライアントがサービスのRPCプログラム番号を送信し、ポート番号を取得します。この時点から、クライアントプログラムはその新しいポートにRPCクエリを送信します。

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。

表記法

ドキュメント表記の詳細については、『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。

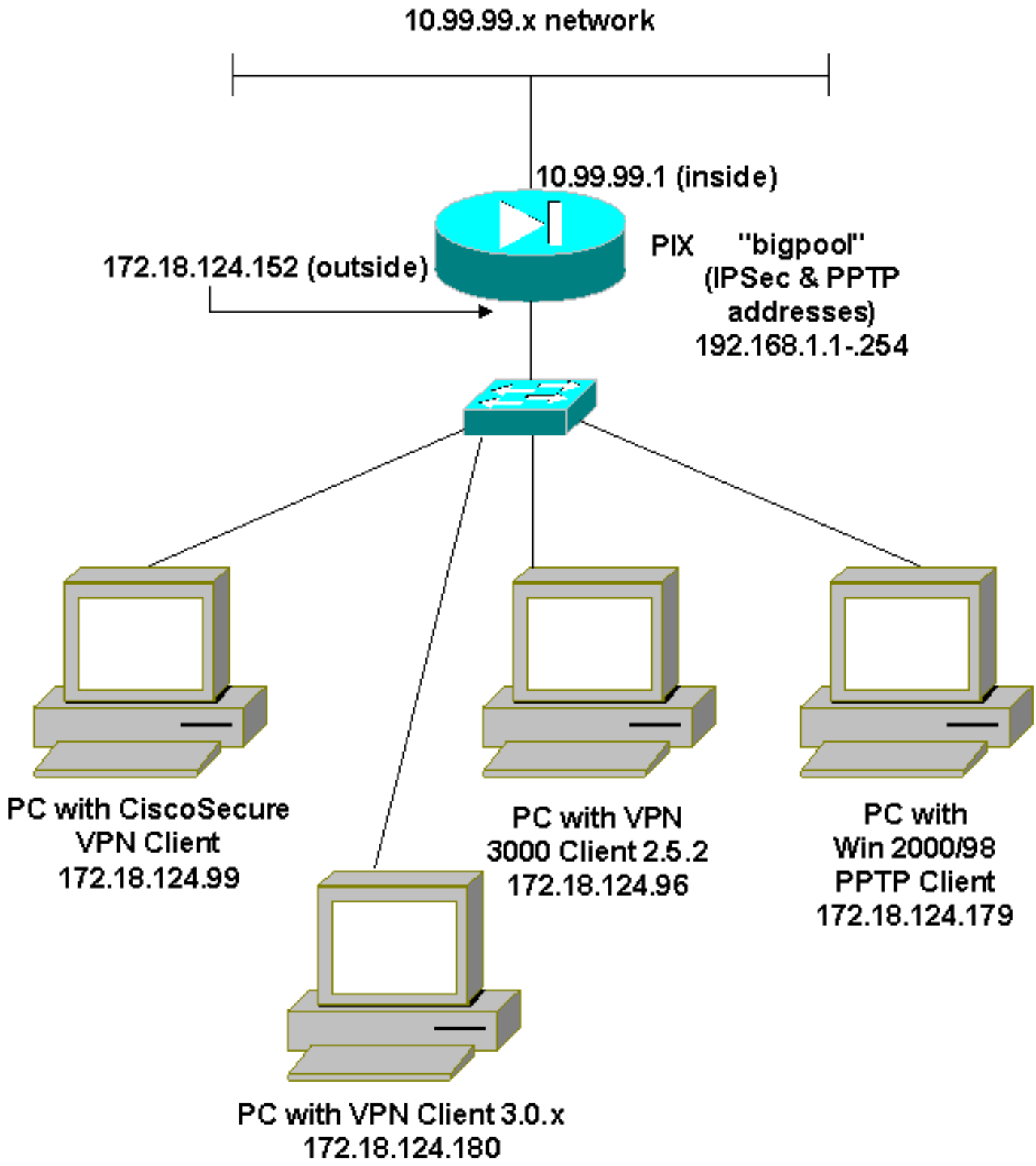
設定

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。

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設定を使用しています。



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クライアントを作成するベンダーに連絡できます。この設定方法の詳細は、『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。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

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 コマンドをサポートします。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。

PIX IPSec のデバッグ

- **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仮想インターフェイスエラーメッセージを表示します。
- **debug vpdn error**:PPTPプロトコルエラーメッセージを表示します。
- **debug vpdn packets**:PPTPトラフィックに関するPPTPパケット情報を表示します。
- **debug vpdn events**:PPTPトンネルイベントの変更情報を表示します。
- **debug ppp uauth**:PPTP PPP仮想インターフェイス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

- **ログオフ後に RAS 接続をアクティブなまま維持する方法** —Windows のリモート アクセス サービス（RAS）クライアントからログオフすると、RAS 接続が自動的に切断されます。ログオフ後も接続を維持するには、RASクライアントのレジストリでKeepRasConnectionsキーを有効にします。
- **キャッシュされたクレデンシャルを使用してログインするときにユーザに警告が通知されない** – 症状 – Windowsベースのワークステーションまたはメンバサーバからドメインにログオンしようとすると、ドメインコントローラが見つからない場合、エラーメッセージは表示されません。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。
- **ドメインの検証および他の名前解決に関する問題のために LMHOSTS ファイルを作成する方法** —TCP/IP ネットワークで名前解決に関する問題が発生し、NetBIOS 名の解決のために LMHOSTS ファイルを使用することが必要な場合があります。この記事では、名前解決とドメインの検証に役立つLmhostsファイルを適切に作成する方法について説明します。

関連情報

- 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
- 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 (RFCs)
- IPsec ネットワーク セキュリティの設定
- Internet Key Exchange 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 – Cisco Systems