Configurando o firewall PIX e clientes VPN utilizando PPTP, MPPE e IPSec.

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configurações](#)
[Cisco VPN 3000 Client 2.5.x ou Cisco VPN Client 3.x e 4.x](#)
[Configuração do cliente PPTP do Windows 98/2000/XP](#)
[Verificar](#)
[Troubleshoot](#)
[Comandos para Troubleshooting](#)
[Problemas relacionados à Microsoft](#)
[Informações Relacionadas](#)

Introduction

Nesse exemplo de configuração, quatro tipos diferentes de clientes se conectam e criptografam o tráfego com o Cisco Secure PIX Firewall como ponto final de túnel:

- Usuários que executam o Cisco Secure VPN Client 1.1 no Microsoft Windows 95/98/NT
- Usuários que executam o Cisco Secure VPN 3000 Client 2.5.x no Windows 95/98/NT
- Usuários que executam clientes Windows 98/2000/XP Point-to-Point Tunneling Protocol (PPTP) nativos
- Usuários que executam o Cisco VPN Client 3.x/4.x no Windows 95/98/NT/2000/XP

Neste exemplo, um único pool para IPsec e PPTP está configurado. No entanto, os pools também podem ser separados.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software PIX versão 6.3.3
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client versão 2.5
- Cisco VPN Client 3.x e 4.x
- Clientes Microsoft Windows 2000 e Windows 98

Nota: Isso foi testado no software PIX versão 6.3.3, mas deve funcionar nas versões 5.2.x e 5.3.1. O software PIX versão 6.x é necessário para o Cisco VPN Client 3.x e 4.x. (O suporte para o Cisco VPN 3000 Client 2.5 é adicionado no PIX Software Release 5.2.x. A configuração também funciona para o software PIX versão 5.1.x, exceto para a parte do Cisco VPN 3000 Client.) IPsec e PPTP/Microsoft Point-to-Point Encryption (MPPE) devem ser feitos para funcionarem separadamente primeiro. Se não funcionam separadamente, não trabalham em conjunto.

Observação: o PIX 7.0 usa o comando **inspect rpc** para manipular pacotes RPC. O comando inspect sunrpc ativa ou desativa a inspeção de aplicativos para o protocolo Sun RPC. Os serviços Sun RPC podem ser executados em qualquer porta do sistema. Quando um cliente tenta acessar um serviço RPC em um servidor, ele deve descobrir em qual porta esse serviço específico é executado. Isso é feito consultando-se o processo do mapeador de porta no número de porta 111, bem conhecido. O cliente envia o número do programa RPC do serviço e retorna o número da porta. Deste ponto em diante, o programa cliente envia suas consultas RPC para essa nova porta.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

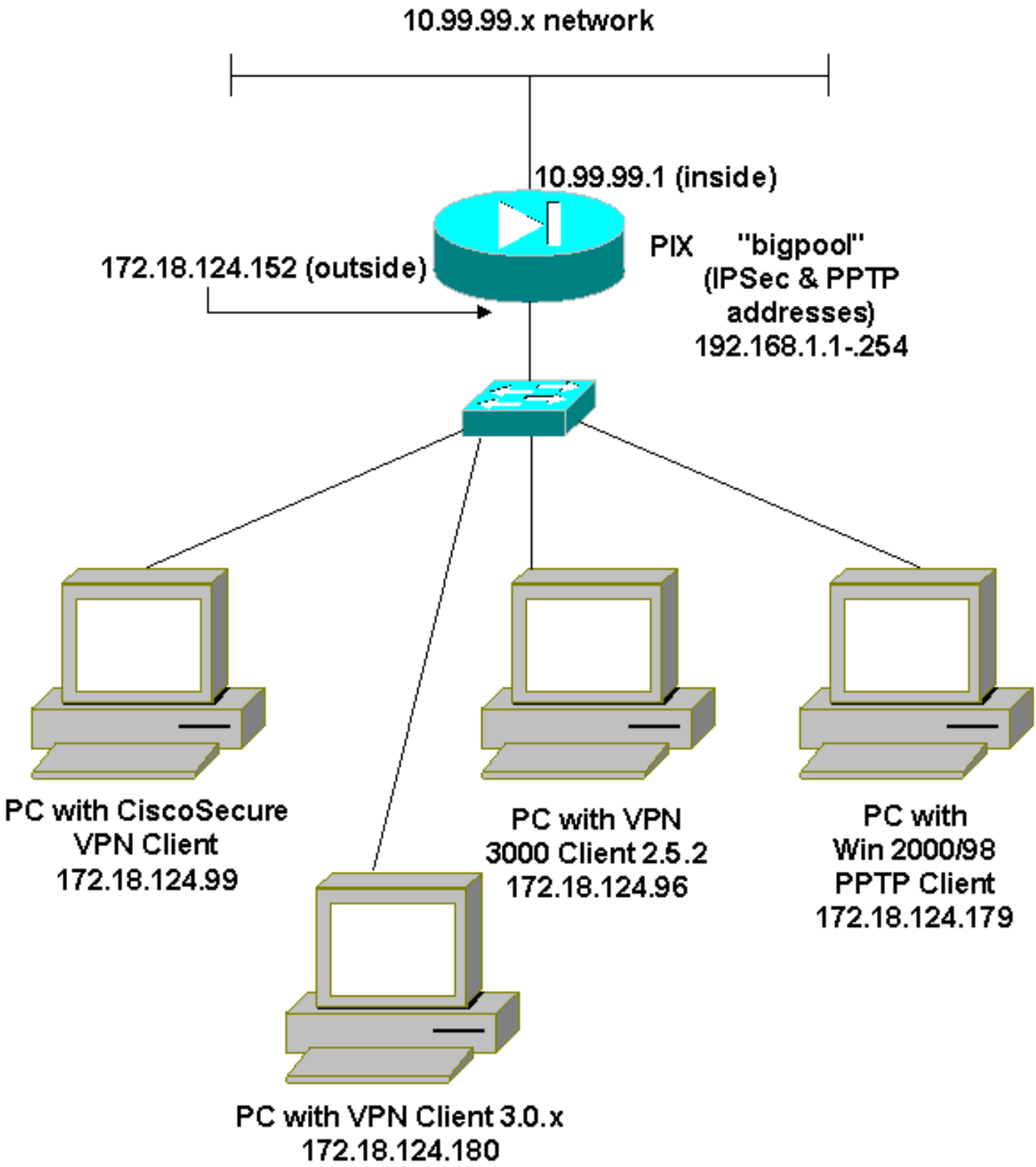
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.



Configurações

Este documento utiliza estas configurações.

- 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 ou Cisco VPN Client 3.x e 4.x

Selecionar opções > Propriedades > Autenticação. Group-name e group password correspondem a group_name e group_password no PIX como em:

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

Configuração do cliente PPTP do Windows 98/2000/XP

Você pode entrar em contato com o fornecedor que faz o cliente PPTP. Consulte Como Configurar o Cisco Secure PIX Firewall para Usar o PPTP para obter informações sobre como configurar isso.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Depuração IPSec PIX

- **debug crypto ipsec — Exibe as negociações de IPSec de fase 2**
- **debug crypto isakmp** — Exibe as negociações de Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.
- **debug crypto engine — Exibe o tráfego que está criptografado.**

Depuração PIX PPTP

- **debug ppp io** — Exibe as informações do pacote para a interface virtual PPTP PPP.
- **debug ppp error** — Exibe mensagens de erro de interfaces virtuais PPTP PPP.
- **debug vpdn error** — Exibe mensagens de erro do protocolo PPTP.
- **debug vpdn packets** —Exibe informações de pacote PPTP sobre o tráfego PPTP.
- **debug vpdn events** —Exibe informações de alteração de evento de túnel PPTP.
- **debug ppp uauth** — Exibe as mensagens de depuração de autenticação de usuário AAA da interface virtual PPTP PPP.

Problemas relacionados à Microsoft

- Como Manter conexões de RAS Ativas Após o Fim da Sessão —Quando você faz logoff de um cliente do Serviço de Acesso Remoto (RAS - Remote Access Service) do Windows, todas as conexões RAS são automaticamente desconectadas. Para permanecer conectado após o logoff, ative a chave KeepRasConnections no registro do cliente RAS.
- O Usuário Não é Alertado ao Conectar com Credenciais no Cache —Sintomas - Quando você tenta fazer logon em um domínio de uma estação de trabalho baseada no Windows ou de um servidor membro e um controlador de domínio não pode ser localizado, nenhuma mensagem de erro é exibida. Em vez disso, você será conectado ao computador local usando as credenciais em cache.
- Como Escrever um Arquivo LMHOSTS para a Validação de Domínio e Outros Problemas de Resolução de Nomes —Pode haver casos em que você enfrenta problemas de resolução de nomes em sua rede TCP/IP e precisa usar arquivos Lmhosts para resolver nomes NetBIOS. Este artigo discute o método apropriado de criar um arquivo Lmhosts para ajudar na resolução de nome e na validação de domínio.

Informações Relacionadas

- Páginas de Suporte de Protocolos de Negociação/IKE de IPsec
- Referências de comando PIX
- Página de suporte dos dispositivos de segurança Cisco PIX 500 Series
- Solicitações de Comentários (RFCs)
- Configuração da segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Suporte Técnico e Documentação - Cisco Systems