PPTP, MPPE 및 IPSec을 사용하여 PIX 방화벽 및 VPN 클라이언트 구성

목차

소개

이 샘플 컨피그레이션에서는 네 가지 종류의 클라이언트가 터널 엔드포인트로 Cisco Secure PIX Firewall을 사용하여 트래픽을 연결 및 암호화합니다.

- Microsoft Windows 95/98/NT에서 Cisco Secure VPN Client 1.1을 실행하는 사용자
- Windows 95/98/NT에서 Cisco Secure VPN 3000 Client 2.5.x를 실행하는 사용자
- 네이티브 Windows 98/2000/XP PPTP(Point-to-Point Tunneling Protocol) 클라이언트를 실행하는 사용자
- Windows 95/98/NT/2000/XP에서 Cisco VPN Client 3.x/4.x을 실행하는 사용자

이 예에서는 IPsec 및 PPTP에 대한 단일 풀이 구성됩니다. 그러나 풀은 따로 만들 수도 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX 소프트웨어 릴리스 6.3.3
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 클라이언트 버전 2.5
- Cisco VPN Client 3.x 및 4.x
- Microsoft Windows 2000 및 Windows 98 클라이언트

참고: PIX 소프트웨어 릴리스 6.3.3에서 테스트되었지만 릴리스 5.2.x 및 5.3.1에서 작동해야 합니다. Cisco VPN Client 3.x 및 4.x에는 PIX 소프트웨어 릴리스 6.x가 필요합니다. (Cisco VPN 3000 Client 2.5에 대한 지원은 PIX 소프트웨어 릴리스 5.2.x에 추가됩니다. 이 컨피그레이션은 Cisco VPN 3000 Client 부품을 제외하고 PIX Software Release 5.1.x에서도 작동합니다.) IPsec 및 PPTP/Microsoft MPPE(Point-to-Point Encryption)가 별도로 작동되어야 합니다. 별도로 작동하지 않으면 함께 작동하지 않습니다.

참고: PIX 7.0에서는 inspect rpc 명령**을** 사용하여 RPC 패킷을 처리합니다. inspect sunrpc 명령은 Sun RPC 프로토콜에 대한 애플리케이션 검사를 활성화하거나 비활성화합니다. Sun RPC 서비스는 시스템의 모든 포트에서 실행할 수 있습니다. 클라이언트가 서버의 RPC 서비스에 액세스하려고 할 때 특정 서비스가 실행되는 포트를 찾아야 합니다. 잘 알려진 포트 번호 111에서 portmapper 프로세스를 쿼리하여 이 작업을 수행합니다. 클라이언트는 서비스의 RPC 프로그램 번호를 전송하고 포트 번호를 다시 가져옵니다. 이 시점부터 클라이언트 프로그램은 RPC 쿼리를 새 포트로 전송합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

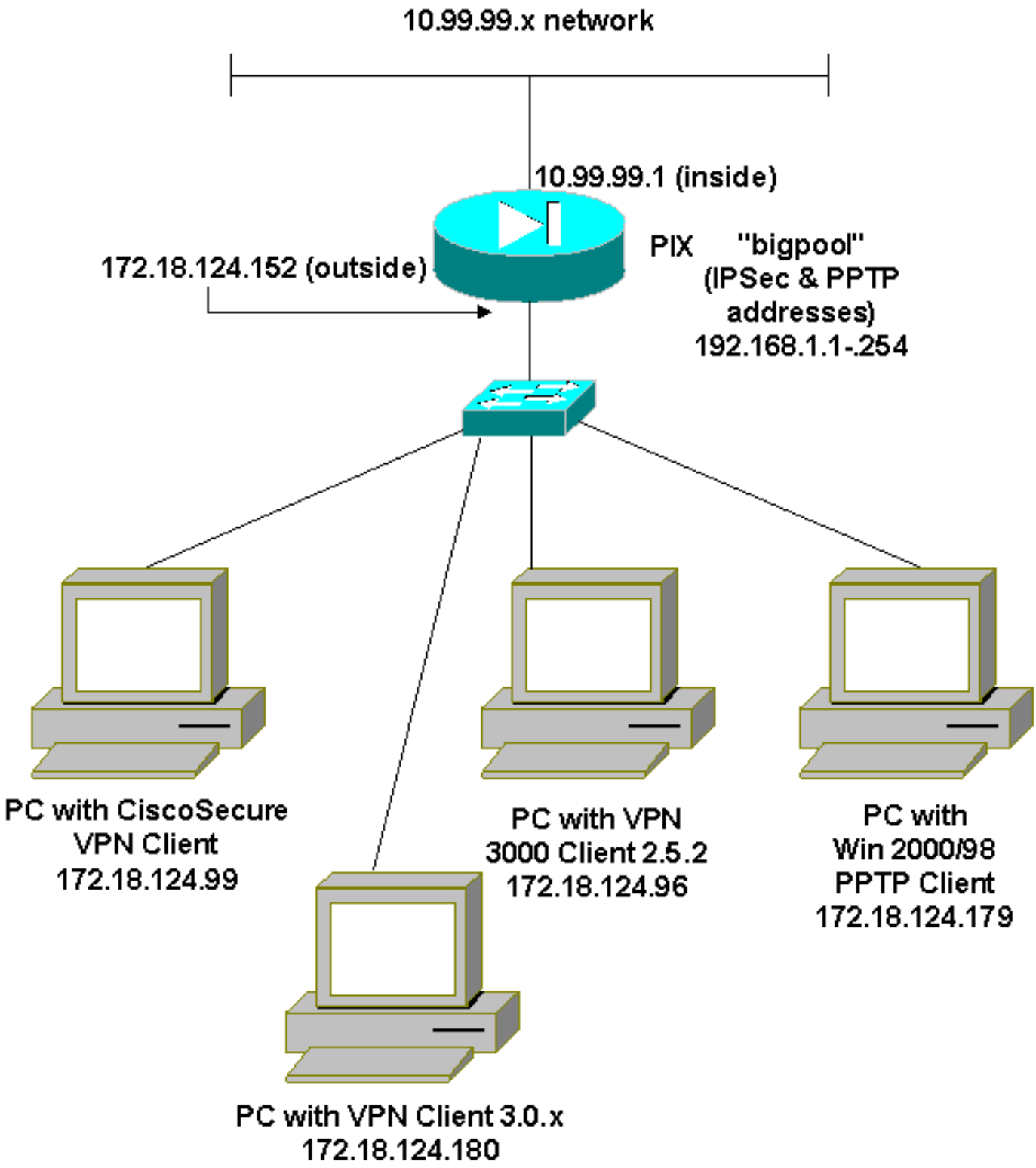
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.



구성

이 문서에서는 이러한 구성을 사용합니다.

- 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 또는 Cisco VPN Client 3.x 및 4.x

Options(**옵션**) > **Properties(속성**) > Authentication(**인증)을 선택합니다**. 그룹 이름 및 그룹 비밀번호는 다음과 같이 PIX의 group_name 및 group_password와 일치합니다.

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

Windows 98/2000/XP PPTP 클라이언트 설치

PPTP 클라이언트를 만드는 공급업체에 문의할 수 있습니다. 설정 방법에 대한 자세한 내용은 PPTP를 사용하도록 Cisco Secure PIX Firewall을 구성하는 방법을 참조하십시오.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

PIX IPsec 디버그

- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP(Internet Security Association and Key Management Protocol) 협상을 표시합니다.
- **debug crypto engine** - 암호화된 트래픽을 표시합니다.

PIX PPTP 디버그

- **debug ppp io** - PPTP PPP 가상 인터페이스에 대한 패킷 정보를 표시합니다.
- **debug ppp error(디버그 ppp 오류)** - PPTP PPP 가상 인터페이스 오류 메시지를 표시합니다.
- **debug vpdn error** - PPTP 프로토콜 오류 메시지를 표시합니다.
- **debug vpdn packets** - PPTP 트래픽에 대한 PPTP 패킷 정보를 표시합니다.
- **debug vpdn events** - PPTP 터널 이벤트 변경 정보를 표시합니다.
- **debug ppp uauth** — PPTP PPP 가상 인터페이스 AAA 사용자 인증 디버깅 메시지를 표시합니다.

Microsoft 관련 문제

- 로그오프 후 RAS 연결을 활성 상태로 유지하는 방법 - Windows RAS(원격 액세스 서비스) 클라이언트에서 로그오프하면 모든 RAS 연결이 자동으로 끊어집니다. 로그오프한 후 연결된 상태를 유지하려면 RAS 클라이언트의 레지스트리에서 KeepRasConnections 키를 활성화합니다.
- 캐시된 자격 증명으로 로그온할 때 사용자에게 경고가 표시되지 않음 —증상 - Windows 기반 워크스테이션이나 구성원 서버에서 도메인에 로그온하려고 할 때 도메인 컨트롤러를 찾을 수 없으면 오류 메시지가 표시되지 않습니다. 대신 캐시된 자격 증명을 사용하여 로컬 컴퓨터에 로그온합니다.
- 도메인 검증 및 기타 이름 확인 문제를 위해 LMHOSTS 파일을 작성하는 방법 - TCP/IP 네트워크에서 이름 확인 문제가 발생하고 Lmhosts 파일을 사용하여 NetBIOS 이름을 확인해야 하는 인스턴스가 있을 수 있습니다. 이 문서에서는 이름 확인 및 도메인 검증을 지원하기 위해 Lmhosts 파일을 생성하는 적절한 방법에 대해 설명합니다.

관련 정보

- IPsec 협상/IKE 프로토콜 지원 페이지
- PIX 명령 참조
- Cisco PIX 500 Series 보안 어플라이언스 지원 페이지
- RFC(Request for Comments)
- IPsec 네트워크 보안 구성
- 인터넷 키 교환 보안 프로토콜 구성
- 기술 지원 및 문서 – Cisco Systems