Конфигурирование межсетевого экрана PIX Firewall и VPN Clients при помощи PPTP, MPPE and IPSec

Содержание

Введение

В этом примере конфигурации четыре клиента разных типов подключаются и шифруют трафик при помощи межсетевого экрана Cisco Secure PIX как конечной точки туннеля:

- Пользователи, которые выполняют Cisco Secure VPN Client 1.1 на Microsoft Windows 95/98/NT
- Пользователи, которые выполняют Cisco Secure VPN 3000 Клиентов 2.5.x на/98/NT Windows 95/98
- Пользователи, которые выполняют собственные окна клиенты Протокола PPTP 98/2000/XP
- Пользователи, которые выполняют Cisco VPN Client 3.x/4.x на/98/NT/2000/XP Windows 95/98

В данном примере настроен отдельный пул для IPsec и PPTP. Однако эти пулы могут быть и раздельными.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Выпуск 6.3.3 программного обеспечения PIX
- Cisco Secure VPN Client 1.1
- Клиент Cisco VPN 3000 версии 2.5
- Cisco VPN Client 3.x и 4.x
- Клиенты Microsoft Windows 2000 и Windows 98

Примечание: Это было протестировано на Релизе программного обеспечения PIX 6.3.3, но должно работать на выпуск 5.2.x и 5.3.1. Релиз программного обеспечения PIX 6.x требуется для Cisco VPN Client 3.x и 4. x. (Поддержка для Cisco VPN 3000 Client 2.5 добавлена в программном обеспечении PIX, релиз 5.2.x. Настройка также работает для программного обеспечения PIX, релиз 5.1.x, кроме части Cisco VPN 3000 Client). Первоначально следует настроить IPsec и PPTP/Microsoft Point-to-Point Encryption (MPPE) для работы по отдельности. Если они не работают отдельно, то не будут работать вместе.

Примечание: PIX 7.0 использует **команду inspect rpc** для обработки пакетов RPC. **Команда inspect sunrpc включает и выключает проверку приложений для протокола Sun RPC.** Сервисы Sun RPC могут работать на любом порте системы. Когда клиент пытается получить доступ к сервису Sun RPC на сервере, он должен выяснить, с каким портом работает этот сервис. Это делается с помощью обращения к процессу сопоставления портов на хорошо известном номере порта 111. Клиент посылает программный номер сервиса RPC и получает в ответ номер порта. С этого момента программа-клиент посылает свои запросы RPC на этот новый порт.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

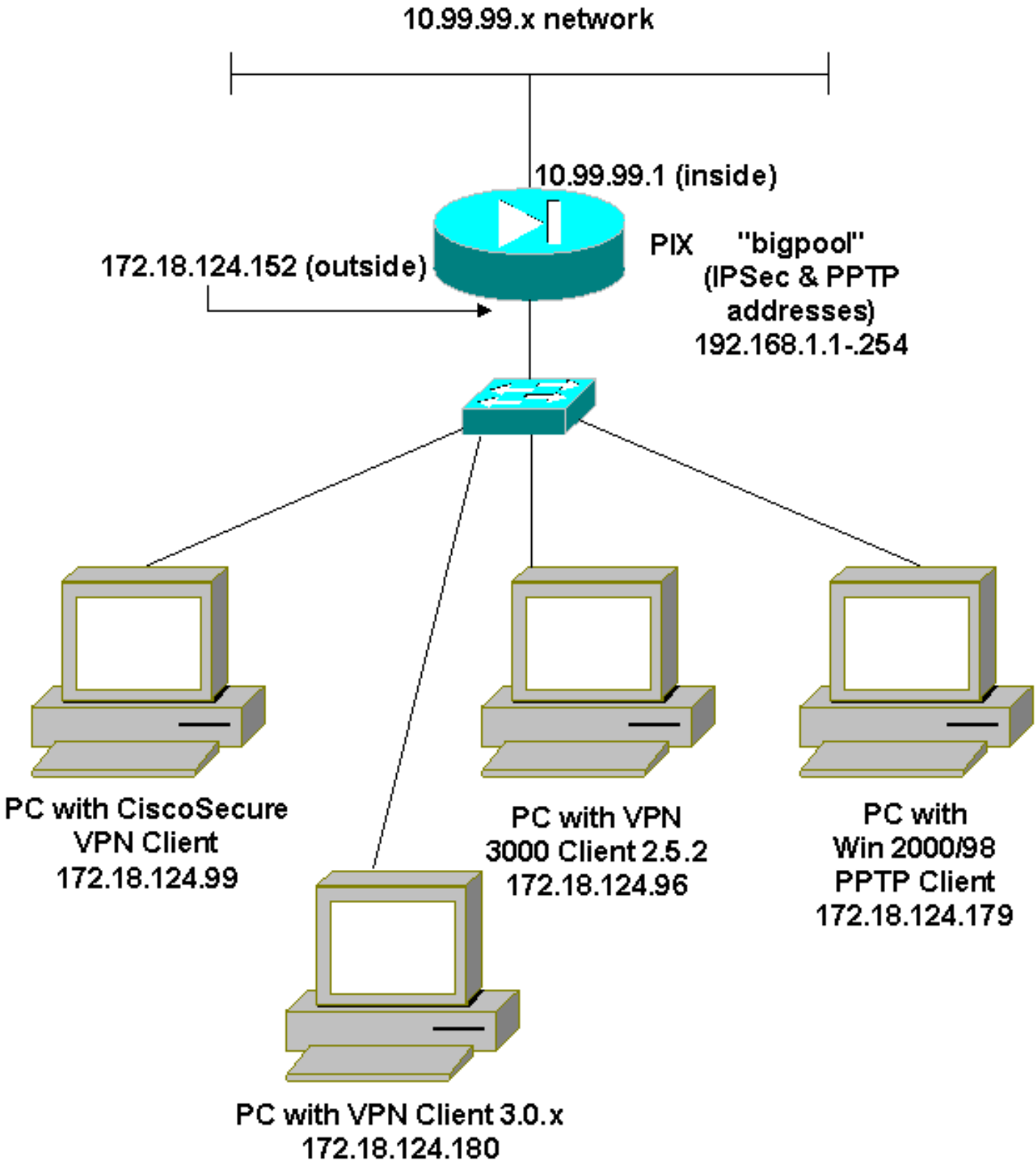
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме.



Конфигурации

Эти конфигурации используются в данном документе.

- Межсетевой экран Cisco Secure PIX
- Cisco Secure VPN Client 1.1

Межсетевой экран Cisco Secure PIX
`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 или Cisco VPN Client 3.x и 4.x

Выберите "Параметры > Свойства > Аутентификация" (Options > Properties > Authentication). Имя группы и пароль группы совпадают с group_name и group_password на PIX, как в:

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

Настройка PPTP-клиента Windows 98/2000/XP

Можно связаться с поставщиком, который делает клиента PPTP. Информацию об установке

см. в разделе Как настроить брандмауэр Cisco Secure PIX для использования PPTP.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Отладка IPSec PIX

- **debug crypto ipsec – отображает согласования IPSec на Этапе 2.**
- **debug crypto isakmp** согласования Протокола ISAKMP фазы 1.
- **debug crypto engine– показывает зашифрованный трафик.**

Отладка PIX PPTP

- **debug ppp io - вывод сведений о пакетах для виртуального интерфейса PPTP PPP.**
- **debug ppp error** — Отображает сообщения об ошибках виртуального интерфейса PPP PPTP.
- **debug vpdn error** — Отображает сообщения об ошибках протокола PPTP.
- **debug vpdn packet** — Отображают информацию о пакете PPTP о трафике PPTP.
- **debug vpdn event** — Отображают сведения об изменении события туннеля PPTP.
- **debug ppp uauth - показывает сообщения отладки аутентификации пользователей AAA виртуального интерфейса PPTP PPP.**

Проблемы с программным обеспечением от Microsoft

- Как Поддержать RAS - подключения Активными После Того, чтобы выходить из системы — Когда вы выходите из системы от клиента Windows Remote Access Service (RAS), любые RAS - подключения автоматически разъединены. Чтобы сохранить подключение, включите в клиенте RAS ключ реестра KeepRasConnections.
- Пользователь не получает уведомления при регистрации с кэшированными учетными данными Симптомы: не возникает никакого сообщения об ошибке, когда делается попытка зарегистрироваться в домене с рабочей станции под управлением Windows или с рядового сервера, и не удается найти контроллер домена. Вместо этого происходит регистрация на локальном компьютере с использованием кэшированных учетных

данных.
- Как написать файл LMHOSTS для проверки данных домена и других проблем разрешения имен Могут возникнуть ситуации, когда появляются проблемы с разрешением имен в сети TCP/IP, и необходимо использовать файлы Lmhosts для разрешения имен NetBIOS. В этой статье обсуждается правильный метод создания файла Lmhosts для помощи в разрешении имен и проверке данных домена.

Дополнительные сведения

- Страницы технической поддержки IPSec Negotiation/IKE Protocols
- Справочник по командам PIX
- Страница поддержки устройств защиты Cisco PIX серии 500
- Запросы комментариев (RFC)
- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- Cisco Systems – техническая поддержка и документация