Configuración del PIX Firewall y los clientes VPN que usan PPTP, MPPE y IPSec

Contenido

Introducción

En esta configuración de ejemplo, cuatro tipos diferentes de clientes conectan y cifran tráfico en el firewall PIX de Cisco Secure como punto final del túnel:

- Usuarios que ejecutan Cisco Secure VPN Client 1.1 en Microsoft Windows 95/98/NT
- Usuarios que ejecutan Cisco Secure VPN 3000 Client 2.5.x en Windows 95/98/NT
- Usuarios que ejecutan clientes nativos del protocolo de túnel punto a punto (PPTP) de Windows 98/2000/XP
- Usuarios que ejecutan Cisco VPN Client 3.x/4.x en Windows 95/98/NT/2000/XP

En este ejemplo, se configura un único conjunto para IPsec y PPTP. Sin embargo, las piscinas también se pueden separar.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software PIX versión 6.3.3
- Secure VPN Client 1.1 de Cisco
- Cliente Cisco VPN 3000 versión 2,5
- Cliente de VPN 3.x y 4.x de Cisco
- Clientes Microsoft Windows 2000 y Windows 98

Nota: Esto se probó en la versión 6.3.3 del software PIX, pero debería funcionar en las versiones 5.2.x y 5.3.1. Se requiere la versión 6.x del software PIX para Cisco VPN Client 3.x y 4.x. (El soporte para Cisco VPN 3000 Client 2.5 se agrega en la versión 5.2.x del software PIX. La configuración también funciona para la versión 5.1.x del software PIX, excepto para la parte Cisco VPN 3000 Client.) IPsec y PPTP/Microsoft Point-to-Point Encryption (MPPE) deben funcionar primero por separado. Si no funcionan por separado, no funcionan juntos.

Nota: PIX 7.0 utiliza el comando **inspect rpc** para manejar los paquetes RPC. El comando **inspect sunrpc** habilita o inhabilita la inspección de la aplicación para el protocolo Sun RPC. Los servicios Sun RPC pueden ejecutarse en cualquier puerto del sistema. Cuando un cliente intenta acceder a un servicio RPC en un servidor, debe averiguar en qué puerto se ejecuta ese servicio concreto. Hace esto consultando el proceso del portmapper en el conocido número de puerto 111. El cliente envía el número de programa RPC del servicio y devuelve el número de puerto. A partir de este punto, el programa cliente envía sus consultas RPC a ese nuevo puerto.

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

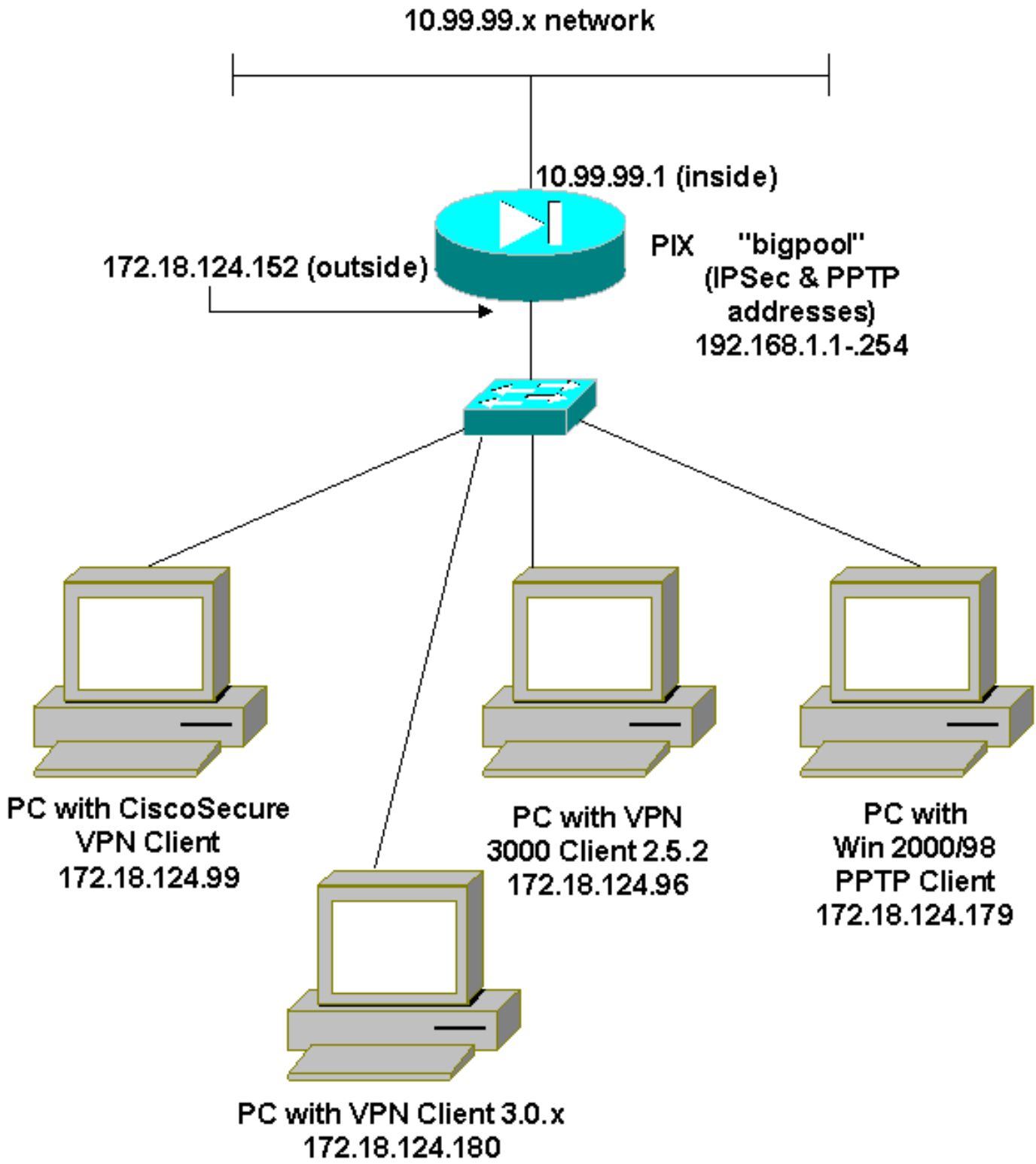
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa estas configuraciones.

- Firewall Secure PIX de Cisco
- Secure VPN Client 1.1 de Cisco

Firewall Secure PIX de Cisco
`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#
```

Secure VPN Client 1.1 de Cisco

```
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
```

Cliente Cisco VPN 3000 2.5.x o Cliente Cisco VPN 3.x y 4.x

Seleccione Opciones > Propiedades > Autenticación. El nombre de grupo y la contraseña de grupo coinciden con aquellas del PIX al igual que en:

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

Configuración del cliente Windows 98/2000/XP PPTP

Puede ponerse en contacto con el proveedor que crea el cliente PPTP. Refiérase a Cómo Configurar Cisco Secure PIX Firewall para Utilizar PPTP para obtener información sobre cómo configurar esto.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

Depuración de PIX IPSec

- **debug crypto ipsec — Muestra los IPSec Negotiations de la Fase 2.**
- **debug crypto isakmp**: muestra las negociaciones de la fase 1 de la Asociación de Seguridad de Internet y del Protocolo de administración de claves (ISAKMP).
- **debug crypto engine**: muestra el tráfico cifrado.

Depuración PIX PPTP

- **debug ppp io — Muestra la información de paquete para la interfaz virtual PPTP PPP.**
- **debug ppp error**: muestra los mensajes de error de la interfaz virtual PPTP PPP.
- **debug vpdn error**—Muestra los mensajes de error del protocolo PPTP.
- **debug vpdn packets**—Muestra información del paquete PPTP sobre el tráfico PPTP.
- **debug vpdn events**—Muestra información de cambio de evento de túnel PPTP.
- **debug ppp uauth**: muestra los mensajes de depuración de autenticación de usuario AAA de la interfaz virtual PPP PPTP.

Problemas relacionados con Microsoft

- Cómo Mantener las Conexiones RAS Activas después de Cerrar una Sesión : cuando se desconecta de un cliente del servicio de acceso remoto de Windows (RAS), las conexiones RAS se desconectan automáticamente. Para permanecer conectado después de cerrar la sesión, habilite la clave KeepRasConnections en el Registro en el cliente RAS.
- No se Alerta al Usuario cuando se Inicia Sesión con las Credenciales Guardadas en Caché —Síntomas: cuando intenta iniciar sesión en un dominio desde una estación de trabajo basada en Windows o un servidor miembro y no se puede encontrar un controlador de dominio, no se muestra ningún mensaje de error. En su lugar, se abre una sesión en el equipo local con las credenciales guardadas en caché.
- Cómo Escribir un Archivo LMHOSTS para la Validación de Dominio y Otros Problemas de Resolución de Nombre —Puede haber instancias en las que experimenta problemas de resolución de nombres en su red TCP/IP y necesita utilizar los archivos Lmhosts para resolver los nombres de NetBIOS. Este artículo trata sobre el método adecuado para crear un archivo Lmhosts para ayudar en la resolución de nombres y la validación de dominios.

Información Relacionada

- Páginas de Soporte de Negociación IPsec/Protocolos IKE
- Referencia de Comandos PIX
- Página de Soporte de Cisco PIX 500 Series Security Appliances
- Solicitudes de Comentarios (RFC)
- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Soporte Técnico y Documentación - Cisco Systems