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 funcionan con al Cliente Cisco Secure VPN 1.1 en Microsoft Windows 95/98/NT
- Usuarios que funcionan con al cliente 2.5.x del VPN de Cisco Secure 3000 en Windows 95/98/NT
- Usuarios que funcionan con a los clientes del Point-to-Point Tunneling Protocol (PPTP) de las ventanas nativas 98/2000/XP
- Usuarios que funcionan con al Cliente Cisco VPN 3.x/4.x en Windows 95/98/NT/2000/XP

En este ejemplo, configuran a una sola agrupación para el IPSec y el PPTP. Sin embargo, los pools pueden también ser hechos separados.

prerrequisitos

Requisitos

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 fue probada en el software PIX versión 6.3.3 pero debe trabajar en la versión 5.2.x y 5.3.1. El software PIX versión 6.x se requiere para el Cliente Cisco VPN 3.x y 4.x. (El soporte para el Cliente Cisco VPN 3000 2.5 se agrega en el software PIX versión 5.2.x. La configuración también trabaja para el software PIX versión 5.1.x, a excepción del IPSec partición del Cliente Cisco VPN 3000) y el Point-to-Point Encryption PPTP/Microsoft (MPPE) se debe hacer para trabajar por separado primero. Si no trabajan por separado, no trabajan juntos.

Nota: El PIX 7.0 utiliza el **comando inspect rpc** de manejar los paquetes RPC. El comando inspect sunrpc habilita o inhabilita la Inspección de la aplicación para el Protocolo RPC de Sun. Los servicios de Sun RPC pueden ejecutarse en cualquier puerto en el sistema. Cuando un cliente intenta acceder un servicio RPC en un servidor, debe descubrir que viran los funcionamientos de ese servicio determinado hacia el lado de babor encendido. Hace esto preguntando el proceso del portmapper en el número de puerto conocido 111. El cliente envía el número del programa RPC del servicio, y consigue detrás el número del puerto. Desde aquí, el programa del cliente envía sus interrogaciones RPC a ese nuevo puerto.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

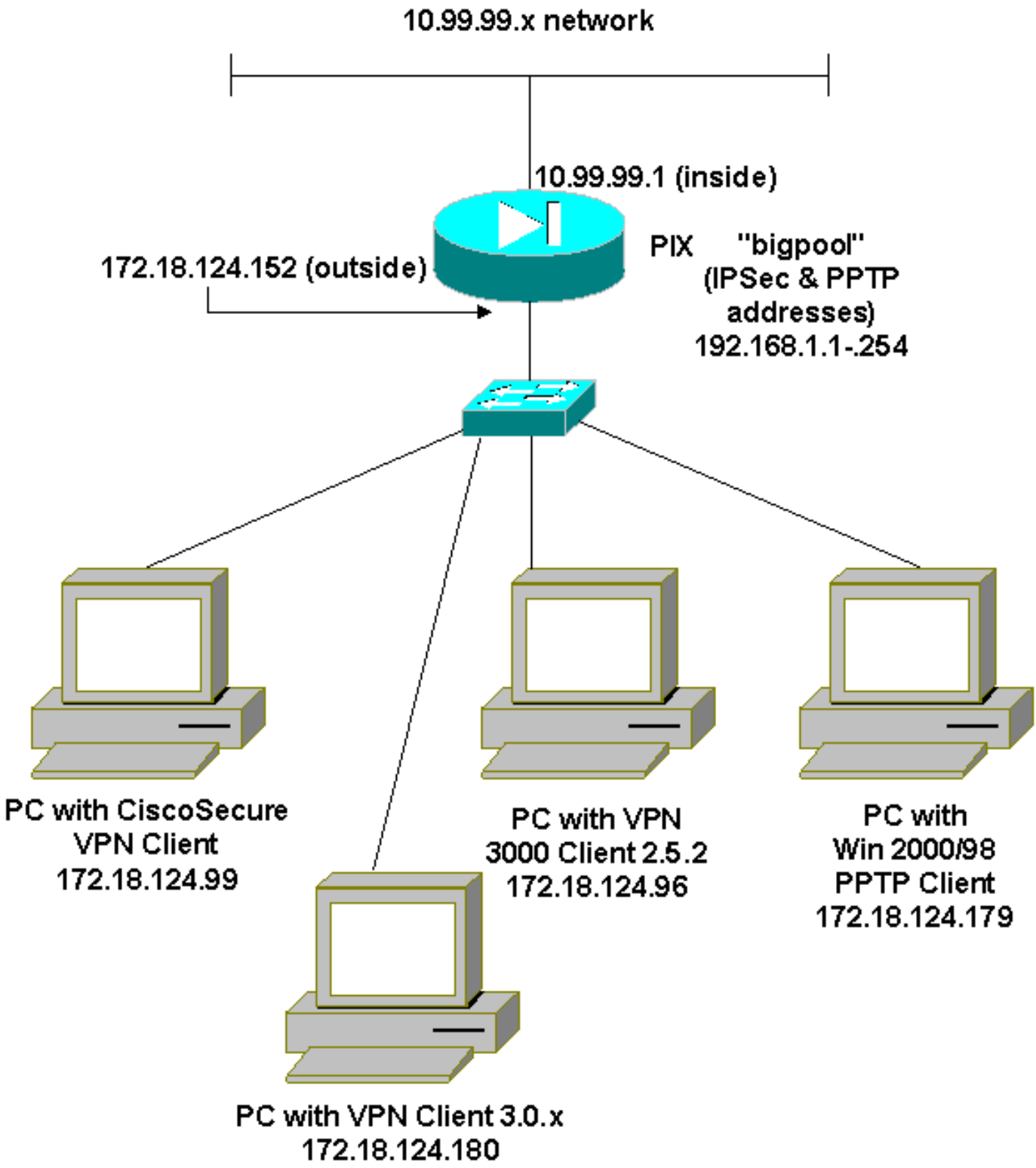
Configurar

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) 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.

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

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#
```

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

Usted puede entrar en contacto al vendedor que hace al cliente PPTP. Refiérase a cómo configurar el Cisco Secure PIX Firewall para utilizar el PPTP para la información sobre cómo configurar esto.

Verificación

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

Troubleshooting

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 de Debug antes de usar un **comando debug**.

Debug del IPSec de PIX

- **IPSec del debug crypto** — Visualiza los IPSec Negotiations de la fase 2.
- **isakmp del debug crypto** — Visualiza las negociaciones del Internet Security Association and Key Management Protocol (ISAKMP) de la fase 1.
- 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** — Mensajes de error de interfaz virtual de las visualizaciones PPTP PPP.
- **debug vpdn error** — Mensajes de error de protocolo de las visualizaciones PPTP.
- **debug vpdn packets** — Información del paquete PPTP de las visualizaciones sobre el tráfico PPTP.
- **debug vpdn events** — Información de cambio de evento de túnel de las visualizaciones PPTP.
- debug ppp uauth - Muestra los mensajes de depuración de autenticación de usuario de AAA de la interfaz virtual de PPTP PPP.

Problemas relacionados con Microsoft

- Cómo mantener las conexiones RAS activas después de terminar una sesión — cuando usted termina una sesión de un cliente del Remote Access Service de Windows (RAS), cualquier conexión RAS se desconecta automáticamente. Para seguir conectado después de que usted termine una sesión, habilite la clave del KeepRasConnections en el registro en el cliente RAS.
- No alertan al usuario al abrir una sesión con las credenciales ocultadas — los síntomas - cuando usted intenta abrir una sesión a un dominio de una estación de trabajo basada en Windows o el servidor miembro y un controlador de dominio no pueden ser localizados, no se visualiza 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 del dominio y otros problemas de la resolución de nombre — puede haber casos cuando usted experimenta los problemas de la resolución de nombre en su red TCP/IP y usted necesita utilizar los archivos de Lmhosts para resolver los nombres de NETBIOS. Este artículo discute el método correcto de crear un archivo de Lmhosts para ayudar en la resolución de nombre y la validación del dominio.

Información Relacionada

- Páginas de soporte de la Negociación IPSec/Protocolos IKE
- Referencia de Comandos PIX
- Página de Soporte de Cisco PIX 500 Series Security Appliances
- Solicitudes de Comentarios (RFC)
- Configurar el IPSec Network Security
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Soporte técnico y documentación Cisco Systems