PIX: Acceso al PDM desde una interfaz externa a través de un túnel VPN

Contenido

Introducción

Esta configuración de muestra ilustra cómo configurar un túnel VPN de LAN a LAN mediante dos firewalls PIX. PIX Device Manager (PDM) se ejecuta en el PIX remoto a través de la interfaz exterior en el lado público y cifra el tráfico en la red común y en PDM.

PDM es una herramienta de configuración basada en navegador diseñada para ayudarle a configurar, configurar y monitorear su PIX Firewall con una GUI. No necesita un amplio conocimiento de la interfaz de línea de comandos (CLI) del firewall PIX.

Prerequisites

Requirements

Este documento requiere una comprensión básica del cifrado IPsec y PDM.

Asegúrese de que todos los dispositivos utilizados en su topología cumplan los requisitos descritos en la Guía de Instalación del Hardware de Cisco PIX Firewall, Versión 6.3.

Componentes Utilizados

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

- Software Cisco PIX Firewall versión 6.3(1) y 6.3(3)
- PIX A y PIX B son Cisco PIX Firewall 515E
- PIX B utiliza PDM versión 2.1(1)**Nota:** PDM 3.0 no se ejecuta con las versiones de software PIX Firewall anteriores a la versión 6.3. PDM versión 3.0 es una única imagen que soporta solamente PIX Firewall versión 6.3.**Nota:** Las configuraciones de políticas NAT obligan a PDM 3.0 a entrar en el modo monitor. La política NAT se soporta en la versión 4.0 y posterior de PDM.**Nota:** Cuando se le solicita un nombre de usuario y una contraseña para el PIX Device Manager (PDM), la configuración predeterminada no requiere ningún nombre de usuario. Si se configuró previamente una contraseña de habilitación, introduzca dicha contraseña como la contraseña de PDM. Si no hay ninguna contraseña de habilitación, deje en blanco las entradas de nombre de usuario y contraseña y haga clic en **Aceptar** para continuar.

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

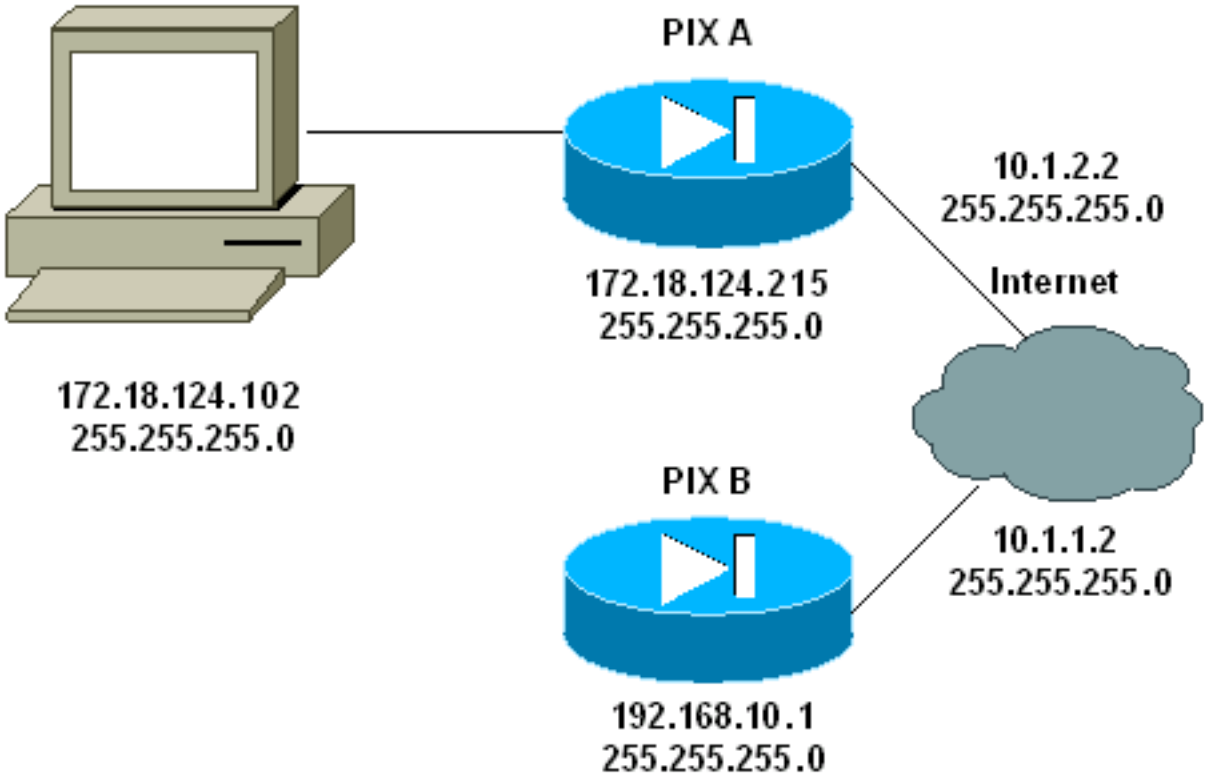
Configurar

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

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- PIX A
- PIX B

PIX A

```
PIX A

PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXA
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Allow traffic from the host PC that is going to !--
- run the PDM to the outside interface of PIX B. access-
list 101 permit ip host 172.18.124.102 host 10.1.1.2
!--- Allow traffic from the private network behind PIX A
!--- to access the private network behind PIX B. access-
list 101 permit ip 172.18.124.0 255.255.255.0
192.168.10.0 255.255.255.0
```

```
pager lines 24
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 10.1.2.2 255.255.255.0
ip address inside 172.18.124.215 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
!--- Do not use NAT !--- on traffic which matches access
control list (ACL) 101. nat (inside) 0 access-list 101
!--- Configures a default route towards the gateway
router. route outside 0.0.0.0 0.0.0.0 10.1.2.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
rpc 0:10:00 h323 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
!--- Enable the HTTP server required to run PDM. http
server enable
!--- This is the interface name and IP address of the
host or !--- network that initiates the HTTP connection.
http 172.18.124.102 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Implicitly permit any packet that came from an
IPsec !--- tunnel and bypass the checking of an
associated access-list, conduit, or !--- access-group
command statement for IPsec connections. sysopt
connection permit-ipsec
!--- Specify IPsec (phase 2) transform set. crypto ipsec
transform-set vpn esp-3des esp-md5-hmac
!--- Specify IPsec (phase 2) attributes. crypto map vpn
10 ipsec-isakmp
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 10.1.1.2
crypto map vpn 10 set transform-set vpn
crypto map vpn interface outside
!--- Specify ISAKMP (phase 1) attributes. isakmp enable
outside
isakmp key ******** address 10.1.1.2 netmask
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:24e43efa87d6ef07dfabe097b82b5b40
: end
[OK]
PIXA(config)#
```

PIX B

```
PIX B
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXB
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80P
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Allow traffic from the host PC that is going to !--
- run the PDM to the outside interface of PIX B. access-
list 101 permit ip host 10.1.1.2 host 172.18.124.102
!--- Allow traffic from the private network behind PIX A
!--- to access the private network behind PIX B. access-
list 101 permit ip 192.168.10.0 255.255.255.0
172.18.124.0 255.255.255.0
pager lines 24
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 10.1.1.2 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
!--- Assists PDM with network topology discovery by
associating an external !--- network object with an
interface. Note: The pdm location !--- command does not
control which host can launch PDM.

pdm location 172.18.124.102 255.255.255.255 outside
pdm history enable
arp timeout 14400
!--- Do not use NAT on traffic which matches ACL 101.
nat (inside) 0 access-list 101
!--- Configures a default route towards the gateway
router. route outside 0.0.0.0 0.0.0.0 10.1.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00
h323 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
!--- Enables the HTTP server required to run PDM. http
server enable
!--- This is the interface name and IP address of the
host or !--- network that initiates the HTTP connection.
http 172.18.124.102 255.255.255.255 outside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
```

```
!--- Implicitly permit any packet that came from an
IPsec !--- tunnel and bypass the checking of an
associated access-list, conduit, or !--- access-group
command statement for IPsec connections. sysopt
connection permit-ipsec
!--- Specify IPsec (phase 2) transform set. crypto ipsec
transform-set vpn esp-3des esp-md5-hmac
!--- Specify IPsec (phase 2) attributes. crypto map vpn
10 ipsec-isakmp
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 10.1.2.2
crypto map vpn 10 set transform-set vpn
crypto map vpn interface outside
isakmp enable outside
!--- Specify ISAKMP (phase 1) attributes. isakmp key
******** address 10.1.2.2 netmask 255.255.255.255
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:d5ba4da0d610d0c6140e1b781abef9d0
: end
[OK]
PIXB(config)#
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

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.

- show crypto isakmp sa/show isakmp sa —Verifica que la fase 1 establece.
- show crypto ipsec sa —Verifica que la fase 2 establece.
- show crypto engine —Muestra las estadísticas de uso del motor de criptografía que utiliza el firewall.

Resumen de Comandos

Una vez que se ponen los comandos VPN en los PIX, un túnel VPN debe establecer cuándo pasa el tráfico entre la PC PDM (172.18.124.102) y la interfaz exterior de PIX B (10.1.1.2). En este punto, el PC PDM puede ir a https://10.1.1.2 y alcanzar la interfaz PDM de PIX B a través del túnel VPN.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. Consulte Resolución de Problemas del PIX Device Manager para resolver problemas relacionados con PDM.

Ejemplo de resultado del comando debug

show crypto isakmp sa

Esta salida muestra un túnel formado entre 10.1.1.2 y 10.1.2.2.

```
PIXA#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst         src         state     pending    created
        10.1.1.2    10.1.2.2    QM_IDLE         0          1
```

show crypto ipsec sa

Esta salida muestra un túnel que pasa el tráfico entre 10.1.1.2 y 172.18.124.102.

```
PIXA#show crypto ipsec sa

interface: outside
    Crypto map tag: vpn, local addr. 10.1.2.2

   local  ident (addr/mask/prot/port): (172.18.124.102/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/0/0)
   current_peer: 10.1.1.2
>     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14472, #pkts encrypt: 14472, #pkts digest 14472
    #pkts decaps: 16931, #pkts decrypt: 16931, #pkts verify 16931
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 9, #recv errors 0

     local crypto endpt.: 10.1.2.2, remote crypto endpt.: 10.1.1.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 4acd5c2a

     inbound esp sas:
      spi: 0xcff9696a(3489229162)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4600238/15069)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4acd5c2a(1254972458)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4607562/15069)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
```

```
outbound pcp sas:
```

Información Relacionada

- Referencia de Comandos PIX
- Dispositivos de seguridad Cisco PIX de la serie 500
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems