PIX/ASA 7.2(1) y posterior: Comunicaciones de la Intra-interfaz

Contenido

Introducción

Este documento ayuda a resolver problemas comunes que ocurren cuando se habilitan las comunicaciones internas de la interfaz sobre un Adaptive Security Appliance (ASA) o PIX que ejecuta la versión 7.2(1) y posteriores del software. El Software Release 7.2(1) incluye la capacidad para rutear los datos del texto claro dentro y fuera de la misma interfaz. Ingrese el **comando intra-interface del permiso del trafico de seguridad igual** para habilitar esta característica. Este documento asume que el administrador de la red ha habilitado esta característica o planes a en el futuro. La configuración y el troubleshooting se proporcionan usando el comando line interface(cli).

Nota: Este documento se centra en los datos (unencrypted) claros que llegan y salen del ASA. Los datos encriptados no se discuten.

Para habilitar la comunicación de la intra-interfaz encendido ASA/PIX para la configuración IPSec, refiera al PIX/ASA y al cliente VPN para el Internet pública VPN en un ejemplo de configuración del palillo.

Para habilitar la comunicación de la intra-interfaz sobre el ASA para la configuración de SSL, refiera a ASA 7.2(2): (SVC) del cliente VPN SSL para el Internet pública VPN en un ejemplo de configuración del palillo.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Listas de acceso
- Ruteo
- Sistema de prevención de intrusiones (IPS) del Módulo de servicios del examen avanzado y de la Prevención-Seguridad (AIP-SSM) — el conocimiento de este módulo es solamente necesario si el módulo es instalado y operativo.
- Software Release 5.x IPS — El conocimiento del software IPS no se requiere si el AIP-SSM es parado.

Componentes Utilizados

- ASA 5510 7.2(1) y posterior
- AIP-SSM-10 que actúa el software 5.1.1 IPS

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.

Productos Relacionados

Esta configuración se puede también utilizar con las Cisco 500 Series PIX que funciona con la versión 7.2(1) y posterior.

Convenciones

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

Antecedentes

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Esta tabla muestra el ASA que comienza la configuración:

ASA
ciscoasa#**show running-config** : Saved : ASA Version 7.2(1) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! *!--- The IP addressing assigned to interfaces.* interface Ethernet0/0 nameif inside security-level 100 ip address 10.1.1.2 255.255.255.0 ! interface Ethernet0/1 nameif outside security-level 0 ip address 172.22.1.160 255.255.255.0 !

```
interface Ethernet0/2 shutdown no nameif no security-
level no ip address ! interface Management0/0 shutdown
no nameif no security-level no ip address ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive !--- Notice
that there are no access-lists. pager lines 24 logging
enable logging buffered debugging mtu inside 1500 mtu
outside 1500 no asdm history enable arp timeout 14400 !-
-- There are no network address translation (NAT) rules.
!--- The static routes are added for test purposes.
route inside 10.2.2.0 255.255.255.0 10.1.1.100 1 route
outside 172.16.10.0 255.255.255.0 172.22.1.29 1 timeout
xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:
```

Resolución de problemas

Estas secciones ilustran varios escenarios de configuración, mensajes de Syslog relacionados, y salidas del paquete-trazalíneas en relación con las comunicaciones de la intra-interfaz.

Comunicaciones de la Intra-interfaz no habilitadas

En la configuración ASA, tentativas de 172.22.1.6 del host de hacer ping el host 172.16.10.1. El host 172.22.1.6 envía un paquete de pedido de eco ICMP al default gateway (ASA). las comunicaciones de la Intra-interfaz no se han habilitado en el ASA. El ASA cae el paquete de pedido de eco. El ping de la prueba falla. El ASA se utiliza para resolver problemas el problema.

Este ejemplo muestra la salida de los mensajes de Syslog y de un paquete-trazalíneas:

- Éste es el mensaje de Syslog registrado al buffer:`ciscoasa(config)#`**`show logging`** *!--- Output is suppressed.* `%ASA-3-106014: Deny inbound icmp src outside:172.22.1.6 dst outside:172.16.10.1 (type 8, code 0)`
- Esto es el paquete-trazalíneas hecho salir:`ciscoasa(config)#`**`packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed`** `Phase: 1 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 2 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.16.10.0 255.255.255.0 outside Phase: 3 Type: ACCESS-LIST Subtype:` ***Result: DROP*** `Config:` ***Implicit Rule*** *!--- Implicit rule refers to configuration rules not configured !--- by the user. By default, intra-interface communication is not permitted. !--- In this example, the user has not enabled intra-interface communications !--- and therefore the traffic is implicitly denied.* `Additional Information: Forward Flow based lookup yields rule: in id=0x3bd8480, priority=111, domain=permit, deny=true hits=0, user_data=0x0, cs_id=0x0, flags=0x4000, protocol=0 src ip=0.0.0.0, mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0 Result:`

```
input-interface: outside input-status: up input-line-status: up output-interface: outside
output-status: up output-line-status: up Action: drop Drop-reason: (acl-drop) Flow is denied
by configured rule
```

El equivalente de los comandos CLI en el ASDM se muestra en estas figuras:

Paso 1:

Paso 2:

La salida del paquete-trazalíneas con el **comando intra-interface del permiso del trafico de seguridad igual** inhabilitado.

`La regla implícita de la` caída de resultados del paquete-trazalíneas… sugiere que una configuración de la configuración predeterminada esté bloqueando el tráfico. El administrador necesita marcar la configuración corriente para asegurarse que las comunicaciones de la intra-interfaz está habilitada. En este caso, la configuración ASA necesita las comunicaciones de la intra-interfaz ser habilitada (intra-**interfaz del permiso del trafico de seguridad igual**).

```
ciscoasa#show running-config !--- Output is suppressed. interface Ethernet5 shutdown no nameif
no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive same-
security-traffic permit intra-interface !--- When intra-interface communications are enabled,
the line !--- highlighted in bold font appears in the configuration. The configuration line !---
appears after the interface configuration and before !--- any access-list configurations.
access-list... access-list...
```

Comunicaciones de la Intra-interfaz habilitadas

las comunicaciones de la Intra-interfaz ahora se habilitan. Agregan al **comando intra-interface del permiso del trafico de seguridad igual a la** configuración previa. Tentativas de 172.22.1.6 del host de hacer ping el host 172.16.10.1. El host 172.22.1.6 envía un paquete de pedido de eco ICMP al default gateway (ASA). Contestaciones acertadas de los expedientes de 172.22.1.6 del host de 172.16.10.1. El ASA pasa el tráfico ICMP con éxito.

Estos ejemplos muestran las salidas del mensaje de Syslog y del paquete-trazalíneas ASA:

- Éstos son los mensajes de Syslog registrados al buffer:`ciscoasa#show logging !--- Output is suppressed. %PIX-7-609001: Built local-host outside:172.22.1.6 %PIX-7-609001: Built local-host outside:172.16.10.1 %PIX-6-302020: Built ICMP connection for faddr 172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-6-302021: Teardown ICMP connection for faddr 172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-7-609002: Teardown local-host outside:172.22.1.6 duration 0:00:04 %PIX-7-609002: Teardown local-host outside:172.16.10.1 duration 0:00:04`
- Esto es el paquete-trazalíneas hecho salir:`ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 Phase: 1 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 2 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.16.10.0 255.255.255.0 outside Phase: 3 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: Phase: 4 (Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 5 Type: INSPECT Subtype: np-inspect Result: ALLOW Config: Additional Information: Phase: 6 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 23, packet dispatched to next module Phase: 7 Type: ROUTE-LOOKUP Subtype: output and adjacency Result: ALLOW Config: Additional Information: found next-hop 172.22.1.29 using egress ifc outside adjacency Active next-hop mac address 0030.a377.f854 hits 0 Result: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up Action: allow` El equivalente de los comandos CLI en el ASDM se muestra en estas figuras:**Paso 1:Paso 2:**La salida del paquete-trazalíneas con el **comando intra-interface del permiso del**

trafico de seguridad igual habilitado.**Nota:** No se aplica ninguna lista de acceso a la interfaz exterior. En la configuración de muestra, la interfaz exterior se asigna el nivel de seguridad 0. por abandono, el Firewall no permite el tráfico de una interfaz de seguridad baja a una interfaz de la gran seguridad. Esto pudo llevar a los administradores a creer que el tráfico de la intra-interfaz no está permitido en la interfaz del exterior (Seguridad baja) sin el permiso de una lista de acceso. Sin embargo, los mismos pasos del tráfico de la interfaz libremente cuando no se aplica ninguna lista de acceso a la interfaz.

Intra-interfaz habilitada y tráfico pasajero al AIP-SSM para el examen

el tráfico de la Intra-interfaz se puede pasar al AIP-SSM para el examen. Esta sección asume que el administrador ha configurado el ASA para remitir el tráfico al AIP-SSM y el administrador sabe configurar el software IPS 5.x.

En este momento la configuración ASA contiene la configuración de muestra anterior, se habilitan las comunicaciones de la intra-interfaz, y todo el (cualquier) tráfico se remite al AIP-SSM. La firma 2004 IPS se modifica para caer el tráfico del pedido de eco. Tentativas de 172.22.1.6 del host de hacer ping el host 172.16.10.1. El host 172.22.1.6 envía un paquete de pedido de eco ICMP al default gateway (ASA). El ASA adelante el paquete de pedido de eco al AIP-SSM para el examen. El AIP-SSM cae el paquete de datos por la configuración IPS.

Estos ejemplos muestran el mensaje de Syslog y el paquete-trazalíneas ASA hechos salir:

- Éste es el mensaje de Syslog registrado al buffer:`ciscoasa(config)#`**`show logging`** *`!--- Output is suppressed.`* `%ASA-4-420002: IPS requested to drop ICMP packet from outside:172.22.1.6/2048 to outside:172.16.10.1/0` *`!--- ASA syslog message records the IPS request !--- to drop the ICMP traffic.`*
- Esto es el paquete-trazalíneas hecho salir:`ciscoasa#`**`packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1`** `Phase: 1 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 2 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.16.10.0 255.255.255.0 outside Phase: 3 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: Phase: 4 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 5 Type: INSPECT Subtype: np-inspect Result: ALLOW Config: Additional Information: Phase: 6 Type: IDS Subtype:` ***`Result: ALLOW`*** `Config:` ***`class-map traffic_for_ips match any policy-map global_policy class traffic_for_ips ips inline fail-open service-policy global_policy global`*** *`!--- The packet-tracer recognizes that traffic is to be sent to the AIP-SSM. !--- The packet-tracer does not have knowledge of how the !--- IPS software handles the traffic.`* `Additional Information: Phase: 7 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 15, packet dispatched to next module Result: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up` ***`Action: allow`*** *`!--- From the packet-tracer perspective the traffic is permitted. !--- The packet-tracer does not interact with the IPS configuration. !--- The packet-tracer indicates traffic is allowed even though the IPS !--- might prevent inspected traffic from passing.`*

Es importante observar que los administradores deben utilizar tantas herramientas de Troubleshooting como sea posible cuando investigan un problema. Este ejemplo muestra cómo dos diversas herramientas de Troubleshooting pueden pintar diversas imágenes. Ambas herramientas juntas cuentan una historia completa. La directiva de configuración ASA permite el tráfico pero la configuración IPS no hace.

Intra-interfaz habilitada y Listas de acceso aplicadas a una interfaz

Esta sección utiliza la configuración de muestra original en este documento, las comunicaciones

de la intra-interfaz habilitadas, y una lista de acceso aplicada a la interfaz probada. Estas líneas se agregan a la configuración. La lista de acceso se piensa para ser una representación simple de qué se pudo configurar en un Firewall de la producción.

```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-group outside_acl in interface outside !--- Production firewalls also have NAT rules configured. !--- This lab tests intra-interface communications. !--- NAT rules are not required.
```

Tentativas de 172.22.1.6 del host de hacer ping el host 172.16.10.1. El host 172.22.1.6 envía un paquete de pedido de eco ICMP al default gateway (ASA). El ASA cae el paquete de pedido de eco por las reglas de la lista de acceso. El ping de la prueba de 172.22.1.6 del host falla.

Estos ejemplos muestran el mensaje de Syslog y el paquete-trazalíneas ASA hechos salir:

- Éste es el mensaje de Syslog registrado al buffer:`ciscoasa(config)#show logging !--- Output is suppressed. %ASA-4-106023: Deny icmp src outside:172.22.1.6 dst outside:172.16.10.1 (type 8, code 0) by access-group "outside_acl" [0xc36b9c78, 0x0]`
- Esto es el paquete-trazalíneas hecho salir:`ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed Phase: 1 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 2 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.16.10.0 255.255.255.0 outside Phase: 3 Type: ACCESS-LIST Subtype: Result: DROP Config: Implicit Rule !--- The implicit deny all at the end of an access-list prevents !--- intra-interface traffic from passing. Additional Information: Forward Flow based lookup yields rule: in id=0x264f010, priority=11, domain=permit, deny=true hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0 src ip=0.0.0.0, mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0 Result: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up Action: drop Drop-reason: (acl-drop) Flow is denied by configured rule`

Refiera al paquete-trazalíneas para más información sobre el comando del paquete-**trazalíneas**.

Nota: En el evento que la lista de acceso aplicada a la interfaz incluye un enunciado de negación, la salida del paquete-trazalíneas cambia. Por ejemplo:

```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any ciscoasa(config)#access-group outside_acl in interface outside ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed !--- Output is suppressed. Phase: 3 Type: ACCESS-LIST Subtype: log Result: DROP Config: access-group outside_acl in interface outside access-list outside_acl extended deny ip any any Additional Information: Forward Flow based lookup yields rule:
```

El equivalente de los comandos CLI antedichos en el ASDM se muestra en estas figuras:

Paso 1:

Paso 2:

La salida del paquete-trazalíneas con el **comando intra-interface del permiso del trafico de seguridad igual** habilitado y el **comando deny ip any any extendido outside_acl de la lista de acceso** configurado para negar los paquetes.

Si las comunicaciones de la intra-interfaz se desean en una interfaz particular y las listas de acceso se aplican a la misma interfaz, las reglas de la lista de acceso deben permitir el tráfico de la intra-interfaz. Con el uso de los ejemplos en esta sección, la lista de acceso necesita ser escrita como:

```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
```

```
255.255.255.0 !--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the ASA. !--- 172.16.10.0 255.255.255.0 represents any network that !--- 172.22.1.0/24 needs to access. ciscoasa(config)#access-list outside_acl deny ip any any ciscoasa(config)#access-group outside_acl in interface outside
```

El equivalente de los comandos CLI antedichos en el ASDM se muestra en estas figuras:

Paso 1:

Paso 2:

La salida del paquete-trazalíneas con el **comando intra-interface del permiso del trafico de seguridad igual** habilitado y el **comando deny ip any any extendido outside_acl de la lista de acceso** configurado en lo mismo interfaz donde se desea el tráfico de la intra-interfaz.

Consulte access-list extended y access-group para obtener más información sobre los comandos **access-list** y **access-group** .

Intra-interfaz habilitada con los parásitos atmosféricos y el NAT

Esta sección explica un escenario donde un usuario interior está intentando acceder al servidor de Web interno con su dirección pública.

En este caso, el cliente en 192.168.100.2 quiere utilizar a la dirección pública del servidor WWW (por ejemplo, 172.20.1.10). El servidor DNS externo en 172.22.1.161 proporcionan los servicios DNS para el cliente. Porque el servidor DNS está situado en otra red pública, no conoce el IP Address privado del servidor WWW. En lugar, el servidor DNS conoce el direccionamiento asociado servidor WWW de 172.20.1.10.

Aquí este tráfico de la interfaz interior tiene que ser traducido y ser reencaminado a través de la interfaz interior para alcanzar al servidor WWW. Esto se llama hairpinning. Esto se puede realizar con estos comandos:

```
same-security-traffic permit intra-interface global (inside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0 static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255
```

Para los detalles de la configuración completos y más información sobre el hairpinning, refiera al hairpinning con la comunicación de la Intra-interfaz.

Lista de acceso con visión de futuro

No todas las políticas de acceso del Firewall son lo mismo. Algunas políticas de acceso son más específicas que otras. En la intra-interfaz del evento se habilitan las comunicaciones y el Firewall no tiene una lista de acceso aplicada a todas las interfaces, él pudo valer el agregar de una lista de acceso cuando se habilitan las comunicaciones de la intra-interfaz. La lista de acceso aplicada necesita permitir las comunicaciones de la intra-interfaz así como mantener otros requisitos de la política de acceso.

Este ejemplo ilustra este punto. El ASA conecta una red privada (interfaz interior) con Internet (interfaz exterior). La interfaz interior ASA no tiene una lista de acceso aplicada. Por abandono, todo el tráfico IP se permite del interior al exterior. La sugerencia es agregar una lista de acceso que mire algo similar hecha salir:

```
access-list inside_acl permit ip <locally connected network> <all other internal networks>
access-list inside_acl permit ip any any access-group inside_acl in interface inside
```

Este conjunto de las listas de acceso continúa permitiendo todo el tráfico IP. La línea específica de la lista de acceso para las comunicaciones de la intra-interfaz recuerda a los administradores que las comunicaciones de la intra-interfaz se deben permitir por una lista de acceso aplicada.

Información Relacionada

- Referencia de comandos del dispositivo del Cisco Security, versión 7.2
- Mensajes del registro del sistema del dispositivo del Cisco Security, versión 7.2
- Cisco PIX Firewall Software
- ASA: Envíe el tráfico de la red del ASA al ejemplo de configuración AIP SS
- Soporte de producto para dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Soporte Técnico y Documentación - Cisco Systems