PIX/ASA 7.x y posteriores: Bloquee el tráfico del peer a peer (P2P) y de la Mensajería inmediata (IM) usando el ejemplo de la configuración MPF

Contenido

Introducción

Este documento describe cómo configurar el PIX/ASA de los dispositivos del Cisco Security usando el Marco de políticas modular (MPF) para bloquear el peer a peer (P2P) y la Mensajería inmediata (IM), por ejemplo MSN Messenger y Yahoo Messenger, tráfico de la red interna a Internet. También, este documento proporciona la información sobre cómo configurar el PIX/ASA para permitir que los dos host utilicen las aplicaciones IM mientras que el resto de los host sigue bloqueado.

Nota: El ASA puede bloquear las aplicaciones del tipo P2P solamente si el tráfico P2P está siendo tunneled con el HTTP. También, el ASA puede caer el tráfico P2P si es tunneled con el HTTP.

prerrequisitos

Requisitos

Este documento asume que el dispositivo del Cisco Security está configurado y trabaja correctamente.

Componentes Utilizados

La información en este documento se basa en el dispositivo de seguridad adaptante de las Cisco 5500 Series (ASA) esa versión de software 7.0 de los funcionamientos y posterior.

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 el firewall PIX de las Cisco 500 Series que funciona con la versión de software 7.0 y posterior.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Descripción modular del Marco de políticas

El MPF proporciona un constante y una manera flexible configurar las características del dispositivo de seguridad. Por ejemplo, usted puede utilizar el MPF para crear una configuración del descanso que sea específica a una aplicación TCP determinada, en comparación con una que se aplique a todas las aplicaciones TCP.

El MPF soporta estas características:

- Normalización TCP, TCP y límites y descansos de la conexión UDP, y distribución aleatoria del número de secuencia TCP
- CSC
- Inspección de la aplicación
- IPS
- Políticas de entrada de QoS
- Policing de la salida de QoS
- Prioridad de Calidad de servicio (QoS) cola

La configuración del MPF consiste en cuatro tareas:

1. Identifique la capa 3 y el tráfico 4 al cual usted quiere aplicar las acciones. Refiera a identificar el tráfico usando un mapa de la clase de la capa 3/4 para más información.
2. (Inspección de la aplicación solamente) defina las acciones especiales para el tráfico de la Inspección de la aplicación. Refiera a configurar las acciones especiales para las Inspecciones de la aplicación para más información.
3. Aplique las acciones a la capa 3 y el tráfico 4. Refiera a definir las acciones usando una correspondencia de políticas de la capa 3/4 para más información.
4. Active las acciones en una interfaz. Refiera a aplicar una directiva de la capa 3/4 a una interfaz usando una política de servicio para más información.

Configure el P2P e IM bloqueo del tráfico

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

En este documento, se utiliza esta configuración de red:

PIX/ASA 7.0 y configuración 7.1

Bloquee el P2P y IM configuración del tráfico para el PIX/ASA 7.0 y 7.1

```
CiscoASA#show run : Saved : ASA Version 7.1(1) !
hostname CiscoASA enable password 8Ry2YjIyt7RRXU24
encrypted names ! !--- Output Suppressed http-map
inbound_http content-length min 100 max 2000 action
reset log content-type-verification match-req-rsp action
reset log max-header-length request 100 action reset log
max-uri-length 100 action reset log port-misuse p2p
action drop port-misuse im action drop port-misuse
default action allow !--- The http-map "inbound_http"
inspects the http traffic !--- as per various parameters
such as content length, header length, !--- url-length
as well as matches the P2P & IM traffic and drops them.
! !--- Output Suppressed ! class-map inspection_default
match default-inspection-traffic class-map http-port
match port tcp eq www !--- The class map "http-port"
matches !--- the http traffic which uses the port 80. !
! policy-map global_policy class inspection_default
inspect dns maximum-length 512 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
policy-map inbound_policy class http-port inspect http
inbound_http !--- The policy map "inbound_policy"
matches !--- the http traffic using the class map "http-
port" !--- and drops the IM traffic as per http map !---
"inbound_http" inspection. ! service-policy
global_policy global service-policy inbound_policy
interface inside !--- Apply the policy map
"inbound_policy" !--- to the inside interface.
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
CiscoASA#
```

Refiera a configurar un mapa HTTP para la sección de control adicional del examen de la guía del comando line configuration del dispositivo del Cisco Security para más información sobre el **comando map HTTP** y los diversos parámetros asociados a ella.

Configuración del PIX/ASA 7.2 y posterior

Nota: El comando del HTTP-**mapa** se desaprueba de la versión de software 7.2 y posterior. Por lo

tanto, usted necesita utilizar el **tipo del directiva-mapa examina el** comando **im** para bloquear el tráfico IM.

Bloquee el P2P y IM configuración del tráfico para el PIX/ASA 7.2 y posterior

```
CiscoASA#show running-config : Saved : ASA Version
8.0(2) ! hostname pixfirewall enable password
8Ry2YjIyt7RRXU24 encrypted names !--- Output Suppressed
class-map inspection_default match default-inspection-
traffic class-map imblock match any !--- The class map
"imblock" matches !--- all kinds of traffic. class-map
P2P match port tcp eq www !--- The class map "P2P"
matches !--- http traffic. ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map type inspect im impolicy parameters match
protocol msn-im yahoo-im drop-connection !--- The policy
map "impolicy" drops the IM !--- traffic such as msn-im
and yahoo-im . policy-map type inspect http P2P_HTTP
parameters match request uri regex _default_gator drop-
connection log match request uri regex _default_x-kazaa-
network drop-connection log !--- The policy map
"P2P_HTTP" drops the P2P !--- traffic that matches the
some built-in reg exp's. policy-map IM_P2P class imblock
inspect im impolicy class P2P inspect http P2P_HTTP !---
The policy map "IM_P2P" drops the !--- IM traffic
matched by the class map "imblock" as well as P2P
traffic matched by class map "P2P". 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 service-policy IM_P2P
interface inside !--- Apply the policy map "IM_P2P" !---
to the inside interface. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
CiscoASA#
```

Lista de expresiones normales incorporadas

```
regex _default_GoToMyPC-tunnel "machinekey"
regex _default_GoToMyPC-tunnel_2 "[/\\]erc[/\\]Poll"
regex _default_yahoo-messenger "YMSG"
regex _default_httport-tunnel "photo[.]exectech[-
]va[.]com"
regex _default_gnu-http-tunnel_uri "[/\\]index[.]html"
regex _default_firethru-tunnel_1 "firethru[.]com"
regex _default_gator "Gator"
regex _default_firethru-tunnel_2 "[/\\]cgi[-
]bin[/\\]proxy"
regex _default_shoutcast-tunneling-protocol "1"
regex _default_http-tunnel "[/\\]HT_PortLog.aspx"
regex _default_x-kazaa-network "[xX]-
[kK][aA][zZ][aA][aA]-[nN][eE][tT][wW][oO][rR][kK]"
regex _default_msn-messenger
"[Aa][Pp][Pp][Ll][Ii][Cc][Aa][Tt][Ii][Oo][Nn][/\\][Xx][-
][Mm][Ss][Nn][-]
[Mm][Ee][Ss][Ss][Ee][Nn][Gg][Ee][Rr]"
regex _default_aim-messenger
"[Hh][Tt][Tt][Pp][.][Pp][Rr][Oo][Xx][Yy][.][Ii][Cc][Qq][
.][Cc][Oo][Mm]"
regex _default_gnu-http-tunnel_arg "crap"
regex _default_icy-metadata "[iI][cC][yY]-
```

```
[mM][eE][tT][aA][dD][aA][tT][aA]"
regex _default_windows-media-player-tunnel "NSPlayer"
```

PIX/ASA 7.2 y posterior: Permita que los dos host utilicen el tráfico IM

Esta sección utiliza esta configuración de red:

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Éstos son los direccionamientos del RFC 1918, que se han utilizado en un ambiente de laboratorio.

Si usted quiere permitir el tráfico IM del número específico de los host, después usted necesita completar esta configuración como se muestra. En este ejemplo, los dos host 10.1.1.5 y 10.1.1.10 de la red interna se permiten utilizar las aplicaciones IM tales como MSN Messenger y Yahoo Messenger. Sin embargo, el tráfico IM de otros host todavía no se permite.

IM configuración del tráfico para el PIX/ASA 7.2 y posterior para permitir dos host

```
CiscoASA#show running-config : Saved : ASA Version
8.0(2) ! hostname pixfirewall enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! interface Ethernet1 nameif outside
security-level 0 ip address 192.168.1.1 255.255.255.0 !
!--- Output Suppressed passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive access-list 101 extended deny ip host
10.1.1.5 any access-list 101 extended deny ip host
10.1.1.10 any access-list 101 extended permit ip any any
!--- The ACL statement 101 is meant for deny the IP !---
traffic from the hosts 10.1.1.5 and 10.1.1.10 !---
whereas it allows the rest of the hosts. pager lines 24
mtu inside 1500 mtu outside 1500 no failover icmp
unreachable rate-limit 1 burst-size 1 no asdm history
enable arp timeout 14400 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 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect timeout uauth
0:05:00 absolute dynamic-access-policy-record
DfltAccessPolicy no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart no crypto isakmp nat-traversal
telnet timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map type inspect im match-all im-
traffic match protocol msn-im yahoo-im !--- The class
map "im-traffic" matches all the IM traffic !--- such as
msn-im and yahoo-im. class-map im_inspection match
access-list 101 !--- The class map "im_inspection"
matches the access list !--- number 101. 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 policy-map type inspect im im-policy
parameters class im-traffic drop-connection log !--- The
```

```
policy map "im-policy" drops and logs the !--- IM
traffic such as msn-im and yahoo-im. policy-map impol
class im_inspection inspect im im-policy !--- The policy
map "impol" inspects the IM traffic !--- as per traffic
matched by the class map "im_inspection". !--- So, it
allows the IM traffic from the host 10.1.1.5 !--- and
10.1.1.10 whereas it blocks from rest. ! service-policy
global_policy global service-policy impol interface
inside !--- Apply the policy map "impol" to the inside
!--- interface. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

Verificación

Use esta sección para confirmar que su configuración funciona 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.

- **muestre el HTTP-mapa de los ejecutar-config** — Muestra las correspondencias HTTP se han configurado que.`CiscoASA#show running-config http-map http-policy ! http-map http-policy content-length min 100 max 2000 action reset log content-type-verification match-req-rsp reset log max-header-length request bytes 100 action log reset max-uri-length 100 action reset log !`
- **muestre el directiva-mapa de los ejecutar-config** — Visualiza todas las configuraciones de correspondencia de políticas así como la configuración de correspondencia de políticas predeterminada.`CiscoASA#show running-config policy-map ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map type inspect im impolicy parameters match protocol msn-im yahoo-im drop-connection policy-map imdrop class imblock inspect im impolicy 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` Usted puede también utilizar las opciones en este comando como se muestra aquí:
  `show running-config [all] policy-map [policy_map_name | type inspect [protocol]]`
  `CiscoASA#show running-config policy-map type inspect im ! policy-map type inspect im impolicy parameters match protocol msn-im yahoo-im drop-connection !`
- **muestre el clase-mapa de los ejecutar-config** — Visualiza la información sobre la configuración de asignación de la clase.`CiscoASA#show running-config class-map ! class-map inspection_default match default-inspection-traffic class-map imblock match any`
- **muestre la servicio-directiva de los ejecutar-config** — Visualiza todas las configuraciones de la política de servicio actualmente que se ejecutan.`CiscoASA#show running-config service-policy service-policy global_policy global service-policy imdrop interface outside`
- **muestre la lista de acceso de los ejecutar-config** — Visualiza la configuración de la lista de acceso que se está ejecutando en el dispositivo de seguridad.`CiscoASA#show running-config access-list access-list 101 extended deny ip host 10.1.1.5 any access-list 101 extended deny ip host 10.1.1.10 any access-list 101 extended permit ip any any`

Troubleshooting

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

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando**

debug.

- **debug im** — Muestra los mensajes del debug para IM el tráfico.
- **servicio-directiva de la demostración** — Visualiza las políticas de servicio configuradas.`CiscoASA#`**`show service-policy interface outside`** `Interface outside: Service-policy: imdrop Class-map: imblock Inspect: im impolicy, packet 0, drop 0, reset-drop 0`
- **lista de acceso de la demostración** — Visualiza los contadores para una lista de acceso.`CiscoASA#`**`show access-list`** `access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300 access-list 101; 3 elements access-list 101 line 1 extended deny ip host 10.1.1.5 any (hitcnt=0) 0x7ef4dfbc access-list 101 line 2 extended deny ip host 10.1.1.10 any (hitcnt=0) 0x32a50197 access-list 101 line 3 extended permit ip any any (hitcnt=0) 0x28676dfa`

Información Relacionada

- Página de soporte de las Cisco 5500 Series ASA
- Página de Soporte de Cisco PIX 500 Series Security Appliances
- Soporte Técnico y Documentación - Cisco Systems