PIX/ASA 7.x y posteriores: Ejemplo de Configuración de Bloqueo del Tráfico de Peer a Peer (P2P) y Mensajería Instantánea (IM) con MPF

Contenido

Introducción

Este documento describe cómo configurar los Cisco Security Appliances PIX/ASA mediante el marco de políticas modular (MPF) para bloquear el tráfico de igual a igual (P2P) y mensajería instantánea (IM), como MSN Messenger y Yahoo Messenger, desde la red interna a Internet. Además, este documento proporciona información sobre cómo configurar el PIX/ASA para permitir que los dos hosts utilicen aplicaciones de IM mientras el resto de los hosts permanezcan bloqueados.

Nota: El ASA puede bloquear las aplicaciones de tipo P2P solamente si el tráfico P2P se tuneliza a través de HTTP. Además, ASA puede descartar el tráfico P2P si se tuneliza a través de HTTP.

Prerequisites

Requirements

Este documento asume que Cisco Security Appliance está configurado y funciona correctamente.

Componentes Utilizados

La información de este documento se basa en el dispositivo de seguridad adaptable (ASA) de la serie 5500 de Cisco que ejecuta la versión de software 7.0 y posteriores.

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.

Productos Relacionados

Esta configuración también se puede utilizar con el firewall PIX de la serie 500 de Cisco que ejecuta la versión de software 7.0 y posterior.

Convenciones

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

Descripción general del marco de políticas modular

MPF proporciona una forma coherente y flexible de configurar las funciones de los dispositivos de seguridad. Por ejemplo, puede utilizar MPF para crear una configuración de tiempo de espera específica de una aplicación TCP determinada, en lugar de una que se aplique a todas las aplicaciones TCP.

MPF admite estas funciones:

- Normalización de TCP, límites y tiempos de espera de conexión TCP y UDP, y aleatorización del número de secuencia TCP
- CSC
- Inspección de Aplicaciones
- IPS
- Regulación de entrada de QoS
- Regulación de salida de QoS
- cola de prioridad de QoS

La configuración de MPF consta de cuatro tareas:

1. Identifique el tráfico de Capa 3 y 4 al que desea aplicar acciones. Refiérase a Identificación del Tráfico Usando un Mapa de Clase de Capa 3/4 para obtener más información.
2. (Solo inspección de aplicaciones) Defina acciones especiales para el tráfico de inspección de aplicaciones. Consulte Configuración de Acciones Especiales para Inspecciones de Aplicaciones para obtener más información.
3. Aplique acciones al tráfico de Capa 3 y 4. Consulte Definición de Acciones con un Policy Map de Capa 3/4 para obtener más información.
4. Active las acciones en una interfaz. Consulte Aplicación de una Política de Capa 3/4 a una Interfaz Usando una Política de Servicio para obtener más información.

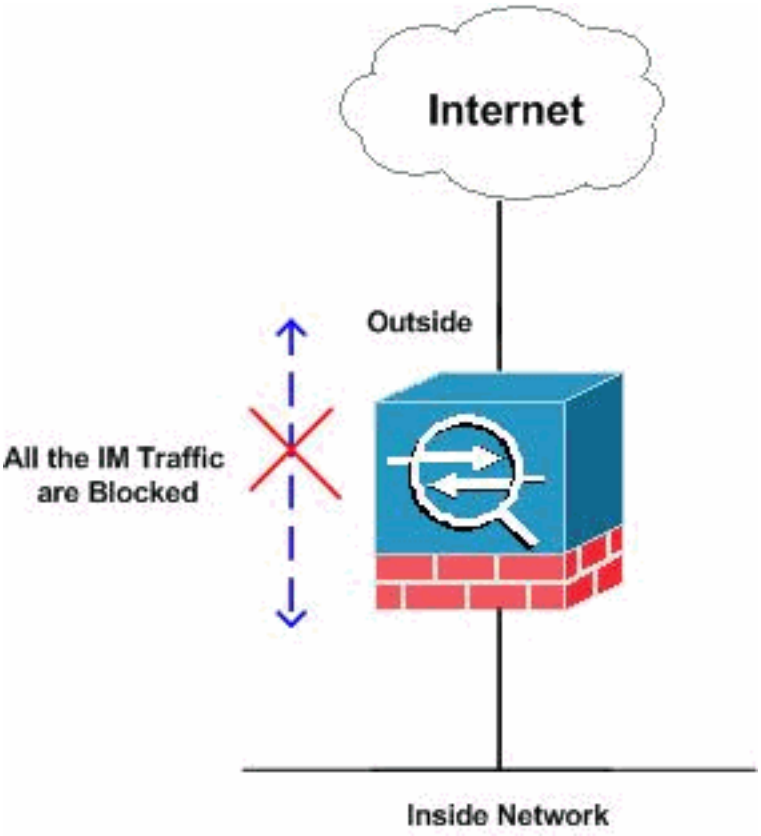
Configuración del Bloqueo de Tráfico P2P e IM

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:



Configuración de PIX/ASA 7.0 y 7.1

Bloquee la configuración del tráfico P2P y IM para 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#
```

Consulte la sección Configuración de un Mapa HTTP para Control de Inspección Adicional de la Guía de Configuración de Línea de Comandos de Dispositivos de Seguridad de Cisco para obtener más información sobre el comando **http map** y varios parámetros asociados con él.

Configuración de PIX/ASA 7.2 y posteriores

Nota: El comando **http-map** está desaprobado de la versión de software 7.2 y posteriores. Por lo tanto, debe utilizar el comando **policy-map type inspect im** para bloquear el tráfico de IM.

Bloquee la configuración del tráfico P2P e IM para PIX/ASA 7.2 y versiones posteriores

```
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#
```

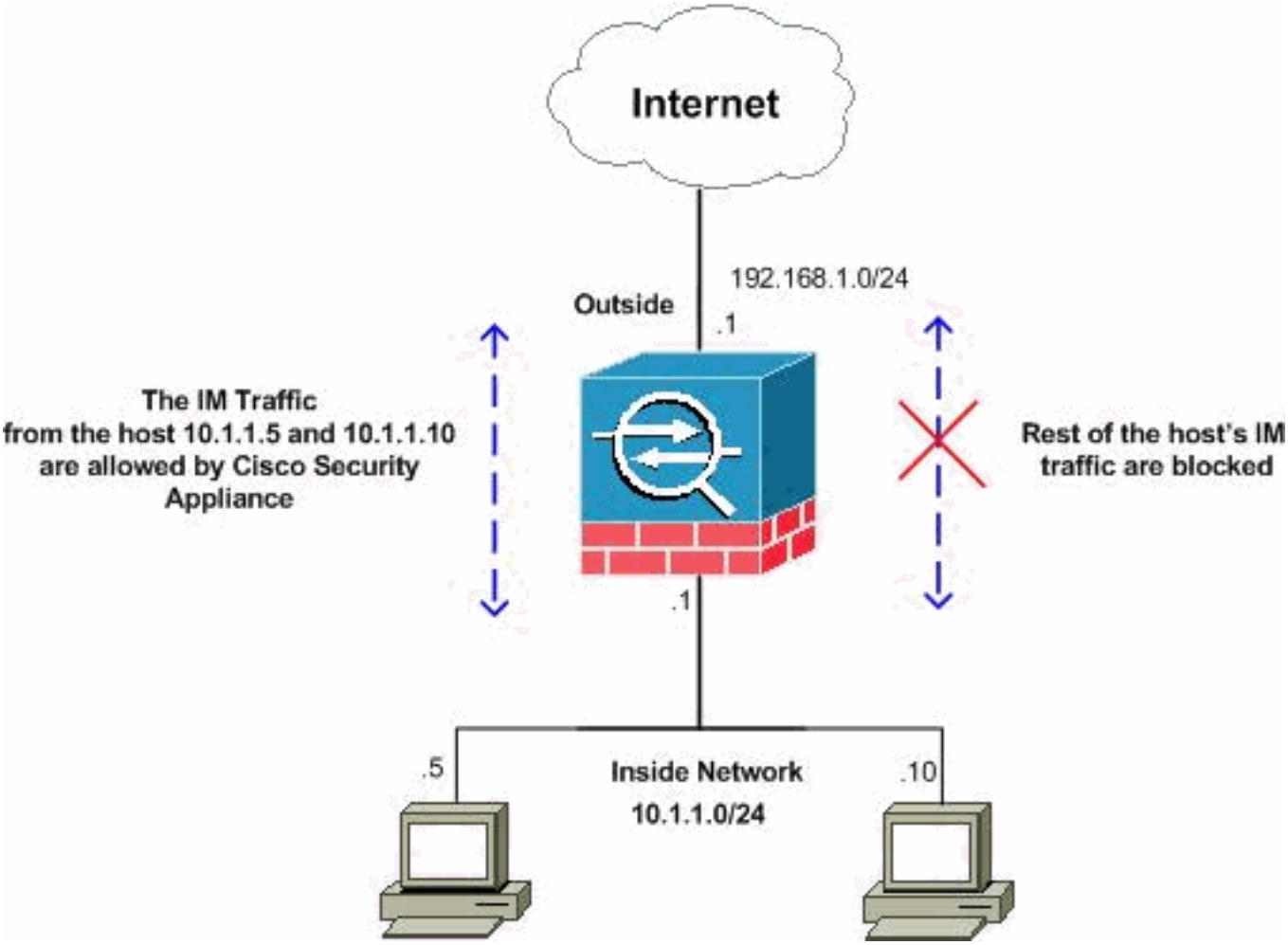
Lista de expresiones regulares integradas

```
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 posteriores: Permitir que los dos hosts utilicen el tráfico de IM

Esta sección utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Estas son direcciones RFC 1918, que se han utilizado en un entorno de laboratorio.

Si desea permitir el tráfico de IM desde el número específico de los hosts, debe completar esta configuración como se muestra. En este ejemplo, los dos hosts 10.1.1.5 y 10.1.1.10 de la red interna pueden utilizar las aplicaciones de mensajería instantánea como MSN Messenger y Yahoo Messenger. Sin embargo, el tráfico de IM de otros hosts todavía no está permitido.

Configuración del Tráfico de IM para PIX/ASA 7.2 y

posteriores para Permitir Dos Hosts

```
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.

- **show running-config http-map**: muestra los mapas HTTP configurados.
```
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
!
```
- **show running-config policy-map**: muestra todas las configuraciones de policy-map así como la configuración predeterminada de policy-map.
```
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
```

También puede utilizar las opciones de 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
!
```

- **show running-config class-map**—Muestra la información sobre la configuración del mapa de clase.

```
CiscoASA#show running-config class-map
!
class-map inspection_default
 match default-inspection-traffic
class-map imblock
 match any
```

- **show running-config service-policy**: muestra todas las configuraciones de política de servicio que se están ejecutando actualmente.

```
CiscoASA#show running-config service-policy
service-policy global_policy global
service-policy imdrop interface outside
```

- **show running-config access-list**: muestra 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
```

Troubleshoot

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

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

- **debug im**: muestra los mensajes de depuración para el tráfico de IM.
- **show service-policy**: muestra 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
```

- **show access-list**: muestra los contadores de 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 Cisco ASA serie 5500
- Página de Soporte de Cisco PIX 500 Series Security Appliances
- Soporte Técnico y Documentación - Cisco Systems