PIX/ASA 7.x e mais tarde: Obstrua o tráfego peer-to-peer (P2P) e das mensagens instantâneas (IM) usando o exemplo da configuração MPF

Índice

Introdução

Este documento descreve como configurar os dispositivos PIX/ASA do Cisco Security usando a estrutura de política modular (MPF) a fim obstruir o peer-to-peer (P2P) e mensagens instantâneas (IM), como MSN Messenger e Yahoo Messenger, tráfego da rede interna ao Internet. Também, este documento fornece a informação em como configurar o PIX/ASA a fim permitir que os dois anfitriões usem os aplicativos IM quando o resto dos anfitriões permanecer obstruído.

Nota: O ASA pode obstruir o tipo aplicativos P2P somente se o tráfego P2P está sendo escavado um túnel com o HTTP. Também, o ASA pode deixar cair o tráfego P2P se é escavado um túnel com o HTTP.

Pré-requisitos

Requisitos

Este documento supõe que o dispositivo do Cisco Security está configurado e trabalha

corretamente.

Componentes Utilizados

A informação neste documento é baseada na ferramenta de segurança adaptável do Cisco 5500 Series (ASA) essa versão de software 7.0 das corridas e mais atrasado.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração pode igualmente ser usada com o PIX Firewall do Cisco 500 Series que executa a versão de software 7.0 e mais atrasado.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Vista geral modular da estrutura de política

O MPF fornece um consistente e uma maneira flexível para configurar características da ferramenta de segurança. Por exemplo, você pode usar o MPF para criar uma configuração do intervalo que seja específica a um aplicativo de TCP/IP particular, ao contrário de um que se aplica a todos os aplicativos de TCP/IP.

O MPF apoia estas características:

- Normalização TCP, TCP e limites e intervalos da conexão de UDP, e de número de sequência TCP randomization
- CSC
- Inspeção de aplicativo
- IPS
- Vigilância de entrada de QoS
- QoS output o policiamento
- Fila de prioridade de QoS

A configuração do MPF consiste em quatro tarefas:

1. Identifique a camada 3 e o tráfego 4 a que você quer aplicar ações. Refira a identificação do tráfego usando um mapa da classe da camada 3/4 para mais informação.
2. (Inspeção de aplicativo somente) defina ações especiais para o tráfego da inspeção de aplicativo. Refira configurar ações especiais para inspeções de aplicativo para mais informação.
3. Aplique ações à camada 3 e o tráfego 4. Refira a definição de ações usando um mapa de política da camada 3/4 para mais informação.

4. Ative as ações em uma relação. Refira a aplicação de uma política da camada 3/4 a uma relação usando uma política de serviços para mais informação.

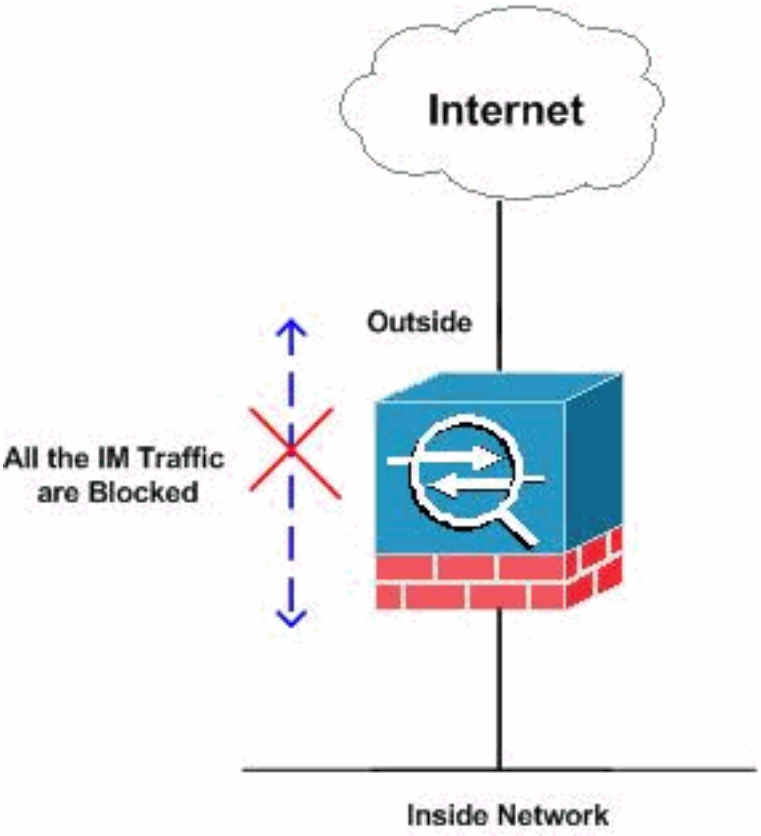
Configurar o P2P e IM obstrução do tráfego

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



PIX/ASA 7.0 e configuração 7.1

Obstrua o P2P & IM configuração do tráfego para PIX/ASA 7.0 e 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#
```

Refira configurar um mapa HTTP para a seção de controle adicional da inspeção do guia do comando line configuration do dispositivo do Cisco Security para obter mais informações sobre do **comando map HTTP** e dos vários parâmetros associados com ele.

PIX/ASA 7.2 e configuração mais atrasada

Nota: O comando do HTTP-**mapa** é suplicado da versão de software 7.2 e mais atrasado. Consequentemente, você precisa de usar o **tipo do mapa de política inspeciona o** comando **im** a fim obstruir o tráfego IM.

Obstrua o P2P & IM configuração do tráfego para PIX/ASA 7.2 e mais atrasado

```
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-
```

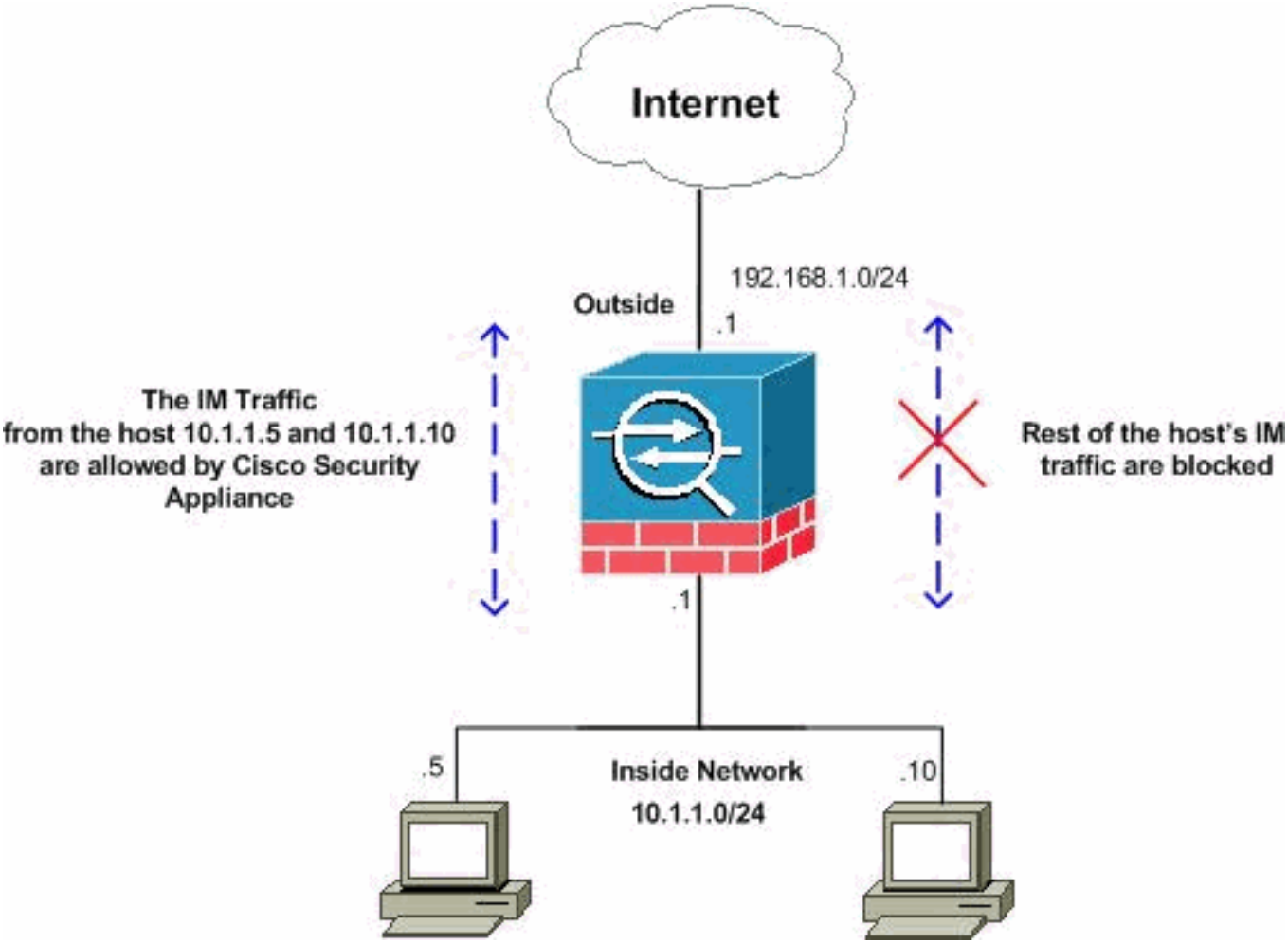
```
policy global_policy global service-policy IM_P2P
interface inside !--- Apply the policy map "IM_P2P" !---
to the inside interface. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
CiscoASA#
```

Lista de expressões regulares incorporados

```
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 e mais atrasado: Permita que os dois anfitriões usem o tráfego IM

Essa seção utiliza esta configuração de rede:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. Estes são os endereços do RFC 1918, que foram usados em um ambiente de laboratório.

Se você quer permitir o tráfego IM do número específico dos anfitriões, a seguir você precisa de terminar como mostrado esta configuração. Neste exemplo, os dois anfitriões 10.1.1.5 e 10.1.1.10 da rede interna são permitidos usar os aplicativos IM tais como MSN Messenger e Yahoo Messenger. Contudo, o tráfego IM de outros anfitriões não é permitido ainda.

IM configuração do tráfego para PIX/ASA 7.2 e mais atrasado para permitir dois anfitriões

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre o HTTP-mapa da executar-configuração** — Mostra os mapas HTTP que foram 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 !`
- **mostre o mapa de política da executar-configuração** — Indica todas as configurações de mapa de política assim como configuração de mapa de política do padrão.`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` Você pode igualmente usar as opções neste comando como mostrado aqui:
  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 !`

- **mostre o mapa de classe da executar-configuração** — Indica a informação sobre a configuração de mapa da classe.`CiscoASA#`**`show running-config class-map`** `! class-map inspection_default match default-inspection-traffic class-map imblock match any`
- **mostre a serviço-política da executar-configuração** — Indica todas as configurações atualmente sendo executado da política de serviços.`CiscoASA#`**`show running-config service-policy`** `service-policy global_policy global service-policy imdrop interface outside`
- **mostre a lista de acesso da executar-configuração** — Indica a configuração de lista de acesso que está sendo executado na ferramenta de segurança.`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

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **debugar im** — Mostra as mensagens debugar para IM o tráfego.
- **serviço-política da mostra** — Indica as políticas de serviços 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 acesso da mostra** — Indica os contadores para uma lista de acessos.`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`

Informações Relacionadas

- Página de suporte do Cisco 5500 Series ASA
- Página de Suporte dos Cisco PIX 500 Series Security Appliances
- Suporte Técnico e Documentação - Cisco Systems