PIX/ASA 7.x ou posterior: Bloqueie o tráfego peer-to-peer (P2P) e mensagens instantâneas (IM) usando o exemplo de configuração do MPF

Contents

Introduction

Este documento descreve como configurar o PIX/ASA dos Cisco Security Appliances usando o Modular Policy Framework (MPF) para bloquear o tráfego de peer-to-peer (P2P) e mensagens instantâneas (IM), como o MSN Messenger e o Yahoo Messenger, da rede interna para a Internet. Além disso, este documento fornece informações sobre como configurar o PIX/ASA para permitir que os dois hosts usem aplicativos IM enquanto o restante dos hosts permanecem bloqueados.

Observação: o ASA pode bloquear aplicativos do tipo P2P somente se o tráfego P2P estiver sendo encapsulado por HTTP. Além disso, o ASA pode descartar o tráfego P2P se ele for encapsulado através do HTTP.

Prerequisites

Requirements

Este documento pressupõe que o Cisco Security Appliance está configurado e funciona corretamente.

Componentes Utilizados

As informações neste documento são baseadas no Cisco 5500 Series Adaptive Security Appliance (ASA) que executa o software versão 7.0 e posterior.

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.

Produtos Relacionados

Essa configuração também pode ser usada com o Cisco 500 Series PIX Firewall que executa o software versão 7.0 e posterior.

Conventions

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

Visão geral da estrutura de política modular

O MPF oferece uma maneira consistente e flexível de configurar os recursos do dispositivo de segurança. Por exemplo, você pode usar o MPF para criar uma configuração de tempo limite específica para um determinado aplicativo TCP, em vez de uma que se aplique a todos os aplicativos TCP.

O MPF suporta estes recursos:

- normalização de TCP, limites e timeouts de conexão TCP e UDP e randomização de número de sequência TCP
- CSC
- Inspeção de aplicações
- IPS
- policiamento de entrada de QoS
- vigilância de saída de QoS
- fila de prioridade de QoS

A configuração do MPF consiste em quatro tarefas:

1. Identifique o tráfego das Camadas 3 e 4 ao qual deseja aplicar ações. Consulte Identificação de Tráfego Usando um Mapa de Classe de Camada 3/4 para obter mais informações.
2. (Somente inspeção de aplicativos) Defina ações especiais para o tráfego de inspeção de aplicativos. Consulte Configuração de Ações Especiais para Inspeção de Aplicativos para obter mais informações.
3. Aplique ações ao tráfego das Camadas 3 e 4. Consulte Definindo Ações Usando um Mapa de Políticas de Camada 3/4 para obter mais informações.
4. Ative as ações em uma interface. Consulte Aplicação de uma Política de Camada 3/4 a uma Interface Usando uma Política de Serviço para obter mais informações.

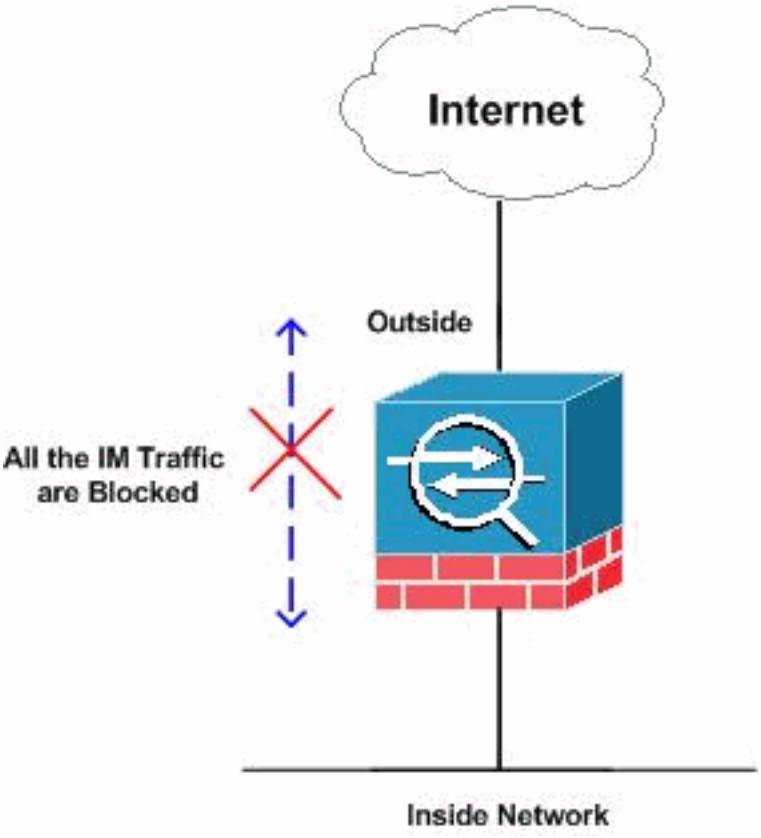
Configurar o bloqueio de tráfego P2P e IM

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:



Configuração do PIX/ASA 7.0 e 7.1

Bloquear a configuração de tráfego P2P e IM 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#
```

Consulte a seção Configurando um Mapa HTTP para Controle de Inspeção Adicional do Guia de Configuração de Linha de Comando do Cisco Security Appliance para obter mais informações sobre o comando **http map** e vários parâmetros associados a ele.

Configuração do PIX/ASA 7.2 e posterior

Observação: o comando **http-map** foi substituído do software versão 7.2 e posterior. Portanto, você precisa usar o comando **policy-map type inspect im** para bloquear o tráfego de IM.

Bloquear a configuração de tráfego P2P e IM para PIX/ASA 7.2 e 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#
```

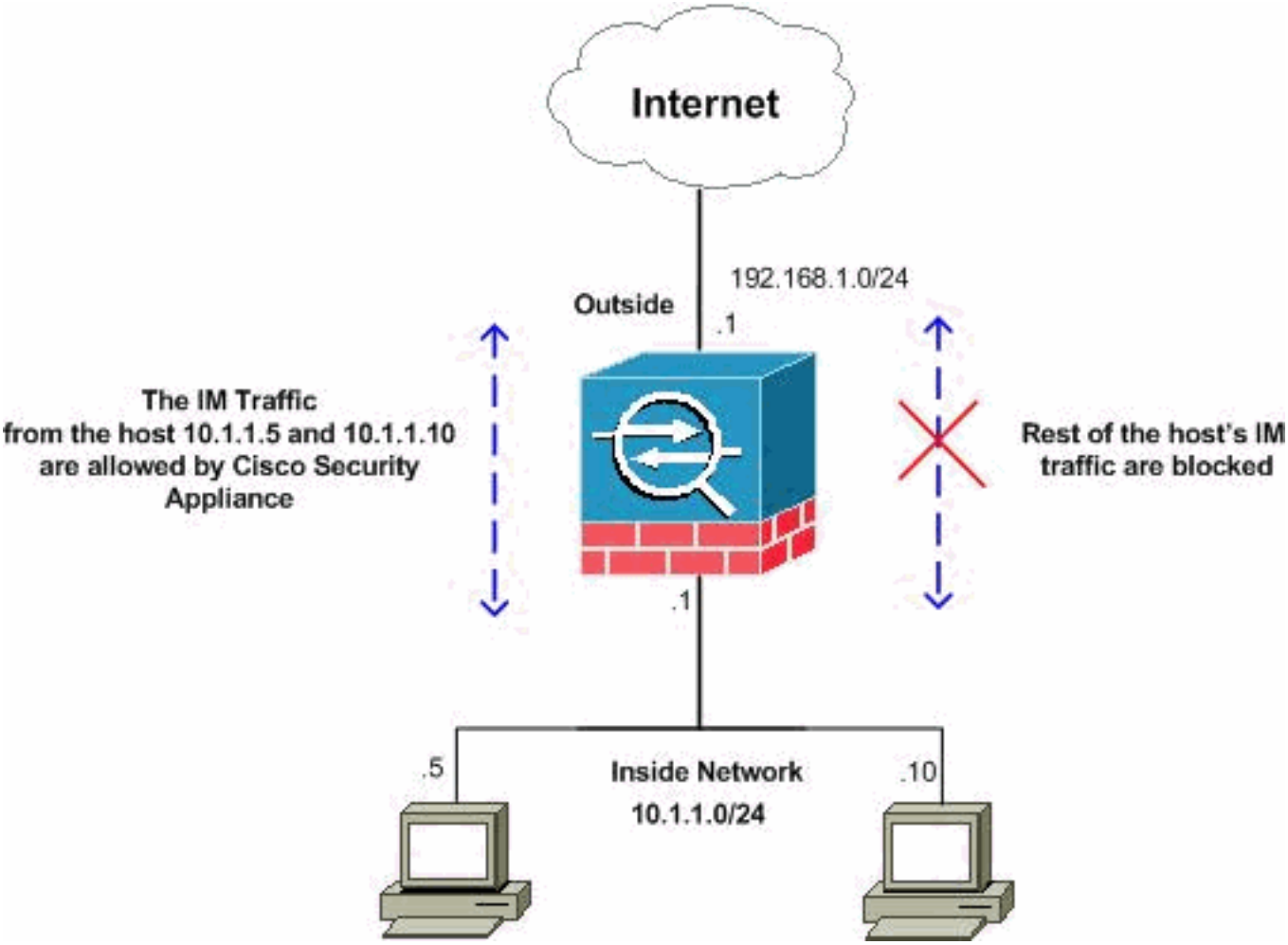
Lista de expressões regulares internas

```
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 posterior: Permitir que os dois hosts usem o tráfego de IM

Essa seção utiliza esta configuração de rede:



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

Se você quiser permitir o tráfego de IM do número específico dos hosts, você precisa concluir esta configuração conforme mostrado. Neste exemplo, os dois hosts 10.1.1.5 e 10.1.1.10 da rede interna têm permissão para usar os aplicativos de IM, como MSN Messenger e Yahoo Messenger. No entanto, o tráfego IM de outros hosts ainda não é permitido.

Configuração de tráfego IM para PIX/ASA 7.2 e posterior

para permitir dois 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
```

Verificar

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

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

- **show running-config http-map** — 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
  !
  ```
- **show running-config policy-map** — Exibe todas as configurações do mapa de políticas, bem como a configuração padrão do mapa de políticas.
  ```
  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 também pode 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
!
```

- **show running-config class-map** — Exibe as informações sobre a configuração do mapa de classes.

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

- **show running-config service-policy** — Exibe todas as configurações de política de serviço em execução no momento.

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

- **show running-config access-list** —Exibe a configuração da lista de acesso que está sendo executada no Security Appliance.

```
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

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.

- **debug im** — Mostra as mensagens de depuração para o tráfego IM.
- **show service-policy** — Exibe as políticas de serviço 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** — Exibe os contadores de uma lista de acesso.

```
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 dispositivos de segurança Cisco PIX 500 Series
- Suporte Técnico e Documentação - Cisco Systems