

PIX/ASA 7.x 及更高版本：使用MPF阻塞对等(P2P)和即时消息(IM)数据流配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[相关产品](#)

[规则](#)

[模块化策略框架概述](#)

[配置 P2P 和 IM 流量阻塞](#)

[网络图](#)

[PIX/ASA 7.0 和 7.1 配置](#)

[PIX/ASA 7.2 及更高版本配置](#)

[PIX/ASA 7.2 及更高版本：允许两台主机使用 IM 流量](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述如何配置Cisco安全伊莱克斯PIX/ASA使用模块化政策架构(MPF)为了阻塞点对点(P2P)和即时消息(IM)，例如MSN Messenger和Yahoo信使，从网络内部的流量到互联网。此外，本文档还提供有关如何配置 PIX/ASA 以在阻止其余主机的情况下允许两台主机使用 IM 应用程序的信息。

注意：只有在通过 HTTP 隧道传输 P2P 流量的情况下，ASA 才能阻止 P2P 类型的应用程序。此外，如果 P2P 流量是通过 HTTP 隧道传输的，则 ASA 可丢弃该流量。

先决条件

要求

本文档假设已配置 Cisco 安全设备且它能正常工作。

使用的组件

本文档中的信息根据Cisco ASA 5500系列自适应安全设备(ASA)该运行软件版本7.0及以后。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[相关产品](#)

此配置也可用于运行软件版本 7.0 及更高版本的 Cisco 500 系列 PIX 防火墙。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[模块化策略框架概述](#)

MPF 提供一种一致且灵活的配置安全设备功能的方式。例如，您可以使用 MPF 创建仅适用于特定 TCP 应用程序的超时配置，而非适用于所有 TCP 应用程序的配置。

MPF 支持以下功能：

- TCP 标准化、TCP 和 UDP 连接限制和超时以及 TCP 序列号随机化
- CSC
- 应用程序检查
- IPS
- QoS 输入策略
- QoS 输出管制
- QoS 优先级队列

MPF 的配置包括四项任务：

1. 识别您要应用操作的第 3 层和第 4 层流量。有关详细信息，请参阅[使用第 3 层/第 4 层类映射识别流量](#)。
2. (仅限应用程序检查) 定义针对应用程序检查流量的特殊操作。有关详细信息，请参阅[配置特殊的应用程序检查操作](#)。
3. 将操作应用于第 3 层和第 4 层流量。有关详细信息，请参阅[使用第 3 层/第 4 层策略映射定义操作](#)。
4. 在接口上激活操作。有关详细信息，请参阅[使用服务策略将第 3 层/第 4 层策略应用到接口](#)。

[配置 P2P 和 IM 流量阻塞](#)

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

[网络图](#)

本文档使用以下网络设置：

[PIX/ASA 7.0 和 7.1 配置](#)

阻止 PIX/ASA 7.0 和 7.1 的 P2P 和 IM 流量配置

```
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#

```

有关 http map 命令及各种相关参数的详细信息，请参阅 [Cisco 安全设备命令行配置指南的配置 HTTP 映射以获得附加检查控制](#) 部分。

[PIX/ASA 7.2 及更高版本配置](#)

注意：自软件版本 7.2 及更高版本开始，http-map 命令已作废。因此，您需要使用 policy-map type inspect im 命令来阻止 IM 流量。

阻止 PIX/ASA 7.2 及更高版本的 P2P 和 IM 流量配置

```

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 ipolicy parameters match
protocol msn-im yahoo-im drop-connection !--- The policy
map "ipolicy" 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 req exp's. policy-map IM_P2P class imblock
inspect im ipolicy 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#

```

内置正则表达式列表

```

regex _default_GoToMyPC-tunnel "machinekey"
regex _default_GoToMyPC-tunnel_2 "[/\]erc[/\]Poll"
regex _default_yahoo-messenger "YMSG"
regex _default_httpport-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 及更高版本：允许两台主机使用 IM 流量

本部分使用以下网络设置：

注意：此配置中使用的 IP 编址方案在 Internet 上不可合法路由。以下地址是在实验室环境中使用的 RFC 1918 地址。

如果想要允许来自特定数量的主机的 IM 流量，您需要完成以下配置，如下所示。在本示例中，允许来自内部网络的两台主机 10.1.1.5 和 10.1.1.10 使用 IM 应用程序，如 MSN Messenger 和 Yahoo Messenger。但是，仍不允许来自其他主机的 IM 流量。

PIX/ASA 7.2 及更高版本允许两台主机的 IM 流量配置

```

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.
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
esmtplib 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

```

验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \(仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 **show** 命令输出的分析。

- **show running-config http-map**—显示已配置的 HTTP 映射。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**—显示所有策略映射配置和默认策略映射配置。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 esmtplib**

inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp 还可以使用以下命令中的选项，如下所示：

```
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**—显示有关类映射配置的信息。CiscoASA#`show running-config class-map ! class-map inspection_default match default-inspection-traffic class-map imblock match any`
- **show running-config service-policy**—显示所有当前运行的服务策略配置。CiscoASA#`show running-config service-policy service-policy global_policy global service-policy imdrop interface outside`
- **show running-config access-list**—显示在安全设备上运行的访问列表配置。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`

故障排除

本部分提供的信息可用于对配置进行故障排除。

注意： 使用 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

- **debug im**—显示 IM 流量的调试消息。
- **show service-policy**—显示已配置的服务策略。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**—显示访问列表的计数器。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`

相关信息

- [Cisco 5500 系列 ASA 支持页](#)
- [Cisco PIX 500 系列安全设备支持页](#)
- [技术支持和文档 - Cisco Systems](#)