PIX/ASA 7.x及更高版本：使用MPF配置示例阻止對等(P2P)和即時消息(IM)流量

目錄

簡介

本文檔介紹如何使用模組化策略框架(MPF)配置思科安全裝置PIX/ASA，以阻止點對點(P2P)和即時消息(IM)（例如MSN Messenger和Yahoo Messenger）從內部網路到網際網路的流量。此外，本文檔還提供了有關如何配置PIX/ASA以允許兩台主機使用IM應用而其餘主機仍被阻止的資訊。

注意：只有通過HTTP隧道傳輸P2P流量時，ASA才能阻止P2P型別應用。此外，如果通過HTTP隧道傳輸P2P流量，ASA可以丟棄該流量。

必要條件

需求

本檔案假設思科安全裝置已設定並正常運作。

採用元件

本檔案中的資訊是根據執行軟體版本7.0和更新版本的Cisco 5500系列調適型安全裝置(ASA)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可以用於運行軟體版本7.0及更高版本的Cisco 500系列PIX防火牆。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

模組化策略框架概述

MPF提供一致且靈活的方法來配置安全裝置功能。例如，可以使用MPF建立特定於特定TCP應用的超時配置，而不是應用於所有TCP應用的超時配置。

MPF支援以下功能：

- TCP規範化、TCP和UDP連線限制和超時以及TCP序列號隨機化
- CSC
- 應用檢測
- IPS
- QoS輸入管制
- QoS輸出管制
- QoS優先順序隊列

MPF的配置包括四項任務：

1. 確定您要對其應用操作的第3層和第4層流量。如需詳細資訊，請參閱使用第3/4層類別對映識別流量。
2. （僅適用於應用檢測）定義應用檢測流量的特殊操作。有關詳細資訊，請參閱為應用程式檢查配置特殊操作。
3. 將操作應用於第3層和第4層流量。有關詳細資訊，請參閱使用第3/4層策略對映定義操作。
4. 啟用介面上的操作。如需詳細資訊，請參閱使用服務原則將第3/4層原則套用到介面。

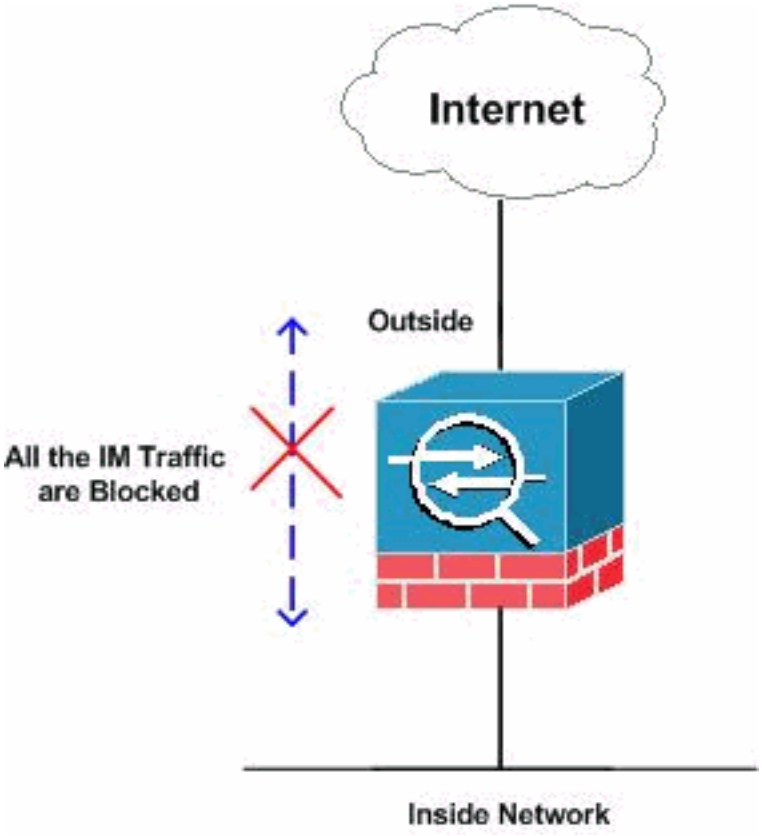
配置P2P和IM流量阻止

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



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#
```

請參閱思科安全裝置命令列配置指南的為其他檢查控制配置HTTP對映部分，以瞭解有關http map命令以及與其關聯的各種引數的詳細資訊。

PIX/ASA 7.2及更高版本的配置

注意：http-map命令從軟體版本7.2及更高版本上已棄用。因此，您需要使用policy-map type inspect im命令來阻止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
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
```

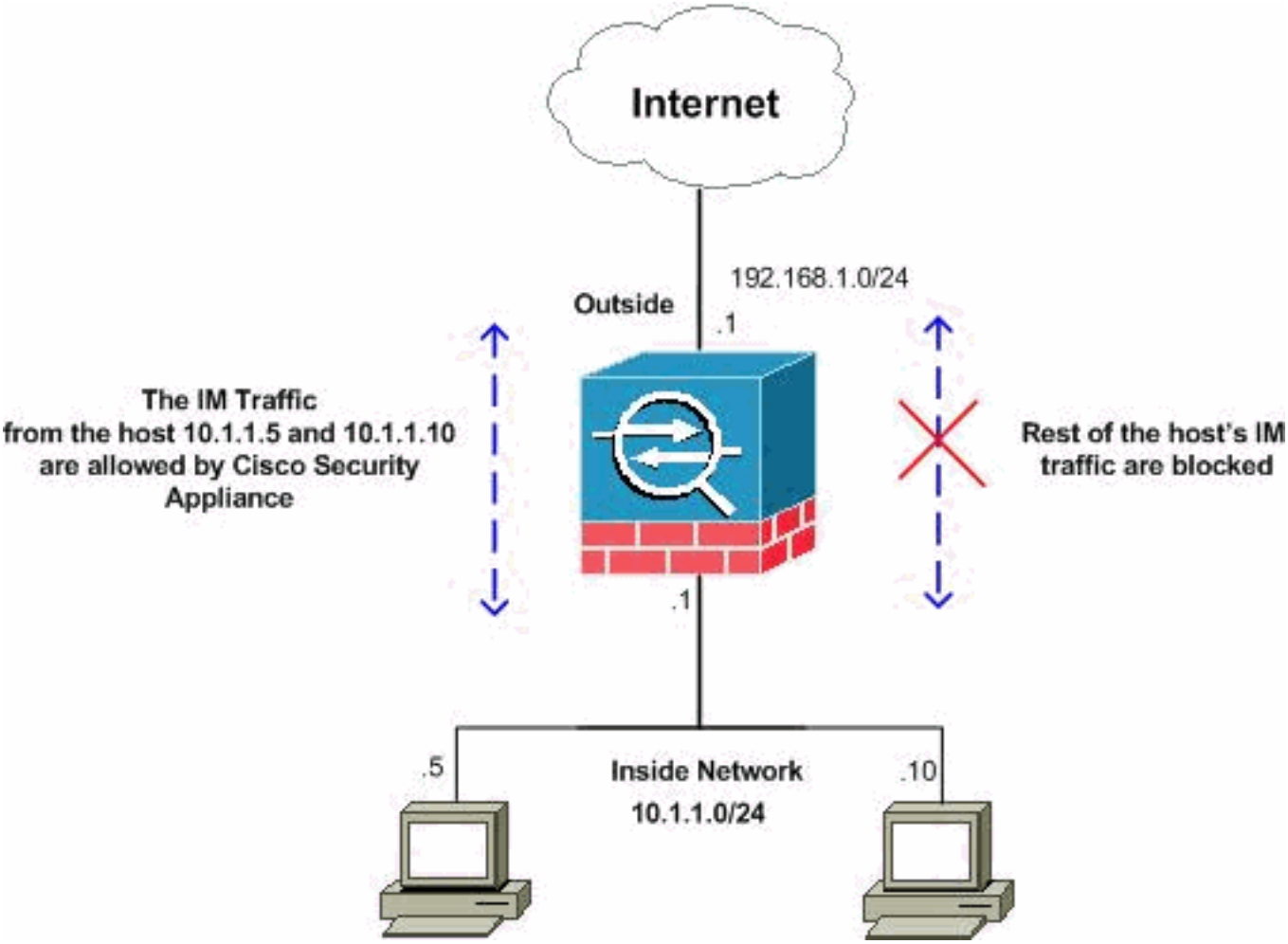
```
 match request uri regex _default_gator
  drop-connection log
 match request uri regex _default_x-kazaa-network
  drop-connection log

!--- 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#
```

內建正規表示式清單

```
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及更高版本：允許兩台主機使用即時消息流量

本節使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

如果要允許來自特定主機數量的IM流量，則需要完成此配置，如下所示。在本示例中，允許來自內部網路的兩台主機10.1.1.5和10.1.1.10使用IM應用程式，如MSN Messenger和Yahoo Messenger。但是，仍不允許來自其他主機的IM流量。

PIX/ASA 7.2及更高版本允許兩台主機的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. 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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- **show running-config http-map** — 顯示已配置的HTTP對映。

```
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** — 顯示所有策略對映配置以及預設策略對映配置。

```
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 esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

您也可以使用此命令中的選項，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** — 顯示有關類對映配置的資訊。

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

```
class-map imblock
 match any
```

- **show running-config service-policy** — 顯示當前運行的所有服務策略配置。

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

- **show running-config access-list** — 顯示正在安全裝置上運行的訪問清單配置。

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug im** — 顯示IM流量的調試消息。
- **show service-policy** — 顯示已配置的服務策略。

```
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** — 顯示訪問清單的計數器。

```
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
```

相關資訊

- Cisco 5500系列ASA支援頁面
- Cisco PIX 500系列安全裝置支援頁面
- 技術支援與文件 - Cisco Systems