

PIX/ASA 7.x and Later: Block the Peer-to-Peer (P2P) and Instant Messaging (IM) Traffic Using MPF Configuration Example

Document ID: 98684

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Modular Policy Framework Overview

Configure the P2P and IM Traffic Blocking

- Network Diagram
- PIX/ASA 7.0 and 7.1 Configuration
- PIX/ASA 7.2 and Later Configuration
- PIX/ASA 7.2 and Later: Allow the Two Hosts to Use the IM Traffic

Verify

Troubleshoot

Related Information

Introduction

This document describes how to configure the Cisco Security Appliances PIX/ASA using Modular Policy Framework (MPF) in order to block the Peer-to-Peer (P2P) and Instant Messaging (IM), such as MSN Messenger and Yahoo Messenger, traffic from the inside network to the Internet. Also, this document provides information on how to configure the PIX/ASA in order to allow the two hosts to use IM applications while the rest of the hosts remain blocked.

Note: The ASA can block P2P type applications only if P2P traffic is being tunneled through HTTP. Also, ASA can drop P2P traffic if it is tunneled through HTTP.

Prerequisites

Requirements

This document assumes that Cisco Security Appliance is configured and works properly.

Components Used

The information in this document is based on the Cisco 5500 Series Adaptive Security Appliance (ASA) that runs software version 7.0 and later.

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.

Related Products

This configuration can also be used with the Cisco 500 Series PIX firewall that runs software version 7.0 and later.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Modular Policy Framework Overview

MPF provides a consistent and flexible way to configure security appliance features. For example, you can use MPF to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications.

MPF supports these features:

- TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization
- CSC
- Application inspection
- IPS
- QoS input policing
- QoS output policing
- QoS priority queue

The configuration of the MPF consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions. Refer to Identifying Traffic Using a Layer 3/4 Class Map for more information.
2. (Application inspection only) Define special actions for application inspection traffic. Refer to Configuring Special Actions for Application Inspections for more information.
3. Apply actions to the Layer 3 and 4 traffic. Refer to Defining Actions Using a Layer 3/4 Policy Map for more information.
4. Activate the actions on an interface. Refer to Applying a Layer 3/4 Policy to an Interface Using a Service Policy for more information.

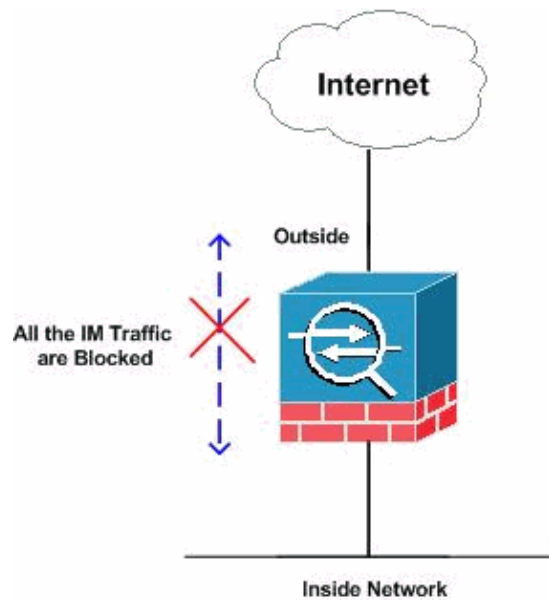
Configure the P2P and IM Traffic Blocking

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



PIX/ASA 7.0 and 7.1 Configuration

Block the P2P & IM Traffic Configuration for PIX/ASA 7.0 and 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#

```

Refer to the Configuring an HTTP Map for Additional Inspection Control section of the Cisco Security Appliance Command Line Configuration Guide for more information about the **http map** command and various parameters associated with it.

PIX/ASA 7.2 and Later Configuration

Note: The **http-map** command is deprecated from software version 7.2 and later. Therefore, you need to use the **policy-map type inspect im** command in order to block the IM traffic.

Block the P2P & IM Traffic Configuration for PIX/ASA 7.2 and
Later

```
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#

```

List of built-in regular expressions

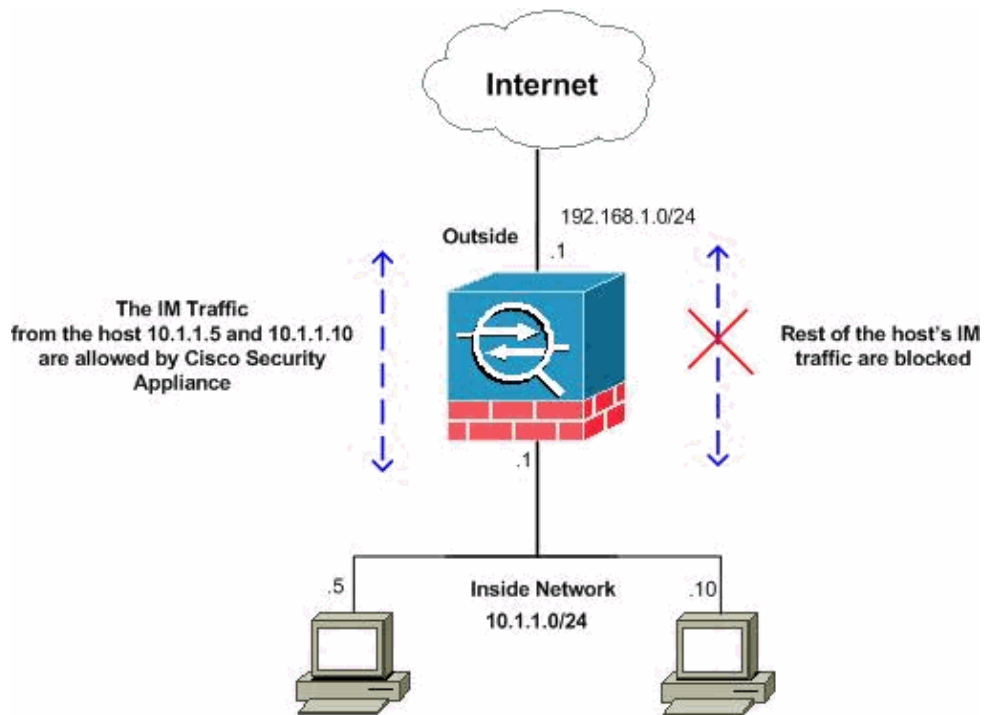
```

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]"
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 and Later: Allow the Two Hosts to Use the IM Traffic

This section uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. These are RFC 1918 addresses, which have been used in a lab environment.

If you want to allow the IM traffic from the specific number of the hosts, then you need to complete this configuration as shown. In this example, the two hosts 10.1.1.5 and 10.1.1.10 from the inside network are allowed to use the IM applications such as MSN Messenger and Yahoo Messenger. However, the IM traffic from other hosts is still not allowed.

IM Traffic Configuration for PIX/ASA 7.2 and Later to Allow Two 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

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show running-config http-map** Shows the HTTP maps that have been configured.

```

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** Displays all the policy-map configurations as well as the default policy-map configuration.

```

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

```

You can also use the options in this command as shown here:

```

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** Displays the information about the class map configuration.

```

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

```

- **show running-config service-policy** Displays all currently running service policy configurations.

```

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

```

- **show running-config access-list** Displays the access-list configuration that is running on the 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

This section provides information you can use to troubleshoot your configuration.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug im** Shows the debug messages for IM traffic.
- **show service-policy** Displays the configured service policies.

```
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** Displays the counters for an access list.

```
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
```

Related Information

- [Cisco 5500 Series ASA Support Page](#)
- [Cisco PIX 500 Series Security Appliances Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 10, 2008

Document ID: 98684
