

# PIX/ASA 7.x et versions ultérieures : Exemple de configuration du blocage du trafic P2P (Peer-to-Peer) et de la messagerie instantanée (IM) à l'aide de MPF

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Produits connexes](#)

[Conventions](#)

[Présentation du cadre de politique modulaire](#)

[Configurer le blocage du trafic P2P et IM](#)

[Diagramme du réseau](#)

[Configuration de PIX/ASA 7.0 et 7.1](#)

[PIX/ASA 7.2 et versions ultérieures](#)

[PIX/ASA 7.2 et versions ultérieures : Autoriser les deux hôtes à utiliser le trafic de messagerie instantanée](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

## [Introduction](#)

Ce document décrit comment configurer les dispositifs de sécurité Cisco PIX/ASA à l'aide du MPF (Modular Policy Framework) afin de bloquer le trafic P2P (Peer to Peer) et IM (Instant Messaging), tel que MSN Messenger et Yahoo Messenger, du réseau interne à Internet. De plus, ce document fournit des informations sur la façon de configurer le PIX/ASA afin de permettre aux deux hôtes d'utiliser des applications de messagerie instantanée tandis que le reste des hôtes reste bloqué.

**Remarque** : l'ASA peut bloquer les applications de type P2P uniquement si le trafic P2P est tunnelisé via HTTP. En outre, ASA peut supprimer le trafic P2P s'il est tunnelisé via HTTP.

## [Conditions préalables](#)

### [Conditions requises](#)

Ce document suppose que le dispositif de sécurité Cisco est configuré et fonctionne correctement.

## Components Used

Les informations de ce document sont basées sur l'apppliance de sécurité adaptable (ASA) de la gamme Cisco 5500 qui exécute les versions 7.0 et ultérieures du logiciel.

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.

## Produits connexes

Cette configuration peut également être utilisée avec le pare-feu PIX de la gamme Cisco 500 qui exécute les versions 7.0 et ultérieures du logiciel.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Présentation du cadre de politique modulaire

Le protocole MPF offre une méthode cohérente et flexible de configuration des fonctionnalités des dispositifs de sécurité. Par exemple, vous pouvez utiliser MPF pour créer une configuration de délai d'attente spécifique à une application TCP particulière, par opposition à une configuration qui s'applique à toutes les applications TCP.

MPF prend en charge ces fonctionnalités :

- Normalisation TCP, limites et délais de connexion TCP et UDP, et randomisation des numéros de séquence TCP
- CSC
- Inspection d'application
- IPS
- Contrôle des entrées QoS
- Contrôle de sortie QoS
- File d'attente de priorité QoS

La configuration du protocole MPF se compose de quatre tâches :

1. Identifiez le trafic des couches 3 et 4 auquel vous voulez appliquer des actions. Référez-vous à [Identification du trafic à l'aide d'une carte de classe de couche 3/4](#) pour plus d'informations.
2. (Inspection d'application uniquement) Définissez des actions spéciales pour le trafic d'inspection d'application. Référez-vous à [Configuration des actions spéciales pour les inspections d'applications](#) pour plus d'informations.
3. Appliquez des actions au trafic des couches 3 et 4. Référez-vous à [Définir des actions à l'aide d'une carte de stratégie de couche 3/4](#) pour plus d'informations.
4. Activez les actions sur une interface. Référez-vous à [Application d'une stratégie de couche 3/4 à une interface à l'aide d'une stratégie de service](#) pour plus d'informations.

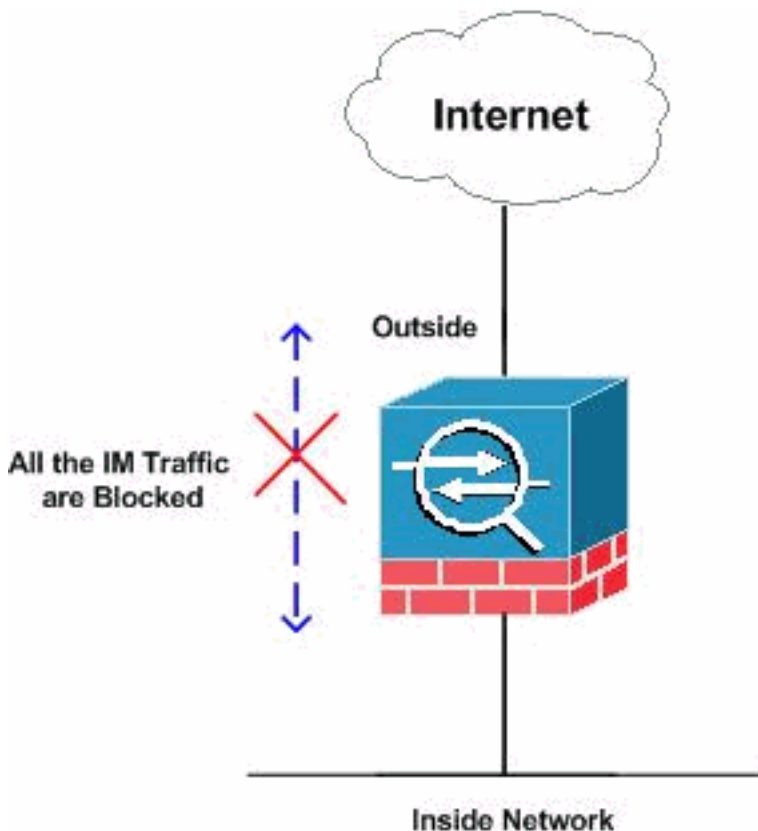
## Configurer le blocage du trafic P2P et IM

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque :** utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

### Diagramme du réseau

Ce document utilise la configuration réseau suivante :



### Configuration de PIX/ASA 7.0 et 7.1

#### **Bloquer la configuration du trafic P2P et IM pour PIX/ASA 7.0 et 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#

```

Reportez-vous à la section [Configuration d'une carte HTTP pour un contrôle d'inspection supplémentaire](#) du [Guide de configuration de ligne de commande de l'appliance de sécurité Cisco](#) pour plus d'informations sur la commande **http map** et les différents paramètres qui lui sont associés.

## [PIX/ASA 7.2 et versions ultérieures](#)

**Remarque :** La commande **http-map** est déconseillée par rapport aux versions 7.2 et ultérieures du logiciel. Par conséquent, vous devez utiliser la commande **policy-map type inspect im** afin de bloquer le trafic de messagerie instantanée.

### **Bloquer la configuration du trafic P2P et IM pour PIX/ASA 7.2 et versions ultérieures**

```

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#

```

## Liste des expressions régulières intégrées

```

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[-

```

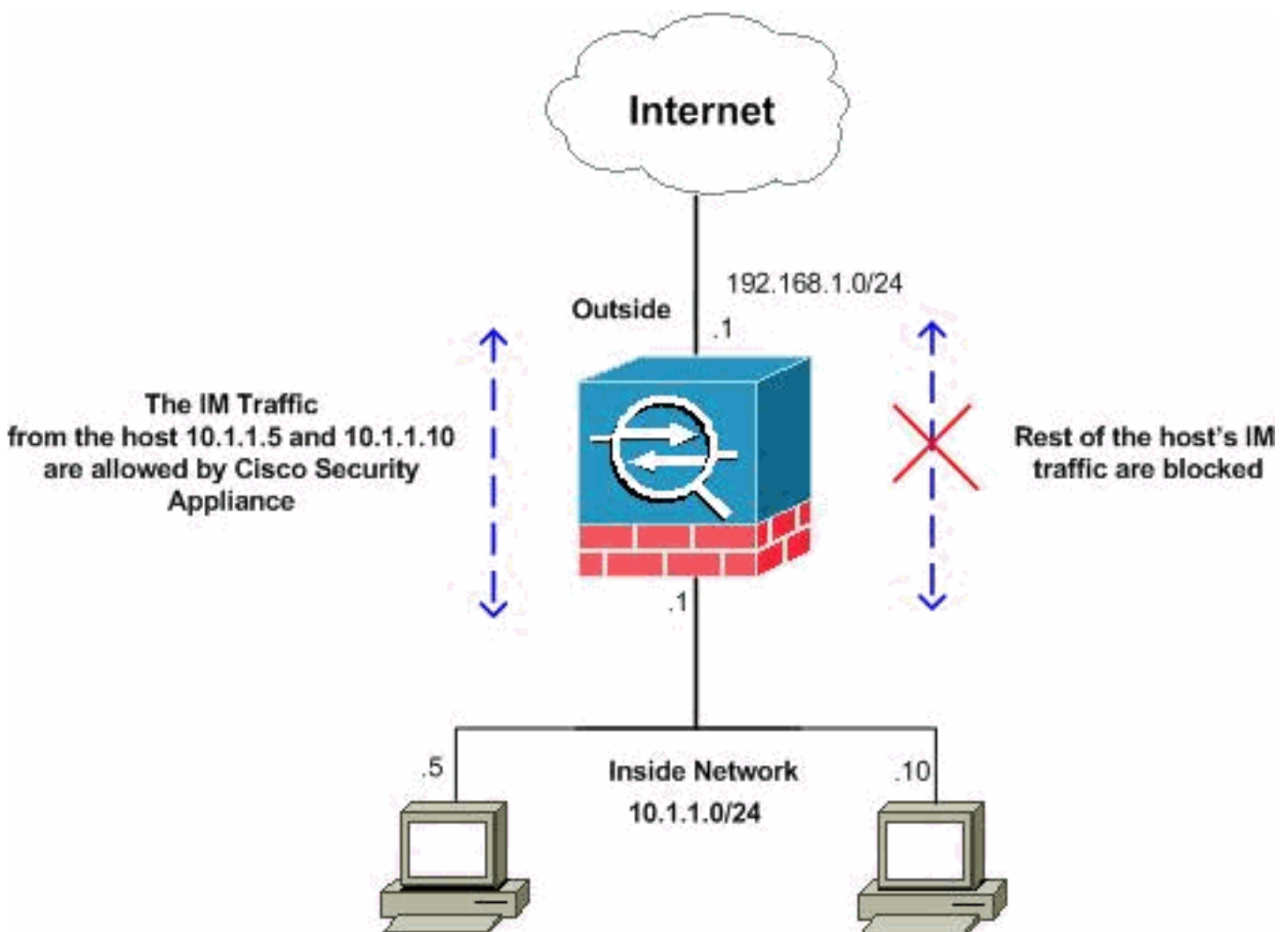
```

]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 et versions ultérieures : Autoriser les deux hôtes à utiliser le trafic de messagerie instantanée](#)

Cette section utilise cette configuration du réseau :



**Remarque :** les schémas d'adressage IP utilisés dans cette configuration ne sont pas routables légalement sur Internet. Il s'agit d'adresses RFC 1918, qui ont été utilisées dans un environnement de travaux pratiques.

Si vous voulez autoriser le trafic de messagerie instantanée à partir du numéro spécifique des hôtes, vous devez terminer cette configuration comme indiqué. Dans cet exemple, les deux hôtes

10.1.1.5 et 10.1.1.10 du réseau interne sont autorisés à utiliser les applications de messagerie instantanée telles que MSN Messenger et Yahoo Messenger. Cependant, le trafic de messagerie instantanée provenant d'autres hôtes n'est toujours pas autorisé.

## Configuration du trafic de messagerie instantanée pour PIX/ASA 7.2 et versions ultérieures pour autoriser deux hôtes

```
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 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

```

## Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie](#) (clients [enregistrés uniquement](#)) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

- **show running-config http-map** : affiche les mappages HTTP configurés.

```

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** - Affiche toutes les configurations de la carte de stratégie ainsi que la configuration de la carte de stratégie par défaut.

```

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
```

Vous pouvez également utiliser les options de cette commande, comme indiqué ici :

```
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** : affiche les informations relatives à la configuration de la carte de classe.

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

- **show running-config service-policy** - Affiche toutes les configurations de stratégie de service en cours d'exécution.

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

- **show running-config access-list** - Affiche la configuration de liste d'accès qui s'exécute sur l'appliance de sécurité.

```
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
```

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

**Remarque** : Consulter les [renseignements importants sur les commandes de débogage](#) avant d'utiliser les commandes de débogage.

- **debug im** - Affiche les messages de débogage pour le trafic de messagerie instantanée.
- **show service-policy** - Affiche les stratégies de service configurées.

```
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** : affiche les compteurs d'une liste d'accès.

```
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
```

## [Informations connexes](#)

- [Page d'assistance ASA de la gamme Cisco 5500](#)
- [Page de support pour serveurs de sécurité de la gamme Cisco PIX 500](#)
- [Support et documentation techniques - Cisco Systems](#)