PIX/ASA 7.x en later: Blokkeer het peer-to-peer (P2P) en Instant Messaging (IM) verkeer met behulp van MPF-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco security applicaties PIX/ASA kunt configureren met behulp van modulair beleidskader (MPF) om het peer-to-peer (P2P) en Instant Messaging (IM) te blokkeren, zoals MSN Messenger en Yahoo Messenger, verkeer van binnen netwerk naar internet. Bovendien geeft dit document informatie over hoe de PIX/ASA te configureren om de twee hosts toegang te geven tot het gebruik van IM-applicaties terwijl de rest van de hosts geblokkeerd blijft.

Opmerking: ASA kan P2P-type toepassingen alleen blokkeren als P2P-verkeer via HTTP wordt getunneld. ASA kan ook P2P-verkeer laten vallen als het via HTTP getunneld is.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat Cisco security applicatie is geconfigureerd en correct werkt.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 5500 Series adaptieve security applicatie (ASA) die softwareversie 7.0 en hoger uitvoert.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met de Cisco 500 Series PIX-firewall die softwareversie 7.0 en hoger uitvoert.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Overzicht van het beleidskader

MPF biedt een consistente en flexibele manier om de functies van security applicaties te configureren. U kunt bijvoorbeeld MPF gebruiken om een tijdelijke configuratie te maken die specifiek is voor een bepaalde TCP-toepassing, in tegenstelling tot een configuratie die van toepassing is op alle TCP-toepassingen.

MPF ondersteunt deze functies:

- TCP-normalisatie, TCP- en UDP-verbindingslimieten en -onderbreking, en TCP-sequentienummer-randomisatie
- CSC
- Toepassingscontrole
- IPS
- QoS-input-toezicht
- QoS-uitvoertoezicht
- QoS-prioriteitswachtrij

De samenstelling van het MPF bestaat uit vier taken:

1. Identificeer Layer 3 en 4 verkeer waarop u acties wilt toepassen. Raadpleeg het Identificeren van verkeer met een Layer 3/4 Class Map voor meer informatie.
2. (Uitsluitend voor de inspectie van toepassingen) Vaststellen van speciale maatregelen voor het verkeer van de inspectie van toepassingen. Zie Speciale acties voor Toepassingsinspecties configureren voor meer informatie.
3. Toepassen acties op Layer 3 en 4 verkeer. Raadpleeg Handelingen definiëren met een Layer 3/4 beleidskaart voor meer informatie.
4. Activeert de acties op een interface. Raadpleeg het gedeelte Layer 3/4-beleid toepassen op een interface met een servicebeleid voor meer informatie.

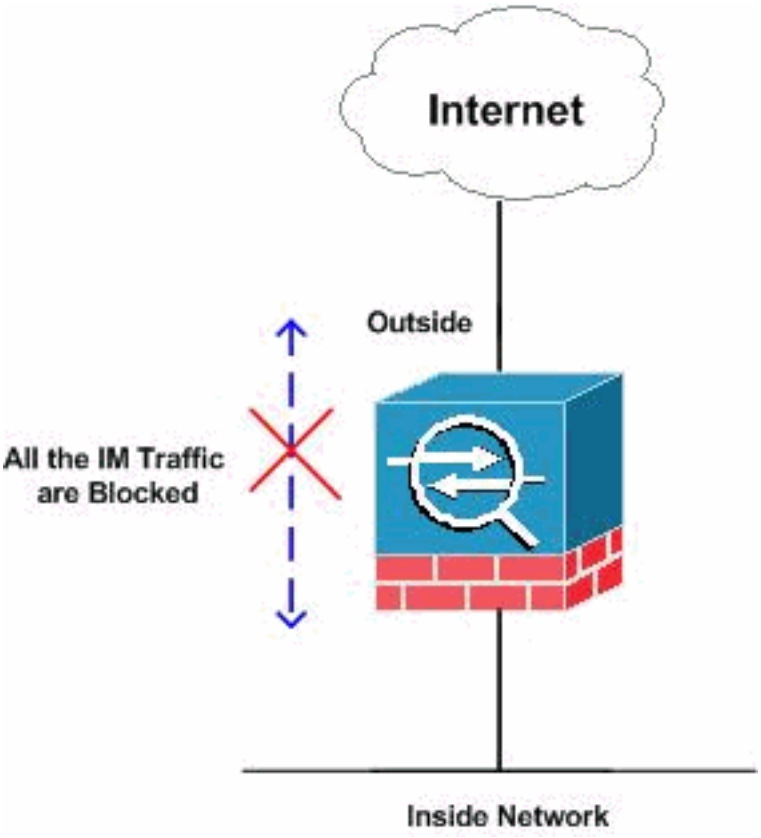
Configuratie van P2P en IM traffic blokkering

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuratie PIX/ASA 7.0 en 7.1

Blokkeer de P2P en IM traffic configuratie voor PIX/ASA 7.0 en 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#
```

Raadpleeg het gedeelte HTTP Map configureren voor extra inspectie-controle van de Cisco Security Appliance Opdracht Line voor meer informatie over de **http map**-opdracht en verschillende parameters die hiermee samenhangen.

PIX/ASA 7.2 en hoger configuratie

Opmerking: De **http-map** opdracht is afgeschreven van softwareversie 7.2 en later. Daarom moet u het **beleid-kaart type** gebruiken **inspecteer im** opdracht om het IM verkeer te blokkeren.

Blokkeer de P2P en IM traffic configuratie voor PIX/ASA 7.2 en 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#
```

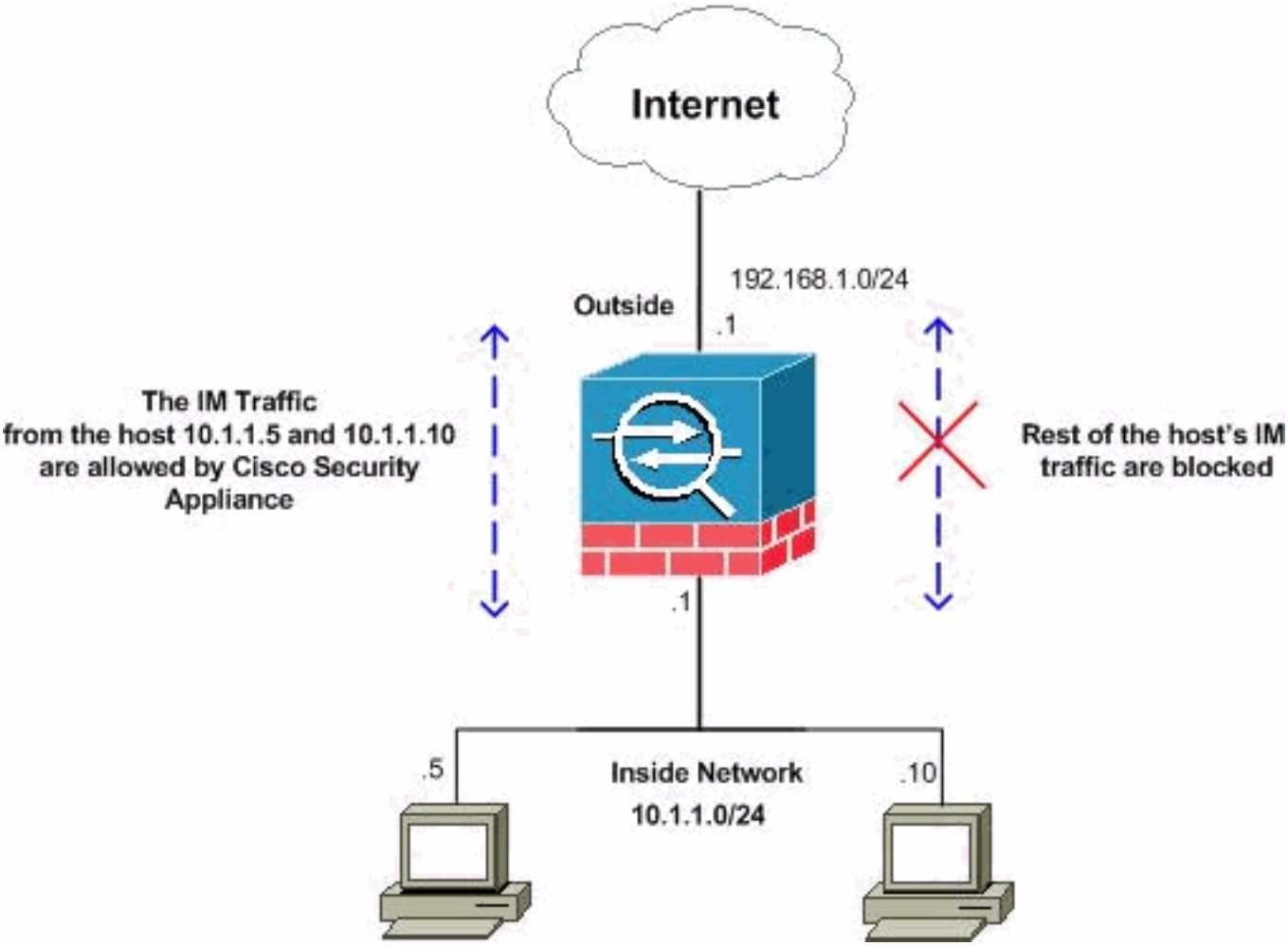
Lijst van ingebouwde reguliere expressies

```
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 en later: toestaan dat de twee hosts gebruik maken van het IM verkeer

In deze sectie wordt deze netwerkinstellingen gebruikt:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Dit zijn RFC 1918-adressen, die in een labomgeving zijn gebruikt.

Als u het IM verkeer van het specifieke aantal hosts wilt toestaan, dan moet u deze configuratie zoals getoond voltooien. In dit voorbeeld zijn de twee hosts 10.1.1.5 en 10.1.1.10 vanaf het binnennetwerk toegestaan de IM-toepassingen te gebruiken, zoals MSN Messenger en Yahoo Messenger. Het IM verkeer van andere hosts is echter nog steeds niet toegestaan.

IM traffic configuratie voor PIX/ASA 7.2 en later om twee hosts mogelijk te maken

```
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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (geregistreerde klanten slechts) (OIT) steunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **tonen in werking stellen-in werking stellen-enig http-map**-toont de HTTP kaarten die zijn gevormd.

```
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
!
```

- **tonen in werking stellen-in werking stellen-enig beleid-kaart**-Toont alle beleid-kaart configuraties evenals de standaard beleid-kaart configuratie.

```
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
```

U kunt de opties in deze opdracht ook gebruiken, zoals hier wordt getoond:

```
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
!
```

- **toon in werking stellen-in werking stellen-enig klas-kaart**-Toont de informatie over de configuratie van de klas.

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

- **toon in werking stellen-wijk service-beleid**-Toont alle momenteel in werking zijnde de dienstbeleidsconfiguraties.

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

- **Toon in werking stellen-beslist toegang-lijst**-Toont de toegang-lijst configuratie die op het veiligheidsapparaat loopt.

```
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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug**-opdrachten gebruikt.

- **debug hem**: toont de debug-berichten voor IM-verkeer.
- **toon service-beleid**-displays het geconfigureerde servicebeleid.

```
CiscoASA#show service-policy interface outside

Interface outside:
  Service-policy: imdrop
    Class-map: imblock
      Inspect: im impolicy, packet 0, drop 0, reset-drop 0
```

- **Toon toegang-lijst**-Toont de tellers voor een toegangslijst.

```
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
```

Gerelateerde informatie

- Cisco 5500 Series ASA-ondersteuningspagina
- Ondersteuning van Cisco PIX 500 Series security applicaties
- Technische ondersteuning en documentatie – Cisco Systems