PIX/ASA 7.x 이상:MPF 컨피그레이션 예를 사용하여 P2P(Peer-to-Peer) 및 IM(Instant Messaging) 트래픽 차단

목차

소개

이 문서에서는 MPF(Modular Policy Framework)를 사용하여 Cisco Security Appliances PIX/ASA를 구성하여 MSN Messenger 및 Yahoo Messenger와 같은 P2P(Peer-to-Peer) 및 IM(Instant Messaging)을 차단하여 내부 네트워크에서 인터넷으로의 트래픽을 차단하는 방법에 대해 설명합니다.또한 이 문서에서는 두 호스트가 IM 애플리케이션을 사용할 수 있도록 PIX/ASA를 구성하는 방법에 대한 정보를 제공하고 나머지 호스트는 차단됩니다.

참고: ASA는 P2P 트래픽이 HTTP를 통해 터널링되는 경우에만 P2P 유형 애플리케이션을 차단할 수 있습니다.또한 ASA는 HTTP를 통해 터널링되는 경우 P2P 트래픽을 삭제할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에서는 Cisco Security Appliance가 구성되어 제대로 작동한다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 7.0 이상을 실행하는 Cisco 5500 Series ASA(Adaptive Security Appliance)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 소프트웨어 버전 7.0 이상을 실행하는 Cisco 500 Series PIX 방화벽과 함께 사용할 수도 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

모듈식 정책 프레임워크 개요

MPF는 보안 어플라이언스 기능을 구성할 수 있는 일관되고 유연한 방법을 제공합니다.예를 들어, 모든 TCP 애플리케이션에 적용되는 것과 달리 MPF를 사용하여 특정 TCP 애플리케이션에 특정한 시간 제한 컨피그레이션을 생성할 수 있습니다.

MPF는 다음 기능을 지원합니다.

- TCP 정규화, TCP 및 UDP 연결 제한 및 시간 제한, TCP 시퀀스 번호 임의 설정
- CSC
- 애플리케이션 검사
- IPS
- QoS 입력 폴리싱
- QoS 출력 폴리싱
- QoS 우선순위 큐

MPF 컨피그레이션은 다음 네 가지 작업으로 구성됩니다.

1. 작업을 적용할 레이어 3 및 4 트래픽을 식별합니다.자세한 내용은 레이어 3/4 클래스 맵을 사용하여 트래픽 식별을 참조하십시오.
2. (애플리케이션 검사만 해당) 애플리케이션 검사 트래픽에 대한 특별 작업을 정의합니다.자세한 내용은 애플리케이션 검사를 위한 특별 작업 구성을 참조하십시오.
3. 레이어 3 및 4 트래픽에 작업을 적용합니다.자세한 내용은 레이어 3/4 정책 맵을 사용하여 작업 정의를 참조하십시오.
4. 인터페이스에서 작업을 활성화합니다.자세한 내용은 서비스 정책을 사용하여 인터페이스에 레이어 3/4 정책 적용을 참조하십시오.

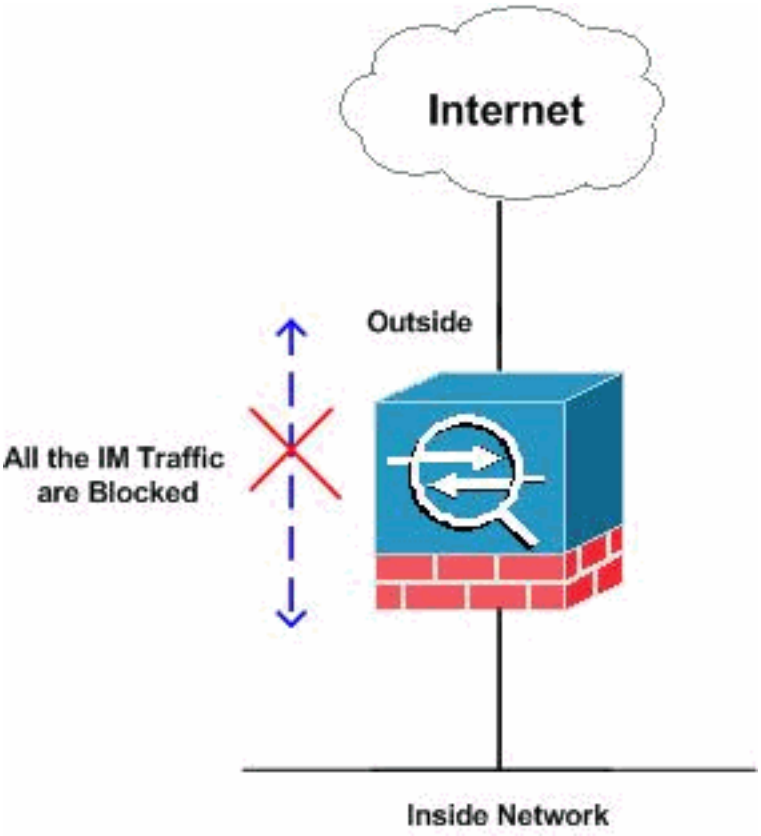
P2P 및 IM 트래픽 차단 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



PIX/ASA 7.0 및 7.1 구성

PIX/ASA 7.0 및 7.1에 대한 P2P 및 IM 트래픽 컨피그레이션 차단

```
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#
```

http map 명령과 연결된 다양한 매개변수에 대한 자세한 내용은 Cisco Security Appliance Command Line Configuration Guide의 Configuring an HTTP Map for Additional Inspection Control 섹션을 참조하십시오.

PIX/ASA 7.2 이상 컨피그레이션

참고: http-map 명령은 소프트웨어 버전 7.2 이상에서 사용되지 않습니다.따라서 **policy-map type inspect im** 명령을 사용하여 IM 트래픽을 차단해야 합니다.

PIX/ASA 7.2 이상에 대한 P2P 및 IM 트래픽 구성 차단

```
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#
```

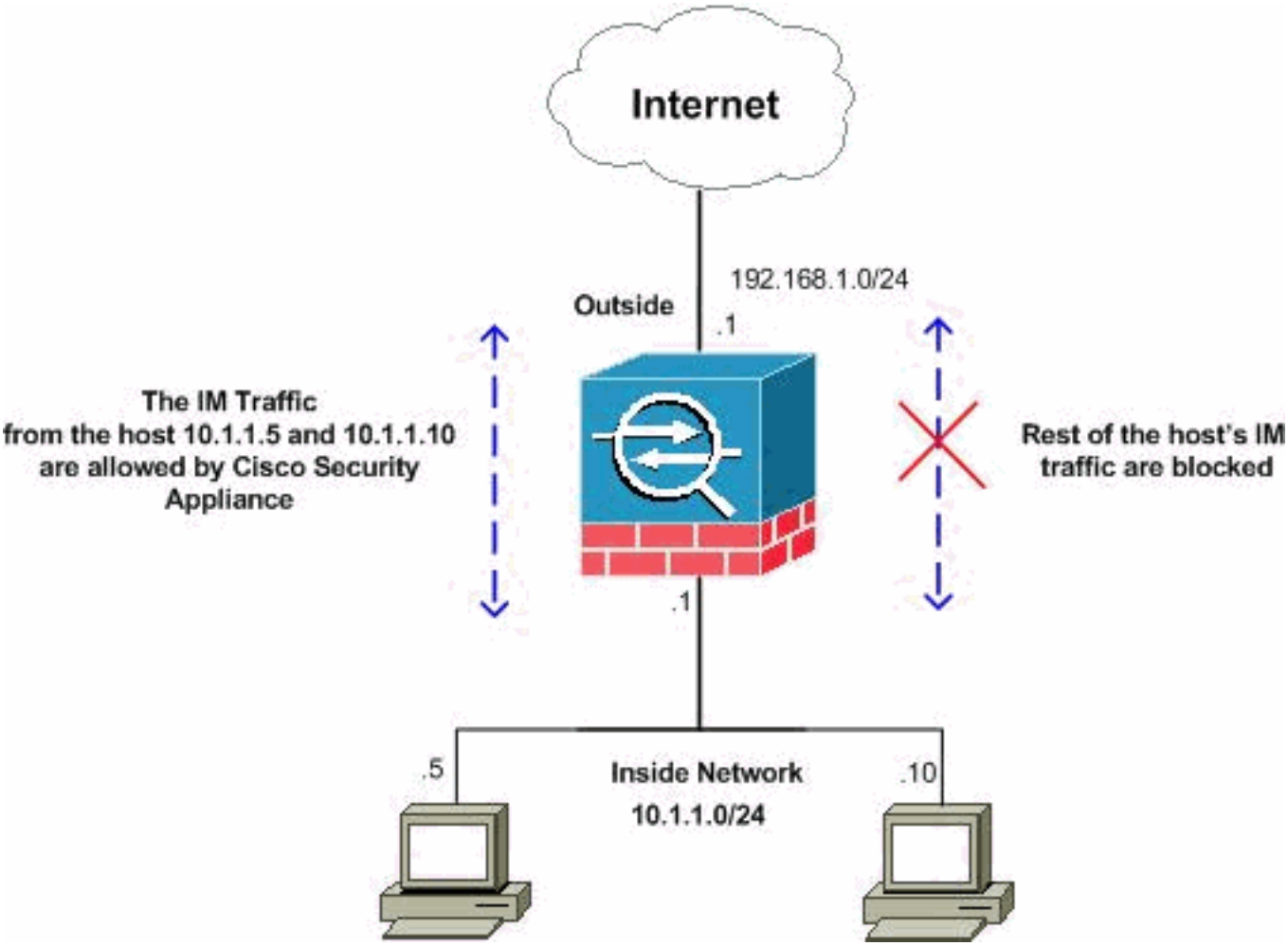
기본 제공 정규식 목록

```
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 이상:두 호스트가 IM 트래픽을 사용하도록 허용

이 섹션에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

호스트의 특정 수로부터 IM 트래픽을 허용하려면 표시된 대로 이 컨피그레이션을 완료해야 합니다.이 예에서는 내부 네트워크의 두 호스트 10.1.1.5 및 10.1.1.10이 MSN Messenger 및 Yahoo Messenger와 같은 IM 애플리케이션을 사용할 수 있습니다.그러나 다른 호스트의 IM 트래픽은 여전히 허용되지 않습니다.

2개의 호스트를 허용하는 PIX/ASA 7.2 이상의 IM 트래픽 구성

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show running-config http-map** - 구성된 HTTP 맵을 표시합니다.

```
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** - 모든 policy-map 컨피그레이션과 기본 policy-map 컨피그레이션을 표시합니다.

```
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
```

다음과 같이 이 명령의 옵션을 사용할 수도 있습니다.

```
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** - 클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

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

- **show running-config service-policy** - 현재 실행 중인 모든 서비스 정책 컨피그레이션을 표시합니다.

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

- **show running-config access-list** - 보안 어플라이언스에서 실행 중인 access-list 컨피그레이션을 표시합니다.

```
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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug im** - IM 트래픽에 대한 디버그 메시지를 표시합니다.
- **show service-policy** - 구성된 서비스 정책을 표시합니다.

```
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** - 액세스 목록에 대한 카운터를 표시합니다.

```
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
```

관련 정보

- Cisco 5500 Series ASA 지원 페이지
- Cisco PIX 500 Series 보안 어플라이언스 지원 페이지
- 기술 지원 및 문서 – Cisco Systems