PIX/ASA 7.x und höher: Blockieren des Peer-to-Peer- (P2P) und Instant Messaging-Datenverkehrs (IM) mithilfe des MPF-Konfigurationsbeispiels

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco Security Appliances PIX/ASA mithilfe von Modular Policy Framework (MPF) konfiguriert werden, um Peer-to-Peer (P2P)- und Instant Messaging (IM)-Datenverkehr wie MSN Messenger und Yahoo Messenger zu blockieren. Außerdem enthält dieses Dokument Informationen zur Konfiguration von PIX/ASA, damit die beiden Hosts IM-Anwendungen verwenden können, während der Rest der Hosts blockiert bleibt.

Hinweis: Die ASA kann Anwendungen vom Typ P2P nur blockieren, wenn der P2P-Datenverkehr über HTTP getunnelt wird. Außerdem kann ASA P2P-Datenverkehr verwerfen, wenn dieser über HTTP getunnelt wird.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die Cisco Security Appliance konfiguriert ist

und ordnungsgemäß funktioniert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance (ASA) der Serie 5500, die Softwareversion 7.0 und höher ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco PIX-Firewall der Serie 500 verwendet werden, die die Softwareversion 7.0 und höher ausführt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Übersicht über das modulare Richtlinien-Framework

MPF bietet eine konsistente und flexible Möglichkeit zur Konfiguration von Security Appliance-Funktionen. Beispielsweise können Sie mit MPF eine Timeout-Konfiguration erstellen, die für eine bestimmte TCP-Anwendung spezifisch ist, im Gegensatz zu einer Konfiguration, die für alle TCP-Anwendungen gilt.

MPF unterstützt folgende Funktionen:

- TCP-Normalisierung, TCP- und UDP-Verbindungsbeschränkungen und -Timeouts sowie Randomisierung der TCP-Sequenznummern
- CSC
- Anwendungsinspektion
- IPS
- QoS-Eingangsüberwachung
- QoS-Output-Policing
- QoS-Prioritätswarteschlange

Die MPF-Konfiguration umfasst vier Aufgaben:

1. Identifizieren Sie den Layer-3- und Layer-4-Datenverkehr, auf den Sie Aktionen anwenden möchten. Weitere Informationen finden Sie unter Identifizieren von Datenverkehr mithilfe einer Layer-3/4-Klassenzuordnung.
2. (Nur Anwendungsinspektion) Legen Sie besondere Aktionen für Anwendungsinspektionsverkehr fest. Weitere Informationen finden Sie unter Konfigurieren von Sonderaktionen für Anwendungsinspektionen.
3. Wenden Sie Aktionen auf den Layer-3- und Layer-4-Datenverkehr an. Weitere Informationen

finden Sie unter Definieren von Aktionen mithilfe einer Layer-3/4-Richtlinienzuordnung.

4. Aktivieren Sie die Aktionen auf einer Schnittstelle. Weitere Informationen finden Sie unter Anwenden einer Layer-3/4-Richtlinie auf eine Schnittstelle mithilfe einer Dienstrichtlinie.

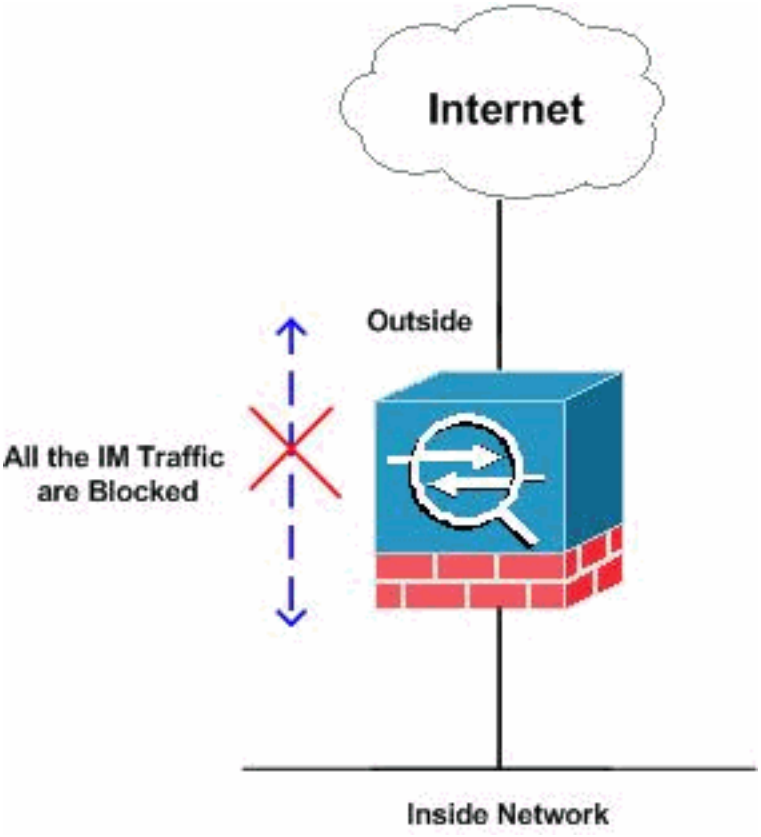
P2P- und IM-Datenverkehrsblockierung konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfiguration von PIX/ASA 7.0 und 7.1

P2P- und IM-Datenverkehrskonfiguration für PIX/ASA 7.0 und 7.1 blockieren

```
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#
```

Weitere Informationen über den Befehl **http map** und verschiedene zugeordnete Parameter finden Sie im Abschnitt Konfigurieren einer HTTP-Map für zusätzliche Inspektionskontrolle im Konfigurationsleitfaden zur Befehlszeilenkonfiguration der Cisco Security Appliance.

PIX/ASA 7.2 und spätere Konfiguration

Hinweis: Der Befehl **http-map** ist von der Softwareversion 7.2 und höher veraltet. Daher müssen Sie den Befehl **policy-map type inspect im** verwenden, um den IM-Datenverkehr zu blockieren.

P2P- und IM-Datenverkehrskonfiguration für PIX/ASA 7.2 und höher blockieren

```
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#
```

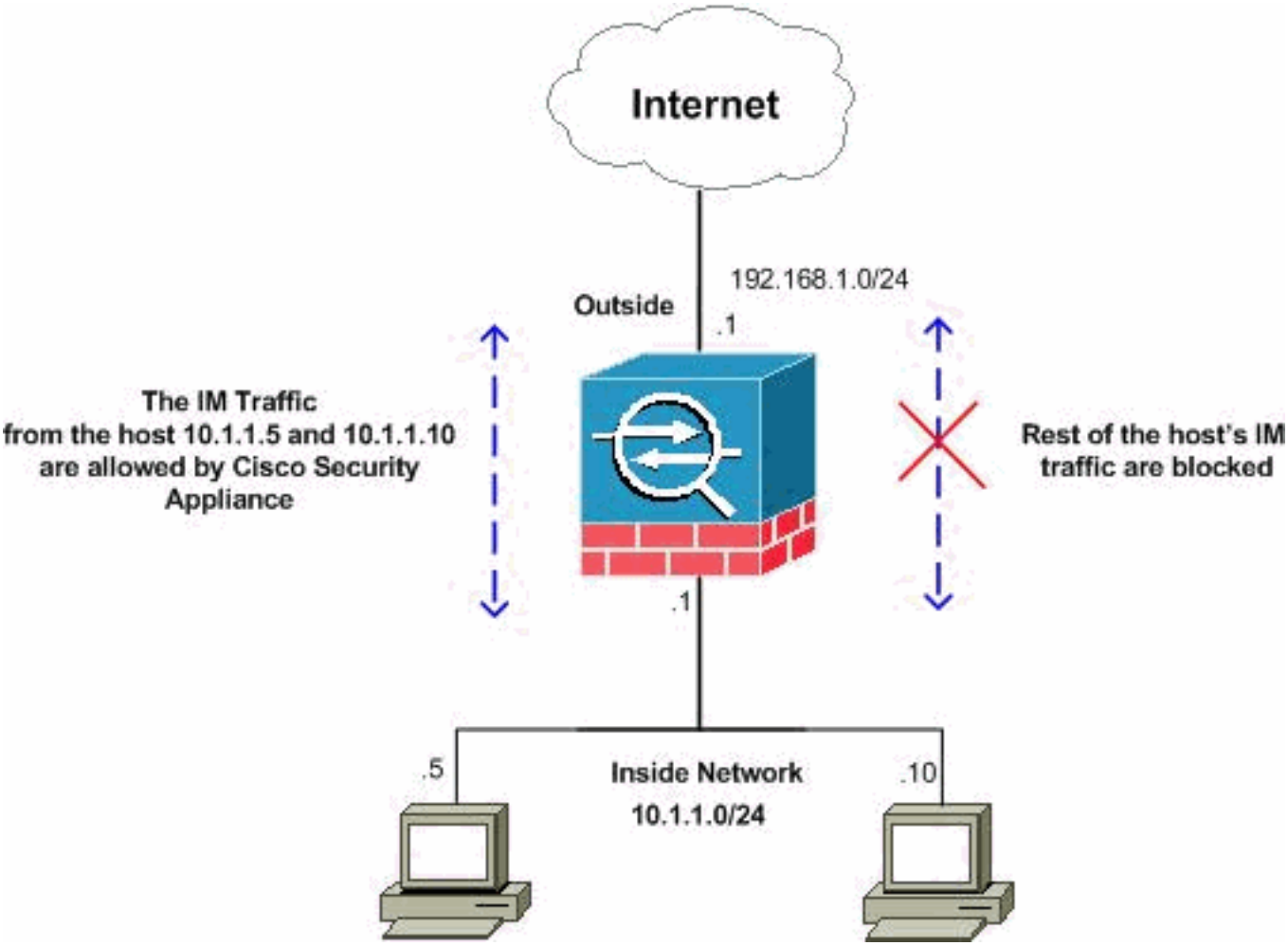
Liste der integrierten regulären Ausdrücke

```
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 und höher: Zwei Hosts dürfen den IM-Datenverkehr verwenden.

In diesem Abschnitt wird diese Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Dies sind RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Wenn Sie den IM-Datenverkehr von der bestimmten Anzahl der Hosts zulassen möchten, müssen Sie diese Konfiguration wie gezeigt abschließen. In diesem Beispiel dürfen die beiden Hosts

10.1.1.5 und 10.1.1.10 im internen Netzwerk die IM-Anwendungen wie MSN Messenger und Yahoo Messenger verwenden. Der IM-Datenverkehr von anderen Hosts ist jedoch weiterhin nicht zulässig.

IM-Datenverkehrskonfiguration für PIX/ASA 7.2 und höher für zwei 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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show running-config http-map**: Zeigt die konfigurierten HTTP-Maps an.
  ```
  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**: Zeigt alle Richtlinienzuordnungskonfigurationen sowie die Standardkonfiguration für Richtlinienzuweisungen an.
  ```
  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
```

Sie können die Optionen in diesem Befehl auch wie folgt verwenden:

```
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**: Zeigt Informationen über die Klassenzuordnungskonfiguration an.

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

- **show running-config service-policy**: Zeigt alle aktuell ausgeführten Servicerichtlinienkonfigurationen an.

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

- **show running-config access-list**: Zeigt die Zugriffslistenkonfiguration an, die auf der Sicherheits-Appliance ausgeführt wird.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Hinweis: Beachten Sie vor der Verwendung von **Debug**-Befehlen die Informationen zu Debug-Befehlen.

- **debug im**: Zeigt die Debug-Meldungen für IM-Datenverkehr an.
- **show service-policy**: Zeigt die konfigurierten Service-Richtlinien an.

```
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**: Zeigt die Zähler für eine Zugriffsliste an.

```
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
```

Zugehörige Informationen

- Support-Seite für Cisco ASA der Serie 5500
- Support-Seite für Cisco PIX Security Appliances der Serie 500
- Technischer Support und Dokumentation - Cisco Systems