PIX/ASA 7.x 以降： MPF を使用したピアツーピア（P2P）およびインスタント メッセージング（IM）トラフィックのブロックの設定例

目次

概要

この資料に Peer-to-Peer （P2P）およびインスタント メッセージを（IM）、MSN Messenger および Yahoo Messenger のような、内部ネットワークからのインターネットにトラフィック ブロックするためにモジュラ 政策の枠組（MPF）を使用して Ciscoセキュリティ アプライアンス PIX/ASA を設定する方法を記述されています。 また、この資料は方法でホストの他がブロックされての間、情報を 2 つのホストが IM アプリケーションを使用するように PIX/ASA を設定する提供したものです。

注: ASA は P2P トラフィックが HTTP によってトンネル伝送されるときだけ P2P 型アプリケーションをブロックできます。 また、ASA は HTTP によってトンネル伝送される場合 P2P トラフィックを廃棄できます。

前提条件

要件

このドキュメントは、Cisco セキュリティ アプライアンスが設定されていて、正常に動作していることを前提としています。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 7.0 以降が稼働する Cisco 5500 シリーズ Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定はまたと PIXファイアウォール ソフトウェア バージョン 7.0 およびそれ以降を実行する Cisco 500 シリーズ使用することができます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

モジュラ ポリシー フレームワークの概要

MPF を使用すると、一貫した柔軟な方法でセキュリティ アプライアンスの機能を設定できるようになります。 たとえば、MPF を使用してタイムアウトを設定すると、すべての TCP アプリケーションにではなく、特定の TCP アプリケーションに固有に適用できます。

MPF は次の機能をサポートします。

- TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化
- CSC
- アプリケーション検査
- IPS
- QoS 入力ポリシング
- QoS 出力ポリシング
- QoS プライオリティ キュー

MPF の設定は、次の 4 つの作業で構成されます。

1. アクションを適用するレイヤ 3 およびレイヤ 4 トラフィックを特定します。 詳細は、『レイヤ 3/4 クラス マップによるトラフィックの特定』を参照してください。
2. （アプリケーション検査のみ）アプリケーション検査トラフィックの特別なアクションを定義します。 詳細は、『アプリケーション検査のための特別なアクションの設定』を参照してください。
3. レイヤ 3 およびレイヤ 4 トラフィックにアクションを適用します。 詳細は、『レイヤ 3/4 ポリシー マップによるアクションの定義』を参照してください。
4. インターフェイスでアクションをアクティブにします。 詳細については、『サービス ポリシーによるインターフェイスへのレイヤ 3/4 ポリシーの適用』を参照してください。

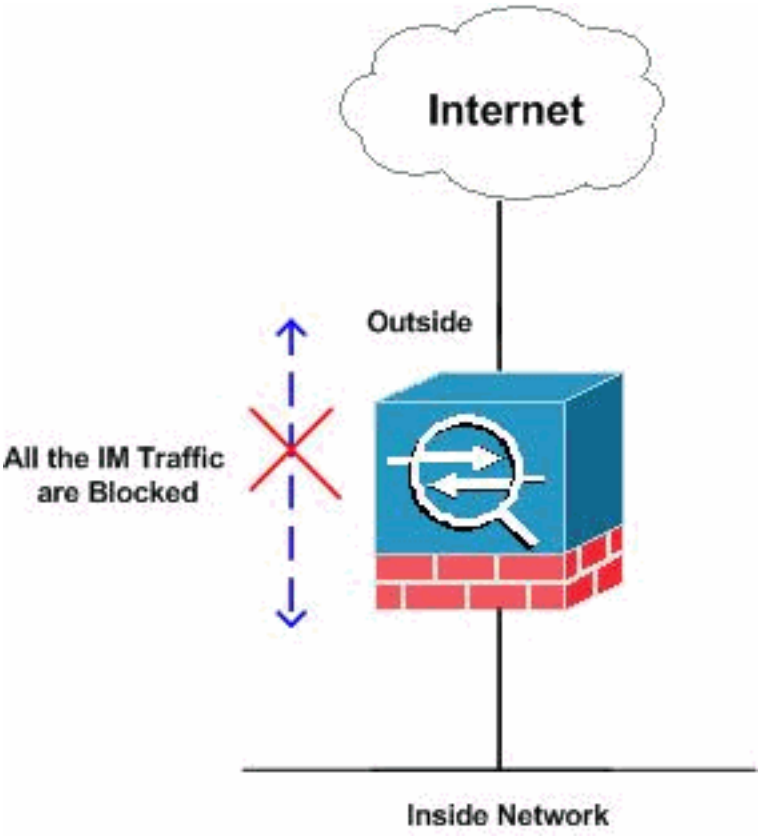
P2P および IM をトラフィック ブロッキング設定して下さい

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



PIX/ASA 7.0 および 7.1 設定

P2P 及び IM を PIX/ASA 7.0 および 7.1 のためのトラフィック 設定ブロックして下さい

```
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#
```

それと関連付けられる **http map コマンド**およびさまざまなパラメータに関する詳細については Ciscoセキュリティ アプライアンス コマンド・ライン コンフィギュレーション ガイドの追加インスペクション制御セクションのための HTTP マップの設定を参照して下さい。

PIX/ASA 7.2 およびそれ以降 設定

注: http MAP コマンドはソフトウェア バージョン 7.2 およびそれ以降から非難されます。 従って、IM トラフィックをブロックするために **policy-map 型 Inspect im** コマンドを使用する必要があります。

P2P 及び IM を PIX/ASA 7.2 およびそれ以降のためのトラフィック 設定ブロックして下さい

```
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#
```

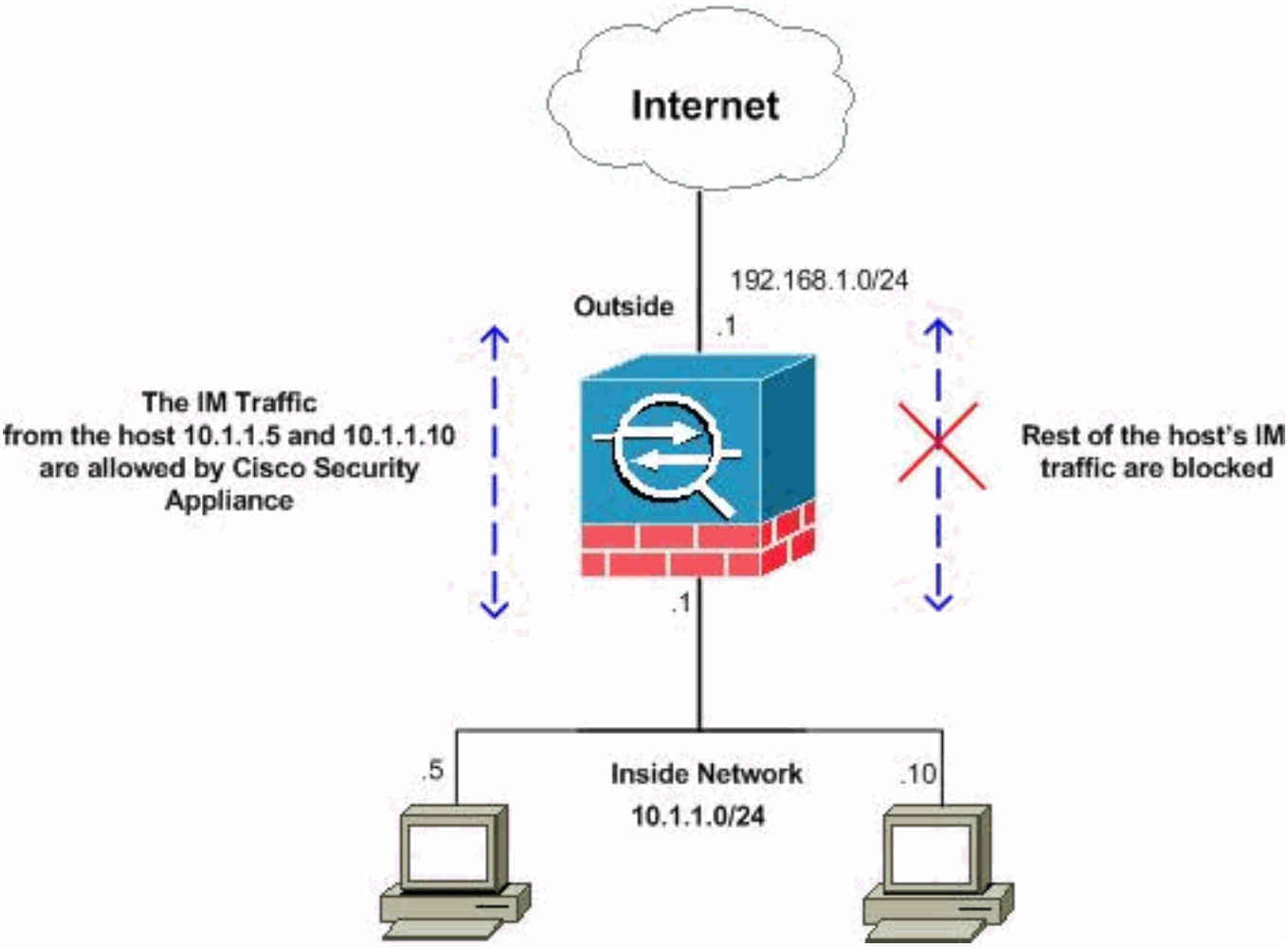
組み込み正規表現のリスト

```
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 およびそれ以降: 2 つのホストが IM トラフィックを使用するようにして下さい

このセクションでは、次のネットワーク設定を使用します。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 ラボ 環境で使用されたこれらは RFC 1918 アドレスです。

ホストの特定の数からの IM トラフィックを許可したいと思う場合示されているようにこの設定を完了する必要があります。 この例では、2 つのホスト 10.1.1.5 および内部ネットワークからの 10.1.1.10 は MSN Messenger および Yahoo Messenger のような IM アプリケーションを使用することができます。 ただし、他のホストからの IM トラフィックはまだ許可されません。

IM 2 つのホストを割り当てる PIX/ASA 7.2 およびそれ以降のためのトラフィック 設定

```
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
```

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show running-config http MAP** —設定された HTTP マップを示します。`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 は policy-map** —すべてのポリシーマップコンフィギュレーション、またデフォルト ポリシーマップコンフィギュレーションを表示します。`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` またここに示されているようにこのコマンドでオプションを使用できます:
  `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 は class-map** — クラスマップ 設定についての情報を表示する。`CiscoASA#`**`show running-config class-map`** `! class-map inspection_default match default-inspection-traffic class-map imblock match any`
- **show running-config は service-policy** —すべてに現在 サービス ポリシー コンフィギュレーションの実行を表示する。`CiscoASA#`**`show running-config service-policy`** `service-policy global_policy global service-policy imdrop interface outside`
- **show running-config は access-list** — セキュリティ アプライアンス モデルで動作しているアクセスリスト設定を表示します。`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`

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

注: debug コマンドを使用する前に、**『debug コマンドの重要な情報』**を参照してください。

- **デバッグ im** — IM トラフィックのためのデバッグ メッセージを表示します。
- **show service ポリシー**—設定されたサービス ポリシーを表示する。`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** — アクセス リストのためのカウンターを表示する。`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`

関連情報

- Cisco 5500 シリーズ ASA サポートページ
- Cisco PIX 500 シリーズ セキュリティ アプライアンス サポート ページ
- テクニカルサポートとドキュメント - Cisco Systems