PIX/ASA 7.x e versioni successive: Blocca il traffico peer-to-peer (P2P) e di messaggistica immediata (IM) utilizzando un esempio di configurazione MPF

Sommario

Introduzione

In questo documento viene descritto come configurare le appliance di sicurezza Cisco PIX/ASA con Modular Policy Framework (MPF) per bloccare il traffico peer-to-peer (P2P) e la messaggistica istantanea (IM), come MSN Messenger e Yahoo Messenger, dalla rete interna a Internet. Inoltre, questo documento fornisce informazioni su come configurare l'appliance PIX/ASA in modo da consentire ai due host di usare le applicazioni IM mentre gli altri host rimangono bloccati.

Nota: l'ASA può bloccare le applicazioni di tipo P2P solo se il traffico P2P viene tunneling tramite HTTP. Inoltre, l'ASA può eliminare il traffico P2P se viene tunneling tramite HTTP.

Prerequisiti

Requisiti

in questo documento si presume che Cisco Security Appliance sia configurato e funzioni

correttamente.

Componenti usati

Per la stesura del documento, è stata usata una appliance Cisco Adaptive Security Appliance (ASA) serie 5500 con software versione 7.0 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco serie 500 PIX firewall con software versione 7.0 e successive.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica del framework di criteri modulari

MPF offre un modo coerente e flessibile per configurare le funzionalità delle appliance di sicurezza. Ad esempio, è possibile utilizzare MPF per creare una configurazione di timeout specifica per una particolare applicazione TCP, a differenza di una configurazione che si applica a tutte le applicazioni TCP.

MPF supporta le seguenti funzionalità:

- normalizzazione TCP, limiti e timeout delle connessioni TCP e UDP e randomizzazione dei numeri di sequenza TCP
- CSC
- Ispezione delle applicazioni
- IPS
- Policy di input QoS
- Policy di output QoS
- Coda priorità QoS

La configurazione dell'MPF prevede quattro attività:

1. Identificare il traffico di layer 3 e 4 a cui si desidera applicare le azioni. per ulteriori informazioni, fare riferimento a Identificazione del traffico con una mappa delle classi del layer 3/4.
2. (Solo ispezione delle applicazioni) Definire azioni speciali per il traffico di ispezione delle applicazioni. per ulteriori informazioni, fare riferimento a Configurazione delle azioni speciali per le ispezioni delle applicazioni.
3. Applicare azioni al traffico di layer 3 e 4. per ulteriori informazioni, fare riferimento a

Definizione delle azioni mediante una mappa dei criteri di layer 3/4.

4. Attivare le azioni su un'interfaccia. Per ulteriori informazioni, fare riferimento a Applicazione di un criterio di layer 3/4 a un'interfaccia tramite un criterio di servizio.

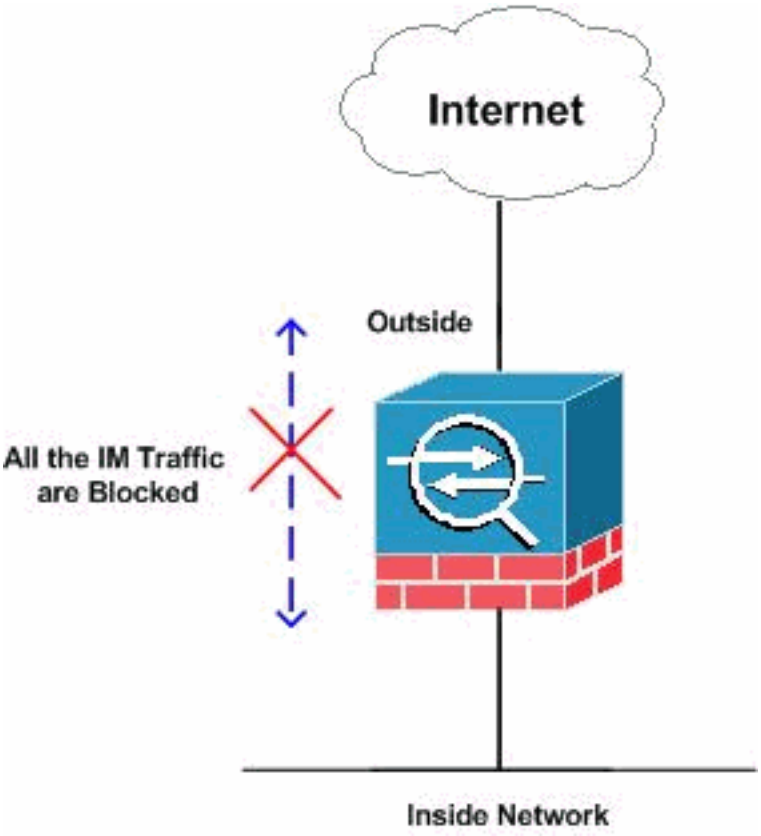
Configurare il blocco del traffico P2P e IM

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione PIX/ASA 7.0 e 7.1

Blocca la configurazione del traffico P2P e IM per PIX/ASA 7.0 e 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#
```

Per ulteriori informazioni sul comando **http map** e sui vari parametri associati, consultare la sezione Configurazione di una mappa HTTP per un controllo aggiuntivo dell'ispezione nella guida alla configurazione della riga di comando di Cisco Security Appliance.

Configurazione di PIX/ASA 7.2 e versioni successive

Nota: il comando **http-map** è obsoleto rispetto alla versione 7.2 e successive del software. Pertanto, è necessario utilizzare il comando **policy-map type inspect im** per bloccare il traffico IM.

Blocca la configurazione del traffico P2P e IM per PIX/ASA 7.2 e versioni successive

```
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#
```

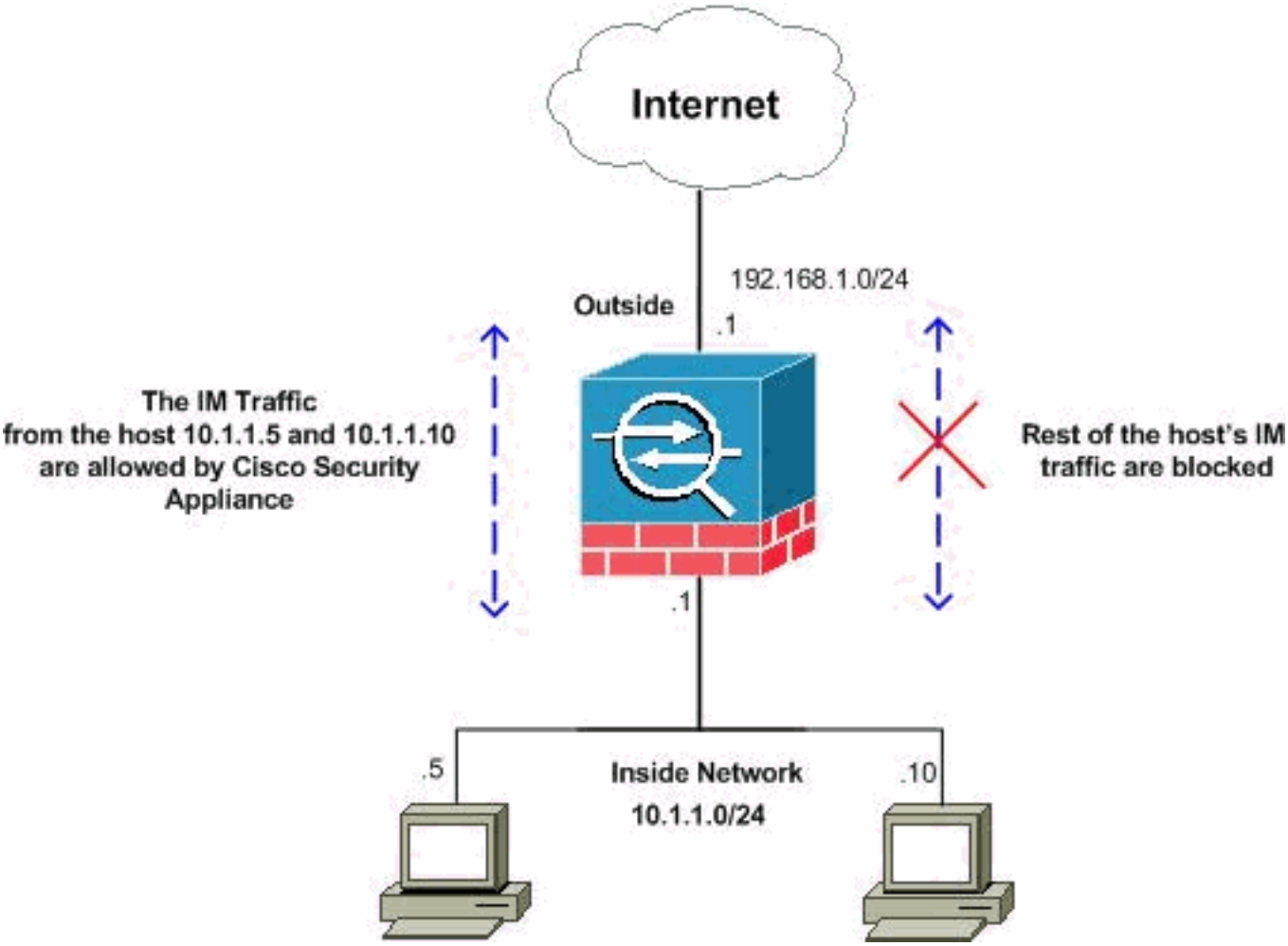
Elenco di espressioni regolari predefinite

```
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 e versioni successive: Consenti ai due host di utilizzare il traffico IM

Questa sezione utilizza questa configurazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Se si desidera consentire il traffico IM dal numero specifico di host, completare questa configurazione come mostrato. Nell'esempio, i due host 10.1.1.5 e 10.1.1.10 della rete interna

possono utilizzare le applicazioni di messaggistica istantanea, ad esempio MSN Messenger e Yahoo Messenger. Tuttavia, il traffico IM proveniente da altri host non è ancora consentito.

Configurazione del traffico IM per PIX/ASA 7.2 e versioni successive per consentire due host

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show running-config http-map**: visualizza le mappe HTTP configurate.
  ```
  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**: visualizza tutte le configurazioni della mappa dei criteri e la relativa configurazione predefinita.
  ```
  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
```

Èinoltre possibile utilizzare le opzioni di questo comando, come illustrato di seguito:

```
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**: visualizza le informazioni sulla configurazione della mappa delle classi.

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

- **show running-config service-policy**: visualizza tutte le configurazioni dei criteri del servizio attualmente in esecuzione.

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

- **show running-config access-list**: visualizza la configurazione dell'elenco degli accessi in esecuzione sull'appliance di sicurezza.

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug im**: visualizza i messaggi di debug per il traffico IM.
- **show service-policy**: visualizza i criteri di servizio configurati.

```
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**: visualizza i contatori per un elenco degli accessi.

```
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
```

Informazioni correlate

- Cisco serie 5500 ASA Support Page
- Cisco PIX serie 500 Security Appliance - Pagina di supporto
- Documentazione e supporto tecnico – Cisco Systems