Пример конфигурации "PIX/ASA 7.x и более поздние версияя: Блокировка Одноранговогo (P2P) и Instant Messaging (IM) трафика, используя MPF"

Содержание

Введение

В этом документе описана настройка устройств защиты Cisco PIX/ASA с использованием модульной системы политик (MPF) для блокирования выхода из внутренней сети в Интернет трафика одноранговых файлообменных сетей (P2P) и приложений мгновенного обмена сообщениями (IM), таких как MSN Messenger и Yahoo Messenger. Кроме того, здесь поясняется порядок настройки PIX/ASA для того, чтобы разрешить двум хостам использовать приложения мгновенного обмена сообщениями, в то время как остальная часть хостов остается блокированной.

Примечание: ASA может заблокировать приложения типа P2P, только если трафик P2P туннелируется через HTTP. ASA также позволяет отбрасывать трафик P2P в случае его туннелирования через HTTP.

Предварительные условия

Требования

В данном документе предполагается, что устройство защиты Cisco корректно настроено и работает нормально.

Используемые компоненты

Информация в этом документе касается устройств адаптивной защиты Cisco серии ASA 5500, работающих под управлением ПО версии 7.0 или более поздней версии.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Эту конфигурацию также можно использовать для устройств Cisco серии PIX 500, работающих под управлением ПО версии 7.0 или более поздней версии.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Обзор модульной системы политик

Модульная система политик (MPF) обеспечивает гибкий способ настройки параметров устройств защиты. Например, MPF можно использовать для создания конфигурации с ограничением по времени, которая является специфичной для определенного TCP-приложения, в отличие от конфигураций, применимых ко всем TCP-приложениям.

MPF поддерживает функции, перечисленные ниже:

- Нормализация TCP, ограничение числа и продолжительности TCP- и UDP-подключений, а также рандомизация порядкового номера TCP
- CSC
- Контроль трафика на прикладном уровне
- IPS
- Входной контроль QoS
- Выходной контроль QoS
- Очередь с приоритетом QoS

Настройка MPF включает следующие 4 задачи:

1. Определение трафика уровней 3 и 4, для которого требуется применить действия. Подробную информацию см. в документе Определение трафика с использованием карты классов уровней 3/4.
2. (Только при анализе трафика приложений) Определение специальных действий, необходимых для анализа трафика на прикладном уровне. Подробную информацию см. в документе Задание специальных действий для анализа трафика на прикладном уровне.

3. Применение действий к трафику 3-го и 4-го уровней. Подробную информацию см. в документе Определение действий с использованием карты политик уровней 3/4.
4. Активация действий на интерфейсе. Подробную информацию см. в документе Применение политики уровня 3/4 к интерфейсу с использованием служебной политики.

Настройка блокирования трафика P2P и IM

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурация PIX/ASA 7.0 и 7.1

Конфигурация для блокирования трафика P2P и IM в устройствах PIX/ASA 7.0 и 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#
```

Дополнительные сведения о команде http map и связанных с ней различных параметрах см. в разделе Настройка карты HTTP для дополнительного управления анализом в Руководстве

по настройке устройств защиты Cisco в командной строке версии 8.0.

Конфигурация PIX/ASA 7.2 и последующих версий

Примечание: Команда http-map осуждается от версии программного обеспечения 7.2 и позже. **Для блокирования трафика IM надлежит использовать команду policy-map type inspect im.**

Конфигурация для блокирования трафика P2P и IM в устройствах PIX/ASA 7.2 и последующих версий

```
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#
```

Список встроенных регулярных выражений

```
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 и последующие версии: Разрешение трафика IM для двух хостов

В данном разделе используются следующие настройки сети:

Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Чтобы разрешить трафик мгновенного обмена сообщениями от определенного количества хостов, необходимо выполнить настройку в соответствии с примером. В этом примере двум хостам из внутренней сети: 10.1.1.5 и 10.1.1.10 разрешено использовать приложения мгновенного обмена сообщениями, такие как MSN Messenger и Yahoo Messenger. При этом трафик мгновенного обмена сообщениями от других хостов по-прежнему запрещен.

Конфигурация для разрешения трафика IM для двух хостов в PIX/ASA 7.2 и последующих версиях

```
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
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **show running-config http-map— показывает настроенные карты HTTP.**`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 – данная команда показывает все конфигурации карт политик, а также конфигурации карт политик по умолчанию.**`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` Параметры в этой команде можно также использовать следующим образом:
  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— показывает сведения о конфигурации карты классов.**`CiscoASA#show running-config class-map ! class-map inspection_default match default-inspection-traffic class-map imblock match any`
- **show running-config service-policy — показывает все конфигурации политик обслуживания, действующие в данный момент.**`CiscoASA#show running-config service-policy service-policy global_policy global service-policy imdrop interface outside`
- **show running-config access-list— показывает конфигурацию списков контроля доступа, действующую в устройстве защиты.**`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`

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **debug im— показывает отладочные сообщения для трафика мгновенного обмена сообщениями.**
- **show service-policy— показывает настроенные политики обслуживания.**
```
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— показывает счетчики для списка контроля доступа.**
```
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
```

Дополнительные сведения

- Страница поддержки устройств адаптивной защиты Cisco серии 5500
- Страница поддержки устройств защиты Cisco PIX серии 500
- Cisco Systems – техническая поддержка и документация