ASA: Пример конфигурации для отправки трафика из ASA в AIP SSM

Содержание

Введение

Этот документ содержит пример конфигурации, предназначенной для отправки сетевого трафика, проходящего через устройство Cisco ASA 5500 в модуль AIP-SSM (IPS). Примерам конфигурации предоставляют интерфейс командной строки (CLI).

Документ ASA: Передайте Сетевой трафик от ASA до Примера конфигурации SSM CSC для передачи сетевого трафика от многофункционального устройства защиты Cisco ASA серии 5500 (ASA) к Модулю Сервисов безопасности Безопасности содержания и Контроля (SSM CSC).

См. Присвоение Действительных Датчиков к Контексту безопасности (Только SSM AIP) для получения дополнительной информации о том, как передать сетевой трафик, который проходит через многофункциональное устройство защиты Cisco ASA серии 5500 (ASA) в многоконтекстном режиме к Усовершенствованному Модулю Сервисов безопасности Контроля и Предотвращения (SSM AIP) (IPS) модуль.

Примечание: Сетевой трафик, который пересекает ASA, включает внутренних пользователей, которые обращаются к интернет-пользователям или интернет-пользователям, которые обращаются к ресурсам, защищенным ASA в демилитаризованной зоне (DMZ) или внутренняя сеть. Сетевой трафик, отправляемый в модуль ASA не отправляется в модуль IPS для проверки. В качестве примеров трафика, который не отправляется в модуль IPS, можно назвать эхо-запросы (ICMP), интерфейсы ASA или подключение к ASA по протоколу Telnet.

Примечание: Модульная Система политик, используемая ASA для классификации трафика для контроля, не поддерживает IPv6. Таким образом, при отклонении трафика IPv6 к SSM AIP через ASA это не поддерживается.

Примечание: Для получения дополнительной информации о начальной конфигурации SSM AIP обратитесь к Начальной конфигурации Датчика SSM AIP.

Предварительные условия

Требования

Этот документ предполагает, что у аудитории есть основное понимание того, как настроить версию программного обеспечения 8.x Cisco ASA и версию программного обеспечения 6 IPS. x.

- Компоненты необходимой конфигурации для ASA 8.x включают интерфейсы, access-lists, технологию NAT и маршрутизацию.
- Компоненты необходимой конфигурации для SSM AIP (программное обеспечение IPS 6.x) включают сетевую установку, позволенную хосты, конфигурацию интерфейса, определения подписи и правила действия события.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- ASA 5510 с версией программного обеспечения 8.0.2
- AIP-SSM-10 с версией программного обеспечения 6.1.2 IPS

Примечание: Этот пример конфигурации совместим с любым Межсетевым экраном серии 5500 Cisco ASA с ОС 7.x и позже и модуль SSM AIP с IPS 5.x и позже.

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.

Условные обозначения

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

Настройка

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

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

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

Схема сети

В настоящем документе используется следующая схема сети:

Начальные конфигурации

Эти конфигурации используются в данном документе. Модули ASA и AIP-SSM запущены со стандартной конфигурацией, в которую внесены определенные изменения для целей тестирования. Дополнения указаны в конфигурации.

- ASA 5510
- SSM AIP (IPS)

ASA 5510

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa enable password
2KFQnbNIdI.2KYOU encrypted names ! !--- IP addressing is
added to the default configuration. interface
Ethernet0/0 nameif outside security-level 0 ip address
172.16.1.254 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 10.2.2.254
255.255.255.0 ! interface Ethernet0/2 nameif dmz
security-level 50 ip address 192.168.1.254 255.255.255.0
! interface Management0/0 nameif management security-
level 0 ip address 172.22.1.160 255.255.255.0
management-only ! passwd 9jNfZuG3TC5tCVH0 encrypted ftp
mode passive !--- Access lists are added in order to
allow test !--- traffic (ICMP and Telnet). access-list
acl_outside_in extended permit icmp any host 172.16.1.50
access-list acl_inside_in extended permit ip 10.2.2.0
255.255.255.0 any access-list acl_dmz_in extended permit
icmp 192.168.1.0 255.255.255.0 any pager lines 24 !---
Logging is enabled. logging enable logging buffered
debugging mtu outside 1500 mtu inside 1500 mtu dmz 1500
mtu management 1500 asdm image disk0:/asdm-613.bin no
asdm history enable arp timeout 14400 !--- Translation
rules are added. global (outside) 1 172.16.1.100 global
(dmz) 1 192.168.1.100 nat (inside) 1 10.2.2.0
255.255.255.0 static (dmz,outside) 172.16.1.50
192.168.1.50 netmask 255.255.255.255 static (inside,dmz)
10.2.2.200 10.2.2.200 netmask 255.255.255.255 !---
Access lists are applied to the interfaces. access-group
acl_outside_in in interface outside access-group
acl_inside_in in interface inside access-group
acl_dmz_in in interface dmz 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 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute http
server enable http 0.0.0.0 0.0.0.0 dmz no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart telnet
timeout 5 ssh timeout 5 console timeout 0 ! 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 !---
Out-of-the-box default configuration includes !---
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 !--- Out-of-the-box default
configuration includes !--- the service-policy
global_policy applied globally. prompt hostname context
. : end
```

SSM AIP (IPS)

```
AIP-SSM#show configuration ! ----------------------------
--- ! Version 6.1(2) ! Current configuration last
modified Mon Mar 23 21:46:47 2009 ! --------------------
---------- service interface exit ! --------------------
---------- service analysis-engine virtual-sensor vs0
physical-interface GigabitEthernet0/1 exit exit ! ------
------------------------ service authentication exit ! -
---------------------------- service event-action-rules
rules0 !--- The variables are defined. variables DMZ
address 192.168.1.0-192.168.1.255 variables IN address
10.2.2.0-10.2.2.255 exit ! -----------------------------
- service host network-settings !--- The management IP
address is set. host-ip 172.22.1.169/24,172.22.1.1 host-
name AIP-SSM telnet-option disabled access-list
x.x.0.0/16 !--- The access list IP address is removed
from the configuration !--- because the specific IP
address is not relevant to this document. exit time-
zone-settings offset -360 standard-time-zone-name GMT-
06:00 exit summertime-option recurring offset 60
summertime-zone-name UTC start-summertime month april
week-of-month first day-of-week sunday time-of-day
02:00:00 exit end-summertime month october week-of-month
last day-of-week sunday time-of-day 02:00:00 exit exit
exit ! ------------------------------ service logger
exit ! ------------------------------ service network-
access exit ! ------------------------------ service
notification exit ! ------------------------------
service signature-definition sig0 !--- The signature is
modified from the default setting for testing purposes.
signatures 2000 0 alert-severity high engine atomic-ip
event-action produce-alert|produce-verbose-alert exit
alert-frequency summary-mode fire-all summary-key AxBx
exit exit status enabled true exit exit !--- The
signature is modified from the default setting for
testing purposes. signatures 2004 0 alert-severity high
engine atomic-ip event-action produce-alert|produce-
verbose-alert exit alert-frequency summary-mode fire-all
summary-key AxBx exit exit status enabled true exit exit
!--- The custom signature is added for testing purposes.
signatures 60000 0 alert-severity high sig-fidelity-
```

```
rating 75 sig-description sig-name Telnet Command
Authorization Failure sig-string-info Command
authorization failed sig-comment signature triggers
string command authorization failed exit engine atomic-
ip specify-l4-protocol yes l4-protocol tcp no tcp-flags
no tcp-mask exit specify-payload-inspection yes regex-
string Command authorization failed exit exit exit exit
exit ! ----------------------------- service ssh-known-
hosts exit ! ----------------------------- service
trusted-certificates exit ! ----------------------------
-- service web-server enable-tls true exit AIP-SSM#
```

Примечание: Если вы - неспособный доступ модуль SSM AIP с https, то выполняете эти шаги:

- Настройте управление IP-адресами для модуля. И можно настроить `network access list`, в котором вы задаете IPS/IP - СЕТИ, которым позволяют соединиться с IP - управлением.
- Удостоверьтесь, что вы подключили внешний Интерфейс Ethernet модуля AIP. Управляющий доступ к модулю AIP возможен через этот интерфейс только.

См. Инициализацию SSM AIP для получения дополнительной информации.

Осмотрите Весь Трафик с SSM AIP во встроенном или разнородном режиме

Администраторы сети и высшее руководство компании часто указывают, что все должно быть проверено. Эта конфигурация удовлетворяет потребность во всеобъемлющем мониторинге. В дополнению к всеобъемлющему мониторингу, необходимо принять два решения о способе взаимодействия ASA и AIP-SSM.

- Будет ли AIP-SSM функционировать или развертываться в случайном или внутриканальном режиме?Случайный режим означает, что копия данных будет отправляться модулю AIP-SSM, в то время как ASA пересылает исходные данные по месту назначения. Модуль AIP-SSM в случайном режиме можно рассматривать как систему обнаружения несанкционированного доступа (IDS). В этом режиме пакет, который вызвал тревогу, может достичь места назначения. Может включиться защита, которая помешает последующим пакетам достичь места назначения, но первый пакет, вызвавший тревогу, остановлен не будет.Внутриканальный режим означает, что модуль ASA передает данные в модуль AIP-SSM для проверки. Если данные проходят проверку AIP-SSM, они возвращаются в модуль ASA для продолжения обработки и отправки по месту назначения. Модуль AIP-SSM во внутриканальном режиме можно рассматривать как систему предотвращения несанкционированного доступа (IPS). В отличие от случайного режима, внутриканальный режим (IPS) может остановить пакет, вызвавший тревогу, на пути к месту назначения.
- В ситуации, когда модулю ASA не удается связаться с модулем AIP-SSM, как ему следует обрабатывать трафик, предназначенный для проверки? Примеры ситуаций, в которых модуль ASA не может связаться с AIP-SSM: перезагрузка AIP-SSM, модуль отказал и нуждается в замене. В этом случае ASA может работать в режимах "fail-open" или "fail-closed".Режим "Fail-open" позволяет модулю ASA продолжить передачу трафика, подлежащего проверке, в окончательное место назначения, если модуль AIP-SSM недоступен.Режим "Fail-closed" блокирует трафик, подлежащий проверке, если модуль ASA не может связаться с модулем AIP-SSM.**Примечание:** Осмотренный

будущим образом трафик определен с использованием access-list. В этом примере выходных данных список доступа разрешает весь IP-трафик от любого источника к любому месту назначения. Поэтому трафик, подлежащий проверке — это любой трафик, проходящий через модуль ASA.

```
ciscoasa(config)#access-list traffic_for_ips permit ip any any ciscoasa(config)#class-map
ips_class_map ciscoasa(config-cmap)#match access-list traffic_for_ips !--- The match any command
can be used in place of !--- the match access-list [access-list name] command. !--- In this
example, access-list traffic_for_ips permits !--- all traffic. The match any command also !---
permits all traffic. You can use either configuration. !--- When you define an access-list, it
can ease troubleshooting. ciscoasa(config)#policy-map global_policy !--- Note that policy-map
global_policy is a part of the !--- default configuration. In addition, policy-map global_policy
!--- is applied globally with the service-policy command. ciscoasa(config-pmap)#class
ips_class_map ciscoasa(config-pmap-c)#ips inline fail-open !--- Two decisions need to be made.
!--- First, does the AIP-SSM function !--- in inline or promiscuous mode? !--- Second, does the
ASA fail-open or fail-closed? ciscoasa(config-pmap-c)#ips promiscous fail-open !--- If AIP-SSM
is in promiscous mode, issue !--- the no ips promiscous fail-open command !--- in order to
negate the command and then use !--- the ips inline fail-open command.
```

Осмотрите Весь Трафик с SSM AIP с помощью ASDM

Выполните эти шаги для осмотра всего трафика с SSM AIP, который использует ASDM:.

1. Выберите **Configuration> IPS> Sensor Setup>** домашняя страница **Startup Wizard in ASDM** для начала конфигурации, как показано:
2. Нажмите **Launch Startup Wizard**.
3. Нажмите **Next** в новом окне, которое подходит после запуска мастера запуска.
4. В новом окне предоставьте Имя хоста, IP-адрес, Маску подсети и Адрес шлюза по умолчанию для модуля SSM AIP в соответствующем пространстве, предоставленном под разделом Настроек сети. Затем **нажмите Add** для добавления access-lists для разрешения всего трафика с SSM AIP.
5. В **Add ACL Entry** окно предоставляют **IP-адрес** и подробные данные **Маски сети** хостов/сетей, которым позволят обратиться к датчику. **Нажмите кнопку ОК.Примечание:** Хост/сетевой IP - адрес должен принадлежать диапазону адресов Сети управления.
6. Нажмите **Next** после того, как вы предоставите подробную информацию в соответствующих предоставленных пробелах.
7. **Нажмите Add** для настройки подробных данных выделения трафика.
8. Предоставьте источник и целевой сетевой адрес и также тип сервиса, например, IP используется здесь. В данном примере **любой** используется для источника и назначения, поскольку вы осматриваете весь трафик с SSM AIP. **Затем нажмите кнопку ОК.**
9. Настроенные правила Выделения Трафика показывают в этом окне, и можно добавить столько правил по мере необходимости при завершении той же процедуры сколько объясненный в шагах 7 и 8. Затем нажмите **Finish**, и это завершает Процедуру настройки ASDM.**Примечание:** Если вы **нажимаете кнопку Старт,** можно просмотреть анимацию потока пакетов.

Проверка определенных типов трафика с помощью AIP-SSM

Если администратор сети хочет иметь монитор SSM AIP как подмножество всего трафика, ASA имеет две независимых переменные, которые могут модифицироваться. Во-первых,

access-list может быть записан, чтобы включать или исключить необходимый трафик. В дополнение к модификации access-lists **стратегия обслуживания** может быть применена к интерфейсу или глобально для изменения трафика, осмотренного SSM AIP.

Рассмотрим сетевую диаграмму, приведенную в этом документе. Администратор сети хочет, чтобы модуль AIP-SSM проверял весь трафик между внешней сетью и сетью DMZ.

```
ciscoasa#configure terminal ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0
255.255.255.0 192.168.1.0 255.255.255.0 ciscoasa(config)#access-list traffic_for_ips permit ip
any 192.168.1.0 255.255.255.0 ciscoasa(config)#access-list traffic_for_ips deny ip 192.168.1.0
255.255.255.0 10.2.2.0 255.255.255.0 ciscoasa(config)#access-list traffic_for_ips permit ip
192.168.1.0 255.255.255.0 any ciscoasa(config)#class-map ips_class_map ciscoasa(config-
cmap)#match access-list traffic_for_ips ciscoasa(config)#policy-map interface_policy
ciscoasa(config-pmap)#class ips_class_map ciscoasa(config-pmap-c)#ips inline fail-open
ciscoasa(config)#service-policy interface_policy interface dmz !--- The access-list denies
traffic from the inside network to the DMZ network !--- and traffic to the inside network from
the DMZ network. !--- In addition, the service-policy command is applied to the DMZ interface.
```

Далее, сетевому администратору необходимо, чтобы модуль AIP-SSM отслеживал трафик, инициированный во внутренней сети и предназначенный для отправки во внешнюю сеть. Трафик между внутренней сетью и DMZ не отслеживается.

Примечание: Этот определенный раздел требует промежуточного понимания с отслеживанием состояния, TCP, UDP, ICMP, соединения и передач без установки соединения.

```
ciscoasa#configure terminal ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0
255.255.255.0 192.168.1.0 255.255.255.0 ciscoasa(config)#access-list traffic_for_ips permit ip
10.2.2.0 255.255.255.0 any ciscoasa(config)#class-map ips_class_map ciscoasa(config-cmap)#match
access-list traffic_for_ips ciscoasa(config)#policy-map interface_policy ciscoasa(config-
pmap)#class ips_class_map ciscoasa(config-pmap-c)#ips inline fail-open ciscoasa(config)#service-
policy interface_policy interface inside
```

Список доступа отклоняет трафик, инициированный во внутренней сети и предназначенный для отправки в сеть DMZ. Вторая строка списка доступа разрешает отправку трафика, инициированного во внутренней сети и предназначенного для отправки во внешнюю сеть через AIP-SSM. В этот момент активируется функция Statefulness модуля ASA. Например, внутренний пользователь инициирует TCP-подключение (Telnet) к устройству во внешней сети (маршрутизатор). Пользователь успешно подключается к маршрутизатору и выполняет вход. Затем пользователь вводит неавторизованную команду. `Command authorizaton failed ( )`. Пакет данных, который содержит строка, имеет источник внешнего маршрутизатора и назначение внутреннего пользователя. Источник (внешний) и назначение (внутреннее) не соответствуют списку доступа, приведенному в этом документе. ASA отслеживает соединения с отслеживанием состояния, из-за этого пакет данных, который возвращается (снаружи к внутренней части) передается SSM AIP для контроля. Пользовательская подпись 60000 0, которая настроена на SSM AIP, сигналах тревоги.

Примечание: По умолчанию ASA не поддерживает состояние для трафика ICMP. В предыдущем примере конфигурации, внутренний пользователь отправляет эхо-запрос (эхо-запрос ICMP) внешнему маршрутизатору. Маршрутизатор возвращает эхо-ответ ICMP. Модуль AIP-SSM проверяет пакет эхо-запроса, но не пакет эхо-ответа. Если проверка ICMP включена в модуле ASA, в модуле AIP-SSM проверяются пакеты эхо-запроса и эхо-ответа.

Исключите определенный сетевой трафик из сканирования SSM AIP

Данный обобщенный пример предоставляет представление об освобождении определенного трафика, который будет просмотрен SSM AIP. Для выполнения этого

необходимо создать access-list, который содержит трафик, который должен быть исключен из сканирования SSM AIP в инструкции deny. В данном примере IPS является названием access-list, которые определяют трафик, который будет просмотрен SSM AIP. Трафик между <source> и <назначением> исключен из сканирования; весь другой трафик осмотрен.

```
access-list IPS deny IP <source> <destination>
access-list IPS permit ip any any
!
class-map my_ips_class
  match access-list IPS
!
!
policy-map my-ids-policy
  class my-ips-class
   ips inline fail-open
```

Проверка

Убедитесь, что предупреждения записываются в AIP-SSM.

Войдите в систему AIP-SSM с помощью учетной записи администратора. **Команда show events alert генерирует следующие выходные данные.**

Примечание: Выходные данные варьируются на основе параметров настройки подписи, тип трафика, передаваемый SSM AIP и сетевой нагрузке.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Используйте OIT для просмотра анализа выходных данных команды show.**

```
show events alert evIdsAlert: eventId=1156198930427770356 severity=high vendor=Cisco originator:
hostId: AIP-SSM appName: sensorApp appInstanceId: 345 time: 2009/03/23 22:52:57 2006/08/24
17:52:57 UTC signature: description=Telnet Command Authorization Failure id=60000 version=custom
subsigId: 0 sigDetails: Command authorization failed interfaceGroup: vlan: 0 participants:
attacker: addr: locality=OUT 172.16.1.200 port: 23 target: addr: locality=IN 10.2.2.200 port:
33189 riskRatingValue: 75 interface: ge0_1 protocol: tcp evIdsAlert: eventId=1156205750427770078
severity=high vendor=Cisco originator: hostId: AIP-SSM appName: sensorApp appInstanceId: 345
time: 2009/03/23 23:46:08 2009/03/23 18:46:08 UTC signature: description=ICMP Echo Request
id=2004 version=S1 subsigId: 0 interfaceGroup: vlan: 0 participants: attacker: addr:
locality=OUT 172.16.1.200 target: addr: locality=DMZ 192.168.1.50 triggerPacket: 000000 00 16 C7
9F 74 8C 00 15 2B 95 F9 5E 08 00 45 00 ....t...+..^..E. 000010 00 3C 2A 57 00 00 FF 01 21 B7 AC
10 01 C8 C0 A8 .<*W....!..... 000020 01 32 08 00 F5 DA 11 24 00 00 00 01 02 03 04 05
.2.....$........ 000030 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 ..... 000040
16 17 18 19 1A 1B 1C 1D 1E 1F .......... riskRatingValue: 100 interface: ge0_1 protocol: icmp
evIdsAlert: eventId=1156205750427770079 severity=high vendor=Cisco originator: hostId: AIP-SSM
appName: sensorApp appInstanceId: 345 time: 2009/03/23 23:46:08 2009/03/23 18:46:08 UTC
signature: description=ICMP Echo Reply id=2000 version=S1 subsigId: 0 interfaceGroup: vlan: 0
participants: attacker: addr: locality=DMZ 192.168.1.50 target: addr: locality=OUT 172.16.1.200
triggerPacket: 000000 00 16 C7 9F 74 8E 00 03 E3 02 6A 21 08 00 45 00 ....t.....j!..E. 000010 00
3C 2A 57 00 00 FF 01 36 4F AC 10 01 32 AC 10 .<*W....6O...2.. 000020 01 C8 00 00 FD DA 11 24 00
00 00 01 02 03 04 05 .......$........ 000030 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15
..... 000040 16 17 18 19 1A 1B 1C 1D 1E 1F .......... riskRatingValue: 100 interface:
ge0_1 protocol: icmp
```

В примерах конфигурации несколько сигнатур IPS настроены на генерацию сигналов тревоги для тестового трафика. Сигнатуры 2000 и 2004 изменены. Добавлена пользовательская сигнатура 60000. В лабораторной среде или сети, куда небольшие данные проходят через ASA, может быть необходимо модифицировать подписи для

инициирования событий. Если модули ASA и AIP-SSM развертываются в среде, через которую проходят большие объемы данных, стандартные сигнатуры скорее всего смогут генерировать события.

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Используйте OIT для просмотра анализа выходных данных команды show.**

Выполните эти **команды показа** от ASA.

- **show module** информацию о SSM на ASA, а также сведениях о системе.`ciscoasa#show module Mod Card Type Model Serial No. --- ---------- ----- ------------ ----------- 0 ASA 5510 Adaptive Security Appliance ASA5510 JMX0935K040 1 ASA 5500 Series Security Services Module-10 ASA-SSM-10 JAB09440271 Mod MAC Address Range Hw Version Fw Version Sw Version --- ---------- ----------- ----------- ---------- 0 0012.d948.e912 to 0012.d948.e916 1.0 1.0(10)0 8.0(2) 1 0013.c480.cc18 to 0013.c480.cc18 1.0 1.0(10)0 6.1(2)E3 Mod SSM Application Name Status SSM Application Version --- ---------- ---------- ---------- 1 IPS Up 6.1(2)E3 Mod Status Data Plane Status Compatibility --- ---------- ---------- ---------- 0 Up Sys Not Applicable 1 Up Up !--- Each of the areas highlighted indicate that !--- the ASA recognizes the AIP-SSM and the AIP-SSM status is up.`
- **show run**`ciscoasa#show run !--- Output is suppressed. access-list traffic_for_ips extended permit ip any any ... class-map ips_class_map match access-list traffic_for_ips ... policy-map global_policy ... class ips_class_map ips inline fail-open ... service-policy global_policy global !--- Each of these lines are needed !--- in order to send data to the AIP-SSM.`
- **show access-list. Отображает счетчики списка доступа.**`ciscoasa#show access-list traffic_for_ips access-list traffic_for_ips; 1 elements access-list traffic_for_ips line 1 extended permit ip any any (hitcnt=2) 0x9bea7286 !--- Confirms the access-list displays a hit count greater than zero.`

Перед установкой и использованием модуля AIP-SSM, убедитесь, что трафик проходит через модуль ASA в соответствии с вашими ожиданиями? В противном случае может быть необходимо устранить неполадки сети и правил политики доступа ASA.

Проблемы аварийного переключения

- **Если в вашей среде установлено два модуля ASA в конфигурации аварийного переключения и каждый из них имеет модуль AIP-SSM, необходимо вручную реплицировать конфигурацию AIP-SSM.** Механизм аварийного переключения реплицирует только конфигурацию ASA. Модуль AIP-SSM не участвует в аварийном переключении. См. PIX/ASA 7.x Активный/Резервный Пример Конфигурации аварийного переключения для получения дополнительной информации о проблемах Аварийного переключения.
- Модуль AIP-SSM не участвует в аварийном переключении с поддержкой stateful, если конфигурация этого аварийного переключения настроена на паре аварийного переключения ASA.

Сообщения об ошибках

Модуль ips (SSM AIP) производит сообщения об ошибках как показано и не увольнение событий.

```
07Aug2007 18:59:50.468 0.757 interface[367] Cid/W errWarning Inline
data bypass has started.

  07Aug2007 18:59:59.619 9.151 mainApp[418] cplane/E Error during socket
read

  07Aug2007 19:03:13.219 193.600 nac[373] Cid/W errWarning New host ip
[192.168.101.76]

  07Aug2007 19:06:13.979 180.760 sensorApp[417] Cid/W errWarning
unspecifiedWarning:There are no interfaces assigned to any virtual
sensors. This can result in some packets not being monitored.

  07Aug2007 19:08:42.713 148.734 mainApp[394] cplane/E Error - accept()
call returned -1

  07Aug2007 19:08:42.740 0.027 interface[367] Cid/W errWarning Inline
data bypass has started.
```

Причина для этого сообщения об ошибках состоит в том, что IPS действительный датчик не был назначен на интерфейс объединительной платы ASA. ASA является настройкой корректным способом для передачи трафика к модулю SSM, но необходимо назначить действительный датчик на интерфейс объединительной платы, который ASA создает для SSM для сканирования трафика.

```
errorMessage: IpLogProcessor::addIpLog: Ran out of file descriptors  name=errWarn

errorMessage: IpLog 1701858066 terminated early due to lack of file handles.
name=ErrLimitExceeded
```

Эти сообщения показательны из включаемой РЕГИСТРАЦИИ IP, который в свою очередь hogged все ресурсы системы. Cisco рекомендует отключить РЕГИСТРАЦИЮ IP, поскольку это должно только использоваться в целях устранения проблем / следственных целях только.

Примечание: `errWarning` сообщение об ошибках, является нормальным поведением, поскольку датчик на мгновение перезапускает аналитический механизм после обновления подписи, которое является необходимой частью процесса обновления подписи.

Поддержка системного журнала

SSM AIP не поддерживает системный журнал как аварийный формат.

Способ по умолчанию для получения аварийной информации от SSM AIP через стандарт Security Device Event Exchange (SDEE). Другая опция должна настроить отдельные подписи для генерации trap-сообщения SNMP как действия для взятия, когда они инициированы.

Перезагрузка SSM AIP

Модуль SSM AIP не отвечает должным образом.

Если модуль SSM AIP не отвечает должным образом, то перезагрузка модуль SSM AIP, не

перезагружая ASA. Используйте команду повторной загрузки модуля 1 hw-module для перезагрузки модуля SSM AIP, и не перезагружайте ASA.

Предупреждение электронной почты SSM AIP

SSM AIP может передать почтовые предупреждения пользователям?

Нет, это не поддерживается.

Дополнительные сведения

- Справочник по командам Cisco Security Appliance, версия 7.2
- Сообщения журнала системы Cisco Security Appliance, версия 7.2
- Справочник по командам для системы предотвращения вторжений Cisco (IPS) 5.1
- Cisco Systems – техническая поддержка и документация