Сценарии конфигурации управления IPS на 5500x модуль ips

Содержание

Введение

В этом документе приводятся сценарии конфигурации модуля системы предотвращения вторжений (IPS) на устройстве адаптивной защиты (ASA) 5500x.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Модули IPS ASA 5500-X

Используемые компоненты

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

- Модули IPS ASA 5500-X

Условные обозначения

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

Общие сведения

С введением ASA 5500x и Программная реализация IPS, существуют коренные изменения к способу, которым управлению IPS позволяют вести себя.

1. IPS может только использовать менеджмент 0/0 интерфейс для внешнего управляющего доступ.
2. Если ASA назначили **nameif** на менеджмент 0/0, IPS должен иметь адрес в той же подсети как **nameif**.
3. Вы не можете удалить **команду management-only** из менеджмента 0/0 интерфейс ASA.
4. Если ASA пытается направить трафик через **nameif управления** с оператором "толька для управления", ASA отбрасывает трафик.
5. Если нет никакого **nameif**, назначенного на менеджмент 0/0, IPS функционирует так же к Усовершенствованному Модулю Сервисов безопасности Контроля и Предотвращения (SSM AIP) интерфейс управления модулей.

Эти способы поведения запрещают связи от IPS до внешних сетей, которые проходят через ASA, если существует **nameif** на менеджменте 0/0 интерфейс. ASA отбрасывает соединения, которые проходят через другие интерфейсы как через трафик через коробку, потому что IP-адрес принадлежит подсети **nameif** "управления". Это может также вызвать проблемы, потому что IPS нужны внешние шлюзы для маршрутизации трафика должным образом к ASA.

Предисловие

Модуль ips на ASA 5500X использует менеджмент 0/0 интерфейс для передачи с внешним миром. Этот документ предоставляет сведения о том, как установить этот интерфейс во множественных средах.

Все сценарии включают эту основную схему адресации:

- Внешний интерфейс ASA: 203.0.113.1/24
- Внутренний интерфейс ASA: 198.51.100.1/24
- Интерфейс управления ASA: 192.0.2.1/24
- Адрес управления IPS: 192.0.2.2/24

Все сценарии предполагают, что внутренний интерфейс и менеджмент 0/0 связаны с тем же коммутатором.

Примечание: Если существует **nameif** assisgned к менеджменту ASA 0/0 интерфейс, прибор слоя 3 с интерфейсами и во "внутри" и в подсети **nameif** "управления" требуется. IPS также требует, чтобы шлюз по умолчанию для IPS был расположен на том приборе слоя 3.

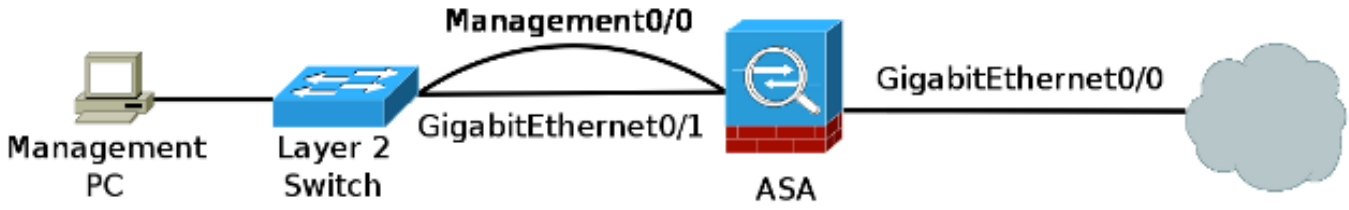
Сценарии

Сценарий 1

Оптимальный метод для настройки IPS и менеджмента ASA

1. К IPS и управлению ASA нельзя оба обратиться через менеджмент 0/0 интерфейс.
2. Не должно быть никакого **nameif**, назначенного на менеджмент ASA 0/0 интерфейс. К управлению ASA обращаются на интерфейсах переноса трафика.
3. IPS дают IP-адрес, достижимый от “внутреннего” **nameif**.
4. Доступ с “внутренней части” происходит через любого коммутатор или маршрутизатор без участия ASA.
5. Для разрешения управления с внешней стороны создайте статическую трансляцию сетевых адресов (NAT) для IP-адреса датчика или определите **переадресацию портов** к соответствующему порту (перенаправление порта используется в данном примере).

В этом сценарии связь управления IPS к внешней сети ведет себя подобная любому другому хосту на внутренней сети. Это используется для обновлений подписи, Глобальной Корреляции, и IPS Обрабатывает запросы Лицензии.



!--- конфигурацию:

```
interface GigabitEthernet0/0
 nameif outside security-level 0 ip address 203.0.113.1 255.255.0.0 !! interface
GigabitEthernet0/1 nameif inside security-level 0 ip address 198.51.100.1 255.255.255.0 !!
interface Management0/0 no nameif security-level 0 management-only !! same-security-traffic
permit inter-interface same-security-traffic permit intra-interface object network IPS-
management host 198.51.100.2 object network ASA-inside host 198.51.100.1 object network ASA-
outside host 203.0.113.1 object-group service HTTP service-object tcp-udp destination eq www
service-object tcp destination eq https access-list global_access extended permit ip any any
access-list global_access_1 remark Allow IPS management out through to the internet. access-list
global_access_1 extended permit object-group HTTP object IPS-management any nat (inside,outside)
source dynamic IPS-management IPS-management interface nat (inside,outside) static IPS-
management ASA-outside service tcp 443 65432 !! Use of an ephemeral port allows for the use of
common ports for other !! network applications. This also conceals the actual management port by
making it !! not well known. ASA# show module ips details | include Mgmt Mgmt IP addr:
198.51.100.2 Mgmt Network mask: 255.255.255.0 Mgmt Gateway: 198.51.100.1 Mgmt Access List:
0.0.0.0/0 Mgmt web ports: 443 Mgmt TLS enabled: true
```

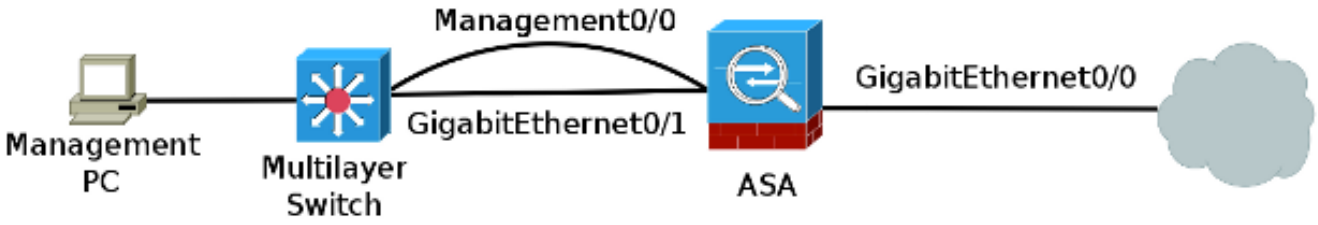
Сценарий 2

Управление IPS находится в той же подсети как nameif “управления” и находится в сети Уровня 3

1. Укажите шлюз IPS к Интерфейсу уровня 3 в сети кроме IP **nameif** управления ASA. Это устройство должно поддержать маршрутизацию между обеими подсетями; например, `192.0.2.2/24,192.0.2.254`.
2. Создайте статический маршрут на внутреннем интерфейсе ASA для обращения трафика к IP-адресу интерфейса уровня 3; например, `route inside 192.0.2.2 255.255.255.255 192.0.1.254`.
3. Удостоверьтесь весь список контроля доступа (ACL) и правила NAT применяются к IP-

адресу управления IPS.

В этой конфигурации IPS отправляет запросы для **Обновлений глобальной взаимосвязи**, запросы **Лицензии** и **обновления подписи IPS** к шлюзу по умолчанию (`192.0.2.254`), и преобразован во внешний адрес. Ответный трафик направляет назад с помощью внутреннего маршрута и передан прибору слоя 3, который помещает интерфейс во внутренней части и сетях управления.



!--- конфигурацию:

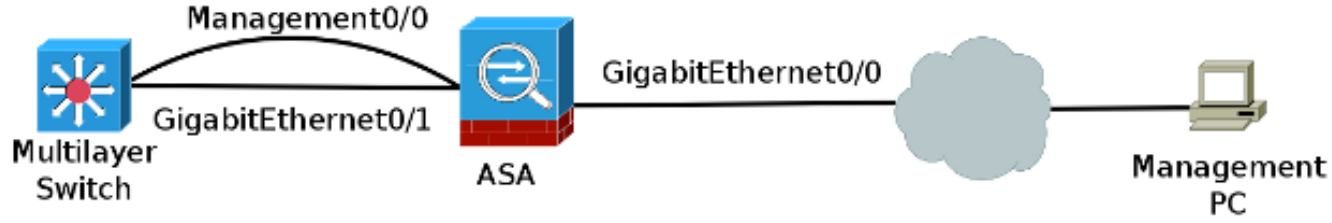
```
interface GigabitEthernet0/0
 nameif outside security-level 0 ip address 203.0.113.1 255.255.0.0 !! interface
GigabitEthernet0/1 nameif inside security-level 100 ip address 198.51.100.1 255.255.255.0 !!
interface Management0/0 nameif management security-level 0 ip address 192.0.2.1 255.255.255.0 !!
same-security-traffic permit inter-interface same-security-traffic permit intra-interface
object-group service HTTP service-object tcp-udp destination eq www service-object tcp
destination eq https access-list global_access extended permit ip any any access-list
global_access_1 remark Allow IPS management out through to the internet. access-list
global_access_1 extended permit object-group HTTP host 192.0.2.2 any route inside 192.0.2.2
255.255.255.255 198.51.100.254 1 ASA# show module ips details | include Mgmt Mgmt IP addr:
192.0.2.2 Mgmt Network mask: 255.255.255.0 Mgmt Gateway: 192.0.2.254 Mgmt Access List: 0.0.0.0/0
Mgmt web ports: 443 Mgmt TLS enabled: true
```

Ситуация 3

Управление IPS необходимо от внешнего интерфейса и существует nameif “управления”

1. Укажите шлюз IPS к Интерфейсу уровня 3 в сети кроме IP **nameif** управления ASA. Это устройство должно поддержать маршрутизацию между обеими подсетями.
2. Создайте статический маршрут на внутреннем интерфейсе ASA для обращения трафика к IP-адресу Интерфейса уровня 3.
3. Удостоверьтесь весь ACL и правила NAT применяются к IP-адресу управления IPS.

Все совпадает с выше, кроме ACL должен быть записан, чтобы позволить хосту с внешней стороны управлять IPS.



!--- конфигурацию:

```
interface GigabitEthernet0/0
 nameif outside security-level 0 ip address 203.0.113.1 255.255.0.0 !! interface
GigabitEthernet0/1 nameif inside security-level 0 ip address 198.51.100.1 255.255.255.0 !!
interface Management0/0 nameif management security-level 0 ip address 192.0.2.1 255.255.255.0
management-only !! same-security-traffic permit inter-interface same-security-traffic permit
intra-interface object network ASA-management host 192.0.2.1 object network ASA-inside host
198.51.100.1 object network IPS-management host 192.0.2.2 object-group service HTTP service-
object tcp-udp destination eq www service-object tcp destination eq https access-list
global_access extended permit ip any any access-list global_access_1 remark Allow IPS management
out through to the internet. access-list global_access_1 extended permit object-group HTTP
object IPS-management any object-group service MGMT_SERVICES service-object tcp-udp destination
eq http service-object tcp destination eq https service-object tcp destination eq ssh access-
list outside_access_in line 1 remark Allow outside management to IPS. access-list
outside_access_in line 2 extended permit object-group MGMT_SERVICES host 203.0.113.1 object IPS-
management access-group outside_access_in in interface outside nat (inside,outside) source
dynamic IPS-management IPS-management interface route inside 192.0.2.2 255.255.255.255
198.51.100.254 1 ASA# show module ips details | include Mgmt Mgmt IP addr: 192.0.2.2 Mgmt
Network mask: 255.255.255.0 Mgmt Gateway: 192.0.2.254 Mgmt Access List: 0.0.0.0/0 Mgmt web
ports: 443 Mgmt TLS enabled: true
```

Сценарий 4

Туннель IPSec, непосредственно связанный к ASA

1. Завершение VPN-туннеля к ASA имеет тот же эффект как управление от интерфейса, на котором вы завершаете VPN.
2. Как только вы имеете, устанавливают вашу VPN, необходимо записать маршрут от интерфейса, на котором VPN завершается к следующему переходу к внутреннему шлюзу Уровня 3.
3. Управление IPS также должно указать к шлюзу, который не находится на ASA, но в **nameif** "управления".
4. Если нет никаких приборов слоя 3 позади ASA, необходимо удалить **nameif** "управления" и IP-адрес на менеджменте ASA 0/0, и затем ввести IPS во "внутреннюю" подсеть **nameif**.

Трафик управления, который оставляет IPS, работает то же как в сети без VPN-подключения. Однако управляющий доступ должен быть обращен от сети, в которой завершается VPN.

!--- конфигурацию:

```
interface GigabitEthernet0/0
 nameif outside security-level 0 ip address 203.0.113.1 255.255.0.0 !! interface
GigabitEthernet0/1 nameif inside security-level 0 ip address 198.51.100.1 255.255.255.0 !!
interface Management0/0 nameif management security-level 0 ip address 192.0.2.1 255.255.255.0
management-only !! same-security-traffic permit inter-interface same-security-traffic permit
intra-interface object network ASA-management host 192.0.2.1 object network ASA-inside host
198.51.100.1 object network IPS-management host 192.0.2.2 object-group service
DM_INLINE_SERVICE_1 service-object tcp-udp destination eq www service-object tcp destination eq
```

https access-list global_access extended permit ip any any access-list global_access_1 remark Allow IPS management out through to the internet. access-list global_access_1 extended permit object-group DM_INLINE_SERVICE_1 object IPS-management any no pager logging enable ip local pool vpn 198.51.100.3-198.51.100.49 mask 255.255.255.0 icmp unreachable rate-limit 1 burst-size 1 icmp permit any outside icmp permit any inside access-group global_access_1 global route outside 0.0.0.0 0.0.0.0 203.0.113.2 route inside 192.0.2.2 255.255.255.255 198.51.100.254 1 dynamic-access-policy-record DfltAccessPolicy description "access" webvpn svc ask enable default svc user-identity default-domain LOCAL aaa authentication ssh console LOCAL http server enable http 0.0.0.0 0.0.0.0 outside crypto ipsec ikev1 transform-set tranny esp-aes esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac crypto ipsec security-association lifetime kilobytes 20000 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5 crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map outside_map interface outside crypto map inside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map inside_map interface inside crypto ca trustpoint ASDM_TrustPoint0 enrollment self subject-name CN=ciscoasa proxy-ldc-issuer crl configure crypto ca certificate chain ASDM_TrustPoint0 crypto isakmp identity address crypto ikev2 remote-access trustpoint ASDM_TrustPoint0 crypto ikev1 enable outside crypto ikev1 enable inside crypto ikev1 policy 5 authentication pre-share encryption aes hash md5 group 2 lifetime 86400 ssh 0.0.0.0 0.0.0.0 outside ssh timeout 60 console timeout 0 dhcp-client client-id interface outside ssl trust-point ASDM_TrustPoint0 inside ssl trust-point ASDM_TrustPoint0 outside webvpn port 8080 enable outside enable inside dtls port 8080 anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1 anyconnect image disk0:/anyconnect-macosx-i386-2.5.2014-k9.pkg 2 anyconnect profiles ANYconnect disk0:/anyconnect.xml anyconnect enable group-policy DfltGrpPolicy attributes vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless address-pools value vpn webvpn anyconnect profiles value ANYconnect type user ASA# **show module ips detail | include Mgmt** Mgmt IP addr: 192.0.2.2 Mgmt Network mask: 255.255.255.0 Mgmt Gateway: 192.0.2.254 Mgmt Access List: 0.0.0.0/0 Mgmt web ports: 443 Mgmt TLS enabled: true

Дополнительные сведения

- Как проверить предупреждения контроля и подписи трафика IPS
- Cisco Systems – техническая поддержка и документация