在5500x IPS模块的IPS管理配置情形

目录

简介

本文在一个可适应安全工具(ASA) 5500x入侵预防系统(IPS)模块提供配置情形。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA 5500x IPS模块

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA 5500x IPS模块

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景

使用ASA 5500x和软件实现的介绍IPS，有对IPS管理允许正常运行的方式的基本更改。

1. IPS能只使用Management0/0接口外部管理访问。
2. 如果ASA有一**nameif**分配到Management0/0， IPS必须有在相同子网的一个地址作为**nameif**。
3. 您不能从ASA的Management0/0接口删除唯一的命令。
4. 如果ASA尝试对路由流量通过与“仅管理”语句的**管理nameif**， ASA降低流量。
5. 如果没有**nameif**分配到Management0/0， IPS类似作用于先进的检查和预防安全服务模块(AIP-SSM)模块管理接口。

这些行为从IPS禁止通信到穿过ASA的外部网络，如果有在Management0/0接口的一**nameif**。ASA切穿过其他接口作为通过这方框流量的连接，因为IP地址属于“管理” **nameif**子网。因为IPS适当地需要外部网关为了路由流量对ASA，这能也引起问题。

前言

在ASA 5500X的IPS模块使用Management0/0接口与外界联络。本文提供信息关于怎样设置在多个环境的此接口。

所有情形包括此基本地址方案：

- ASA外部接口：203.0.113.1/24
- ASA内部接口：198.51.100.1/24
- ASA管理接口：192.0.2.1/24
- IPS管理地址：192.0.2.2/24

所有情形假设，内部接口和Management0/0连接到同一交换机。

注意： 如果有**nameif** assisgned对ASA Management0/0接口，与接口的一第3层设备在“里面”和“管理” **nameif**子网络要求。IPS也要求IPS的默认网关在该第3层设备查找。

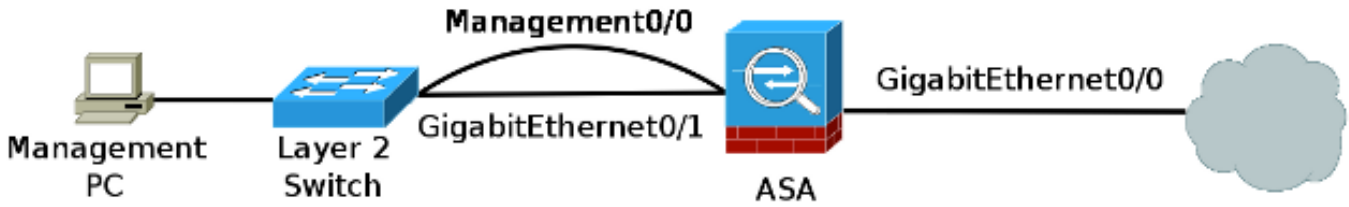
方案

场景 1

IPS和ASA管理设置的最佳实践

1. IPS和ASA管理不可能两个通过Management0/0接口访问。
2. 不应该有**nameif**分配到ASA Management0/0接口。ASA管理在流量载有数据接口访问。
3. IPS给IP地址可及的从“里面” **nameif**。
4. 从“里面的”访问通过交换机或路由器发生，不用ASA的介入。
5. 为了允许**转发的**管理从外面，为传感器IP地址创建静态网络地址转换(NAT)或者定义**端口**自适当的端口(端口重定向用于此示例)。

在此方案中，对外部网络的IPS管理通信正常运行类似于在网络内部的其他主机。这使用签名更新、全局相关性和IPS服务许可证请求。



配置：

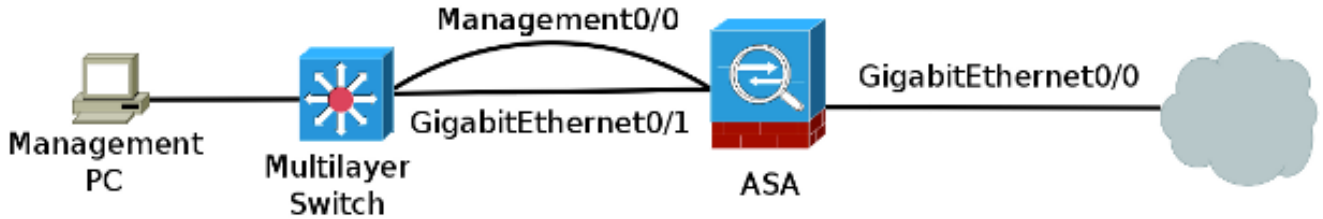
```
interface GigabitEthernet0/0
 nameif outside security-level 0 ip address 203.0.113.1 255.255.0.0 !! interface
GigabitEthernet0/1 nameif inside security-level 0 ip address 198.51.100.1 255.255.255.0 !!
interface Management0/0 no nameif security-level 0 management-only !! same-security-traffic
permit 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
```

场景 2

IPS管理是在相同子网作为“管理” nameif并且是在第3层网络

1. 除ASA管理**nameif** IP之外，指向IPS的网关在网络的一个第3层接口。此设备必须支持在两子网之间的路由;例如， `192.0.2.2/24,192.0.2.254`。
2. 创建在ASA的内部接口的静态路由指向流量第3层接口IP地址;例如，请`192.0.2.2 255.255.255.255 192.0.1.254`。
3. 确保所有访问控制表(ACL)和NAT规则适用于IPS管理的IP地址。

在此配置中， IPS发送要求**全局相关性**更新，**准许**请求和**IPS签名更新**到默认网关(`192.0.2.254`)和翻译对外部地址。回程数据流路由通过在里面和管理网络安置一个接口的里面路由返回和转发对第3层设备。



配置：

```
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
```

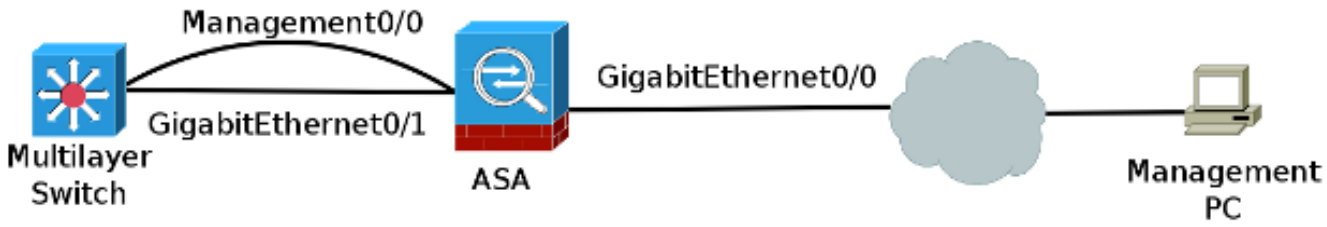
```
object-group service HTTP service-object tcp-udp destination eq www service-object tcp
destination eq https access-list global_access extended permit ip any any access-list
global_access_1 remark Allow IPS management out through to the internet. access-list
global_access_1 extended permit object-group 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
```

场景 3

IPS管理从外部接口是需要的，并且有“管理” nameif

1. 除ASA管理nameif IP之外，指向IPS的网关在网络的一个第3层接口。此设备必须支持在两子网之间的路由。
2. 创建在ASA的内部接口的静态路由指向流量第3层接口IP地址。
3. 确保所有ACL和NAT规则适用于IPS管理的IP地址。

一切是相同的如上所述，除了必须写入ACL允许一台主机从外面管理IPS。



配置：

```
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
```

场景 4

IPSec隧道直接地连接对ASA

1. 一个VPN通道的终端对ASA的有效果和从您终止VPN的接口的管理一样。
2. 一旦设置您的VPN，您需要写入从VPN终止对下一跳到一个内部第3层网关的接口的一个路由。
3. IPS管理也需要指向在ASA不驻留的网关，但是里面“管理” nameif。

4. 如果没有在ASA后的第3层设备，您必须删除“管理” **nameif**和IP地址在ASA Management0/0，然后输入IPS在“里面” **nameif**子网。

离开IPS的管理数据流在网络工作同一样，不用VPN连接。然而，必须从VPN终止的网络寻址管理访问。

配置：

```
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
```

相关信息

- 如何验证IPS流量检查和签名警报
- 技术支持和文档 - Cisco Systems