ASA/PIX/IOS路由器的IPS避开或阻塞配置示例

目录

简介

本文档介绍如何在Cisco IPS的帮助下在PIX/ASA/Cisco IOS路由器上配置分流。ARC（传感器上的阻塞应用）在路由器、Cisco 5000 RSM和Catalyst 6500系列交换机、PIX防火墙、FWSM和ASA上启动和停止阻塞。ARC向受管设备发出阻止或回避恶意IP地址。ARC向传感器管理的所有设备发送相同的块。如果配置了主阻塞传感器，则会将阻塞转发到此设备并从该设备发出。ARC监控块的时间，并在时间到期后删除块。

当您使用IPS 5.1时，在多情景模式下避开防火墙时必须特别小心，因为不会随回避请求发送VLAN信息。

> **注意：**在多情景FWSM的管理情景中不支持阻止。

块有三种类型：

- Host block — 阻止来自给定IP地址的所有流量。
- 连接块 — 阻止从给定源IP地址到给定目标IP地址和目标端口的流量。从同一源IP地址到不同目的IP地址或目的端口的多个连接块会自动将块从连接块切换到主机块。**注意：**安全设备不支持连接块。安全设备仅支持包含可选端口和协议信息的主机块。
- 网络块 — 阻止来自给定网络的所有流量。您可以手动或在触发签名时自动启动主机和连接块。您只能手动启动网络块。

对于自动块，必须选择Request Block Host或Request Block Connection作为特定签名的事件操作，以便SensorApp在触发签名时向ARC发送块请求。ARC收到来自SensorApp的阻止请求后，会更新设备配置以阻止主机或连接。有关向签名添加请求阻止主机或请求阻止连接事件操作的过程的详细信息，请参阅第5-22页的为签名分配操作。有关将请求阻止主机或请求阻止连接事件操作添加到特定风险评级警报的覆盖配置过程的详细信息，请参阅第7-15页的配置事件操作覆盖。

在思科路由器和Catalyst 6500系列交换机上，ARC通过应用ACL或VACL创建块。ACL和VACL将过

滤器分别应用于接口（包括方向）和VLAN，以允许或拒绝流量。。PIX防火墙、FWSM和ASA不使用ACL或VACL。使用内置shun和no shun命令。

配置ARC时需要以下信息：

- 如果设备配置了AAA，则登录用户ID
- 登录密码
- 启用密码，如果用户具有启用权限，则不需要此密码
- 要管理的接口，例如ethernet0、vlan100
- 要在创建的ACL或VACL的开始（Pre-Block ACL或VACL）或结束（Post-Block ACL或VACL）应用任何现有ACL或VACL信息。这不适用于PIX防火墙、FWSM或ASA，因为它们不使用ACL或VACL进行阻止。
- 使用Telnet或SSH与设备通信
- 您从不希望被阻止的IP地址（主机或主机范围）
- 你希望这些块能持续多久

先决条件

要求

在为阻塞或速率限制配置ARC之前，必须完成以下任务：

- 分析网络拓扑，了解哪些设备应被哪些传感器阻止，哪些地址不应被阻止。
- 收集登录每台设备所需的用户名、设备密码、启用密码和连接类型（Telnet或SSH）。
- 了解设备上的接口名称。
- 如果需要，请了解Pre-Block ACL或VACL和Post-Block ACL或VACL的名称。
- 了解应阻止和不应阻止的接口以及方向（输入或输出）。

使用的组件

本文档中的信息基于Cisco Intrusion Prevention System 5.1及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

> **注意：**默认情况下，ARC配置为最多250个块条目。有关ARC支持的阻塞设备列表的详细信息，请参阅支持的设备。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

使用Blocking页可配置启用阻止和速率限制所需的基本设置。

ARC控制受管设备上的阻塞和速率限制操作。

必须调整传感器，以识别不应被阻止的主机和网络。受信任设备的流量可以触发签名。如果将此签名配置为阻止攻击者，则会影响合法网络流量。为了防止出现此情况，设备的IP地址可以列在Never Block列表中。

在“从不阻止”(Never Block)条目中指定的网络掩码将应用于“从不阻止”(Never Block)地址。如果未指定网络掩码，则应用默认/32掩码。

> **注意**：默认情况下，传感器不允许为自己的IP地址发出阻止，因为这会干扰传感器和阻止设备之间的通信。但是，此选项可由用户配置。

一旦ARC配置为管理阻塞设备，阻塞设备的分流和用于阻塞的ACL/VACL不应手动更改。这可能导致ARC服务中断，并可能导致未来不会发出数据块。

> **注意**：默认情况下，Cisco IOS设备仅支持阻塞。如果选择速率限制或阻塞加速率限制，则可以覆盖阻塞默认值。

要发出或更改阻止，IPS用户必须具有管理员或操作员角色。

配置传感器以管理Cisco路由器

本节介绍如何配置传感器以管理思科路由器。它包含以下主题：

- 配置用户配置文件
- 路由器和ACL
- 使用CLI配置思科路由器

配置用户配置文件

传感器使用user-profiles profile_name命**令管理其***他设备*，以便设置用户配置文件。用户配置文件包含用户ID、密码和启用密码信息。例如，所有共享相同密码和用户名的路由器都可以位于一个用户配置文件下。

> **注意**：在配**置阻**塞设备之前，必须创建用户配置文件。

要设置用户配置文件，请完成以下步骤：

1. 使用具有管理员权限的帐户登录 CLI。
2. 进入网络访问模式。
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. 创建用户配置文件名称。
   ```
   sensor(config-net)#user-profiles PROFILE1
   ```

4. 键入该用户配置文件的用户名。
```
sensor(config-net-use)#username username
```
5. 指定用户的密码。
```
sensor(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```
6. 指定用户的使能密码。
```
sensor(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```
7. 检验设置。
```
sensor(config-net-use)#show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
sensor(config-net-use)#
```
8. 退出网络访问子模式。
```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```
9. 按**Enter**以应用更改，或输入no以放弃更改。

路由器和ACL

当ARC配置了使用ACL的阻塞设备时，ACL的组成方式如下：

1. 带有传感器IP地址的允许行，或者（如果指定）传感器的NAT地址**注意：**如果允许阻止传感器，则此行不会显示在ACL中。
2. 预阻止ACL（如果指定）：此ACL必须已存在于设备上。**注意：**ARC读取预配置ACL中的行，并将这些行复制到块ACL的开头。
3. 任何活动块
4. 后**阻止ACL或**允**许ip any any** :**后块ACL**（如果指定）：此ACL必须已存在于设备上。**注意：**ARC读取ACL中的行，并将这些行复制到ACL的末尾。**注意：**如果希望允许所有不匹配的数据包，请确保ACL的最后一行是permit ip any any。**permit ip any any**（如果指定了后阻止ACL，则不使用）

   注意：ARC生成的ACL不应由您或任何其他系统修改。这些ACL是临时的，而新ACL由传感器不断创建。您只能对Pre-Block和Post-Block ACL进行修改。

如果需要修改预阻止或后阻止ACL，请完成以下步骤：

1. 禁用传感器上的阻塞。
2. 更改设备配置。
3. 在传感器上重新启用阻塞。

重新启用阻塞时，传感器读取新设备配置。

注意：单个传感器可以管理多个设备，但多个传感器无法管理单个设备。如果从多个传感器发

出的块用于单个阻塞设备，则必须将主阻塞传感器并入设计中。主阻塞传感器接收来自多个传感器的阻塞请求并向阻塞设备发出所有阻塞请求。

在路由器配置中创建并保存预阻止和后阻止ACL。这些ACL必须是扩展IP ACL，可以是命名ACL，也可以是编号ACL。有关如何创建ACL的详细信息，请参阅路由器文档。

注意：预阻止和后阻止ACL不适用于速率限制。

ACL从上到下进行评估，并执行第一匹配操作。Pre-Block ACL可能包含一个允许，该允许优先于由块导致的拒绝。

后块ACL用于解释预块ACL或块未处理的任何条件。如果接口上和发出地址块的方向上有现有ACL，则该ACL可用作后块ACL。如果没有Post-Block ACL，传感器会在新ACL的末尾插入permit ip any any。

当传感器启动时，它会读取两个ACL的内容。它使用以下条目创建第三个ACL:

- 传感器IP地址的允许行
- 预阻止ACL的所有配置行的副本
- 传感器阻止的每个地址的拒绝行
- 阻止后ACL的所有配置行的副本

传感器将新ACL应用于您指定的接口和方向。

注意：当新的块ACL在特定方向上应用于路由器的接口时，它会在该方向上替换该接口上现有的任何ACL。

使用CLI配置思科路由器

要配置传感器以管理思科路由器以执行阻塞和速率限制，请完成以下步骤：

1. 使用具有管理员权限的帐户登录 CLI。
2. 进入网络访问子模式。
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. 指定由ARC控制的路由器的IP地址。
   ```
   sensor(config-net)#router-devices ip_address
   ```
4. 输入配置用户配置文件时创建的逻辑设备名称。
   ```
   sensor(config-net-rou)#profile-name user_profile_name
   ```
   注意：ARC接受您输入的任何内容。它不检查用户配置文件是否存在。
5. 指定用于访问传感器的方法。
   ```
   sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
   ```
   如果未指定，则使用SSH 3DES。**注意**：如果使用DES或3DES，则必须使用**ssh host-key ip_address**命令才能从设备接受SSH密钥。
6. 指定传感器NAT地址。
   ```
   sensor(config-net-rou)#nat-address nat_address
   ```
   注意：这会将ACL第一行中的IP地址从传感器地址更改为NAT地址。NAT地址是传感器地址

，即后NAT，由中间设备转换，位于传感器和阻塞设备之间。

7. 指定路由器是执行阻塞、速率限制还是同时执行两者。**注意：**默认为阻塞。如果希望路由器仅执行阻止，则无需配置响应功能。仅限速率限制
```
sensor(config-net-rou)#response-capabilities rate-limit
```

   阻塞和速率限制
```
sensor(config-net-rou)#response-capabilities block|rate-limit
```

8. 指定接口名称和方向。
```
sensor(config-net-rou)#block-interfaces interface_name {in | out}
```

   注意：接口名称必须是路由器在接口命令后使用时识别的**缩写**。

9. （可选）添加ACL之前的名称（仅阻止）。
```
sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
```
10. （可选）添加后ACL名称（仅阻止）。
```
sensor(config-net-rou-blo)#post-acl-name post_acl_name
```
11. 检验设置。
```
sensor(config-net-rou-blo)#exit

sensor(config-net-rou)#show settings

   ip-address: 10.89.127.97
   ----------------------------------------------
      communication: ssh-3des default: ssh-3des
      nat-address: 19.89.149.219 default: 0.0.0.0
      profile-name: PROFILE1
      block-interfaces (min: 0, max: 100, current: 1)
      ----------------------------------------------
         interface-name: GigabitEthernet0/1
         direction: in
         ----------------------------------------------
            pre-acl-name: <defaulted>
            post-acl-name: <defaulted>
         ----------------------------------------------
      ----------------------------------------------
      response-capabilities: block|rate-limit default: block
   ----------------------------------------------
sensor(config-net-rou)#
```
12. 退出网络访问子模式。
```
sensor(config-net-rou)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```
13. 按**Enter**以应用更改，或输入**no**以放弃更改。

配置传感器以管理思科防火墙

要配置传感器以管理思科防火墙，请完成以下步骤：

1. 使用具有管理员权限的帐户登录 CLI。
2. 进入网络访问子模式。
```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```
3. 指定由ARC控制的防火墙的IP地址。
```
sensor(config-net)#firewall-devices ip_address
```

4. 输入在配置用户配置文件时创建的用户配置文件名称。
   ```
   sensor(config-net-fir)#profile-name user_profile_name
   ```
   注意：ARC接受您键入的任何内容。它不检查逻辑设备是否存在。
5. 指定用于访问传感器的方法。
   ```
   sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
   ```

   如果未指定，则使用SSH 3DES。**注意**：如果使用DES或3DES，则必须使用**ssh host-key ip_address**命令来接受密钥，否则ARC无法连接到设备。
6. 指定传感器NAT地址。
   ```
   sensor(config-net-fir)#nat-address nat_address
   ```
   注意：这会将ACL第一行中的IP地址从传感器的IP地址更改为NAT地址。NAT地址是传感器地址，即后NAT，由中间设备转换，位于传感器和阻塞设备之间。
7. 退出网络访问子模式。
   ```
   sensor(config-net-fir)#exit
   sensor(config-net)#exit
   sensor(config)#exit
   Apply Changes:?[yes]:
   ```
8. 按 **Enter 键以应用更改或输入“no”以放弃更改。**

在PIX/ASA中使用SHUN进行阻止

发出**shun**命令会阻止来自攻击主机的连接。与命令中的值匹配的数据包将被丢弃并记录，直到删除阻止功能。无论指定主机地址的连接当前是否处于活动状态，都会应用**shun**。

如果指定目标地址、源和目标端口以及协议，则将避开范围缩小为与这些参数匹配的连接。每个源IP地址只能**有**一个shun命令。

由于**shun**命令用于动态阻止攻击，因此它不会显示在安全设备配置中。

每当删除接口时，连接到该接口的所有分流也会被删除。

本示例显示违规主机(10.1.1.27)与受害者(10.2.2.89)建立TCP连接。安全设备连接表中的连接如下所示：

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

要阻止来自攻击主机的连接，请在特权EXEC模式下使用**shun**命令。将**shun**命令与以下选项一起应用：

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

该命令从安全设备连接表中删除连接，并防止从10.1.1.27:555到10.2.2.89:666(TCP)的数据包通过安全设备。

相关信息

- [配置传感器以管理Catalyst 6500系列交换机和Cisco 7600系列路由器]
- [技术支持和文档 - Cisco Systems]