ASA/PIX/IOS路由器的IPS避开或阻塞配置示例

目录

简介

本文描述如何在思科IPS帮助下配置在PIX/ASA/Cisco IOS路由器的避开。弧，在传感器的阻塞应用程序，开始和在路由器的终止块、Cisco 5000 RSM和Catalyst 6500系列交换机、PIX防火墙、FWSM和ASA。弧问题每块或避开到有恶意的IP地址的受管理设备。弧发送同一块到传感器管理的所有设备。如果一个重要的阻塞传感器配置，块转发对并且从此设备发出。弧监控块的时期并且在时间之后删除块超时。

当您使用IPS 5.1时，必须保重特别注意，当避开对在多个上下文模式的防火墙作为没有VLAN信息用避开请求时传送。

注意： 多个上下文FWSM的admin状况不支持阻塞。

有块的三种类型：

- 主机块—阻塞从一个给的IP地址的所有流量。
- 连接块—从指定源IP地址的块流量到指定目的地IP地址和目的地端口。从同样源IP地址的多个连接块到一不同的目的IP地址或目的地端口自动地换成从连接块的块主机块。**注意：** 安全工具不支持连接块。安全工具支持有可选端口和协议信息的仅主机块。
- 网络地址块—阻塞从给的网络的所有流量。当签名被触发时，您可以启动主机和连接块手工或自动。您可以手工只启动网络块。

对于自动块，您必须选择请求分程序主机或请求分程序连接作为特定的签名的事件操作，因此SensorApp发送块请求形成弧光，当签名被触发时。一旦弧收到从SensorApp的块请求，更新设备配置阻塞主机或连接。参考分配操作到签名，页5-22关于步骤添加的更多信息请求分程序主机或请求分程序连接事件操作到签名。参考配置事件操作改写，关于步骤的更多信息页7-15配置的改写添加请求分程序主机或请求分程序连接事件操作到特定风险评价报警。

在Cisco路由器和Catalyst 6500系列交换机上，弧通过应用ACL或VACL创建块。ACL和VACL应用过滤器对接口，包括方向和VLAN，为了分别允许或否决流量。PIX防火墙、FWSM和ASA不使用ACL或VACL。镶入避开，并且**没有shun命令**使用。

此信息为弧的配置要求：

- 如果设备配置与AAA，登陆用户ID
- 登录密码
- 特权密码，不是需要的，如果用户有enable (event)权限
- 将管理的接口，例如， ethernet0， vlan100
- 您希望首先应用的任何现有ACL或VACL信息(PRE块ACL或VACL)或结尾(POST块ACL或VACL) ACL或VACL创建。因为他们不使用ACL或VACL阻塞，这不适用于PIX防火墙、FWSM或者ASA。
- 您是否使用Telnet或SSH与设备联络
- IP地址(主机或范围主机)您从未想要阻止
- 您多久希望块持续

先决条件

要求

在您配置阻塞的弧或对限制估计前，您必须完成这些任务：

- 分析您的网络拓扑了解应该阻塞哪些设备不应该阻塞传感器，和寻址。
- 采集用户名，设备密码，特权密码，并且连接类型(Telnet或SSH)需要登陆到每个设备。
- 认识在设备的接口名称。
- 若需要认识PRE块ACL的名称或VACL和POST块ACL或者VACL。
- 了解哪些接口应该并且不应该阻塞，并且在哪个方向(在或)。

使用的组件

本文档中的信息根据思科入侵防御系统5.1及以后。

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，弧为250块条目限制配置。关于阻塞设备的更多信息列表的参考的支持设备弧支持的。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

请使用阻塞属性窗格为了配置要求的基本设置启用阻塞和对限制估计。

弧控制限制在受管理设备的阻塞和速率操作。

您必须调整您的传感器为了识别不应该阻塞的主机和网络。射击签名可信的设备的流量是可能的。如果此签名配置阻塞攻击者，合法网络流量可以受影响。设备的IP地址在阻塞列表不可以列出为了防止此方案。

在一块条目指定的网络屏蔽从未从未应用对块地址。如果网络屏蔽没有指定，默认/32掩码应用。

注意： 默认情况下，当这干涉传感器和阻塞设备之间的通信传感器没有允许发出其自己的IP地址的一块。但是，此选项由用户是可配置。

一旦弧配置管理阻塞设备，阻塞设备的避开，并且使用阻塞的ACL/VACL不应该手工修改。这导致弧服务的中断，并且能导致不发出的将来块。

注意： 默认情况下，只阻塞Cisco IOS设备支持。如果选择速率限制或阻塞加上速率限制，您能改写阻塞默认。

为了发出或修改块， IPS用户必须有管理员或操作员角色。

配置传感器管理Cisco路由器

此部分描述如何配置传感器管理Cisco路由器。它包含这些主题：

- 配置用户配置文件
- 路由器和ACL
- 配置使用CLI的Cisco路由器

配置用户配置文件

传感器管理其它设备以**用户配置文件***profile_name*命令为了设置用户配置文件。用户配置文件包含userid、密码和特权密码信息。例如，所有共享同样密码和用户名的路由器可以是在一用户配置文件以下。

注意： 在您配置阻塞设备前，您**必须**创建用户配置文件。

完成这些步骤为了设置用户配置文件：

1. 使用具有管理员权限的帐户登录 CLI。
2. 输入网络访问存取状态。`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. 指定用户的特权密码。`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. 退出网络访问从属方式。`sensor(config-net-use)#`**`exit`** `sensor(config-net)#`**`exit`** `Apply Changes:?[yes]:`
9. 按回车为了应用更改或输入不丢弃他们。

路由器和ACL

当弧用使用ACL的阻塞设备时配置， ACL这样撰写：

1. 有传感器IP地址的一条permit线路或，如果指定，传感器的NAT地址**注意：** 如果允许传感器阻塞，此线路在ACL没出现。
2. PRE块ACL (如果指定)此ACL在设备必须已经存在。**注意：** 弧读在预先配置的ACL的线路并且复制这些线路对块ACL的开始。
3. 任何有源组件
4. ：POST块ACL permit ip any any- POST**块ACL** (如果指定)此ACL在设备必须已经存在。**注意：** 弧读在ACL的线路并且复制这些线路对ACL的结尾。**注意：** 如果希望所有不匹配数据包允许，请确保在ACL的最后一行是permit ip any any。- **permit ip any any** (没使用，如果POST块ACL指定)

注意： 弧做应该由您从未修改的ACL或其他系统。这些ACL是临时的，并且新的ACL由传感器经常创建。您能做的唯一的修改是对前和POST块ACL。

如果需要修改PRE块或POST块ACL，请完成这些步骤：

1. 禁用在传感器的阻塞。
2. 做对设备的配置的变动。
3. 重新授权给在传感器的阻塞。

当阻塞重新授权给时，传感器读新设备配置。

注意： 单个传感器能管理多个设备，但是多个传感器不能管理单个设备。在案件中从多个传感器发出的块为单个阻塞设备含义，必须合并一个重要的阻塞传感器到设计里。一个重要的阻塞传感器收到从多个传感器的阻塞请求并且发出所有阻塞请求到阻塞设备。

您在您的路由器配置方面创建并且保存PRE块和POST块ACL。这些ACL必须是扩展的IP ACL，名为或被编号。请参阅您的路由器文档关于如何创建ACL的更多信息。

注意： PRE块和POST块ACL不应用对限制估计。

ACL被评估自上而下，并且第一个匹配条件行动采取。PRE块ACL可能包含将优先于拒绝起因于块的permit。

POST块ACL用于占PRE块ACL或块没处理的所有情况。如果有现有ACL在接口和在块发出的方向，该ACL可以使用作为POST块ACL。如果没有POST块ACL，传感器插入permit ip any any在新的ACL结束时。

当传感器启动时，读两个ACL的内容。它创建与这些条目的第三ACL ：

- 传感器IP地址的一条permit线路
- PRE块ACL的所有配置行份数
- 由传感器阻塞的每个地址的一条拒绝线路
- POST块ACL的所有配置行份数

您选定的传感器应用新的ACL对接口和方向。

注意： 当新的块ACL应用对路由器的接口，在特定的方向时，替换在该接口的所有事先存在的ACL在该方向。

配置使用CLI的Cisco路由器

完成这些步骤为了配置传感器管理Cisco路由器执行阻塞和对限制估计：

1. 使用具有管理员权限的帐户登录 CLI。
2. 输入网络访问从属方式。sensor#**configure terminal** sensor(config)#**service network-access** sensor(config-net)#
3. 指定弧控制的路由器的IP地址。sensor(config-net)#**router-devices** *ip_address*
4. 当您配置用户配置文件，请输入该逻辑设备的设备名称您创建。sensor(config-net-rou)#**profile-name** *user_profile_name* 弧接受您输入的任何事。它不检查发现用户配置文件是否存在。
5. 指定使用的方法访问传感器。sensor(config-net-rou)# **communication {telnet | ssh-des | ssh-3des}** 如果， SSH 3DES使用未指定。**注意：** 如果使用DES或3DES，您必须使用**ip_address命令SSH的主机键**为了接受从设备的SSH密钥。
6. 指定传感器NAT地址。sensor(config-net-rou)#**nat-address** *nat_address* **注意：** 这更改在ACL的第一行的IP地址从传感器的地址的对NAT地址。NAT地址是传感器地址， POST NAT，翻译由一个中介设备，查找在传感器和阻塞设备之间。
7. 指定路由器是否执行限制阻塞的速率或者两个。**注意：** 默认是阻塞。如果希望路由器执行仅，阻塞您不必须配置答复功能。只限制的速率sensor(config-net-rou)#**response-capabilities rate-limit** 阻塞并且对限制估计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：** 接口的名称必须是路由器认可，当使用在**interface命令以后的**简称。
9. (可选)请添加PRE ACL名称(只阻塞)。sensor(config-net-rou-blo)#**pre-acl-name** *pre_acl_name*
10. (可选)请添加POST ACL名称(只阻塞)。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. 退出网络访问从属方式。sensor(config-net-rou)#**exit** sensor(config-net)#**exit** sensor(config)#**exit** Apply Changes:?[yes]:
13. 按回车为了应用更改或输入**不**丢弃他们。

配置传感器管理思科防火墙

完成这些步骤为了配置传感器管理思科防火墙：

1. 使用具有管理员权限的帐户登录 CLI。
2. 输入网络访问从属方式。sensor#**configure terminal** sensor(config)#**service network-access** sensor(config-net)#
3. 指定弧控制的防火墙的IP地址。sensor(config-net)#**firewall-devices** *ip_address*
4. 当您配置用户配置文件，请输入该用户配置文件的名称您创建。sensor(config-net-fir)#**profile-name** *user_profile_name* 弧接受您键入的任何事。它不检查发现逻辑设备是否存在。
5. 指定使用的方法访问传感器。sensor(config-net-fir)#**communication {telnet | ssh-des | ssh-**

3des} 如果， SSH 3DES使用未指定。**注意：** 如果使用DES或3DES，您必须使用**ip_address命令SSH的主机键**为了接受密钥或弧不能连接到设备。

6. 指定传感器NAT地址。`sensor(config-net-fir)#`**`nat-address`** *`nat_address`* **注意：** 这更改在ACL的第一行的IP地址从传感器的IP地址的对NAT地址。NAT地址是传感器地址， POST NAT，翻译由一个中介设备，查找在传感器和阻塞设备之间。
7. 退出网络访问从属方式。`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。

块与在PIX/ASA避开

发出从一台攻击的主机的**shun命令**块连接。匹配在命令的值的数据包丢弃并且被记录，直到阻塞功能删除。**避开**应用不管与指定的主机地址的一连接是否当前活跃的。

如果指定目的地址、源及目的地端口和协议，您缩小避开对匹配那些参数的连接。

您能只有一**shun命令**为每源IP地址。

由于**shun命令**用于动态地拦截攻击，没有在安全工具配置里显示。

每当接口删除，附加对该接口也删除的所有避开。

此示例显示触犯的主机(10.1.1.27)建立与受害者(10.2.2.89)的联系对TCP。连接在安全工具连接表里读如下：

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

为了阻塞从一台攻击的主机的连接，请使用**shun命令**在特权EXEC模式。实施**shun命令**与这些选项：

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

命令删除从安全工具连接表的连接并且防止数据包10.1.1.27:555到10.2.2.89:666 (TCP)从通过安全工具。

相关信息

- 配置传感器管理Catalyst 6500系列交换机和思科7600系列路由器
- 配置攻击限制使用IDM 7.0的阻塞和速率的答复控制器
- 技术支持和文档 - Cisco Systems