使用VM IDS MC配置IDS阻塞

目录

简介

通过VPN/安全管理解决方案(VMS)、IDS管理控制台(IDS MC)，本文为Cisco入侵检测系统(IDS)的配置提供一个示例。在这种情况下，从IDS传感器的阻塞到Cisco路由器配置。

先决条件

要求

在您配置阻塞前，请保证您符合了这些情况。

- 传感器为感觉必要的流量安装并且配置。
- 探测接口被跨过对路由器外部接口。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- 与IDS MC和安全监视器1.2.3的VM 2.2

- Cisco IDS传感器4.1.3S(63)
- Cisco路由器运行Cisco IOS软件版本12.3.5

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用此图所示的网络设置。

配置

本文档使用此处所示的配置。

- 路由器灯
- 路由器 House

路由器灯

```
Current configuration : 906 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light ! enable password cisco ! username cisco
password 0 cisco ip subnet-zero ! ! ! ip ssh time-out
120 ip ssh authentication-retries 3 ! call rsvp-sync ! !
! fax interface-type modem mta receive maximum-
recipients 0 ! controller E1 2/0 ! ! ! interface
FastEthernet0/0 ip address 100.100.100.2 255.255.255.0
duplex auto speed auto ! interface FastEthernet0/1 ip
address 1.1.1.1 255.255.255.0 duplex auto speed auto !
interface BRI4/0 no ip address shutdown ! interface
BRI4/1 no ip address shutdown ! interface BRI4/2 no ip
address shutdown ! interface BRI4/3 no ip address
shutdown ! ip classless ip route 0.0.0.0 0.0.0.0
100.100.100.1 ip http server ip pim bidir-enable ! !
dial-peer cor custom ! ! line con 0 line 97 108 line aux
0 line vty 0 4 login ! end
```

路由器 House

```
Building configuration...

Current configuration : 797 bytes
```

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname House ! logging queue-limit 100 enable password
cisco ! ip subnet-zero no ip domain lookup ! ! interface
Ethernet0 ip address 10.66.79.210 255.255.255.224 hold-
queue 100 out ! interface Ethernet1 ip address
100.100.100.1 255.255.255.0 !--- After Blocking is
configured, the IDS Sensor !--- adds this access-group
ip access-group. IDS_Ethernet1_in_0 in ip classless ip
route 0.0.0.0 0.0.0.0 10.66.79.193 ip route 1.1.1.0
255.255.255.0 100.100.100.2 ip http server no ip http
secure-server ! !--- After Blocking is configured, the
IDS Sensor !--- adds this access list. ip access-list
extended IDS_Ethernet1_in_0. permit ip host 10.66.79.195
any permit ip any any ! line con 0 stopbits 1 line vty 0
4 password cisco login ! scheduler max-task-time 5000
end
```

最初的传感器配置

完成这些步骤最初配置传感器。

注意： 如果执行您的传感器初始设置，请继续对导入传感器的部分到IDS MC。

1. 控制到传感器。系统会提示您输入用户名和密码。如果这是您第一次控制传感器，您必须使用用户名cisco和密码cisco进行登录。
2. 提示您更改密码然后重新代表新密码确认。
3. 键入**设置**并且进入相应的信息在每及时根据此示例设置您的传感器的基本参数，

   ：sensor5#**setup** --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration: networkParams ipAddress **10.66.79.195** netmask **255.255.255.224** defaultGateway **10.66.79.193** hostname **sensor5** telnetOption **enabled accessList ipAddress 10.66.79.0 netmask 255.255.255.0** exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit
4. 按**2**为了保存您的配置。

导入传感器到IDS MC

完成这些步骤导入传感器到IDS MC。

1. 浏览对您的传感器。在这种情况下，请浏览对**http://10.66.79.250:1741**或**https://10.66.79.250:1742**。
2. 登陆与适当的用户名和密码。在本例中，使用了用户名**admin**和密码**cisco**。
3. 选择**VPN/Security Management Solution > Management Center**并且选择**IDS传感器**。
4. 点击Devices选项，选择**传感器组**，突出显示**全局**，并且单击**创建小群**。
5. 输入组名，并保证默认单选按钮已选，然后点击OK，添加子群到IDS MC。
6. 选择设备>传感器，突出显示先前步骤(如测试)创建的子群，并点击Add。
7. 突出显示小群，并且**其次**单击。
8. 根据此示例输入详细信息，然后单击**在旁边**继续。

9. 在您提交与陈述消息后，请点击**芬通社**继续。
10. 您的传感器导入到IDS MC。在这种情况下，传感器5导入。

导入传感器到安全监视器

完成此步骤导入传感器到安全监视器。

1. 在VMS Server菜单，请选择**VPN/安全管理解决方案>监听集中>** Security**箴言报**。
2. 选择Devices选项，然后点击**导入**并且根据此示例输入IDS MC服务器信息。
3. 选择您的传感器(在这种情况下，**传感器5**)并且单击**在旁边**继续。
4. 如果需要，更新您的传感器的网络地址转换(NAT)地址，然后点击Finish，继续。
5. 点击OK键完成导入从IDS MC的传感器到安全监视器。
6. 您的传感器顺利地导入。

请使用IDS MC签名更新

完成此步骤使用IDS MC签名更新。

1. 下载网络ID签名更新(仅限注册用户)从下载并且救他们在您的VMS服务器的C:\PROGRA~1\CSCOpx\MDC\etc\ids\updates\目录。
2. 在VMS服务器控制台，请选择**VPN/Security Management Solution > Management Center >传感器**。
3. 点击Configuration选项，选择**更新**，并且点击**更新网络ID签名**。
4. 选择您想要从下拉菜单升级的签名，然后点击Apply继续。
5. 选择传感器更新，并且单击**在旁边**继续。
6. 提示您更新管理中心以及传感器之后，点击Finish，继续。
7. 远程登录或控制到传感器命令行界面。信息类似于此出现：`sensor5# Broadcast message from root (Mon Dec 15 11:42:05 2003): Applying update` **`IDS-sig-4.1-3-S63. This may take several minutes.`** `Please do not reboot the sensor during this update. Broadcast message from root (Mon Dec 15 11:42:34 2003):` **`Update complete. sensorApp is restarting This may take several minutes.`**
8. 请等待几分钟，以完成升级，然后输入show version 进行 验证。`sensor5#`**`show version`** `Application Partition:` **`Cisco Systems Intrusion Detection Sensor, Version 4.1(3)S63 Upgrade History: * IDS-sig-4.1-3-S62 07:03:04 UTC Thu Dec 04 2003 IDS-sig-4.1-3-S63.rpm.pkg 11:42:01 UTC Mon Dec 15 2003`**

配置IOS路由器的阻塞

完成此步骤配置IOS路由器的阻塞。

1. 在VMS服务器控制台，请选择**VPN/Security Management Solution > Management Center > IDS Sensors**。
2. 选择Configuration选项，选择您的从对象选择器的传感器，并且点击**设置**。
3. 选择**签名**，点击**自定义**，然后单击**添加**添加一个新的签名。
4. 输入新的签名名称，然后选择引擎(在这种情况下，**STRING.TCP**)。
5. 您能通过检查appropriate单选按钮定制可用的参数，并且单击请**编辑**。在本示例中，ServicePorts参数值被编辑更改为23(端口23)。RegexString参数是也编辑的添加值**testattack**。当这完成时，请点击OK键继续。
6. 编辑Signature Severity和Actions，或者启用/禁用签名，点击签名的名字。
7. 在这种情况下，严重性应更改为“高”，同时选中块主机动作。单击 **OK** 继续。块主机阻塞攻击

的IP主机或IP子网。块连接阻塞TCP或UDP端口(根据攻击TCP或UDP连接)。
8. 完整签名看起来类似于此：
9. 为了配置阻塞设备，选择**阻塞>**从对象选择器(在屏幕的左手边的菜单的**阻塞设备**)，和单击**添加**输入以下信息：
10. 单击**编辑接口**(请参阅上一屏幕捕获)，单击**添加**，输入此信息，然后点击OK键继续。
11. 两次点击OK键完成阻塞设备的配置。
12. 要配置阻塞属性，请选择**阻塞>阻塞属性**。可以修改长度自动块。在这种情况下，它更改对**15分钟**。单击**应用**继续。
13. 从主菜单选择Configuration，然后选择Pending，检查待定配置，确保其正确，并点击Save。
14. 要推动配置更改到传感器，选择Deployment>Generate，并点击Apply，生成并部署更改。
15. 选择**Deployment > Deploy**，然后单击**提交**。
16. 在您的传感器旁边检查复选框，然后单击**部署**。
17. 检查复选框在队列的工作，然后单击**在旁边**继续。
18. 输入任务名称并且安排工作如立即，然后点击**芬通社**。
19. 选择**待定的Deployment > Deploy >**。请等待几分钟，直到所有待定工作完成。队列是然后空的。
20. 要确认部署，请选择**Configuration>历史记录**。保证配置的状况显示如**部署**。这意味着传感器配置顺利地更新。

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

启动攻击和阻塞

验证阻塞流程在正常地运作，请发送一个测试攻击，并检查结果。

1. 在启动攻击前，请选择**VPN/安全管理解决方案>监听集中>** Security**箴言报**。
2. 从主菜单选择**箴言报**，点击**事件**和然后单击**启动事件查看器**。
3. 远程登录到路由器(在这种情况下，远程登录到House路由器)，验证传感器的通信。`house#**show user** Line User Host(s) Idle Location * 0 con 0 idle 00:00:00 226 vty 0 idle 00:00:17 **10.66.79.195** house#**show access-list** Extended IP access list IDS_Ethernet1_in_0 10 permit ip host 10.66.79.195 any 20 permit ip any any (20 matches) House#`
4. 如果要发送攻击，请从一个路由器远程登录另一个路由器，同时输入testattack。在这种情况下，我们使用Telnet从光路由器连接到房间路由器。当您输入testattack，并按<space>或<enter>之后，您的Telnet会话将重置。`light#**telnet 100.100.100.1** Trying 100.100.100.1 ... Open User Access Verification Password: house>en Password: house#**testattack** *!--- Host 100.100.100.2 has been blocked due to the !--- signature "testattack" being triggered.* **[Connection to 100.100.100.1 lost]**`
5. 远程登录到路由器(议院)并且输入show access-list命令。`house#**show access-list** Extended IP access list IDS_Ethernet1_in_1 10 permit ip host 10.66.79.195 any *!--- You will see a temporary entry has been added to !--- the access list to block the router from which you connected via Telnet previously.* **20 deny ip host 100.100.100.2 any (37 matches)** 30 permit ip any any`
6. 从Event Viewer，点击Query Database，查询新事件，查看以前发出的警报。
7. 在Event Viewer中，高亮显示并右击告警，然后选择View Context Buffer或View NSDB，查看

告警的更多详细信息。**注意：** NSDB也是线上可以得到的在Cisco Secure百科全书(仅限注册用户)。

故障排除

故障排除步骤

使用为了实现故障排除目的以下步骤。

1. 在IDS MC中，请选择**报告>生成**。根据问题类型，可以从七个可用报告中的一个报告中找到更详细的资料。
2. 在传感器控制台上，输入show statistics networkaccess 命令，然后检查输出，以保证"状态"是活跃状态。`sensor5#**show statistics networkAccess** Current Configuration AllowSensorShun = false ShunMaxEntries = 100 NetDevice Type = Cisco IP = 10.66.79.210 NATAddr = 0.0.0.0 Communications = telnet ShunInterface InterfaceName = FastEthernet0/1 InterfaceDirection = in State ShunEnable = true NetDevice IP = 10.66.79.210 AclSupport = uses Named ACLs State = **Active** ShunnedAddr Host IP = **100.100.100.2** ShunMinutes = **15** MinutesRemaining = **12** sensor5#`
3. 保证通信参数显示正确协议正在使用，例如Telnet或带有3DES的Secure Shell (SSH)。您可以从PC上的SSH/Telnet客户端，尝试SSH或远程登陆，检查用户名和秘密是否正确。您可以从传感器本身尝试远程登陆或SSH到路由器，保证您能够成功登录。

相关信息

- Cisco安全入侵检测支持页
- CiscoWorks VPN/Security Management Solution支持
- 技术支持和文档 - Cisco Systems