配置Firepower 6.1与ISE的pxGrid修正

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 配置 <u>网路置Firepower</u> 配置ISE <u>验证</u> 指除 相关信息

简介

本文描述如何配置Firepower 6.1 pxGrid修正用身份服务引擎(ISE)。Firepower 6.1+ ISE修正模块可以与ISE终端保护业务(EPS)一起使用自动化qurantine/列入黑名单在网络接入层的攻击者。

<u>先决条件</u>

<u>要求</u>

Cisco 建议您具有以下主题的基础知识:

- 思科ISE
- 思科Firepower

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Cisco ISE版本2.0 Patch4
- 思科Firepower 6.1.0
- 虚拟无线局域网控制器(vWLC) 8.3.102.0

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。

配置

此条款用Firepower不包括ISE集成初始配置,与激活目录(AD)的ISE集成,与AD的Firepower集成。 对于此信息请导航对References部分。Firepower 6.1修正模块允许Firepower系统使用ISE EPS功能 (检疫、unquarantine,端口关闭)作为修正,当关联规则匹配时。





流说明:

- 1. 客户端连接对网络,验证与ISE并且点击与准许对网络的无限制访问的授权配置文件的一个授权规则。
- 2. 从客户端的流量然后流经Firepower设备。
- 3. 用户开始执行恶意活动并且点击反过来触发Firepower管理中心的关联规则(FMC)通过pxGrid执行ISE修正。
- 4. ISE分配EPSStatus检疫到终端并且触发RADIUS授权崔凡吉莱对网络接入设备(WLC或交换机)。
- 5. 客户端点击分配限制访问的另一项授权策略(对门户的更改SGT或重定向或拒绝访问)。

Note:应该配置网络接入设备(纳季)发送认为的RADIUS到ISE为了提供它用于映射IP地址到终端的IP地址信息。

配置Firepower

步骤1.配置pxGrid缓解实例。

如镜像所显示,导航对策略>操作>实例并且添加pxGrid缓解实例。

| Overview Analysis Policies Devices Objects AM | P | | Deploy | 0 1 | System | Help 🔻 | admin 🔻 |
|---|----------------|-------------------------|--------|------------|----------|--------------|---------|
| Access Control v Network Discovery Application Detectors | Correlation | Actions > Instances | | | | | |
| | | | | | Alerts F | Remediations | Groups |
| | Edit Instanc | ce | | | | | |
| | Instance Name | ISE-NEW-INSTANCE | | | | | |
| | Module | pxGrid Mitigation(v1.0) | | | | | |
| | | | | | | | |
| | Description | | | | | | |
| | | | | | | | |
| | Enable Logging | ● On C Off | | | | | |
| | | Create Cancel | | | | | |
| | | | | | | | |

步骤2.配置修正。

有两类型联机:缓和目的地并且缓和来源。在此示例来源使用缓解。如镜像所显示,选择修正类型 并且单击**添加**:

| emediation Name | Remediation Type | Description |
|-----------------------|-------------------------|---------------|
| No conf | igured remediations ava | ailable |
| Add a new remediatior | of type Mitigate Desti | ination 💌 🛛 🗛 |
| | Mitigate Desti | nation |

如镜像所显示,分配缓解操作到修正:

| Edit Remediation | |
|--|-------------------|
| Remediation Name | QUARANTINE-SOURCE |
| Remediation Type | Mitigate Source |
| Description | |
| Mitigation Action | quarantine 💌 |
| Whitelist (an <i>optional</i> list of networks) | |
| | Create Cancel |

步骤3.配置关联规则。

导航对**策略>相关性>规则管理**并且单击**创建规则**关联规则是修正的触发能发生。关联规则能包含几 个情况。在此示例关联规则PingDC点击,如果入侵事件发生,并且目的IP地址是192.168.0.121。 如镜像所显示,匹配ICMP echo应答的自定义入侵规则为测验的目的配置:

| Overview Analysis Policies Devices Objects AMP | System Help 🔻 admin |
|--|------------------------------|
| Access Control v Network Discovery Application Detectors Correlation Actions v | |
| | Alerts Remediations Groups |
| Policy Management Rule Management White List Traffic Profiles | |
| Rule Information Image: Add User Qualification Image: Add User Qualification Image: Add User Qualification | d Host Profile Qualification |
| Rule Name PingDC | |
| Rule Description | |
| Rule Group Ungrouped | |
| | |
| Select the type of event for this rule | |
| If an intrusion event occurs 📩 and it meets the following conditions: | |
| Add complex condition | |
| X Destination IP is I192.168.0.121 | |
| | |
| Rule Options | O Add Inactive Period |
| Snooze If this rule generates an event, snooze for 0 hours | |
| Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add Inactive Period". | |

步骤4.配置相关性策略。

如镜像所显示,导航对**策略>相关性>Policy管理**并且单击**创建策略**,增加规则到策略并且分配对它 的答复:

| Overview Analysis Po | olicies Devices Obj | ects AMP | | Deploy ෫ System Help 🔻 admin 🔻 |
|--------------------------|------------------------|--------------------------------------|-----------|--------------------------------|
| Access Control Network | Discovery Application | Detectors Correlation | Actions • | |
| | | | | Alerts Remediations Groups |
| Policy Management | Rule Management | White List Traffic Profi | les | |
| Correlation Policy Info | ormation | You have unsaved changes Save Cancel | | |
| Policy Name | ise_corellation_policy | | | |
| Policy Description | | | | |
| Default Priority | None 💌 | | | |
| Policy Rules | | | | O Add Rules |
| Rule | | Responses | | Priority |
| PingDC | | QUARANTINE-SOURCE (Reme | ediation) | Default 💽 🏼 🌗 🗒 |

如镜像所显示,启用相关性策略:

| Overview Analysis Policies Devices Objects AMP | Deploy 🤑 | System He | elp 🔻 admin 🔻 |
|--|----------|-------------|-----------------|
| Access Control Network Discovery Application Detectors Correlation Actions Actions | | | |
| | | Alerts Reme | diations Groups |
| Policy Management Rule Management White List Traffic Profiles | | | |
| | | | Oreate Policy |
| Name | | Sort b | y State |
| ise corellation policy | | | D 🦉 🐚 🛙 |

配置ISE

步骤1.配置授权策略。

导航对**策略>授权**并且添加将点击的一项新的授权策略,在修正发生后。使用**会话:EPSStatus等于 检疫**作为情况。有可以使用结果的几个选项:

• 允许访问并且分配不同的SGT (请强制执行在网络设备的访问控制限制)

•拒绝访问(用户应该插入在网络外面,并且不应该能再连接)

• 对黑名单门户的重定向(在此方案自定义热点门户为此配置

| diable Identity | Services Engine | Home ▶ Operatio | s velicy | → Guest Access | ► Administration | Work Centers | 1 | License Warning 🔺 | ୍ | 0 | 4 | \$ | | |
|--|---|----------------------|--------------------|------------------------|------------------|--------------|-------------------------|-------------------|---|---|----------|----|--|--|
| Authentication | Authorization Prof | iling Posture Client | Provisioning + | Policy Elements | | | | | | | | | | |
| Authorization Define the Authori For Policy Export | uthorization Policy afine the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. ar Policy Export go to Administration > System > Backup & Restore > Policy Export Page isst Matched Rule Apples | | | | | | | | | | | | | |
| Exceptions | 3 (3) | | | | | | | | | | | | | |
| Status | Rule Name | | Conditions (identi | ity groups and other c | onditions) | | Permissions | | | | | | | |
| 1 / 🗹 | AssignSGTBlockOnFl | b If | Session:EPSState | us EQUALS Quaranti | ne | | MaliciousUser AND Pe | rmitAccess | | E | Edit 🕶 | | | |
| | BlockOnISE | if | Session:EPSSt | atus EQUALS Quarar | ntine | th | en DenyAccess | | | E | Edit 🔻 | | | |
| | BlockOnISE_copy | | f Session:EPS | Status EQUALS Quar | antine | | then blacklist_redirect | | | E | Edit 🕶 | | | |

自定义Portal配置

在本例中,热点门户配置作为**黑名单**。有与自定义文本的仅Acceptable Use Policy (AUP)页,并且 没有接受AUP的可能性(这执行与Javascript)。为了达到此,您首先需要启用Javascript然后粘贴隐 藏AUP按钮和控制在门户自定义配置方面的代码。

步骤1. Enable (event) Javascript。

导航对**管理>System > Admin Access>设置>门户自定义。**选择与HTML和Javascript的Enable (event)门户自定义并且点击"Save"。

| dentity Services Engine | Home > Operations > Policy > Guest Access - Administration > Work Centers 1 License Warning A Q @ 1 🔅 | | | | | | | | | | | | | |
|---------------------------------------|---|--|--|--|--|--|--|--|--|--|--|--|--|--|
| System Identity Management | Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping | | | | | | | | | | | | | |
| Deployment Licensing + Certificate | is → Logging → Maintenance Upgrade Backup & Restore → Admin Access → Settings | | | | | | | | | | | | | |
| 0 | | | | | | | | | | | | | | |
| Authentication Portal Customization | | | | | | | | | | | | | | |
| ► Authorization |) Enable Portal Customization with HTML | | | | | | | | | | | | | |
| Administrators | Enable Portal Customization with HTML and JavaScript | | | | | | | | | | | | | |
| - Settings | Save | | | | | | | | | | | | | |
| Access | | | | | | | | | | | | | | |
| Session | | | | | | | | | | | | | | |
| Portal Customization | | | | | | | | | | | | | | |

步骤2.创建热点门户。

导航对**访客访问>配置>访客门户**并且单击**创建**,然后选择热点类型。

| diaba Identity Services | Engine _{Home} | ▶ Operations | ▶ Policy | ✓ Guest Access | ► Administration | ► Work Centers | 1 | License Warning 🔺 | ् | 0 | £ | \$ |
|-------------------------|------------------------|-----------------|----------------|----------------|------------------|----------------|---|-------------------|---|---|---|----|
| ▼ Configure Manage Ac | counts + Settings | | | | | | | | | | | |
| Overview Guest Portals | Guest Types Spo | onsor Groups Sp | ponsor Portals | | | | | | | | | |
| | | | | | | | | | | | | |
| Guest Portals | | | | | | | | | | | | |

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

Create Edit Duplicate Delete

步骤3.配置门户自定义。

导航对入口页面自定义和更改标题和内容提供一适当的警告给用户。

| diala cisco | Identi | ty Services Er | ngine F | lome 🔸 | Operations | ▶ Policy | ✓ Guest Access | ► Administration | ▶ Work Centers | | 1 | License Warning 🔺 | | | |
|----------------|---------|-----------------|-------------|--------|----------------|-----------------|------------------------|-------------------------|----------------|------|----------|-------------------|-----|--|--|
| ▼ Cor | nfigure | Manage Acco | unts ► Sett | ings | | | | | | | | | | | |
| Overv | /iew | Guest Portals | Guest Types | Sponso | r Groups Sp | onsor Portals | | | | | | | | | |
| P | ages | | | | Page | Customization | s | | | | | | | | |
| | ▼ Pa | ges | | | Browser Pag | ge Title | | | | | | Preview Settings | | | |
| | Acc | eptable Use Po | licy | | Optional Cor | ntent 1 | | | | | du | | | | |
| | Aut | hentication Suc | ccess | | Font X - (2) 8 | 3 | • Size | • <u>A</u> • B I | I ⊞ ∦≣ Ø • | cise | co. R | ESTRICTED ACC | ESS | | |
| | Erro | pr | | | | | | | | RE | | CTED ACCESS | 2 | | |
| | ▼ Me | ssages | | | | | | | | ma | alicious | user and blocked | | | |
| | Erro | or Messages | | | | | | | | | | | | | |
| | | | | | (text or HTM | L) Click Previe | w to test HTML render | ring. | | | | | | | |
| | | | | | Content Title | • | | | | | | | | | |
| | | | | | RESTRICTE | D ACCESS | | | | | | | | | |
| | | | | | Instructional | Text | | | | | | | | | |
| | | | | | Font | 3 | • Size | • <u>A</u> • B I | I ⊞ }≣ ∅ • | | | | | | |
| | | | | | You have be | en identified a | is a malicious user ar | nd blocked. | | | | | | | |

移动对选项内容2,点击乒乓键HTML来源,并且粘贴脚本里面:

```
<script> (function() { jQuery('.cisco-ise-aup-text').hide(); jQuery('.cisco-ise-aup-
controls').hide(); setTimeout(function() { jQuery('#portal-session-timeout-popup-screen, #portal-
session-timeout-popup-popup, #portal-session-timeout-popup').remove(); }, 100); })(); </script>
```

点击Untoggle HTML来源。

Optional Content 2

| Font | | Size | <u>A</u> - 1 | BI | U∣≘ | 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - |
|---|--|---|--|-----------------------|---------------------|---|
| <i>x</i> - | 00 | | | | | |
| <script< th=""><th>></th><th></th><th></th><th></th><th></th><th></th></script<> | > | | | | | |
| (function jQuo jQuo setTim timeou })(); <th>on(){ ery('.cisco-ise-aup-text'). ery('.cisco-ise-aup-contr eout(function(){ jQuery(t-popup-popup, #portal- t></th> <th>hide(); ols').hide(); '#portal-sess session-time</th> <th>ion-timeout-popup out-popup').remov</th> <th>-screen re(); }, 1</th> <th>n, #portal- 00);</th> <th>-session-</th> | on(){ ery('.cisco-ise-aup-text'). ery('.cisco-ise-aup-contr eout(function(){ jQuery(t-popup-popup, #portal- t> | hide(); ols').hide(); '#portal-sess session-time | ion-timeout-popup out-popup').remov | -screen re(); }, 1 | n, #portal- 00); | -session- |
| <th>noz editor bogus node</th> <th>="TRUE" /></th> <th></th> <th></th> <th></th> <th></th> | noz editor bogus node | ="TRUE" /> | | | | |
| | 0 _ | | | | | |

(text or HTML) Click Preview to test HTML rendering.

<u>验证</u>

请使用在此部分被提供为了验证的信息您的配置适当地工作。

Firepower

修正的触发能发生是相关性策略/规则命中数。导航对**分析>相关性>相关性事件**并且验证相关性事件 发生。

| C | Overview | Analy | sis Polici | es Devic | es Obje | cts AMP | | | | | | Deploy | . 😲 System Help | 🔻 admin 🔻 |
|---|---|-----------------|-------------|----------------------------|--------------------|-------------|---------------------|---------------------|---------------------------------|-------------------------------------|---------------|------------------------|------------------------------|-----------------------------|
| (| Context Ex | xplorer | Connections | Intrus | sions 🔻 | Files Hos | its 🔹 Users 🔻 | Vulnerabilities | Correlation | Correlation Events | Custom • Look | up 🔻 Search | | |
| | | | | | | | | | | | Bookmark Th | is Page Report Designe | r Dashboard View Booki | narks Search |
| 9 | Correlation Events 2017-02-16 11:44:29 - 2017-02-16 13:31:0 Correlation Events Expandin | | | | | | | | | | | | | |
| P | Vo Search Constraints (Edit Search) | | | | | | | | | | | | | |
| | Jump to. | | | | | | | | | | | | | |
| | | ▼ <u>Time</u> × | | Impact × | Inline × Result | Source IP × | Source × Country | Destination × IP | Destination × Country | Security Intelligence × Category | Source User × | Destination × User | Source Port / X ICMP Type | Destination Pe ICMP Code |
| | ↓ □ | 2017-02-1 | 6 13:27:51 | 1 | | 172.16.10 | .19 | 192.168.0.121 | | | | | 8 (Echo Request) / icmp | <u>0 / icmp</u> |

ISE

ISE应该然后触发Radius :CoA和重新鉴别用户,这些事件可以验证的运转中> RADIUS Livelog。

| 2017-02-16 13:26:22.894 | | -0 | alice | E4:B3:18:69:EB:8C | Windows10-Workst Default >> Dot1X >> D Default >> AssignSGT MaliciousUser,PermitAcc | vWLC |
|-------------------------|----------|----|-------|-------------------|--|------|
| 2017-02-16 13:26:21.040 | ~ | à | | E4:B3:18:69:EB:8C | | vWLC |
| 2017-02-16 13:25:29.036 | V | 0 | alice | E4:B3:18:69:EB:8C | Windows10-Workst Default >> Dot1X >> D Default >> Standard R PermitAccess,Administra | vWLC |

在本例中, ISE分配不同的SGT **MaliciousUser**到终端。一旦请**拒绝**用户丢失无线连接并且不能再连 接的访问权限配置文件。

与黑名单门户的修正。如果修正授权规则配置重定向到门户,它如下所示:从攻击者方面:

| Sestricted access × + | - 0 | × |
|---|-----------|-----|
| 🗲 🛈 🗞 https://vpalkin-ise20-1.example.com:8443/portal/PortalSetup.action?portal=74d92220-e56a-11e6-b87e-005056993cb38xsessionld=b6 🔻 1 33% 🛛 C 🗍 🔍 Search | ☆ 自 ♣ 余 (| , ≡ |
| CISCO RESTRICTED ACCESS | | ^ |
| RESTRICTED ACCESS You have been identified as a malicious user and blocked. | | |

故障排除

本部分提供了可用于对配置进行故障排除的信息。

如此镜像所显示,导航对**分析>相关性>状态**。

| Overview Analysis Policies Devices Objects AMP | | | | | | | | | | | |
|--|--|--------------|--------------------|-------------------|---------|--------------------------|------------------------|----------|--|--------|--|
| Context Explorer | Connections • | Intrusions 🔻 | Files 🔻 | Hosts 🔻 | Users • | Vulnerabilities v | Correlation + Status | Custom • | Lookup 🔻 | Search | |
| | | | | | | | | | | | Bookmark This Page Report Designer View Bookmarks Search |
| Remediation | Remediation Status 2017-02-16 14:25:00 - 2017-02-16 14:27:00 Table View of Remediations Static | | | | | | | | | | |
| No Search Constraints (<u>Edit Search</u>) | | | | | | | | | | | |
| Jump to 🔻 | | | | | | | | | | | |
| Time | × | | Remediation Name × | | | Policy × | Rule × | | Result Message × | | |
| J 2017-02 | 2-16 14:26:19 | | QUARAN | OUARANTINE-SOURCE | | | ise corellation policy | PingDC | ingDC Successful completion of remediation | | |
| < <page 1="" of="">> Displaying row 1 of 1 rows</page> | | | | | | | | | | | |
| View | Delete | | | | | | | | | | |

结果消息应该返回**修正成功的完成**或特定的错误消息。验证Syslog :**系统> Monitoring> Syslog**和 过滤器输出了与pxgrid。同样日志在/var/log/messages可以验证。

相关信息

- https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html
- <u>https://communities.cisco.com/docs/DOC-68284</u>
- <u>https://communities.cisco.com/docs/DOC-68285</u>
- <u>https://communities.cisco.com/thread/64870?start=0&tstart=0</u>
- http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20.html
- http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-configguide-v61.html