CES ESA的配置最佳实践

目录

简介

本文提供建议摘要使用思科的Cloud电子邮件安全(CES)的管理员的配置他们的思科电子邮件安全工具(ESA)。

先决条件

要求

Cisco 建议您了解以下主题：

- ESA管理， CLI和GUI级别管理

使用的组件

本文档中的信息根据最佳实践和建议CES客户和管理员的。

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。

相关产品

本文档也可用于以下硬件和软件版本：

- ESA (目前)运行AsyncOS的任何版本电子邮件安全的在前提硬件和虚拟设备

CES ESA的配置最佳实践

> 警告： 应该在确认您的在生产环境上的配置更改之前检查和了解对根据最佳实践的配置的所有变化如所提供在本文上。 请与您的CES系统工程师或客户团队协商在您100%不了解也没有舒适，当管理时的进行的配置更改之前。

安全性服务

IronPort反垃圾邮件(IPAS)

- 总是扫描1.5 MB和从未扫描2 MB

URL 过滤

- Enable (event) URL目录和名誉
- Enable (event) Web交互作用跟踪

Graymail检测

- Enable (event)和最大消息容量1 MB

爆发过滤器

- 启用可适应规则，最大值扫描大小1 MB
- 启用Web交互作用跟踪

先进的恶意软件保护

- Enable (event)在启用功能以后的其它文献类型

消息跟踪

- Enable (event)已拒绝连接记录日志(如果必须)

系统管理

用户

- Set password策略
- 若可能验证的利用轻量级目录访问协议(LDAP)

日志订阅

- Enable (event)配置历史记录日志
- Enable (event) URL过滤日志
- 日志另外的报头“从’

CLI级别更改

Web安全SDS URL过滤

- **websecurityadvancedconfig**

```
Do you want to disable DNS lookups? [N]> y

Enter the maximum number of URLs that should be scanned:
[100]> 20

Enter the threshold value for outstanding requests:
[50]> 5

Enter the default time-to-live value (seconds):
[30]> 600

Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
```

URL记录

- ESA启用URL过滤和最佳实践
- **outbreakconfig**

```
Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.
```

反欺骗过滤器

- 伪造的电子邮件检测(联邦机关)以思科电子邮件安全

标记过滤器的报头

- 写入并且启用下列信息过滤器：

```
Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.
```

主机访问表

另外的发送方组

- ESA用户指南： 创建消息处理的一发送方组 SKIP_SBRS –放置高跳过名誉的来源的 SPOOF_ALLOW –一部分的伪装过滤器合作伙伴–TLS被强制的连接

在预定义的SUSPECTLIST发送方组中

- ESA用户指南：发送方验证：主机 enable (event) “在无的SBRS分数”随意地， “连接主机 PTR记录查找的enable (event)发生故障由于临时DNS失败”

积极的帽子示例

- 对-2]策略的黑名单[-10 ：阻止
- 对-1]策略的SUSPECTLIST [-2 ：HEAVYTHROTTLED

- GRAYLIST[-1到2和无]策略：LIGHTTHROTTLED
- 对10]策略的ACCEPTLIST [2 ：已接受

Note:上述帽子示例显示另外配置的邮件流量策略。 关于MFP的全部信息，请参考AsyncOS适当的版本的用户指南电子邮件安全运行的在您的ESA。 示例， AsyncOS 10.0 ：主机访问表(帽子)，发送方组和邮件流量策略

邮件流量策略(默认策略参数)

安全设置

- 设置传输层安全(TLS)为首选的
- 启用发送方政策架构(SPF)
- 启用DomainKeys识别的邮件(DKIM)
- 启用基于域的信息认证、报告和符合(DMARC)验证和发送聚集反馈报告

Note:DMARC要求调整的其他配置。 关于DMARC的全部信息，请参考AsyncOS适当的版本的用户指南电子邮件安全运行的在您的ESA。 示例， AsyncOS 10.0 ：DMARC验证

流入的邮件策略

反垃圾邮件阈值

- 应该留下阈值在默认阈值。 计分的修改能导致错误肯定增加。

防病毒

- 消息扫描：仅病毒的扫描
- Unscannable消息，病毒传染了消息： 集“存档原始消息”对没有

AMP

- 添加“AMP”服从为Unscannable加在前面，禁用“存档消息”

Graymail

- 为每个判决启用的扫描，加在前面主题并且传送
- 添加大批电子邮件的x报头，报头= “X-BulkMail”， “真”的value=

爆发过滤器

- 默认威胁级别是3，根据您的安全需求请调节 如果威胁级为消息等于或超出此阈值，信息将传送对爆发检疫。(1=lowest威胁， 5=highest威胁)
- 启用留言修改。 未签名的消息的重写URL
- 崔凡吉莱主题加在前面对： [Possible $threat_category Fraud]

流出的邮件策略

防病毒

- 消息扫描
- 仅病毒的扫描不选定包括与AV的一个X报头扫描结果消息

- 所有消息：先进>其他通知， enable (event) “其他”和包括admin/SOC联系方式电子邮件地址

策略检疫

PRE创建以下检疫：

- 不相应入站
- 不相应出站
- URL有恶意入站
- URL有恶意出站
- 可疑的欺骗
- 恶意软件

其他设置

字典

- Enable (event)/复核亵渎和性期限字典
- 创建与行政名称的伪造的电子邮件字典
- 创建限制或其他关键字的字典

目的地控制

- 默认目的地的Enable (event) TLS
- 设置webmail域的低限阈值
- 速率限制您与目的地控制设置的自己的出站邮件

内容过滤器

> **Note**:关于内容过滤器的全部信息，请参考AsyncOS适当的版本的用户指南电子邮件安全运行的在您的ESA。 示例， AsyncOS 10.0 ：内容过滤器

不相应的内容过滤器

- 情况亵渎或性字典匹配，发送复制对不相应的检疫

URL有恶意的名誉内容过滤器

- 发送复制对有恶意的URL (-10到-6)检疫

URL类别有选择的这些的内容过滤器

- 成人，色情，虐待儿童，赌博
- 发送复制对不相应的检疫

伪造的电子邮件检测

- 字典名为“Executives_FED”
- FED()阈值90检疫复制

宏观已启用文档内容过滤器

- 如果一个或更多附件包含万家乐
- 可选情况- >从不信任SBRS范围
- 发送复制检疫

附件保护

- 如果一个或更多附件保护
- 可选情况- >从不信任SBRS范围
- 发送复制检疫

相关信息

- BRKSEC-2131 -思科电子邮件安全：最佳实践和微调(2016拉斯维加斯)
- BRKSEC-2131 -非E MAIL人的(2015圣地亚哥)电子邮件安全
- BRKSEC-3770 - (DMARC) -不phish ：深潜到电子邮件验证技术(2014旧金山)里
- CES终端用户许可权协定
- CES服务说明
- 思科通用Cloud期限
- 技术支持和文档 - Cisco Systems