CES ESA的配置最佳实践

Contents

Introduction

本文提供推荐汇总对使用思科的Cloud电子邮件安全(CES)的管理员的配置他们的Cisco电子邮件安全工具(ESA)。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- ESA管理， CLI和GUI级别管理

Components Used

本文的信息根据最佳实践和推荐对CES用户和管理员。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

相关产品

本文档还可与以下硬件和软件版本一起使用：

- 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工具

CES ESA的配置最佳实践

> **警告：** 应该在确认您的在生产环境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系统工程师或客户小组协商在做您100%不了解也没有舒适，当管理时的配置更改之前。

基本配置

接收访问表(RATS)

在接收访问表里配置的入站邮件域

SMTP路由

如果smtp路由目的地是365主机的办公室，

安全服务

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

- Enable (event)可适应的规则，最大扫描大小1 MB
- Enable (event) Web交互作用跟踪

先进的Malware保护

- Enable (event)在启用功能以后的其它文献类型

消息跟踪

- Enable (event)被拒绝的连接记录(如果必须)

LDAP

如果曾经LDAP，请推荐使用LDAP以被启用的SSL。

SPF

提供指令在添加CES主机到用户的现有的SPF记录。宏指令为所有CES主机发布每个分配主机名-使更加容易添加所有主机：

在~all前放置以下宏指令或-所有在当前TXT/SPF内记录是否存在。

```
exists:%{i}.spf.<allocation>.iphmx.com
```

> **Note**: 保证spf与或者**~all的**记录结束或**-所有**。放置spf记录的这部分别处可能导致错误邮件发送问题。请在做任何变动前总是验证。

在所有更改前后，验证用户的域的SPF记录

示例工具：

- 验证现有记录：
- https://www.kitterman.com/spf/validate.html ?
- PRE验证提出的更改：

SPF记录的基本元素的细分。

[v=spf1]This识别TXT记录作为SPF记录。
[exists]执行记录存在
用连接IP替换的**[%{i}]**宏观表达式。
[-all]失败： 只请允许匹配其中一个参数的邮件(IPv4、MX等等)在记录

[all] SoftFail ： 允许邮件是否匹配在记录的参数

更多SPF示例

如果在CES接受并且从其他邮件服务器发送outbound邮件，一个好开始是以下示例。 您能使用“a：”指定邮件主机的机制。

```
v=spf1 mx a:mail01.yourdomain.com a:mail99.yourdomain.com ~all
```

如果通过CES发送仅outbound邮件，您可能使用：

```
v=spf1 mx exists:%{i}.spf.<allocation>.iphmx.com ~all
```

在本例中， "ip4:"或"ip6:"机制用于指定IP地址或IP地址范围。

```
v=spf1 exists:%{i}.spf.<allocation>.iphmx.com ip4:192.168.0.1/16 ~all
```

系统管理

用户

- Set password策略
- 若可能认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

- 入门Enable (event)伪造了电子邮件检测(联邦机关)在Cisco电子邮件安全

标记过滤器的报头

- 写和enable (event)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： 创建消息处理的一个发送方组 SKIP_SBRS –为跳过名誉的来源放置更高 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

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

积极的帽子示例

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

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

Note:上述帽子示例显示另外被配置的邮件流量策略。 关于MFP的全部信息，请参见AsyncOS的适当的版本的用户指南运行在您的ESA的电子邮件安全的。 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)对更喜欢
- Enable (event)发送方政策架构(SPF)
- Enable (event) DomainKeys被识别的邮件(DKIM)
- Enable (event)基于域的信息验证，报告和符合(DMARC)验证和发送聚集反馈报告

Note:DMARC要求另外调整配置。 关于DMARC的全部信息，请参见AsyncOS的适当的版本的用户指南运行在您的ESA的电子邮件安全的。 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。 计分的修改能导致假善意告警增量。

抗病毒

- 消息扫描：仅病毒的扫描
- Unscannable消息，病毒传染了消息： 设置“档案原始消息”对没有

AMP

- 添加“AMP”服从为Unscannable加在前面，功能失效“档案消息”

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整 如果消息的威胁级别等于或超出此阈值，信息将传送到爆发检疫。(1=lowest威胁， 5=highest威胁)
- 启用留言修改。 未签名的消息的重写URL
- 更改主题加在前面对： [Possible $threat_category Fraud]

Whitelist邮件策略

Whitelist邮件策略配置有Antispam，并且Graymail禁用。

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	BLACKLIST	Disabled	Disabled	Disabled	Disabled	BLACKLIST_DROP	(use default)	
2	WHITELIST	Disabled	(use default)	(use default)	Disabled	(use default)	Retention Time: Virus: 1 day Other: 4 hours	

黑名单邮件策略

黑名单邮件策略配置有内容过滤器的服务被禁用的所有和链路有丢弃的动作的。

Blacklist_Drop

通过连接创建内容过滤器对GUI >邮件策略>流入内容过滤器

请勿指定情况和Drop()的动作

连接内容过滤器通过邮寄策略的returing列入黑名单邮件策略>流入的邮件策略>黑名单>内容过滤器

Edit Incoming Content Filter

Mode —**Cluster: Hosted_Cluster** Change Mode...

Centralized Management Options

Content Filter Settings

Name:	Blacklist_Drop
Currently Used by Policies:	Blocklist Policy
Editable by (Roles):	Cloud Operator
Description:	Blocklist
Order:	4 *(of 22)*

Conditions

Add Condition...

There are no conditions, so actions will always apply.

Actions

Add Action...

Order	Action	Rule	Delete
Final	Drop (Final Action)	drop()	

Cancel Submit

流出的邮件策略

抗病毒

- 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outbound
- URL有恶意入站
- URL有恶意outbound
- 可疑的欺骗
- Malware

其他设置

字典

- Enable (event)/复核亵渎和性术语字典
- 用行政名字创建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域的下限值
- 速率限制您与目的地控制设置的自己的outbound邮件

内容过滤器

> **Note**:关于内容过滤器的全部信息，请参见AsyncOS的适当的版本的用户指南运行在您的ESA的电子邮件安全的。 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，发送复制到不相应的检疫

URL有恶意的名誉内容过滤器

- 发送复制到有恶意的URL (-10到-6)检疫

URL类别有这些的内容过滤器选择了

- 成人，色情，虐待儿童，赌博
- 发送复制到不相应的检疫

伪造的电子邮件检测

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

宏观启用文件内容过滤器

- 如果一个或更多附件包含一个宏指令
- 可选的情况- >从不信任的SBRS范围
- 发送复制检疫

附件保护

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

Related Information

- BRKSEC-2131 -Cisco电子邮件安全：最佳实践和优化(2016拉斯维加斯)
- BRKSEC-2131 -非E邮件人的(2015圣地亚哥)电子邮件安全
- BRKSEC-3770 - (DMARC) -不phish ：深潜到电子邮件认证技术(2014旧金山)里
- CES终端用户许可权协定
- CES服务说明
- Cisco通用Cloud术语
- **Technical Support & Documentation - Cisco Systems**
- SPF记录语法
- 验证与SPF ：-所有或~all