了解与邮件流策略和目标控制相关的参数

目录

简介

本文档介绍邮件安全设备(ESA)在如何限制/速率限制发件人和发送方面的一些配置方面。本文将介绍的功能是邮件流策略和目标控制。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解邮件流策略和目标控制
- 熟悉ESA配置中这些功能的使用

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

邮件流策略和目标控制的优点

这两个功能都具有一个非常重要的功能，即速率限制/限制。此方面有助于管理员控制哪些流量应该自由流动，哪些流量应允许限制。

邮件流策略

这些策略适用于ESA的发件人组，根据这些策略执行邮件流量调制。

邮件流策略始终适用于传入到ESA的流量，而不考虑邮件是入站或出站的流量。

邮件流策略在后端与该策略的所选连接行为相关。ESA中可用的不同连接行为包括：

1. 接受
2. 拒绝
3. 中继
4. TCP拒绝
5. 继续

接受：接受连接，然后邮件接受受受到监听程序设置（包括收件人访问表）的进一步限制（适用于公共侦听程序）。 此连接行为将电子邮件视为入站邮件

拒绝：尝试连接的客户端获取4XX或5XX SMTP状态代码。不接受任何电子邮件。这主要用于黑名单发件人

中继：接受连接。允许接收任何收件人，且不受收件人访问表的限制。这会将邮件视为出站邮件

TCP拒绝：在TCP级别拒绝连接。

继续：HAT中的映射被忽略，HAT的处理继续。如果传入连接与以后不为CONTINUE的条目匹配，则使用该条目。CONTINUE规则用于在GUI中简化HAT的编辑。

邮件流策略的组件

最大值.每个连接的消息数：每个连接可通过此侦听程序从远程主机发送的最大邮件数。每个ICID描述一个连接

最大值.每封邮件的收件人数：使用此邮件流策略处理的从此主机接受的每封邮件的最大收件人数

最大值.消息大小:此侦听程序将接受标记到邮件流策略的邮件的最大大小。最小的最大邮件大小为1千字节。

最大值.来自单个IP的并发连接：允许从单个IP地址连接到此侦听程序的最大并发连接数。

自定义SMTP标语代码：与此侦听程序建立连接时返回的SMTP代码。

自定义SMTP标语文本：与此侦听程序建立连接时返回的SMTP标语文本。可以在此字段中使用一些变量。

覆盖SMTP标语主机名：默认情况下，当向远程主机显示SMTP标语（例如，220-hostname ESMTP）时，设备将包括与侦听程序接口关联的主机名。 您可以在此处输入不同的主机名来覆盖

此标语。此外，您可以将主机名字段留空，以选择不在标语中显示主机名。

邮件流限制

最大值.每小时收件人数：此侦听程序每小时从远程主机接收的最大收件人数。全局跟踪每个发件人IP地址的收件人数量。每个侦听程序都会跟踪自己的速率限制阈值，但是，由于所有侦听程序都根据单个计数器进行验证，因此，如果同一IP地址（发送方）连接到多个侦听程序，则更有可能超出速率限制。可以在此字段中使用一些变量。

最大值.每小时收件人代码：当主机超过为此侦听程序定义的每小时最大收件人数时返回的SMTP代码。

最大值.每小时收件人文本：当主机超过为此侦听程序定义的每小时最大收件人数时，返回的SMTP标语文本。

信封发件人的速率限制

最大值.每时间间隔收件人数：根据邮件发件人地址，此侦听程序在指定时间段内从唯一信封发件人接收的最大收件人数。全局跟踪收件人数。每个侦听程序跟踪其自己的速率限制阈值；但是，由于所有侦听程序都对单个计数器进行验证，因此如果多个侦听程序收到来自同一邮件发件人地址的邮件，则更有可能超出速率限制。

发件人速率限制错误代码：当信封超过为此侦听程序定义的时间间隔内的最大收件人数时，返回的SMTP代码。

发件人速率限制错误文本：当信封发件人超出为此侦听程序定义的时间间隔内的最大收件人数时，返回的SMTP标语文本。

例外： 如果希望某些信封发件人免除定义的速率限制，请选择包含信封发件人的地址列表。

地址列表从邮件策略(Mail Policies)>地址列表（完整邮件地址、域、IP地址可用于豁免）定义

将SenderBase用于流控制：为此侦听程序启用对SenderBase信誉服务的“查找”。

按IP地址的相似性分组：用于在管理大型CIDR块中侦听程序主机访问表(HAT)中的条目时按IP地址跟踪传入邮件并对其进行速率限制。您可以定义一个有效位范围（从0到32），根据此范围对类似IP地址进行分组以便进行速率限制，同时仍为该范围内的每个IP地址保留一个单独的计数器。

NOTE:需要禁用“Use SenderBase”。

目录搜集攻击防御(DHAP)

最大值.每小时无效收件人数：此侦听程序每小时从远程主机接收的无效收件人的最大数量。此阈值表示RAT拒绝和SMTP Call-Ahead服务器拒绝的总数，以及SMTP会话中丢弃或工作队列中退回的无效LDAP收件人的邮件总数（如关联侦听程序的LDAP接受设置中配置）。

如果SMTP会话中达到DHAP阈值，则丢弃连接：

如果达到无效收件人的阈值，设备将断开与主机的连接。

最大值.每小时无效收件人代码：指定删除连接时要使用的代码。默认代码为550。

最大值.每小时无效收件人文本：指定用于丢弃的连接的文本。默认文本为“无效收件人太多。

安全特性

垃圾邮件/AMP/病毒/发件人域信誉验证/病毒爆发过滤器/高级网络钓鱼防护/灰色邮件/内容和邮件过滤器：安全引擎/扫描和过滤器的相关扫描可从此处启用或禁用

加密和身份验证：我们可以在此侦听程序的SMTP会话中将设置修改为关闭、首选或要求传输层安全(TLS)。

如果客户端证书有效，则验证客户端证书选项会指示邮件安全设备建立到用户邮件应用的TLS连接。

对于TLS首选，如果用户没有证书，设备仍允许非TLS连接，但如果用户具有无效证书，则拒绝连接。

对于TLS Required设置，选择此选项要求用户拥有有效的证书，以便设备允许连接。

SMTP身份验证：允许、禁止或要求从连接到侦听程序的远程主机进行SMTP身份验证

如果同时启用TLS和SMTP身份验证：要求TLS提供SMTP身份验证

域密钥/DKIM签名：在此侦听程序上启用域密钥或DKIM签名

DKIM验证：启用DKIM验证。

S/MIME解密/验证：启用S/MIME解密或验证。

处理后签名：选择在S/MIME验证后是保留还是从邮件中删除数字签名。

S/MIME公钥搜集：启用S/MIME公钥搜集。

验证失败时收集证书：如果传入签名邮件的验证失败，请选择是否收集公钥。

存储更新的证书：选择是否收集更新的公钥

SPF/SIDF验证： 在此侦听程序上启用SPF/SIDF签名。

一致性级别：设置SPF/SIDF一致性级别。您可以从SPF、SIDF或SIDF兼容中进行选择

如果使用“Resent-Sender：”或“Resent-From：”，则降级PRA验证结果：如果选择兼容SIDF的一致性级别，请配置是否要将PRA身份验证的Pass结果降级为None（如果存在重发发件人）：或重发自：邮件中显示的信头

HELO测试：配置是否要根据HELO标识执行测试（将此用于SPF和SIDF兼容一致性级别）

DMARC验证：在此侦听程序上启用DMARC验证

使用DMARC验证配置文件：选择要在此侦听程序上使用的DMARC验证配置文件。从邮件策略 — >

DMARC —>添加配置文件创建相同的策略

DMARC反馈报告：启用发送DMARC汇总反馈报告。

退回验证

认为无标记退回有效：仅在启用退回验证标记时应用。默认情况下，设备会认为无标记退回无效，并会拒绝退回或添加自定义信头，具体取决于退回验证设置。如果您选择将无标记退回视为有效，设备将接受退回邮件。

发件人验证

信封发件人DNS验证：

发件人可能因不同原因未经验证。未验证发件人分为以下类别：

- DNS中不存在连接主机PTR记录。
- 由于临时DNS故障，连接主机PTR记录查找失败。
- 连接主机反向DNS查找(PTR)与正向DNS查找(A)不匹配。

我们可以启用或禁用发件人验证功能。

使用发件人验证例外表：我们可以使用发件人验证域例外表来允许豁免。我们只能有一个例外表，但可以按邮件流策略启用。

例外表可以从邮件策略(Mail Policies)->发件人验证例外表(Sender Verification Exception Table)->添加发件人验证例外(Add Sender Verification Exception)创建

目标控制

此功能可控制邮件传送。通过ESA完成处理并即将退出ESA以进一步交付的所有邮件都可通过目标控制功能进行控制。

默认目**标控**制配置文件适用于所有交货。以防万一，需要特定于域的交付控制，然后我们必须创建自定义的目标控制配置文件。

目标控制配置文件的组件

限制

并发连接：设备将尝试打开以完成传送的与远程主机的同时连接(DCID)数。

每个连接的最大消息数：ESA将通过连接(DCID)发送到目标域的消息数，然后设备启动新连接。

收件人：设备将在给定时间段内发送给给定远程主机的收件人数。

应用限制：这些方面有助于确定如何应用我们在每个目标和每个MGA主机名上指定的限制。

TLS支持

这有助于确定到远程主机的TLS连接是否设置为无/首选/必需

DANE支持：如果将DANE配置为“Osprotic”，并且远程主机不支持DANE，则机会TLS是加密SMTP会话的首选。

如果将DANE配置为“强制”，并且远程主机不支持DANE，则不会与目标主机建立连接。

如果将DANE配置为“Mandatory”或“Ospritic”，并且远程主机支持DANE，则它首选用于加密SMTP会话。

NOTE:对于已配置SMTP路由的域，不会实施DANE。

退回验证

这有助于确定是否通过退回验证执行信封发件人地址标记(prvs-xxxxx-xxxx)。

可以从邮件策略 — >退回验证 — >添加新密钥配置退回验证

退回配置文件

退回配置文件可由设备用于给定远程主机。它决定在硬退回电子邮件之前，如果存在交付问题，电子邮件在ESA的交付队列中保留多长时间

退回配置文件通过Network —> Bounce Profiles设置

全局设置

证书:这是我们定义在建立SSL/TLS连接时要使用的证书，同时启动到下一跳的邮件传送。始终建议在此方面使用证书颁发机构(CA)签名的证书。

当所需的TLS连接失败时发送警报：我们可以指定在向需要TLS连接的域传送邮件时，如果TLS协商失败，设备是否发送警报。警报消息包含失败TLS协商的目标域的名称。设备将警报消息发送给所有收件人，这些收件人设置为接收**系统警**报类型的警**告严重**级别警报。

我们可以通过“系统管理”(System Administration)—>“警报”(Alerts)管理警报收件人