网络安全设备设计指南

目录

简介

本文档介绍如何设计思科网络安全设备(WSA)和相关组件以实现最佳性能。

背景信息

当您为WSA设计解决方案时，不仅要仔细考虑设备本身的配置，还要考虑相关网络设备及其功能。每个网络都由多台设备协作，如果其中一台设备不能正确参与网络，则用户体验可能会下降。

配置WSA时必须考虑以下两个主要组件：硬件和软件。硬件有两种不同类型。第一种是硬件的物理类型，如S170、S380和S680系列型号，以及其他寿命终止(EoL)型号，如S160、S360、S660、S370和S670系列型号。另一种硬件类型是虚拟的，例如S000v、S100v和S300v系列型号。在此硬件上运行的操作系统(OS)称为*AsyncOS for Web*，它以FreeBSD为核心。

WSA提供代理服务，并扫描、检查和分类所有流量(HTTP、HTTPS和文件传输协议(FTP))。 所有这些协议都在TCP上运行，并且严重依赖域名系统(DNS)来正确运行。因此，网络运行状况对于设备的正常运行及其与网络不同部分（包括企业控制内部和外部）的通信至关重要。

设计

使用本节中介绍的信息设计WSA和相关组件，以实现最佳性能。

网络

无错误、快速的网络对于WSA的正确运行至关重要。如果网络不稳定，用户体验可能会下降。网络问题通常在网页访问时间较长或无法访问时检测到。最初的倾向是将设备归咎于设备，但通常是网络行为不当。因此，应仔细考虑和审核，以确保网络为HTTP、HTTPS、FTP和DNS等高级应用协议提供最佳服务。

一般注意事项

为确保最佳网络行为，您可以实施以下一些一般注意事项：

- 确保第2层(L2)网络稳定，生成树操作正确，并且生成树计算和拓扑更改不频繁。
- 使用的路由协议还应提供快速收敛和稳定性。开放最短路径优先(OSPF)快速计时器或增强型内部网关路由协议(EIGRP)是此类网络的理想选择。
- 始终在WSA上至少使用两个数据接口：一个面向最终用户计算机，另一个面向出站操作（连接到上游代理或互联网）。 这样做是为了消除可能的资源限制，例如当TCP端口数耗尽或网络缓冲区变满时（尤其对内部和外部使用单个接口）。
- 将管理接口专用于仅管理流量，以提高安全性。要通过GUI实现此目的，请导航至**Network > Interfaces**并选中**Separate routing(M1 port restricted to appliance management services only)复选框。**
- 使用快速DNS服务器。通过WSA的任何事务都至少需要一次DNS查找（如果不在缓存中）。DNS服务器速度慢或行为不当会影响任何事务，并被视为延迟或缓慢的互联网连接。
- 使用单独的路由表时，这些规则适用：

  所有接口都包含在默认管理路由表中(M1、P1、P2)。

  “数据”路由表中只包含数据接口。

  注意：路由表的分离不是按接口，而是按服务。例如，WSA和Microsoft Active Directory(AD)域控制器之间的流量始终遵循管理路由表中指定的路由，并且可以配置指向此表中P1/P2接口之外的路由。不能在使用管理接口的数据路由表中包含路由。

负载均衡

为确保最佳网络行为，您可以实施以下一些负载均衡注意事项：

- DNS轮替 — 这是当单个主机名用作代理时使用的术语，但它在DNS服务器上有多个A记录。每个客户端将其解析为不同的IP地址并使用不同的代理。限制在于，DNS记录的更改在重新启动（本地DNS缓存）后反映在客户端上，因此，如果必须进行更改，它会提供较低的稳定性。但是，这对最终用户是透明的。
- 代理地址控制(PAC)文件 — 这些是代理自动脚本文件，根据浏览器中写入的功能确定如何在浏览器上处理每个URL。它具有始终直接转发同一URL或转发到同一代理的功能。
- 自动发现 — 介绍如何使用DNS/DHCP方法来获取PAC文件（在前面的注意事项中介绍）。 通常，前三个考虑事项会合并到一个解决方案中。但是，这可能非常复杂，而且许多用户代理（如Microsoft Office、Adobe下载程序、Javascript和Flash）根本无法读取PAC文件。
- Web缓存控制协议(WCCP) — 此协议（尤其是WCCP版本2）提供了一种强大且功能强大的方法，可在多个WSA之间创建负载均衡，并且融合了高可用性。

- 独立的负载均衡设备 — 思科建议您将负载均衡器用作专用计算机。

防火墙

下面是一些防火墙注意事项，您可以实施这些注意事项以确保最佳网络行为：

- 确保允许来自每个源的Internet控制消息协议(ICMP)在整个网络中运行。这非常重要，因为WSA取决于路径最大转换单元(MTU)发现机制(如RFC 1191中所述)，该机制取决于ICMP回应请求(类型��和回应应答（类型0），并且需要ICMP不可达分段（类型3，代码4）。 如果使用**pathmtudiscovery** CLI命令在WSA上禁用路径MTU发现，则WSA会按照RFC 879使用默认MTU 576字节。这会因增加开销和重组数据包而影响性能。

- 确保网络内部不存在非对称路由。虽然这在WSA上不是问题，但路径上遇到的任何防火墙都会丢弃数据包，因为它没有收到通信的两端。

- 使用防火墙，将WSA IP地址排除在威胁之外是非常重要的，因为这是常规终端计算机站。防火墙可能会阻止
- 由于连接太多（根据一般防火墙知识）导致的WSA IP地址。

- 如果对客户端设备上的任何WSA IP地址使用网络地址转换(NAT)，请确保每个WSA在NAT中使用单独的外部全局地址。如果对具有单个外部全局地址的多个WSA使用NAT，您可能会遇到以下问题：

  从所有WSA到外部世界的所有连接都使用一个外部全局地址，防火墙资源会迅速耗尽。

  如果向该单个目标的流量激增，则目标服务器可能会阻止该流量并切断整个企业对此资源的访问。这可能是公司云存储、办公室云连接或每台计算机防病毒软件更新的宝贵资源。

身份

请记住，*逻辑AND*原则适用于身份的所有组件。例如，如果同时配置用户代理和IP地址，则表示来自此IP地址的*用户*代理。它不表示用户代理*或*此IP地址。

使用一个身份对同一代理类型（或无代理）和/或用户代理进行身份验证。

必须确保需要身份验证的每个身份都包括支持代理身份验证的已知浏览器/用户代理的用户代理字符串，例如Internet Explorer、Mozilla Firefox和Google Chrome。有些应用需要Internet访问，但不支持代理/WWW身份验证。

标识自上而下与搜索第一个匹配条目上结束的匹配项进行匹配。因此，如果您配置了*身份1*和*身份2*，并且事务与身份1匹配，则系统不会根据身份2检查该事务。

访问/解密/路由/出站恶意软件策略

这些策略适用于不同类型的流量：

- 访问策略应用于纯HTTP或FTP连接。它们确定应接受还是丢弃事务。

- 解密策略确定HTTPS事务是应解密、丢弃还是通过。如果事务被解密，则其连续部分可视为纯HTTP请求，并与访问策略匹配。如果必须删除HTTPS请求，请将其放在解密策略中，而不是访问策略中。否则，它会消耗更多CPU和内存，用于首先解密然后丢弃的丢弃事务。

- 路由策略在允许通过WSA后确定事务的上游方向。如果存在上游代理或WSA处于连接器模式并将流量发送到云网络安全塔，则*此情况*适用。

- 出站恶意软件策略针对从最终用户到Web服务器的HTTP或FTP上传应用。这通常是HTTP发布请求。

对于每种策略类型，务必记住逻辑OR*原则*适用。如果引用了多个身份，则事务应匹配所配置的任何身份。

要实现更精细的控制，请使用这些策略。每个策略配置错误的身份可能会产生问题，其中使用策略中引用的多个身份更有益。请记住，身份不会影响流量，它们只标识稍后在策略中匹配的流量类型。

通常，解密策略使用身份和身份验证。虽然这并不错误，有时也需要，但使用身份与解密策略中引用的身份验证意味着所有与解密策略匹配的事务都会被解密，以便进行身份验证。解密操作可能会被丢弃或通过，但是，由于存在具有身份验证的身份，因此会进行解密，以便稍后丢弃或通过流量。这很昂贵，应避免。

已观察到包含30个或更多身份和30个或更多访问策略的某些配置，其中所有访问策略都包含所有身份。在这种情况下，如果所有访问策略中都匹配这些身份，则无需使用这些身份。虽然这不会损害设备运行，但会使故障排除尝试产生混乱，并且在性能方面成本高昂。

自定义URL类别

自定义URL类别的使用是WSA上常常被误解和误用的强大工具。例如，有配置包含身份中匹配项的所有视频站点。WSA具有内置工具，可在视频站点更改URL时自动更新，这种情况经常发生。因此，允许WSA自动管理URL类别，并对特殊的尚未分类的站点使用自定义URL类别是有意义的。

对正则表达式要特别小心。如果使用点(.)和星(*)等特殊字符匹配，则它们可能会证明CPU和内存非常丰富。WSA将扩展任何正则表达式，使其与每个事务相匹配。例如，以下是正则表达式：

```
example.*
```

此表达式将匹配包含单词example的任何URL，*而不*仅是example.*com*域。避免在正则表达式*中*使用*点和*星，并仅将其用作最后手段。

以下是可能引起问题的正则表达式的另一个示例：

```
www.example.com
```

如果在Regular Expressions字段中使用此示例，它不仅会匹配*www.example.com*，还会匹配*www.www3example2com.com*，因为此处的点表示任*何字符*。如果您只想匹配*www.example.com*，请转*开圆*点：

```
www\.example\.com
```

在这种情况下，如果可以将此功能包含在自定义URL类别域中，则没有理由使用正则表达式功能，其格式如下：

防恶意软件和信誉

如果启用了多个扫描引擎，请考虑启用自适应扫描的选项。自适应扫描是WSA上功能强大但小型的引擎，可预扫描每个请求并确定扫描请求时应使用的综合引擎。这会略微提高WSA的性能。