Web安全工具设计指南

目录

简介

本文描述如何设计思科Web安全工具(WSA)和最佳性能的相关的组件。

背景信息

当您设计WSA的时一解决方案，要求仔细的考虑，不仅关于设备的配置，而且相关的网络设备和他们的功能。每网络是体验也许拒绝多个设备和，如果他们中的一个不正确地参加网络，然后用户的协作。

有必须考虑的两个主要组件，当您配置WSA时：硬件和软件。硬件进来两个不同的类型。第一是物理硬件类型，例如生活(EoL)型号S170、S380和S680系列型号，以及另一端，例如S160、S360、S660、S370和S670系列型号。另一种硬件类型是虚拟，例如S000v、S100v和S300v系列型号。操作系统(OS)在的此硬件运行呼叫*Web的AsyncOS*，根据在其核心的FreeBSD。

WSA提供代理服务并且扫描，检查，并且分类所有流量(HTTP、HTTPS和文件传输协议(FTP))。所有在TCP顶部的这些协议正在运行和非常依靠正常操作的域名系统(DNS)。对于这些原因，网络健康是对设备的正常操作和其与网络的多种部分的通信至关重要，在企业控制内外。

设计

请使用在此部分描述为了设计WSA和涉及的组件最佳性能的信息。

网络

无错，快速网络是对WSA的正常操作至关重要。如果网络是不稳定的，用户体验也许拒绝。网络问题通常检测，当网页采取更加长到达时或是不可得到的。最初的倾向是责备设备，但是它通常是行为不端的网络。因此，应该做仔细的考虑和审计为了保证网络提供高层次应用协议的最好的服务例如HTTP、HTTPS、FTP和DNS。

一般考虑事项

这是您能实现为了保证最好的网络工作情况的一些一般考虑事项：

- 保证Layer2 (L2)网络稳定的，生成树操作正确，并且没有常见的生成树计算和拓扑更改。
- 使用的路由协议应该也提供快速收敛和稳定性。开放最短路径优先(OSPF)快速计时器或增强的内部网关路由选择协议(EIGRP)是这样网络的好选择。
- 总是请使用在WSA的至少两个数据接口：面对最终用户计算机的一和另一个出站操作的(连接对上行代理或互联网)。这执行为了排除可能的资源限制条件，例如，当TCP端口数量用尽时或，当网络缓冲变得全双工时(与使用单个接口为在特别是内外)。
- 投入仅管理流量的管理接口为了强化安全。为了通过GUI达到此，请导航对**网络>接口**并且检查**分开的路由(M1端口限制对仅设备管理服务)**复选框。
- 请使用快速DNS服务器。所有处理通过WSA要求至少一DNS查找(如果不在缓存)。慢或行为不端影响所有处理和被观察作为延迟的或缓慢的Internet连接的DNS服务器。
- 当使用时分开的路由路线表，这些规则适用：

  所有接口在默认*管理*路由表(M1、P1， P2)里包括。

  仅数据接口在*数据*路由表里包括。

  Note:路由表的分离是没有每个接口，然而相当每服务。例如， WSA和Microsoft Active Directory (AD)域控制器之间的流量总是服从在管理路由表里指定的路由，并且配置在此表里指出P1/P2接口的路由是可能的。包括使用管理接口的路由在数据路由表里是不可能的。

负载均衡

这是您能实现为了保证最好的网络工作情况的一些负载平衡考虑事项：

- DNS循环â 这是此术语用于，当单个主机名使用作为代理时，但是有在DNS服务器的多个A记录。每个客户端解决此对一个不同的IP地址并且使用不同的代理。限制是DNS记录更改在客户端反射在重新启动(缓存的本地DNS)，因此提供低水平稳健性，如果必须做变动。然而，这是透明对最终用户。
- 代理地址控制(PAC)文件â 这些是确定的代理自动脚本文件如何在根据写入的功能的浏览器在它里面应该处理每个URL。它有功能转发同样URL总是直接地或对同一个代理。

- 自动发现â 这描述使用DNS/DHCP方法为了得到PAC文件(描述在上一个考虑事项)。通常，这些前三考虑事项被结合到一解决方案。然而，这可以是复杂的，并且许多用户代理，例如微软办公软件， Adobe下载者， Javascript和闪存，不能读PAC文件。

- WEB缓存控制协议(WCCP) â 此协议(特别是WCCP版本2)提供一个稳健和非常强大的方式创建在几之间的负载平衡WSAs并且合并高可用性。

- 分开的负载平衡设备â 思科建议您使用负载均衡设备作为专用的机器。

防火墙

这是您能实现为了保证最好的网络工作情况的一些防火墙考虑事项：

- 保证互联网控制消息协议(ICMP)允许在从每来源的网络中。这是重要的，因为WSA取决于路径最大转换单元(MTU)发现机制，正如RFC 1191所描述，取决于ICMP echo请求(类型8)和Echo replies (类型0)，并且ICMP不可达的分段要求(type3，代码4)。如果禁用在WSA的路径MTU发现与CLI命令的**pathmtudiscovery**，则WSA根据RFC 879使用576个字节默认MTU。这影响性能由于增加的开销和数据包重组。

- 保证没有不对称的路由在网络里面。当这不是在WSA时的一问题，沿路径遇到的所有防火墙丢弃数据包，因为未接收通信的两边。

- 使用防火墙，从威胁屏蔽WSA IP地址作为正常末端计算机站点是非常重要的。防火墙也许列入黑名单WSA IP地址由于许多连接(根据一般防火墙知识)。

- 如果网络地址转换(NAT)为在客户驻地设备的任何WSA IP地址被使用，请保证每个WSA在NAT使用一个分开的外部全局地址。如果使用NAT有单个外部全局地址的多个WSAs，您也许遇到这些问题：

  所有从所有的连接WSAs对外界使用单个外部全局地址和防火墙迅速用尽资源。

  如果有流量尖峰往该单个目的地的，目标服务器也许列入黑名单它和中断从访问的整个企业到此资源。这也许是重要的资源作为公司Cloud存储设备、办公室Cloud连接或者每计算机防病毒软件更新。

标识

切记*逻辑和*原理在标识的所有组件应用。例如，如果配置用户代理和IP地址，它含义*从*此IP地址的用户代理。它不含义用户代理*或*此IP地址。

请使用一标识同一个代理人类型(或没有代理人)并且/或者用户代理的验证。

保证要求验证包括已知浏览器/用户代理支持代理验证，例如Internet Explorer， Mozilla Firefox和谷歌镀铬物的用户代理字符串的每标识是重要的。有要求互联网访问的一些应用程序，但是不支持proxy/WWW验证。

标识是匹配的由上至下的与在第一个匹配的条目结束匹配的搜索。为此，如果安排*标识1*和*标识2*配置和处理匹配标识1，没有根据标识2.核对。

访问/解密/路由/出站恶意软件策略

这些策略应用不同类型的流量：

- 访问策略应用无格式HTTP或FTP连接。他们确定是否应该接受或丢弃处理。
- 解密策略确定是否应该通过解密，丢弃或者通过HTTPS处理。如果处理解密，则连续的部分它能被看到作为一个无格式HTTP请求和匹配访问策略。如果必须下降HTTPS请求，请下降它在解密策略，不在访问策略。否则，它首先浪费更多的CPU和内存将解密然后将丢弃的已丢失处理的。
- 路由策略一次确定处理的上行方向它通过WSA允许的他的。这应用，如果有上行代理或，如果WSA在*连接器*模式并且发送流量对Cloud Web安全塔。
- 出站恶意软件策略应用从最终用户的HTTP或FTP加载往Web服务器。这通常被看到是HTTP波斯特请求。

对于策略的每种类型，请记住*逻辑或*原理应用。如果安排多标识参考，则处理应该匹配配置的其中任一标识。

对于更加粒状的控制，请使用这些策略。错误配置的标识每项策略能创建问题，使用策略参考的几标识是更加有利的。切记标识不影响流量，他们识别最新匹配的流量类型在策略。

通常时期，解密策略以验证使用标识。当这不是错误的并且是有时需要的时，使用标识与解密策略参考的验证意味着匹配解密策略的所有处理解密为了验证能发生。解密操作也许通过下降或通过，但是，因为有与验证的一标识，解密发生为了最新丢弃或穿过流量。这昂贵，并且应该避免。

包含30或更多标识和30个或更多访问策略的一些配置被观察了，其中所有访问策略包括所有标识。在这种情况下，如果他们总计访问策略，匹配没有需要使用此许多标识。当这不危害设备操作时，创建与尝试的混乱排除故障并且关于性能是昂贵。

自定义URL类别

使用自定义URL类别是在通常被误会并且被误用的WSA的一个强大的工具。例如，有包含匹配的所有视频站点在标识的配置。WSA有自动地更新的一个内置的工具，当视频站点更改URL时，频繁地发生。因此，它有意义允许WSA自动地管理URL类别，并且使用自定义URL类别特殊，不分类的站点。

对常规表达非常小心。如果例如小点(。)和星号(*)使用特殊字符匹配，他们也许被证明是非常广泛的CPU和的内存。WSA展开所有常规表示它与每处理相符。例如，这是常规表示：

```
example.*
```

包含词*示例的*此表达式将匹配所有URL，不仅*example.com*域。避免使用*小点*并且*担任主角*在常规表达并且仅请使用他们作为最后一招。

这是也许创建问题常规表示的另一示例：

```
www.example.com
```

如果在常规表达使用此示例被归档，不仅将匹配*www.example.com*，而且*www.www3example2com.com*，作为这里小点含义所有*字符*。如果希望匹配仅*www.example.com*，请退出小点：

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

在这种情况下，没有理由使用常规表达功能，当您能包括此在与此格式的自定义URL类别域里面：

```
www.example.com
```

反恶意软件和名誉

如果超过一个扫描的引擎启用，请设想选项启用可适应也扫描。可适应扫描是在预扫描每请求和确定全面的引擎应该是被使用的为了扫描请求的WSA的一个强大，但是小引擎。这轻微增加在WSA的性能。