使用安全Web设备最佳实践

目录

简介

背景信息

网络环境

- ICMP
- 防火墙
- 单播反向路径转发
- 使用WCCP进行IP欺骗

SWA网络配置

- 接口
- 管理网络路由
- TALOS遥测
- DNS
- 负载平衡
- 主动身份验证
- 被动身份验证

服务配置

- Web代理
- HTTPS代理
- 第4层流量监控器(L4TM)

策略配置

- 复杂性
- 标识配置文件
- 解密策略
- 访问策略
- 自定义和外部URL类别

监控和警报

- CLI监视器
- 日志记录
- 高级网络安全报告(AWSR)
- 邮件警报
- 可用性监控
- SNMP 监控

结论

简介

本文档介绍如何配置思科安全网络设备(SWA)的最佳实践。

背景信息

本指南旨在作为最佳实践配置的参考，它涉及SWA部署的很多方面，包括支持的网络环境、策略配置、监控和故障排除。虽然此处记录的最佳实践对于所有管理员、架构师和操作员都很重要，但是它们只是指导原则，因此必须作为原则对待。每个网络都有自己特定的要求和挑战。

作为安全设备，SWA以几种独特的方式与网络进行交互。它既是网络流量的源也是目标。它可同时充当Web服务器和Web客户端。它至少采用服务器端IP地址欺骗和中间人技术来检查HTTPS事务。它还可以伪装客户端IP地址，这会增加部署的复杂性，并对支持网络配置提出额外要求。本指南解决与网络设备配置相关的最常见问题。

SWA策略配置不仅会影响安全效力和实施，还会影响设备的性能。本指南介绍配置的复杂性如何影响系统资源。它定义了这种情况的复杂性，并描述了如何在策略设计中将其降至最低。此外，还关注特定功能以及如何配置这些功能以提高安全性、可扩展性和有效性。

本文档的监控和警报部分介绍了监控设备的最有效方法；还介绍了性能和可用性监控以及系统资源使用情况。它还提供了对基本故障排除有用的信息。

网络环境

ICMP

路径MTU发现(如RFC 1191中所定义)，该机制可确定沿任意路径的数据包的最大大小。对于IPv4，设备可以通过在数据包的IP报头中设置不分段(DF)位来确定路径上任何数据包的最大传输单元(MTU)。如果在路径沿途的某个链路上，设备无法在不对数据包进行分段的情况下转发数据包，则会将Internet控制消息协议(ICMP)需要分段（类型3，代码4）消息发送回源。然后，客户端重新发送较小的数据包。这种情况一直持续到发现完整路径的MTU。IPv6不支持分段，并且使用Packet Too Big (Type 2) ICMPv6消息表示无法通过给定链路容纳数据包。

由于数据包分段过程会严重影响TCP流的性能，因此SWA使用路径MTU发现。必须在相关网络设备上启用上述ICMP消息，以允许SWA确定其在网络中路径的MTU。此行为可在SWA使用pathmtudiscovery 命令行界面(CLI)命令禁用。这样做会导致默认MTU降至576字节（根据RFC 879），严重影响性能。管理员必须采取额外步骤，通过etherconfig CLI命令在SWA中手动配置MTU。

在使用Web缓存通信协议(WCCP)的情况下，Web流量会从客户端路径到Internet的另一台网络设备重定向到SWA。在这种情况下，其他协议（例如ICMP）不会重定向到SWA。有可能SWA会触发来自网络上路由器的ICMP需要分段消息，但消息不会发送到SWA。如果网络中存在这种可能性，则必须禁用路径MTU发现。如前所述，对于此配置，需要使用etherconfig CLI命令手动设置SWA上的MTU的附加步骤。

防火墙

在默认配置中，代理连接时，SWA不会欺骗客户端IP地址。这意味着所有出站网络流量都来自SWA IP地址。必须确保网络地址转换(NAT)设备具有足够大的外部地址和端口池来满足此要求。为此提供一个专用地址是一个好主意。

有些防火墙采用拒绝服务(DoS)保护或其他安全功能，当大量并发连接来自单个客户端IP地址时触发这些功能。当客户端IP欺骗未启用时，必须将SWA IP地址排除在这些保护之外。

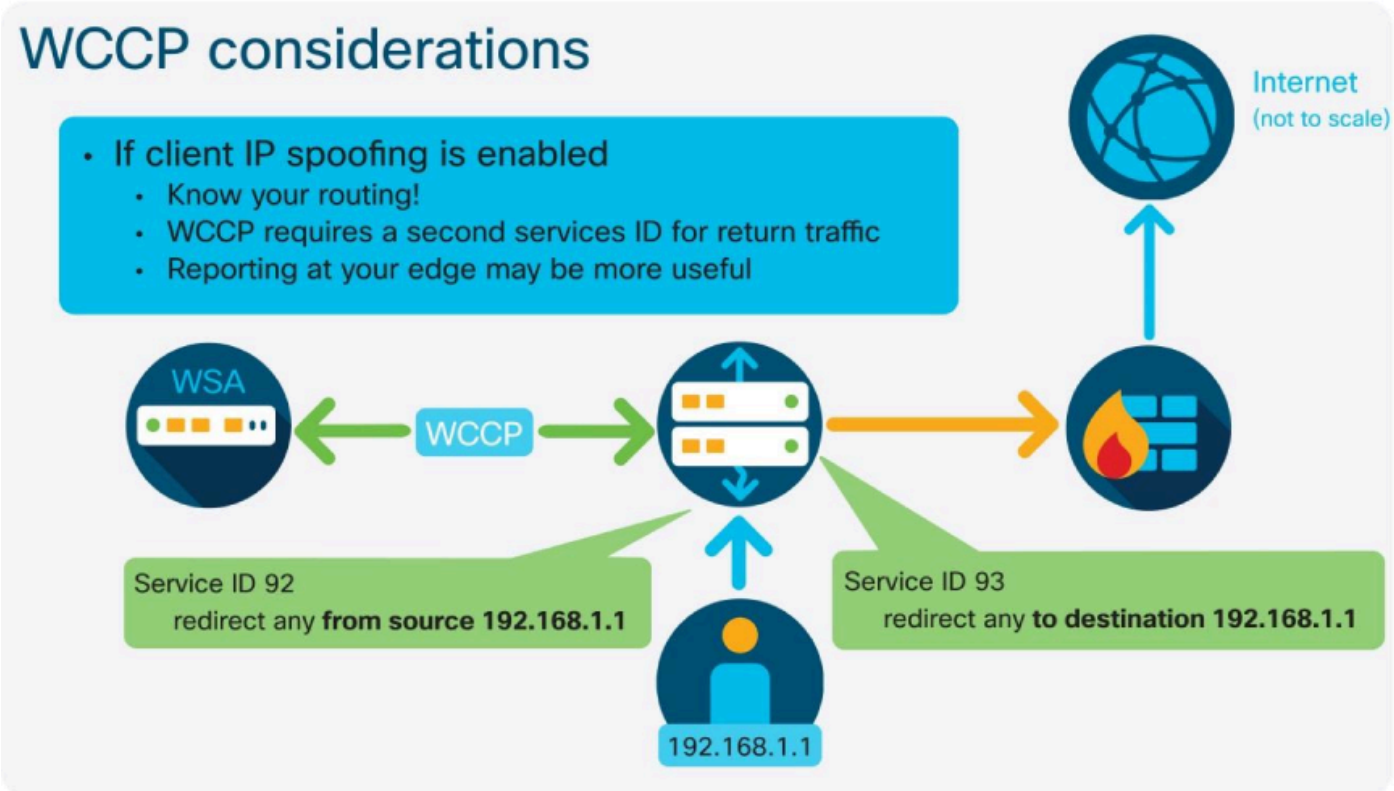
单播反向路径转发

SWA在与客户端通信时伪装服务器IP地址，或者可以配置为在与上游服务器通信时伪装客户端IP地址。可以在交换机上启用单播反向路径转发(uRPF)等保护，以确保传入的数据包与预期的入口端口匹配。这些保护会根据路由表检查数据包的源接口，以确保其到达预期端口。有必要酌情豁免全部门性做法，使其免受这些保护。

使用WCCP进行IP欺骗

在SWA中启用IP欺骗功能时，出站请求从设备使用原始客户端请求的源地址。这需要对相关网络基础设施进行额外配置，以确保返回的数据包被路由到SWA出站接口，而不是发起请求的客户端。

在网络设备（路由器、交换机或防火墙）上实施WCCP时，会定义一个根据访问控制列表(ACL)匹配流量的服务ID。然后，服务ID将应用到接口并用于匹配流量以进行重定向。如果启用了IP欺骗，则必须创建第二个服务ID，以确保返回流量也重定向到SWA。



SWA网络配置

接口

SWA有五个可用的网络接口：M1、P1、P2、T1和T2。在可能的情况下，必须针对其特定目的使用上述每个工具。出于各自的原因使用每个端口是有益的。M1接口必须连接到专用管理网络，并且必须启用分割路由以限制管理服务的泄露。P1可以限制为客户端请求流量，相反，不允许P2接受显式代理请求。这样可以减少每个接口上的流量，并在网络设计中实现更好的分段。

T1和T2端口可用于第4层流量监控(L4TM)功能。此功能监控镜像的第2层端口，并增加了根据阻止的已知恶意IP地址和域名列表阻止流量的功能。它通过查看流量的源和目标IP地址执行此操作，如果阻止列表匹配，它会发送TCP重置数据包或端口不可达消息。使用此功能可以阻止通过任何协议发送的流量。

即使L4TM功能未启用，当T1和T2端口连接到镜像端口时，也可以增强透明旁路。对于WCCP，SWA只知道传入数据包的源和目标IP地址，必须决定代理该数据包，或基于该信息绕过它。SWA每隔30分钟解析一次绕行设置列表中的任何条目，而不管记录的生存时间(TTL)。但是，如果启用L4TM功能，SWA可以使用已监听的DNS查询更频繁地更新这些记录。这降低了客户端解析了与SWA不同的地址时出现误报的风险。

管理网络路由

如果专用管理网络无法访问Internet，可以将每项服务配置为使用数据路由表。可以定制此网络以适合网络拓扑，但一般而言，建议对所有系统服务使用管理网络，对客户端流量使用数据网络。自AsyncOS版本11.0起，可以设置路由的服务包括：

- 外部URL源
- 高级恶意软件防护(AMP)文件信誉和分析
- 更新和升级
- DNS
- Active Directory

对于管理流量的其他出口过滤，可以配置静态地址用于以下服务：

- 外部URL源：
  1.自定义取决于托管位置
  2. AMP文件信誉和分析
  3. cloud-sa.amp.cisco.com （北美）
  4.cloud-sa.eu.amp.cisco.com （欧洲）
  5.cloud-sa.apjc.amp.cisco.com（亚太地区）

- 更新和升级：
  1. downloads-static.ironport.com
  2. updates-static.ironport.com

TALOS遥测

Cisco Talos团队以识别新威胁和新兴威胁著称。发送到Talos的所有数据均进行匿名处理，并存储在美国数据中心。参与SensorBase可增强对Web威胁的分类和识别，从而更好地保护SWA和其他思科安全解决方案。

DNS

域名服务器(DNS)安全最佳实践表明，每个网络必须托管两个DNS解析器：一个用于本地域内的权威记录，另一个用于递归解析Internet域。为了满足这一要求，SWA允许为特定域配置DNS服务器。如果只有一个DNS服务器可用于本地查询和递归查询，请考虑它用于所有SWA查询时增加的额外负载。更好的选择是使用本地域的内部解析器和外部域的根互联网解析器。这取决于管理员风险状况和容差能力。

默认情况下，无论记录的TTL如何，SWA都会缓存DNS记录至少30分钟。大量使用内容交付网络(CDN)的现代网站的TTL记录较低，因为其IP地址经常变化。这可能会导致客户端缓存给定服务器的IP地址，并且SWA缓存同一服务器的不同地址。为此，可以使用以下CLI命令将SWA默认TTL降低到五分钟：

```
SWA_CLI> dnsconfig
...
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.
[]> SETUP
...
Enter the minimum TTL in seconds for DNS cache.
...
```

必须配置辅助DNS服务器，以防主要服务器不可用。如果所有服务器都配置了相同的优先级，则会随机选择服务器IP。根据配置的服务器数量，给定服务器的超时时间可能会有所不同。此表表示最多六台DNS服务器的查询超时：

DNS服务器数量	查询超时（按顺序）
1	60
2	5 、45
3	5、10、45
4	1、3、11、45
5	1、3、11、45、1
6	1、3、11、45、1、1

还有仅通过CLI提供的高级DNS选项。这些选项在CLI中使用advancedproxyconfig > DNS 命令可用。

Select one of these options:

- 0 -始终按顺序使用DNS应答
- 1 -使用客户端提供的地址，然后使用DNS
- 2 -有限的DNS使用
- 3 - DNS使用非常有限

对于选项1和2，如果启用Web信誉，则使用DNS。

对于选项2和3，如果没有上游代理，或在配置的上游代理发生故障的情况下，DNS用于显式代理请求。

对于所有选项，在策略成员身份中使用目标IP地址时使用DNS。

这些选项控制SWA在评估客户端请求时如何决定要连接的IP地址。收到请求后，SWA会看到目标IP地址和主机名。SWA必须决定是信任用于TCP连接的原始目标IP地址，还是执行自己的DNS解析并使用解析的地址。默认值为“0 =始终按顺序使用DNS答案”，这意味着SWA不信任客户端提供IP地址。

- 选项1 - SWA尝试客户端提供的连接IP地址，但如果失败，则回退到解析地址。解析的地址用于策略评估(Web类别、Web信誉等)。
- 选项2 - SWA仅使用客户端提供的地址进行连接，不会回退。解析的地址用于策略评估（Web类别、Web信誉等）。
- 选项3 - SWA仅使用客户端提供的地址进行连接，不会回退。客户端提供的IP地址用于策略评估（Web类别、Web信誉等）。

所选的选项取决于管理员在确定给定主机名的解析地址时，在客户端中必须有多少信任。如果客户端是下游代理，请选择选项3以避免不必要的DNS查找增加延迟。

负载平衡

WCCP允许在最多使用八台设备时实现透明流量负载均衡。它允许根据散列或掩码平衡流量，如果网络中混合了设备型号，可以对其进行加权，并且可以在不停机的情况下在服务池中添加和删除设备。一旦需求超过可以使用八个SWA处理的范围，建议使用专用负载均衡器。

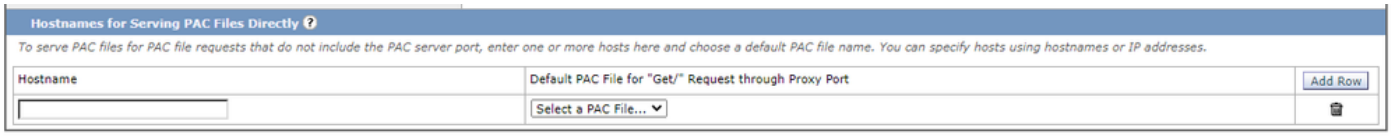
WCCP配置的具体最佳实践因使用的平台而异。对于Cisco Catalyst®交换机，最佳实践记录在Cisco Catalyst即时接入解决方案白皮书中。

WCCP与思科自适应安全设备(ASA)配合使用时存在局限性。即不支持客户端IP欺骗。此外，客户端和SWA必须位于同一接口之后。因此，使用第4层交换机或路由器来重定向流量更为灵活。有关ASA平台上的WCCP配置，请参阅ASA上的WCCP：概念、限制和配置。

对于显式部署，代理自动配置(PAC)文件是部署最广泛的方法，但它有许多缺点和安全影响不在本

文档的讨论范围之内。如果部署了PAC文件，建议使用组策略对象(GPO)配置位置，而不是依赖Web代理自动发现协议(WPAD)，WPAD是攻击者的常见目标，如果配置错误，很容易被利用。SWA可以托管多个PAC文件，并在浏览器缓存中控制其过期。

可以通过可配置的TCP端口号（默认情况下为9001）直接从SWA请求PAC文件。如果未指定端口，请求可以发送到代理进程本身，就像它是出站Web请求一样。在这种情况下，可以根据请求中的HTTP主机报头为特定PAC文件提供服务。



在高可用性环境中使用时，Kerberos的配置必须不同。SWA提供对keytab文件的支持，从而允许多个主机名与服务主体名称(SPN)关联。有关详细信息，请参阅在Windows Active Directory中创建服务帐户，以便在高可用性部署中进行Kerberos身份验证。

主动身份验证

Kerberos比NT LAN Manager安全支持提供程序(NTLMSSP)更安全、更广受支持的身份验证协议。Apple OS X操作系统不支持NTLMSSP，但如果域已加入，则可以使用Kerberos进行身份验证。不能使用基本身份验证，因为它在HTTP报头中发送未加密的凭证，并且很容易被网络上的攻击者嗅探。如果必须使用基本身份验证，则必须启用凭证加密，以确保通过加密隧道发送凭证。

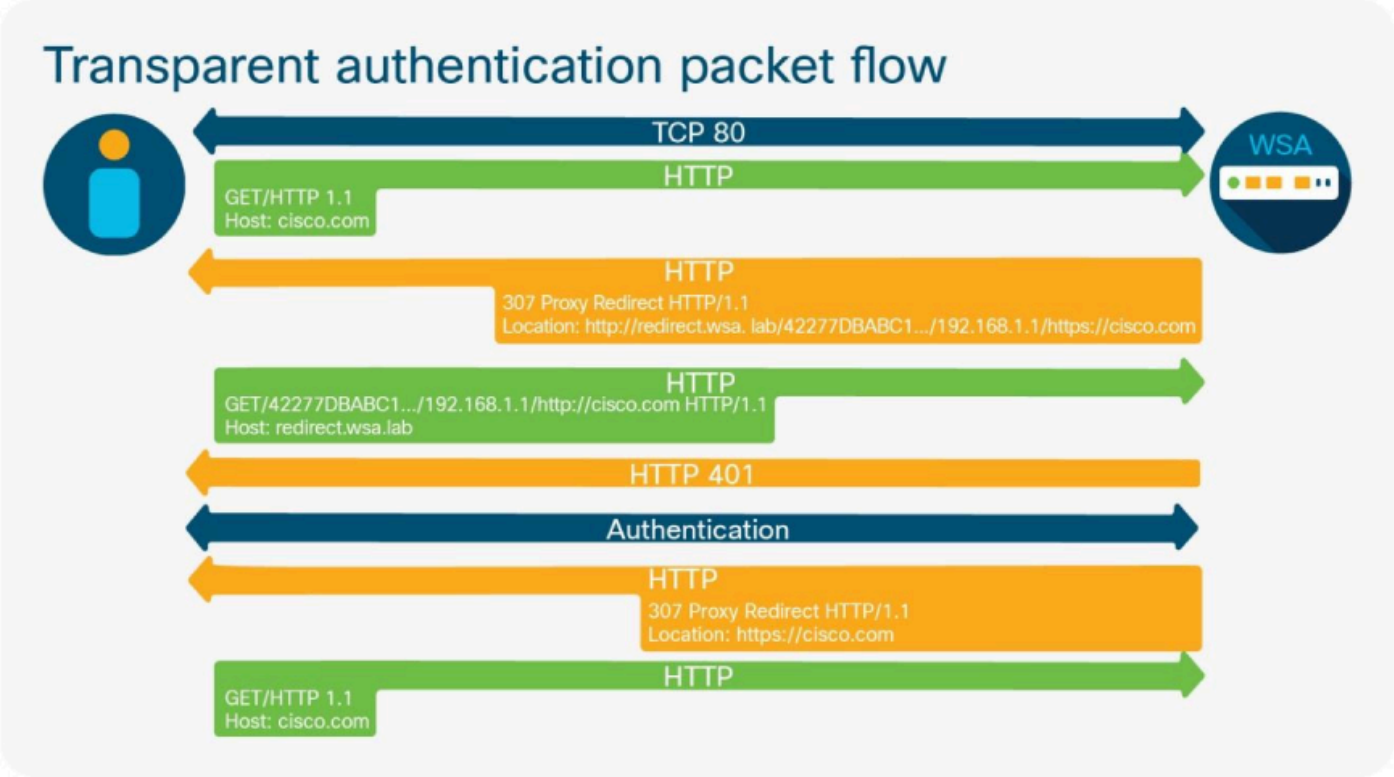
必须将多个域控制器添加到配置以确保可用性，但是此流量没有固有的负载平衡。SWA向所有已配置的域控制器发送TCP SYN数据包，第一个响应数据包用于身份验证。

在身份验证设置(authentication settings)页面中配置的重定向主机名确定透明客户端在何处发送以完成身份验证。要使Windows客户端完成集成身份验证并实现单点登录(SSO)，重定向主机名必须位于“Internet选项”控制面板的“受信任的站点”区域中。Kerberos协议要求使用完全限定域名(FQDN)指定资源，这意味着，如果Kerberos是预期的身份验证机制，则不能使用“短名称”（或“NETBIOS”名称）。需要将FQDN手动添加到受信任的站点（例如，通过组策略）。此外，必须在Internet选项控制面板中设置“使用用户名和口令自动登录”。

Firefox中还需要其他设置，浏览器才能完成使用网络代理的身份验证。这些设置可在about：config页中进行配置。要成功完成Kerberos，必须将重定向主机名添加到network.negotiate-auth.trusted-uris选项。对于NTLMSSP，必须将其添加到network.automatic-ntlm-auth.trusted-uris选项。

身份验证代理用于在完成身份验证后的一段时间内记住经过身份验证的用户。必须尽可能使用IP代理来限制发生的主动身份验证事件的数量。主动对客户端进行身份验证是一项资源密集型任务，在使用Kerberos时尤其如此。替代超时默认为3600秒（1小时），可以降低，但建议的最低值为900秒（15分钟）。

下图显示如何使用“redirect.WSA.lab”作为重定向主机名：



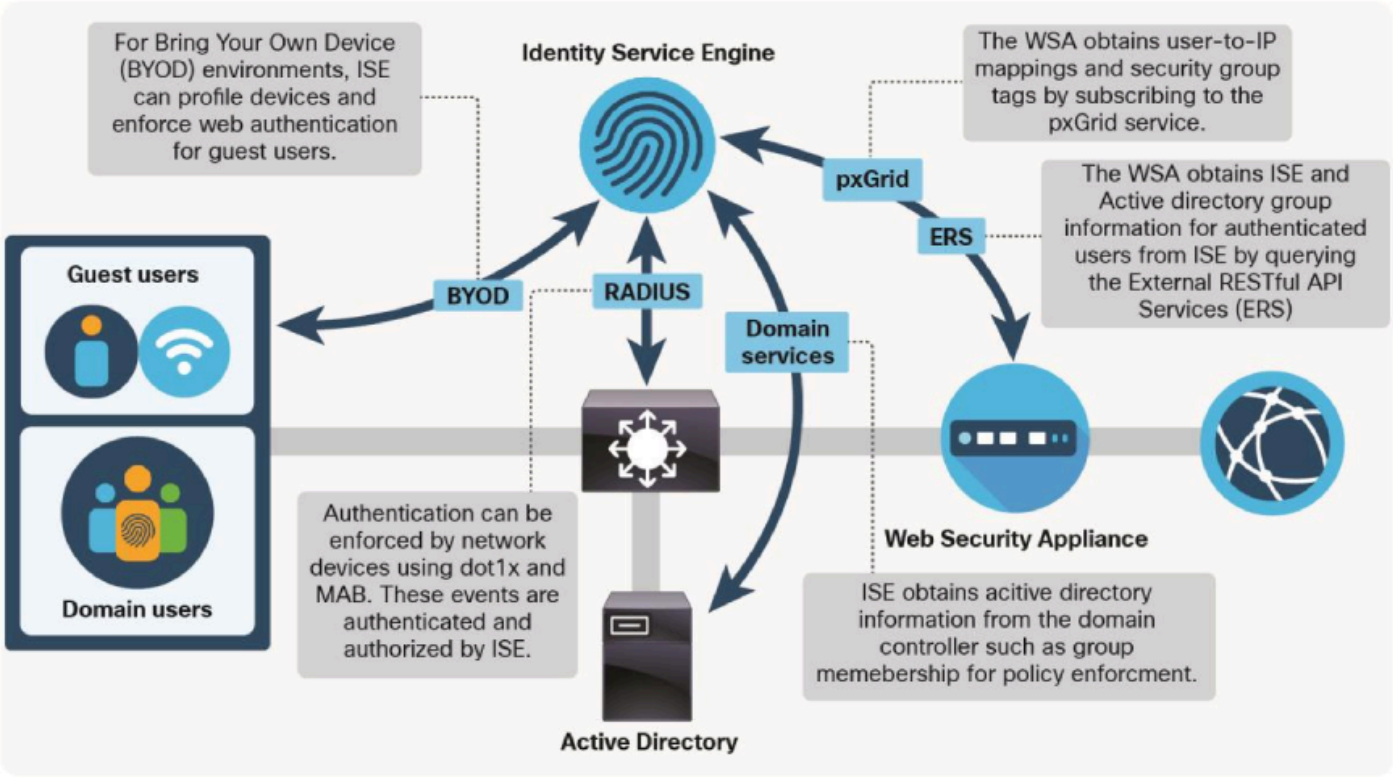
被动身份验证

SWA可以利用其他思科安全平台被动识别代理用户。被动用户识别无需直接身份验证质询和来自SWA的任何Active Directory通信，这反过来会降低设备上的延迟和资源利用率。当前可用的被动身份验证机制是通过情景目录代理(CDA)、身份服务引擎(ISE)和身份服务连接器被动身份连接器(ISE-PIC)。

ISE是一种功能丰富的产品，可帮助管理员集中其身份验证服务并利用广泛的网络访问控制。当ISE了解用户身份验证事件（通过Dot1x身份验证或Web身份验证重定向）时，它会填充包含身份验证中涉及的用户和设备信息的会话数据库。SWA通过平台交换网格(pxGrid)连接到ISE，并获取与代理连接关联的用户名、IP地址和安全组标记(SGT)。从AsyncOS版本11.7开始，SWA还可以查询ISE上的外部Restful服务(ERS)以获取组信息。

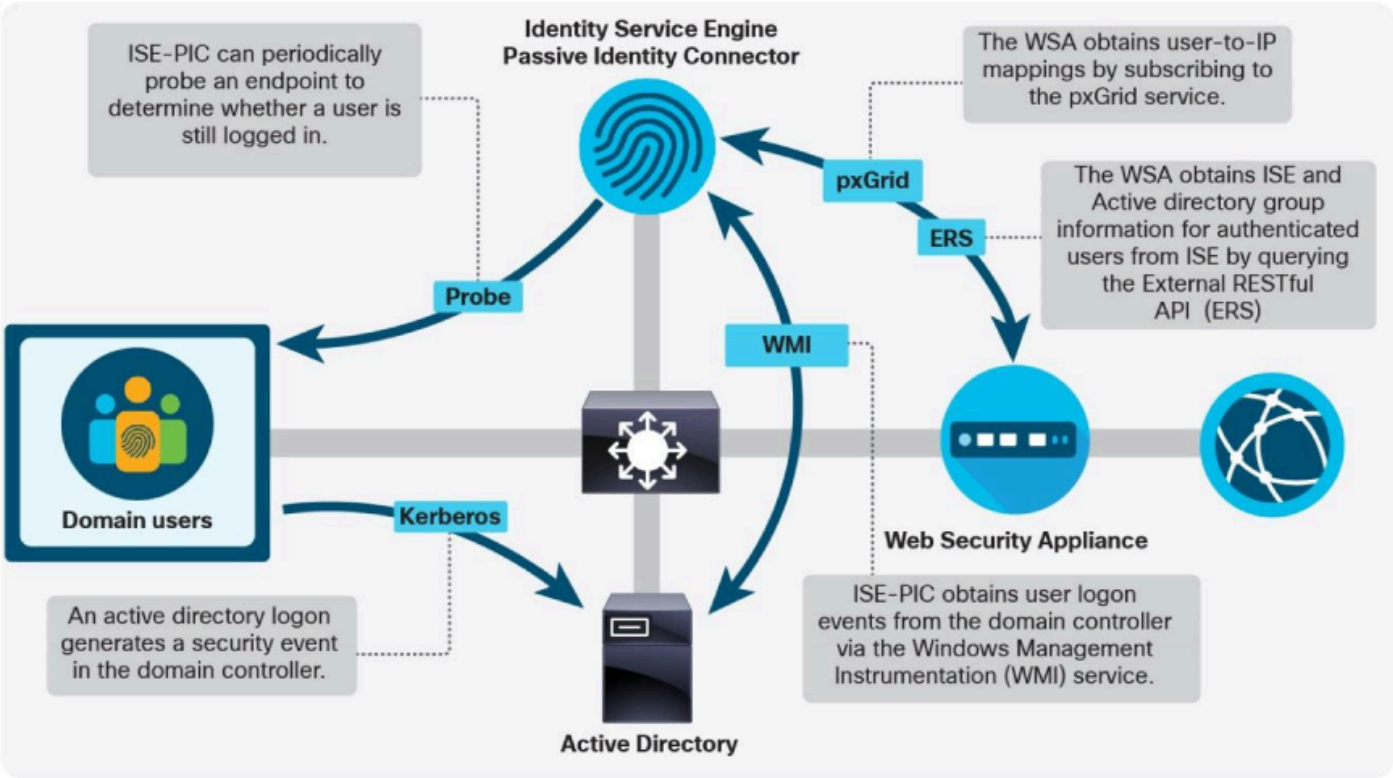
建议版本为ISE 3.1和SWA 14.0.2-X及更高版本。有关SWA的ISE兼容性矩阵的详细信息，请参阅安全Web设备的ISE兼容性矩阵。

有关完全集成步骤的详细信息，请参阅网络安全设备最终用户指南。



思科宣布Cisco Context Directory Agent (CDA)软件的生命周期结束，请参阅[Cisco Context Directory Agent (CDA)]。

自CDA补丁6起，与Microsoft Server 2016兼容。但是，我们积极鼓励管理员将其CDA部署迁移到ISE-PIC。两种解决方案都使用WMI订阅Windows安全事件日志以生成用户到IP的映射（称为“会话”）。对于CDA，SWA使用RADIUS查询这些映射。对于ISE-PIC，使用与完整ISE部署相同的pxGrid和ERS连接。ISE-PIC功能在完整ISE安装中以及在独立虚拟设备中可用。

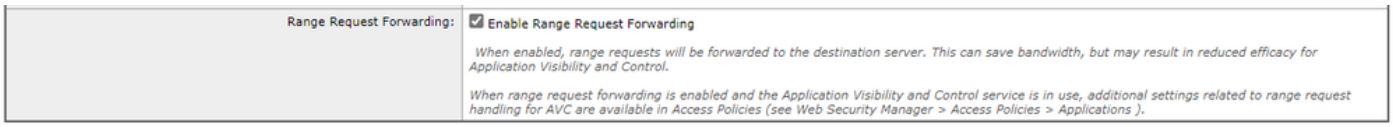


服务配置

Web代理

必须在Web代理配置中启用缓存，以节省带宽并提高性能。随着HTTPS流量的百分比增加，这一点变得不那么重要，因为SWA不会默认缓存HTTPS事务。如果将代理部署为仅为显式客户端提供服务，则必须指定转发模式以拒绝并非专门流向代理服务的所有流量。通过这种方式，设备攻击面得以减少，并实施了良好的安全原则：如果不需要则将其关闭。

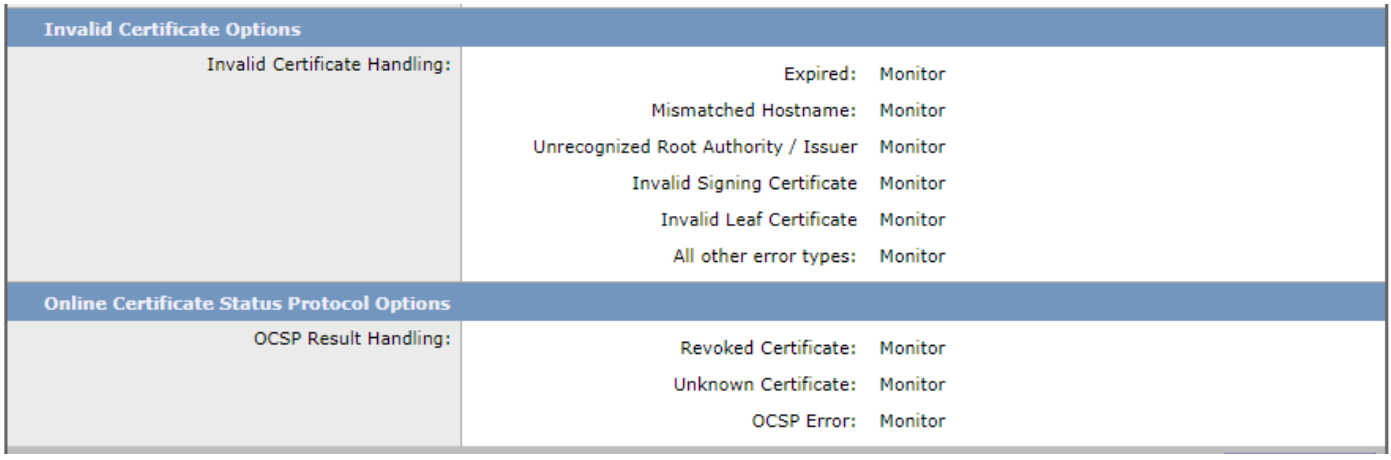
HTTP请求中使用范围请求报头来指定要下载的文件的字节范围。它通常由操作系统和应用程序更新守护程序使用，以便一次传输文件的小部分。默认情况下，SWA会删除这些报头，以便获取整个文件，用于防病毒(AV)扫描、文件信誉和分析以及应用可视性控制(AVC)。通过在代理设置中全局启用范围请求报头的转发，管理员可以创建转发或删除这些报头的单独访问策略。有关此配置的详细信息，请参阅访问策略部分。



HTTPS代理

安全最佳实践建议，私钥必须在使用它们的设备上生成，并且决不能传输到其他位置。HTTPS代理向导允许创建用于解密传输层安全(TLS)连接的密钥对和证书。然后，可以下载证书签名请求(CSR)并由内部证书颁发机构(CA)签署。在Active Directory (AD)环境中，这是最佳方法，因为AD集成的CA自动受域所有成员的信任，并且不需要其他步骤来部署证书。

HTTPS代理的一个安全功能是验证服务器证书。最佳实践建议无效证书要求断开连接。启用Decrypt for EUN允许SWA显示块页面，解释块的原因。如果未启用此功能，则任何被阻止的HTTPS站点都会导致浏览器错误。这会导致帮助台通知单增加，并且用户认为发生了故障，而不是SWA阻止了连接。所有无效的证书选项必须设置为至少Decrypt。如果证书问题阻止加载站点，将其中任何选项保留为监控无法记录有用的错误消息。



同样，必须保持启用在线证书服务协议(OCSP)检查，并且不得将监控器用于任何选项。必须丢弃吊销的证书，所有其他证书必须至少设置为“解密”，以允许记录相关错误消息。授权信息访问跟踪

（AIA跟踪）是客户端收集证书签名者和URL的方法，从中可以获取其他证书。例如，如果从服务器接收的证书链不完整（它缺少中间或根证书），则SWA可以检查AIA字段并使用该字段获取缺失的证书和验证真实性。此设置仅在CLI中从以下命令可用：

```
SWA_CLI> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters
[]> HTTPS
...
Do you want to enable automatic discovery and download of missing Intermediate Certificates?
[Y]>
...
```

注意：由于许多现代服务器依靠此机制为客户端提供完全信任链，因此默认情况下启用此设置，且不得禁用此设置。

第4层流量监控器(L4TM)

L4TM是将SWA的覆盖范围扩展到包括不通过代理的恶意流量以及所有TCP和UDP端口上的流量的一种高效方式。T1和T2端口用于连接到网络分路器或交换机监控会话。这允许SWA被动监控来自客户端的所有流量。如果发现流向恶意IP地址的流量，则SWA可以通过在欺骗服务器IP地址的同时发送RST来终止TCP会话。对于UDP流量，它可以发送Port Unreachable消息。配置监控会话时，最好排除任何指向SWA管理接口的流量，以防止该功能潜在地干扰对设备的访问。

除了监控恶意流量外，L4TM还监听DNS查询以更新绕行设置列表。此列表在WCCP部署中使用，用于将某些请求返回到WCCP路由器，以直接路由到Web服务器。与绕行设置列表匹配的数据包不由代理处理。列表可以包含IP地址或服务器名称。SWA每隔30分钟解析一次旁路设置列表中的任何条目，而不考虑记录的TTL。但是，如果启用L4TM功能，SWA可以使用已监听的DNS查询更频繁地更新这些记录。这降低了客户端解析了与SWA不同的地址时出现误报的风险。

策略配置

正确的策略配置对SWA的性能和可扩展性至关重要。这不仅是因为策略本身在保护客户端和执行公

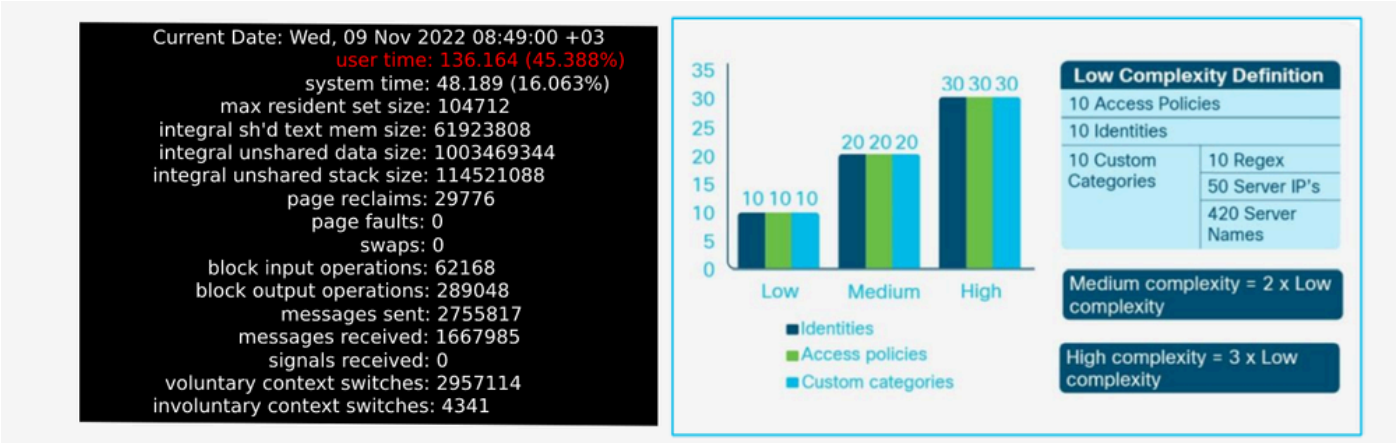
司要求方面的有效性，还因为配置的策略对资源使用以及SWA的整体运行状况和性能有直接影响。一套过于复杂或设计欠佳的策略可能会导致设备不稳定，并减缓响应速度。

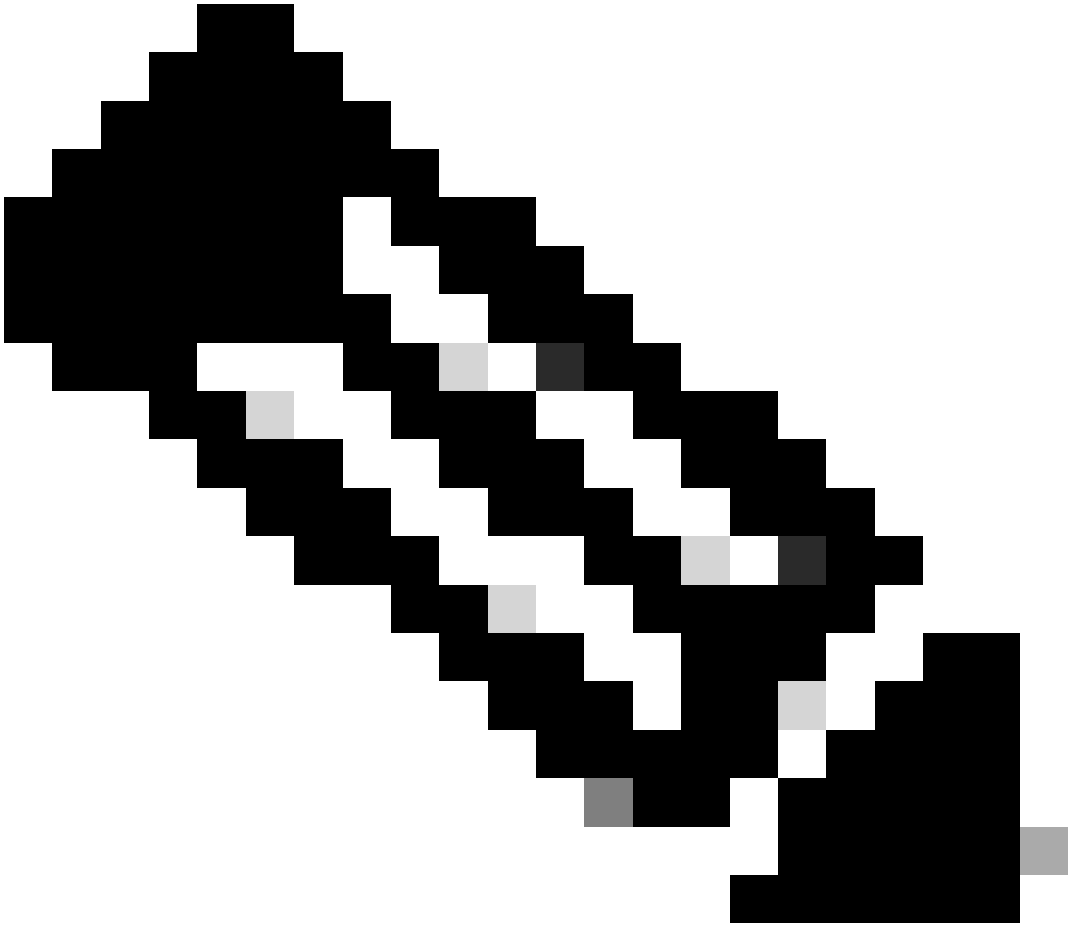
复杂性

SWA策略的构建使用了各种策略要素。从配置生成的XML文件用于创建大量后端配置文件和访问规则。配置越复杂，代理进程需要花费更多时间来评估每个事务的各种规则集。在SWA基准和规模确定过程中，会创建一组基本策略元素，这些元素代表三个级别的配置复杂性。十个身份配置文件、解密策略和访问策略，以及十个包含10个正则表达式条目、50个服务器IP地址和420个服务器主机名的自定义类别，被视为低复杂性配置。将其中每个数字分别乘以2和3可得到中等复杂性和高复杂性配置。

当配置变得过于复杂时，首先出现的症状通常包括Web界面和CLI响应缓慢。最初不会对用户产生重大影响。但是，配置越复杂，代理进程在用户模式下必须花费的时间就越多。因此，检查在此模式下所花费时间的百分比是一种将过于复杂的配置诊断为SWA缓慢原因的有效方法。

每五分钟在track_stats日志中记录一次CPU时间（以秒为单位）。这意味着用户时间百分比可以计算为（用户时间+系统时间）/300。当用户时间接近270时，该进程在用户模式中花费过多的CPU周期，这几乎总是因为配置太复杂，无法有效地进行分析。





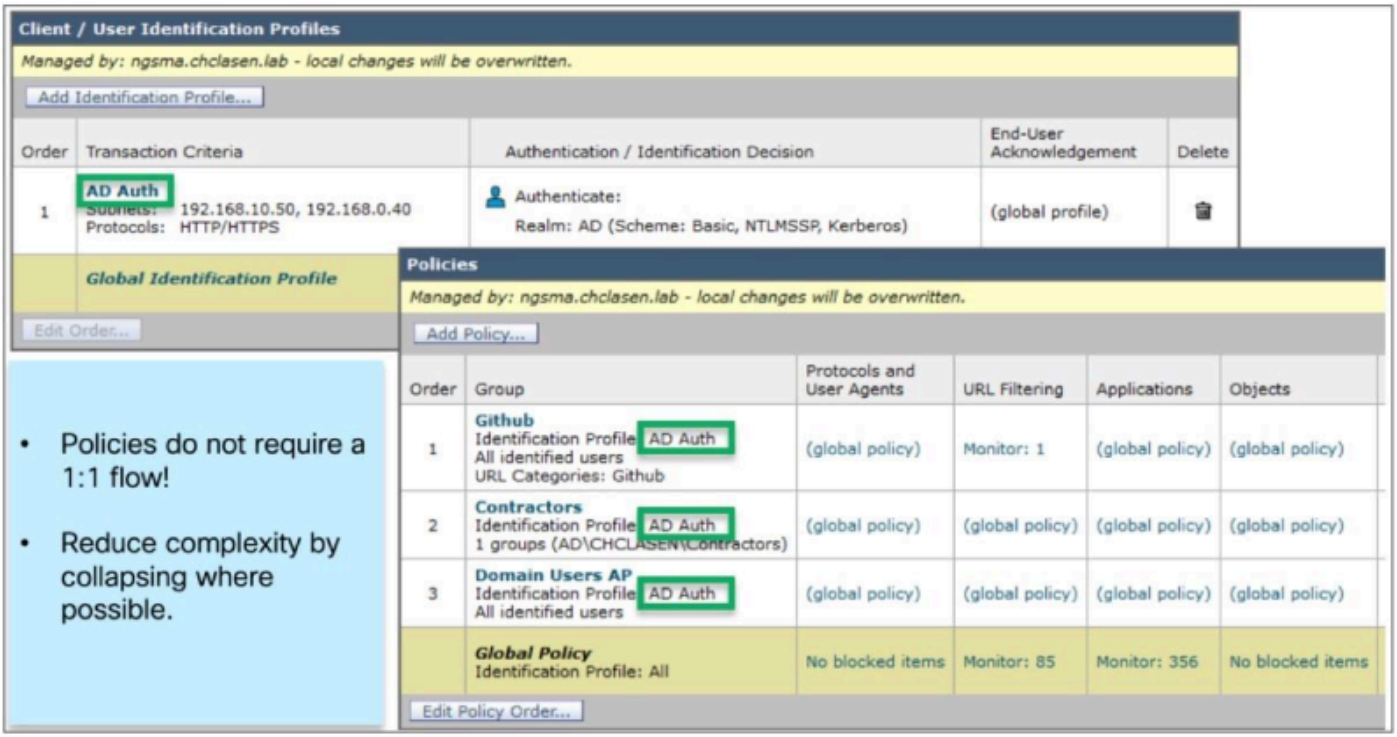
注意：到目前为止，SWA的最大限制是60,000个并发客户端连接和60,000个并发服务器连接。

标识配置文件

标识(ID)配置文件是在收到新请求时评估的第一个策略元素。ID配置文件第一部分配置的所有信息都使用逻辑AND进行评估。这意味着所有条件必须匹配，请求才能与配置文件匹配。创建策略时，策略必须严格到绝对必要的程度。包含单个主机地址的配置文件几乎从不需要使用，而且可能会导致配置无序扩展。使用HTTP报头、自定义类别列表或子网中的用户代理字符串通常是限制配置文件范围的更好策略。

一般来说，需要身份验证的策略配置在底部，例外项则添加到顶部。在对不需要身份验证的策略进行排序时，最常用的策略必须尽可能最接近顶部。不要依赖失败的身份验证来限制访问。如果已知网络上的客户端无法向代理进行身份验证，则必须在访问策略中免除身份验证并阻止该客户端。无法进行身份验证的客户端重复将未经身份验证的请求发送到SWA，SWA使用资源并可能导致CPU和内存利用率过高。

对管理员来说，一个常见的误解是必须有一个唯一的ID配置文件以及相应的解密策略和访问策略。对于策略配置来说，这种策略效率很低。如有可能，策略必须“折叠”，以便单个ID配置文件可与多个解密和访问策略相关联。这是可能的，因为给定策略中的所有条件必须匹配，流量才能与策略匹配。在身份验证策略中更一般化，在生成的策略中更具体，这样可以整体减少策略数量。



解密策略

与ID配置文件一样，解密策略中设置的条件也会评估为逻辑AND，但使用ISE中的信息时有一个重要例外。策略匹配的工作方式如下，具体取决于配置的元素（AD组、用户或SGT）：

- AD组和用户-不改变以前的行为；如果用户是组的成员，或者已在策略中指定用户，则匹配策略。
- SGT和AD组及用户-如果用户与SGT相关联且是AD组的成员，或者已在策略中指定用户，则匹配策略。
- SGT和用户-如果用户与SGT关联或在策略中指定用户，则匹配策略。

在SWA执行的所有服务中，从性能角度来看，对HTTPS流量的评估最为重要。已解密流量的百分比对设备的大小有直接影响。管理员可以依靠至少75%的网络流量进行HTTPS。

初始安装后，必须确定解密流量的百分比，以确保准确设定对未来增长的预期。部署后，必须每季度检查一次此编号。使用access_logs副本可以轻松查找SWA解密的HTTPS流量的百分比，即使没有其他日志管理软件也是如此。可以使用简单的Bash或PowerShell命令来获取此数字。下面是为每个环境描述的步骤：

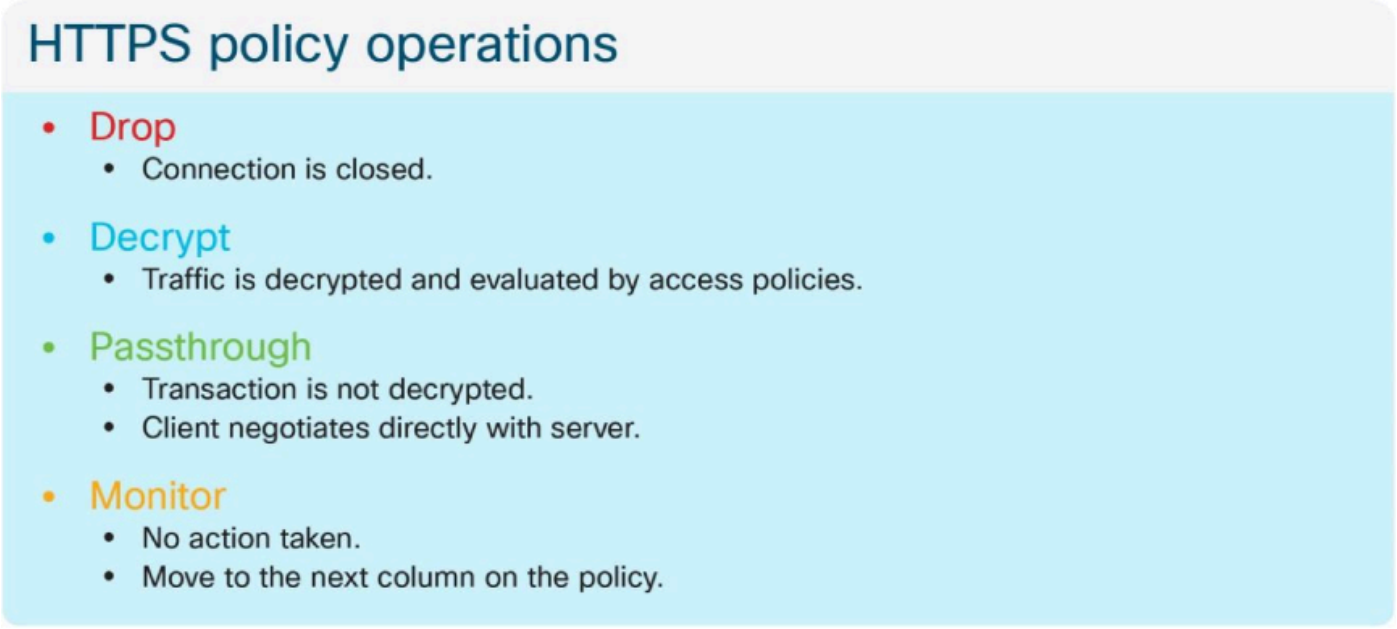
1. Linux命令：

```
cat aclog.current | grep -Ev "\/407|\/401" | awk 'BEGIN { total=0; decrypt=0; ssl=0;} {total++; if($0 ~
```

2. Powershell命令：

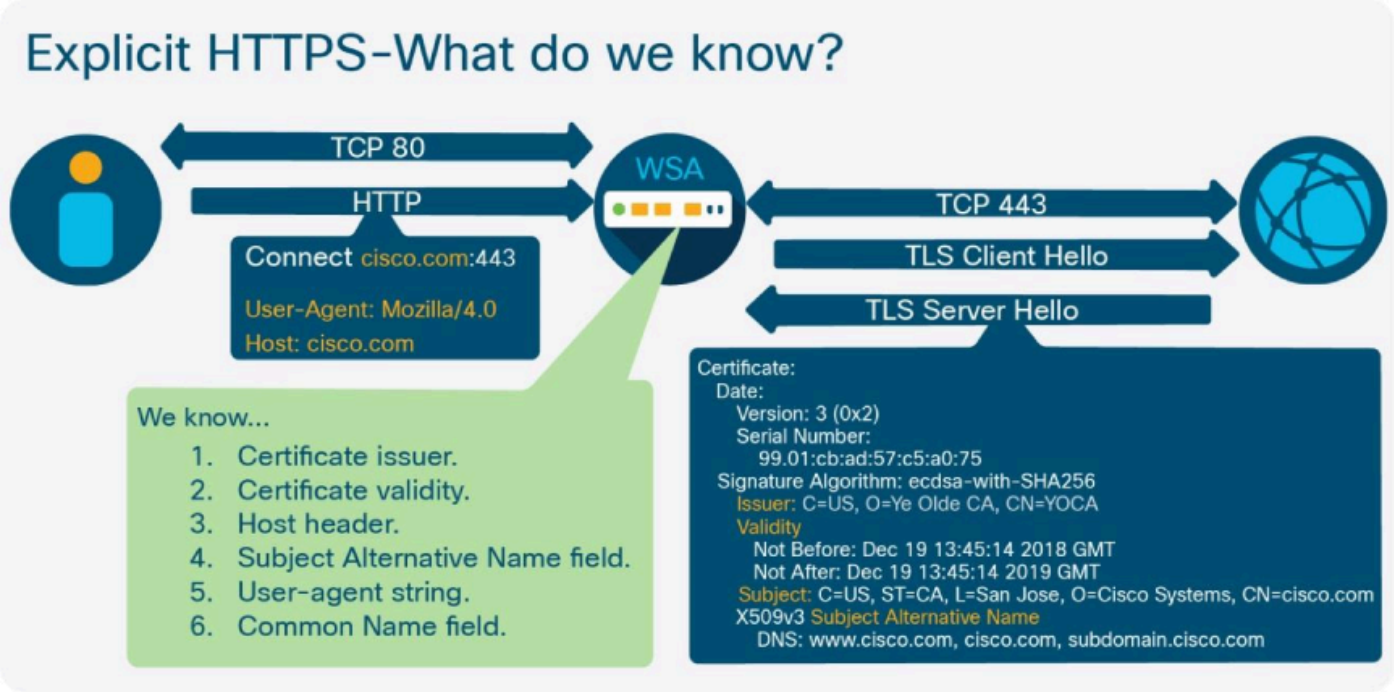
```
$lines = Get-Content -Path "aclog.current" | Where-Object { $_ -notmatch "/407|/401" }; $total = 0; $de
```

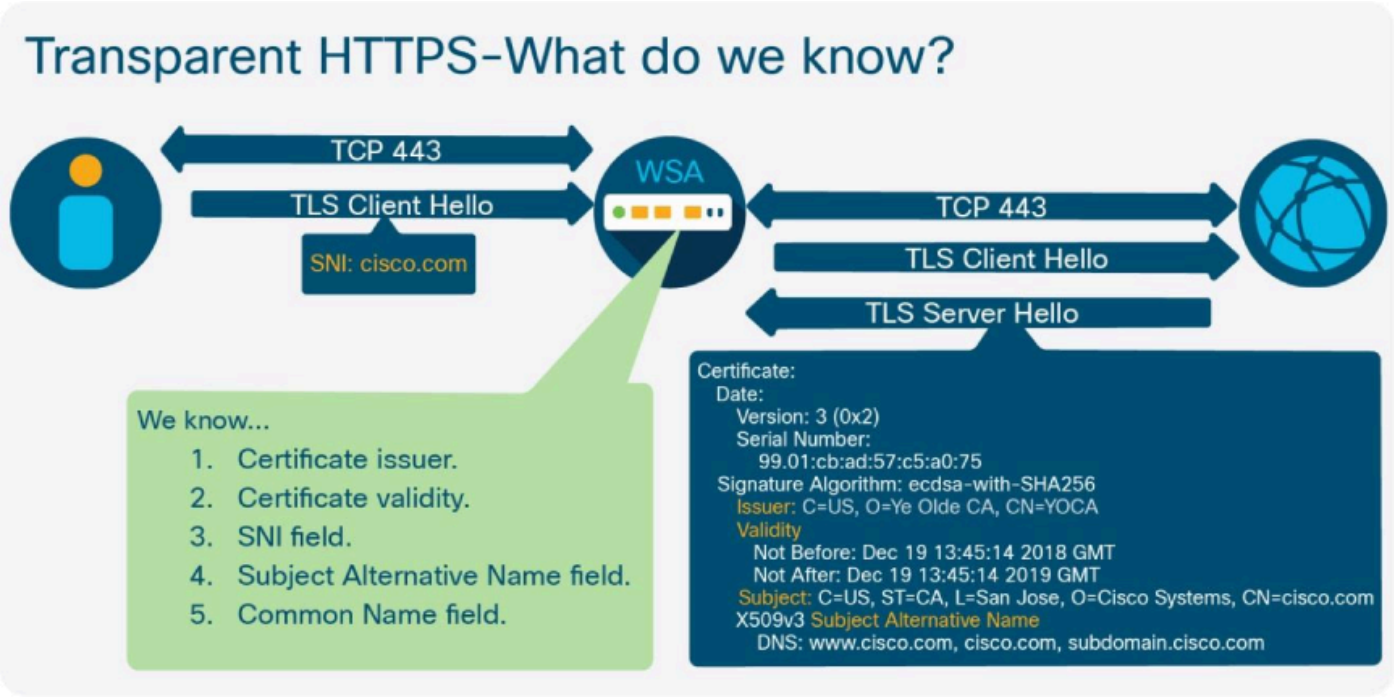
在设计解密策略时，必须了解策略中列出的各种操作如何导致设备评估HTTPS连接。当必须允许客户端和服务器终止其TLS会话的每一端，而无需SWA解密每个数据包时，将使用直通操作。即使站点设置为直通，仍必须要求SWA与服务器完成一次TLS握手。这是因为SWA必须选择根据证书有效性阻止连接，并且必须启动与服务器的TLS连接以获取证书。如果证书有效，SWA将关闭连接，并允许客户端继续直接与服务器建立会话。



SWA不执行任何TLS握手的唯一情况是，服务器名称或IP地址存在于自定义类别中（设置为passthrough），并且服务器名称在HTTP CONNECT或TLS客户端Hello中可用。在显式方案中，客户端在TLS会话启动之前（在主机报头中）向代理提供服务器的主机名，因此会根据自定义类别检查此字段。在透明部署中，SWA检查TLS客户端Hello消息中的服务器名称指示(SNI)字段并根据自定义类别进行评估。如果主机报头或SNI不存在，SWA必须继续与服务器握手，以按此顺序检查证书上的主题备用名称(SAN)和公用名称(CN)字段。

此行为对于策略设计意味着可以通过确定已知和内部信任的服务器并将其设置为从自定义类别列表传递，而不是依赖网络类别和信誉得分（仍需要SWA完成与服务器的TLS握手）来减少TLS握手的数量。但是，请注意，这也会阻止证书有效性检查。





鉴于新网站在网上出现的速度，可能会发现一些网站未按SWA使用的Web信誉和分类数据库进行分类。这并不意味着该站点更可能是恶意站点，此外，所有这些站点仍会受到AV扫描、AMP文件信誉和分析，以及配置的任何对象阻止或扫描。出于这些原因，建议不要在多数情况下丢弃未分类站点。最好将其设置为由AV引擎解密和扫描，并由AVC、AMP、访问策略等进行评估。在访问策略部分中有有关未分类站点的详细信息。

访问策略

与ID配置文件一样，解密策略中设置的条件也会评估为逻辑AND，但使用ISE中的信息时有一个重要例外。接下来根据配置的元素（AD组、用户或SGT）解释策略匹配行为：

- AD组和用户-不改变以前的行为；如果用户是组的成员，或者已在策略中指定用户，则匹配策

略。
- SGT和AD组及用户-如果用户与SGT相关联且是AD组的成员，或者已在策略中指定用户，则匹配策略。
- SGT和用户-如果用户与SGT关联或在策略中指定用户，则匹配策略。

HTTP流量在经过身份验证后立即根据访问策略进行评估。HTTPS流量在经过身份验证后进行评估，并且如果按照匹配的解密策略应用了解密操作。对于已解密的请求，有两个access_log条目。第一个日志条目显示应用于初始TLS连接（解密）的操作，第二个日志条目显示访问策略应用于已解密HTTP请求的操作。

如Web代理部分所说明的，范围请求报头用于请求文件的特定字节范围，通常供操作系统和应用程序更新服务使用。默认情况下，SWA会从出站请求中删除这些报头，因为如果没有整个文件，将无法执行恶意软件扫描或使用AVC功能。如果网络中的许多主机经常请求小字节范围来检索更新，则可能会触发SWA同时下载整个文件几次。这会快速耗尽可用互联网带宽并导致服务中断。此故障场景的最常见原因是Microsoft Windows更新和Adobe软件更新守护程序。

要缓解此问题，最佳解决方案是将此流量完全转向SWA周围。这对于透明部署的环境并非总是可行，在这些情况下，下一个最佳选项是为流量创建专用访问策略，并在这些策略上启用范围请求报头转发。必须考虑这些请求无法进行AV扫描和AVC，因此必须仔细设计策略以仅针对预期流量。通常，完成此操作的最佳方式是匹配请求报头中的用户代理字符串。常见更新守护程序的用户-代理字符串可以在线找到，或者可以由管理员捕获并检查请求。大多数更新服务（包括Microsoft Windows和Adobe软件更新）不使用HTTPS。

如解密策略部分中所述，不建议删除解密策略中的未分类站点。出于同样的原因，建议不要在访问策略中阻止它们。动态内容分析(DCA)引擎可以使用给定站点的内容以及其他启发式数据来分类站点，否则，这些站点将被URL数据库查找标记为未分类。启用此功能可减少SWA中未分类裁决的数量。

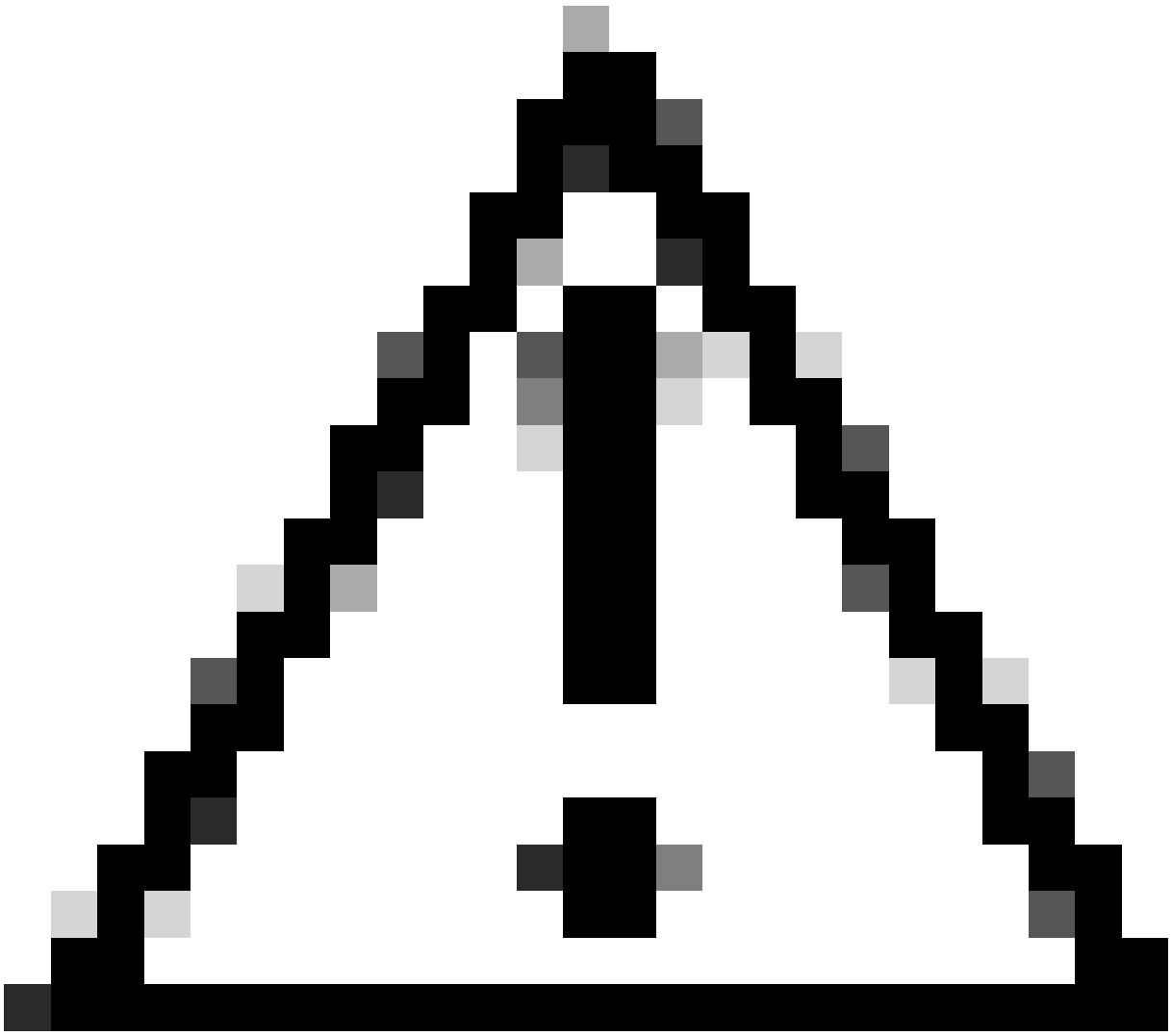
通过访问策略的“对象扫描”(Object Scanning)设置，可以检查多种类型的存档文件。如果网络在应用程序更新过程中定期下载存档文件，则启用存档文件检查会显著增加CPU使用率。如果要检查所有存档文件，必须提前识别并免除此流量。首先调查识别此流量的可能方法的是用户代理字符串，因为这样有助于避免可能变得难以维护的IP允许列表。

自定义和外部URL类别

自定义类别列表用于按IP地址或主机名标识服务器。可以使用正则表达式(regex)指定服务器名称匹配的模式。与使用子字符串匹配相比，使用regex模式匹配服务器名称会耗费更多的资源，因此只有在绝对必要时才必须使用这些模式。可以在域名的开头添加“。”以匹配子域，无需正则表达式。例如，“.cisco.com”也与“www.cisco.com”匹配。
如复杂性部分所说明的，低复杂性定义为10个自定义类别列表，中等复杂性定义为20个，高复杂性定义为30个。建议将此数字保持在20以下，尤其是当列表使用regex模式或包含大量条目时。有关每种类型的条目数的详细信息，请参阅访问策略部分。

外部URL源比静态自定义类别列表灵活得多，利用这些源可直接影响安全性，因为它们不再需要管理员手动维护它们。由于此功能可用于检索不由SWA管理员维护或控制的列表，因此在AsyncOS版本11.8中增加了向下载的地址添加单个例外的功能。

Office365 API对于针对此常见部署的服务制定策略决策特别有用，并且可用于各个应用（PowerPoint、Skype、Word等）。Microsoft建议绕过所有Office365流量的代理以优化性能。Microsoft文档说明：



警告：“虽然SSL中断和检查导致最大延迟，但代理身份验证和信誉查找等其他服务可能导致性能下降和用户体验不佳。此外，这些外围网络设备需要足够的容量来处理所有网络连接请求。我们建议绕过您的代理或检查设备来获得直接Office 365网络请求。”- https://learn.microsoft.com/en-us/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide

---

在透明代理环境中使用此指南可能会很困难。从AsyncOS版本11.8开始，可以使用从Office365 API检索的动态类别列表填充绕行设置列表。此列表用于将透明重定向的流量发送回WCCP设备进

行直接路由。

绕过所有Office365流量会为需要一些基本安全控制和此流量报告的管理员创建盲点。如果SWA没有绕过Office365流量，了解可能出现的特定技术挑战就很重要。其中之一是应用程序所需的连接数。大小调整必须适当调整，以适应Office365应用程序所需的其他持续TCP连接。这会将每个用户的持续TCP会话总数增加10到15个。

HTTPS代理执行的解密和重新加密操作会为连接带来少量延迟。Office365应用对延迟非常敏感，如果其他因素（如WAN连接缓慢和地理位置分散）加剧了这一问题，则会影响用户体验。

某些Office365应用程序使用专有的TLS参数，这些参数会阻止HTTPS代理与应用程序服务器完成握手。验证证书或检索主机名时需要此步骤。当这与Skype for Business之类的应用(不会在其TLS客户端Hello消息中发送服务器名称指示(SNI)字段)组合时，需要完全绕过此流量。AsyncOS 11.8引入了仅根据目标IP地址绕过流量的功能，无需进行证书检查即可解决此情况。

监控和警报

CLI监视器

SWA CLI提供用于实时监控重要进程的命令。最有用的命令是显示与代理进程相关的统计信息的命令。status detail 命令是资源使用率和性能指标的摘要的理想来源，包括正常运行时间、使用的带宽、响应延迟、连接数等。以下是此命令的示例输出：

```
SWA_CLI>  status detail

Status as of:                  Fri Nov 11 14:06:52 2022 +03
Up since:                      Fri Apr 08 10:15:00 2022 +03 (217d 3h 51m 52s)
System Resource Utilization:
  CPU                                3.3%
  RAM                                6.2%
  Reporting/Logging Disk            45.6%
Transactions per Second:
  Average in last minute               55
  Maximum in last hour                201
  Average in last hour                 65
  Maximum since proxy restart       1031
  Average since proxy restart          51
Bandwidth (Mbps):
  Average in last minute            4.676
  Maximum in last hour            327.258
  Average in last hour             10.845
  Maximum since proxy restart    1581.297
  Average since proxy restart      11.167
Response Time (ms):
  Average in last minute               635
  Maximum in last hour              376209
  Average in last hour                 605
  Maximum since proxy restart      2602943
  Average since proxy restart          701
```

```
Cache Hit Rate:
  Average in last minute                    0
  Maximum in last hour                      2
  Average in last hour                      0
  Maximum since proxy restart              15
  Average since proxy restart               0
Connections:
  Idle client connections                 186
  Idle server connections                 184
  Total client connections               3499
  Total server connections               3632
SSLJobs:
  In queue Avg in last minute               4
  Average in last minute                45214
  SSLInfo Average in last min              94
Network Events:
  Average in last minute                  0.0
  Maximum in last minute                   35
  Network events in last min           124502
```

rate 命令显示有关prox进程使用的CPU百分比的实时信息，以及每秒请求数(RPS)和缓存统计信息。此命令继续轮询并显示新输出，直到中断。以下是此命令的输出示例：

```
SWA_CLI>  rate

Press Ctrl-C to stop.
  %proxy  reqs                          client    server    %bw  disk  disk
     CPU  /sec   hits blocks misses     kb/sec    kb/sec  saved   wrs   rds
  5.00    51      1    147    370       2283      2268    0.6    48    37
  4.00    36      0    128    237      21695     21687    0.0    47    38
  4.00    48      2    179    307       8168      8154    0.2    65    33
  5.00    53      0    161    372       2894      2880    0.5    48    32
  6.00    52      0    198    328      15110     15100    0.1    63    33
  6.00    77      0    415    363       4695      4684    0.2    48    34
  7.00    85      1    417    433       5270      5251    0.4    49    35
  7.00    67      1    443    228       2242      2232    0.5    85    44
```

tcpservices命令显示有关选定进程侦听端口的信息。每个过程以及地址和端口组合的说明也会显示：

```
SWA_CLI> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon
```

```
Feature Processes
  coeuslogd    - Main WSA controller
  gui          - GUI process
  hermes       - Mail server for sending alerts, etc.
  java         - Processes for storing and querying Web Tracking data
  musd         - AnyConnect Secure Mobility server
  pacd         - PAC file hosting daemon
  prox         - WSA proxy
  trafmon      - L4 Traffic Monitor
  uds          - User Discovery System (Transparent Auth)
  wccpd        - WCCP daemon

COMMAND      USER         TYPE NODE   NAME
connector    root         IPv4 TCP    127.0.0.1:8823
java         root         IPv6 TCP    [::127.0.0.1]:18081
hybridd      root         IPv4 TCP    127.0.0.1:8833
gui          root         IPv4 TCP    172.16.40.80:8443
ginetd       root         IPv4 TCP    172.16.40.80:ssh
nginx        root         IPv6 TCP    *:4431
nginx        root         IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
api_serve    root         IPv4 TCP    172.16.40.80:6080
api_serve    root         IPv4 TCP    127.0.0.1:60001
api_serve    root         IPv4 TCP    172.16.40.80:6443
chimera      root         IPv4 TCP    127.0.0.1:6380
nectar       root         IPv4 TCP    127.0.0.1:6382
redis-ser    root         IPv4 TCP    127.0.0.1:6383
redis-ser    root         IPv4 TCP    127.0.0.1:6379
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25255
```

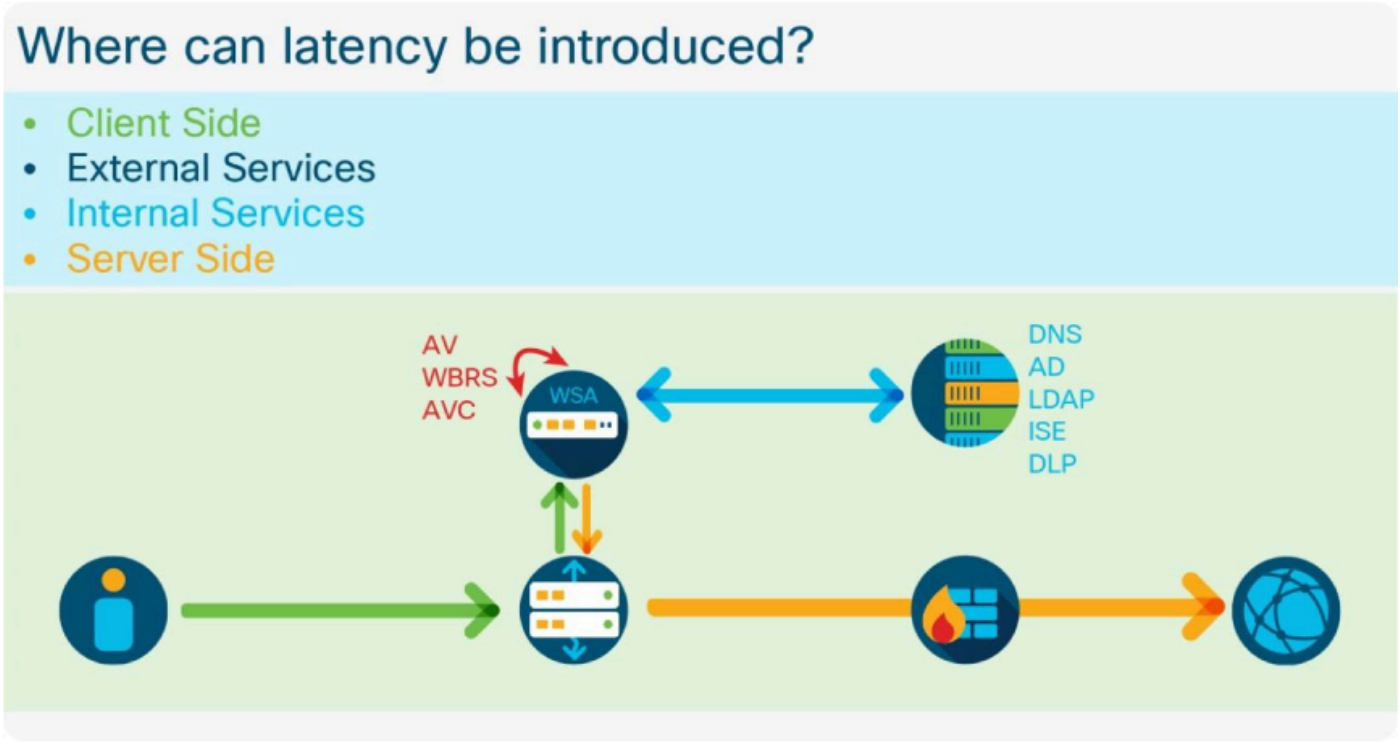
```
prox         root         IPv4 TCP    127.0.0.1:socks
prox         root         IPv6 TCP    [::1]:socks
prox         root         IPv4 TCP    172.16.11.69:socks
prox         root         IPv4 TCP    172.16.11.68:socks
prox         root         IPv4 TCP    172.16.11.252:socks
prox         root         IPv4 TCP    127.0.0.1:ftp-proxy
prox         root         IPv6 TCP    [::1]:ftp-proxy
prox         root         IPv4 TCP    172.16.11.69:ftp-proxy
prox         root         IPv4 TCP    172.16.11.68:ftp-proxy
prox         root         IPv4 TCP    172.16.11.252:ftp-proxy
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25256
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.21.11.69:https
prox         root         IPv4 TCP    172.21.11.68:https
prox         root         IPv4 TCP    172.21.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25257
smart_age    root         IPv6 TCP    [::127.0.0.1]:65501
smart_age    root         IPv6 TCP    [::127.0.0.1]:28073
interface    root         IPv4 TCP    127.0.0.1:domain
stunnel      root         IPv4 TCP    127.0.0.1:32137
```

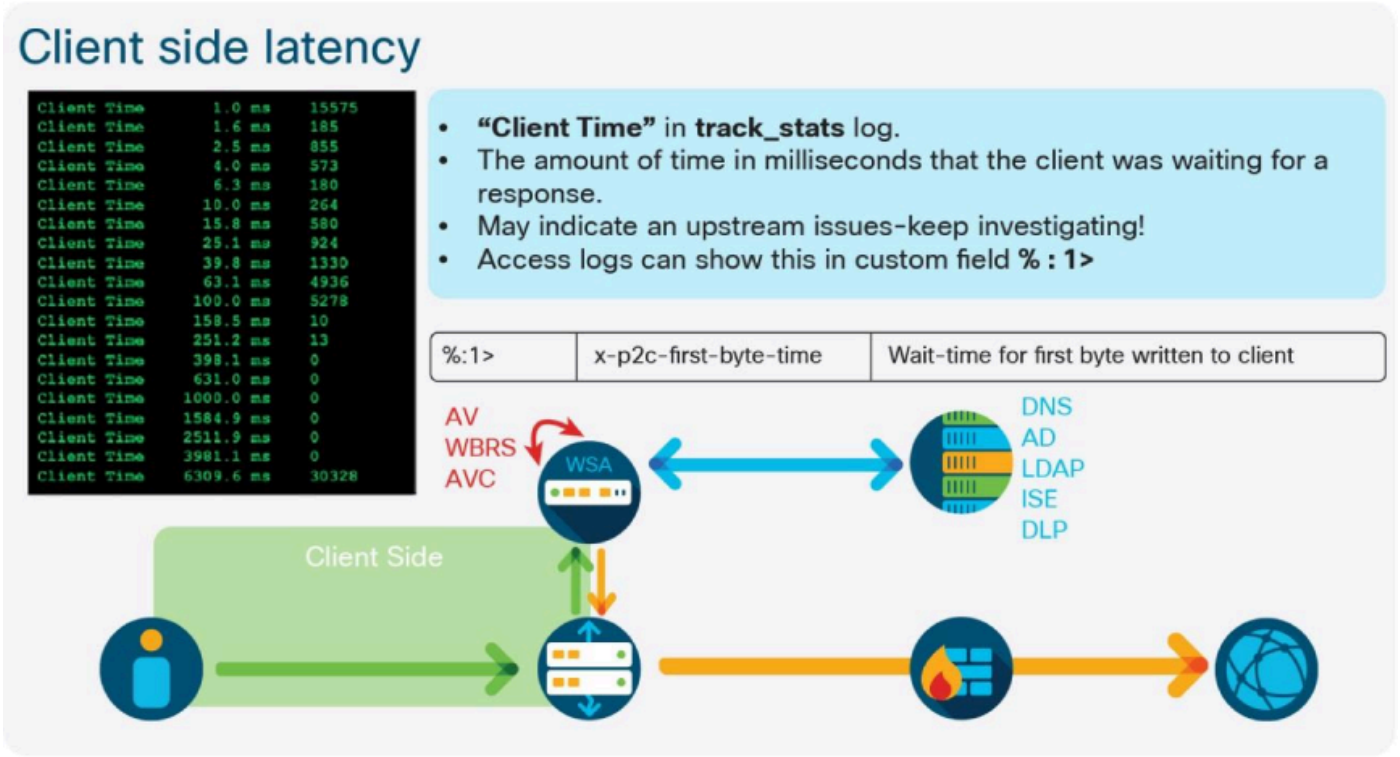
日志记录

Web流量具有高度动态性和多样性。代理部署完成后，定期重新评估通过设备的数据流的数量和构成非常重要。您必须定期（每季度一次）检查解密流量的百分比，以确保大小与初始安装的预期和规格一致。这可以通过高级网络安全报告(AWSR)等日志管理产品实现，也可以通过访问日志使用简单的Bash或PowerShell命令实现。还必须定期重新评估RPS的数量，以确保设备有足够的开销来应对高可用性、负载均衡配置中的流量高峰和可能的故障切换。

每五分钟添加一次track_stats日志，该日志包含与代理进程及其在内存中的对象直接相关的输出的

多个部分。性能监控中最有用的部分显示了各种请求进程的平均延迟，包括DNS查找时间、AV引擎扫描时间和许多更有用的字段。此日志不能从GUI或CLI进行配置，只能通过安全复制协议(SCP)或文件传输协议(FTP)进行访问。这是排除性能故障时所需的最重要的日志，因此必须经常轮询它。



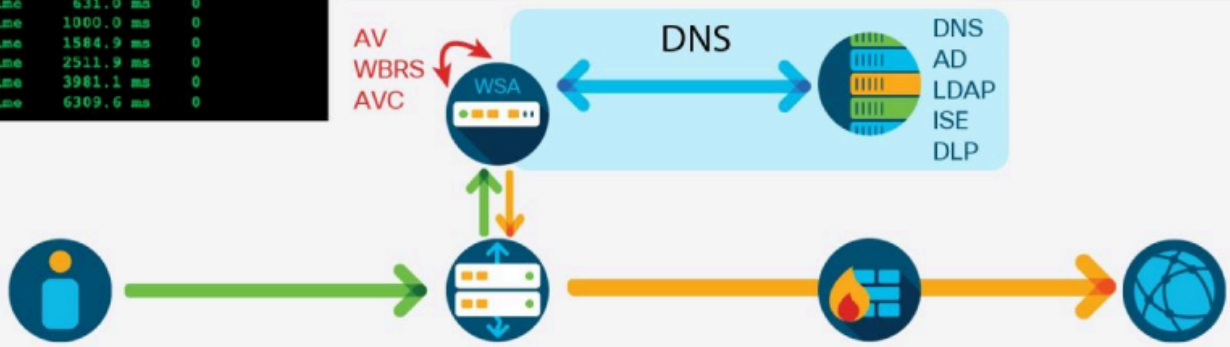


DNS latency

```
DNS Time       1.0 ms    51
DNS Time       1.6 ms    347
DNS Time       2.5 ms    152
DNS Time       4.0 ms    71
DNS Time       6.3 ms    98
DNS Time      10.0 ms    7
DNS Time      15.8 ms    11
DNS Time      25.1 ms    13
DNS Time      39.8 ms    2
DNS Time      63.1 ms    3
DNS Time     100.0 ms    7
DNS Time     158.5 ms    16
DNS Time     251.2 ms    4
DNS Time     398.1 ms    1
DNS Time     631.0 ms    0
DNS Time    1000.0 ms    0
DNS Time    1584.9 ms    0
DNS Time    2511.9 ms    0
DNS Time    3981.1 ms    0
DNS Time    6309.6 ms    0
```

- The amount of time in milliseconds that the WSA waited for a DNS response.
- Calls for investigation for your DNS resolvers (or path to them).
- **access logs** can show this in custom field **% : >d**

%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS Process to send a DNS result to ehe Web proxy.

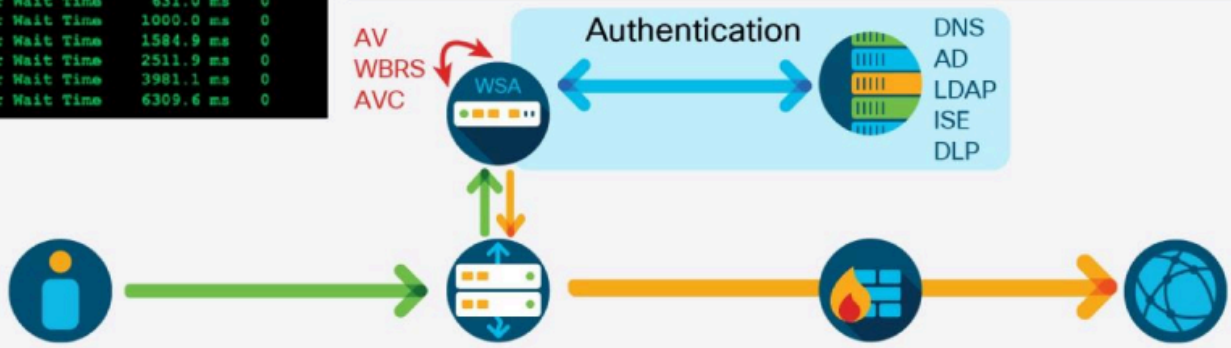


Authentication latency

```
Server Wait Time       1.0 ms    0
Server Wait Time       1.6 ms    0
Server Wait Time       2.5 ms    0
Server Wait Time       4.0 ms    0
Server Wait Time       6.3 ms    0
Server Wait Time      10.0 ms    0
Server Wait Time      15.8 ms    0
Server Wait Time      25.1 ms    0
Server Wait Time      39.8 ms    0
Server Wait Time      63.1 ms    0
Server Wait Time     100.0 ms    0
Server Wait Time     158.5 ms    1
Server Wait Time     251.2 ms    1
Server Wait Time     398.1 ms    0
Server Wait Time     631.0 ms    0
Server Wait Time    1000.0 ms    0
Server Wait Time    1584.9 ms    0
Server Wait Time    2511.9 ms    0
Server Wait Time    3981.1 ms    0
Server Wait Time    6309.6 ms    0
```

- There are two metrics: **“Auth Helper Wait Time”** and **“Auth Helper Service Wait Time.”**
- Use the first to get pure auth time without the request time added.
- **access logs** can show this in custom field **% : >a**

%:<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.

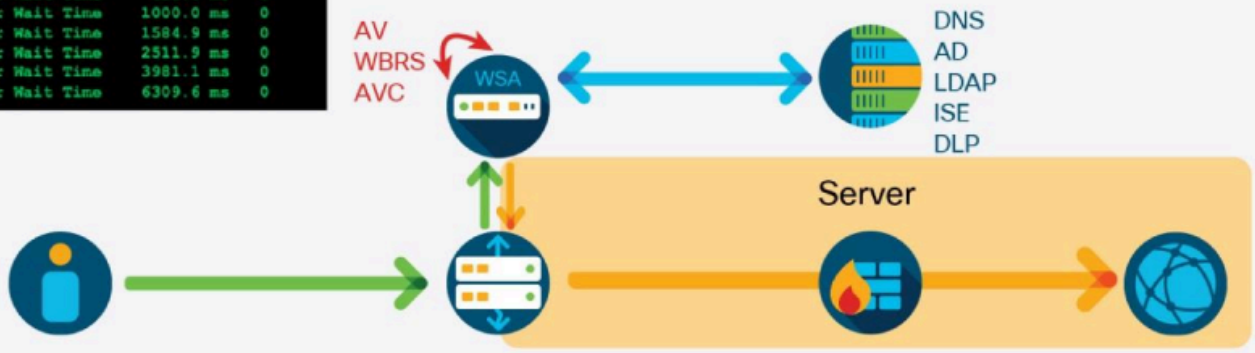


Server latency-wait time

```
Server Wait Time        1.0 ms    0
Server Wait Time        1.6 ms    0
Server Wait Time        2.5 ms    0
Server Wait Time        4.0 ms    0
Server Wait Time        6.3 ms    0
Server Wait Time       10.0 ms    0
Server Wait Time       15.8 ms    0
Server Wait Time       25.1 ms    0
Server Wait Time       39.8 ms    0
Server Wait Time       63.1 ms    0
Server Wait Time      100.0 ms    0
Server Wait Time      158.5 ms    1
Server Wait Time      251.2 ms    1
Server Wait Time      398.1 ms    0
Server Wait Time      631.0 ms    0
Server Wait Time     1000.0 ms    0
Server Wait Time     1584.9 ms    0
Server Wait Time     2511.9 ms    0
Server Wait Time     3981.1 ms    0
Server Wait Time     6309.6 ms    0
```

- The amount of time in milliseconds that the WSA waited for the first byte of the server response.
- Calls for investigation of your upstream devices and WAN connection.
- **access logs** can show this in custom field **% : >1**

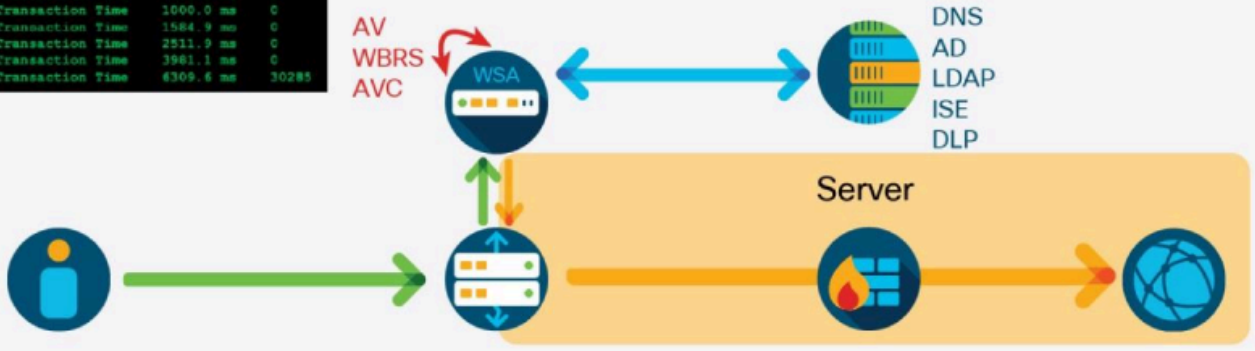
%:>1	x-s2p-first-byte-time	Wait-time for first response byte from server

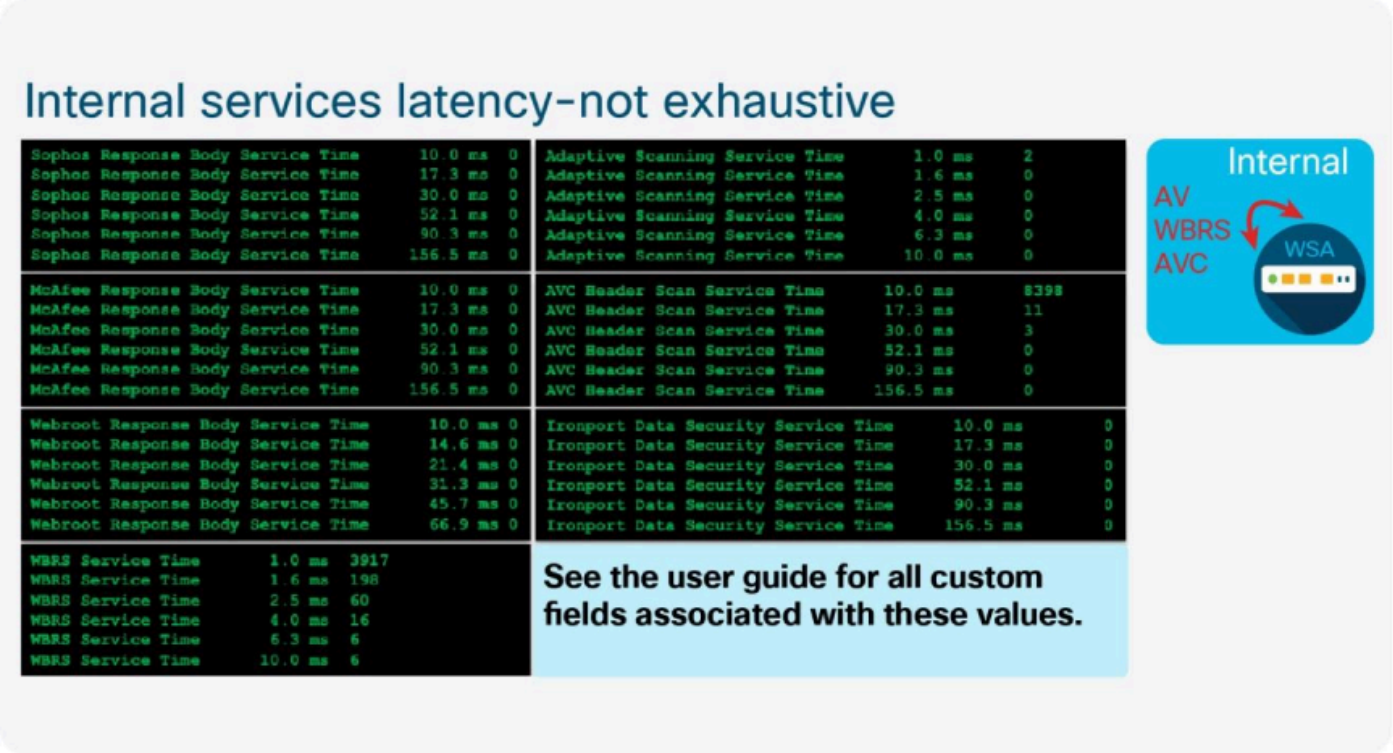


Server latency-transaction time

```
Server Transaction Time        1.0 ms    1422
Server Transaction Time        1.6 ms    858
Server Transaction Time        2.5 ms    1035
Server Transaction Time        4.0 ms    1106
Server Transaction Time        6.3 ms    758
Server Transaction Time       10.0 ms    810
Server Transaction Time       15.8 ms    288
Server Transaction Time       25.1 ms    45
Server Transaction Time       39.8 ms    73
Server Transaction Time       63.1 ms    4221
Server Transaction Time      100.0 ms    8897
Server Transaction Time      158.5 ms    5
Server Transaction Time      251.2 ms    0
Server Transaction Time      398.1 ms    2
Server Transaction Time      631.0 ms    0
Server Transaction Time     1000.0 ms    0
Server Transaction Time     1584.9 ms    0
Server Transaction Time     2511.9 ms    0
Server Transaction Time     3981.1 ms    0
Server Transaction Time     6309.6 ms    30285
```

- The amount of time in milliseconds for the entire server-side transaction to complete.
- Calls for investigation of your upstream devices and WAN connection.
- No **access logs** custom field, but can be determined by a combinationof them.





每个SHD日志行每60秒写入一次，包含许多对性能监控重要的字段，包括延迟、RPS以及客户端和服务器端连接总数。以下是SHD日志行的示例：

```
Fri Nov 11 14:16:42 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 62 Band 11383 Latency 61
Fri Nov 11 14:17:42 2022 Info: Status: CPULd 2.6 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 10532 Latency 77
Fri Nov 11 14:18:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.6 Reqs 48 Band 7285 Latency 579
Fri Nov 11 14:19:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.6 Reqs 52 Band 34294 Latency 79
Fri Nov 11 14:20:43 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 8696 Latency 691
Fri Nov 11 14:21:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 49 Band 7064 Latency 140
Fri Nov 11 14:22:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.8 Reqs 41 Band 5444 Latency 788
Fri Nov 11 14:23:43 2022 Info: Status: CPULd 2.2 DskUtil 45.7 RAMUtil 6.8 Reqs 48 Band 6793 Latency 820
Fri Nov 11 14:24:44 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 44 Band 8735 Latency 673
Fri Nov 11 14:25:44 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 53 Band 8338 Latency 731
```

可向access_logs添加其他自定义字段，这些字段表示单个请求的延迟信息。这些字段包括服务器响应、DNS解析和AV扫描程序延迟。这些字段必须添加到日志中，以收集用于故障排除的重要信息。这是推荐使用的自定义字段字符串：

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms)
```

```
, Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<,
```

```
a; DNS response = %:

d, WBRS response = %:

r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respon

s, AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ][Client Port = %F, Server IP = %k
```

从这些值中得到的性能信息如下：

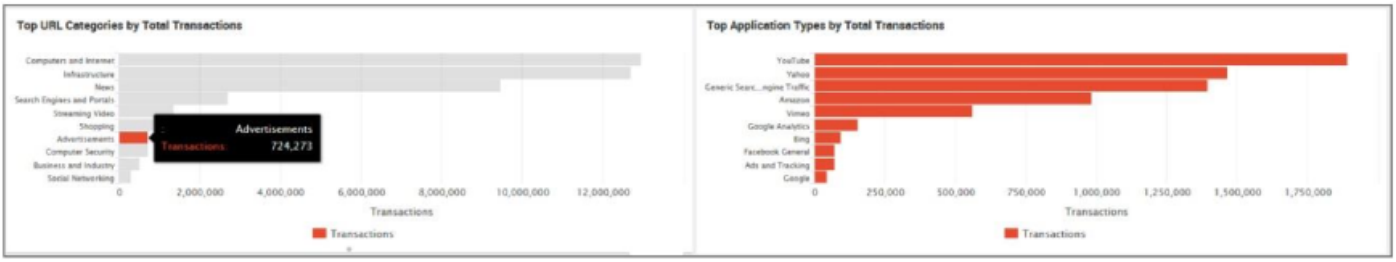
自定义字段	描述
%：<a	Web代理发送请求后，从Web代理身份验证过程接收响应的等待时间。
%：<b	在报头之后将请求正文写入服务器的等待时间。
%：<d	Web代理发送请求后，从Web代理DNS进程接收响应的等待时间。
%：<h	在第一字节之后将请求报头写入服务器的等待时间。
%：<r	在Web代理发送请求后，从Web信誉过滤器接收响应的等待时间。
%：<s	在Web代理发送请求后，从Web代理反间谍软件进程接收判定的等待时间。
%：>	等待服务器发出第一个响应字节的时间。
%：>a	从Web代理身份验证过程接收响应的等待时间，包括Web代理发送请求所需的时间。

%：>b	收到标头后等待完成响应正文的时间。
%：>c	Web代理从磁盘缓存读取响应所需的时间。
%：>d	从Web代理DNS进程接收响应的等待时间，包括Web代理发送请求所需的时间。
%：>h	第一个响应字节之后的服务器报头的等待时间。
%：>r	从Web信誉过滤器接收裁决的等待时间，包括Web代理发送请求所需的时间。
%：>s	从Web代理反间谍软件进程接收判定的等待时间，包括Web代理发送请求所需的时间。
%：1<	等待新客户端连接第一个请求字节的时间。
%：1>	向客户端写入第一个字节的等待时间。
%：b<	等待时间以完成客户端正文。
%：b>	将完整正文写入客户端的等待时间。
%：e>	在Web代理发送请求后，等待一段时间以接收来自AMP扫描引擎的响应。
%：e<	从AMP扫描引擎接收判定的等待时间，包括Web代理发送请求所需的时间。
%：h<	第一个字节后完成客户端报头的等待时间。
%：h>	将完整报头写入客户端的等待时间。
%：m<	从McAfee扫描引擎接收判定的等待时间，包括Web代理发送请求所需的时间。
%：m>	在Web代理发送请求后，等待一段时间以接收来自McAfee扫描引擎的响应。
%F	客户端源端口。
%p	Web服务器端口。
%k	数据源IP地址（网络服务器IP地址）。
%：w<	从Webroot扫描引擎接收判定的等待时间，包括Web代理发送请求所需的时间。
%：w>	在Web代理发送请求后，从Webroot扫描引擎接收响应的等待时间。

SWA许可模式允许对虚拟设备重复使用物理设备许可证。您可以利用此优势并部署测试SWAv设备，以便在实验室环境中使用。可以通过这种方式试用新功能和配置，以确保稳定性和可靠性，同时不会违反许可条款。

高级网络安全报告(AWSR)

必须利用AWSR来充分利用来自SWA的报告数据。特别是在部署了许多SWA的环境中，此解决方案的可扩展性比在安全管理设备(SMA)上使用集中报告要高许多倍，并提供自定义报告属性，从而向数据添加大量深度和自定义信息。可对报告进行分组和自定义，以满足任何组织的需求。在确定AWSR规模时，必须利用思科高级服务组。



邮件警报

最好将SWA上的内置邮件警报系统用作基线警报系统。它必须进行适当调整以满足管理员的需求，因为如果启用了所有的信息事件，它可能会非常嘈杂。限制警报并主动监控警报比对所有警报发出警报并忽略它们作为垃圾邮件更重要。

警报设置	配置
发送警报时要使用的发件人地址	自动生成
发送重复警报之前等待的初始秒数	300 秒
发送重复警报之前等待的最大秒数	3600 秒

可用性监控

有两种方法可用于监控Web代理的可用性。

1. 第一个是第3层(L3)监控，用于测试设备IP地址在网络上是否可达。测试此情况的最简单方法是定期向该地址发送ICMP响应(ping)请求并检查应答数据包。可以解析应答的属性（如TTL和延迟）以确定网络层的运行状况。
2. 设备可能会响应ping，但代理进程无响应或时断时续。因此，建议使用第7层(L7)监控器，该监控器会向设备发送显式代理请求，并需要200 OK HTTP响应代码。这不仅测试了网络接口的可达性，还测试了代理服务的响应性，以及在请求外部资源时上游服务的生存能力。此类监控通常采用请求代理连接到资源的显式HTTP HEAD请求的形式。HEAD方法请求客户端发送GET请求时要返回的报头，但仅包括响应报头，不包括数据。
    - 如果使用L7监控工具或脚本，请确保流量免于身份验证，这一点非常重要。否则，会导致定期身份验证失败和资源消耗。当您在监控工具中使用自定义用户代理字符串时，必须采用它来识别流量。即使流量免于身份验证，仍可以通过访问策略限制其访问不必要的Internet。

当您使用这些方法中的一种或多种时，管理员必须围绕代理响应建立可接受度量的基准，并使用该基准构建警报阈值。在决定如何配置阈值和警报之前，您必须专门花时间收集此类检查的响应。

SNMP 监控

简单网络管理协议(SNMP)是监控设备运行状况的主要方法。它可用于接收来自设备的警报（陷阱）或轮询各种对象标识符(OID)以收集信息。SWA上有许多OID，涵盖从硬件到资源使用再到单个流程信息和请求统计信息的所有内容。

由于与硬件和性能相关的原因，必须监控许多特定的计算机信息库(MIB)。您可以在此处找到MIB的完整列表：https://www.cisco.com/web/ironport/tools/web/asyncosweb-mib.txt。

这是推荐监控的MIB的列表，而不是详尽的列表：

硬件OID	名称
1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	raidStatus
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError
1.3.6.1.4.1.15497.1.1.1.10	fanTable
1.3.6.1.4.1.15497.1.1.1.9.1.2	摄氏度

下面是OID直接映射到status detail CLI命令的输出：

OID	名称	状态详细信息字段
系统资源		
1.3.6.1.4.1.15497.1.1.1.2.0	百分比CPUutilization	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	percentMemoryUtilization	RAM
每秒事务数		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruNow	过去一分钟内每秒的平均事务数。
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	过去一小时内每秒的最大事务数。
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMean	过去一小时内每秒的平均事务数。
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	自代理重新启动以来每秒的最大事务数。
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	自代理重新启动以来的平均每秒事务数。
带宽		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalNow	过去一分钟内的平均带宽。
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	过去一小时内的最大带宽。
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	过去一小时内的平均带宽。
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	自代理重新启动以来的最大带宽。
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	自代理重新启动以来的平均带宽。
响应时间		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	过去一分钟内的平均缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	过去一小时内的最大缓存命中率。

1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	过去一小时内的平均高速缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	自代理重新启动以来的最大缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	自代理重新启动以来的平均缓存命中率。
缓存命中率		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	过去一分钟内的平均缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	过去一小时内的最大缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	过去一小时内的平均高速缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	自代理重新启动以来的最大缓存命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	自代理重新启动以来的平均缓存命中率。
连接		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	空闲客户端连接。
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	空闲服务器连接。
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConns	客户端连接总数。
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	服务器连接总数。

结论

本指南旨在介绍SWA配置、部署和监控的最重要方面。作为参考指南，其目标是为那些希望确保最有效地使用全部门办法的人提供有价值的信息。此处介绍的最佳实践对于作为安全工具的设备的稳定性、可扩展性和有效性非常重要。它还寻求作为相关资源继续发展，因此必须频繁更新，以反映网络环境和产品功能集的变化。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。