安全Web设备版本更改

目录

简介

本文档介绍不同版本Secure Web Appliance(SWA)的主要更改和新增功能。

先决条件

要求

本文没有特殊要求。

本文使用的缩写为：

LD:有限部署。

GD:通用部署。

MD:维护部署

ED:早期部署。

HP:热修补程序。

CLI:命令行界面。

GUI:图形用户界面

HTTP:超文本传输协议。

HTTPS:安全超文本传输协议。

ECDSA:Elliptic Curve数字签名算法。

PID：进程标识符。

CTR:思科威胁响应。

AMP:高级恶意软件防护。

URL:统一资源定位器。

CDA:上下文目录代理。

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。

更改每个版本的历史记录

version	类型	行为变化	增强功能/新增功能
12.0.1-268	LD	— 系统CPU和内存要求从12.0版本开始更改。 — 默认情况下，TLSv1.3在设备上启用。 — 密码“TLS_AES_256_GCM_SHA384”已添加到默认密码列表中。	- Cisco AsyncOS 12.0版本为平台S680、S690和S695提供高性能(HP)网络安全设备。 — 在advancedproxyconfig主命令下添加新的子命令highperformance，以启用和禁用高性能模式。 — 将SWA与思科威胁响应(CTR)门户集成。 — 设备支持TLSv1.3版本。 — 配置文件备份功能从System Administration下的Log Subscriptions子菜单移动到Configuration File。 — 设备现在支持为HTTPS代理上传ECDSA证书。 -新的诊断CLI proxyscannermap子命令添加在diagnostic > proxy下。显示每个代理和相应的扫描程序进程之间的PID映射。 — 新的选项searchdetails添加在CLI命令authcache下。 — 在CLI命令reportingconfig下添加新的子命令CTROBSERVABLE，以启用或禁用CTR基于可观察的索引。

12.0.1-334	GD		— 在advancedproxyconfig主命令下添加新的子命令扫描程序，以排除AMP引擎要扫描的MIME类型。
12.0.2-004	MD	— 使用TLS 1.2或更高版本将设备连接到AMP文件信誉服务器。 - AMERICAS（传统）cloud-sa.amp.sourcefire.com无法在设备上配置。	— 主CLI命令advancedproxyconfig > scanners > AMP中添加了新选项“Enter the number of concurrent scans to be supported by AMP”（输入AMP支持的并发扫描数）。 您可以在主CLI命令advancedproxyconfig > scanners中将长时间运行的扫描逐出的默认Unscannable判定更改为Timeout，反之亦然，从新的CLI子命令逐出命令中进行更改。
12.02-012	MD		— 在设备的Web用户界面上触发警报消息 当代理Malloc Memory超过90%的代理Malloc Memory限制时，会向配置为接收“Web Proxy”严重警报的所有“警报收件人”发送邮件通知。 — 新的网络界面为监控报告和跟踪网络服务提供新外观。
12.0.3-005	MD		
12.0.3-007	MD		— 新URL类别更新通知
12.0.4-002	MD		
12.0.5-011	MD	— 设备管理Web用户界面默认启用TLSv1.2 — 默认情况下禁用会话恢复。	— 在CDA配置部分添加消息以指示CDA支持终止。
12.5.1-011	LD	-默认情况下，在设备上启用思科成功网络功能。 — 修改这些日志以包含更多详细信息： 现在，身份验证失败时，访问日志会显示用户名。	- Cisco AsyncOS 12.5版本为平台S680、S690和S695提供高性能(HP)网络安全设备。这提高了当前高端设备的流量性能。 — 现在您可以升级到12.5版本并在型号（S680、S690、S695、S680F、S690F和S695F）上使用高性能模式，即使您已在设备上启用以下功能：

		身份验证框架日志现在显示以下失败身份验证协议的客户端IP地址：NTLM、BASIC、SSO（透明）	• Web流量分接头 • 数量和时间配额 • 整体带宽限制 -现在可以通过创建IP欺骗配置文件并将其添加到路由策略来配置Web代理IP欺骗。 - 现在，您可以为YouTube创建自定义URL类别，并在YouTube自定义类别上设置策略以实现安全访问控制。 - 在新网络界面中，设备有一个新页面(Monitoring > System Status)以显示设备的当前状态和配置。 - 思科成功网络(CSN)功能使思科能够收集设备的功能使用信息遥感勘测。 - 用于网络、日志订阅和其他配置的REST API。
12.5.1-035	GD	— 弃用TLS 1.0/1.1: 使用TLS 1.2或更高版本将设备连接到AMP文件信誉服务器。AMERICAS（传统）cloud-sa.amp.sourcefire.com从AMP文件信誉服务器列表中删除，因此无法在设备上配置AMERICAS（传统）cloud-sa.amp.sourcefire.com。	— 在AsyncOS 12.5.1-035及更高版本中不支持配置身份验证的缓存大小(网络(Network)>身份验证(Authentication)>身份验证设置(Authentication Settings)>凭证缓存选项(Credential Cache Options))。
12.5.1-043	GD		— 警报消息显示在设备的Web用户界面上(“系统管理”(System Administration)>“警报”(Alerts)>“查看排名靠前的警报”(View Top Alerts)): • 当代理malloc内存超过90%的代理malloc内存限制时 • 当代理在malloc内存的100%上重新启动时 在这两种情况下，都会向配置为接收“Web代理”严重警报的所有“警报收件人”发送电子邮件通知。

12.5.2-007	MD		— 新URL类别更新通知引入标语中。有关即将进行的URL类别更新的电子邮件通知也会发送给用户。
12.5.2-011	MD		
12.5.3-002	MD		
12.5.4-005	MD	— 在Cisco AsyncOS 12.5.4版本中，TLSv1.2默认启用设备管理Web用户界面。 - 升级到Cisco AsyncOS 12.5.4版本后，默认情况下会禁用会话恢复。 — 在CDA配置部分添加消息以指示CDA支持终止	
12.5.4-011	MD刷新		
12.5.5-004	MD		-升级到Cisco AsyncOS 12.5后，首次执行networktuning命令时，您会收到重新启动代理进程的提示。
12.5.5-008	MD刷新		
12.5.6-008	MD		
14.0.1-014	LD	— 默认情况下，HTTP 2.0功能处于禁用状态。要启用此功能，请使用<HTTP2>命令。 — 适用于思科网络安全设备的AsyncOS 14.0支持客户端和服务器中的TLSv1.3会话恢复。 — 修改这些证书的有效期： • HTTPS • ISE • SAAS	— 思科网络安全设备现在支持与Cisco SecureX集成。 — 您可以为HTTP请求配置自定义报头配置文件，也可以在报头重写配置文件下创建多个报头。 — 您现在可以为Active Directory配置基于报头的身份验证方案。客户端和网络安全设备将用户视为已验证用户，并且不会再次提示用户进行身份验证或输入用户凭证。当网络安全设备充当上游设备时，X验证功能会发挥作用。

		• 设备证书 • 演示/管理证书 — 由于日志订阅中的日志名称和文件名无效，升级失败时，设备的CLI和GUI会显示消息。 — 默认情况下，轮询间隔设置为24小时。 — 升级到此版本后，如果Base DN(Base Distinguished Name)字段(“网络”(Network)>“身份验证”(Authentication)>“添加领域”(Add Realm))为空，则无法执行LDAP身份验证的启动测试。	- 设备的系统状态控制面板已增强： • Capacity选项卡 — 提供时间范围、系统CPU和内存使用情况、带宽和RPS、按功能划分的CPU使用情况以及客户端或服务器连接的详细信息。 • Status选项卡下的Proxy Traffic Characteristics提供客户端和服务器连接的详细信息。 • 服务响应时间现在包括条形图的更多详细信息以及之前日期的图例数据。 — 您现在可以在设备的配置数据中使用管理策略、访问策略和旁路策略的REST API，检索配置信息并执行更改（如修改当前信息、添加新信息或删除条目） - Cisco AsyncOS 14.0版本支持HTTP 2.0，用于Web请求和通过TLS的响应。HTTP 2.0支持需要基于TLS ALPN的协商，该协商仅在TLS 1.2版本以后可用。 在此版本中，以下功能不支持HTTPS 2.0: • Web流量分接头 • 外部DLP • 整体带宽和应用带宽 — 引入新的CLI命令<HTTP2>以启用或禁用HTTP 2.0配置。您无法通过设备Web用户界面启用或禁用HTTP 2.0并限制HTTP 2.0的域。 — 通过Cisco Secure Email and Web Manage不支持HTTP 2.0的配置 — 当您尝试使用以下任何功能的默认证书时，CLI会显示新的警告消息： • 设备证书（在Web用户界面中，导航到Network > Certificate Management > Appliance Certificate） • 凭证加密证书（在Web用户界面中，导航到Network > Authentication > Edit Settings > Advanced部分）

			• HTTPS管理UI证书（在命令行界面中，使用certconfig > SETUP） — 新的子命令OCSPVALIDATION_FOR_SERVER_CERT添加在certconfig下。使用此新子命令，您可以为LDAP和更新服务器证书启用OCSP验证。如果启用了证书验证，则当通信中涉及的证书被撤销时，您会收到警报。 — 添加了一个新的CLI命令gatheredconfig，以配置设备和身份验证服务器之间的轮询功能。 — 现在，您可以在设备上配置智能许可证功能时，选择管理和数据接口。
14.0.1-040	LD	— 当您启用智能软件许可并在思科智能软件管理器中注册网络安全设备时，思科云服务 (Network > Cloud Service Settings)通过思科云服务门户自动启用和注册安全Web设备。 — 如果在设备上注册了智能许可，则无法禁用或注销思科云服务。 — 如果您已将设备注册到思科智能软件管理器，但尚未配置思科云服务，则升级到AsyncOS 14.0.1-040后，思科云服务将自动启用。默认情况下，区域注册为美洲，您可以根据需要修改区域（欧洲和APJC）。 — 如果在设备上注册了智能许可证，则无法禁用或注销思科云服务。	— 您可以通过CLI中的smartaccountinfo命令查看在思科智能软件管理器门户中创建的智能帐户的详细信息。 — 如果思科云服务证书已过期或即将过期，思科云服务会在升级到AsyncOS 14.0.1-040后自动续订证书。 — 如果思科云服务证书已过期，现在您可以从CLI中的cloudserviceconfig > fetchcertificate子命令从思科Talos情报服务门户下载新证书。 — 您可以使用思科云服务门户自动注册网络安全设备(CLI中的cloudserviceconfig > autoregister子命令) — 可以从CLI中的updateconfig > clientcertificate子命令加载虚拟设备和硬件设备的证书。 — 新URL类别更新通知引入标语中。 系统还会向用户发送有关即将进行的URL类别更新的电子邮件通知。
14.0.1-053	GD		
14.0.1-503	惠普		

14.0.2-012	MD	— 在Cisco AsyncOS 14.0.2版本中，在System Administrator > SSL Configuration下，默认启用Appliance Management Web User Interface的TLSv1.2。 — 默认情况下禁用会话恢复。	— 在CDA配置部分添加消息以指示CDA支持终止。 — 现在，您可以从Test Interface下拉列表选择用于智能许可证注册的数据或管理接口。
14.0.3-014	MD	— 升级到Cisco AsyncOS 14.0后，首次执行networktuning命令时，您会收到重新启动代理进程的提示。	
14.0.3-502	惠普	— 当安全Web设备在高性能模式下运行时，堆限制耗尽会禁用高延迟并接受处理程序。这会导致连接数量减少。	
14.0.4-005	MD		
14.5.0-498	LD	— 产品重新命名： • 面向终端的AMP、高级恶意软件防护和AMP已更改为 安全终端 • 线程网格（文件分析）更改为恶意软件分析 — 错误分类请求通过HTTPS发送，因此您不会收到安全警报通知。 - Samba版本已升级到版本4.11.15。 — 默认情况下，TLSv1.2在“系统管理员”(System Administrator)>“SSL配置”(SSL Configuration)下为设备管理Web用户界面启用。 — 在AsyncOS 14.5全新安装中，默认情况下，HTTPS代理页面中的Expired and Mismatched Hostname certificate configurations值被选为Drop，而	— 安全网络设备现在可以验证从DNS服务器收到的DNS响应是否支持加密签名。 — 安全Web设备将客户端发起的并发连接数限制为已配置的值。 — 在AsyncOS版本14.5中，思科网络安全设备已重新命名为思科安全网络设备 — 当客户端Web浏览器上显示EUN页面时，解密策略组中的访问日志决策标记会附加EUN（最终用户通知）。 — 克隆策略功能允许您复制或克隆策略的配置以及创建新策略。 — 您可以通过配置配额配置文件中的带宽值并映射访问策略URL类别或整体网络活动配额中的配额配置文件来管理流量带宽。 — 用于配置管理策略、解密策略、路由策略、IP欺骗策略、防恶意软件和信誉、身份验证领域、思科智能软件许可证、Cisco Umbrella无缝ID、身份服务和系统设置的REST API。

		不是Monitor。	— 您可以将ISE-SXP部署与思科安全Web设备集成以实现被动身份验证。这允许您获取所有已定义的映射，包括通过SXP发布的SGT到IP地址的映射。 - Cisco Umbrella无缝ID功能使设备能够在身份验证成功后将用户识别信息传递到Cisco Umbrella安全网络网关(SWG)。 — 在CDA配置部分添加消息以指示CDA支持终止。 — 现在，您可以从Test Interface下拉列表选择用于智能许可证注册的数据或管理接口。 — 升级到Cisco AsyncOS 14.5后，首次执行networktuning命令时，您会收到重新启动代理进程的提示。
14.5.0-537	GD		— 这些安全网络设备中具有克隆选项的策略也可由Cisco Secure Email and Web Manager(SMA)管理： • 访问策略 • 标识配置文件 • 解密策略 • 路由策略
14.5.1-008	MD		
14.5.1-016	MD		
14.6.0-108	LD		- AsyncOS 14.6通过思科安全网络设备(SWA)为Cisco Umbrella提供支持。Umbrella和安全网络设备的集成有助于部署从Umbrella到安全网络设备的通用网络策略。
15.0.0-322	LD	- FreeBSD版本已升级到FreeBSD 13.0。 - Cisco SSL 1.0.2版到Cisco SSL 1.1.1版。 - AVC、WBRSD、DCA和	— 对智能软件许可功能进行了以下增强： • 许可证预留 • 设备Led转换 — 使用智能许可证注册安全Web设备后，所有当前有效的传统许可证都会通过设备Led转换(DLC)流程自动转换为智能许可证。这些转换的许可

		Beaker等Talos引擎已升级。 — 已升级Webroot和McAfee等扫描程序引擎。	证将在CSSM门户的虚拟帐户中更新。 — 可以通过在配额配置文件中配置带宽值并映射解密策略和访问策略中的配额配置文件、URL类别或整体网络活动配额来管理流量带宽。 — 克隆策略功能允许您复制或克隆策略的配置以及创建新策略。 — 应用发现和控制(ADC)引擎： 可接受的使用策略组件，用于检查Web流量以深入了解和控制用于应用的Web流量。 使用AsyncOS 15.0，您可以使用AVC或ADC引擎来监控Web流量。默认情况下，AVC处于启用状态。ADC引擎支持高性能模式。 — 用于ADC配置的REST API — 管理员可以选择配置除默认用户名v3get以外的自定义SNMPv3用户名。 — 自定义信头的最大长度为16k。 — 用于选择安全隧道接口和远程访问连接的选项。
15.0.0-335	GD	- Device Led Conversion — 使用智能许可注册安全Web设备后，所有当前有效的经典许可证将通过Device Led Conversion(DLC)流程自动转换为智能许可证。这些转换的许可证将在CSSM门户的虚拟帐户中更新。 — 默认情况下，AVC处于启用状态。 - Cisco SSL 1.0.2版到Cisco SSL 1.1.1版 - AVC、WBRSD、DCA和Beaker等Talos引擎已升级。 - Webroot和McAfee等扫描引擎已	— 许可证预留 — 您可以为安全网络设备中启用的功能保留许可证，而无需连接到思科智能软件管理器(CSSM)门户。这主要适用于在高度安全的网络环境中部署安全Web设备，而不与互联网或外部设备通信的用户。 -可以通过配置配额配置文件中的带宽值并映射解密策略和访问策略URL类别或整体网络活动配额中的配额配置文件来管理流量带宽。 -克隆策略功能允许您复制或克隆策略的配置以及创建新策略。 — 支持应用发现与控制(ADC)引擎，这是一个可接受的使用策略组件，用于检查Web流量，以便更深入地了解和控制用于应用的Web流量。

		升级。 - FreeBSD 13.0仅与Cisco SSL 1.1.1版兼容。 只有与Cisco SSH兼容的密码、mac和kex算法才能支持与FreeBSD 13.0的SSH连接。 -作为AsyncOS15.0 GD版本的一部分，安全网络设备中的DCA功能被禁用。您可以在升级到此版本后通过导航到安全服务>可接受使用控制并选中DCA复选框来启用它。 -多处理器SWA(S690、S695、S1000V)不支持代理Malloc内存的SNMP OID的SNMPWALK/SNMPGET操作。	现在可以使用AVC或ADC引擎监控Web流量。 - ADC引擎支持高性能模式。 — 您现在可以在具有REST API的设备的访问策略配置数据中检索配置信息，并执行任何更改（例如修改当前信息、添加新信息或删除条目）。 -Admin可以选择配置除默认用户名v3get以外的自定义SNMPv3用户名。 - Web请求的自定义报头最大长度为16k。 - 用于选择安全隧道接口和远程访问连接的选项
15.0.0-364	惠普	已修复以下缺陷： Cisco Bug ID CSCvz26149 Cisco Bug ID CSCwf78874 Cisco Bug ID CSCwf84371 Cisco Bug ID CSCwh31573 Cisco Bug ID CSCwh37834 Cisco Bug ID CSCwh41379 Cisco Bug ID CSCwh48523 Cisco Bug ID CSCwh71926	
15.1.0-287	LD	— 在AsyncOS 15.1及更高版本中，必须提供智能软件许可证。 — 思科Umbrella和思科安全网络设备的集成有助于部署从	

		Umbrella到安全网络设备的通用Web策略。此外，您还可以通过Umbrella控制面板配置策略并查看日志。	

开源组件

以下是SWA中使用的开源组件的更改列表：

version	11.8.X	12.0.X	12.5.X	14.0.X	14.5.X	14.6.X	15.0.X
freebsd	10.4	10.4	10.4	11.2	11.2	11.2	13.0

相关信息

- 思科网络安全设备AsyncOS 12.0版本说明 — 思科
- 思科网络安全设备AsyncOS 12.5版本说明 — 思科
- 思科网络安全设备AsyncOS 14.0版本说明 — 思科
- 思科安全网络设备AsyncOS 14.5版本说明 — 思科
- 内容安全的版本术语是什么？(cisco.com)
- 思科安全邮件和Web虚拟设备安装指南
- 技术支持和文档 - Cisco Systems
- 思科安全网络设备AsyncOS 15.1版本说明 — 思科
- 思科安全网络设备AsyncOS 15.0热补丁1版本说明 — 思科

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）。