Alterações na versão do Secure Web Appliance

Contents

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Histórico de alterações por versão](#)
[Componentes de Código Aberto](#)
[freebsd](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve as principais alterações e recursos adicionados em diferentes versões do Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

Não há requisitos especiais para este artigo.

As abreviações usadas neste artigo são:

LD: Implantação limitada.

GD: Implantação geral.

MD: Implantação de manutenção

ED: Implantação antecipada.

HP: Hot Patch (Patch automático).

CLI: Command Line Interface (Interface de Linha de Comando).

GUI: interface gráfica do usuário

HTTP: Protocolo HTTP.

HTTPS: protocolo de transferência de hipertexto seguro.

ECDSA: Elliptic Curve Digital Signature Algorithm (Algoritmo de Assinatura Digital de Curva Elíptica).

PID: Identificador do processo.

CTR: Cisco Threat Response (Resposta às ameaças da Cisco).

AMP: Advanced Malware Protection (Proteção avançada contra malware).

URL: Uniform Resource Locator (Localizador Uniforme de Recursos).

CDA: Context Diretory Agent (Agente de Diretório de Contexto).

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Histórico de alterações por versão

Versão	Tipo	Alterações de comportamento	Aprimoramentos/recursos adicionados
12.0.1-268	LD	- Os requisitos de CPU e memória do sistema são alterados a partir da versão 12.0. - Por padrão, o TLSv1.3 está habilitado no dispositivo. - A cifra "TLS_AES_256_GCM_SHA384" é adicionada à lista de cifras predefinida.	- O Cisco AsyncOS versão 12.0 fornece o Web Security Appliance com alto desempenho (HP) para as plataformas S680, S690 e S695. - Um novo subcomando **highperformance** é adicionado sob o comando principal **advancedproxyconfig** para ativar e desativar o modo de alto desempenho. - Integração do SWA com o portal Cisco Threat Response (CTR). - O dispositivo oferece suporte à versão TLSv1.3. O recurso de backup do arquivo de configuração é movido do submenu "**Log Subscriptions**" para "**Configuration File**" em **System Administration**. - O dispositivo agora suporta o carregamento do certificado **ECDSA** para o **proxy HTTPS**. Um novo subcomando diagnostic **CLI** proxyscannermap é adicionado em **diagnostic** > **proxy**. Tto exibe o mapeamento **PID** entre cada proxy e o processo de scanner correspondente. A nova opção **searchdetails** é adicionada sob o comando **CLI authcache**. - Novo subcomando **CTROBSERVABLE** é adicionado sob o comando **CLI reportingconfig** para habilitar ou desabilitar

			a indexação baseada em **CTR** observável.
12.0.1-334	GD		- Novos scanners de subcomando são adicionados sob o comando principal **advancedproxyconfig** para excluir os tipos MIME a serem verificados pelo mecanismo **AMP**.
12.0.2-004	MD	- Use TLS 1.2 ou versões posteriores para conectar o dispositivo ao servidor AMP File Reputation. - AMÉRICAS (Legado) cloud-sa.amp.sourcefire.com não pode ser configurado no dispositivo.	- Uma nova opção "Enter the number of concurrent scans to be supported by AMP" é adicionada no **comando** principal da **CLI** advanced proxyconfig > scanners > AMP. você pode alterar o veredito não verificável padrão da remoção de verificação de longa execução para Tempo limite e vice-versa da **remoção** de novo subcomando CLI no comando principal **CLI** advancedproxyconfig > scanners.
12.02-012	MD		- As mensagens de alerta são acionadas na interface de usuário da Web do equipamento quando o proxy **Malloc Memory** ultrapassa 90% do limite de proxy de Malloc Memory e uma notificação por e-mail é enviada a todos os "destinatários de alerta" configurados para receber alertas críticos do "Web Proxy". - A nova interface da Web oferece uma nova aparência para relatórios de **monitoramento** e serviços da Web de **rastreamento**.
12.0.3-005	MD		
12.0.3-007	MD		Notificação de atualização de novas categorias de **URL**
12.0.4-002	MD		
12.0.5-011	MD	- O TLSv1.2 é habilitado por padrão para a interface de usuário da Web de gerenciamento de dispositivo - **Reinício de sessão** está desabilitado por padrão.	- Uma mensagem é adicionada para indicar o fim do suporte ao CDA na seção de configuração do CDA.

12.5.1-011	LD	- Por padrão, o recurso Cisco Success Network está habilitado no dispositivo. - Esses registros são modificados para incluir mais detalhes: Os logs de acesso agora exibem o nome do usuário quando a autenticação falhar. Os logs da estrutura de autenticação agora exibem o endereço IP do cliente para estes protocolos de autenticação com falha: NTLM, BASIC, SSO (Transparent)	- O Cisco AsyncOS versão 12.5 fornece o Web Security Appliance com alto desempenho (HP) para as plataformas S680, S690 e S695. Isso aumenta o desempenho do tráfego dos dispositivos high-end atuais. - Agora você pode atualizar para a versão 12.5 e aproveitar o modo de alto desempenho nos modelos (S680, S690, S695, S680F, S690F e S695F), mesmo que você tenha habilitado estes recursos em seu dispositivo: • Toque no tráfego da Web • Cotas de volume e tempo • Limites de largura de banda gerais - Agora você pode configurar o Spoofing de IP do Web Proxy criando um perfil de spoofing de IP e adicionando-o às políticas de roteamento. - Agora você pode criar uma categoria de URL personalizada para o YouTube e definir políticas na categoria personalizada do YouTube para controle de acesso seguro. - Na nova interface da Web, o equipamento tem uma nova página (Monitoramento > Status do sistema) para exibir o status atual e a configuração do equipamento. - O recurso Cisco Success Network (CSN) permite que a Cisco colete telemetria de informações de uso de recursos do dispositivo. - API REST para rede, inscrição de log e outras configurações.
12.5.1-035	GD	- Substituição do TLS 1.0/1.1 : Use TLS 1.2 ou versões posteriores para conectar o dispositivo ao servidor do AMP File Reputation. AMERICAS (Legacy) **cloud-sa.amp.sourcefire.com** é removido da lista de servidores do AMP File Reputation, portanto AMERICAS (Legacy) **cloud-sa.amp.sourcefire.com** não pode ser configurado no dispositivo.	- A configuração do tamanho do cache para autenticação (Rede > Autenticação > Configurações de Autenticação > Opções de Cache de Credencial) não é suportada no AsyncOS 12.5.1-035 e versões posteriores.

12.5.1-043	GD		- As mensagens de alerta são exibidas na interface de usuário da Web do equipamento (Administração do sistema > Alertas > Exibir alertas principais): • quando a memória de malloc do proxy ultrapassar 90% do limite de memória de malloc do proxy • quando o proxy é reiniciado em 100% da memória malloc Em ambos os casos, uma notificação por e-mail é enviada a todos os "Destinatários de alertas" configurados para receber alertas críticos do "Web Proxy".
12.5.2-007	MD		- Uma nova notificação de atualização de categorias de URL é apresentada no banner. Uma notificação por e-mail sobre as próximas atualizações de categoria de URL também é enviada aos usuários.
12.5.2-011	MD		
12.5.3-002	MD		
12.5.4-005	MD	- Na versão 12.5.4 do Cisco AsyncOS, o TLSv1.2 é habilitado por padrão para a interface de usuário da Web de gerenciamento de dispositivos. - Após uma atualização para a versão 12.5.4 do Cisco AsyncOS, a retomada da sessão é desabilitada por padrão. - A mensagem é adicionada para indicar o fim do suporte ao CDA na seção de configuração do CDA	
12.5.4-011	Atualização MD		
12.5.5-004	MD		- Após uma atualização para o Cisco AsyncOS 12.5, você recebe um prompt para reiniciar o processo de proxy ao executar o

			comando **networktuning** pela primeira vez.
12.5.5-008	Atualização MD		
14.0.1-014	LD	- Por padrão, o recurso HTTP 2.0 está desabilitado. Para habilitar este recurso, use o comando <HTTP2>. - O AsyncOS 14.0 para o Cisco Web Security Appliance oferece suporte à retomada de sessão TLSv1.3 no cliente e no servidor. - Os períodos de validade destes certificados são alterados: • HTTPS • ISE • SAAS • Certificados do equipamento • Certificado de demonstração/gerenciamento - A CLI e a GUI do dispositivo agora exibem uma mensagem quando uma atualização falha devido a nome de log e nome de arquivo inválidos nas inscrições de log. - Por padrão, o intervalo de pesquisa é definido como 24 horas. - Depois de atualizar para esta versão, você não poderá executar o Teste inicial para autenticação LDAP se o campo DN base (Nome distinto base) (Rede > Autenticação > Adicionar território) estiver vazio.	- O Cisco Web Security Appliance agora suporta integração com o Cisco SecureX. - Você pode configurar perfis de cabeçalho personalizados para solicitações HTTP e pode criar vários cabeçalhos em um perfil de regravação de cabeçalho. - Agora você pode configurar o esquema de Autenticação Baseada em Cabeçalho para um diretório ativo. O cliente e o Web Security Appliance consideram o usuário como autenticado e não solicitam novamente a autenticação ou credenciais de usuário. O recurso X-Authenticated funciona quando o Web Security Appliance atua como um dispositivo upstream. - O Painel de status do sistema do equipamento foi aprimorado: • Guia Capacidadeâ€”Um que fornece detalhes sobre Intervalo de tempo, Uso de memória e CPU do sistema, Largura de banda e RPS, Uso de CPU por função e Conexões cliente ou servidor. • As Características de Tráfego de Proxy na guia Status fornecem detalhes das conexões de cliente e servidor. • O Tempo de Resposta do Serviço agora inclui mais detalhes em gráficos de barras e também dados de legenda para datas anteriores. - Agora você pode recuperar informações de configuração e executar alterações (como modificar informações atuais, adicionar novas informações ou excluir uma entrada) nos dados de configuração do dispositivo usar APIs REST para políticas de gerenciamento, políticas de acesso e políticas de desvio - A versão 14.0 do Cisco AsyncOS suporta

			HTTP 2.0 para solicitação e resposta da Web sobre TLS. O suporte a HTTP 2.0 requer a negociação baseada em TLS ALPN, que está disponível somente a partir da versão TLS 1.2. Nesta versão, o HTTPS 2.0 não é suportado para estes recursos: • Toque no tráfego da Web • DLP externo • Largura de banda geral e largura de banda do aplicativo - Um novo comando CLI <HTTP2> é introduzido para habilitar ou desabilitar configurações HTTP 2.0. Você não pode habilitar ou desabilitar o HTTP 2.0 e restringir o domínio para HTTP 2.0 através da interface de usuário da Web do equipamento. - A configuração do HTTP 2.0 não é suportada pelo Cisco Secure Email e Web Manage - O CLI exibe a nova mensagem de aviso quando você tenta usar o certificado padrão de qualquer um destes recursos: • Certificado do equipamento (Na interface de usuário da Web, navegue para Rede > Gerenciamento de certificado > Certificado do equipamento) • Certificado de Criptografia de Credencial (na interface de usuário da Web, navegue para Rede > Autenticação > Editar Configurações > seção Avançado) • Certificado de IU de gerenciamento HTTPS (na interface de linha de comando, use certconfig > SETUP) - Um novo subcomando OCSPVALIDATION_FOR_SERVER_CERT é adicionado em **certconfig**. Com esse novo subcomando, você pode habilitar a validação OCSP para certificados de servidor LDAP e Atualizador. Se a validação do certificado estiver ativada, você poderá receber um alerta se os certificados envolvidos na comunicação forem revogados. - Um novo comando CLI **gathererdconfig** é

			adicionado para configurar a funcionalidade de pesquisa entre o dispositivo e o servidor de autenticação. - Agora você pode escolher entre Gerenciamento e Interface de Dados, enquanto configura o recurso de licença inteligente no dispositivo.
14.0.1-040	LD	- Quando você habilita o licenciamento de software inteligente e registra seu Web Security Appliance com o Cisco Smart Software Manager, o Cisco Cloud Services (Network > Cloud Service Settings) habilita e registra automaticamente seu Secure Web Appliance por meio do portal Cisco Cloud Services. - Você não pode desativar ou cancelar o registro do Cisco Cloud Service se o Smart Licensing estiver registrado no seu dispositivo. - Se você já registrou seus dispositivos no Cisco Smart Software Manager e não configurou o Cisco Cloud Services, o Cisco Cloud Services será ativado automaticamente após a atualização para o AsyncOS 14.0.1-040. Por padrão, a região está registrada como Américas e você pode modificar a região (Europa e APJC) conforme necessário. - Você não pode desativar ou cancelar o registro do Cisco Cloud Service se a licença inteligente estiver registrada em seu dispositivo.	- Você pode visualizar os detalhes da Smart Account criada no portal do Cisco Smart Software Manager a partir do comando **smartaccountinfo** na CLI. - Se o certificado do Cisco Cloud Services expirou ou está prestes a expirar, o Cisco Cloud Service renova automaticamente o certificado após a atualização para o AsyncOS 14.0.1-040. - Se o certificado do Cisco Cloud Services tiver expirado, você poderá fazer o download de um novo certificado do portal do Cisco Talos Intelligence Services no subcomando **cloudserviceconfig** > **fetchcertificate** na CLI. - Você pode registrar automaticamente o Web Security Appliance no portal do Cisco Cloud Service (subcomando **cloudserviceconfig** > **autoregister** na CLI) Você pode carregar o certificado para dispositivos virtuais e de hardware a partir do subcomando **updateconfig** > **clientcertificate** na CLI. - Uma nova notificação de atualização de categorias de URL é apresentada no banner. Uma notificação por e-mail também é enviada aos usuários sobre as próximas atualizações de categoria de URL.
14.0.1-053	GD		
14.0.1-503	HP		
14.0.2-012	MD	- Na versão Cisco AsyncOS 14.0.2, o TLSv1.2 é habilitado por padrão	- Uma mensagem é adicionada para indicar o fim do suporte ao CDA na seção de

		para a interface de usuário da Web de gerenciamento de dispositivos em Administrador do sistema > Configuração SSL. - A retomada da sessão é desativada por padrão.	configuração do CDA. - Agora você pode escolher entre a interface de dados ou de gerenciamento para o Smart License Registration na lista suspensa Test Interface (Interface de teste).
14.0.3-014	MD	- Após uma atualização para o Cisco AsyncOS 14.0, você recebe um prompt para reiniciar o processo de proxy ao executar o comando **networktuning** pela primeira vez.	
14.0.3-502	HP	- Quando o Secure Web Appliance opera no modo de alto desempenho, o esgotamento do limite de heap desativa a alta latência e aceita manipuladores. Isso resulta em um número menor de conexões.	
14.0.4-005	MD		
14.5.0-498	LD	- Nova marca de produto: • A AMP para endpoints, a proteção avançada contra malware e a AMP foram alteradas para **Endpoint seguro** • Thread Grid (Análise de arquivo) alterado para **Malware Analytics** - A solicitação de erro de classificação é enviada por HTTPS e, portanto, você não recebe notificações de alerta de segurança. - A versão Samba foi atualizada para a versão 4.11.15. - O TLSv1.2 é ativado por padrão para a interface de usuário da Web Gerenciamento de dispositivo em Administrador do sistema > Configuração SSL . - Em uma nova instalação do AsyncOS 14.5, o valor de	- O Secure Web Appliance agora pode validar a resposta DNS recebida do servidor DNS que suporta assinaturas criptográficas. - O Secure Web Appliance restringe o número de conexões simultâneas iniciadas pelo cliente a um valor configurado. - Com o AsyncOS versão 14.5, o Cisco Web Security Appliance foi renomeado para Cisco Secure Web Appliance - A marca de decisão accesslog no grupo Decrypt Policy é anexada com EUN (End user Notification, Notificação de usuário final) quando a página EUN aparece no navegador do cliente. - O recurso de política de clonagem permite copiar ou clonar as configurações de uma política e criar uma nova política. - Você pode gerenciar a largura de banda de tráfego configurando o valor da largura de banda no perfil de cota e mapeando o perfil de cota na categoria de URL da política de acesso ou na cota de atividade geral da Web.

		configurações de certificado de nome de host expirado e incompatível na página Proxy HTTPS é selecionado por padrão como **Drop** em vez de **Monitor**.	- API REST para configurar políticas de gerenciamento, políticas de descriptografia, políticas de roteamento, políticas de falsificação de IP, antimalware e reputação, domínios de autenticação, Cisco Smart Software License, Cisco Umbrella Seamless ID, serviços de identidade e configuração do sistema. - Você pode integrar a implantação do ISE-SXP com o Cisco Secure Web Appliance para autenticação passiva. Isso permite que você obtenha todos os mapeamentos definidos, incluindo mapeamentos de endereço SGT para IP que são publicados por meio do SXP. - O recurso Cisco Umbrella Seamless ID permite que o dispositivo passe as informações de identificação do usuário para o Cisco Umbrella Secure Web Gateway (SWG) após a autenticação bem-sucedida. - Uma mensagem é adicionada para indicar o fim do suporte ao CDA na seção de configuração do CDA. - Agora você pode escolher entre a interface de dados ou de gerenciamento para o Smart License Registration na lista suspensa Test Interface (Interface de teste). - Após uma atualização para o Cisco AsyncOS 14.5, você receberá um prompt para reiniciar o processo de proxy quando executar o comando **networktuning** pela primeira vez.
14.5.0-537	GD		- Essas políticas com opção de clonagem no Secure Web Appliance também podem ser gerenciadas pelo Cisco Secure Email e Web Manager (SMA): • Política de acesso • Perfil de identificação • Política de descriptografia • Política de roteamento
14.5.1-008	MD		
14.5.1-016	MD		

14.6.0-108	LD		- O AsyncOS 14.6 oferece suporte ao Cisco Umbrella com Cisco Secure Web Appliance (SWA). A integração do Umbrella e do Secure Web Appliance facilita a implantação de políticas comuns da Web do Umbrella para o Secure Web Appliance.
15.0.0-322	LD	- A versão do FreeBSD foi atualizada para o FreeBSD 13.0. - Cisco SSL versão 1.0.2 para Cisco SSL versão 1.1.1. - Os mecanismos Talos, como AVC, WBRSD, DCA e Beaker, foram atualizados. - Mecanismos de varredura, como Webroot e McAfee, foram atualizados.	- Estes aprimoramentos foram feitos no recurso Smart Software Licensing: • Reserva de licença • Conversão conduzida por dispositivoâ€”Depois de registrar o Secure Web Appliance com a smart license, todas as licenças clássicas válidas atuais são automaticamente convertidas em licenças inteligentes com o processo de Conversão conduzida por dispositivo (DLC). Essas licenças convertidas são atualizadas na conta virtual do portal CSSM. - Você pode gerenciar a largura de banda de tráfego configurando o valor da largura de banda no perfil de cota e mapear o perfil de cota na política de descriptografia e na política de acesso, na categoria de URL ou na cota geral de atividade da Web. - O recurso de política de clonagem permite copiar ou clonar as configurações de uma política e criar uma nova política. - Mecanismo de detecção e controle de aplicativos (ADC): um componente de política de uso aceitável que inspeciona o tráfego da web para obter compreensão e controle mais profundos do tráfego da web usado para aplicativos. Com o AsyncOS 15.0, você pode usar o mecanismo AVC ou ADC para monitorar o tráfego da Web. Por padrão, o AVC está habilitado. O mecanismo ADC suporta o modo de alto desempenho. - API REST para configuração ADC - O administrador pode optar por configurar um nome de usuário SNMPv3 personalizado diferente do nome de usuário padrão v3get.

			- O comprimento máximo do cabeçalho personalizado é 16k. - Opção de escolher a interface do túnel seguro e a conexão de acesso remoto.

Componentes de Código Aberto

Aqui está a lista de alterações no componente de código aberto usado no SWA:

Versão	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

Informações Relacionadas

- Notas de versão do AsyncOS 12.0 para Cisco Web Security Appliances - Cisco
- Notas de versão do AsyncOS 12.5 para Cisco Web Security Appliances - Cisco
- Notas de versão do AsyncOS 14.0 para Cisco Web Security Appliances - Cisco
- Notas de versão do AsyncOS 14.5 para Cisco Secure Web Appliance - Cisco
- Qual é a terminologia da versão para segurança de conteúdo? (cisco.com)
- Guia de instalação do Cisco Secure Email and Web Virtual Appliance
- **Suporte Técnico e Documentação - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.