Modifiche alla release di Secure Web Appliance

Sommario

Introduzione

In questo documento vengono descritte le principali modifiche e le funzionalità aggiunte nelle diverse versioni di Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Nessun requisito speciale previsto per questo articolo.

Le abbreviazioni utilizzate in questi articoli sono:

LD: Implementazione limitata.

GD: Distribuzione generale.

MD: Installazione manutenzione

ED: Installazione rapida.

HP: Hot Patch.

CLI: Command Line Interface.

GUI: interfaccia utente grafica

HTTP: protocollo di trasferimento ipertestuale.

HTTPS: protocollo di trasferimento ipertestuale protetto.

ECDSA: algoritmo di firma digitale a curva ellittica.

PID: Identificativo processo.

CTR: Cisco Threat Response.

AMP: Advanced Malware Protection

URL: Uniform Resource Locator.

CDA: agente directory contesto.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Cronologia modifiche per release

Version	Tipo	Cambiamenti di comportamento	Miglioramenti / Caratteristiche aggiunte
12.0.1-268	LD	- I requisiti della CPU e della memoria del sistema sono stati modificati a partire dalla versione 12.0. - per impostazione predefinita, TLSv1.3 è attivato sull'accessorio. - Il cifrario "TLS_AES_256_GCM_SHA384" viene aggiunto all'elenco dei cifrari di default.	- Cisco AsyncOS versione 12.0 fornisce Web Security Appliance con High Performance (HP) per le piattaforme S680, S690 e S695. - Per abilitare e disabilitare la modalità a **prestazioni elevate,** viene aggiunto un nuovo sottocomando **high performance** con il comando **advancedproxyconfig** principale. - Integrazione dell'SWA con il portale Cisco Threat Response (CTR). - L'accessorio supporta TLSv1.3. - La funzione di backup del file di configurazione viene spostata dal sottomenu "**Log Subscriptions**" (Sottoscrizioni registro) al **file di configurazione** (**file di configurazione**) in **System Administration (Amministrazione sistema)**. - L'accessorio supporta ora il caricamento del certificato **ECDSA** per il proxy **HTTPS**. - Un nuovo sottocomando **proxyscannermap della CLI di** diagnostica è stato aggiunto in **diagnostica** > **proxy**. Tto visualizza la mappatura dei **PID** tra ciascun proxy e il processo dello scanner corrispondente. - La nuova opzione **searchdetails** viene aggiunta con il comando **CLI** di **authcache**. - Il nuovo sottocomando **CTROBSERVABLE** viene aggiunto con il comando **CLI** reportingconfig per abilitare o

			disabilitare l'indicizzazione basata sull'osservazione **CTR**.
12.0.1-334	GD		- Sotto il comando **advancedproxyconfig** principale viene aggiunto un nuovo sottocomando scanner per escludere i tipi MIME che devono essere scansionati dal motore **AMP**.
12.0.2-004	MD	- Utilizzare TLS 1.2 o versioni successive per collegare l'accessorio al server AMP File Reputation. - Impossibile configurare AMERICAS (Legacy) cloud-sa.amp.sourcefire.com sull'accessorio.	- Nel comando **advancedproxyconfig** > **scanners** > AMP viene aggiunta la nuova opzione "Immettere il numero di scansioni simultanee supportate da AMP" > **AMP**. è possibile modificare il verdetto predefinito Non scansionabile di eliminazione di analisi a esecuzione prolungata in Timeout e viceversa da nuova **eliminazione di** sottocomandi CLI nel comando **CLI** principale **advancedproxyconfig** > **scanner**.
12.02-012	MD		- I messaggi di avviso vengono attivati sull'interfaccia utente Web dell'accessorio quando la **memoria malloc** del proxy supera il 90% del limite di memoria malloc del proxy e viene inviata una notifica e-mail a tutti i 'destinatari avviso' configurati per la ricezione di avvisi critici 'Proxy Web'. - La nuova interfaccia Web offre un nuovo aspetto per i report di **monitoraggio** e la **tracciabilità** dei servizi Web.
12.0.3-005	MD		
12.0.3-007	MD		- Notifica di aggiornamento di nuove categorie di **URL**
12.0.4-002	MD		
12.0.5-011	MD	- TLSv1.2 è abilitato per impostazione predefinita per l'interfaccia utente Web di Gestione accessorio	- Viene aggiunto un messaggio per indicare la fine del supporto per CDA nella sezione di configurazione CDA.

		- **Ripresa della sessione** disabilitata per impostazione predefinita.	
12.5.1-011	LD	- per impostazione predefinita, sull'accessorio è attivata la funzione Cisco Success Network (Rete Cisco riuscita). - Questi log vengono modificati per includere maggiori dettagli: Quando l'autenticazione non riesce, nei log degli accessi viene visualizzato il nome utente. Nei log del framework di autenticazione viene ora visualizzato l'indirizzo IP del client per i seguenti protocolli di autenticazione non riusciti: NTLM, BASIC, SSO (trasparente)	- Cisco AsyncOS versione 12.5 fornisce Web Security Appliance con High Performance (HP) per le piattaforme S680, S690 e S695. In questo modo si migliorano le prestazioni del traffico degli attuali dispositivi di fascia alta. - È ora possibile eseguire l'aggiornamento alla versione 12.5 e utilizzare la modalità ad alte prestazioni sui modelli (S680, S690, S695, S680F, S690F e S695F), anche se sono state abilitate queste funzioni sull'accessorio: • Traffic Tap Web • Volume e quote temporali • Limiti generali larghezza di banda - È ora possibile configurare lo spoofing IP dei proxy Web creando un profilo di spoofing IP e aggiungendolo ai criteri di routing. - A questo punto è possibile creare una categoria URL personalizzata per YouTube e impostare i criteri nella categoria personalizzata di YouTube per un controllo dell'accesso sicuro. - Nella nuova interfaccia Web, l'accessorio presenta una nuova pagina (Monitoraggio > Stato del sistema) in cui è possibile visualizzare lo stato e la configurazione correnti dell'accessorio. - La funzionalità Cisco Success Network (CSN) consente a Cisco di raccogliere dati telemetrici sull'utilizzo delle funzionalità dell'accessorio. - API REST per rete, sottoscrizione log e altre configurazioni.
12.5.1-035	GD	- Deprecazione di TLS 1.0/1.1 : Utilizzare TLS 1.2 o versioni successive per collegare l'accessorio al server AMP File Reputation. AMERICAS (Legacy) **cloud-sa.amp.sourcefire.com**	- La configurazione delle dimensioni della cache per l'autenticazione (Rete > Autenticazione > Impostazioni di autenticazione > Opzioni cache credenziali) non è supportata da AsyncOS 12.5.1-035 e versioni successive.

		viene rimosso dall'elenco dei server AMP File Reputation, pertanto **cloud-sa.amp.sourcefire.com** (Legacy) non può essere configurato sull'accessorio.	
12.5.1-043	GD		- I messaggi di avviso vengono visualizzati nell'interfaccia utente Web dell'accessorio (Amministrazione sistema > Avvisi > Visualizza primi avvisi): • quando la memoria malloc del proxy supera il 90% del limite di memoria malloc del proxy • quando il proxy viene riavviato sul 100% della memoria malloc In entrambi i casi viene inviata una notifica tramite posta elettronica a tutti i destinatari degli avvisi configurati per la ricezione degli avvisi critici del proxy Web.
12.5.2-007	MD		- Nel banner viene introdotta una nuova notifica di aggiornamento delle categorie di URL. Agli utenti viene inoltre inviata una notifica e-mail con i prossimi aggiornamenti della categoria URL.
12.5.2-011	MD		
12.5.3-002	MD		
12.5.4-005	MD	- Dalla versione Cisco AsyncOS 12.5.4, TLSv1.2 è abilitato per impostazione predefinita per l'interfaccia utente Web di gestione degli accessori. - Dopo un aggiornamento a Cisco AsyncOS versione 12.5.4, la ripresa della sessione è disabilitata per impostazione predefinita. - Viene aggiunto un messaggio per indicare la fine del supporto per CDA nella sezione di	

		configurazione CDA	
12.5.4-011	Aggiornamento MD		
12.5.5-004	MD		- Dopo un aggiornamento a Cisco AsyncOS 12.5, viene visualizzato un messaggio in cui si chiede di riavviare il processo proxy quando si esegue per la prima volta il comando **networktuning**.
12.5.5-008	Aggiornamento MD		
12.5.6-008	MD		
14.0.1-014	LD	- Per impostazione predefinita, la funzione HTTP 2.0 è disattivata. Per abilitare questa funzionalità, utilizzare il comando <HTTP2>. - AsyncOS 14.0 for Cisco Web Security Appliance supporta la ripresa della sessione TLSv1.3 nel client e nel server. - I periodi di validità dei certificati sono modificati: • HTTPS • ISE • SAAS • Certificati accessorio • Certificato demo/gestione - La CLI e la GUI dell'accessorio visualizzano ora un messaggio quando un aggiornamento non riesce a causa di un nome di registro e di file non validi nelle sottoscrizioni dei registri. - Per impostazione predefinita, l'intervallo di polling è impostato su 24 ore. - Dopo l'aggiornamento a questa release, non è possibile eseguire il test di avvio per l'autenticazione	- Cisco Web Security Appliance supporta ora l'integrazione con Cisco SecureX. - È possibile configurare profili di intestazione personalizzati per le richieste HTTP e creare più intestazioni in un profilo di riscrittura dell'intestazione. - È ora possibile configurare lo schema di autenticazione basata su intestazione per una directory attiva. Il client e Web Security Appliance considerano l'utente autenticato e non richiedono nuovamente l'autenticazione o le credenziali utente. La funzionalità X-Authenticated funziona quando Web Security Appliance funge da dispositivo a monte. - Il Dashboard dello stato del sistema dell'accessorio è stato migliorato: • Scheda Capacità - Consente di visualizzare i dettagli relativi all'intervallo di tempo, all'utilizzo della CPU e della memoria del sistema, alla larghezza di banda e a RPS, all'utilizzo della CPU per funzione e alle connessioni client o server. • Le caratteristiche del traffico proxy nella scheda Stato forniscono dettagli sulle connessioni client e server.

		LDAP se il campo DN di base (Nome distinto di base) (Rete > Autenticazione > Aggiungi realm) è vuoto.	• Il Tempo di risposta del servizio include ora ulteriori dettagli sui grafici a barre e i dati delle legende per le date precedenti. - È ora possibile recuperare le informazioni di configurazione ed eseguire modifiche (ad esempio, modificare le informazioni correnti, aggiungere nuove informazioni o eliminare una voce) nei dati di configurazione dell'accessorio. Utilizzare le API REST per i criteri di gestione, i criteri di accesso e i criteri di bypass. - Cisco AsyncOS versione 14.0 supporta HTTP 2.0 per la richiesta e la risposta Web su TLS. Il supporto HTTP 2.0 richiede una negoziazione basata su ALPN TLS che è disponibile solo dalla versione TLS 1.2 in poi. In questa release, HTTPS 2.0 non è supportato per queste funzionalità: • Traffic Tap Web • DLP esterno • Larghezza di banda complessiva e larghezza di banda dell'applicazione - Viene introdotto un nuovo comando CLI <HTTP2> per abilitare o disabilitare le configurazioni HTTP 2.0. Non è possibile attivare o disattivare HTTP 2.0 e limitare il dominio per HTTP 2.0 tramite l'interfaccia utente Web dell'accessorio. - La configurazione di HTTP 2.0 non è supportata tramite Cisco Secure Email e Web Manager - La CLI visualizza il nuovo messaggio di avviso quando si cerca di utilizzare il certificato predefinito di una delle seguenti funzionalità: • Certificato accessorio (nell'interfaccia utente Web, selezionare Rete > Gestione certificati > Certificato accessorio) • Certificato di crittografia delle credenziali (nell'interfaccia utente Web, selezionare Rete > Autenticazione > Modifica impostazioni > Sezione Avanzate) • Certificato interfaccia utente gestione HTTPS (nell'interfaccia della riga di

			comando, utilizzare certconfig > SETUP) - Sotto il comando **certconfig** viene aggiunto un nuovo sottocomando OCSPVALIDATION_FOR_SERVER_CERT. Con questo nuovo sottocomando è possibile abilitare la convalida OCSP per i certificati server LDAP e Updater. Se la convalida del certificato è attivata, è possibile ricevere un avviso se i certificati coinvolti nella comunicazione vengono revocati. - Viene aggiunto un nuovo comando **gatherdconfig** della CLI per configurare la funzionalità di polling tra l'accessorio e il server di autenticazione. - È ora possibile scegliere tra la gestione e l'interfaccia dati, mentre si configura la funzione di licenza intelligente sull'accessorio.
14.0.1-040	LD	- Quando si abilita la licenza software intelligente e si registra Web Security Appliance con Cisco Smart Software Manager, i servizi cloud Cisco (Rete > Impostazioni servizio cloud) abilita e registra automaticamente Secure Web Appliance tramite il portale dei servizi cloud Cisco. - Non è possibile disabilitare o annullare la registrazione di Cisco Cloud Service se sul dispositivo è stata registrata una licenza Smart. - Se gli accessori sono già stati registrati in Cisco Smart Software Manager e non sono stati configurati i servizi cloud Cisco, i servizi cloud Cisco vengono automaticamente abilitati dopo l'aggiornamento ad AsyncOS 14.0.1-040. Per impostazione predefinita, l'area è registrata come Americhe ed è possibile modificarla (Europa e APJC) in base alle esigenze. - Non è possibile disabilitare o	- È possibile visualizzare i dettagli dello smart account creato nel portale Cisco Smart Software Manager usando il comando **smartaccountinfo** nella CLI. - Se il certificato dei servizi cloud Cisco è scaduto o sta per scadere, il servizio cloud Cisco rinnova automaticamente il certificato dopo l'aggiornamento a AsyncOS 14.0.1-040. - Se il certificato dei servizi cloud Cisco è scaduto, è ora possibile scaricare un nuovo certificato dal portale Cisco Talos Intelligence Services dal sottocomando **cloudserviceconfig** > **fetchcertificate** dalla CLI. - È possibile registrare automaticamente Web Security Appliance con il portale dei servizi Cisco Cloud (**cloudserviceconfig** > sottocomando **autoregister** nella CLI) - È possibile caricare il certificato per appliance virtuali e appliance hardware dal sottocomando **updateconfig** > **clientcertificate** dalla CLI. - Nel banner viene introdotta una nuova notifica di aggiornamento delle categorie di URL.

		annullare la registrazione di Cisco Cloud Service se la licenza intelligente è registrata sull'appliance.	Inoltre, viene inviata una notifica via e-mail agli utenti per informarli dei prossimi aggiornamenti della categoria dell'URL.
14.0.1-053	GD		
14.0.1-503	HP		
14.0.2-012	MD	- Nella versione Cisco AsyncOS 14.0.2, TLSv1.2 è abilitato per impostazione predefinita per l'interfaccia utente Web di gestione degli accessori in Amministratore di sistema > Configurazione SSL. - La ripresa della sessione è disabilitata per impostazione predefinita.	- Viene aggiunto un messaggio per indicare la fine del supporto per CDA nella sezione di configurazione CDA. - È ora possibile scegliere tra l'interfaccia di gestione o di dati per la registrazione di una licenza Smart dall'elenco a discesa Test Interface (Interfaccia di test).
14.0.3-014	MD	- Dopo un aggiornamento a Cisco AsyncOS 14.0, quando si esegue per la prima volta il comando **network tuning** viene visualizzato un messaggio in cui si chiede di riavviare il processo proxy.	
14.0.3-502	HP	- Quando Secure Web Appliance funziona in modalità a elevate prestazioni, l'esaurimento del limite di heap disabilita l'alta latenza e accetta gli handler. Il risultato è un numero inferiore di connessioni.	
14.0.4-005	MD		
14.5.0-498	LD	- Rebrand del prodotto: • AMP for Endpoints, Advanced Malware Protection e AMP sono stati modificati in **Endpoint sicuro**	- L'appliance Web sicura è ora in grado di convalidare la risposta DNS ricevuta dal server DNS per il supporto delle firme crittografiche. - L'appliance Web sicura limita a un valore configurato il numero di connessioni

		• Griglia thread (analisi file) modificata in **Analisi malware** - La richiesta di classificazione errata viene inviata tramite HTTPS e pertanto non si ricevono notifiche di avviso di protezione. - La versione Samba è stata aggiornata alla versione 4.11.15. - TLSv1.2 è abilitato per impostazione predefinita per l'interfaccia utente Web di Gestione accessorio in Amministratore di sistema > Configurazione SSL. - In una nuova installazione di AsyncOS 14.5, il valore delle configurazioni dei certificati Nome host scaduto e non corrispondente nella pagina Proxy HTTPS è selezionato per impostazione predefinita come **Drop** anziché come **Monitor**.	simultanee avviate dal client. - Con AsyncOS release 14.5, Cisco Web Security Appliance è stata rinominata in Cisco Secure Web Appliance - Il tag di decisione accesslog nel gruppo Decrypt Policy viene aggiunto a EUN (End User Notification) quando la pagina EUN viene visualizzata sul browser Web del client. - La funzione di duplicazione dei criteri consente di copiare o duplicare le configurazioni di un criterio e di creare un nuovo criterio. - È possibile gestire la larghezza di banda del traffico configurando il valore della larghezza di banda nel profilo della quota e mappando il profilo della quota nella categoria URL dei criteri di accesso o nella quota complessiva dell'attività Web. - API REST per configurare criteri di gestione, criteri di decrittografia, criteri di routing, criteri di spoofing IP, antimalware e reputazione, realm di autenticazione, licenza Cisco Smart Software, Cisco Umbrella Seamless ID, servizi di identità e configurazione del sistema. - È possibile integrare l'implementazione ISE-SXP con Cisco Secure Web Appliance per l'autenticazione passiva. In questo modo è possibile ottenere tutti i mapping definiti, inclusi i mapping di indirizzi da SGT a IP pubblicati tramite SXP. - La funzione Cisco Umbrella Seamless ID consente all'appliance di passare le informazioni di identificazione dell'utente a Cisco Umbrella Secure Web Gateway (SWG) dopo la corretta autenticazione. - Viene aggiunto un messaggio per indicare la fine del supporto per CDA nella sezione di configurazione CDA. - È ora possibile scegliere tra l'interfaccia di gestione o di dati per la registrazione di una licenza Smart dall'elenco a discesa Test Interface (Interfaccia di test). - Dopo un aggiornamento a Cisco AsyncOS

			14.5, viene visualizzato un messaggio in cui si chiede di riavviare il processo proxy quando si esegue per la prima volta il comando **network tuning**.
14.5.0-537	GD		- Questi criteri con opzione clone in Secure Web Appliance possono essere gestiti anche da Cisco Secure Email e Web Manager (SMA): • Criteri di accesso • Profilo di identificazione • Criterio di decrittografia • Criteri di routing
14.5.1-008	MD		
14.5.1-016	MD		
14.6.0-108	LD		- AsyncOS 14.6 supporta Cisco Umbrella con Cisco Secure Web Appliance (SWA). L'integrazione di Umbrella e Secure Web Appliance semplifica la distribuzione di criteri Web comuni da Umbrella a Secure Web Appliance.
15.0.0-322	LD	- FreeBSD versione aggiornata a FreeBSD 13.0. - da Cisco SSL versione 1.0.2 a Cisco SSL versione 1.1.1. - I motori Talos come AVC, WBRSD, DCA e Beaker sono stati aggiornati. - I motori scanner come Webroot e McAfee sono stati aggiornati.	- I seguenti miglioramenti apportati alla funzionalità Smart Software Licensing: • Prenotazione licenza • Conversione Led dispositivo: dopo la registrazione di Secure Web Appliance con una licenza Smart, tutte le licenze standard valide correnti vengono convertite automaticamente in licenze Smart con il processo di conversione Led dispositivo (DLC). Le licenze convertite vengono aggiornate nell'account virtuale del portale CSM. - È possibile gestire la larghezza di banda del traffico configurando il valore della larghezza di banda nel profilo della quota e mappando il profilo della quota nei criteri di decrittografia e di accesso, nella categoria URL o nella quota dell'attività Web complessiva. - La funzione di duplicazione dei criteri

			consente di copiare o duplicare le configurazioni di un criterio e di creare un nuovo criterio. - Motore Application Discovery and Control (ADC): componente di policy per l'utilizzo accettabile che controlla il traffico web per comprendere e controllare in modo più approfondito il traffico web utilizzato per le applicazioni. Con AsyncOS 15.0, è possibile utilizzare il motore AVC o ADC per monitorare il traffico Web. Per impostazione predefinita, AVC è attivato. Il motore ADC supporta la modalità ad alte prestazioni. - API REST per configurazione ADC - L'amministratore può scegliere di configurare un nome utente SNMPv3 personalizzato diverso dal nome utente predefinito v3get. - La lunghezza massima dell'intestazione personalizzata è 16k. - Opzione per scegliere l'interfaccia del tunnel sicuro e la connessione di accesso remoto.
15.0.0-335	GD	- Conversione Led dispositivo - Dopo aver registrato Secure Web Appliance con le licenze Smart, tutte le licenze standard valide correnti vengono automaticamente convertite in licenze Smart con il processo di conversione Led dispositivo (DLC). Le licenze convertite vengono aggiornate nell'account virtuale del portale CSM. - Per impostazione predefinita, AVC è attivato. - Da Cisco SSL versione 1.0.2 a Cisco SSL versione 1.1.1 - I motori Talos, quali AVC, WBRSD, DCA e Beaker sono stati aggiornati.	- Prenotazione licenze: è possibile riservare licenze per le funzionalità abilitate in Secure Web Appliance senza connettersi al portale Cisco Smart Software Manager (CSSM). Ciò risulta particolarmente vantaggioso per gli utenti che installano Secure Web Appliance in un ambiente di rete altamente protetto senza alcuna comunicazione con Internet o dispositivi esterni. - È possibile gestire la larghezza di banda del traffico configurando il valore della larghezza di banda nel profilo della quota e mappando il profilo della quota nel criterio di decrittografia e nella categoria URL del criterio di accesso o nella quota dell'attività Web complessiva. - La funzione di duplicazione dei criteri consente di copiare o duplicare le configurazioni di un criterio e di creare un nuovo criterio.

		- I motori di scansione come Webroot e McAfee sono stati aggiornati. - FreeBSD 13.0 è compatibile solo con Cisco SSL versione 1.1.1. Per la connettività SSH a FreeBSD 13.0, possono essere supportati solo algoritmi cifratura, mac e kex compatibili con Cisco SSH. - La funzione DCA in Secure Web Appliance è disabilitata in AsyncOS15.0 GD release.È possibile abilitarla dopo l'aggiornamento a questa versione passando a Security Services>Acceptable Use Controls e selezionando la casella di controllo **DCA**. - Le operazioni SNMPWALK/SNMPGET per gli OID SNMP per la memoria Malloc dei proxy non sono supportate negli SWA multi-prox (S690, S695, S1000V).	- Supporta il motore ADC (Application Discovery and Control), un componente delle regole sull'utilizzo accettabile che controlla il traffico Web per ottenere una comprensione e un controllo più approfonditi del traffico Web utilizzato per le applicazioni. è ora possibile utilizzare il motore AVC o ADC per monitorare il traffico Web. - Il motore ADC supporta la modalità ad alte prestazioni. - È ora possibile recuperare le informazioni di configurazione ed eseguire le modifiche (ad esempio, modificare le informazioni correnti, aggiungere nuove informazioni o eliminare una voce) nei dati di configurazione dei criteri di accesso dell'accessorio con le API REST. -Al'amministratore può scegliere di configurare un nome utente SNMPv3 personalizzato diverso dal nome utente predefinito **v3get**. - La lunghezza massima delle intestazioni personalizzate per le richieste Web è 16k. - Opzione per scegliere l'interfaccia del tunnel sicuro e la connessione di accesso remoto

Apri componenti di origine

Di seguito è riportato l'elenco delle modifiche apportate al componente open source utilizzato nell'SWA:

Version	11,8 X	12,0,X	12,5 X	14,0,X	14,5 X	14,6 X	15,0,X
libere	10.4	10.4	10.4	11.2	11.2	11.2	13.0

Informazioni correlate

- Note sulla versione di AsyncOS 12.0 per Cisco Web Security Appliance - Cisco
- Note sulla versione di AsyncOS 12.5 per Cisco Web Security Appliance - Cisco
- Note sulla versione di AsyncOS 14.0 per Cisco Web Security Appliance - Cisco
- Note sulla versione di AsyncOS 14.5 per Cisco Secure Web Appliance - Cisco
- Qual è la terminologia della release per la sicurezza dei contenuti? (cisco.com)
- Guida all'installazione di Cisco Secure Email e Web Virtual Appliance
- **Documentazione e supporto tecnico â€“ Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).