Zugreifen auf Protokolle der sicheren Web-Appliance

Inhalt

Einleitung

In diesem Dokument werden die Methoden zum Anzeigen von SWA-Protokollen (Secure Web Appliance) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Installierte physische oder virtuelle SWA.
- Lizenz aktiviert oder installiert.
- Secure Shell (SSH)-Client.
- Der Setup-Assistent ist abgeschlossen.

- Administratorzugriff auf die SWA.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

SWA-Protokolltypen

Die sichere Web-Appliance zeichnet ihre eigenen System- und Datenverkehrsmanagementaktivitäten auf, indem sie sie in Protokolldateien schreibt. Administratoren können diese Protokolldateien zur Überwachung und Fehlerbehebung der Appliance einsehen.

In dieser Tabelle werden die Protokolldateitypen der sicheren Web-Appliance beschrieben.

Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäß aktiviert?
Protokolle der Zugriffssteuerungs-Engine	Zeichnet Nachrichten im Zusammenhang mit dem Evaluierungsmodul für die Webproxy-ACL (Zugriffssteuerungsliste) auf.	Nein	Nein
Sichere EndpointEngine-Protokolle	Aufzeichnung von Informationen über Dateireputations-Scans und Dateianalysen (Secure Endpoint)	Ja	Ja
Überwachungsprotokolle	Zeichnet AAA-Ereignisse (Authentifizierung, Autorisierung und Abrechnung) auf. Zeichnet alle Benutzerinteraktionen mit der Anwendung und den Befehlszeilenschnittstellen auf und erfasst bestätigte Änderungen. Im Prüfprotokoll finden sich u. a. folgende Details: • Benutzer - Anmeldung • Benutzer - Anmeldung fehlgeschlagen, falsches Kennwort • Benutzer - Anmeldung fehlgeschlagen, unbekannter Benutzername • Benutzer - Anmeldung fehlgeschlagen Konto abgelaufen • Benutzer - Abmelden • Benutzer - Sperre	Ja	Ja

Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäß aktiviert?
	• Benutzer - Aktiviert • Benutzer - Kennwortänderung • Benutzer - Kennwortzurücksetzung • Benutzer - Sicherheitseinstellungen/Profiländerung • Benutzer - Erstellt • Benutzer - Gelöscht/geändert • Gruppe/Rolle - Löschen/Ändern • Gruppe/Rolle - Berechtigungsänderung		
Zugriffsprotokolle	Protokolliert den Verlauf des Webproxy-Clients.	Ja	Ja
ADC-Modul-Framework-Protokolle	Zeichnet Nachrichten auf, die sich auf die Kommunikation zwischen dem Webproxy und dem ADC-Modul beziehen.	Nein	Nein
Protokolle des ADC-Moduls	Zeichnet Debug-Meldungen vom ADC-Modul auf.	Ja	Ja
Authentifizierungs-Framework-Protokolle	Zeichnet den Authentifizierungsverlauf und Nachrichten auf.	Nein	Ja
AVC Engine Framework-Protokolle	Zeichnet Nachrichten auf, die sich auf die Kommunikation zwischen dem Webproxy und dem AVC-Modul beziehen.	Nein	Nein
Protokolle des AVC-Moduls	Zeichnet Debug-Meldungen des AVC-Moduls auf.	Ja	Ja
CLI-Audit-Protokolle	Verlaufsüberwachung der	Ja	Ja

Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäß aktiviert?
	Befehlszeilenschnittstellenaktivität.		
Konfigurationsprotokolle	Zeichnet Nachrichten im Zusammenhang mit dem Webproxy-Konfigurationsmanagementsystem auf.	Nein	Nein
Verbindungsverwaltungsprotokolle	Zeichnet Nachrichten im Zusammenhang mit dem Webproxy-Verbindungsmanagementsystem auf.	Nein	Nein
Datensicherheits-Protokolle	Protokolliert den Client-Verlauf für Upload-Anforderungen, die von den Cisco Datensicherheitsfiltern ausgewertet werden.	Ja	Ja
Protokolle des Datensicherheitsmoduls	Zeichnet Nachrichten im Zusammenhang mit den Cisco Datensicherheitsfiltern auf.	Nein	Nein
DCA Engine Framework-Protokolle (Dynamische Inhaltsanalyse)	Zeichnet Nachrichten im Zusammenhang mit der Kommunikation zwischen dem Webproxy und dem Cisco Web Usage Controls Dynamic Content Analysis Engine auf.	Nein	Nein
Protokolle des DCA-Moduls (Dynamische Inhaltsanalyse)	Zeichnet Nachrichten im Zusammenhang mit dem Cisco Web Usage Controls Dynamic Content Analysis Engine auf.	Ja	Ja
Standard-Proxy-Protokolle	Zeichnet Fehler im Zusammenhang mit dem Webproxy auf. Dies ist das grundlegendste aller Webproxy-bezogenen Protokolle. Um spezifischere Aspekte in Bezug auf den Webproxy zu beheben, erstellen Sie ein Protokoll-Abonnement für das entsprechende Webproxy-Modul.	Ja	Ja

Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäß aktiviert?
Disk Manager-Protokolle	Zeichnet Webproxy-Nachrichten auf, die sich auf das Schreiben in den Cache auf dem Datenträger beziehen.	Nein	Nein
Externe Authentifizierungsprotokolle	Zeichnet Nachrichten auf, die mit der externen Authentifizierungsfunktion zusammenhängen, wie erfolgreiche oder fehlgeschlagene Kommunikation mit dem externen Authentifizierungsserver. Auch wenn die externe Authentifizierung deaktiviert ist, enthält dieses Protokoll Meldungen über erfolgreiche lokale Benutzer oder fehlgeschlagene Anmeldung.	Nein	Ja
Feedback-Protokolle	Zeichnet die Webbenutzer auf, die falsch klassifizierte Seiten melden.	Ja	Ja
FTP-Proxy-Protokolle	Zeichnet Fehler- und Warnmeldungen im Zusammenhang mit dem FTP-Proxy auf.	Nein	Nein
FTP-Server-Protokolle	Zeichnet alle Dateien auf, die über FTP auf die sichere Web-Appliance hochgeladen und von dieser heruntergeladen wurden.	Ja	Ja
GUI-Protokolle (Grafische Benutzeroberfläche)	Protokolliert den Verlauf von Seitenaktualisierungen in der Webschnittstelle. GUI-Protokolle enthalten außerdem Informationen zu SMTP-Transaktionen, z. B. Informationen zu geplanten Berichten, die von der Appliance per E-Mail versendet wurden.	Ja	Ja
Haystack-Protokolle	Heuhaufen-Protokolle zeichnen die Verarbeitung von Daten zur Web-Transaktionsverfolgung auf.	Ja	Ja

Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäß aktiviert?
HTTPS-Protokolle	Protokolliert Webproxynachrichten speziell für den HTTPS-Proxy (wenn der HTTPS-Proxy aktiviert ist).	Nein	Nein
ISE-Serverprotokolle	Aufzeichnung der Verbindungs- und Betriebsinformationen für ISE-Server	Ja	Ja
Lizenzmodul-Protokolle	Zeichnet Nachrichten auf, die sich auf das Lizenz- und Feature-Key-Handling-System des Webproxys beziehen.	Nein	Nein
Protokollierung der Framework-Protokolle	Zeichnet Nachrichten im Zusammenhang mit dem Protokollierungssystem des Webproxys auf.	Nein	Nein
Protokollierungsprotokolle	Zeichnet Fehler im Zusammenhang mit der Protokollverwaltung auf.	Ja	Ja
McAfee Integration Framework-Protokolle	Zeichnet Nachrichten auf, die sich auf die Kommunikation zwischen dem Webproxy und dem McAfee-Scanmodul beziehen.	Nein	Nein
McAfee-Protokolle	Zeichnet den Status der Anti-Malware-Scanaktivitäten vom McAfee-Scanmodul auf.	Ja	Ja
Speicher-Manager-Protokolle	Zeichnet Webproxy-Nachrichten auf, die sich auf die Verwaltung des gesamten Speichers beziehen, einschließlich des Cache im Speicher für den Webproxy-Prozess.	Nein	Nein
Verschiedene Protokolle der Proxymodule	Zeichnet Webproxy-Nachrichten auf, die hauptsächlich von Entwicklern oder vom Kundensupport verwendet werden.	Nein	Nein
AnyConnect Secure Mobility	Zeichnet die Interaktion zwischen der	Ja	Ja

Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäß aktiviert?
Daemon-Protokolle	sicheren Web-Appliance und dem AnyConnect-Client auf, einschließlich der Statusprüfung.		
NTP-Protokolle (Network Time Protocol)	Zeichnet Änderungen an der Systemzeit auf, die vom Network Time Protocol vorgenommen wurden.	Ja	Ja
Protokolle des PAC-Dateihostingdaemons	Protokolliert die Verwendung der Proxy-Autokonfigurationsdatei (PAC) durch Clients.	Ja	Ja
Protokolle der Proxyumgehung	Zeichnet Transaktionen auf, die den Webproxy umgehen.	Nein	Ja
Reporting-Protokolle	Zeichnet einen Verlauf der Berichterstellung auf.	Ja	Ja
Reporting-Abfrageprotokolle	Zeichnet Fehler im Zusammenhang mit der Berichterstellung auf.	Ja	Ja
Debugprotokolle anfordern	Protokolliert sehr detaillierte Debuginformationen zu einer bestimmten HTTP-Transaktion aus allen Webproxy-Modulprotokolltypen. Es ist ratsam, dieses Protokoll-Abonnement zu erstellen, um ein Proxy-Problem mit einer bestimmten Transaktion zu beheben, ohne alle anderen Proxy-Protokoll-Abonnements zu erstellen. Hinweis: Sie können dieses Protokoll-Abonnement nur in der CLI erstellen.	Nein	Nein
Authentifizierungsprotokolle	Zeichnet Nachrichten im Zusammenhang mit der Zugriffskontrollfunktion auf.	Ja	Ja
SHD-Protokolle	Protokolliert einen Verlauf des	Ja	Ja

Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäß aktiviert?
(Systemstatusdaemon)	Systemzustands und einen Verlauf unerwarteter Neustarts des Daemons.		
SNMP-Protokolle	Zeichnet Debug-Meldungen für das SNMP-Netzwerkmanagement-Modul auf.	Ja	Ja
SNMP-Modulprotokolle	Protokolliert Webproxy-Meldungen, die sich auf die Interaktion mit dem SNMP-Überwachungssystem beziehen.	Nein	Nein
Sophos Integration Framework-Protokolle	Zeichnet Nachrichten im Zusammenhang mit der Kommunikation zwischen dem Webproxy und dem Sophos-Scanmodul auf.	Nein	Nein
Sophos-Protokolle	Protokolliert den Status der Anti-Malware-Scan-Aktivität der Sophos-Scan-Engine.	Ja	Ja
Statusprotokolle	Zeichnet systembezogene Informationen auf, z. B. Downloads von Feature-Schlüsseln.	Ja	Ja
Systemprotokolle	Zeichnet DNS-, Fehler- und Commit-Aktivitäten auf	Ja	Ja
Fehlerprotokolle der Datenverkehrsüberwachung	Zeichnet L4TM-Schnittstellen auf und erfasst Fehler.	Ja	Ja
Protokolle der Datenverkehrsüberwachung	Zeichnet dem L4TM-Block hinzugefügte Standorte und Zulassungslisten auf.	Nein	Ja
UDS-Protokolle (Benutzererkennungsdienst)	Zeichnet Daten darüber auf, wie der Webproxy den Benutzernamen erkennt, ohne die eigentliche Authentifizierung durchzuführen. Sie enthält Informationen zur Interaktion mit der Cisco Adaptive Security Appliance für Secure Mobility sowie zur	Ja	Ja

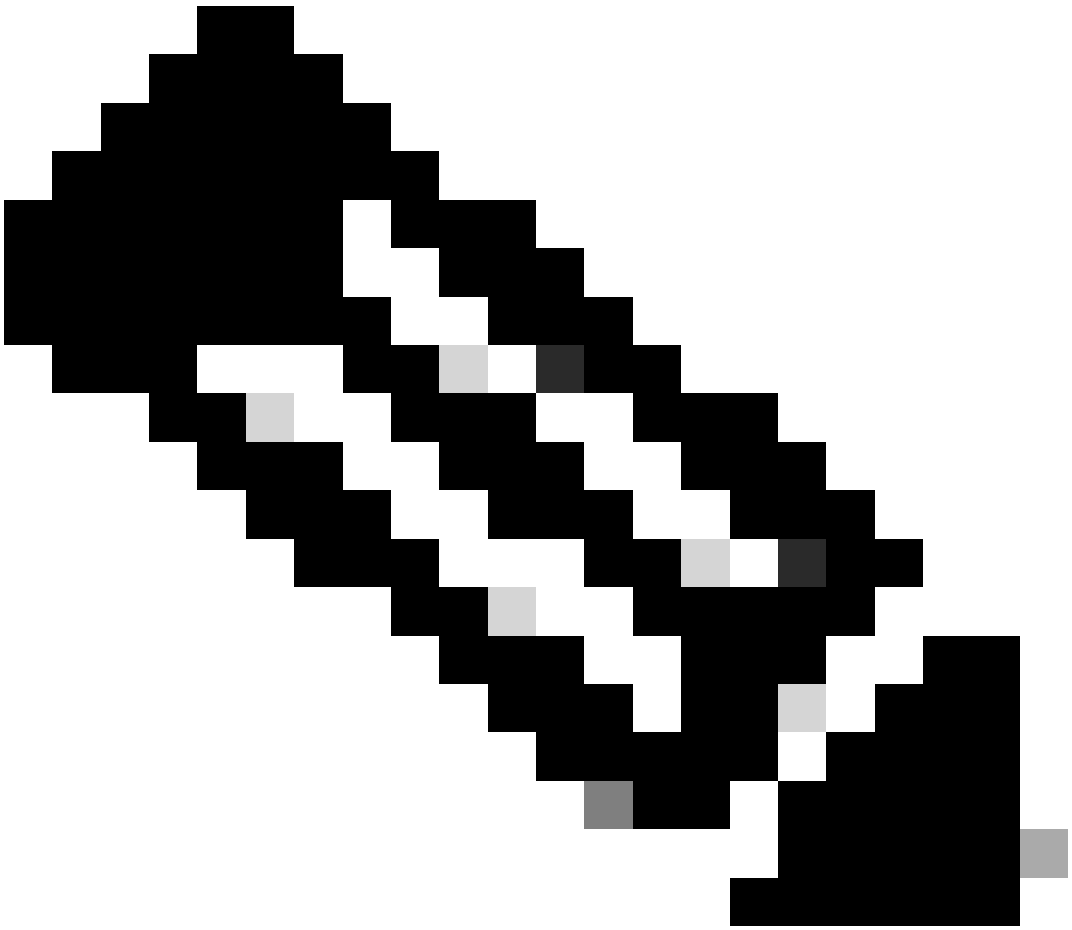
Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäß aktiviert?
	Integration mit dem Novell eDirectory-Server für eine transparente Benutzeridentifizierung.		
Aktualisierungsprotokolle	Zeichnet einen Verlauf von WBRS und anderen Updates auf.	Ja	Ja
W3C-Protokolle	Zeichnet den Verlauf des Webproxy-Clients in einem W3C-kompatiblen Format auf. finden Sie weitere Informationen.	Ja	Nein
WBNP-Protokolle (SensorBase-Netzwerkteilnahme)	Aufzeichnung des Verlaufs der Teilnahme am Cisco SensorBase-Netzwerk-Uploads in das SensorBase-Netzwerk	Nein	Ja
WBRS-Framework-Protokolle (Webreputations-Bewertung)	Zeichnet Nachrichten auf, die sich auf die Kommunikation zwischen dem Webproxy und den Webreputationsfiltern beziehen.	Nein	Nein
Protokolle des WCCP-Moduls	Zeichnet Webproxy-Nachrichten im Zusammenhang mit der Implementierung von WCCP auf.	Nein	Nein
Webcat Integration Framework-Protokolle	Zeichnet Nachrichten auf, die sich auf die Kommunikation zwischen dem Webproxy und der URL-Filter-Engine beziehen, die den Cisco Web Usage Controls zugeordnet ist.	Nein	Nein
Webroot-Integrations-Framework-Protokolle	Zeichnet Nachrichten auf, die sich auf die Kommunikation zwischen dem Webproxy und dem Webroot-Scanmodul beziehen.	Nein	Nein
Webroot-Protokolle	Protokolliert den Status der Anti-Malware-Scanaktivität des Webroot-Scanmoduls.	Ja	Ja
Protokolle zur Bestätigung der	Zeichnet einen Verlauf der Web-Clients auf,	Ja	Ja

Protokolldateityp	Beschreibung	Unterstützt Syslog Push?	Standardmäß aktiviert?
Willkommensseite	die auf der Endbenutzer-Bestätigungsseite auf die Schaltfläche Akzeptieren klicken.		

Protokolle anzeigen

Standardmäßig werden die Protokolle lokal im SWA gespeichert. Sie können die lokal gespeicherten Protokolldateien über die Benutzeroberfläche herunterladen oder die Protokolle über die CLI anzeigen.

Protokolldateien über GUI herunterladen



Hinweis: FTP muss auf der Appliance aktiviert sein. Weitere Informationen zum Aktivieren von FTP finden Sie in diesem Artikel unter Aktivieren von FTP auf einer sicheren Webappliance.

Sie können die Protokolldateien von der Benutzeroberfläche herunterladen:

Schritt 1: Bei GUI anmelden

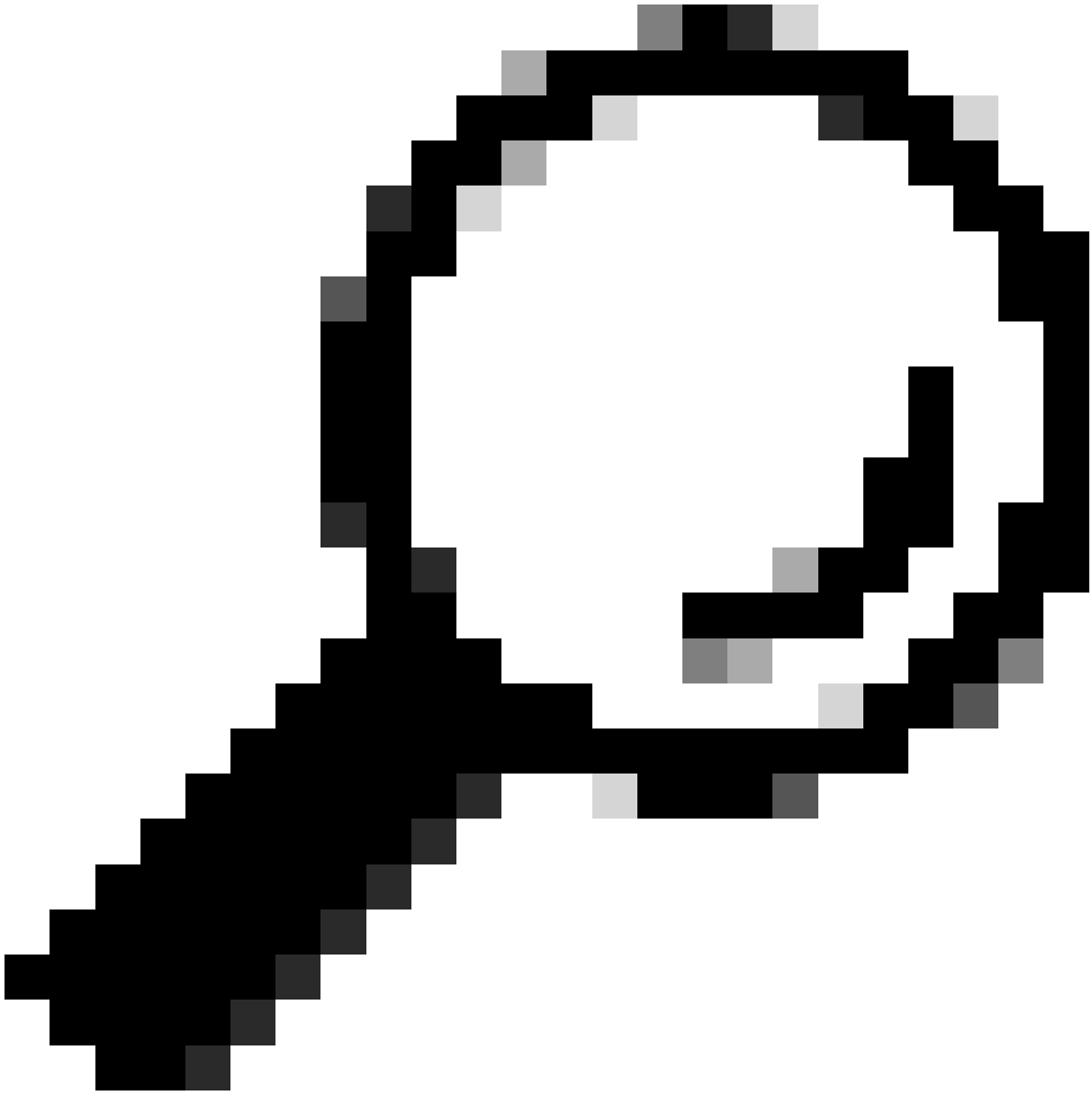
Schritt 2: Navigieren Sie zur Systemverwaltung.

Schritt 3: Protokoll-Subscriptions auswählen

Schritt 4: Klicken Sie in der Liste der Protokoll-Subscriptions in der Spalte Log Files (Protokolldateien) auf den Namen der Protokoll-Subscription.

Schritt 5.Geben Sie auf Aufforderung den Benutzernamen und das Kennwort des Administrators für den Zugriff auf die Appliance ein.

Schritt 6.Wenn Sie eingeloggt sind, klicken Sie auf eine der Protokolldateien, um sie in Ihrem Browser anzuzeigen oder auf einer Festplatte zu speichern.



Tipp: Aktualisieren Sie den Browser, um aktualisierte Ergebnisse zu erhalten.

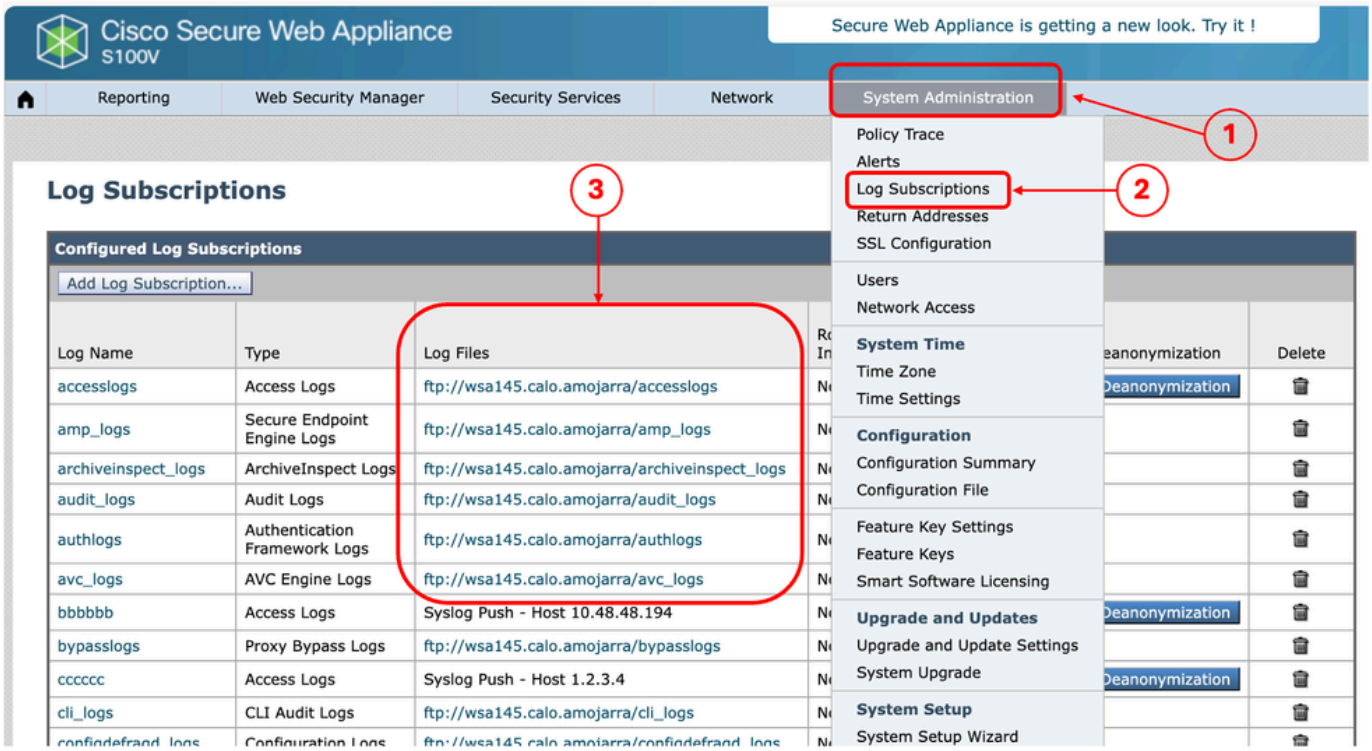
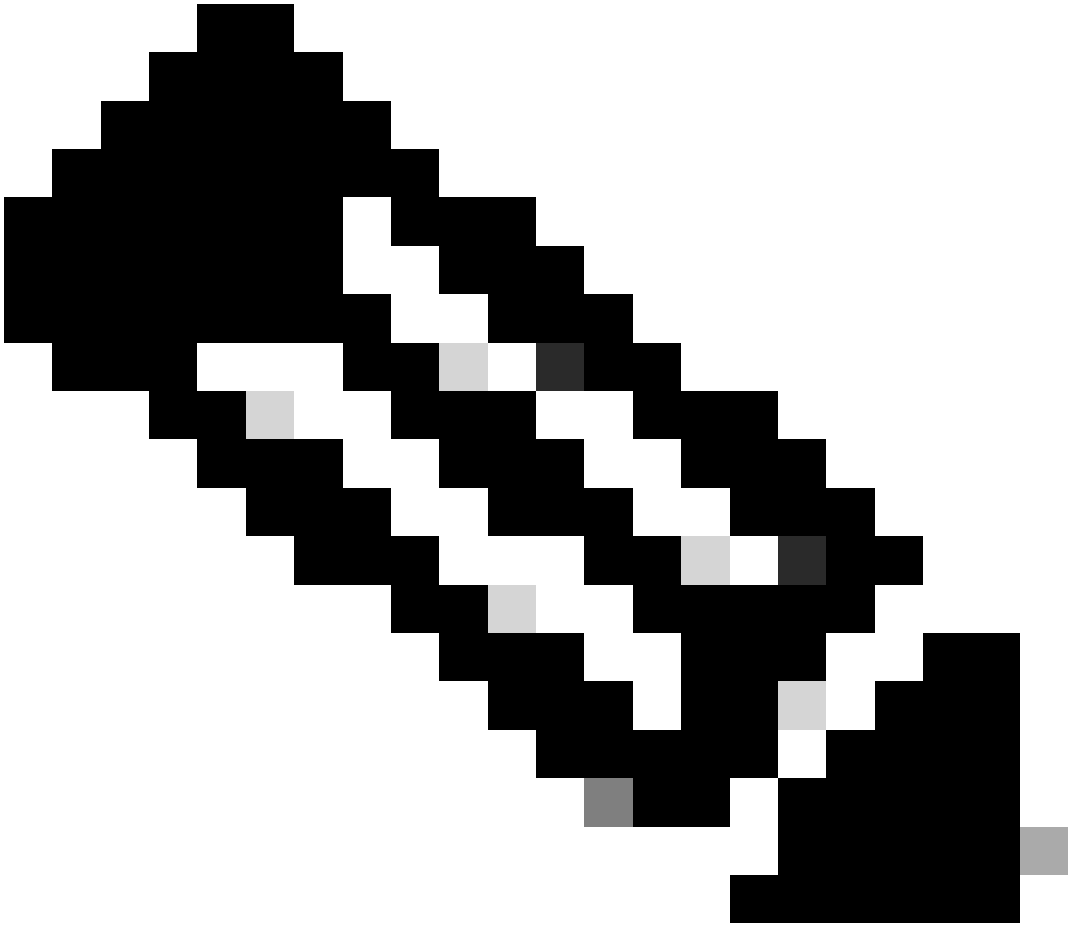


Bild - Protokolldateien herunterladen



Hinweis: Wenn ein Protokoll-Abonnement komprimiert wurde, können Sie es herunterladen, dekomprimieren und dann öffnen.

Protokolle über CLI anzeigen

Sie können die Protokolle über die CLI anzeigen. In diesem Fall können Sie auf Live-Protokolle zugreifen oder nach einem Schlüsselwort in den Protokollen filtern.

Schritt 1: Mit CLI verbinden

Schritt 2: Geben Sie grep ein, und drücken Sie die Eingabetaste.

Schritt 3: Geben Sie die Nummer des Protokolls ein, das Sie anzeigen möchten

Schritt 4. (Optional) Sie können die Ausgabe filtern, indem Sie einen regulären Ausdruck oder ein Wort definieren, oder drücken Sie die Eingabetaste

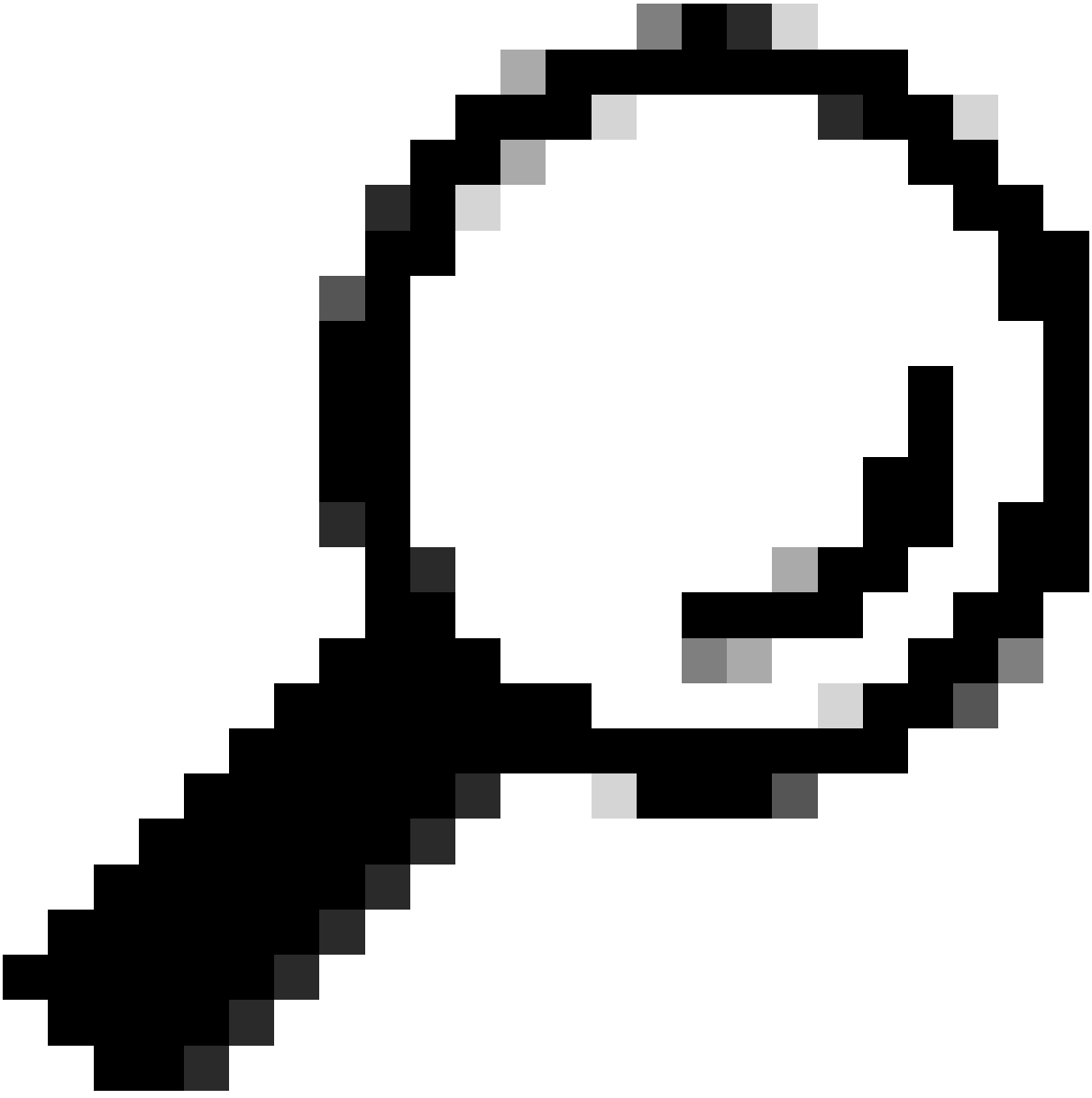
Schritt 5. Wenn Sie die Suche nach dem in Schritt 4 eingegebenen Schlüsselwort benötigen, um

die Groß-/Kleinschreibung nicht zu berücksichtigen, drücken Sie die Eingabetaste in "Soll diese Suche die Groß-/Kleinschreibung nicht berücksichtigen? [Y]>" drücken Sie andernfalls "N" und betätigen Sie die Eingabetaste.

Schritt 6: Wenn Sie Ihr Stichwort von der Suche ausnehmen möchten, geben Sie "Y" in "Möchten Sie nach nicht übereinstimmenden Zeilen suchen? [N]>" drücken Sie die Eingabetaste.

Schritt 7. Wenn Sie Live-Protokolle anzeigen möchten, geben Sie "Y" in "Do you want to tail the logs? [N]>" drücken, andernfalls die Eingabetaste.

Schritt 8: Wenn Sie die Protokolle seitenweise anzeigen möchten, geben Sie "Y" in "Möchten Sie die Ausgabe paginieren? [N]>" drücken, andernfalls die Eingabetaste.



Tipp: Wenn Sie paginieren möchten, können Sie die Protokolle durch Drücken von "q" verlassen.

Hier ist ein Beispiel Ausgabe zeigt alle Zeilen, die "Warnung" in ihnen:

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "Secure Endpoint Engine Logs" Retrieval: FTP Poll
3. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
4. "audit_logs" Type: "Audit Logs" Retrieval: FTP Poll
5. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
6. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
7. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
8. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
...
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 40

Enter the regular expression to grep.
[]> Warning

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]>

Do you want to paginate the output? [N]>
```

FTP auf sicherer Webappliance aktivieren

Standardmäßig ist FTP auf dem SWA nicht aktiviert. So aktivieren Sie FTP:

Schritt 1: Bei GUI anmelden

Schritt 2: Navigieren zum Netzwerk

Schritt 3: Schnittstellen auswählen

Schritt 4: Klicken Sie auf Einstellungen bearbeiten.

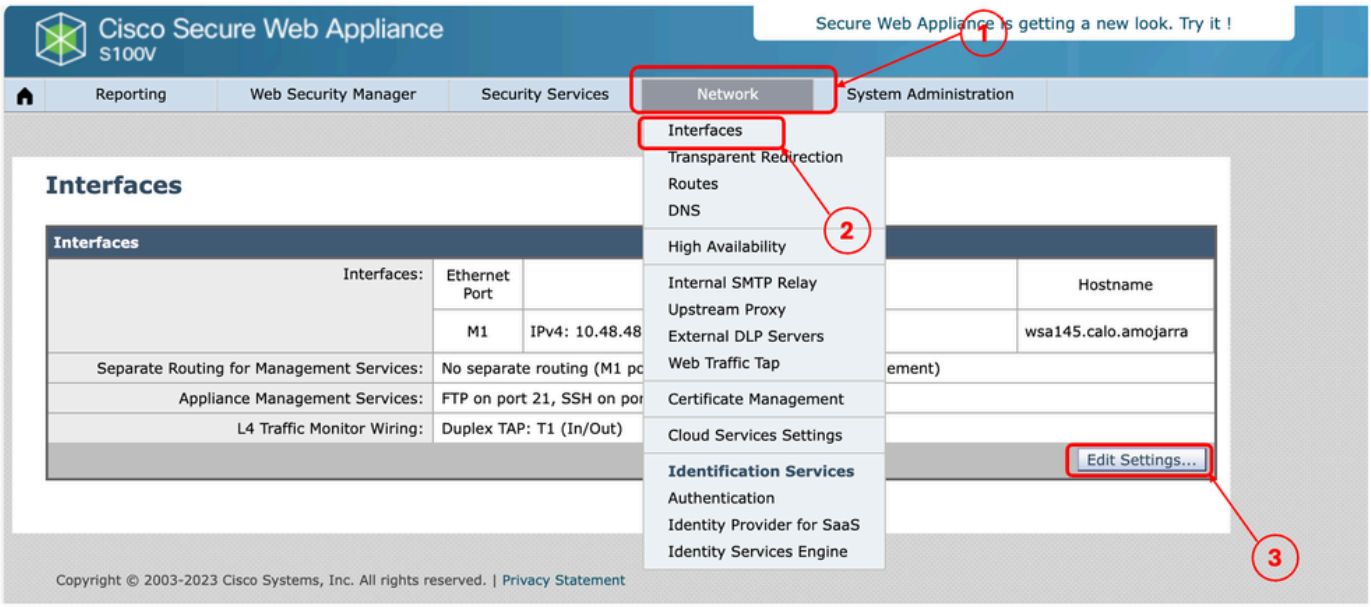


Image: Aktivieren Sie FTP auf SWA

Schritt 5: Aktivieren Sie das Kontrollkästchen für FTP.

Schritt 6: Geben Sie die TCP-Portnummer für FTP an (Standard-FTP-Port ist 21).

Schritt 7. Änderungen übermitteln und bestätigen

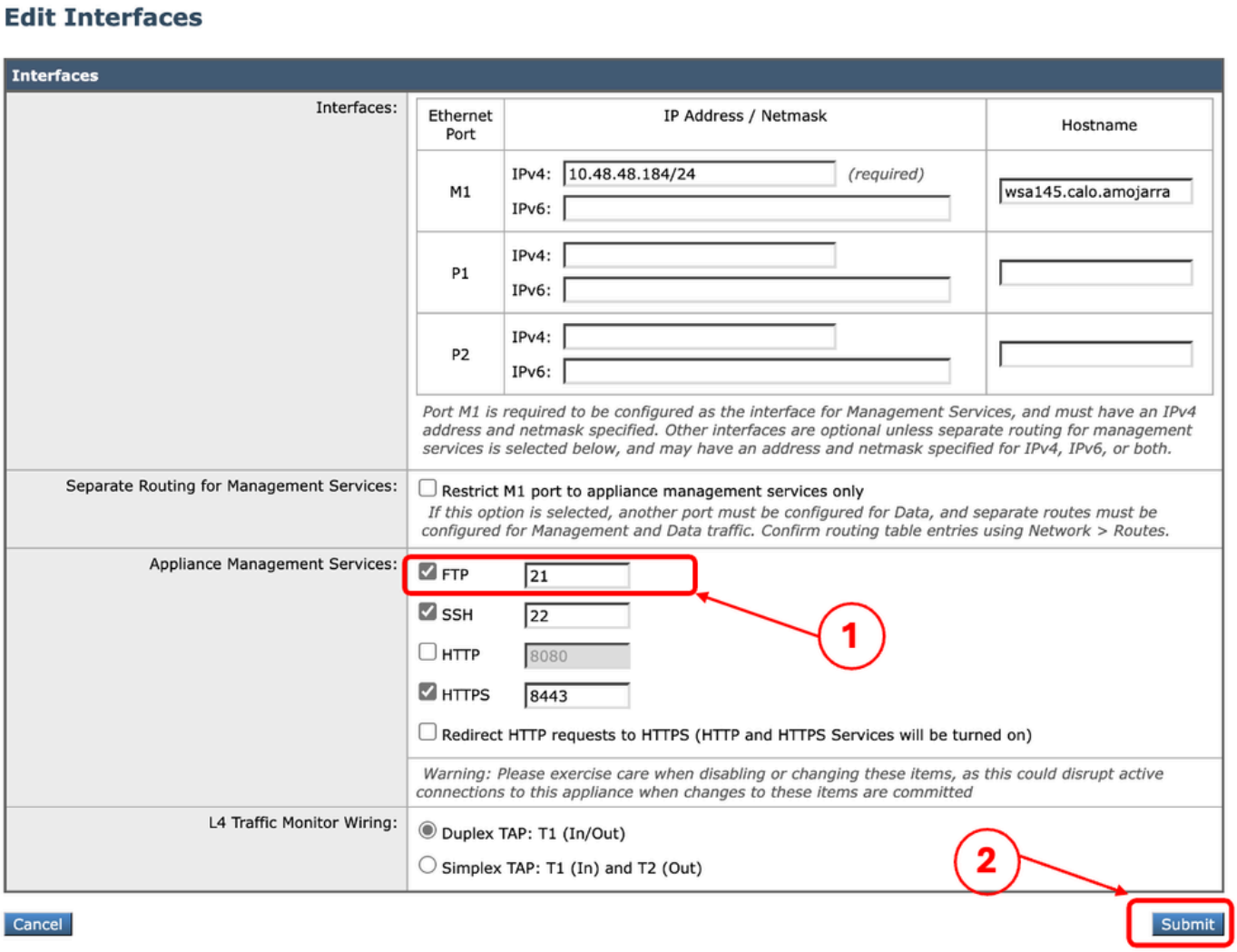


Bild: Konfigurieren des FTP-Parameters in SWA

Zugehörige Informationen

- [Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - LD (begrenzte Bereitstellung) - Fehlerbehebung...]
- [Konfigurieren von SCP-Push-Protokollen in einer sicheren Web-Appliance mit Microsoft Server - Cisco]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.