セキュアなWebアプライアンスのログへのアクセス

内容

はじめに

このドキュメントでは、セキュアWebアプライアンス(SWA)のログを表示する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 物理または仮想SWAがインストールされている。
- ライセンスの有効化またはインストール
- セキュアシェル(SSH)クライアント。
- セットアップウィザードが完了しました。

- SWAへの管理アクセス。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

SWAログタイプ

セキュアWebアプライアンスは、自身のシステムとトラフィックの管理アクティビティをログファイルに書き込むことによって記録します。管理者は、これらのログファイルを参照して、アプライアンスの監視とトラブルシューティングを行うことができます。

次の表に、Secure Web Applianceのログファイルのタイプを示します。

ログファイルの種類	説明	Syslogプッシュをサポートしていますか。	デフォルトで有効？
アクセスコントロールエンジンログ	Webプロキシ ACL（アクセスコントロールリスト）評価エンジンに関連するメッセージを記録します。	いいえ	いいえ
EndpointEngineログの保護	ファイルレピュテーションスキャンとファイル分析に関する情報を記録します(セキュアエンドポイント)。	Yes	Yes
監査ログ	AAA（認証、許可、アカウンティング）イベントを記録します。アプリケーションインターフェイスおよびコマンドラインインターフェイスとのすべてのユーザの対話を記録し、コミットされた変更をキャプチャします。 監査ログの詳細の一部を次に示します。 • ユーザー – ログオン • ユーザー – ログオンに失敗したパスワードが正しくありません • ユーザー – ログオンに失敗しました。不明なユーザー名 • ユーザー – ログオンに失敗したアカウントの有効期限が切れました • ユーザ – ログオフ • ユーザー – ロックアウト • ユーザ – アクティブ化	Yes	Yes

ログファイルの種類	説明	Syslogプッシュをサポートしていますか。	デフォルトで有効？
	• ユーザ – パスワードの変更 • ユーザ：パスワードのリセット • ユーザ – セキュリティ設定/プロファイルの変更 • ユーザ – 作成済み • ユーザー – 削除/変更 • グループ/ロール – 削除/変更 • グループ/ロール：権限の変更		
アクセスログ	Webプロキシクライアント履歴を記録します。	Yes	Yes
ADCエンジンフレームワークログ	WebプロキシとADCエンジン間の通信に関連するメッセージを記録します。	いいえ	いいえ
ADCエンジンログ	ADCエンジンからのデバッグメッセージを記録します。	Yes	Yes
認証フレームワークのログ	認証履歴とメッセージを記録します。	いいえ	Yes
AVCエンジンフレームワークログ	WebプロキシとAVCエンジン間の通信に関連するメッセージを記録します。	いいえ	いいえ
AVCエンジンログ	AVCエンジンからのデバッグメッセージを記録します。	Yes	Yes
CLI監査ログ	コマンドラインインターフェイスのアクティビティの履歴監査を記録します。	Yes	Yes
設定ログ	Webプロキシ構成管理システムに関連するメッセージを記録します。	いいえ	いいえ

ログファイルの種類	説明	Syslogプッシュをサポートしていますか。	デフォルトで有効？
接続管理ログ	Webプロキシ接続管理システムに関連するメッセージを記録します。	いいえ	いいえ
データセキュリティログ	Ciscoデータセキュリティフィルタによって評価されたアップロード要求のクライアント履歴を記録します。	Yes	Yes
データセキュリティモジュールログ	シスコのデータセキュリティフィルタに関連するメッセージを記録します。	いいえ	いいえ
DCAエンジンフレームワークログ （動的コンテンツ分析）	WebプロキシとCisco Web Usage Controls Dynamic Content Analysisエンジン間の通信に関連するメッセージを記録します。	いいえ	いいえ
DCAエンジンログ （動的コンテンツ分析）	Cisco Web Usage Controlsダイナミックコンテンツ分析エンジンに関連するメッセージを記録します。	Yes	Yes
デフォルトのプロキシログ	Webプロキシに関連するエラーを記録します。 これは、すべてのWebプロキシ関連のログの中で最も基本的なものです。Webプロキシに関連するより具体的な側面のトラブルシューティングを行うには、該当するWebプロキシモジュールのログサブスクリプションを作成します。	Yes	Yes
ディスクマネージャログ	ディスク上のキャッシュへの書き込みに関連するWebプロキシメッセージを記録します。	いいえ	いいえ
外部認証ログ	外部認証サーバとの通信の成功や失敗など、外部認証機能の使用に関連するメッセージを記録します。 外部認証が無効になっている場合でも、このログにはローカルユーザのログイン成功または失敗に関するメ	いいえ	Yes

ログファイルの種類	説明	Syslogプッシュをサポートしていますか。	デフォルトで有効？
	ッセージが含まれています。		
フィードバックログ	間違って分類されたページを報告するWebユーザーを記録します。	Yes	Yes
FTPプロキシログ	FTPプロキシに関連するエラーメッセージと警告メッセージを記録します。	いいえ	いいえ
FTPサーバログ	Secure Web Applianceとの間でFTPを使用してアップロードおよびダウンロードされたすべてのファイルを記録します。	Yes	Yes
GUIログ (グラフィカル ユーザ インターフェイス)	ページ更新の履歴をWebインターフェイスに記録します。GUIログには、SMTPトランザクションに関する情報（アプライアンスから電子メールで送信されるスケジュール済みレポートに関する情報など）も含まれます。	Yes	Yes
ヘイスタックのログ	Haystackログは、Webトランザクション追跡データ処理を記録します。	Yes	Yes
HTTPSログ	HTTPSプロキシに固有のWebプロキシメッセージを記録します（HTTPSプロキシが有効な場合）。	いいえ	いいえ
ISEサーバログ	ISEサーバの接続と動作情報を記録します。	Yes	Yes
ライセンスモジュールログ	Webプロキシのライセンスおよび機能キー処理システムに関連するメッセージを記録します。	いいえ	いいえ
ロギング・フレームワークのログ	Webプロキシのロギングシステムに関連するメッセージを記録します。	いいえ	いいえ
ログのロギング	ログ管理に関連するエラーを記録します。	Yes	Yes

ログファイルの種類	説明	Syslogプッシュをサポートしていますか。	デフォルトで有効？
McAfee統合フレームワークログ	WebプロキシとMcAfeeスキャンエンジン間の通信に関連するメッセージを記録します。	いいえ	いいえ
McAfeeログ	McAfeeスキャンエンジンからのマルウェア対策スキャンアクティビティのステータスを記録します。	Yes	Yes
メモリマネージャログ	Webプロキシプロセスのインメモリキャッシュを含むすべてのメモリの管理に関連するWebプロキシメッセージを記録します。	いいえ	いいえ
その他のプロキシモジュールログ	主に開発者またはカスタマーサポートが使用するWebプロキシメッセージを記録します。	いいえ	いいえ
AnyConnectセキュアモビリティデーモンログ	セキュアWebアプライアンスとAnyConnectクライアントの間の対話（ステータスチェックを含む）を記録します。	Yes	Yes
NTPログ (ネットワーク タイム プロトコル)	Network Time Protocol（NTP；ネットワークタイムプロトコル）によってシステム時刻が変更されたことを記録します。	Yes	Yes
PACファイルホスティングデーモンログ	クライアントによるプロキシ自動設定(PAC)ファイルの使用状況を記録します。	Yes	Yes
プロキシバイパスログ	Webプロキシをバイパスするトランザクションを記録します。	いいえ	Yes
レポートログ	レポート生成の履歴を記録します。	Yes	Yes
レポートクエリログ	レポート生成に関連するエラーを記録します。	Yes	Yes
デバッグログの要求	すべてのWebプロキシモジュールログタイプから特定	いいえ	いい

ログファイルの種類	説明	Syslogプッシュをサポートしていますか。	デフォルトで有効？
	のHTTPトランザクションに関する詳細なデバッグ情報を記録します。他のすべてのプロキシログサブスクリプションを作成せずに、特定のトランザクションのプロキシ問題をトラブルシューティングするには、このログサブスクリプションを作成することをお勧めします。 注：このログサブスクリプションは、CLIでのみ作成できます。		え
認証ログ	アクセス制御機能に関連するメッセージを記録します。	Yes	Yes
SHDログ （システム正常性デーモン）	システムサービスの状態の履歴と予期しないデーモンの再起動の履歴を記録します。	Yes	Yes
SNMPログ	SNMPネットワーク管理エンジンに関連するデバッグメッセージを記録します。	Yes	Yes
SNMPモジュールログ	SNMP監視システムとの対話に関連するWebプロキシメッセージを記録します。	いいえ	いいえ
Sophos統合フレームワークのログ	WebプロキシとSophosスキャンエンジン間の通信に関連するメッセージを記録します。	いいえ	いいえ
Sophosログ	Sophosスキャンエンジンからのマルウェア対策スキャンアクティビティのステータスを記録します。	Yes	Yes
ステータスログ	機能キーのダウンロードなど、システムに関連する情報を記録します。	Yes	Yes
システム ログ	DNS、エラー、コミットのアクティビティを記録します。	Yes	Yes

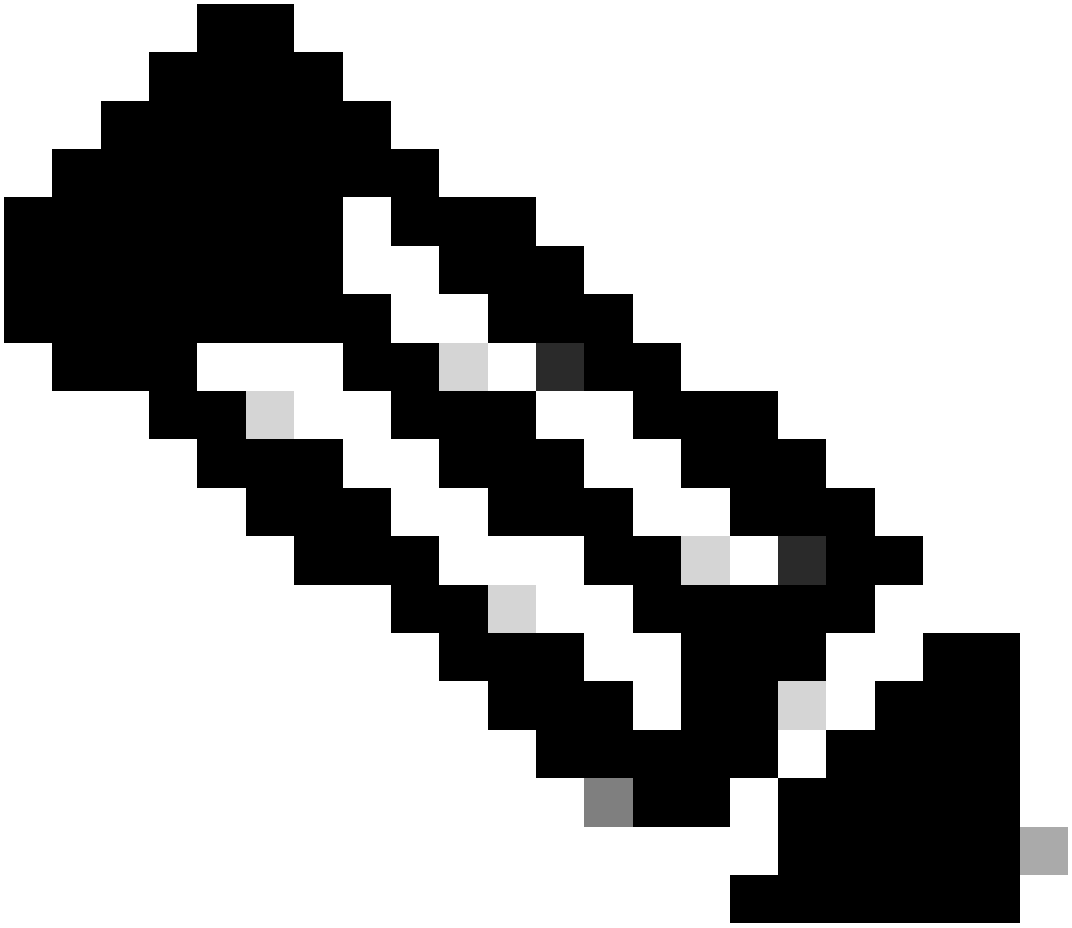
ログファイルの種類	説明	Syslogプッシュをサポートしていますか。	デフォルトで有効？
トラフィックモニタのエラーログ	L4TMインターフェイスとキャプチャエラーを記録します。	Yes	Yes
トラフィックモニタログ	L4TMブロックと許可リストに追加されたサイトを記録します。	いいえ	Yes
UDSログ （ユーザ検出サービス）	Webプロキシが実際の認証を行わずにユーザー名を検出する方法に関するデータを記録します。このガイドでは、Cisco適応型セキュリティアプライアンスを使用したセキュアモビリティの操作、およびNovell eDirectoryサーバとの統合による透過的なユーザ識別について説明します。	Yes	Yes
更新ログ	WBRSおよびその他の更新の履歴を記録します。	Yes	Yes
W3Cログ	Webプロキシクライアントの履歴をW3C準拠の形式で記録します。 参照してください。	Yes	いいえ
WBNPログ （SensorBaseネットワークへの参加）	Cisco SensorBaseネットワークへのSensorBaseネットワークへの参加アップロードの履歴を記録します。	いいえ	Yes
WBRSフレームワークログ （Webレピュテーションスコア）	WebプロキシとWebレピュテーションフィルタ間の通信に関連するメッセージを記録します。	いいえ	いいえ
WCCPモジュールログ	WCCPの実装に関連するWebプロキシメッセージを記録します。	いいえ	いいえ
Webcat統合フレーム	WebプロキシとCisco Web Usage Controlsに関連付け	いいえ	いい

ログファイルの種類	説明	Syslogプッシュをサポートしていますか。	デフォルトで有効？
ワークのログ	られたURLフィルタリングエンジン間の通信に関連するメッセージを記録します。		え
Webroot統合フレームワークのログ	WebプロキシとWebrootスキャンエンジン間の通信に関連するメッセージを記録します。	いいえ	いいえ
Webrootログ	Webrootスキャンエンジンからのマルウェア対策スキャンアクティビティのステータスを記録します。	Yes	Yes
ウェルカムページの確認ログ	エンドユーザの確認ページでAcceptボタンをクリックしたWebクライアントの履歴を記録します。	Yes	Yes

View Logs

デフォルトでは、ログはSWAにローカルに保存されます。ローカルに保存されたログファイルは、GUIを介してダウンロードするか、CLIから表示できます。

GUIを使用したログファイルのダウンロード



注：アプライアンスでFTPが有効になっている必要があります。FTPを有効にするには、この記事の「Secure Web ApplianceでFTPを有効にする」を参照してください。

ログファイルはGUIからダウンロードできます。

ステップ 1：GUIへのログイン

ステップ 2：System Administrationに移動します

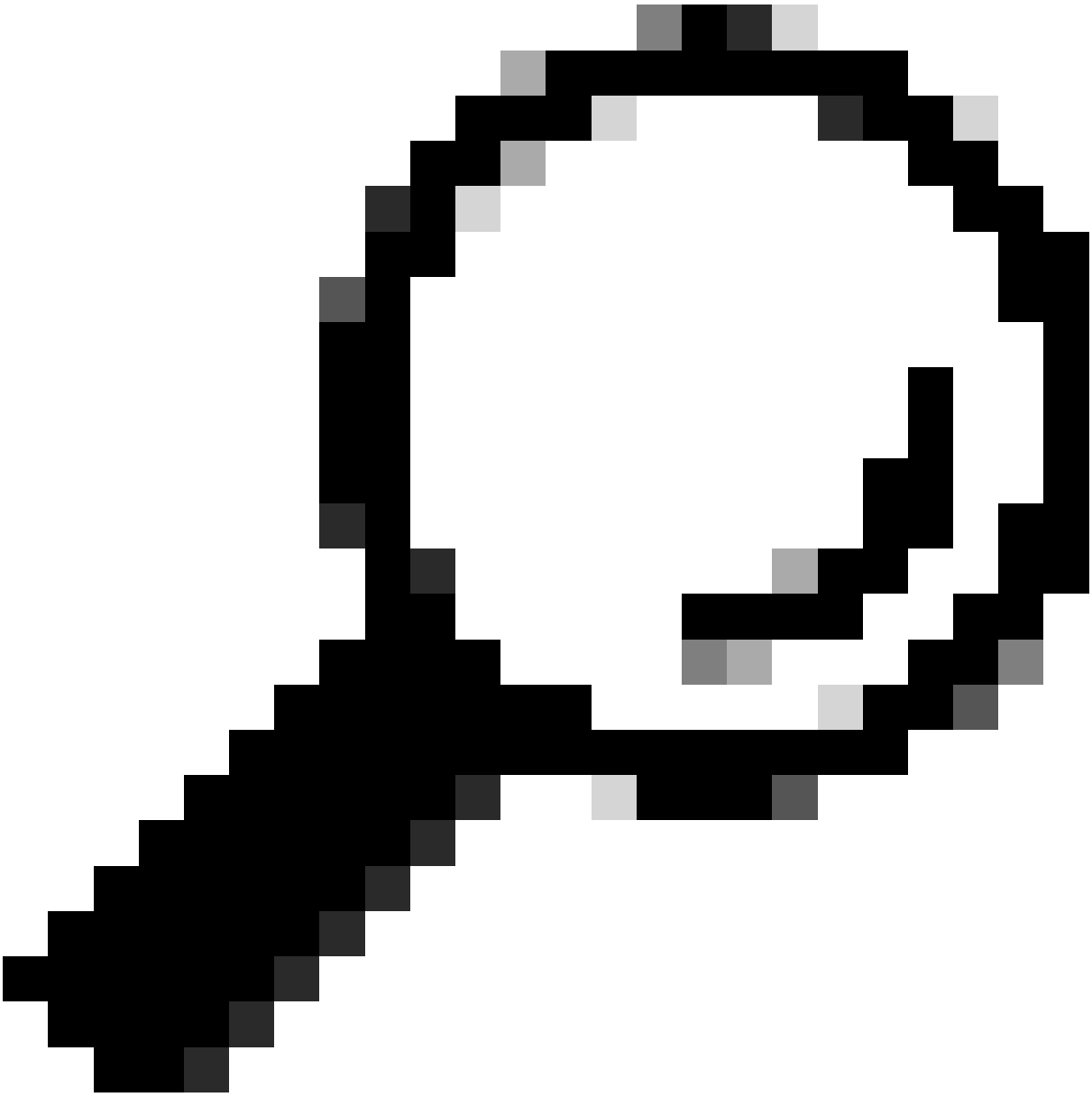
ステップ 3：ログサブスクリプションの選択

ステップ4:ログサブスクリプションのリストのログファイル列で、ログサブスクリプションの名前をクリックします。

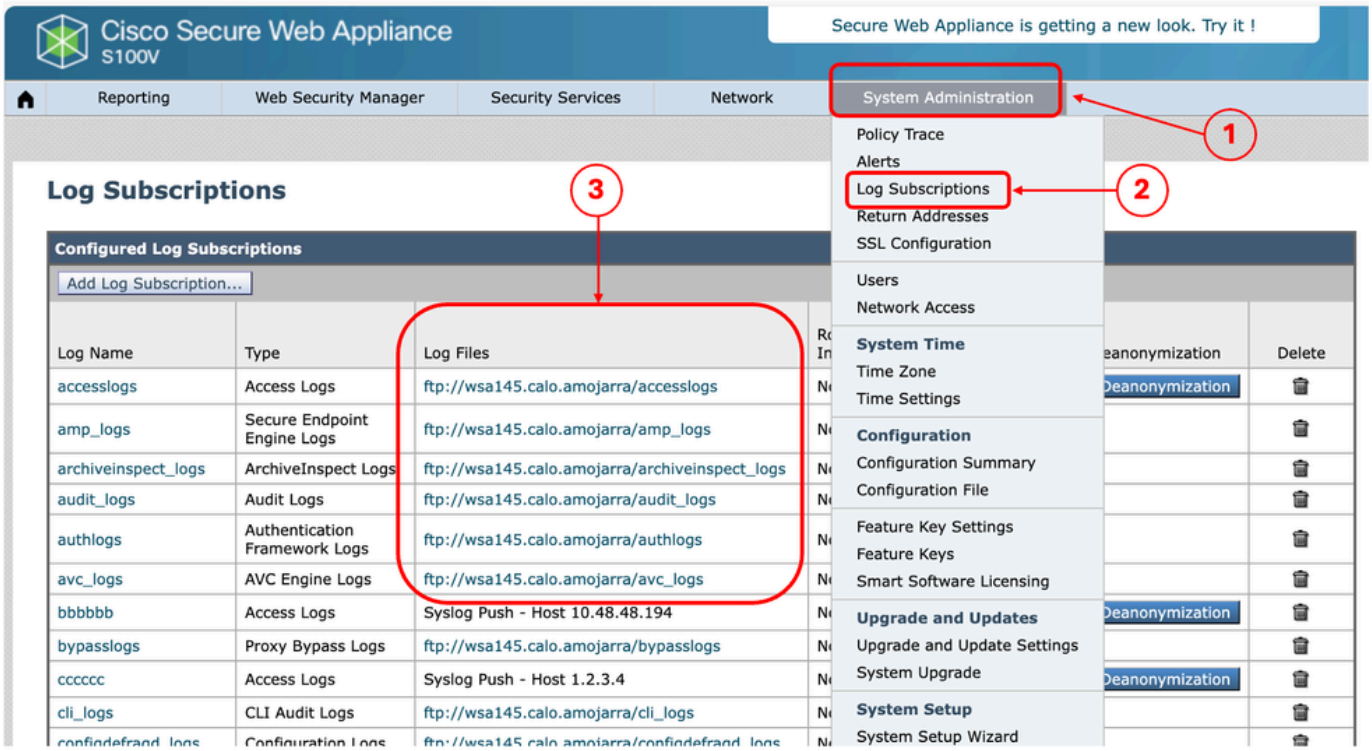
ステップ5:プロンプトが表示されたら、アプライアンスにアクセスするための管理者ユーザ名とパスワードを入力します。

ステップ6:ログインしたら、いずれかのログファイルをクリックしてブラウザで表示するか、デ

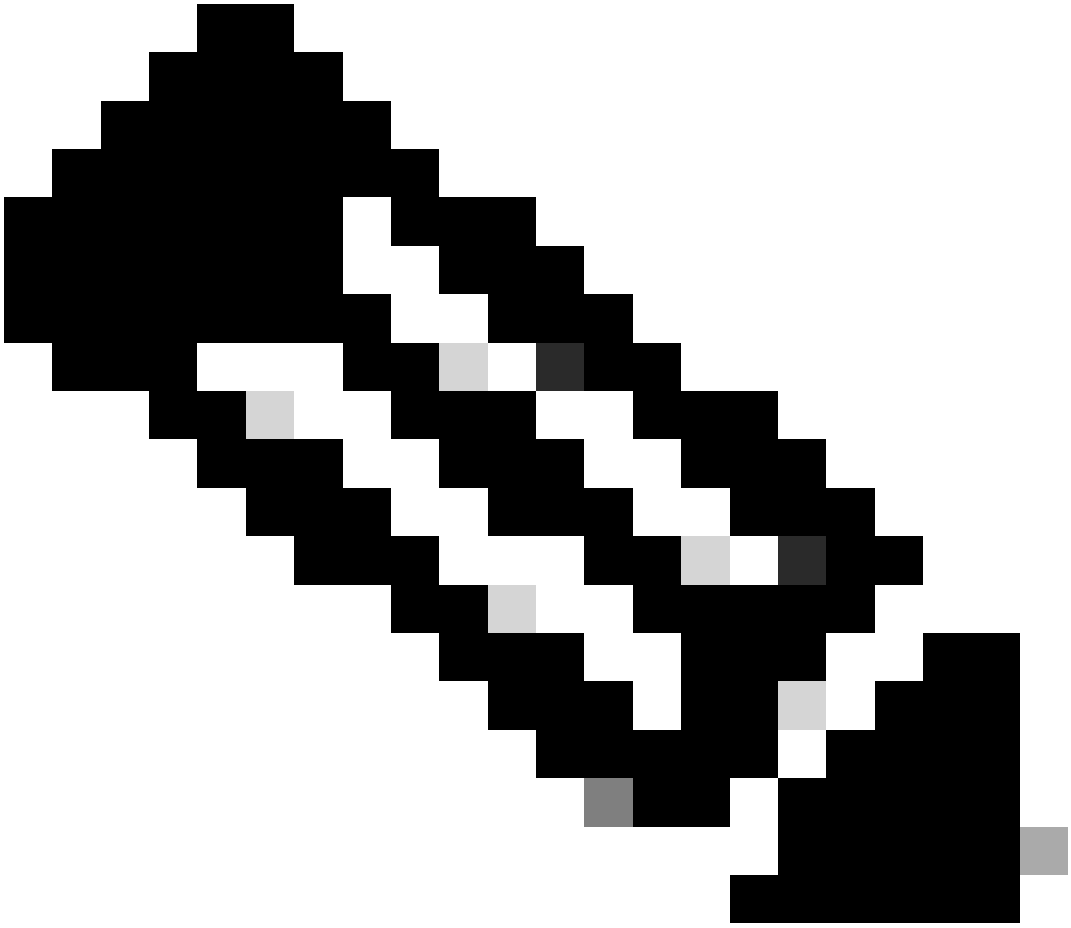
ィスクに保存します。



ヒント：結果を更新するには、ブラウザを更新します。



イメージ – ログファイルのダウンロード



注：ログサブスクリプションが圧縮されている場合、ダウンロードして圧縮解除し、開きます。

CLIからのログの表示

CLIからログを表示できます。この場合、ライブログにアクセスしたり、ログ内のキーワードをフィルタリングしたりできます。

ステップ 1：CLIへの接続

ステップ 2： grepと入力してEnterキーを押す。

ステップ 3：表示するログの番号を入力します

ステップ4: (オプション) 正規表現または単語を定義して出力をフィルタリングするか、Enterキーを押します

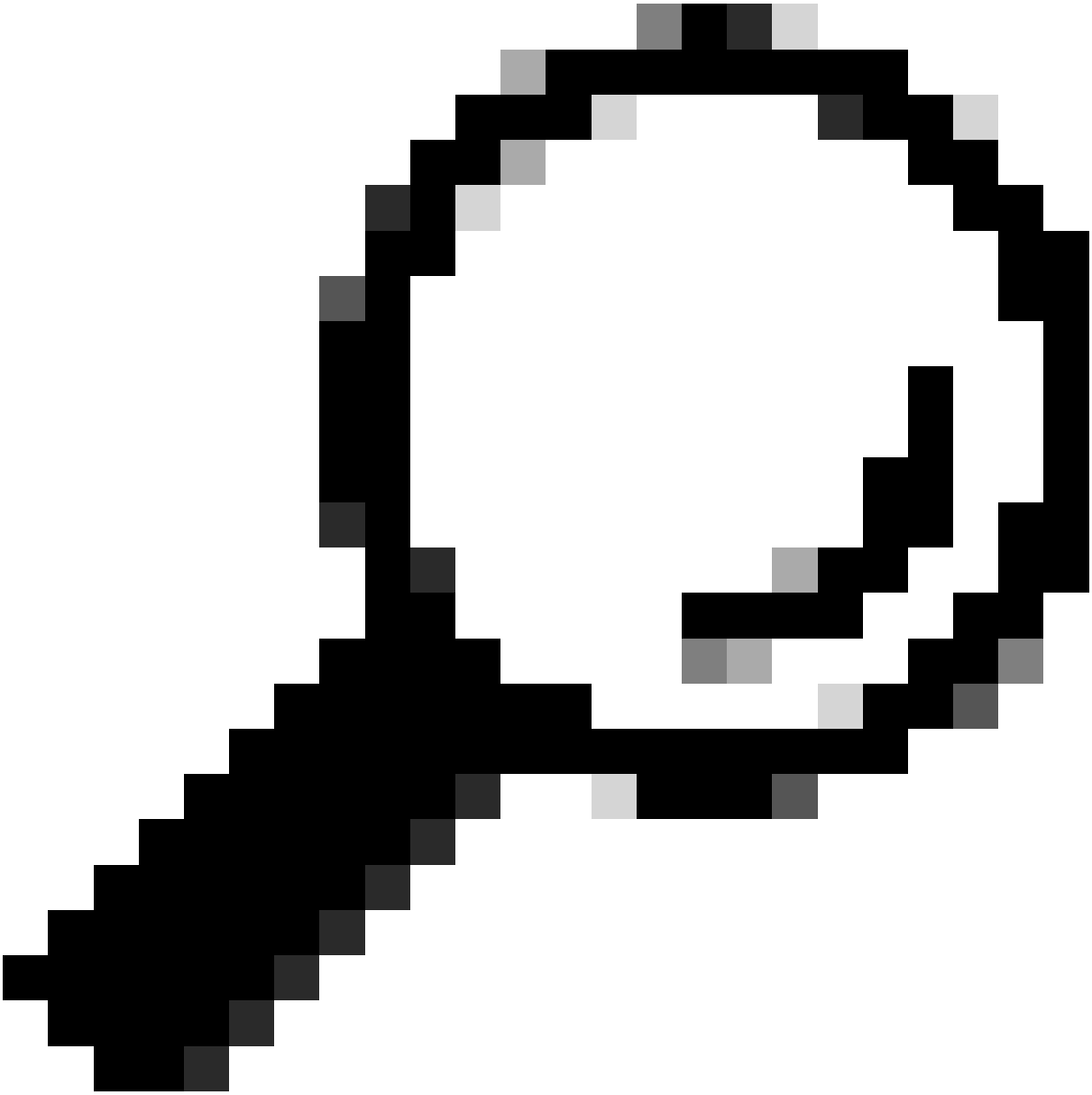
ステップ5：ステップ4で入力したキーワードの検索で大文字と小文字を区別する必要がある場合

は、「この検索で大文字と小文字を区別しますか？」でEnterキーを押します。[Y]>」または「N」と入力し、Enterキーを押します。

手順 6：キーワードを検索から除外する必要がある場合は、「Do you want to search for non-matching lines? (一致しない行を検索しますか？) 」に「Y」と入力します。[N]>」と入力するか、Enterキーを押します。

手順 7： ライブログを表示する必要がある場合は、「Do you want to tail the logs?[N]>」と入力するか、Enterキーを押します。

ステップ 8：ログをページ分割してページを表示するには、「出力をページ分割しますか？」でページタイプ「Y」を選択します。[N]>」と入力するか、Enterキーを押します。



ヒント：ページングを選択する場合は、「q」を押してログを終了できます

次の出力例は、「Warning」が含まれるすべての行を示しています。

```
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]>
```

セキュアWebアプライアンスでのFTPの有効化

デフォルトでは、SWAではFTPは有効になっていません。FTPを有効にするには、次の手順を実行します。

ステップ 1：GUIへのログイン

ステップ 2：Networkに移動します。

ステップ 3：インターフェイスの選択

ステップ 4：[Edit Settings] をクリックします。

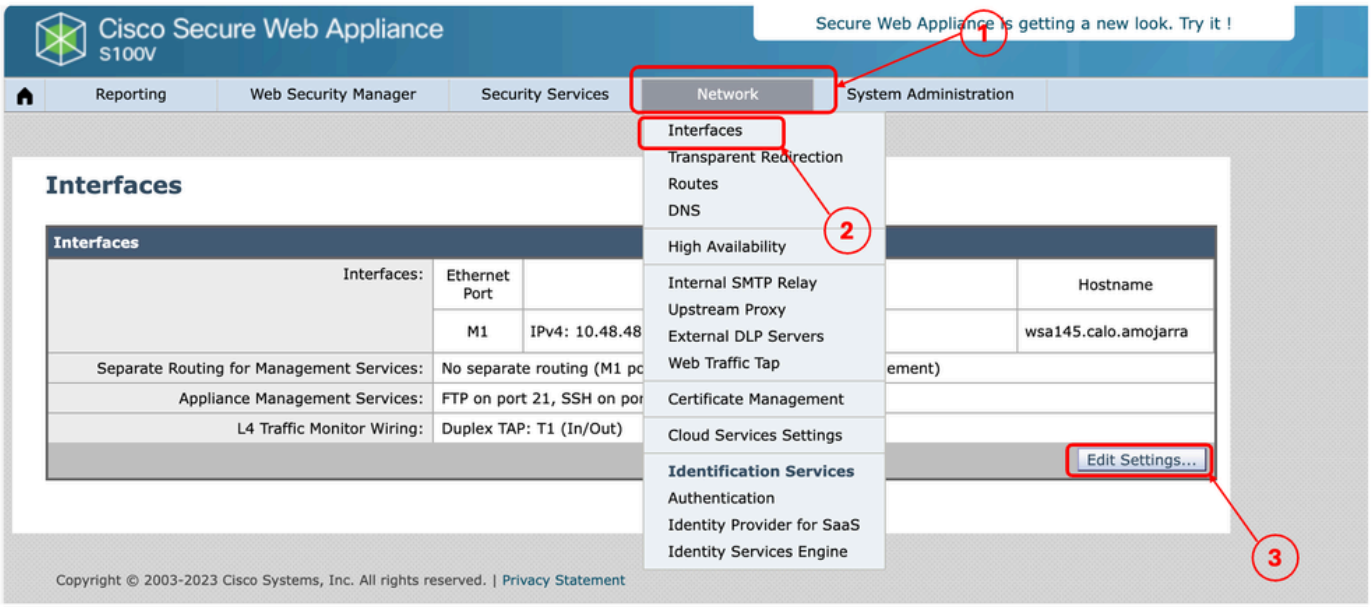


図 – SWAでのFTPの有効化

ステップ 5：FTPのチェックボックスをオンにします

手順 6：FTPのTCPポート番号を入力します（デフォルトのFTPポートは21）。

手順 7：変更を送信して確定します。

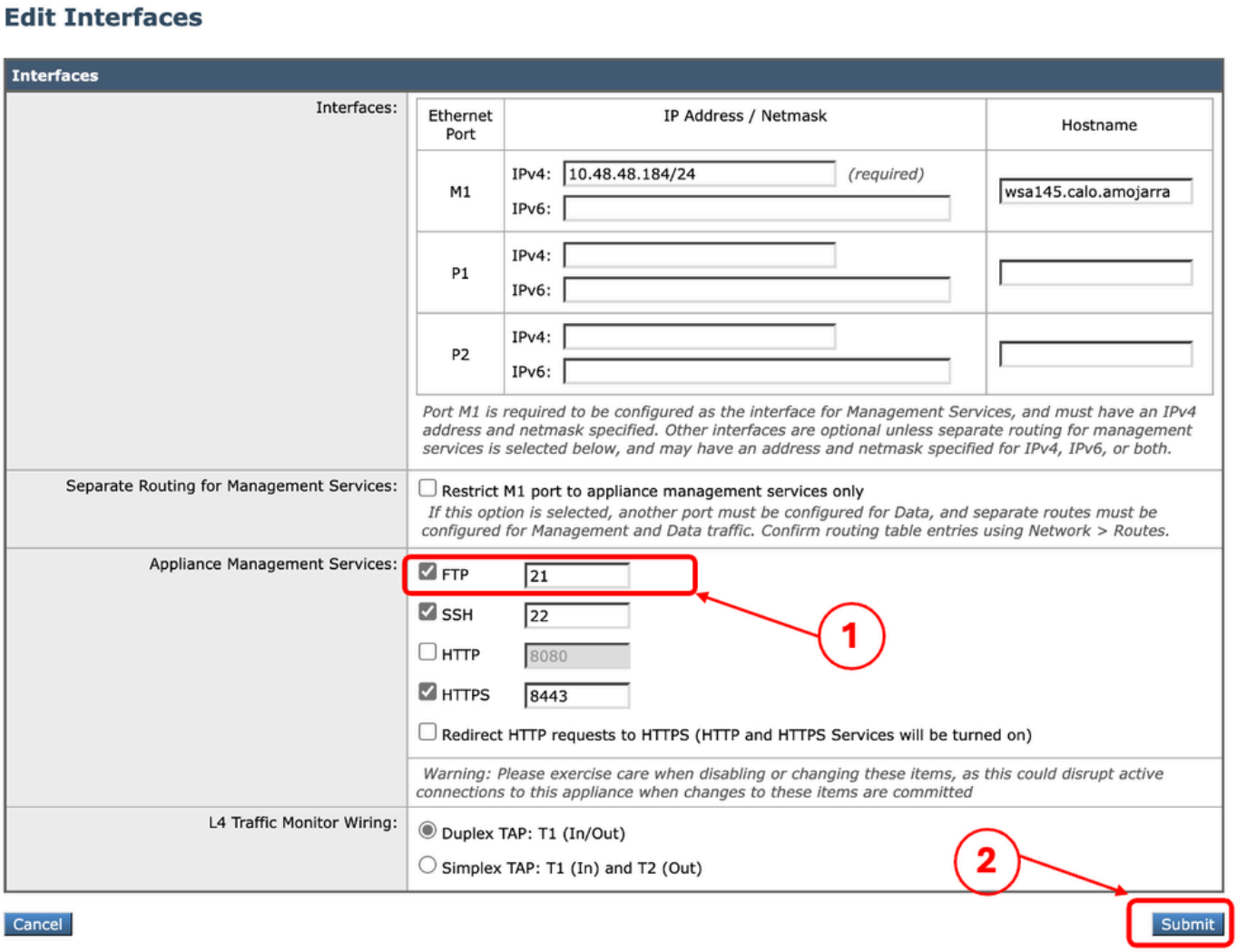


図 – SWAでのFTPパラメータの設定

関連情報

- AsyncOS 15.0ユーザガイドfor Cisco Secure Web Appliance - LD（限定導入）– トラブルシューティング…
- Microsoftサーバを使用したセキュアWebアプライアンスでのSCPプッシュログの設定：シスコ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。