Cisco Secure Network Analytics

プロキシ ログ コンフィギュレーション ガイド 7.5.0

目次

はじめに

概要

Cisco Secure Network Analytics（旧 Stealthwatch）プロキシログのネットワーク プロキシ サーバーからユーザー情報を収集するには、Flow Collector が情報を受信でき、Manager（旧 StealthWatch 管理コンソール）によってフロー プロキシ レコード ページに情報が表示されるように、プロキシサーバーログを設定する必要があります。このページには、プロキシ サーバーを経由するネットワーク内のトラフィックの URL とアプリケーション名が表示されます。

このドキュメントでは、さまざまなプロキシ サーバーのログを設定するために必要なさまざまな手順について説明します。対象サーバーは、Blue Coat、McAfee、Cisco WSA、Squid です。このドキュメントでは、プロキシ サーバーがネットワークの一部としてすでに実行されていることを前提としています。手順では、フロー コレクタに必要なファイルが指定され、情報が提供されるように、プロキシのログを設定する方法について説明します。

Secure Network Analytics プロキシログを設定するには、次の手順を実行します。

1. プロキシ サーバーを設定します。
   a. Blue Coat
   b. McAfee
   c. Cisco WSA
   d. Squid
2. フロー コレクタを設定します。
3. フローを確認します。

設定時の重要なガイドライン

いずれかのプロキシのログを設定する場合、必ず次のガイドラインに従う必要があります。

- フロー コレクタとプロキシは、フロー レコードとプロキシ レコードを一致させるために、同じ NTP サーバーを使用するか、共通のソースから時間を受信する必要があります。
- フロー コレクタの IP アドレスを設定するときに、プロキシ ログで調査する必要があるエクスポータとエンド ポイントからデータを収集するフロー コレクタを選択してください。
- Secure Network Analytics によって課される syslog プロキシメッセージには、特定のサイズ制限はありません。ただし、プロキシと Flow Collector の間のパスに沿った最短の最大伝送ユニット（MTU）よりも短いメッセージを保持することを推奨します（通常は 1500）。これにより、パケットフラグメンテーションが解消され、信頼性が向上します。
- プロキシログは、ハイアベイラビリティ（HA）モードではサポートされていません。

Blue Coat プロキシ ログの設定

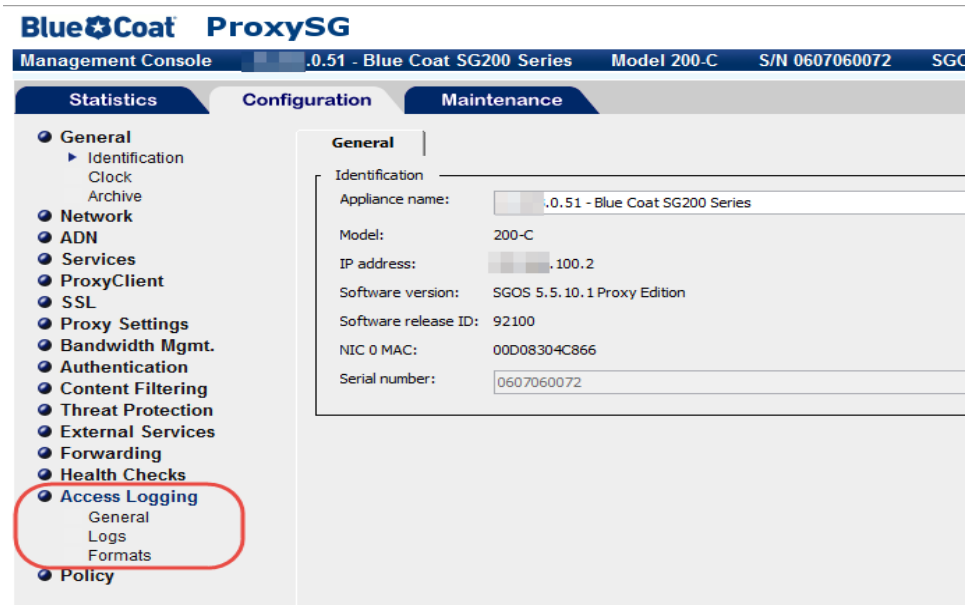
この章では、Secure Network Analytics に配信するために Blue Coat プロキシログを設定する手順について説明します。

> テストに使用された Blue Coat プロキシ バージョンは、SG V100、SGOS 6.5.5.7 SWG Edition でした。

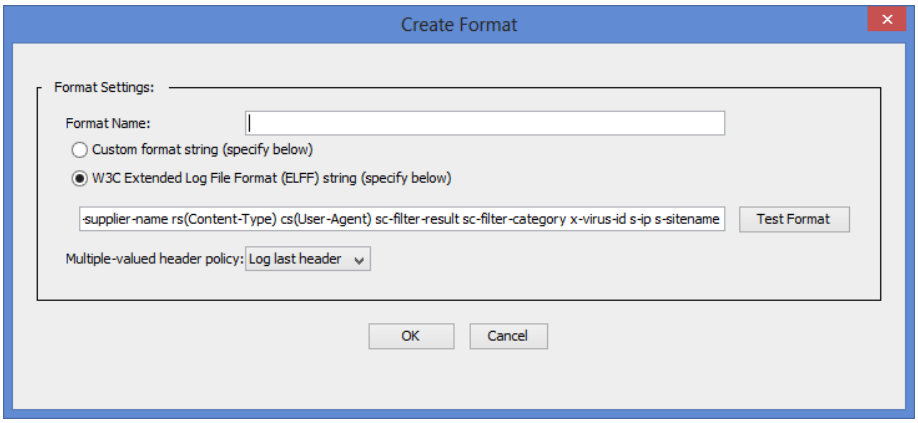
形式の作成

新しいログ形式を作成するには、次の手順を実行します。

1. ブラウザで、Blue Coat プロキシ サーバーにアクセスします。
2. [設定（Configuration）] タブをクリックします。



3. 管理コンソールのメインメニューで、[アクセスログ（Access Logging）] > [形式（Formats）] をクリックします。
4. ページの下部にある [新規（New）] をクリックします。[形式の作成（Create Format）] ページが開きます。



5. [形式名（Format Name）] フィールドに、新しい形式の名前を入力します。
6. [W3C拡張ログファイル形式（ELFF）（W3C Extended Log File format（ELFF））] のオプションを選択します。
7. [形式（Format）] フィールドに、次の文字列を入力します。

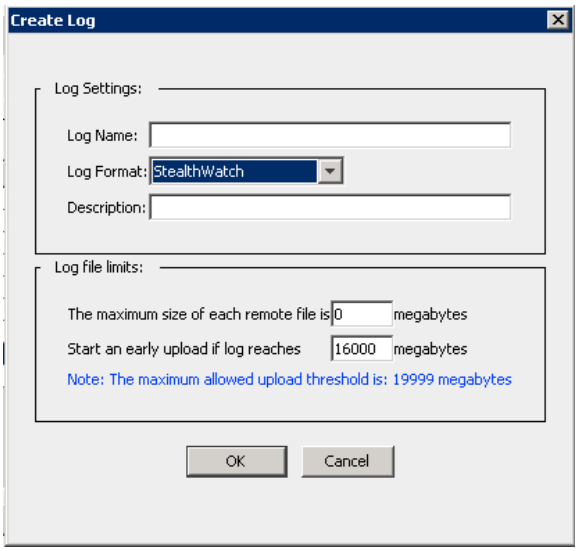
```
timestamp duration c-ip c-port r-ip r-port s-ip s-port cs-bytes
sc-bytes cs-user cs-host cs-uri
```

8. [OK] をクリックします。次の項「**新規ログの作成**」に進みます。

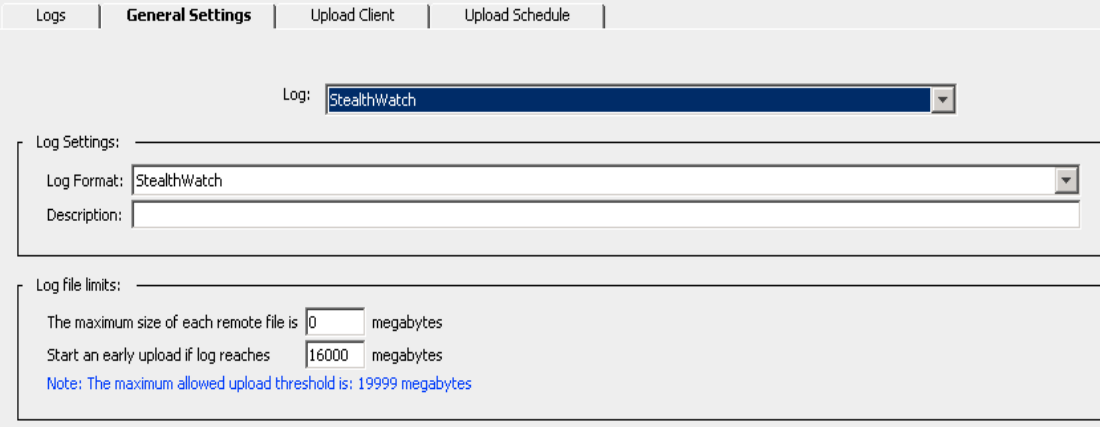
新規ログの作成

ログを作成するには、次の手順に従います。

1. メインメニューで、[アクセスログ（Access Logging）] > [ログ（Logs）] をクリックし、新しいログ形式を選択します。[ログ（Log）] ページが開きます。



2. [General Settings] タブをクリックします。

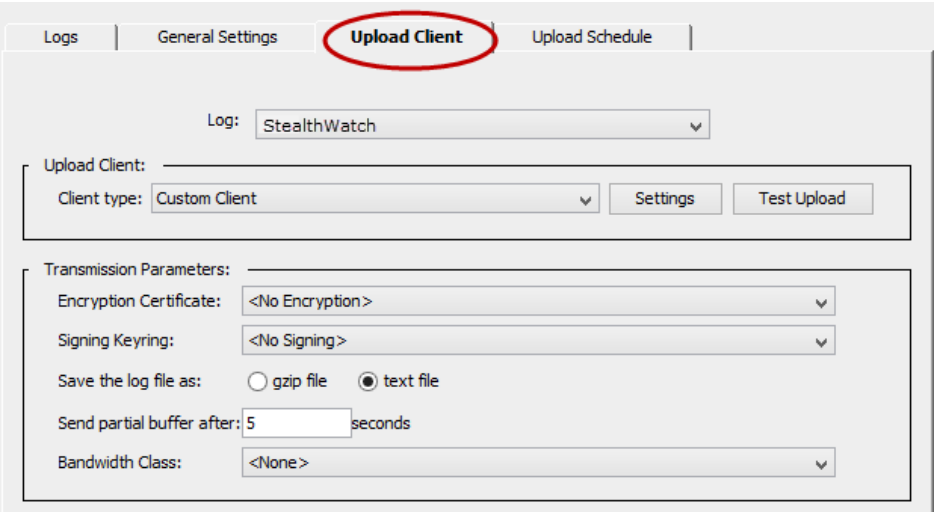


3. [ログ形式(Log Format)]ドロップダウン リストから、手順 1 で作成したログを選択します。
4. [説明(Description)]フィールドに、新規ログの説明を入力します。
5. ページの下部にある [適用(Apply)] ボタンをクリックします。次の項「**アップロードクライアントの設定**」に進みます。

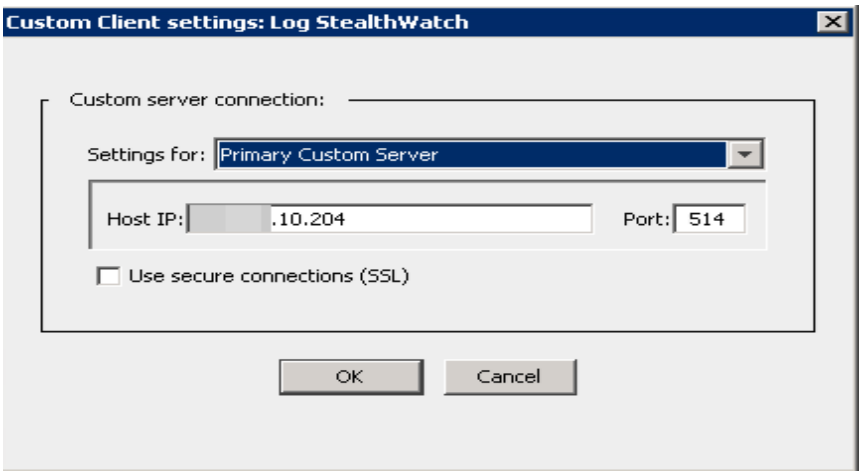
アップロードクライアントの設定

アップロード クライアントを設定するには、次の手順を実行します。

1. [アップロードクライアント(Upload Client)]タブをクリックします。[アップロード クライアント(Upload Client)] ページが開きます。



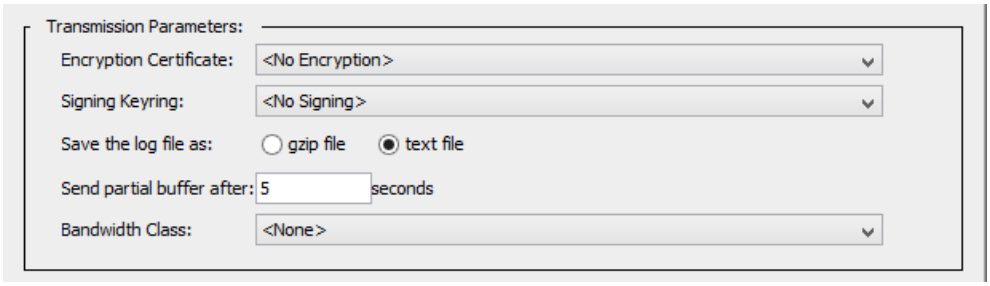
2. [クライアントタイプ(Client type)]ドロップダウン リストから、[カスタムクライアント(Custom Client)]を選択します。
3. [設定(Settings)] ボタンをクリックします。[カスタムクライアント設定(Custom Client settings)] ページが開きます。



4. 該当するフィールドに、フロー コレクタの IP アドレスとプロキシ パーサーのリスニング ポートを入力します。

> この時点では SSL はサポートされていません。

5. [OK] をクリックします。



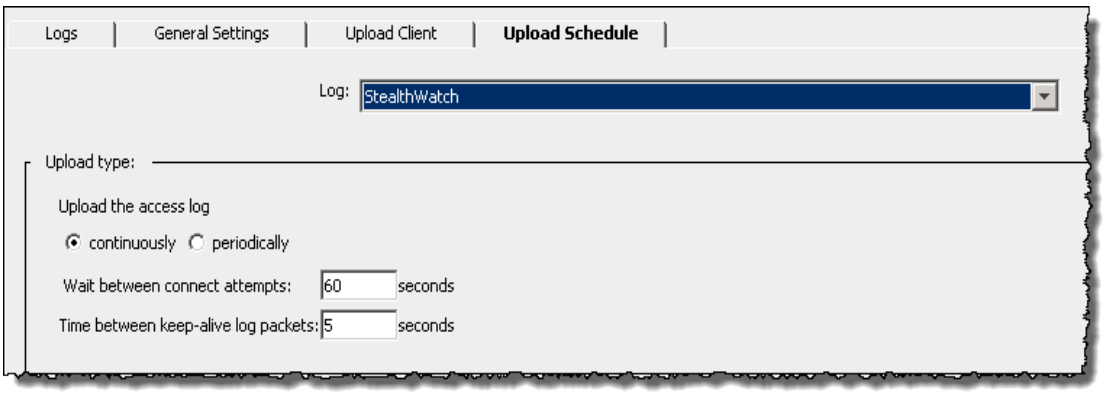
6. 送信パラメータでは、次の手順を実行します。
   a. [暗号化証明書(Encryption Certificate)] で、[暗号化なし(No encryption)] を選択します。
   b. [キーリングの署名(Signing Keyring)] ドロップダウン リストから、[署名なし(no signing)] を選択します。
   c. [ログ ファイルの保存形式(Save the log file as)] から、[テキスト ファイル(Text file)] オプションを選択します。
   d. [部分バッファを送信するまでの時間(Send partial buffer after)] テキスト ボックスに **5** と入力します。
   e. [アップロードスケジュール(Upload Schedule)] タブをクリックし、[アクセスログのアップロード(Upload the access log)] で [継続的(continuously)] オプションを選択します。
   f. [接続試行の間隔(Wait between connect attempts)] フィールドに **60** と入力します。
   g. [キープアライブログパケット間の時間(Time between keep-alive log packets)] フィールドに **5** と入力します。

7. ページ下部の [適用(Apply)] ボタンをクリックします。次の項「**アップロードスケジュールの設定**」に進みます。

アップロードスケジュールの設定

アップロード スケジュールを設定するには、次の手順を実行します。

1. [アップロードスケジュール(Upload Schedule)] タブをクリックします。



2. [アクセスログのアップロード(Upload the access log)] で [継続的(continuously)] を選択します。
3. [接続試行の間隔(Wait between connect attempts)] は **60** 秒です。
4. [キープアライブログパケット間の時間(Time between keep-alive log packets)] は **5** 秒です。
5. ページ下部の [適用(Apply)] ボタンをクリックします。

これで、フロー コレクタの Blue Coat プロキシ ログの設定が完了しました。

注記

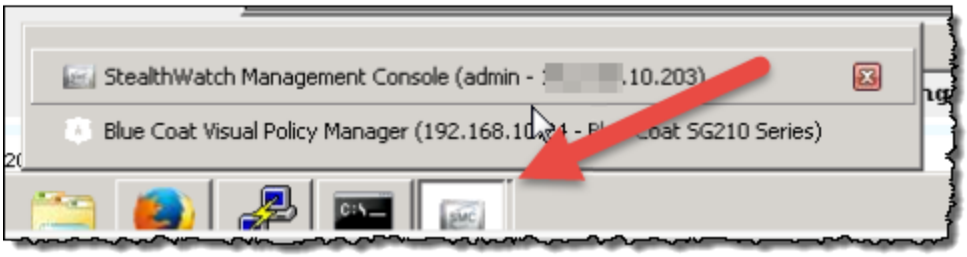
設定に関する補足説明を示します。

- フロー コレクタとプロキシは、フロー レコードとプロキシ レコードを一致させるために、同じ NTP サーバーにあるか、共通のソースから時間を受信する必要があります。
- サポートされているプロキシのログ出力メカニズムは 1 つのみです。特定の理由ですでにログをエクスポートしている場合は、プロキシ レコードを取得して解析することはできません。
- UDP はサポートされていません。

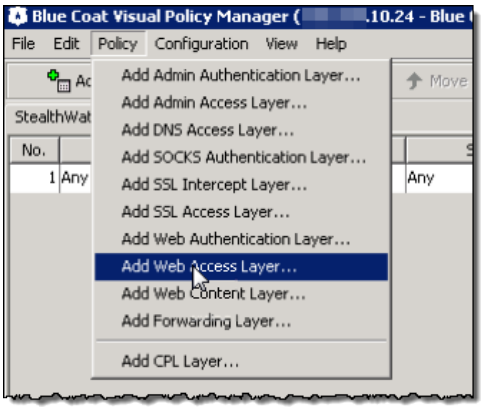
Visual Policy Manager の設定

Visual Policy Manager の設定を使用すると、プロキシ ログがフロー コレクタに送信されていることを確認できます。

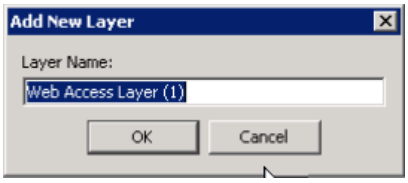
1. メインメニューの [設定（Configuration）] タブページで、[ポリシー（Policy）] > [Visual Policy Manager] をクリックします。Visual Policy Manager が開きます。



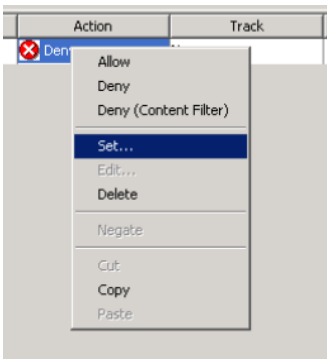
2. 設定されているログの下部にある [起動（Launch）] ボタンをクリックします。ログ ウィンドウの Visual Policy Manager が開きます。



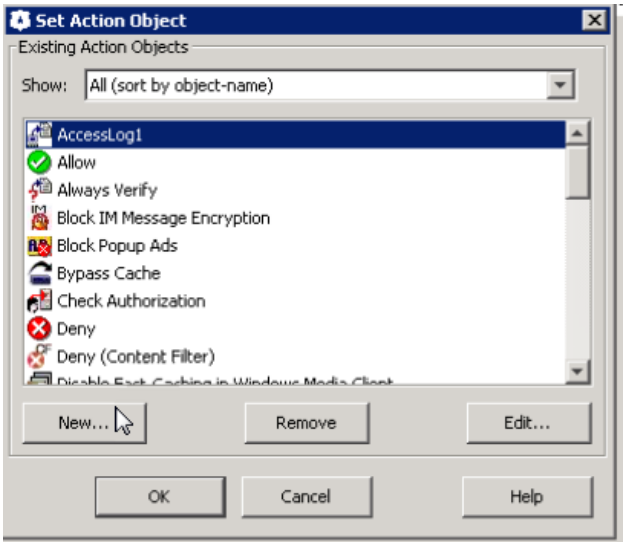
3. [ポリシー（Policy）] > [Webアクセスレイヤを追加（Add Web Access Layer）] をクリックします。[新規レイヤの追加（Add New layer）] 画面が表示されます。



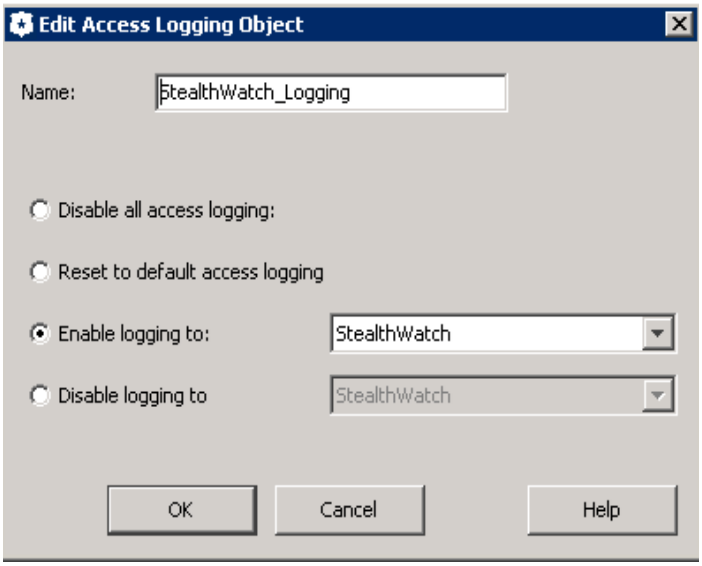
4. 新しいレイヤの名前を入力して、[OK] をクリックします。



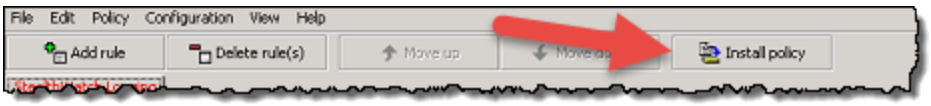
5. [アクション(Action)] 列の [拒否(Deny)] を右クリックしてから、[設定(Set)] をクリックします。[アクションオブジェクトの設定(Set Action Object)] ダイアログが開きます。



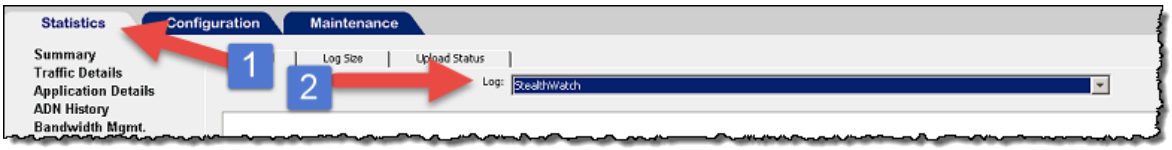
6. [新規(New)] をクリックし、[アクセスログを変更(Modify Access Logging)] を選択します。[アクセスログオブジェクトの編集(Edit Access Logging Object)] ダイアログが表示されます。



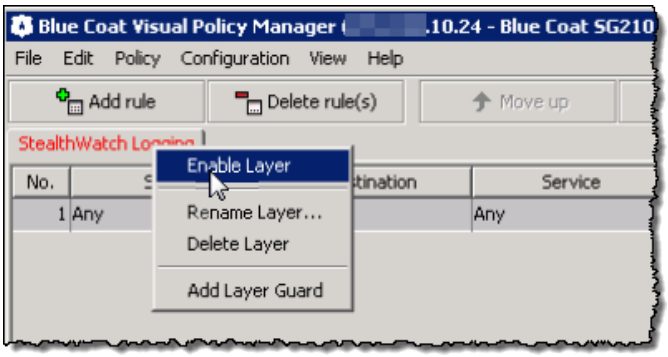
7. [次へのログを有効化（Enable logging to）] をクリックします。
8. ログの名前を入力し、ログを選択します。
9. [OK] をクリックします。オブジェクトが追加されます。
10. [アクションオブジェクトの設定（Set Action Object）] ダイアログで、**[OK]** をクリックします。



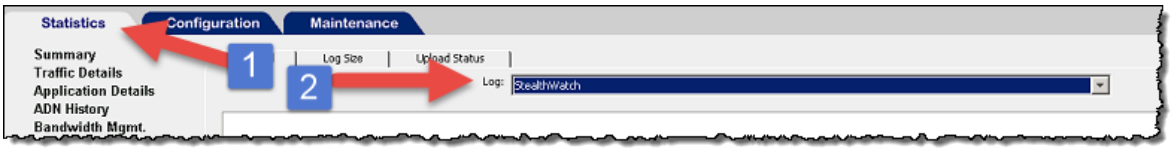
11. 右上にある [ポリシーをインストール（Install Policy）] ボタンをクリックします。
12. [いいえ（No）] をクリックし、次のウィンドウで [OK] をクリックします。



13. Blue Coat Visual Policy Manager を再度起動します。

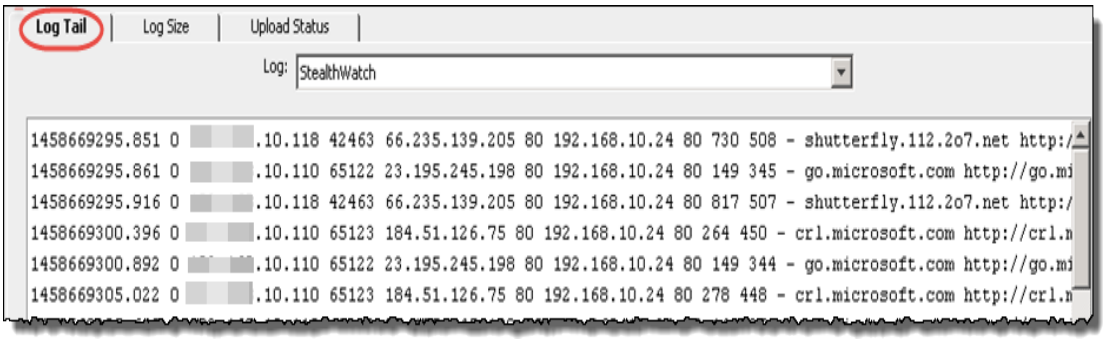


14. [ロギング（Logging）] タブを右クリックしてから、[レイヤの有効化（Enable Layer）] を選択します。
15. [ポリシーをインストール（Install Policy）] ボタンをクリックします。[インストールされたポリシー（Policy Installed）] が開きます。
16. [OK] をクリックします。

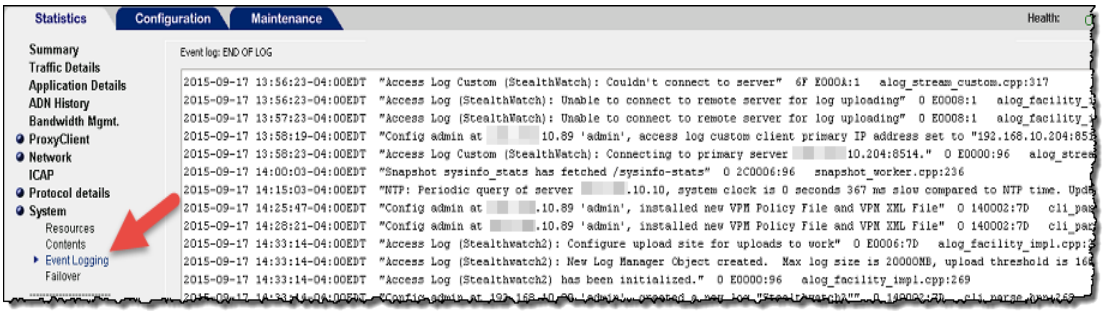


17. [統計（Statistics）] タブをクリックし、ログ メニューでログを選択します。

18. メイン メニューで、[アクセスログ（Access Logging）] をクリックしてから、[ログテール（Log Tail）] タブをクリックします。[ログ テール（Log Tail）] ウィンドウが開きます。



19. ページの下部にある [テールの開始 (Start Tail)] ボタンをクリックします。
20. 統計のメイン メニューで、[システム (System)] > [イベントロギング (Event Logging)] をクリックします。このページでは、ログ ファイルがフロー コレクタにアップロードされ、変更が行われたかどうかを示します。プロキシがフロー コレクタに接続されているかどうかを示します。



21. 続いて「フロー コレクタの設定」の章に進み、syslog 情報を受信するようにフロー コレクタを設定します。

McAfee プロキシ ログの設定

この章では、Secure Network Analytics に配信するために McAfee Web Gateway の McAfee プロキシログを設定する手順について説明します。

- McAfee プロキシの XML 構成ファイルをダウンロードしていることを確認してください。**Cisco Software Central** に移動して、readme およびプロキシログ XML 構成ファイルをダウンロードします。
- https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。
- テストに使用された McAfee プロキシ バージョンは 7.4.2.6.0 – 18721 でした。

McAfee プロキシ ログを設定するには、次の手順を実行します。

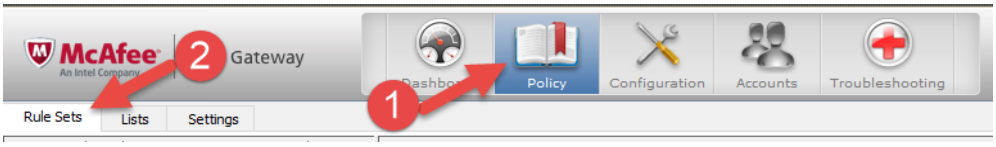
1. XML ファイル（FlowCollector_[date]_McAfee_Log_XML_Config_[v].xml）をダウンロードし、それを適切な場所に保存します。

「date」は XML ファイルの日付を示し、「v」は McAfee プロキシ バージョンのバージョンを示します。必ず McAfee プロキシと同じバージョン番号の XML ファイルを選択してください。

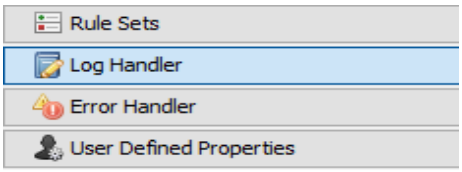
次の手順に従って取得します。

a. **Cisco Software Central**（https://software.cisco.com）に移動します。
b. [ダウンロードと管理（Download and manage）] > [ダウンロードとアップグレード（Download and Upgrade）] セクションで、[ダウンロードに**アクセス**（Access downloads）] を選択します。
c. [製品の選択（Select a Product）] フィールドまで下にスクロールします。
d. [製品の選択（Select a Product）] フィールドで「Cisco Secure Network Analytics」と入力します。[Enter] キーを押します。
e. Secure Network Analytics Virtual Flow Collector または別のフローコレクタを選択します。
f. [Cisco Secure Network Analytics システムソフトウェア（Secure Network Analytics System Software）] > [構成ファイル（Configuration Files）] を選択します。

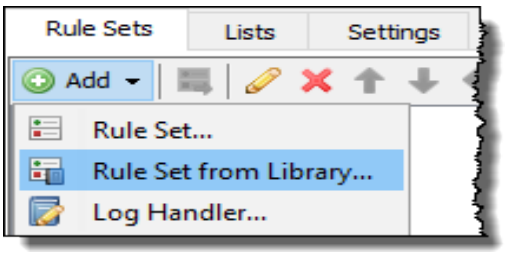
2. McAfee プロキシ サーバーにログインします。



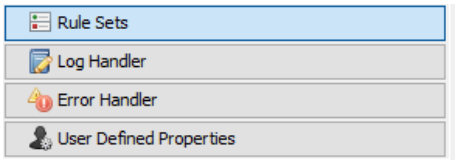
3. [ポリシー(Policy)] アイコンをクリックし、[ルールセット(Rule Sets)] タブをクリックします。



4. [ログ ハンドラ(Log Handler)] を選択し、[デフォルト(Default)] を選択します。



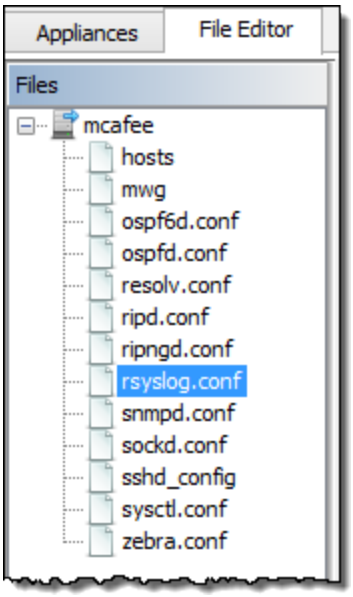
5. [追加(Add)] > [ライブラリのルールセット(Rule Set from the Library)] をクリックします。



6. [ファイルからのインポート(Import from file)] をクリックし、XML ファイルを選択します。
7. インポートされたログ ハンドラから [mcafeelancopelog] を選択します。

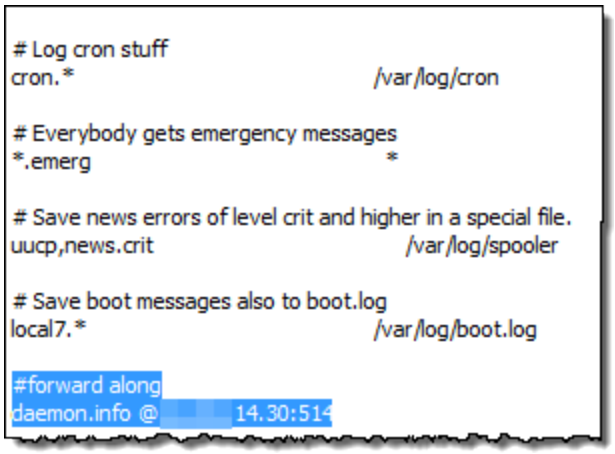
> ルール セットと「create access logline」および「send to syslog」のルールが有効になっていることを確認します。

8. ページの上部にある [設定(Configuration)] アイコンをクリックします。
9. ページの左側にある [ファイルエディタ(File Editor)] タブをクリックし、rsyslog.conf ファイルを選択します。



10. テキストボックスの下部に（ファイルリストの横）、次のテキストを入力します。

    `daemon.info @[FlowCollector IP Address:514]`



> プロキシログで調査する必要があるエクスポータとエンドポイントからデータを収集する Flow Collector を選択していることを確認してください。

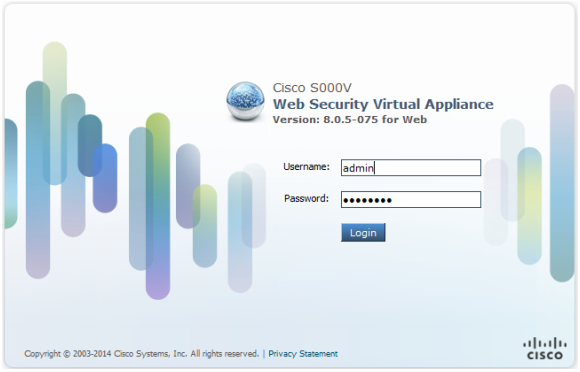
11. 次の行をコメント アウトします。`*.info;mail.none;authpriv.none;cron.none`
12. 次の行を追加します。
    `*.info;daemon.!=info;mail.none;authpriv.none;cron.none -/var/log/messages`
13. ページの右上にある［変更の保存（Save Changes）］ボタンをクリックします。
14. 続いて「フロー コレクタの設定」の章に進み、syslog 情報を受信するようにフロー コレクタを設定します。

Cisco Web Security Appliance (WSA) プロキシ ログの設定

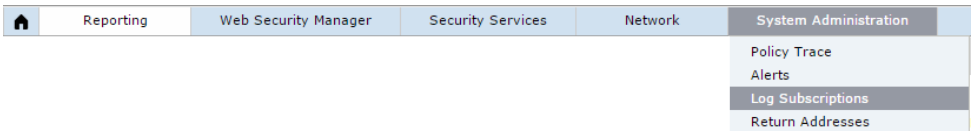
この章では、Secure Network Analytics に配信するために Cisco プロキシログを設定する手順について説明します。

> Cisco WSA プロキシは、プロキシ デバイスの追加に関して仮想 IP をサポートしていません。

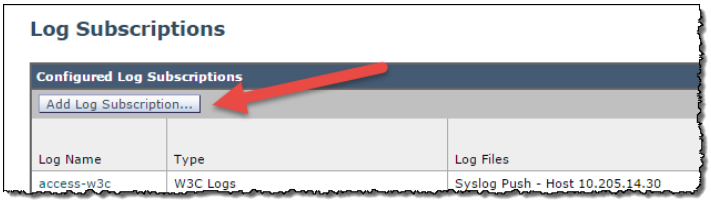
Cisco プロキシ ログを設定するには、次の手順を実行します。



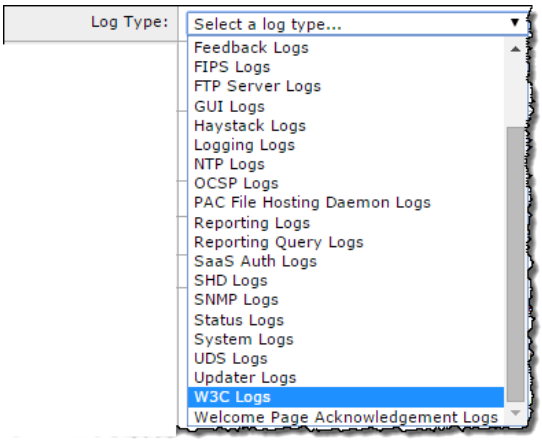
1. Cisco プロキシ サーバーにログインします。



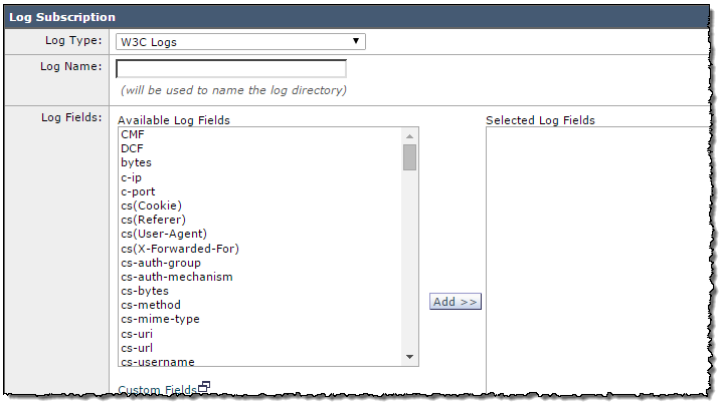
2. メイン メニューで、[システム管理(System Administration)] > [ログサブスクリプション(Log Subscriptions)] をクリックします。[ログサブスクリプション(Log Subscriptions)] ページが開きます。



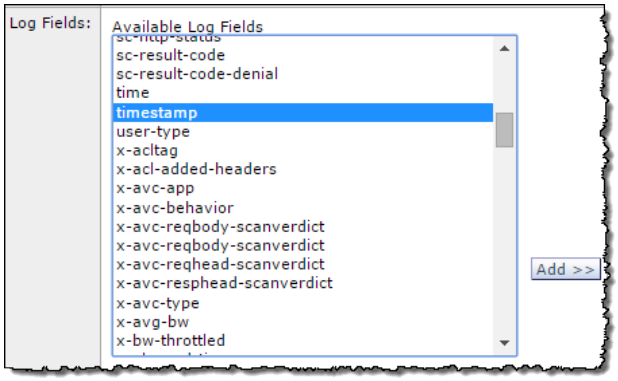
3. [ログサブスクリプションを追加(Add Log Subscriptions)] ボタンをクリックします。新しい [ログサブスクリプション(Log Subscriptions)] ページが開きます。



4. [ログ タイプ(Log Type)]ドロップダウン リストから、[W3C ログ(W3C Logs)]を選択します。使用可能な W3C ログ フィールドが表示されます。

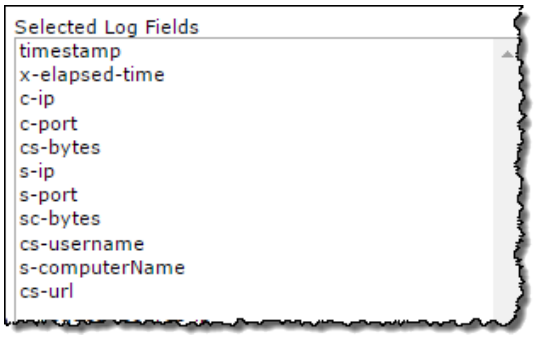


5. [ログ名(Log Name)]フィールドに、使用するログの名前を入力します。
6. [使用可能なログフィールド(Available Log Fields)]リストから[タイムスタンプ(Timestamp)]を選択し、[追加(Add)]をクリックして[選択されたログフィールド(Selected Log Fields)]リストに移動させます。



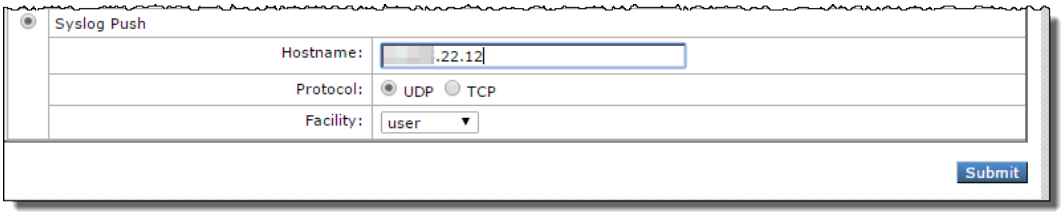
7. 次の各ログフィールドに対して前の手順を順に繰り返します。
    a. timestamp
    b. x-elapsed-time
    c. c-ip
    d. c-port
    e. cs-bytes
    f. s-ip
    g. s-port
    h. sc-bytes
    i. cs-usernames
    j. s-computerName
    k. cs-url

    [選択されたログ フィールド(Selected Log Fields)] リストには、これらのフィールドが図のように含まれている必要があります。



⚠ 選択したログフィールドリストは、上記の順序で、他のフィールドは存在しない必要があります。

8. ページの下部までスクロールし、[Syslog送信(Syslog Push)] オプションを選択します。



9. [ホスト名(Hostname)] フィールドに、フロー コレクタの IP アドレスまたはプロキシがログを送信するホスト名を入力します。

ℹ プロキシログで調査する必要があるエクスポータとエンドポイントからデータを収集する Flow Collector を選択していることを確認してください。

10. [送信(Submit)] をクリックします。新しいログが [ログサブスクリプション(Log Subscriptions)] リストに追加されます。
11. 続いて「**Flow Collector の設定**」の章に進み、syslog 情報を受信するように Flow Collector を設定します。

Squid プロキシ ログの設定

この章では、Secure Network Analytics に配信するために Squid プロキシログを設定する手順について説明します。ログを設定するには、SSH を使用してプロキシ サーバー上のファイルを編集する必要があります。

Squid プロキシ ログを設定するには、次の手順を実行します。

1. Squid を実行しているマシンのシェルにログインします。
2. squid.conf が含まれているディレクトリ（通常は /etc/squid）に移動して、それをエディタで開きます。
3. squid.conf に次の行を追加して、ロギングを設定します。

```
logformat access_format %ts%03tu %<tt %>a %>p %>st %<A %<st %<la
%<lp %la %lp %un %ru

access_log syslog:user.6 access_format
```

4. 次を使用して squid を再起動します。

```
/etc/init.d/squid3 restart
```

5. フロー コレクタにログを転送するように、Squid サーバーの syslog サービスを設定します。これは Linux ディストリビューションによって異なりますが、syslog-ng の場合は次を /etc/syslog-ng に追加します。

```
# Audit Log Facility BEGIN

filter bs_filter { filter(f_user) and level(info) };

destination udp_proxy { udp("10.205.14.15" port(514)); };

log {

source(s_all);

filter(bs_filter);

destination(udp_proxy);

};

# Audit Log Facility END
```

> プロキシログで調査する必要があるエクスポータとエンドポイントからデータを収集する Flow Collector を選択していることを確認してください。

6. `/etc/init.d/syslog-ng` restart を使用して `syslog-ng` を再起動します。
7. syslog 情報を受信するには、「フローコレクタの設定」に進みます。

Flow Collector の設定

プロキシ サーバーを設定したら、データを受信するようにフロー コレクタを設定する必要があります。

syslog 情報を受信するようにフロー コレクタを設定するには、次の手順を実行します。

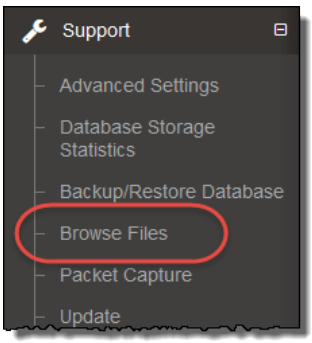
1. Manager にログインします。
2. [構成(Configure)] > [グローバル集中管理(GLOBAL Central Management)] を選択します。
3. Flow Collector の ••• (**省略符号**)アイコンをクリックし、[アプライアンス統計情報の表示(View Appliance Statistics)] をクリックします。Flow Collector のインターフェイスが開きます。
4. **[設定(Configuration)] > [プロキシの取得(Proxy Ingest)]** をクリックします。[プロキシサーバー(Proxy Servers)] ページが開きます。
5. プロキシサーバーの IP アドレスを入力します。
6. [プロキシタイプ(Proxy Type)] ドロップダウン リストから、プロキシ サーバーを選択します。

> プロキシ サーバーのタイプがリストにない場合、この時点ではプロキシ ログを使用できません。

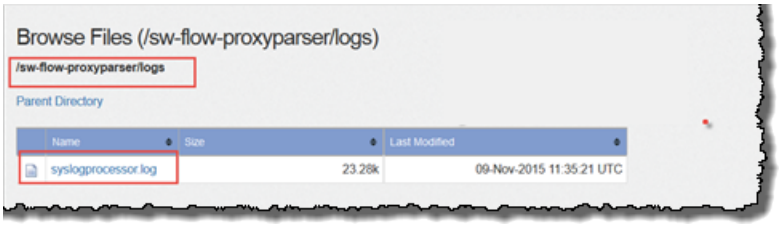
7. [プロキシ ID(Proxy ID)] フィールドに、プロキシ サーバーの IP アドレスを入力します。
8. [プロキシ サービス ポート(Proxy Service Port)] フィールドに、プロキシ サーバーのポート番号を入力します。
9. プロキシ サーバーによってアラームをトリガーするには、[アラームから除外(Excluded from Alarming)] チェックボックスをオフにします。
10. [追加(Add)] をクリックします。
11. [適用(Apply)] をクリックします。ページ上部にある [プロキシの取得(Proxy Ingest)] テーブルに、プロキシ サーバーが表示されます。
12. 次の章「**フローの確認**」に進みます。

フローの確認

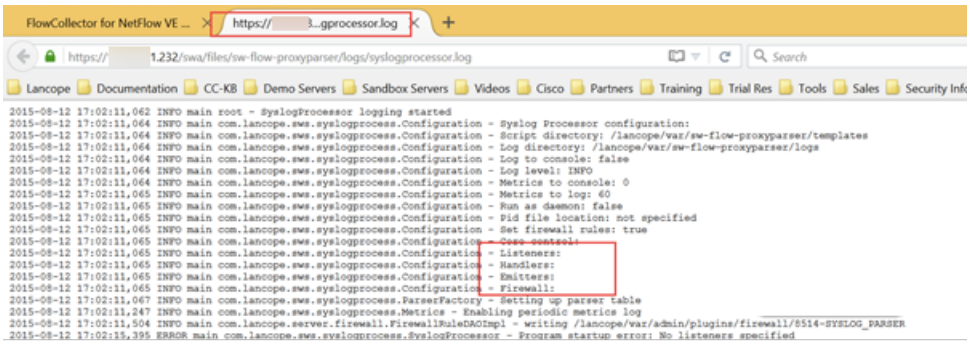
フローを受信していることを確認するには、次の手順を実行します。



1. Flow Collector のインターフェイスで、メインメニューの [サポート（Support）] > [ファイルの参照（Browse Files）] をクリックします。[ファイルの参照（Browse Files）] ページが開きます。



2. syslog ファイルを開きます。



3. マークされているファイルがブランクではないことを確認します。ブランクである場合、問題があります。
   - Listeners にはプロキシの数が表示されます。
   - Handlers は 1 つのみで、データを解析します。
   - Emitters はハンドラから解析済みのデータを取得し、エンジンが求めている形式に変換します。
   - ファイアウォール

4. カウントが増加し、データの受信を示していることを確認します。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2024 年 1 月 17 日	最初のバージョン。

著作権情報