Cisco Stealthwatch

バージョン 7.0 プロキシ ログ設 定ガイド

目次

はじめに

概要

Stealthwatch システム プロキシ ログのネット ワーク プロキシ サーバからユーザ情報を収集するには、フロー コレクタが情報を受信でき、SMC 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 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。

Stealthwatch 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 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。

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。
- Cisco Stealthwatch サポートのお問い合わせ先 :
- 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：www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

Blue Coat プロキシ ログの設定

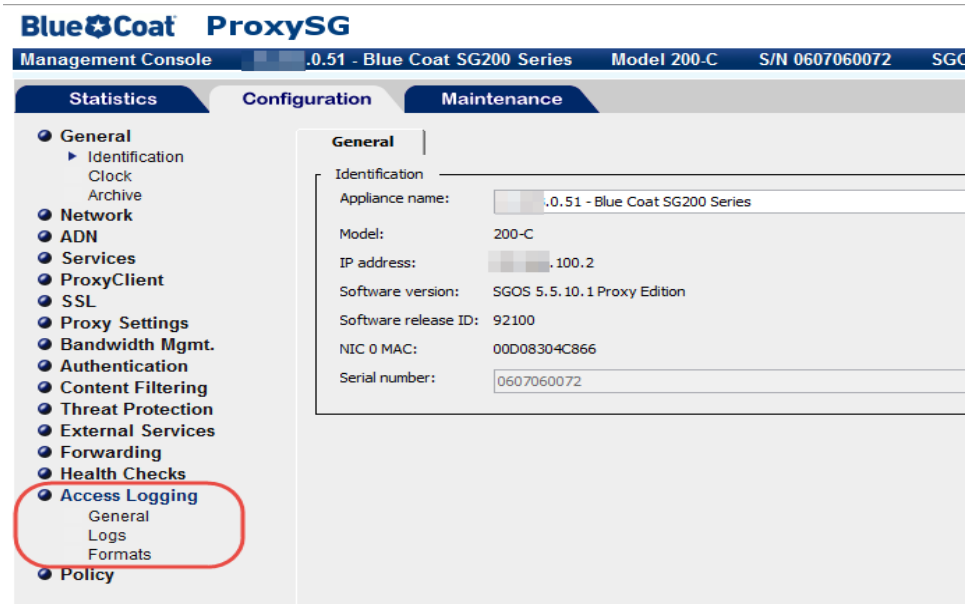
この章では、Stealthwatch システムに配信するために Blue Coat プロキシ ログを設定する手順について説明します。

> 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。

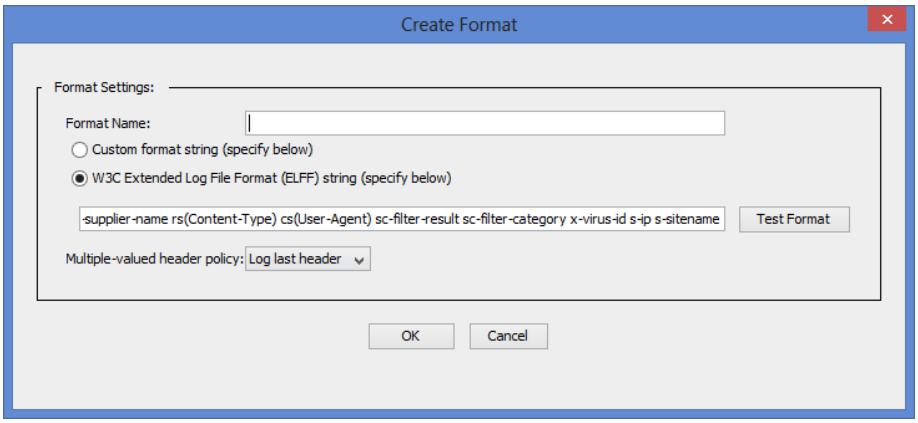
形式の作成

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。

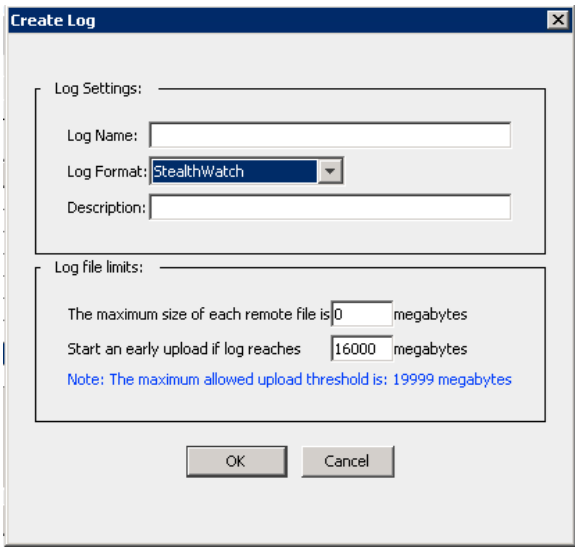
```
timestamp duration c-ip c-port r-ip r-port s-ip s-port cs-bytes sc-bytes cs-user cs-host cs-uri
```

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。

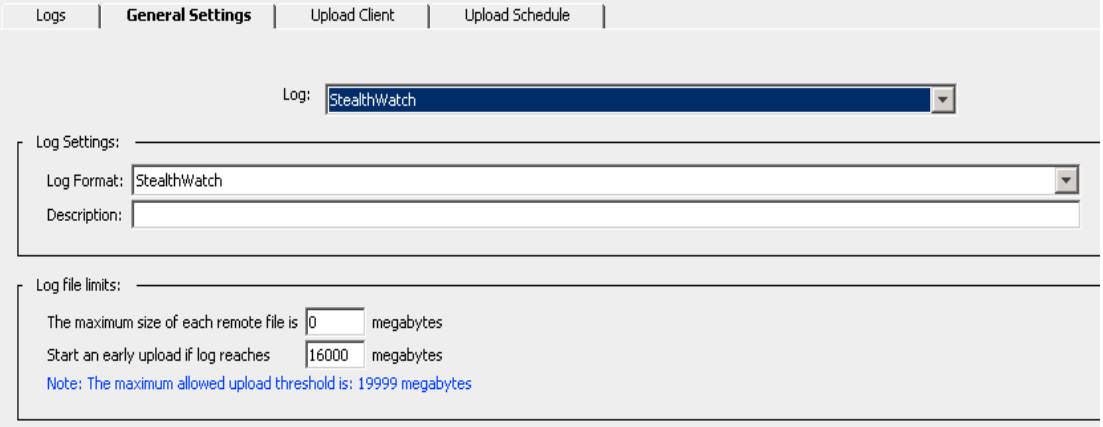
新規ログの作成

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. [一般設定(General Settings)]タブをクリックします。

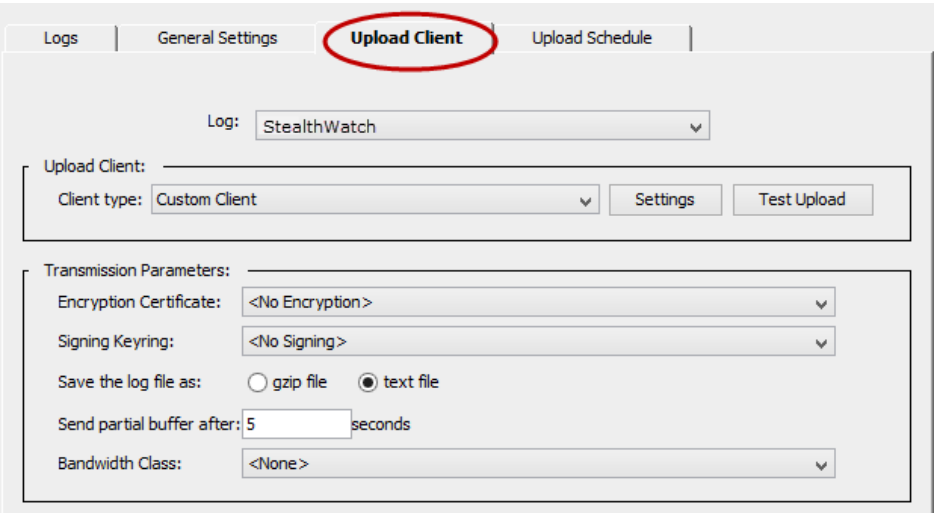


3. [ログ形式(Log Format)]ドロップダウンリストから、手順 1 で作成したログを選択します。
4. [説明(Description)]フィールドに、新規ログの説明を入力します。
5. ページの下部にある [適用(Apply)] ボタンをクリックします。次の項「アップロード クライアントの設定」に進みます。

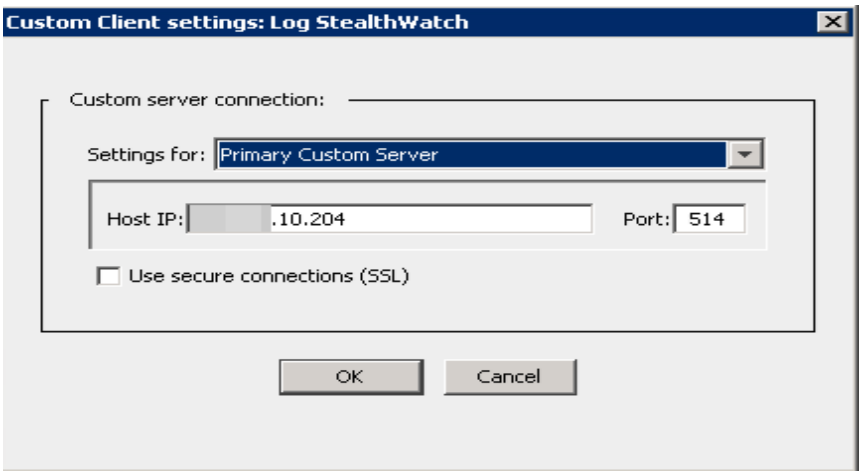
アップロード クライアントの設定

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。



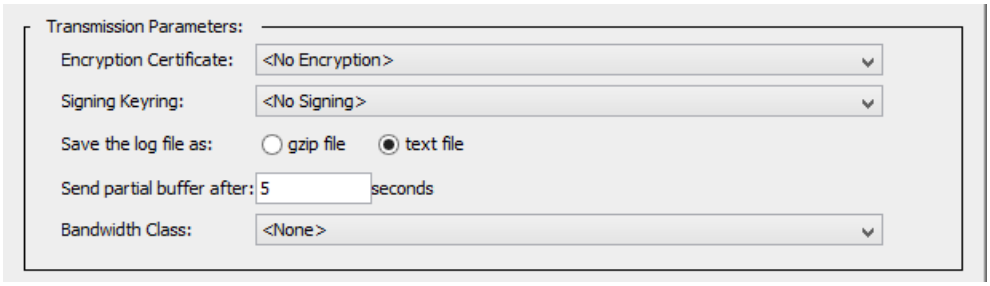
2. [クライアントタイプ(Client type)]ドロップダウンリストから、[カスタムクライアント(Custom Client)]を選択します。
3. [設定(Settings)] ボタンをクリックします。[カスタムクライアント設定(Custom Client settings)]ページが開きます。



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。



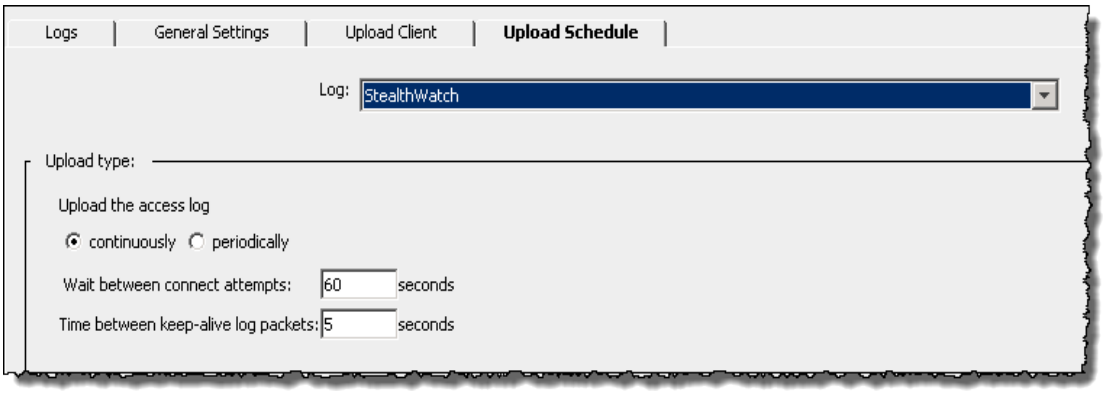
6. 送信パラメータでは、次の手順を実行します。
   a. [暗号化証明書 (Encryption Certificate)] で、[暗号化なし(No encryption)] を選択します。
   b. [キーリングの署名 (Signing Keyring)] ドロップダウン リストから、[署名なし(no signing)] を選択します。
   c. [ログファイルの保存形式 (Save the log file as)] から、[テキスト ファイル(Text file)] オプションを選択します。
   d. [部分バッファを送信するまでの時間 (Send partial buffer 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)

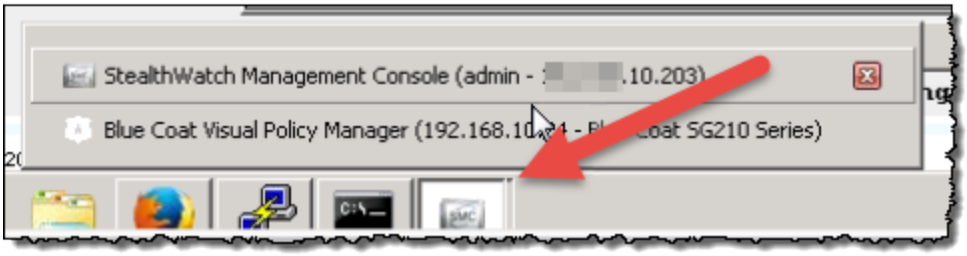
設定に関する補足説明を示します。

- 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。

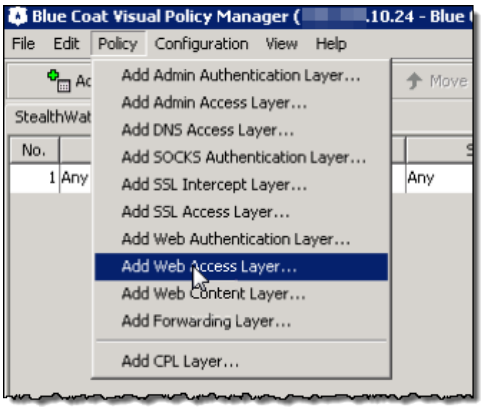
Visual Policy Manager の設定

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。

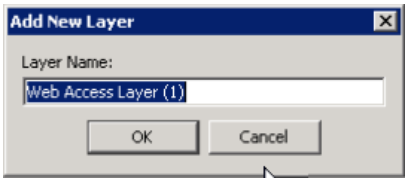
1. メイン メニューの [設 定 (Configuration)] タブ ページで、[ポリシー(Policy)] > [Visual Policy Manager] をクリックします。Visual Policy Manager が開きます。



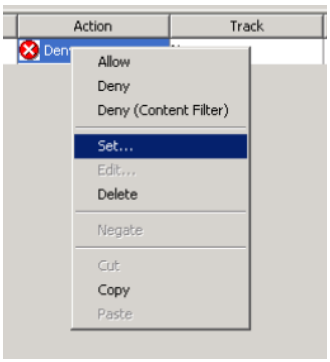
2. 設 定されているログの下 部 にある [起 動 (Launch)] ボタンをクリックします。ログ ウィンドウの Visual Policy Manager が開きます。



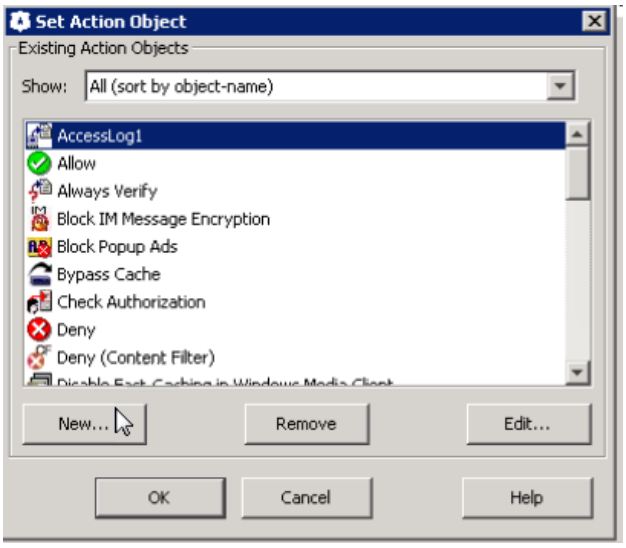
3. [ポリシー(Policy)] > [Webアクセスレイヤを追 加 (Add Web Access Layer)] をクリックします。[新 規 レイヤの追 加 (Add New layer)] 画 面 が表 示 されます。



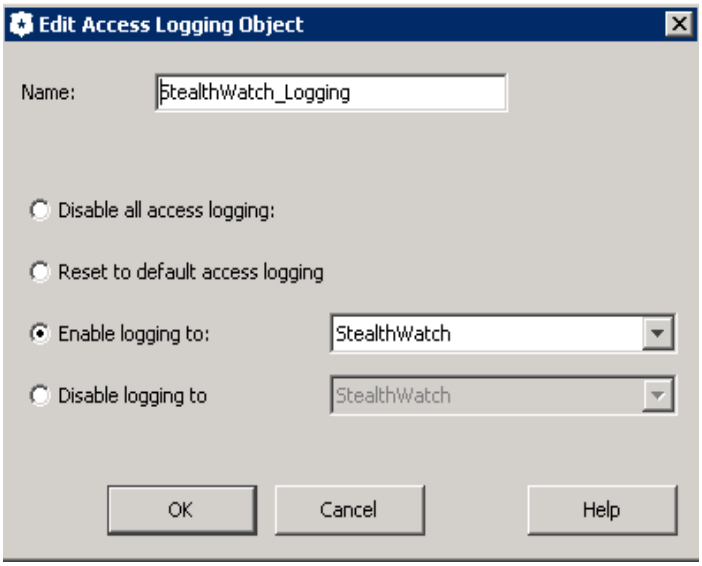
4. 新 しいレイヤの名 前 を入 力 して、[OK] をクリックします。



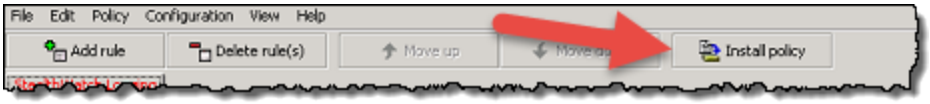
5. [アクション(Action)] 列 の [拒 否 (Deny)] を右 クリックしてから、[設 定 (Set)] をクリックしま す。[アクションオブジェクト の設 定 (Set Action Object)] ダイアログが開きます。



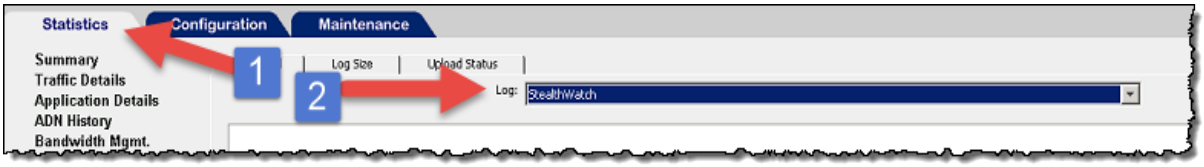
6. [新 規 (New)] をクリックし、[アクセスログを変 更 (Modify Access Logging)] を選 択します。[アクセスログオブジェクト の編 集 (Edit Access Logging Object)] ダイアログが表 示 されます。



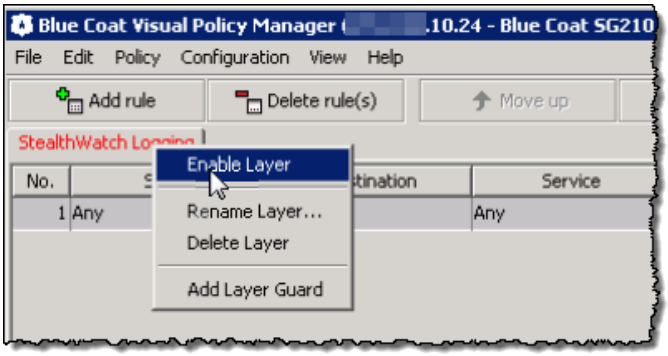
7. [次 へのログを有 効 化 (Enable logging to)] をクリックします。
8. ログの名 前 を入 力 し、ログを選 択 します。
9. [OK] をクリックします。オブジェクト が追 加 されます。
10. [アクションオブジェクト の設 定 (Set Action Object)] ダイアログで、[OK] をクリックします。



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。



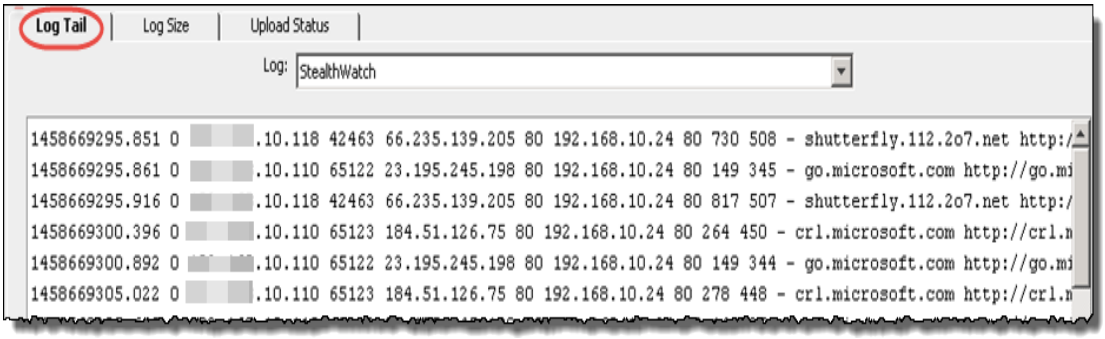
13. Blue Coat Visual Policy Manager を再 度 起 動 します。



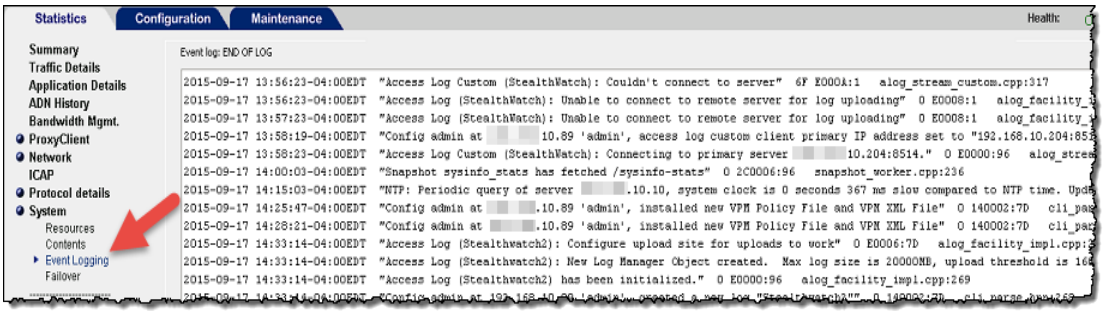
14. [ロギング(Logging)] タブを右 クリックしてから、[レイヤの有 効 化 (Enable Layer)] を選 択しま す。
15. [ポリシーをインスト ール(Install Policy)] ボタンをクリックします。[インスト ールされたポリシー (Policy Installed)] が開きます。
16. [OK] をクリックします。

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、Stealthwatch システムに配信するために 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 コンフィギュレーション 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。Stealthwatch ダウンロードおよびライセンス センター (https://stealthwatch.flexnetoperations.com) にアクセスして、ファイル、Readme、プロキシ ログの XML コンフィギュレーション ファイルを取得します。
- 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。

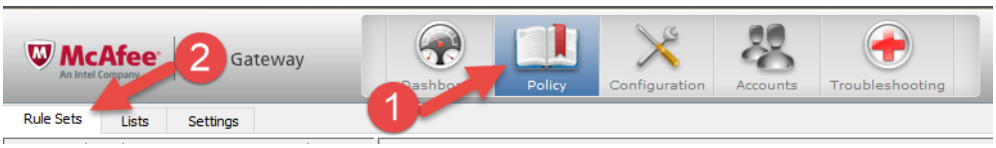
1. XML ファイル (FlowCollector_[date]_McAfee_Log_XML_Config_[v].xml) をダウンロードし、適切な場所に保存します。

「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。

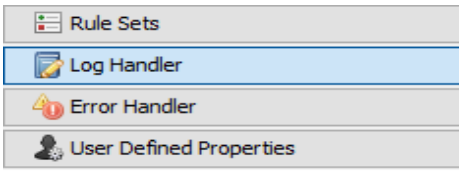
次の手順に従って取得します。

a. Stealthwatch ダウンロードおよびライセンス センター (https://stealthwatch.flexnetoperations.com) にアクセスします。ログイン ページが開きます。
b. ログイン ID とパスワードを該当するフィールドに入力し、[ログイン (Login)] をクリックします。製品ホームページが開きます。
c. [ダウンロード (Downloads)] をクリックします。
d. リンク「vX.X Updates for the FlowCollector NetFlow Series」を選択します。
e. XML ファイルをダウンロードして保存します。

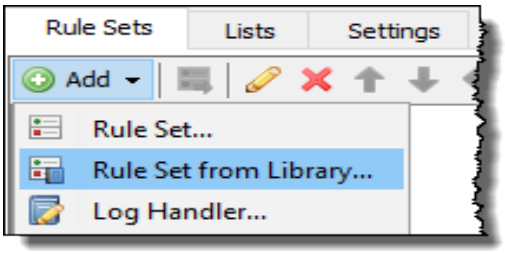
2. McAfee プロキシ サーバにログインします。



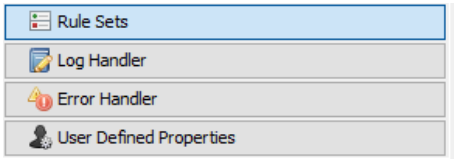
3. [ポリシー (Policy)] アイコンをクリックし、[ルールセット (Rule Sets)] タブをクリックします。



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。



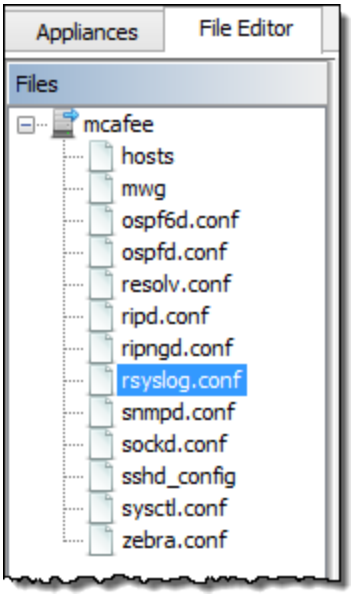
5. [追 加 (Add)] > [ライブラリのルールセット (Rule Set from the Library)] をクリックします。



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。

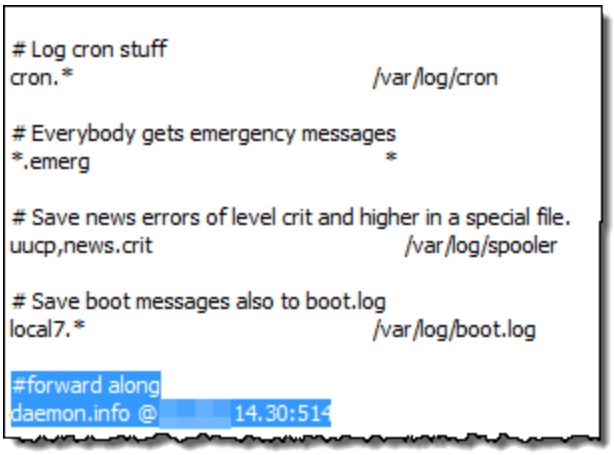
ルール セット と「create access logline」および「send to syslog」のルールが有 効 になって いることを確 認します。

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 (ファイル リスト の横) に、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フローコレクタを選択していることを確認してください。

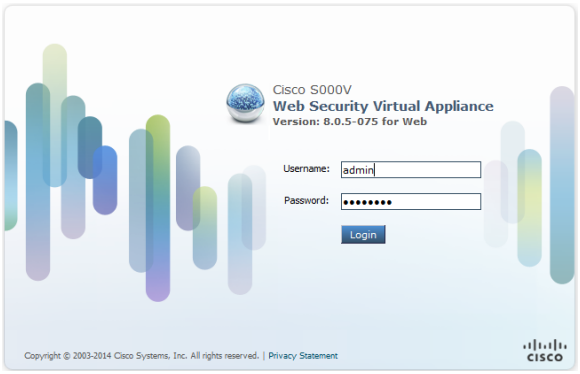
11. 次の行をコメント アウトします。
    `*.info;mail.none;authpriv.none;cron.none`
12. 次の行を追加します。
    `*.info;daemon.!=info;mail.none;authpriv.none;cron.none -/var/log/messages`
13. ページの右上にある [変更の保存 (Save Changes)] ボタンをクリックします。
14. 続いて「フローコレクタの設定」の章に進み、syslog 情報を受信するようにフローコレクタを設定します。

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

この章では、Stealthwatch システムに配信するために Cisco プロキシ ログを設定する手順について説明します。

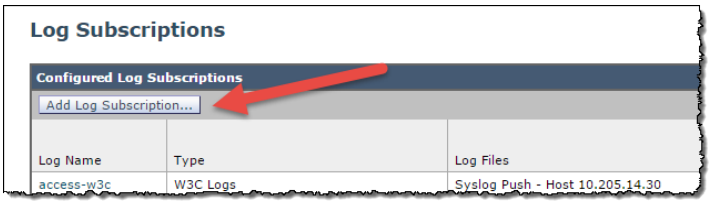
> Cisco WSA プロキシは、プロキシ デバイスの追加に関して仮想 IP をサポートしていません。

Cisco プロキシ ログを設定するには、次の手順を実行します。

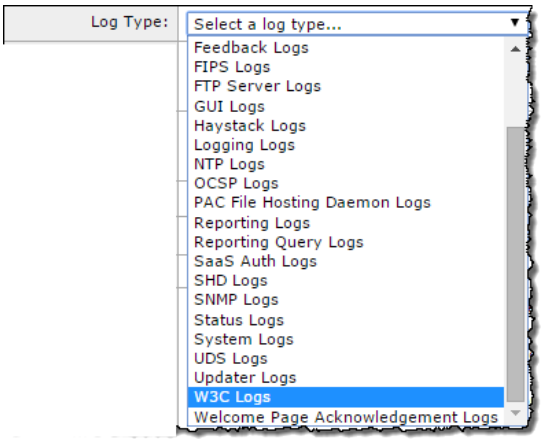


1. Cisco プロキシ サーバにログインします。

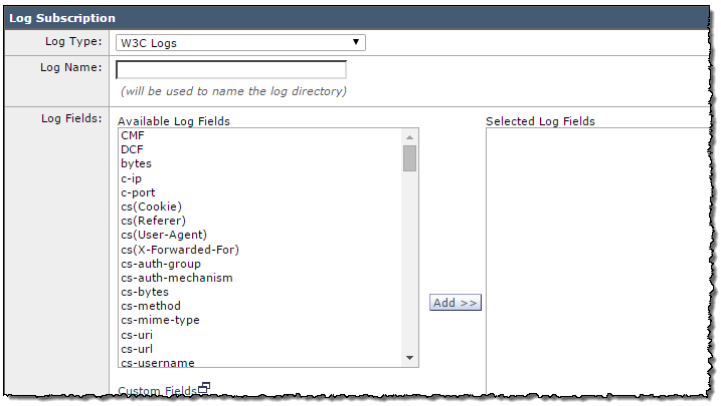
2. メイン メニューで、[システム管理 (System Administration)] > [ログサブスクリプション(Log Subscriptions)] をクリックします。[ログサブスクリプション(Log Subscriptions)] ページが開きます。



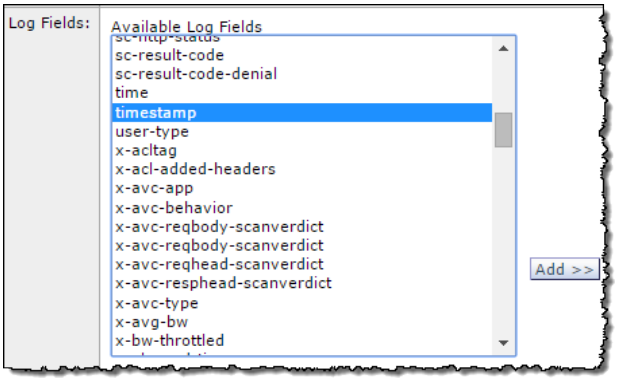
3. [ログサブスクリプションを追加 (Add Log Subscriptions)] ボタンをクリックします。新しい [ログサブスクリプション(Log Subscriptions)] ページが開きます。



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。



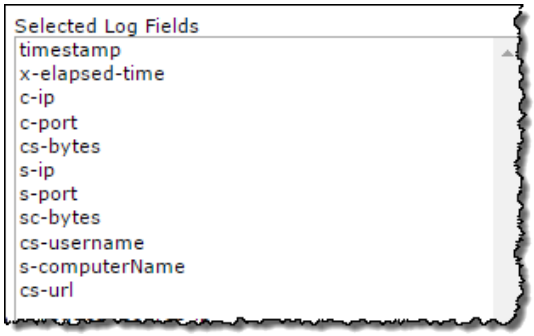
5. [ログ名 (Log Name)]フィールド に、使 用 するログの名 前を入 力します。



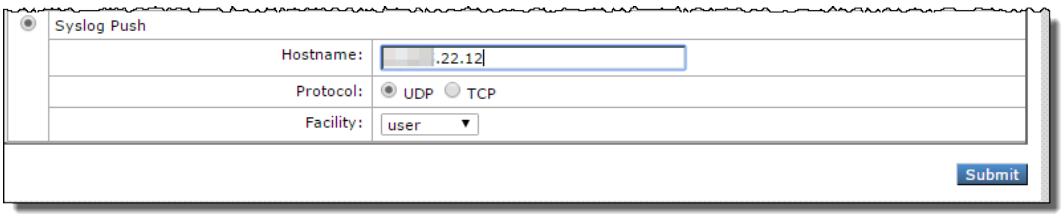
6. [使 用 可 能なログフィールド (Available Log Fields)]リスト から [タイムスタンプ(Timestamp)]を選 択し、[追 加 (Add)] をクリックして [選 択されたログフィールド (Selected Log Fields)]リスト に移 動させます。

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. x-elapsed-time
   b. c-ip
   c. c-port
   d. cs-bytes
   e. s-ip
   f. s-port
   g. sc-bytes
   h. cs-usernames
   i. s-computerName
   j. 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。



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。

> 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「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。

Squid プロキシ ログの設定

この章では、Stealthwatch システムに配信するために 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、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フローコレクタ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. 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。

フロー コレクタの設 定

プロキシ サーバを設 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。

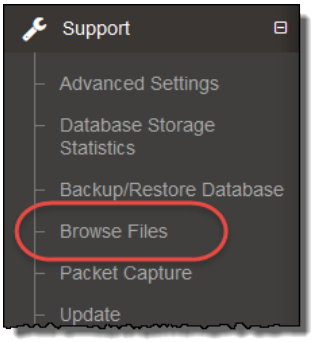
1. フロー コレクタの管 理 インターフェイスにログインします。
2. メイン メニューで、[設 定 (Configuration)] > [プロキシの取 得 (Proxy Ingest)] をクリックします。[プロキシ サーバ(Proxy Servers)] ページが開きます。
3. プロキシ サーバの IP アドレスを入 力します。
4. [プロキシタイプ(Proxy Type)] ドロップダウン リスト から、プロキシ サーバを選 択します。

> プロキシ サーバのタイプがリスト 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。

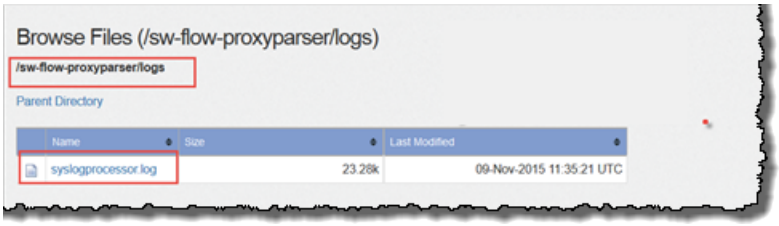
5. [プロキシID(Proxy ID)] フィールド に、プロキシ サーバの IP アドレスを入 力します。
6. [プロキシ サービス ポート (Proxy Service Port)] フィールド に、プロキシ サーバのポート 番 号 を入 力します。
7. プロキシ サーバによってアラームをトリガーするには、[アラームから除 外 (Excluded from Alarming)] チェックボックスをオフにします。
8. [追 加 (Add)] をクリックします。
9. [適 用 (Apply)] をクリックします。ページ上 部 にある [プロキシの取 得 (Proxy Ingest)] テーブルに、プロキシ サーバが表 示 されます。
10. 次 の章「フローの確 認 」に進 みます。

フローの確認

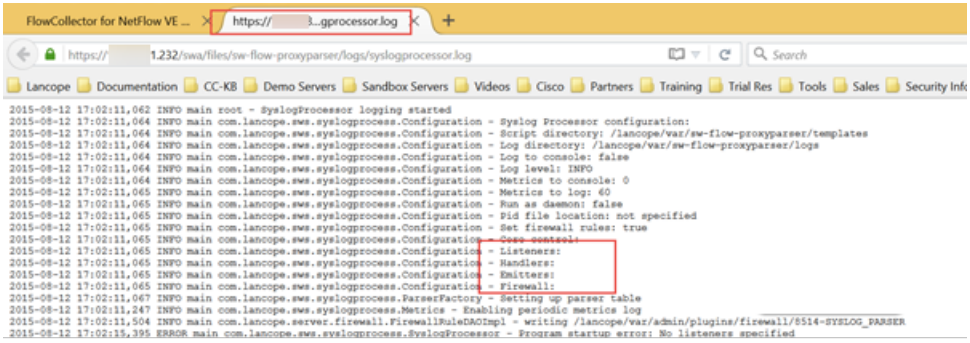
フローを受信していることを確認するには、次の手順を実行します。



1. フローコレクタの管理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。
   - エミッタ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。

著作権情報