

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	3
概要	3
設定時の重要なガイドライン	3
サポートへの問い合わせ	3
Blue Coat プロキシ ログの設定	5
形式の作成	5
新規ログの作成	6
アップロード クライアントの設定	7
アップロード スケジュールの設定	10
(注)	10
Visual Policy Manager の設定	10
McAfee プロキシ ログの設定	16
Cisco Web Security Appliance (WSA) プロキシ ログの設定	19
Squid プロキシ ログの設定	23
フローコレクタの設定	25
フローの確認	26

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ト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

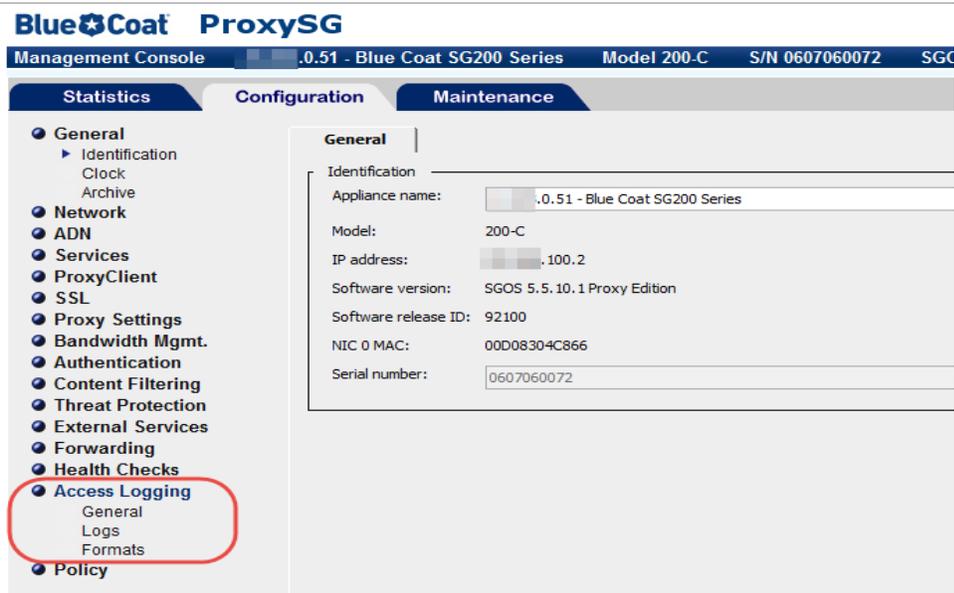
この章では、Stealthwatch システムに配信するために Blue Coat プロキシ ログを設定する手順について説明します。

i 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。

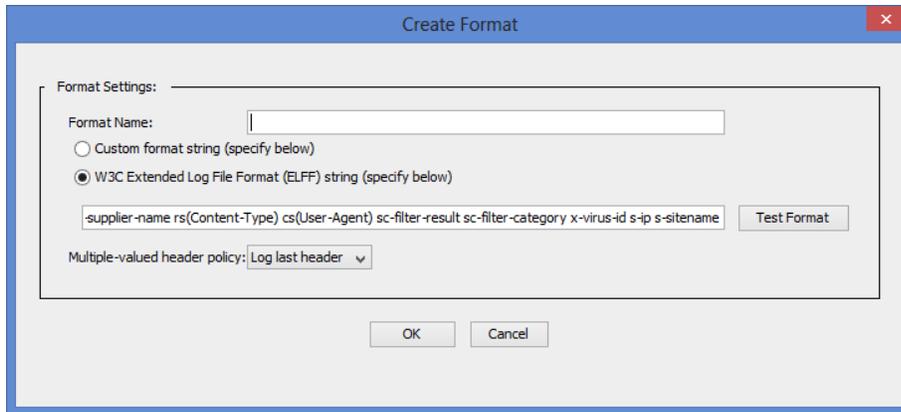
形式の作成

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。



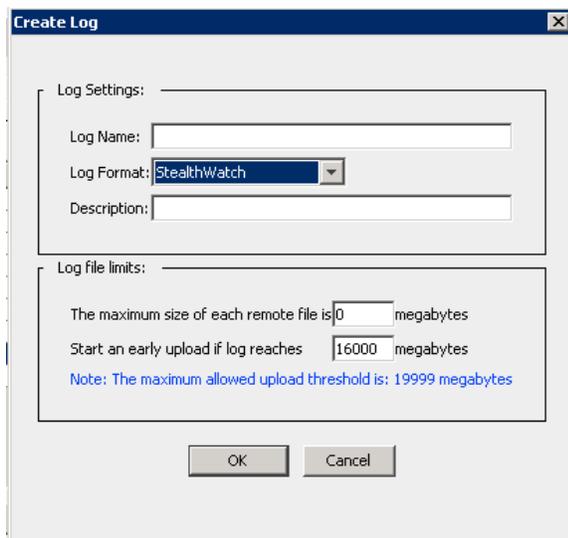
5. [形式名 (Format Name)] フィールドに、新しい形式の名前を入力します。
6. [W3C 拡張ログファイル形式 (ELFF) (W3C Extended Log File format (ELFF))] のオプションを選択します。
7. [形式 (Format)] フィールドに、次の文字列を入力します。

```
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。

Logs | **General Settings** | Upload Client | Upload Schedule

Log: StealthWatch

Log Settings:

Log Format: StealthWatch

Description:

Log file limits:

The maximum size of each remote file is 0 megabytes

Start an early upload if log reaches 16000 megabytes

Note: The maximum allowed upload threshold is: 19999 megabytes

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。

Logs | General Settings | **Upload Client** | Upload Schedule

Log: StealthWatch

Upload Client:

Client type: Custom Client Settings Test Upload

Transmission Parameters:

Encryption Certificate: <No Encryption>

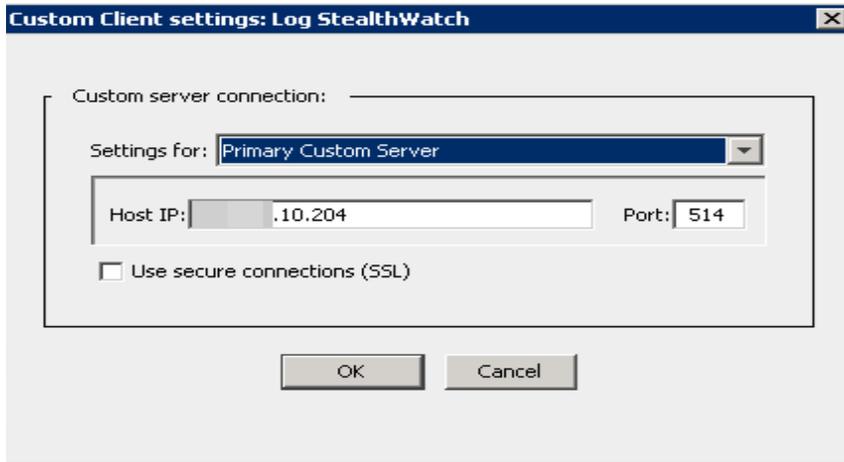
Signing Keyring: <No Signing>

Save the log file as: gzip file text file

Send partial buffer after: 5 seconds

Bandwidth Class: <None>

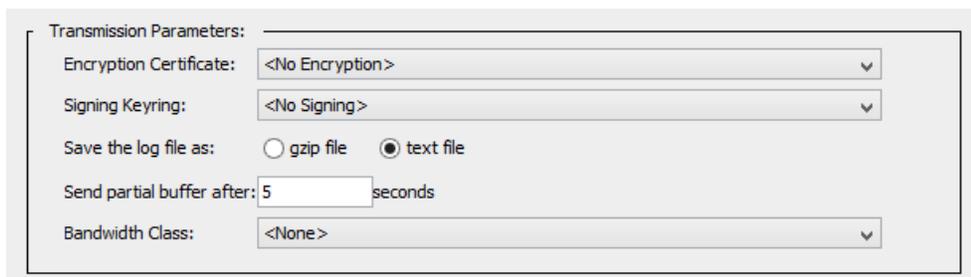
2. [クライアントタイプ (Client type)] ドロップダウンリストから、[カスタムクライアント (Custom Client)] を選択します。
3. [設定 (Settings)] ボタンをクリックします。[カスタムクライアント設定 (Custom Client settings)] ページが開きます。



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。

i 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。



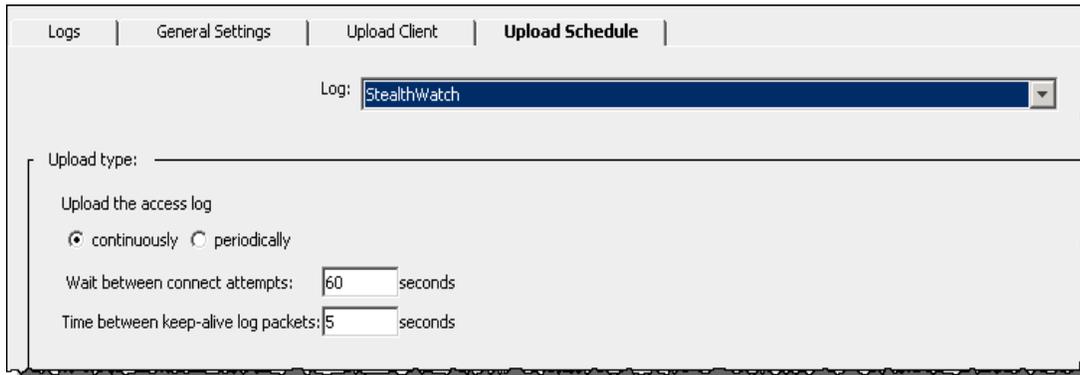
6. 送信パラメータでは、次の手順を実行します。
 - a. [暗号化証明書 (Encryption Certificate)] で、[暗号化なし (No encryption)] を選択します。
 - b. [キーリングの署名 (Signing Keyring)] ドロップダウンリストから、[署名なし (no signing)] を選択します。
 - c. [ログファイルの保存形式 (Save the log file as)] から、[テキストファイル (Text file)] オプションを選択します。
 - d. [部分バッファを送信するまでの時間 (Send partial buffer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

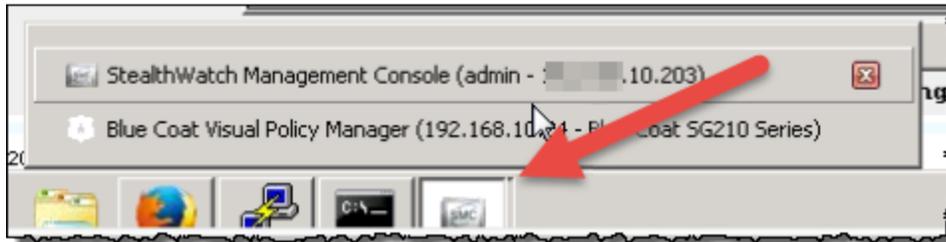
- フローコレクタとプロキシは、フローレコードとプロキシレコードを一致させるために、同じ NTP サーバにあるか、共通のソースから時間を受信する必要があります。
- サポートされているプロキシのログ出力メカニズムは1つのみです。特定の理由ですでにログをエクスポートしている場合は、プロキシレコードを取得して解析することはできません。
- UDP はサポートされていません。

Visual Policy Manager の設定

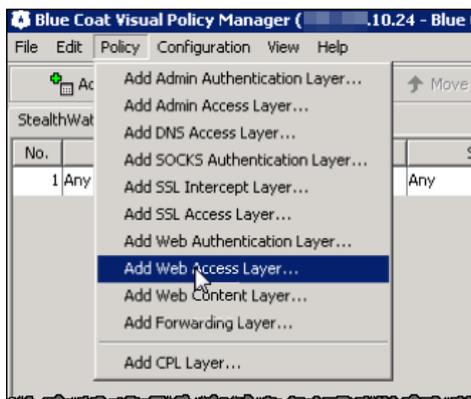
Visual Policy Manager の設定を使用すると、プロキシ ログがフローコレクタに送信されていることを確認できます。



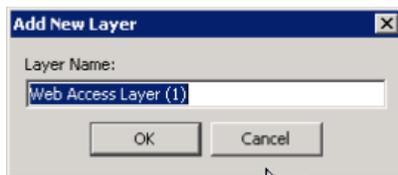
1. メインメニューの[設定 (Configuration)] タブ ページで、[ポリシー (Policy)] > [Visual Policy Manager] をクリックします。Visual Policy Manager が開きます。



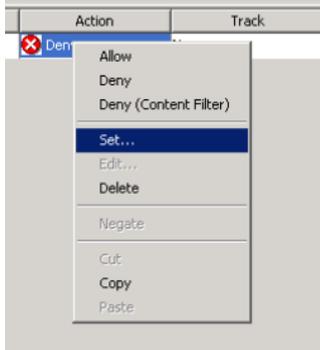
2. 設定されているログの下部にある[起動 (Launch)] ボタンをクリックします。ログ ウィンドウの Visual Policy Manager が開きます。



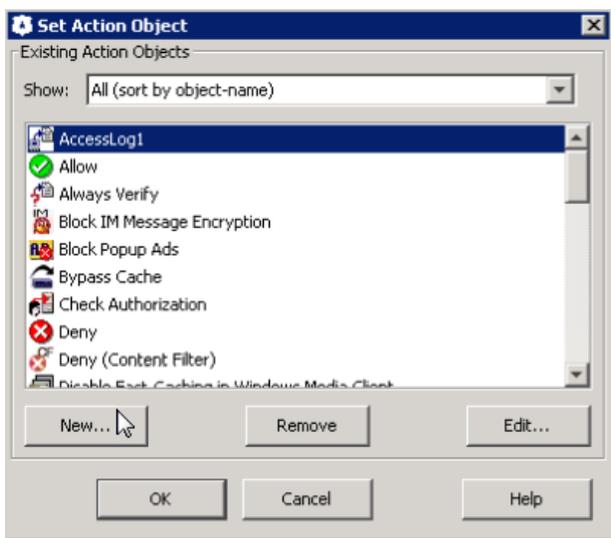
3. [ポリシー (Policy)] > [Webアクセスレイヤを追加 (Add Web Access Layer)] をクリックします。[新規レイヤの追加 (Add New layer)] 画面が表示されます。



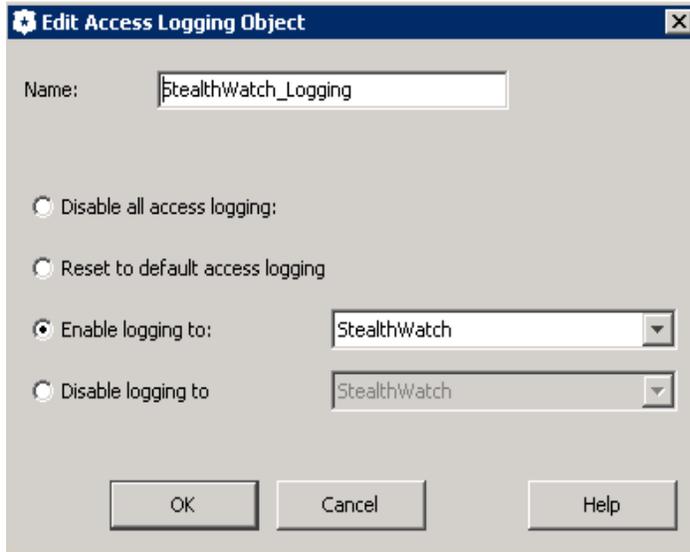
4. 新しいレイヤの名前を入力して、[OK] をクリックします。



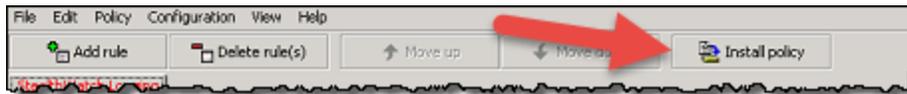
5. [アクション (Action)] 列の [拒否 (Deny)] を右クリックしてから、[設定 (Set)] をクリックします。[アクションオブジェクトの設定 (Set Action Object)] ダイアログが開きます。



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。



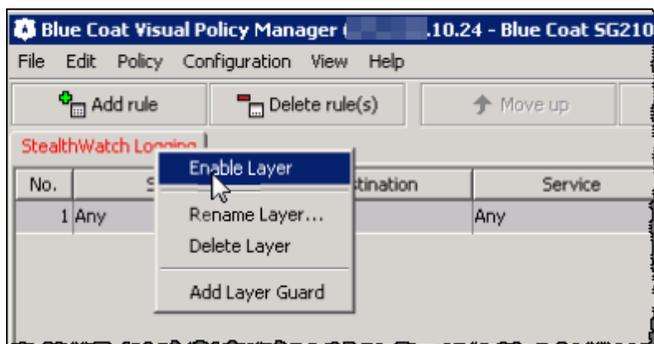
7. [次へのログを有効化 (Enable logging to)] をクリックします。
8. ログの名前を入力し、ログを選択します。
9. [OK] をクリックします。オブジェクトが追加されます。
10. [アクションオブジェクトの設定 (Set Action Object)] ダイアログで、[OK] をクリックします。



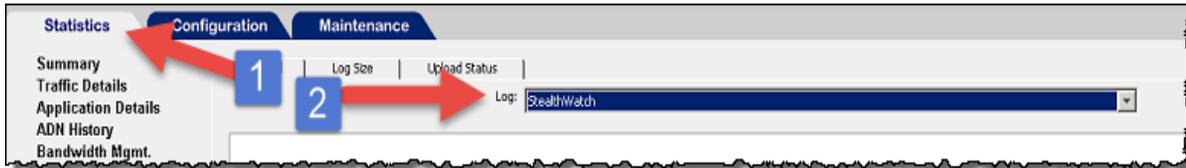
11. 右上にある [ポリシーをインストール (Install Policy)] ボタンをクリックします。
12. [いいえ (No)] をクリックし、次のウィンドウで [OK] をクリックします。



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



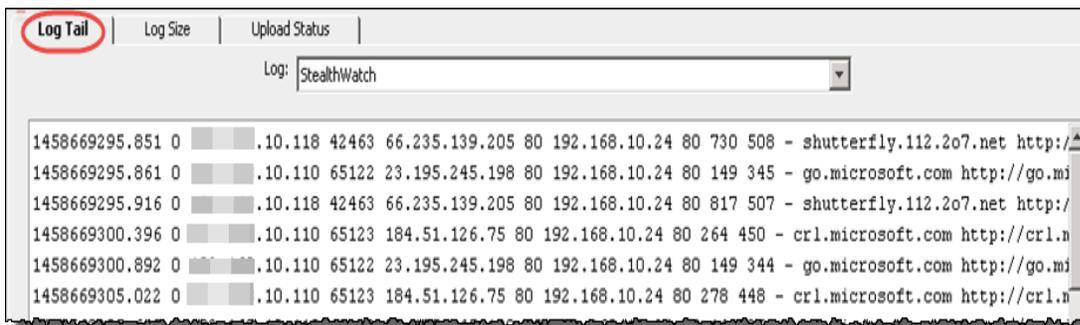
14. [ロギング(Logging)] タブを右クリックしてから、[レイヤの有効化 (Enable Layer)] を選択します。
15. [ポリシーをインストール(Install Policy)] ボタンをクリックします。[インストールされたポリシー (Policy Installed)] が開きます。
16. [OK] をクリックします。



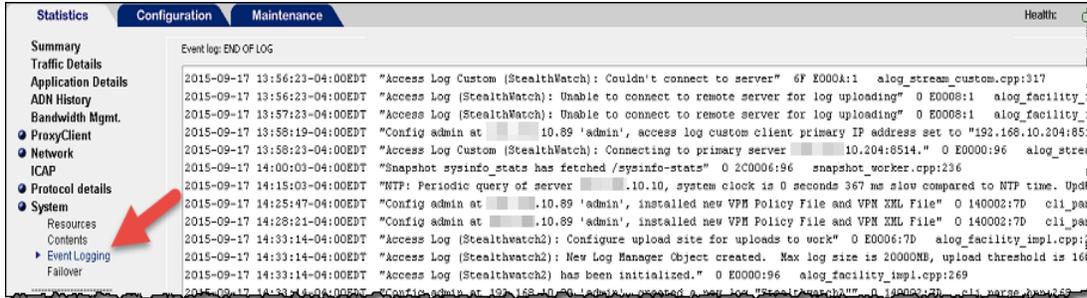
17. [統計 (Statistics)] タブをクリックし、ログメニューでログを選択します。



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。

i 「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。

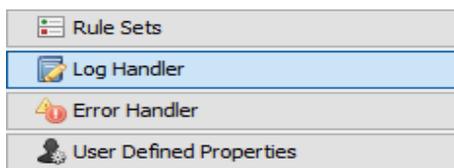
次の手順に従って取得します。

- 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。

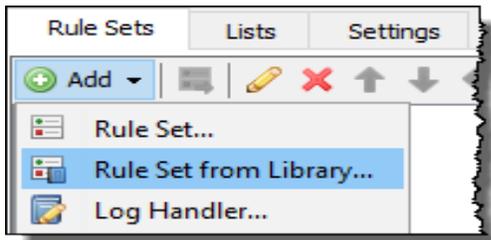
2. McAfee プロキシ サーバにログインします。



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。



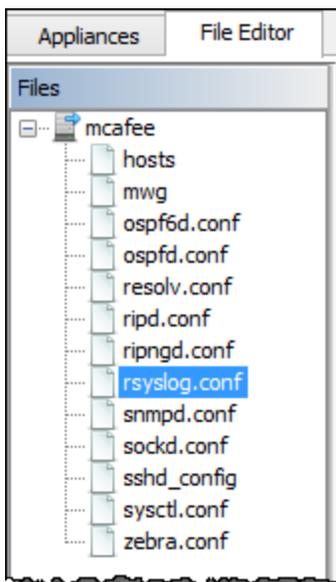
5. [追加(Add)] > [ライブラリのルールセット(Rule Set from the Library)] をクリックします。



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。

i 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]
```

```
# Log cron stuff
cron.*                /var/log/cron

# Everybody gets emergency messages
*.emerg               *

# Save news errors of level crit and higher in a special file.
uucp,news.crit       /var/log/spooler

# Save boot messages also to boot.log
local7.*             /var/log/boot.log

#forward along
daemon.info @ 14.30:514
```



プロキシ ログで調査する必要があるエクスポート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。

i 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。

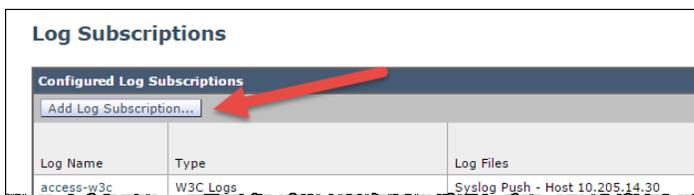
Cisco プロキシ ログを設定するには、次の手順を実行します。



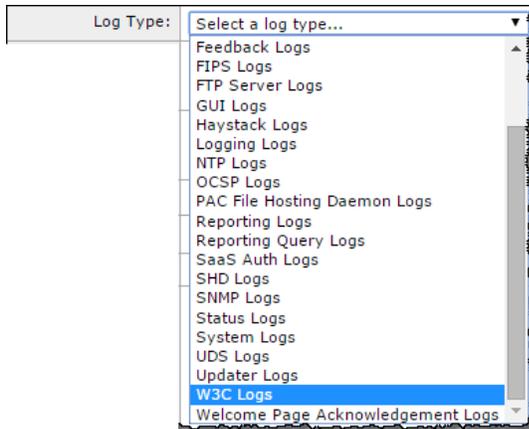
1. Cisco プロキシ サーバにログインします。



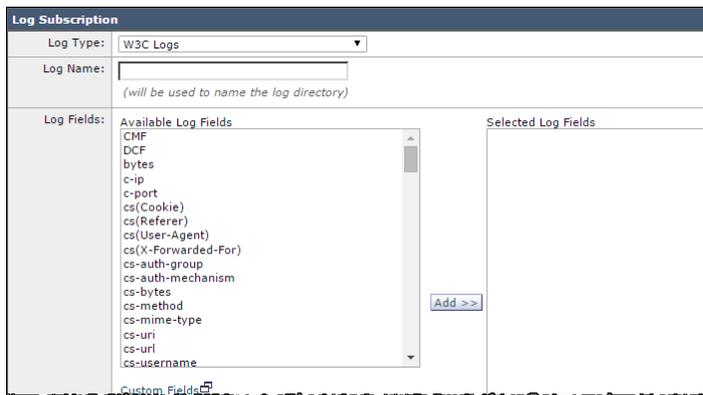
2. メインメニューで、[システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] をクリックします。[ログサブスクリプション (Log Subscriptions)] ページが開きます。



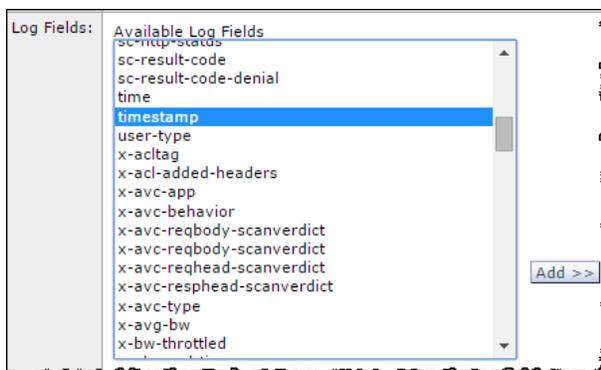
3. [ログサブスクリプションを追加 (Add Log Subscriptions)] ボタンをクリックします。新しい [ログサブスクリプション (Log Subscriptions)] ページが開きます。



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。



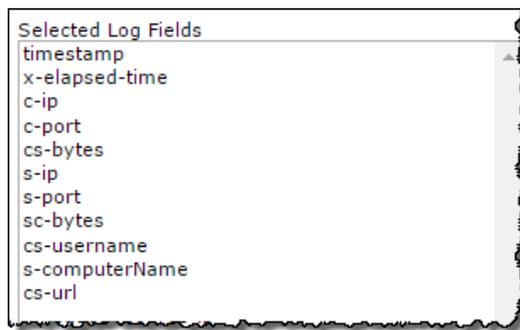
5. [ログ名(Log Name)]フィールドに、使用するログの名前を入力します。



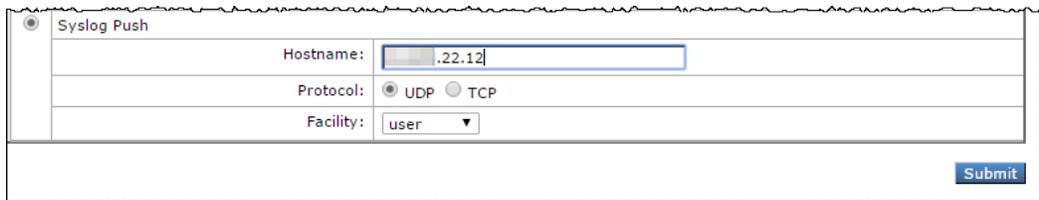
6. [使用可能なログフィールド(Available Log Fields)]リストから[タイムスタンプ(Timestamp)]を選択し、[追加(Add)]をクリックして[選択されたログフィールド(Selected Log Fields)]リストに移動させます。

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-username
 - 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。

i プロキシログで調査する必要があるエクスポート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ト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。

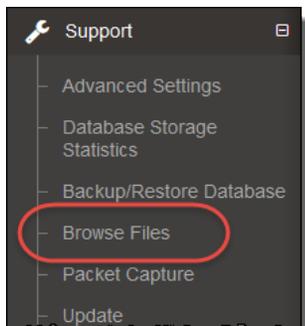
1. フローコレクタの管理インターフェイスにログインします。
2. メインメニューで、[設定 (Configuration)] > [プロキシの取得 (Proxy Ingest)] をクリックします。[プロキシサーバ (Proxy Servers)] ページが開きます。
3. プロキシサーバの IP アドレスを入力します。
4. [プロキシタイプ (Proxy Type)] ドロップダウンリストから、プロキシサーバを選択します。

 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。

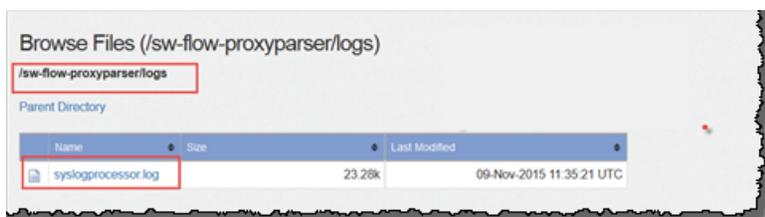
5. [プロキシID (Proxy ID)] フィールドに、プロキシサーバの IP アドレスを入力します。
6. [プロキシサービスポート (Proxy Service Port)] フィールドに、プロキシサーバのポート番号を入力します。
7. プロキシサーバによってアラームをトリガーするには、[アラームから除外 (Excluded from Alarming)] チェックボックスをオフにします。
8. [追加 (Add)] をクリックします。
9. [適用 (Apply)] をクリックします。ページ上部にある [プロキシの取得 (Proxy Ingest)] テーブルに、プロキシサーバが表示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

フローの確認

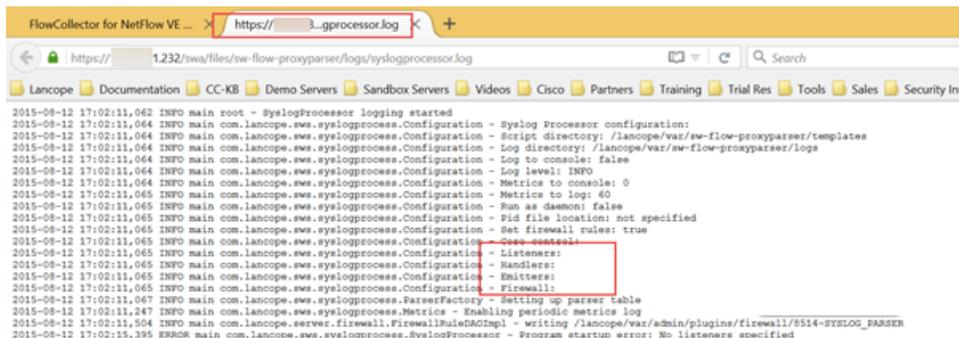
フローを受信していることを確認するには、次の手順を実行します。



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空白ではないことを確認します。空白である場合、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

```

2015-11-11 16:04:26,704 INFO main com.lancope.sse.syslogprocess.configuration - Using Prometheus configuration
2015-11-11 16:04:26,754 INFO main com.lancope.sse.syslogprocess.configuration - Script directory: /lancope/var/te-flow-prongparser/templates
2015-11-11 16:04:26,754 INFO main com.lancope.sse.syslogprocess.configuration - Log directory: /lancope/var/te-flow-prongparser/logs
2015-11-11 16:04:26,754 INFO main com.lancope.sse.syslogprocess.configuration - Log to console: false
2015-11-11 16:04:26,754 INFO main com.lancope.sse.syslogprocess.configuration - Log level: INFO
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - Metrics to console: 0
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - Metrics to log: 0
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - Run as daemon: false
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - PID file location: not specified
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - Set firewall rules: true
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - Core control:
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - Listeners:
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - @ syslog: port-8514
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - Handlers:
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - @ promy: sourceip-10.205.14.14 emitter-promy@engine pr
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - @ etters:
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - @ @@IMP/promy@engine:
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - Firewall:
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - @ REJECT: ipsec-eth0 protocol=udp destport=8514 srcport=0
2015-11-11 16:04:26,755 INFO main com.lancope.sse.syslogprocess.configuration - @ 1: 20 port=8514 protocol=udp source=0 src=10.205.14.14
2015-11-11 16:04:26,757 INFO main com.lancope.sse.syslogprocess.ParserFactory - Setting up parser table
2015-11-11 16:04:26,830 INFO main com.lancope.sse.syslogprocess.Metrics - Enabling periodic metrics log
2015-11-11 16:04:26,830 INFO main com.lancope.server.firewall.FirewallRuleEngineImpl - writing /lancope/var/admin/plugins/firewall/8514-576100
2015-11-11 16:04:27,751 INFO main com.lancope.sse.syslogprocess.core.StartupCore - Core configuration started
2015-11-11 16:04:27,751 INFO main com.lancope.sse.syslogprocess.core.StartupCore - Core configuration: single producer, blocking wait st
2015-11-11 16:04:27,881 INFO main com.lancope.sse.syslogprocess.SyslogProcess - Starting metrics log job
2015-11-11 16:04:27,881 INFO pool-2-thread-1 com.lancope.sse.syslogprocess.Metrics - Listeners: c0 @ rate:0 rate1:0 rate5:0
2015-11-11 16:04:27,881 INFO pool-2-thread-2 com.lancope.sse.syslogprocess.core.StartupCore - Starting thread 11 for listener syslog(8514)
2015-11-11 16:04:27,881 INFO pool-2-thread-1 com.lancope.sse.syslogprocess.Metrics - Handlers: c0 @ met:0 met1:0 met5:0
2015-11-11 16:04:27,881 INFO pool-2-thread-1 com.lancope.sse.syslogprocess.Metrics - @ etters: c0 @
2015-11-11 16:04:27,881 INFO pool-2-thread-1 com.lancope.sse.syslogprocess.Metrics - Listeners: c0 @ rate:0 rate1:0 rate5:0
2015-11-11 16:04:27,881 INFO pool-2-thread-1 com.lancope.sse.syslogprocess.Metrics - Handlers: c0 @ met:0 met1:0 met5:0

```

The C is the count. These should go up when logs going through.

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

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、<https://www.cisco.com/go/trademarks> をご覧ください。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。