非標準ポートでの不正トラフィックの検出

この章は、次の項で構成されています。

- 不正トラフィックの検出の概要 （1 ページ）
- L4 トラフィック モニタの設定 （1 ページ）
- 既知のサイトのリスト （2 ページ）
- L4 トラフィック モニタのグローバル設定 （3 ページ）
- L4 トラフィック モニタ アンチマルウェア ルールのアップデート （3 ページ）
- 不正トラフィック検出ポリシーの作成 （3 ページ）
- L4 トラフィック モニタのアクティビティの表示 （5 ページ）

不正トラフィックの検出の概要

Web セキュリティ アプライアンスは、すべてのネットワーク ポート全体にわたって不正なトラフィックを検出し、マルウェアがポート 80 をバイパスしようとするのを阻止する統合レイヤ4トラフィック モニタを備えています。内部クライアントがマルウェアに感染し、標準以外のポートとプロトコルを介して Phone Home を試みた場合、L4 トラフィック モニタは Phone Home アクティビティが企業ネットワークから外部に発信されるのを阻止します。デフォルトでは、L4 トラフィック モニタがイネーブルになり、すべてのポートでトラフィックをモニタするように設定されます。これには、DNS やその他のサービスが含まれます。

L4 トラフィック モニタは、独自の内部データベースを使用し、保持します。このデータベースは、IP アドレスとドメイン名の一致した結果によって継続的に更新されます。

L4 トラフィック モニタの設定

ステップ 1 ファイアウォールの内側に L4 トラフィック モニタを設定します。

ステップ 2 L4 トラフィック モニタが、プロキシ ポートの後ろ、かつクライアント IP アドレスのネットワーク アドレス変換（NAT）を実行する任意のデバイスの前に、「論理的に」接続されていることを確認します。

ステップ 3 グローバル設定項目を設定する

L4 トラフィック モニタのグローバル設定 （3 ページ）を参照してください。

ステップ 4 L4 トラフィック モニタのポリシーを作成する

不正トラフィック検出ポリシーの作成 （3 ページ）を参照してください。

既知のサイトのリスト

アドレス（**Address**）	説明
既知の許可アドレス（Known allowed）	[許可リスト（Allow List）] プロパティに記載されている IP アドレスまたはホスト名。これらのアドレスは、「ホワイトリスト」アドレスとしてログ ファイルに表示されます。
未記載（Unlisted）	マルウェア サイトであるか既知の許可アドレスであるかが不明な IP アドレス。これらは、[許可リスト（Allow List）]や[追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティに記載されておらず、L4 トラフィック モニタ データベースにも含まれていません。これらのアドレスはログ ファイルに表示されません。
不明瞭なアドレス（Ambiguous）	これらは「グレーリスト」アドレスとしてログ ファイルに表示され、以下のアドレスが該当します。 • リストに記載されていないホスト名と既知のマルウェアのホスト名の両方に関連付けられている *IP* アドレス。 • リストに記載されていないホスト名と [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティに含まれるホスト名の両方に関連付けられている *IP* アドレス。
既知のマルウェア（Known malware）	これらは「ブラックリスト」アドレスとしてログ ファイルに表示され、以下のアドレスが該当します。 • L4 トラフィック モニタ データベースで既知のマルウェア サイトと判定され、[許可リスト（Allow List）] に記載されていない IP アドレスまたはホスト名。 • [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティに記載され、[許可リスト（Allow List）] リストに記載されていない、不明瞭ではない *IP* アドレス。

L4 トラフィック モニタのグローバル設定

ステップ 1 [セキュリティ サービス（Security Services）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] を選択します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 L4 トラフィック モニタをイネーブルにするかどうかを選択します。

ステップ 4 L4 トラフィック モニタをイネーブルにする場合は、モニタ対象のポートを選択します。

- **[すべてのポート（All ports）]。**不正なアクティビティに対して TCP ポート 65535 をすべてモニタします。
- **[プロキシ ポートを除くすべてのポート（All ports except proxy ports）]。**不正なアクティビティに対して、以下のポートを除くすべての TCP ポートをモニタします。
  - [セキュリティ サービス（Security Services）] > [Web プロキシ（Web Proxy）] ページの [プロキシを設定する HTTP ポート（HTTP Ports to Proxy）] プロパティで設定したポート（通常はポート 80）。
  - [セキュリティ サービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] ページの [プロキシを設定する透過 HTTPS ポート（Transparent HTTPS Ports to Proxy）] プロパティで設定したポート（通常はポート 443）。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

L4 トラフィック モニタ アンチマルウェア ルールのアップデート

ステップ 1 [セキュリティ サービス（Security Services）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] を選択します。

ステップ 2 [今すぐ更新（Update Now）] をクリックします。

不正トラフィック検出ポリシーの作成

L4 トラフィック モニタがとるアクションは、設定する L4 トラフィック モニタのポリシーによって異なります。

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [L4 トラフィック モニタ（L4 Traffic Monitor）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [L4 トラフィック モニタのポリシーの編集（Edit L4 Traffic Monitor Policies）] ページで、L4 トラフィック モニタのポリシーを設定します。

a) [許可リスト（Allow List）] を**定義します**。

b) [許可リスト（Allow List）] に既知の安全なサイトを追加します。

（注） [許可リスト（Allow List）] には Web セキュリティ アプライアンスの IP アドレスやホスト名を含めないでください。それらを含めると、L4 トラフィック モニタがトラフィックを一切ブロックしなくなります。

c) **不審なマルウェア アドレス**に対して実行するアクションを決定します。

アクション	説明
許可（Allow）	既知の許可されたアドレスおよびリストに未記載のアドレスの発着信トラフィックを常に許可します。
モニタ（Monitor）	以下のような状況の下で、トラフィックをモニタします。 • [サスペクト マルウェア アドレスに対するアクション（Action for Suspected Malware Addresses）] オプションが [モニタ（Monitor）] に設定されている場合、既知の許可されたアドレスのすべての着発信トラフィックを常にモニタします。 • [サスペクト マルウェア アドレスに対するアクション（Action for Suspected Malware Addresses] オプションが [ブロック（Block）] に設定されている場合、不明瞭なアドレスのすべての着発信トラフィックをモニタします。
ブロック（Block）	[サスペクトマルウェア アドレスに対するアクション（Action for Suspected Malware Addresses] オプションが [ブロック（Block）] に設定されている場合、既知のマルウェア アドレスのすべての着発信トラフィックをブロックします。

（注） ：不審なマルウェア トラフィックをブロックすることを選択した場合は、不明瞭なアドレスを常にブロックするかどうかも選択できます。デフォルトでは、不明瞭なアドレスはモニタされます。

：ブロックを実行するように L4 トラフィック モニタを設定する場合は、L4 トラフィック モニタと Web プロキシを同じネットワーク上に設定する必要があります。すべてのクライアントがデータ トラフィック用に設定されたルートにアクセスできることを確認するには、[ネットワーク（Network）] > [ルート（Routes）] ページを使用します。

d) [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティを定義します。

（注） [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] のリストに内部 IP アドレスを追加すると、正当な宛先 URL が L4 トラフィック モニタのレポートにマルウェアとして表示されます。このような誤りを回避するために、[Web セキュリティ マネージャ（Web Security Manager）] > [L4 トラフィック モニタ ポリシー（L4 Traffic Monitor Policies）] ページの [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] フィールドに内部 IP アドレスを入力しないでください。

ステップ 4 変更を送信して確定します。

次のタスク

関連項目

- 不正トラフィックの検出の概要 （1 ページ）
- 有効な形式 （5 ページ）。

有効な形式

[許可リスト（Allow List）] または [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティにアドレスを追加する場合は、空白カンマを使用して複数のエントリを区切ります。以下のいずれかの形式でアドレスを入力できます。

- **IPv4 IP アドレス。**例：IPv4 形式：10.1.1.0。IPv6 形式：2002:4559:1FE2::4559:1FE2
- **CIDR アドレス。**例：10.1.1.0/24。
- **ドメイン名。**例：example.com
- **ホスト名。**例：crm.example.com

L4 トラフィック モニタのアクティビティの表示

Sシリーズアプライアンスは、サマリー統計情報の機能固有のレポートおよびインタラクティブな表示を生成するために、複数のオプションをサポートしています。

モニタリング アクティビティとサマリー統計情報の表示

[レポート（Reporting）] > [L4トラフィックモニタ（L4 Traffic Monitor）] ページには、モニタリング アクティビティの統計的なサマリーが表示されます。以下の表示とレポート ツールを使用して、L4 トラフィック モニタのアクティビティの結果を表示できます。

表示対象	参照先
クライアントの統計	[レポート（Reporting）] > [クライアント アクティビティ（Client Activity）]

表示対象	参照先
マルウェアの統計情報 ポートの統計情報	[レポート（Reporting）] > [L4 トラフィック モニタ（L4 Traffic Monitor）]
L4 トラフィック モニタのログ ファイル	[システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] • trafmon_errlogs • trafmonlogs

（注） Web プロキシが転送プロキシとして設定され、L4 トラフィック モニタがすべてのポートをモニタするように設定されている場合は、プロキシのデータ ポートの IP アドレスが記録され、[レポート（Reporting）] > [クライアント アクティビティ（Client Activity）] ページのクライアント アクティビティ レポートにクライアント IP アドレスとして表示されます。Web プロキシが透過プロキシとして設定されている場合は、クライアントの IP アドレスが正しく記録され、表示されるように IP スプーフィングをイネーブルにします。

L4 トラフィック モニタのログ ファイルのエントリ

L4 トラフィック モニタ ログ ファイルはモニタリング アクティビティの詳細を記録します。