非標準ポートでの不正トラフィックの検出

この章で説明する内容は、次のとおりです。

- 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 モニターの設定 （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 モニターのグローバル設定 （3 ページ）
- L4 トラフィック モニター 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 モニター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

Secure Web Appliance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 モニターは 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 モニター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ー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 モニターは、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 アドレスおよびドメイン名の照合によって継続的に更新されます。

L4 トラフィック モニターの設定

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

ステップ 2 L4 トラフィック モニターが、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 モニターのグローバル設定 （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 モニター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、「許可リスト」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 モニター 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「ブロックリスト」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 モニター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 モニターのグローバル設定

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ー（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 モニター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 モニターをイネーブルにする場合は、モニター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 をすべてモニターします。
- **[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 ポートをモニターします。
  - [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 モニター 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ー（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 モニターがとるアクションは、設定する L4 トラフィック モニター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ー（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ーのポリシーの編集（Edit L4 Traffic Monitor Policies）] ページで、L4 トラフィックモニター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） Secure Web Applianceの IP アドレスやホスト名を許可されたリストに含めないでください。さもないと、L4 トラフィック モニタは、どんなトラフィックもブロックしません。

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。
モニター	以下のような状況の下で、トラフィックをモニターします。 • [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 [モニター（Monitor）] に設定されている場合、既知の許可されたアドレス以外のすべての着発信トラフィックを常にモニターします。 • [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着発信トラフィックをモニターします。
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ーされます。

：ブロックを実行するように L4 トラフィック モニターを設定する場合は、L4 トラフィック モニターと 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で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。

- VM のセットアップでは、透過モードの要求が断続的な時間差で P1 インターフェイスと T1 インターフェイスを通過する間に、それらの要求が複製されます。そのため、一部の IP は、ブロックした後でもアプライアンスを通過する可能性があります。

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 モニター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ーポリシー（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（[送信（Submit）] と [変更を確定（Commit Changes）]）。

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、空白または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 モニター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。

モニターリング 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ー（L4 Traffic Monitor）] ページには、モニターリング 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 モニター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）]
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ー（L4 Traffic Monitor）]
L4 トラフィック モニターのログ 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 モニターがすべてのポートをモニター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 モニターのログ ファイルのエントリ

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。