Cisco Web Security Appliance と RSA DLP Network を相互運用するように設定するには、どうすればよいですか。

目次

質問：

Cisco Web Security Appliance と RSA DLP Network を相互運用するように設定するには、どうすればよいですか。

概要

このドキュメントでは、「Cisco WSA AsyncOS User Guide」と「RSA DLP Network 7.0.2 Deployment Guide」を補完する追加情報として、これら 2 つの製品の相互運用のための情報を提供しています。

製品説明：

Cisco Web Security Appliance（WSA）は、企業のセキュリティを脅かし、知的財産を漏えいする Web ベースのマルウェアおよびスパイウェア プログラムから企業ネットワークを保護する、堅牢性、安全性、および効率性に優れたデバイスです。 この Web セキュリティ アプライアンスでは、HTTP、HTTPS、FTP などの標準の通信プロトコルに対する Web プロキシ サービスを提供することで、詳細なアプリケーション コンテンツ検査機能が実現されています。

RSA DLP Suite には、包括的なデータ損失防止ソリューションが組み込まれています。このソリューションを使用すれば、ユーザは企業内の機密データを検出して保護することが可能になります。これは、インフラストラクチャ全体にわたる共通のポリシーを活用して、データセンター内、ネットワーク上、およびエンドポイントにある機密データを検出して保護することによって実現されます。 DLP Suite には、次のコンポーネントが含まれています。

- **RSA DLP Datacenter**。 DLP Datacenter は、データセンター、ファイル システム、データベース、電子メール システム、および大規模な SAN/NAS 環境のいずれに存在するものであれ、機密データの検出に役立ちます。
- **RSA DLP Network**。 DLP Network では、電子メールや Web トラフィックなどのネットワーク上の機密情報の伝送をモニタおよびブロックします。
- **RSA DLP Endpoint**。 DLP Endpoint は、ラップトップやデスクトップなどのエンドポイント上の機密情報の検出、モニタ、および制御に役立ちます。

Cisco WSA は、RSA DLP Network と相互運用することができます。

RSA DLP Network には、次のコンポーネントが含まれています。

- 。 機密データとコンテンツ伝送ポリシーに関する情報を保持するメイン アプライアンス。 Network Controller では、ポリシーおよび機密コンテンツ定義と、初期設定後のそれらの設定に対する変更を使用して、管理対象デバイスを管理および更新します。
- **管理対象デバイス**。 これらのデバイスは、次に説明するように、DLP Network によるネットワーク伝送のモニタ、および伝送のレポートまたはインターセプトを支援します。 **Sensor**。 Sensor は、ネットワーク境界にインストールされ、ネットワークから出ていくトラフィックや、ネットワーク境界を通過するトラフィックを受動的にモニタし、それらのコンテンツを分析して、機密コンテンツがないかどうかを確認します。 Sensor は、アウトオブバンド（帯域外）のソリューションです。 したがって、Sensor がモニタおよびレポートできるのは、ポリシー違反だけです。**Interceptor**。 Interceptor もネットワーク境界にインストールされます。Interceptor によって、機密コンテンツが含まれた電子メール（SMTP）トラフィックの検疫や拒否をすることができます。 Interceptor はインライン ネットワーク プロキシであるため、機密データの企業からの流出**ICAP サーバ**。 機密コンテンツが含まれた HTTP、HTTPS、または FTP のトラフィックのモニタまたはブロックの実行を可能にする専用のサーバ デバイス。 ICAP サーバはプロキシ サーバ（ICAP クライアントとして設定される）と連携して、機密データの企業からの流出をモニタまたはブロックします。

Cisco WSA は、RSA DLP Network の ICAP Server と相互運用できます。

既知の制限

Cisco WSA の RSA DLP Network との外部 DLP 統合では、 許可（Allow）およびブロック（Block）の操作がサポートされますが、 「コンテンツの変更（Modify）/削除（Remove）」（「修正/編集（Redaction）」とも呼ばれます）操作はまだサポートされていません。

相互運用性のための製品要件

Cisco WSA と RSA DLP Network の相互運用性は、次の表の製品モデルとソフトウェア バージョンでテストおよび検証を実施済みです。 この統合は、機能的に言えば、このモデルおよびソフトウェアとは違うものでも機能することがあり、次の表は、テストと検証が行われた、サポートされる組み合わせを表しているにすぎません。 両方の製品のサポート対象の最新バージョンを使用することを強くお勧めします。

製品	[Software Version]
Cisco Web セキュリティ アプライアンス（WSA）	AsyncOS バージョン 6.3 以上
RSA DLP Network	7.0.2

外部 DLP 機能

Cisco WSA の外部 DLP 機能を使用すれば、WSA からのすべてまたは特定の発信 HTTP、HTTPS、および FTP のトラフィックを DLP Network に転送できます。 すべてのトラフィックは、Internet Control Adaptation Protocol（ICAP）を使用して転送されます。

アーキテクチャ

「RSA DLP Network Deployment Guide」では、RSA DLP Network をプロキシ サーバと相互運用するための次のような汎用的なアーキテクチャが示されています。 このアーキテクチャは WSA に特有なものではなく、RSA DLP Network と相互運用するプロキシに適用されます。

図 1： RSA DLP Network および Cisco Web Security Appliance の展開アーキテクチャ

Cisco Web Security Appliance の設定

1. DLP Network の ICAP サーバと連携する WSA 上に外部 DLP システムを定義します。 手順については、「WSA User Guide」から抜粋したこのページの最後に添付した「ユーザー ガイドの手順：外部 DLP システムの定義」を参照してください。

2. 次の手順を使用して、コンテンツのスキャンのために WSA が DLP Network に送信するトラフィックを定義する 1 つ以上の外部 DLP ポリシーを作成します。

- [GUI] > [Web Security Manager] > [External DLP policies] > [Add Policy] の下で、
- 設定するポリシー グループの [Destinations] カラムの下にあるリンクをクリックします。
- [Edit Destination Settings] セクションの下で、ドロップダウン メニューから [Define Destinations Scanning Custom Settings] を選択します。
- ポリシーで、[Scan all uploads] を設定するか、または [Custom URL Categories] で指定された特定のドメインまたはサイトへのアップロードをスキャンするように設定できます。

RSA DLP Network の設定

このドキュメントでは、RSA DLP の Network Controller、ICAP Server、および Enterprise Manager がインストールおよび設定済みであることを想定しています。

1. Network ICAP Server を設定するには、RSA DLP の Enterprise Manager を使用します。 DLP Network ICAP Server の設定の詳細については、「RSA DLP Network Deployment Guide」を参照してください。 ICAP Server の構成ページで指定する必要がある主なパラメータは、次のとおりです。 ICAP Server のホスト名または IP アドレス。構成ページの [General Settings] セクションで、次の情報を入力します。 [Server Timeout in Seconds] フィールドの秒単位の時間。この時間を過ぎると、サーバはタイムアウトしたと見なされます。[Upon Server Timeout] 。応答として次のいずれかを選択します。[Fail Open]。 このオプションは、サーバのタイムアウト後に伝送を許可する場合に選択します。[Fail Closed]。 このオプションは、サーバのタイムアウト後に伝送をブロックする場合に選択します。
2. 1 つ以上の Network 固有のポリシーを作成して、機密コンテンツが含まれたネットワーク トラフィックを監査およびブロックするには、RSA DLP の Enterprise Manager を使用します。 DLP ポリシーの作成の詳細については、「RSA DLP Network User Guide」または Enterprise Manager のオンライン ヘルプを参照してください。 実行する主な手順は、次のとおりです。 ポリシー テンプレート ライブラリで、お客様の環境とモニタするコンテンツ

にとって意味をもつ少なくとも 1 つのポリシーを有効にします。選択したポリシー内で、イベント（ポリシー違反）が発生した場合に DLP Network 製品で自動的に実行するアクションを指定する、DLP Network 固有のポリシー違反ルールをセットアップします。 すべてのプロトコルを検出するためのポリシーの検出ルールを設定します。「監査およびブロック」を行うためのポリシー アクションを設定します。

オプションとして、RSA Enterprise Manager を使用して、ポリシー違反が発生した場合にユーザに送信される Network 通知をカスタマイズできます。 この通知は、DLP Network によって元のトラフィックの代わりに 送信されます。

セットアップのテスト

1. ブラウザからの発信トラフィックが WSA プロキシに直接送信されるようにブラウザを設定します。

   たとえば、Mozilla FireFox ブラウザを使用している場合は、次の手順を実行します。FireFox ブラウザで、[Tools] > [Options] を選択します。 [Options] ダイアログが表示されます。[Network] タブをクリックしてから、[Settings] をクリックします。 [Connection Settings] ダイアログが表示されます。[Manual Proxy Configuration] チェックボックスをオンにしてから、[HTTP Proxy] フィールドに WSA のプロキシ サーバの IP アドレスまたはホスト名、およびポート番号の 3128（デフォルト）を入力します。[OK] をクリックしてから、この新しい設定を保存するために再度 [OK] をクリックします。
2. 上で有効にした DLP Network ポリシーに違反することがわかっているコンテンツのアップロードを試みます。
3. ブラウザに Network ICAP の廃棄メッセージが表示されるはずです。
4. [Enterprise Manager] を使用して、このポリシーの違反の結果として生成された結果のイベントとインシデントを表示します。

トラブルシューティング

1. Web Security Appliance 上に RSA DLP Network 用の外部 DLP サーバを設定する場合、次の値を使用します。

   Server Address： RSA DLP Network ICAP サーバの IP アドレスまたはホスト名Port: RSA DLP Network サーバへのアクセスに使用する TCP ポート（通常 **1344**）Service URL Format： **icap://*<hostname_or_ipaddress>/srv_conalarm***例：icap://dlp.example.com/srv_conalarm
2. WSA プロキシと Network ICAP サーバ間のトラフィックをキャプチャするには、WSA のトラフィック キャプチャ機能を有効にします。 この機能は、接続の問題を診断する際に役立ちます。 この機能を有効にするには、次の手順を実行します。

   WSA GUI で、ユーザ インターフェイスの右上にある [Support and Help] メニューに移動します。 メニューから [Packet Capture] を選択して、[Edit Settings] ボタンをクリックします。 [Edit Capture Settings] ウィンドウが表示されます。

   この画面の [Packet Capture Filters] セクションで、[Server IP] フィールドに Network ICAP サーバの IP アドレスを入力します。**Submit** をクリックして、変更を保存します。

3. 詳細を入手するには、WSA アクセス ログ（[GUI] > *[System Administration]* > *[Log Subscriptions]* > *[accesslogs]* の下にあります）内の次のカスタム フィールドを使用します。
   %Xp： 外部 DLP サーバのスキャンの判定（0 = ICAP サーバで一致なし、 1 = ICAP サーバに対するポリシーの一致、および「-（ハイフン）」= スキャンが外部 DLP サーバによって開始されなかった）

ユーザー ガイドの手順：外部 DLP システムの定義