Cisco Security Analytics and Logging

Security Analytics and Logging（オンプレミス）スタートアップガイド

目次

スタートアップ ガイド：Cisco Security Analytics and Logging（オンプレミス）

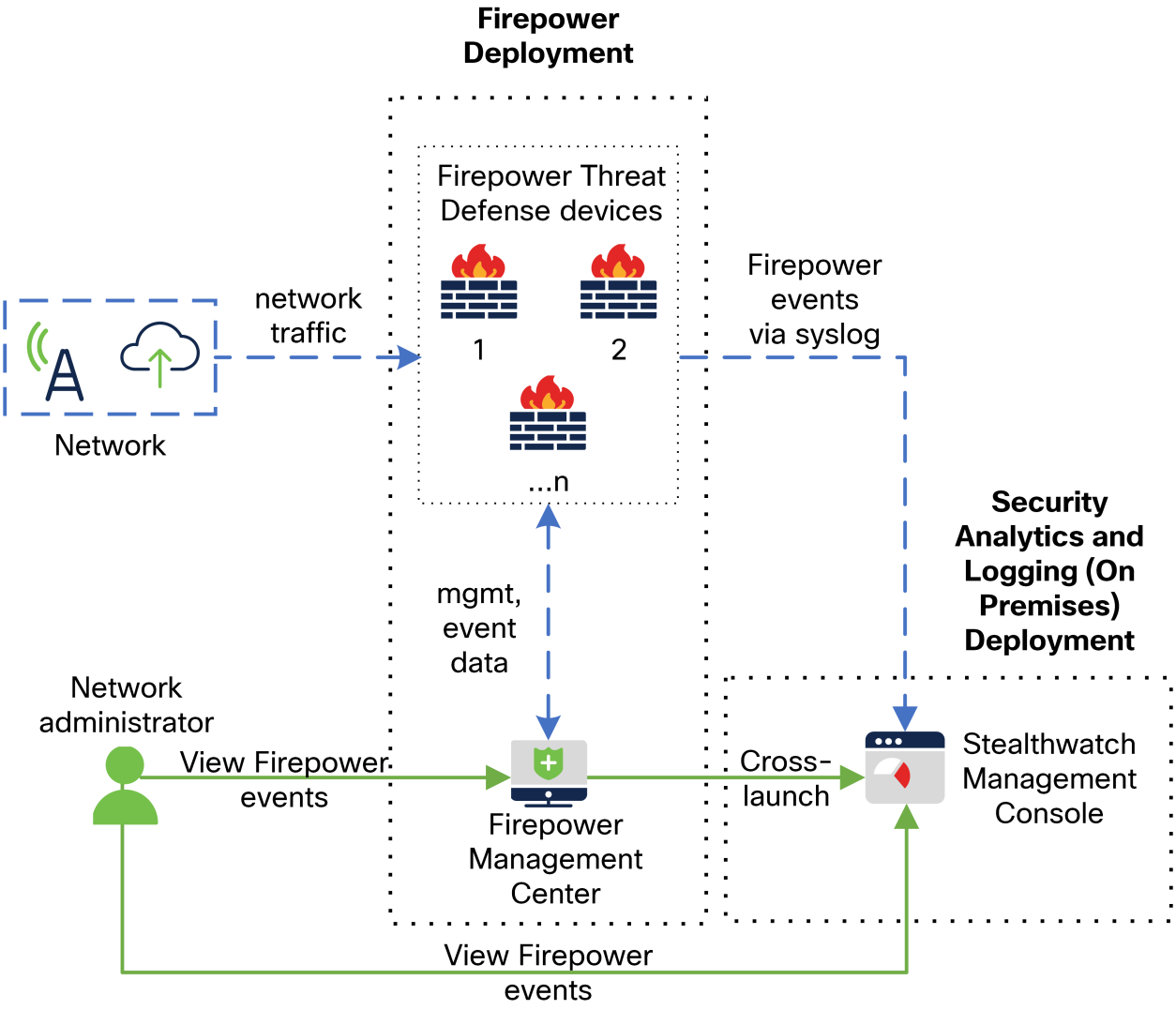
オンプレミスではなくCisco Cloud に Firepower イベントデータを保存する場合の詳細については、Cisco Security Analytics and Logging（SaaS）のマニュアルを参照してください。

はじめに

Cisco Security Analytics and Logging（オンプレミス）展開では、Stealthwatch アプライアンスを使用して、Firepower アプライアンス展開などの別のシスコ製品展開からのデータを保存できます。Firepower 展開の場合、Firepower 接続（セキュリティ インテリジェンスを含む）、侵入、ファイル、およびマルウェアイベントを、Firepower Management Center によって管理される Firepower Threat Defense デバイスから Stealthwatch Management Console に UDP 経由で syslog としてエクスポートして、その情報を保存できます。その後、Stealthwatch Management Console の Web アプリケーション UI からイベントデータを確認できます。Firepower Management Center UI から Stealthwatch Management Console Web アプリケーション UI に相互起動して、相互起動元の情報に関する追加のコンテキストを表示することもできます。

スタンドアロン アプライアンスとしての SMC への Security Analytics and Logging（オンプレミス）アプリケーションのインストールのみをサポートしています。1 つ以上のフローコレクタを管理する SMC にこのアプリケーションをインストールすることはできません。

例として次の図を参照してください。



次に、Firepower イベントデータを保存するために SAL（オンプレミス）の Stealthwatch アプライアンスを展開する方法の概要を示します。

参照資料

次の表に、SAL（オンプレミス）アプライアンスの互換性、展開、使用に関する参照資料を示します。

ドキュメント	説明
FirePOWER リリース ノート	Firepower リリースノートを参照して、最新の Firepower リリースに関する最新情報（直前の情報を含む）を確認してください。
Stealthwatch スマート ライセンシング ガイド [英語]	Stealthwatch 製品インスタンスを登録し、Stealthwatch Management Console VE のライセンスを取得する方法については、『Stealthwatch Smart Licensing Guide』を参照してください。
Stealthwatch Installation and Configuration Guide	Stealthwatch Management Console VE の展開および設定方法については、『Stealthwatch Installation and Configuration Guide』を参照してください。
Stealthwatch Enterprise のリリースノート	Stealthwatch Enterprise を参照して、最新の Stealthwatch Enterprise およびアプリケーションのリリースに関する最新情報（直前の情報を含む）を確認してください。
Security Analytics and Logging のリリースノート	SAL（オンプレミス）リリースノートを参照して、最新の SAL（オンプレミス）リリースおよび Security Analytics and Logging（オンプレミス）アプリケーションに関する最新情報（直前の情報を含む）を確認してください。

Firepower をまだ展開していないか、予想される接続、侵入、ファイル、およびマルウェアイベントを生成するように Firepower 展開を設定していない場合は、次を参照してください。

ドキュメント	説明
Firepower 互換性ガイド	『Firepower Compatibility Guide』を参照して、Firepower Management Center および Firepower Threat Defense デバイス のアプライアンスモデルのバージョンサポートを確認してください。
Firepower のインストールおよび設定のガイド	Firepower アプライアンスのインストールおよび設定の方法については、Firepower のインストールおよび設定のガイドを参照してください。
『Firepower Management Center Configuration Guide』	『Firepower Management Center Configuration Guide』を参照して、Firepower アプライアンスのライセンスと、Firepower Management Center によって管理される Firepower Threat Defense デバイス、アクセス コントロール ポリシー、侵入ポリシー、およびファイルポリシーの設定について確認してください。

SAL（オンプレミス）導入の前提条件

展開と統合を開始する前に、『Security Analytics and Logging On Premises: Firepower Event Integration Guide』で詳細を確認してください。

次の表に、Stealthwatch Management Console を使用して SAL（オンプレミス）展開に Firepower イベントデータを保存するために必要なソリューションのコンポーネントの概要を示します。

ソリューションのコンポーネント	必要なバージョン	ライセンス：SAL（オンプレミス）	注記
Firepower Management Center（ハードウェアまたは仮想）	• Firepower 6.4 以降（syslog 経由のイベントエクスポート用） • Firepower 6.4 ～ 6.6（手動相互起動クエリ設定用） • Firepower 6.7 以降（自動相互起動クエリ設定用）	なし	• Firepower Management Center ごとに 1 つの Stealthwatch Management Console に syslog を保存できます。
Firepower Threat Defense デバイス（ハードウェアまたは仮想）	Firepower 6.4 以降と、そのバージョン以降で実行されている Firepower Management Center	なし	• 1 つの Firepower Management Center によって管理される複数の Firepower Threat Defense デバイスは、syslog を同じ Stealthwatch Management Console にエクスポートできます
Stealthwatch Management Console	Stealthwatch 7.3.0 以降	なし	• SMC 2210 ハードウェアアプライアンスまたは SMC バーチャルエディション（VE）アプライアンスのいずれかを展開できます • すべて 1 つの Firepower Management Center で管理される、複数の Firepower Threat Defense デバイスから syslog を受信できます • syslog の取り込み、および Stealthwatch Management Console Web アプリケーショ

			ンでの Firepower イベントの表示のために Security Analytics and Logging（オンプレミス）アプリケーションをインストールする必要があります
Security Analytics and Logging（オンプレミス）App	Security Analytics and Logging（オンプレミス）アプリケーション 1.0 以降	取り込まれた GB／日に基づく、スマートライセンスのロギングおよびトラブルシューティング	• Stealthwatch Management Console にこのアプリケーションをインストールし、syslog の取り込みを有効にするように設定します

これらのコンポーネントに加えて、すべてのアプライアンスが NTP を使用して時刻を同期できることを確認する必要があります。Firepower または Stealthwatch アプライアンスのコンソールにリモートでアクセスする場合は、SSH 経由のアクセスを有効にできます。

Stealthwatch ライセンス

ライセンスなしで、SAL（オンプレミス）を 90 日間評価モードで使用できます。90 日間を経過しても SAL（オンプレミス）の使用を継続するには、Firepower 展開から Stealthwatch アプライアンスに syslog データで送信する見込みの 1 日あたりの GB 数に基づいて、SAL（オンプレミス）スマートライセンスのロギングおよびトラブルシューティング（SMC UI）スマートライセンスを取得する必要があります。

> ライセンスの計算のために、データ量は最も近い GB 数（切り捨て）で報告されます。たとえば、1 日あたり 4.9 GB を送信する場合は、4 GB と報告されます。

Stealthwatch アプライアンスのライセンスの詳細については、『Stealthwatch Smart Software Licensing Guide』を参照してください。

Stealthwatch リソースの割り当て

SAL（オンプレミス）の Stealthwatch Management Console を展開すると、平均で 1 秒あたり約 20,000 件のイベント（EPS）を取り込むことができます。割り当てたハードドライブストレージに基づいて、最大で数週間データを保存できます。これらの推定値は、ネットワーク負荷、トラフィックスパイク、イベントごとに送信される情報など、さまざまな要因の影響を受けます。

> Security Analytics and Logging（オンプレミス）アプリケーションは平均 20,000 EPS をサポートするように設計され、最大 35,000 EPS の急増をサポートしています。より高い EPS の取り込みレートでは、アプリケーションがデータをドロップすることがあります。また、接続、侵入、ファイル、およびマルウェアのイベントのみではなく、すべてのイベントタイプを送信する場合は、全体的な EPS が増加するにつれて、アプリケーションがデータをドロップする可能性があります。この場合は、ログファイルを確認してください。詳細については、『Firepower Event Integration Guide』の「Troubleshooting」の項を参照してください。

最適なパフォーマンスを得るために、Stealthwatch Management Console VE を展開する場合は、次のリソースを割り当てます。

リソース	推奨
CPU	12
RAM	64 GB
ハードドライブストレージ	2 TB

割り当てるストレージスペースに基づいて、大まかに次の期間のデータを保存できます。

平均 EPS	1 TB ストレージの推定保持期間	2 TB ストレージの推定保持期間	4 TB ストレージの推定保持期間
1000	250 日	500 日	1000 日
5000	50 日	100 日	200 日
10000	25 日	50 日	100 日
20000	12.5 日	25 日	50 日

Stealthwatch Management Console が最大ストレージ容量に達すると、着信データ用のスペースを確保するために最も古いデータが最初に削除されます。

シスコは、この推定取り込みおよびストレージ期間について、これらのリソース割り当てで Stealthwatch Management Console VE をテストしました。仮想アプライアンスに十分な CPU または RAM を割り当てないと、リソース割り当てが不十分なために予期しないエラーが発生する場合があります。ストレージ割り当てを 4 TB を超えて増やすと、リソース割り当てが不十分なために予期しないエラーが発生する可能性があります。

SAL（オンプレミス）通信ポート

次の表に、SAL（オンプレミス）の統合のために開く必要がある通信ポートを示します。

#	送信元（クライアント）	宛先（サーバ）	ポート	プロトコルまたは目的
1	外部インターネット（NTP サーバ）	Firepower Management Center、Firepower Threat Defense デバイス、および Stealthwatch Management Console	123/UDP	すべて同じ NTP サーバへの NTP 時刻同期

2	ユーザワークステーション	Firepower Management Center および Stealthwatch Management Console	443/TCP	Web ブラウザを使用した HTTPS 経由でのアプライアンスの Web インターフェイスへのログイン
3	Firepower Management Center が管理する Firepower Threat Defense デバイス	Stealthwatch Management Console	8514/UDP	Firepower Threat Defense デバイスからの syslog エクスポート、Stealthwatch Management Console への取り込み

SAL（オンプレミス）：Firepower イベントストレージの展開

次に、Firepower イベントデータを保存するための Stealthwatch 展開の大まかな設定手順を説明します。

- Stealthwatch Management Console をネットワークに展開する
- SMC に Security Analytics and Logging（オンプレミス）アプリケーションをダウンロードしてインストールし、Firepower syslog 情報を受信して保存するように Stealthwatch 展開を設定する
- syslog を Stealthwatch Management Console Virtual Edition にエクスポートするように Firepower システムを設定する
- Firepower Management Center と Stealthwatch Management Console の間に相互起動を設定する

導入を開始する前に、次のタスクを確認してください。

コンポーネントとタスク	SAL（オンプレミス）展開に必要かどうか	手順
Stealthwatch Management Console 展開	○	次の選択肢があります。 • SMC 2210 をネットワークに展開し、eth0 管理インターフェイスの IP アドレスやその他の情報の割り当てを含む、初期設定を実行します。詳細については、『x2xx Series Hardware Installation Guide』および『Stealthwatch System Configuration Guide』を参照してください。 • SMC VE OVA をダウンロードし、SMC VE をハイパーバイザに展開します。初期設定を実行し、eth0 管理インターフェイスの IP アドレスとその他の情報を割り当てます。詳細については、『Firepower Event Integration Guide』の付録を参照してください。

Stealthwatch の設定	○	• SMC で、[集中管理（Central Management）] の [アプリケーションマネージャ（App Manager）] に移動し、SAL（オンプレミス）アプリケーションをダウンロードします。Firepower Threat Defense 管理対象デバイスから syslog を受信するための設定を実行します。 ⚠ スタンドアロン アプライアンスとしての SMC への Security Analytics and Logging（オンプレミス）アプリケーションのインストールのみをサポートしています。1 つ以上のフローコレクタを管理する SMC にこのアプリケーションをインストールすることはできません。 • アプリケーションの使用方法の詳細については、SAL（オンプレミス）アプリケーションのリリースノートとヘルプを参照してください。
Firepower 設定	○	• SMC の eth0 管理 IP アドレスを使用してネットワーク ホスト オブジェクトを設定します。 • 管理対象の Firepower Threat Defense デバイスについて、Firepower Threat Defense プラットフォーム設定で Syslog サーバを設定し、作成したネットワーク ホスト オブジェクトをポイントして、ポート 8514/UDP 経由でエクスポートします。 • アクセス コントロール ポリシーで syslog ロギングを有効にします。 • アクセス コントロール ポリシー、アクセスコントロールルール、ファイルポリシー、および侵入ポリシーが、イベントを生成して syslog に記録するように設定されていることを確認します。 • Firepower Management Center によって管理されている Firepower Threat Defense デバイスに変更を展開します。
SAL（オンプレミス）の相互起動設定	×、ただし推奨	• Firepower Management Center から相互起動 URL を設定します。
SAL（オンプレミス）設定完了後の次の手順の確認	推奨	• Firepower の使用方法については、Firepower のマニュアルを参照してください。 • Stealthwatch の使用方法については、SMC Web アプリケーションのオンラインヘルプを参照してください。

SAL（オンプレミス）：Firepower イベントストレージの次の手順

SAL（オンプレミス）の一部として syslog イベントデータを Stealthwatch アプライアンスに渡すように Firepower 展開を設定したら、次の手順を実行できます。

- Firepower の詳細については、Firepower Management Center のオンラインヘルプを参照してください。
- Stealthwatch の詳細については、Stealthwatch Management Console Web アプリケーションのオンラインヘルプを参照してください。

著作権情報