

Cisco Secure Firewall 統合概要ガイド

最終更新：2026 年 10 月 7 日

はじめに

このガイドでは、イベント分析のために Cisco Secure Firewall Threat Defense（旧 Firepower Threat Defense）デバイスを次の各ツールと統合する手順について説明します。

- Cisco XDR
- Cisco Event Streamer
- Splunk
- IBM QRadar
- Cisco Security Analytics and Logging（オンプレミスおよび SaaS）

イベント分析ツールと必要な統合のタイプに基づいて、Cisco Secure Firewall Management Center（旧 Firepower Management Center）または Cisco Secure Firewall Device Manager（旧 Firepower Device Manager）管理対象 Firewall Threat Defense デバイスのいずれかを使用して統合を実行できます。このガイドには Firewall Management Center、または Firewall Device Manager のいずれかによって管理される Firewall Threat Defense デバイスを統合する手順が含まれています（該当する場合）。



Note

2024 年 7 月 31 日付けで Cisco SecureX は廃止され、使用できなくなりました。Cisco SecureX のアクセスは、Cisco Secure Firewall 製品の購入に伴って提供されなくなりました。サポート終了日以降、ユーザーに対して Cisco SecureX をプロビジョニングすることはできません。さらに、既存のすべての Cisco SecureX 環境が無効化され、すべての機能が利用できなくなりました。

使用例

このセクションでは、一般的なユースケースを、統合を実行するために使用するツールとともにリストします。

使用例	ソリューション	サポート対象 の Firewall Threat Defense 最小リリース	詳細情報
複数のテレメトリソースで可視性を統合し、検出を関連付け、最大のリスクに基づいて脅威に優先順位付け、セキュリティアナリストが緊急対応が必要な案件に対して迅速かつ効果的なアクションを実行できるようにしたい。	Cisco XDR	6.4	シスコ XDR との統合
Management Center からのホストデータ、検出データ、関連データ、コンプライアンスのホワイトリストデータ、侵入データ、ユーザー アクティビティ データ、ファイルデータ、マルウェアデータ、接続データをストリーミングしたい。	Cisco Event Streamer (eStreamer)	6.0	Cisco Event Streamer との統合
Splunkを使用して Firewall Management Center から受信した脅威とトラフィックデータを保存し、このデータを使用して脅威を検出および調査する必要がある。	Cisco Secure Firewall (旧 Firepower) App for Splunk	6.0	Splunk との統合
QRadar で複数のセキュリティ製品からインサイトを提供することによって、ネットワークに対する脅威を分析し、封じ込める必要がある。	Cisco Firepower App for IBM QRadar	6.0	IBM QRadar との統合
オンプレミス ファイアウォールのイベントストレージ容量を増やし、そのデータをより長期間保持し、イベントデータを Cisco Secure Network Analytics アプライアンスにエクスポートしたい。	Cisco Security Analytics and Logging (オンプレミス)	6.4	Cisco Security Analytics and Logging (オンプレミス) との統合, on page 9

使用例	ソリューション	サポート対象 の Firewall Threat Defense 最小リリース	詳細情報
オンプレミスストレージで提供されるストレージよりも多くのストレージが必要なため、ストレージ用にファイアウォールイベントを Cisco Secure Cloud Analytics（旧 Stealthwatch Cloud）に送信し、必要に応じて Cisco Secure Cloud Analytics を使用して、ファイアウォールイベントデータをセキュリティ分析に使用できるようにしたい。	シスコのセキュリティ分析とロギング（SaaS）	6.4	Cisco Security Analytics and Logging（SaaS）との統合, on page 11

Cisco XDR との統合

Cisco Extended Detection and Response（Cisco XDR）は、複数のテレメトリソースの脅威検出を関連付けることで可視性を統合し、セキュリティチームが最も高度な脅威を検出、優先順位付け、対応できるようにするクラウドベースのソリューションです。このソリューションは、リスクに基づいてインシデントに優先順位を付けることで、脅威の検出と対応機能を強化し、セキュリティアナリストが緊急の対応が必要な案件に対して迅速かつ効果的なアクションを実行できるようにします。

この統合により、サポートされているイベントが Firewall Threat Defense デバイスから Cisco XDR に分析のために送信されます。



- (注) Cisco XDR は別個にライセンス供与される製品です。Cisco Secure Firewall 製品に必要なライセンス以外に、追加のサブスクリプションが必要です。詳細については、「[Cisco XDR Licenses](#)」を参照してください。

統合のタイプ

Firewall Threat Defense デバイスを Cisco XDR と統合するには、次の 2 つの方法があります。

- 直接統合：Firewall Management Center でサポート
- Syslog 統合：Firewall Management Center および Firewall Device Manager でサポート

直接統合

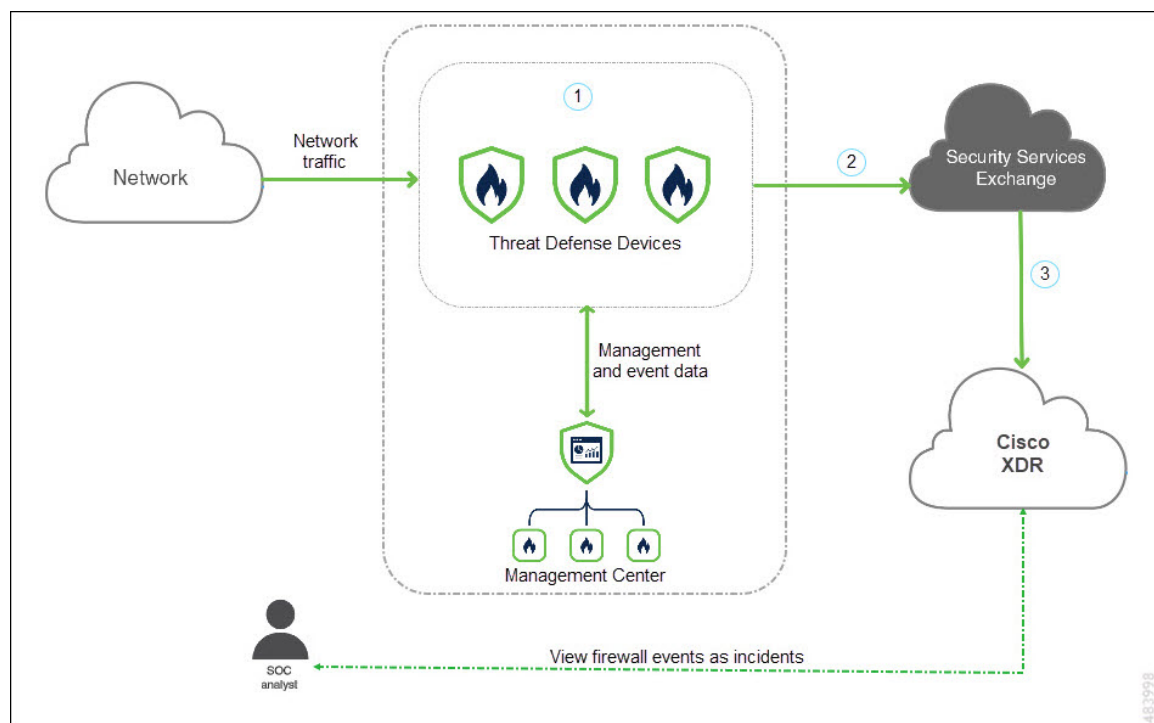
管理対象 Firewall Threat Defense デバイスが、サポートされているイベントを Cisco Security Cloud 内の Security Services Exchange に直接送信できるように設定できます。

- 統合を実行するためにサポートされている Secure Firewall ユーザーロール：管理者。
- サポート対象の最小 Firewall Threat Defense バージョン：北米クラウドの場合は 6.4、ヨーロッパ、APJC、インド、およびオーストラリアのクラウドでは 6.5。
- サポート対象の最小 Firewall Management Center バージョン：7.0.2 から 7.0.x、および 7.2.0 以降。



(注) SecureX サブスクリプションを使用してすでに Cisco Security Cloud にイベントを送信していた場合は、Cisco XDR に引き続きイベントを送信できます。ただし、Security Cloud Control アカウントを使用してクラウドテナントに Firewall Management Center を登録する場合、Security Cloud Control アカウントにはイベントを Cisco XDR に転送するためのセキュリティ分析とロギングライセンスが必要です。

次の図は、直接統合の仕組みを示しています。



①	Firewall Threat Defense デバイスがイベントを生成します。
②	Firewall Threat Defense デバイスはサポートされているイベントを Security Services Exchange に送信します。

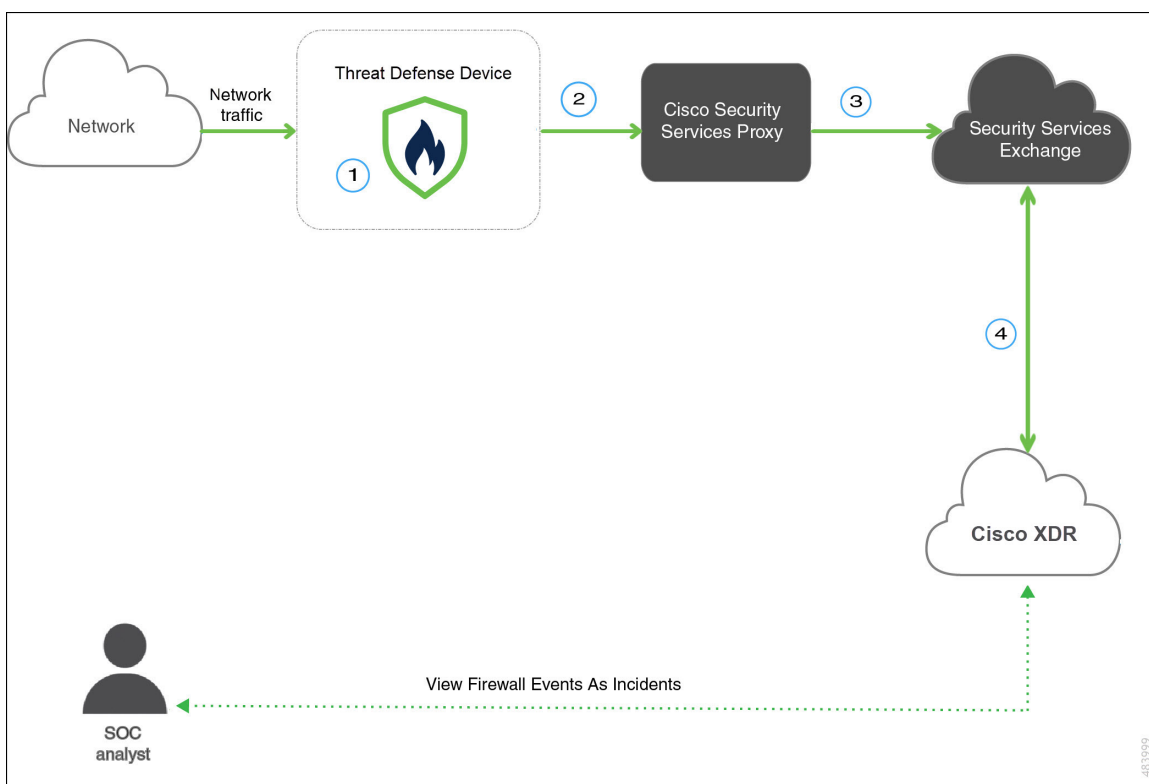
③	Cisco XDR は、調査対象の IP アドレスに関する検出情報を Security Services Exchange に照会し、セキュリティアナリストに追加のコンテキストを提供します。イベントは、Cisco XDR に表示されるインシデントに自動的にまたは手動で昇格されます。
---	---

Syslog 統合

ファイアウォールデバイスからシスコクラウドに syslog を使用してサポートされているイベントを送信します。

- 統合を実行するためにサポートされている Secure Firewall ユーザーロール：管理者。
- サポートされる Secure Firewall の最小リリース：すべてのクラウドリージョンで 6.3。

次の図は、Syslog 統合の仕組みを示しています。



①	Firewall Threat Defense デバイスがイベントを生成します。
②	Firewall Threat Defense デバイスは、サポートされている syslog イベントをシスコセキュリティサービス プロキシ（CSSP）サーバーに送信します。
③	10 分ごとに、CSSP は収集したイベントを Security Services Exchange に転送します。

4	Cisco XDR は、調査対象の IP アドレスに関する検出情報を Security Services Exchange に照会し、セキュリティアナリストに追加のコンテキストを提供します。イベントは、Cisco XDR に表示されるインシデントに自動的にまたは手動で昇格されます。
---	---

Cisco Event Streamer との統合

Cisco Event Streamer (eStreamer と呼ばれる) を使用すると、ファイアウォールシステムイベントを外部のクライアントアプリケーションにストリーミングできます。

eStreamer サービスは最高レベルでファイアウォールシステムから要求元クライアントにデータをストリーミングするメカニズムです。このサービスでは、次のデータカテゴリをストリーミングできます：

- 侵入イベント データおよび追加のイベント データ
- 相関 (コンプライアンス) イベント データ
- 検出イベント データ
- ユーザー イベント データ
- イベントのメタデータ
- ホスト情報
- マルウェア イベント データ

eStreamer は、NGIPSv、ファイアウォールサービス、Firewall Threat Defense Virtual、および Firewall Threat Defense ではサポートされていないことに注意してください。これらのデバイスからのイベントをストリーミングするには、そのデバイスが報告する Management Center で eStreamer を構成します。

eStreamer クライアントを作成し、ファイアウォールシステムと統合するには 3 つの主要な手順があります。

1. eStreamer アプリケーションプロトコルを使用して、Management Center または管理対象デバイスとメッセージを交換するクライアントアプリケーションを記述します。eStreamer SDK には、参照クライアントアプリケーションが含まれます。
2. クライアントアプリケーションに必要なイベントのタイプを送信するために Management Center またはデバイスを設定します。
3. クライアントアプリケーションを Management Center またはデバイスに接続し、データの交換を開始します。

統合を実行するためにサポートされているファイアウォール ユーザーロール：管理者

サポート対象の最小 Firepower リリース：6.0

ファイアウォールの統合に関する詳細については、『[Secure Firewall Management Center Event Streamer 統合ガイド](#)』を参照してください。

Splunk との統合

Cisco Secure Firewall (f.k.a. Firepower) App for Splunk には、バージョン 6.0 以降を実行している Firewall Management Center から Splunk に送信されたセキュリティおよびネットワークイベント情報が表示されます。Firewall Management Center からの脅威データとトラフィックデータを使用して、脅威を検出し、調査します。Splunk は、Firewall Management Center よりもはるかに多くのデータを保存できるため、ネットワーク上のアクティビティをより詳細に把握できます。

このアプリケーションは、Cisco Firepower eNcore App for Splunk (<https://splunkbase.splunk.com/app/3663/>) の後継アプリケーションです。必要に応じて、両方のアプリケーションを並行して実行できます。

統合を実行するためにサポートされているファイアウォール ユーザーロール：管理者

サポート対象の最小 Firepower リリース：6.0

サポートされている Splunk のバージョンおよびその他の互換性情報については、<https://splunkbase.splunk.com/app/4388/> を参照してください。

このアプリケーションを使用する前に、ファイアウォールのイベントデータが Splunk にある必要があります。ファイアウォールのデータを Splunk に取り込むには、Cisco Secure eStreamer Client Add-On for Splunk (旧 Cisco eStreamer eNcore Add-on for Splunk) を使用します。このテクニカルアドオン (TA) は <https://splunkbase.splunk.com/app/3662/> から入手できます。

この TA のドキュメントは https://www.cisco.com/c/ja_jp/support/security/defense-center/products-programming-reference-guides-list.html から利用できます。

Cisco Secure Firewall (旧 Firepower) App for Splunk の詳細については、『[Cisco Secure Firewall \(旧 Firepower\) App for Splunk](#)』を参照してください。

IBM QRadar との統合

Cisco Firepower App for IBM QRadar は、QRadar の複数のセキュリティ製品からのインサイトを提供することで、ネットワークに対する脅威を分析して封じ込めます。

QRadar セキュリティ情報イベント管理 (SIEM) ツールは、異常検出、インシデントフォレンジック、および脆弱性管理を提供します。

このアプリケーションを設定すると、QRadar コンソールでファイアウォールシステムからのイベントデータをグラフィカル形式で表示できます。

統合を実行するためにサポートされているファイアウォール ユーザーロール：管理者

サポート対象の最小 Firepower リリース：6.0

Cisco Firepower App for IBM QRadar の詳細については、『[Integration Guide for the Cisco Firepower App for IBM QRadar](#)』を参照してください。

Cisco Security Analytics and Logging (CSAL) との統合

Cisco Security Analytics and Logging (CSAL) は、シスコのさまざまなデバイスからのログを集約し、ネットワークアクティビティの直感的なビューを提供することで、意思決定を合理化します。Security Analytics and Logging はユーザーの裁量で拡張可能であり、長期間の保持と分析が可能になり、ファイアウォールやその他のネットワークデバイスで見つかった潜在的な脅威に関するアラートも可能になります。

ファイアウォールデバイスは、オンプレミスと Security as a Service (SaaS) の 2 つの方法を使用して CSAL と統合できます。

シスコのセキュリティ分析とロギング リモート イベント ストレージ オプションの比較

オンプレミス	SaaS
ファイアウォールの背後に設置するストレージシステムを購入し、ライセンスを取得してセットアップします。	ライセンスとデータストレージプランを購入し、データをシスコのクラウドに送信します。
サポートされるイベントタイプ： • 接続 • セキュリティインテリジェンス • 侵入 • ファイルおよびマルウェア • LINA	サポートされるイベントタイプ： • 接続 • セキュリティインテリジェンス • 侵入 • ファイルおよびマルウェア
syslog と直接統合の両方をサポートします。	syslog と直接統合の両方をサポートします。
• Secure Network Analytics Manager ですべてのイベントを表示します。 • Firewall Management Center イベントビューアから相互起動して、Secure Network Analytics Manager でイベントを表示します。 • Firewall Management Center でリモートに保存された接続およびセキュリティ インテリジェンス イベントを表示します。	ライセンスに応じて Security Cloud Control または Secure Network Analytics でイベントを表示します。Firewall Management Center イベントビューアから相互起動します。

詳細については、『[Cisco Secure Firewall Management Center デバイス設定ガイド](#)』またはオンラインヘルプの「Data Storage」の章にあるリンクを参照してください。

Cisco Security Analytics and Logging (オンプレミス) との統合

長期間保持できる大容量ストレージで、ファイアウォールイベントのデータを保存するように Cisco Security Analytics and Logging (オンプレミス) を設定できます。Cisco Secure Network Analytics (旧 Stealthwatch) アプライアンスを展開し、ファイアウォール展開に統合することで、イベントデータを Secure Network Analytics アプライアンスにエクスポートできます。

統合を実行するためにサポートされているファイアウォールユーザーロール：管理者、アナリスト、セキュリティアナリスト

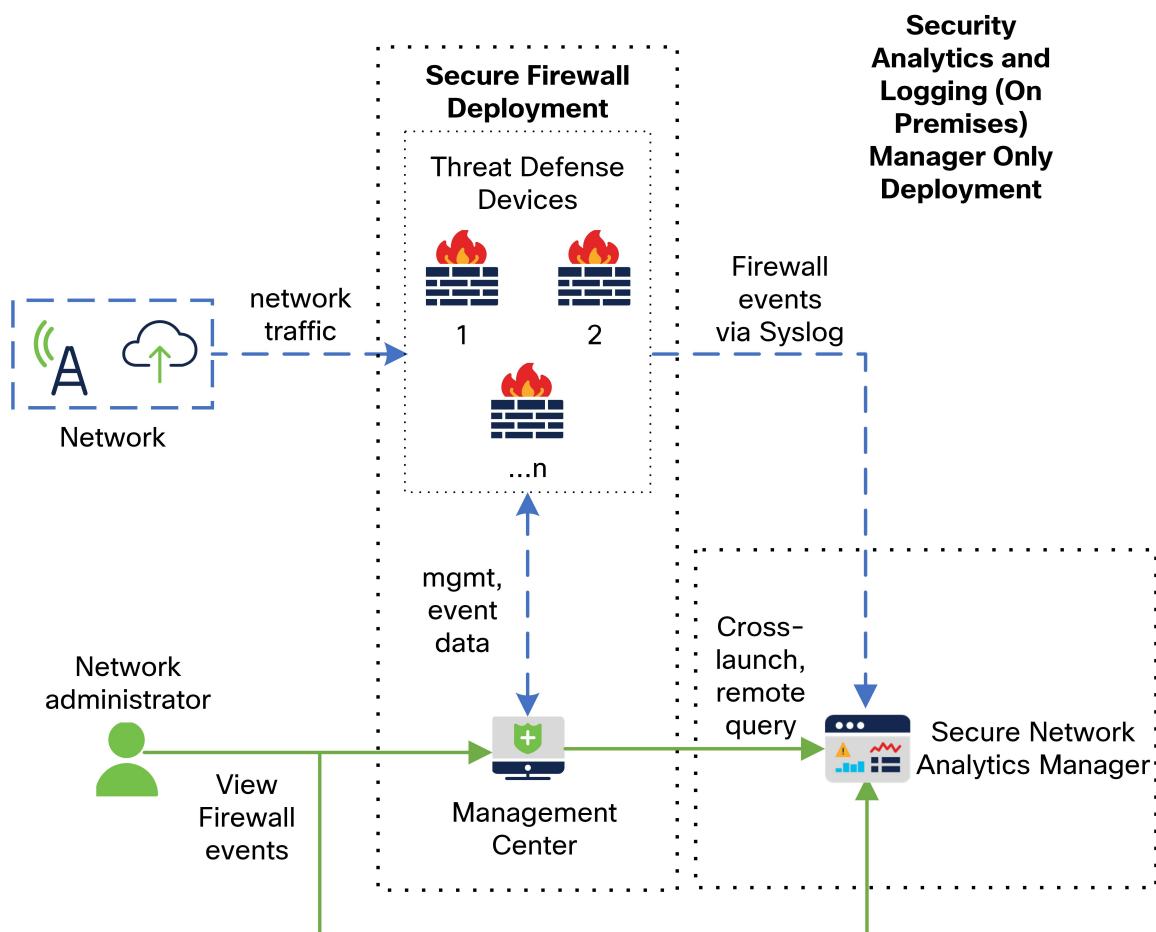
サポートされる Secure Firewall の最小リリース：6.4

展開のタイプ

マネージャのみの展開

スタンドアロンのマネージャを展開してイベントを受信および保存し、そこからイベントを確認および照会します。

マネージャを使用したマネージャのみの展開の例については、次の図を参照してください。



この展開では、Firewall Threat Defense デバイスはファイアウォールのイベントをマネージャに送信し、マネージャがこれらのイベントを保存します。ユーザーは Firewall Management Center のUIからマネージャを相互起動して保存されたイベントに関する詳細情報を表示できます。さらに、Firewall Management Center からイベントのリモートクエリを実行できます。

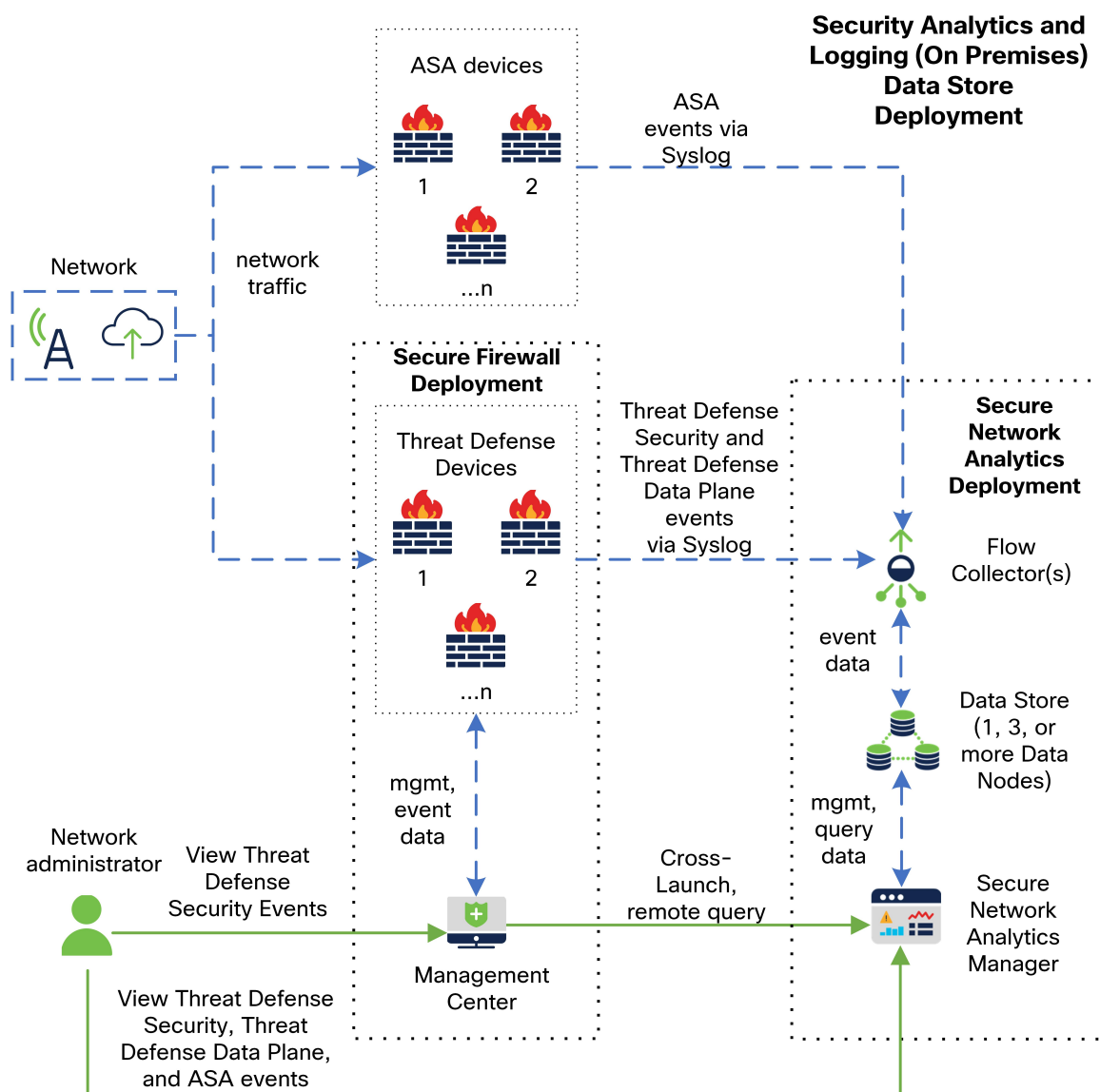


Note Secure Network Analytics アプライアンスバージョン 7.5.1 以降では、**マネージャのみの展開**はサポートされていません。詳細については、「[Cisco Security Analytics and Logging](#)」を参照してください。

データストアの展開

Cisco Secure Network Analytics フローコレクタを展開してイベントを受信し、Cisco Secure Network Analytics データストア（3 つの Cisco Secure Network Analytics データノードを含む）を展開してイベントを保存し、そこからイベントを確認および照会できます。

マネージャ、3 つのデータノード、およびフローコレクタを使用したデータストアの展開の例については、次の図を参照してください。



この展開では、Firewall Threat Defense デバイスおよび ASA デバイスはファイアウォールのイベントをフローコレクタに送信します。フローコレクタは、保存のためにデータストア（データノード X 3）にイベントを送信します。ユーザーは Firewall Management Center の UI からマネージャーを相互起動して保存されたイベントに関する詳細情報を表示できます。さらに、Firewall Management Center からイベントのリモートクエリを実行できます。

ファイアウォールと SAL（オンプレミス）の統合の詳細については、『[Cisco Security Analytics and Logging（オンプレミス）：ファイアウォールイベント統合ガイド](#)』を参照してください。

Cisco Security Analytics and Logging（SaaS）との統合

ファイアウォールイベントを保存するための追加の容量が必要な場合は、Cisco Security Analytics and Logging（SaaS）を使用して、ファイアウォールイベントを Cisco Secure Cloud Analytics（旧

Stealthwatch Cloud) に送信し、必要に応じてファイアウォールイベントデータを Cisco Secure Cloud Analytics を使用したセキュリティ分析に利用可能にすることができます。

この統合は、Firewall Management Center が管理する Firewall Threat Defense デバイス専用です。この統合は、ファイアウォールソフトウェアを実行していないデバイス、Firewall Device Manager によって管理されるデバイス、または Firewall Management Center によって管理される Firewall Threat Defense 以外のデバイスではサポートされません。

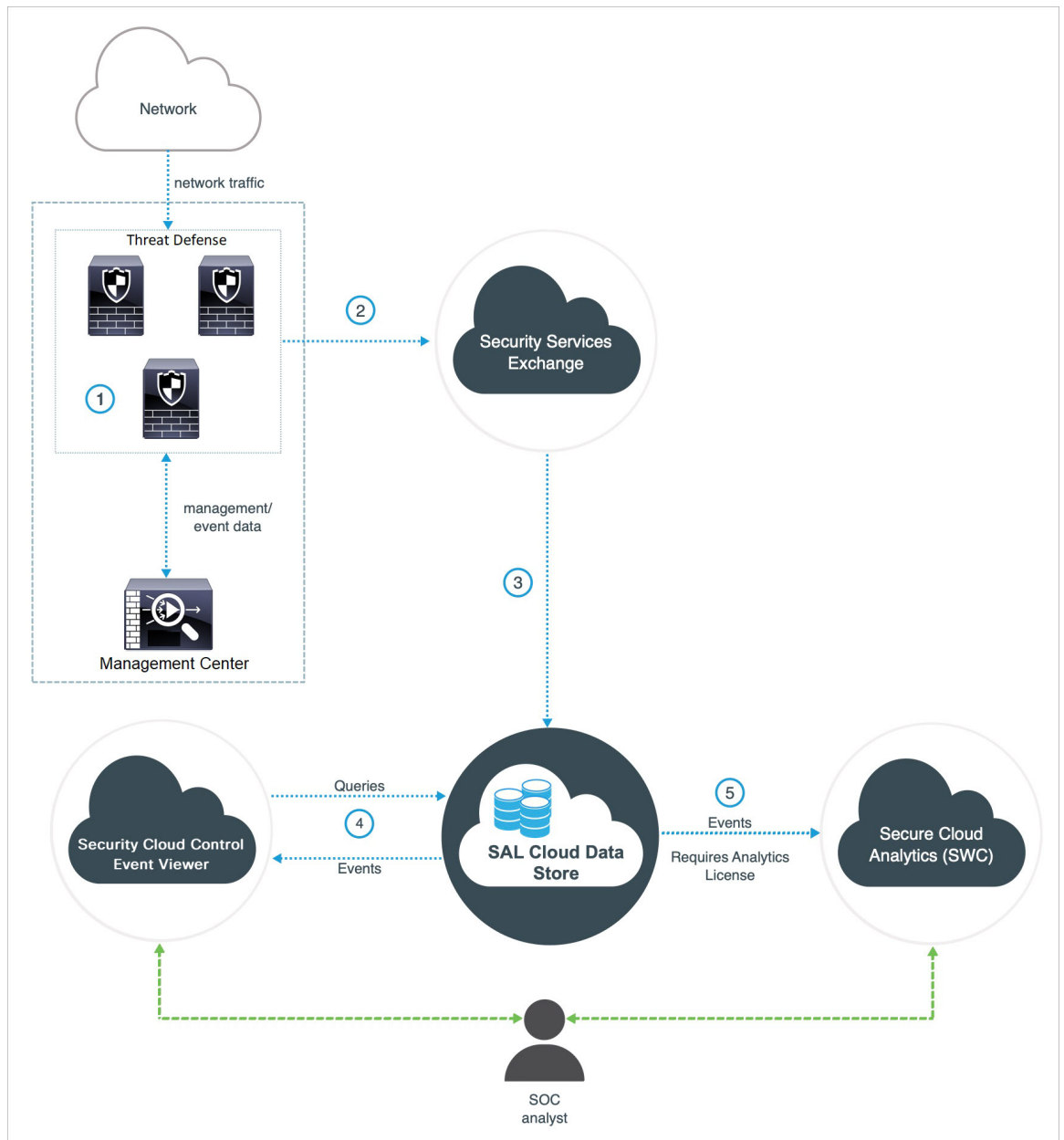
統合のタイプ

直接統合

統合を実行するためにサポートされているファイアウォールユーザーロール：管理者、アクセス管理者、ネットワーク管理者、セキュリティ承認者

サポート対象の最小 **Firepower** リリース：6.4

次の図は、直接統合の動作の仕組みを示しています。



1	Firewall Threat Defense デバイスがイベントを生成します。
2	Firewall Threat Defense デバイスはサポート対象のイベントを、シスコのクラウドセキュリティ製品に使用される、クラウド間およびオンプレミス間での識別と認証、およびデータストレージを処理するセキュアな中間クラウドサービス、Security Services Exchange に送信します。

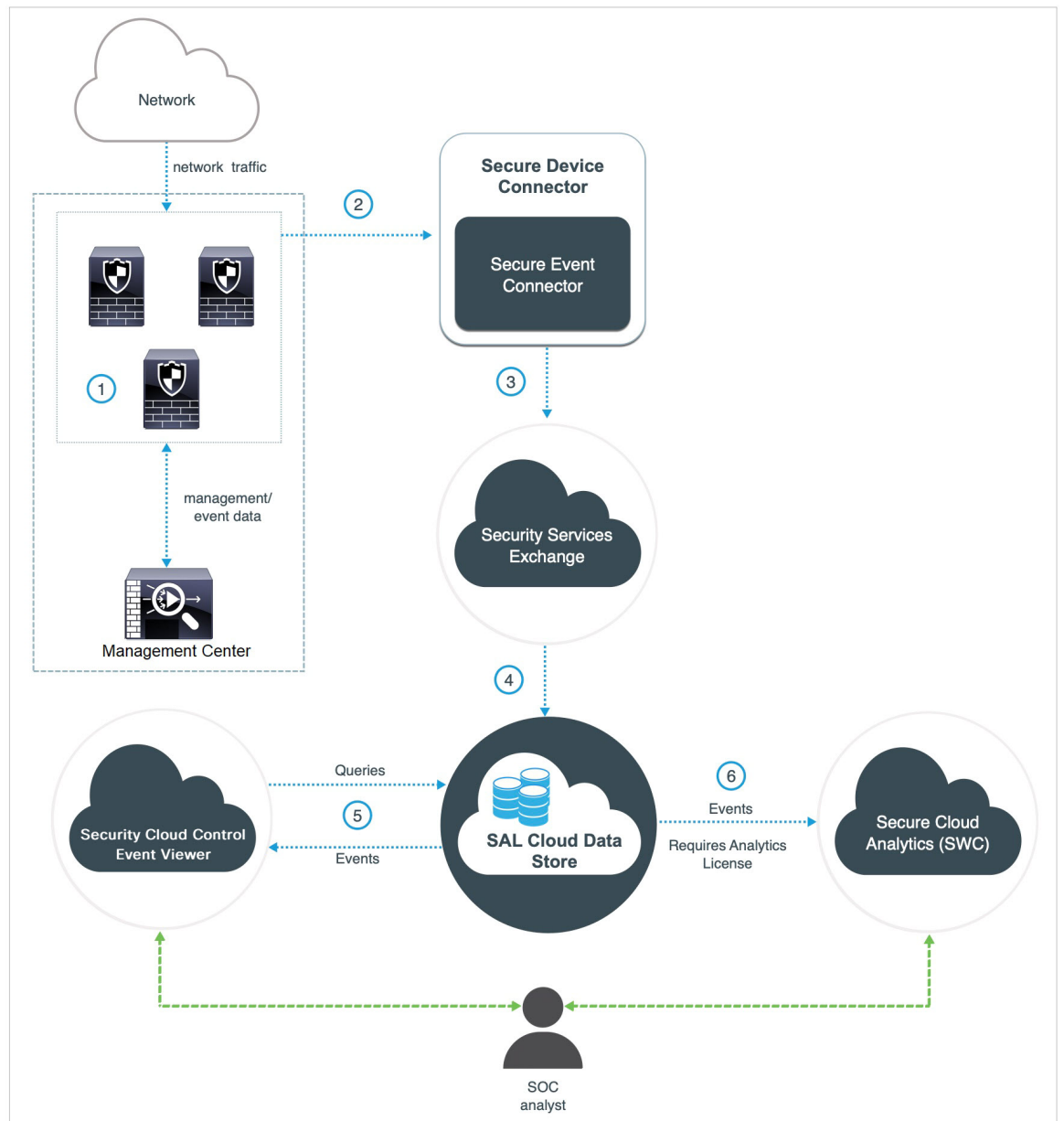
③	Security Services Exchange は、イベントを Cisco Security Analytics and Logging (SAL) クラウドデータストアに転送します。
④	Security Cloud Control イベントビューアは、イベントについて SAL クラウドデータストアにクエリを実行し、SOC アナリストに追加のコンテキストを提供します。
⑤	(Analytics ライセンスがある場合のみ) Cisco Secure Cloud Analytics (旧 SWC) は、SAL クラウドデータストアからイベントを受信し、SOC アナリストに製品の分析機能へのアクセスを提供します。

Syslog 統合

統合を実行するためにサポートされているファイアウォールユーザーロール：管理者、アクセス管理者、ネットワーク管理者、セキュリティ承認者

サポート対象の最小 **Firepower** リリース：7.0

次の図は、Syslog 統合の仕組みを示しています。



1	Firewall Threat Defense デバイスがイベントを生成します。
2	Firewall Threat Defense デバイスは、サポートされているイベントを syslog メッセージとして、ネットワーク上の仮想マシンにインストールされている Secure Event Connector (SEC) に送信します。

③	SEC はイベントを、シスコのクラウドセキュリティ製品に使用される、クラウド間およびオンプレミス間での識別と認証、およびデータストレージを処理するセキュアな中間クラウドサービス、Security Services Exchange に送信します。
④	Security Services Exchange は、イベントを Cisco Security Analytics and Logging (SAL) クラウドデータストアに転送します。
⑤	Security Cloud Control イベントビューアは、イベントについて SAL クラウドデータストアにクエリを実行し、SOC アナリストに追加のコンテキストを提供します。
⑥	(Analytics ライセンスがある場合のみ) Cisco Secure Cloud Analytics (旧 SWC) は、SAL クラウドデータストアからイベントを受信し、SOC アナリストに製品の分析機能へのアクセスを提供します。

ファイアウォールと CSAL (SaaS) の統合に詳細については、『[Cisco Cisco Secure Firewall Management Center](#) および [Security Analytics and Logging \(SaaS\) 統合ガイド](#)』を参照してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

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。

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。