Security Cloud Control Firewall Management

Security Cloud Control Firewall Management の概要

Security Cloud Control Firewall Management （旧Cisco Defense OrchestratorまたはCDO）は、Cisco IOS や SSH などの Cisco ファイアウォールやその他のデバイス間でセキュリティポリシーを簡素化し、統合するのに役立つクラウドベースのセキュリティポリシーマネージャです。ファイアウォールとデバイスは、Security Cloud Control ダッシュボードの**[Products]** の下にリストされている **[Firewall]** から管理できます。

Security Cloud Control Firewall Management は、セキュリティポリシー内の不整合を特定し、修正するためのツールを提供することにより、セキュリティポリシーを最適化するのに役立ちます。オブジェクトとポリシーを共有できるだけでなく、設定テンプレートを作成することで、デバイス間でのポリシーの一貫性を維持できます。

Security Cloud Control Firewall Management は Cisco Adaptive Security Device Manager（ASDM）と共存するため、ASDM によって行われた設定の変更が追跡され、違いが調整されます。

さまざまなデバイスを一元的に管理できます。上級ユーザーは、従来の CLI インターフェイスに新しい機能拡張を追加して、管理の効率をさらに向上させます。

Security Cloud Control Firewall Management では、ガイド付きの「Day 0」エクスペリエンスも提供され、Threat Defense デバイスをオンプレミスまたは クラウド提供型 Firewall Management Centerにすばやくオンボーディングできます。また、有効化および設定するのに役立つその他の主要な機能も紹介されています。

デバイスのオンボーディング要件

デバイスを導入準備する前に、次の前提条件を満たしてください。

- インストール構成ウィザードを完了します。
- デバイスのライセンスを取得します。

これらの前提条件を満たした後、 Security Cloud Control Firewall Management オンボーディングウィザードを使用してデバイスを導入準備します。

「デバイスとサービスのオンボーディング」を参照してください。

次の制約事項に注意してください。

- 組織に関連付けられている Security Cloud Control Firewall Management にデバイスを導入準備した後は、それらのデバイスを別の組織に移行できません。
- デバイスを新しい組織に移動するには、新しい組織にデバイスを再度オンボーディングする必要があります。

Security Cloud Control のサポート対象デバイスの完全なリストについては、Security Cloud Control Firewall Management でサポートされるデバイス、ソフトウェア、ハードウェア を参照してください。

シスコ オンライン プライバシー ポリシー

Cisco Systems, Inc. およびその子会社（以下総称して「シスコ」といいます）は、皆様のプライバシーを保護し、シスコの Web サイト、ならびに製品およびサービス（以下「ソリューション」）を快適にお使いいただけるよう全力を尽くします。『シスコ オンライン プライバシー ポリシー』をよく読み、シスコがユーザーの個人情報を収集、使用、共有、保護する方法を明確に理解してください。

Security Cloud Control による Secure Firewall ASA の管理

Security Cloud Control （旧称 Cisco Defense Orchestrator）はクラウドベースのマルチデバイスマネージャであり、すべての Cisco ASA デバイスのセキュリティポリシーを、シンプルで一貫性のあるセキュアな方法で管理できます。

このドキュメントの目的は、Security Cloud Control を初めて使用するお客様に、オブジェクトとポリシーの標準化、管理対象デバイスのアップグレード、VPN ポリシーの管理、リモートワーカーの監視に使用できる機能の概要を提供することです。このマニュアルでは、次のことを前提としています。

- 30 日間のトライアル用アカウントを作成している。または Security Cloud Control を購入しており、シスコが Security Cloud Control テナントを作成している。
- すでに ASA が構成されており、企業で使用している。
- Security Cloud Control で管理する Cisco ASA にインターネットから直接アクセスできない場合は、ネットワークに Secure Device Connector（SDC）を展開する必要があります。SDC は、Security Cloud Control と Cisco ASA 間の通信を管理します。

  詳細については、Secure Device Connector および Secure Event Connector を実行するための VM の展開を参照してください。

Secure Device Connector

デバイスのログイン情報を使用して Security Cloud Control を Cisco ASA に接続する場合、Security Cloud Control と Cisco ASA 間の通信を管理するために、ネットワークに Secure Device Connector（SDC）をダウンロードして展開することがベストプラクティスです。デバイスのログイン情報を使用して、すべての Cisco ASA の Security Cloud Control への導入準備を行うことができます。Cisco ASA と Security Cloud Control 間の通信を SDC で管理しない場合で、デバイスにインターネットから直接アクセスできる場合は、ネットワークに SDC をインストールする必要はありません。Cloud Connector を使用して Cisco ASA の Security Cloud Control への導入準備を行うことができます。

テナントに複数の SDC を展開すると、パフォーマンスを低下させることなく、Security Cloud Control テナントでより多くのデバイスを管理できます。1 つの SDC が管理できるデバイスの数は、それらのデバイスに実装されている機能と、構成ファイルのサイズによって異なります。ただし、展開計画の目安として、1 つの SDC で約 500 台のデバイスをサポートできることを想定しています。

SDC を表示するには：

1. Security Cloud Control にログインします。
2. Security Cloud Control メニューから**[管理（Admin）]** > **[セキュアコネクタ（Secure Connectors）]**に移動します。

デバイスの導入準備

Cisco ASA の Security Cloud Control への導入準備は、まとめて、または一度に 1 つずつ実行できます。

Security Cloud Control でサポートされる Cisco ASA ソフトウェアおよびハードウェアの説明については、「サポートの詳細」を参照してください。

テナントに追加する Security Cloud Control ユーザーを作成する

Security Cloud Control には、読み取り専用、編集専用、展開専用、管理者、ネットワーク管理者など、さまざまなユーザーロールがあります。ユーザーロールは、各テナントのユーザーごとに設定されます。1 人の Security Cloud Control ユーザーが複数のテナントにアクセスできる場合、ユーザー ID は同じでも、テナントごとにロールが異なる場合があります。インターフェイスまたはマニュアルで読み取り専用ユーザー、管理者ユーザー、ネットワーク管理者ユーザーについて言及されている場合、特定のテナントにおけるそのユーザーの権限レベルを意味しています。

異なるタイプのユーザーに付与される権限については、Security Cloud Control Firewall Management におけるユーザーロールを理解する を参照してください。

テナントが作成された際、ネットワーク管理者ユーザーが自動的に割り当てられています。スーパー管理は、テナントに他のユーザーを作成する権限を持ちます。これらの新しいユーザーがテナントに接続するには、Security Cloud Control のユーザーレコードと同じ E メールアドレスで Cisco Secure Sign-On アカウントを持っているか、それを作成する必要があります。

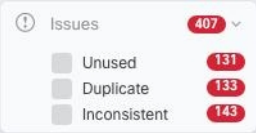
Security Cloud Control でユーザーレコードを作成するには、Security Cloud Control へのユーザーアカウントの追加 を参照してください。

ポリシー オーケストレーション

ポリシーオーケストレーションには、オブジェクトとポリシーのレビューが含まれます。Cisco ASA のポリシーを処理する際は、Security Cloud Control では「アクセスグループ」が「アクセスポリシー」と呼ばれることに注意してください。Cisco ASA のアクセスポリシーを探すには、Security Cloud Control メニューバーの [ポリシー（Policies）] > [Cisco ASAアクセスポリシー（ASA Access Policy）] の順に移動します。

ネットワークオブジェクトの問題を解決する

年月が経つにつれて、使用されなくなったオブジェクト、他のオブジェクトと重複したオブジェクト、デバイス間で値が一致しないオブジェクトがセキュリティデバイスに存在している場合があります。オーケストレーションタスクの第一歩としてこれらのオブジェクトの問題を修正します。



以下の順序でオブジェクトの問題に対処します。初期の手順で行う作業により、後の手順で対処する必要がある問題の多くが解決される場合があります。

1. 未使用のオブジェクトを解決する。未使用オブジェクトとは、デバイスに存在するが、別のオブジェクト、アクセスリスト、または NAT ルールによって参照されていないオブジェクトです。
2. 重複オブジェクトを解決する。重複オブジェクトとは、同じデバイス上にある、名前は異なるが値は同じである 2 つ以上のオブジェクトです。通常、重複したオブジェクトは誤って作成され、同じ目的を果たし、さまざまなポリシーによって使用されます。重複オブジェクトの問題を解決した後、Security Cloud Control は、残されたオブジェクト名に対する、影響を受けるすべてのオブジェクト参照を更新します。
3. 不整合オブジェクトを解決する。不整合オブジェクトとは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーが異なる構成の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。これはセキュリティ上の問題となる場合があります。古いリソースを保護するルールが設定されている可能性があります。

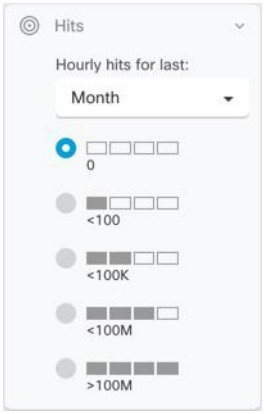
シャドウルールの修正

ネットワークオブジェクトの問題を解決したら、次にシャドウルールのネットワークポリシーを確認して修正します。**シャドウルール**は、ASA のアクセスポリシーページで半月のバッジ ◑ で示されます。アクセスポリシーのルールはリストで構成され、上から下に 1 つずつ評価さ

れます。ネットワークトラフィックはポリシー内のシャドウルールより上位のルールと一致するため、ポリシー内のシャドウルールが一致することはありません。ヒットすることのないシャドウルールがある場合は、それを削除するか、ポリシーを編集してルールを有効にします。

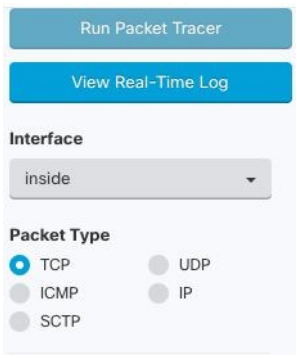
ポリシーのヒット率の評価

ポリシーのルールが実際にネットワークトラフィックを評価しているかどうかを判断します。Security Cloud Control は、ポリシーのルールのヒット率データを毎時間収集します。デバイスが Security Cloud Control によって管理されている時間が長いほど、特定のルールのヒット率データが持つ意味は大きくなります。特定の期間のヒット数で ASA アクセスポリシーをフィルタ処理して、ヒットしているかどうかを確認します。ヒットしていない場合は、ポリシーを作成し直すか削除することを検討してください。



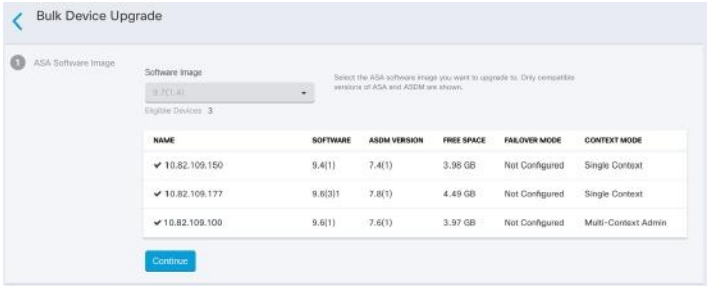
ポリシーのトラブルシュート

ASA パケットトレーサーを使用して、模擬パケットに対するポリシーの適用をテストして、ルールによってアクセスが誤ってブロックまたは許可されていないかを判断できます。



ASA と ASDM のアップグレード

次に、ASA と ASDM を最新バージョンにアップグレードします。お客様は、Security Cloud Control を使用して Cisco ASA をアップグレードすると、75% ～ 90% の時間を節約できると報告しています。



Security Cloud Control は、シングルコンテキストまたはマルチコンテキストモードで、個々の Cisco ASA または複数の Cisco ASA にインストールされている Cisco ASA および ASDM イメージをアップグレードできるウィザードを提供しています。Security Cloud Control は、Cisco ASA および ASDM イメージのデータベースを維持します。

Security Cloud Control は、必要なアップグレード互換性チェックをバックグラウンドで実行します。ウィザードは、互換性のある Cisco ASA および ASDM イメージを選択し、それらをインストールし、デバイスをリブートしてアップグレードを完了するプロセスを導きます。Security Cloud Control で選択したイメージが Cisco ASA にコピーおよびインストールされているものであることを検証することにより、Security Cloud Control はアップグレードプロセスを保護します。

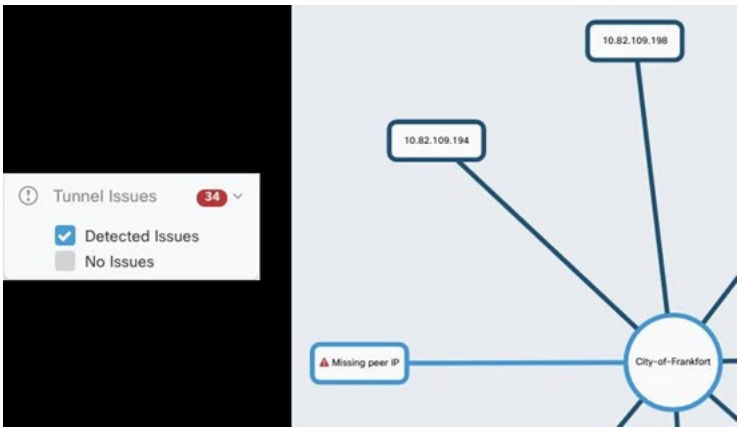
Security Cloud Control は定期的にデータベースを確認し、最新の Cisco ASA および ASDM イメージをデータベースに追加します。Security Cloud Control は、一般に利用可能な（GA）イメージのみをサポートし、データベースにカスタムイメージを追加しません。リストに特定の GA イメージがない場合は、[サポートに連絡] ページから Cisco TAC にお問い合わせください。確立されたサポートチケット SLA によってリクエストを処理し、リストにない GA イメージをアップロードします。

単一 ASA 上の ASA と ASDM イメージのアップグレード を確認してから、独自のリポジトリからのイメージを含む複数の ASA のアップグレード で ASA のアップグレードについてさらに学習してください。

VPN 接続の監視と管理

サイト間 VPN の問題を確認する

Security Cloud Control は、ネットワーク内の Cisco ASA デバイスに存在する VPN の問題を報告します。環境の表示方法は 2 つあります。VPN ピアのリストを示す表と、ハブ アンド スポーク トポロジで VPN 接続を示すマップです。サイドバーのフィルタを使用して、注意が必要な VPN トンネルを検索します。



以下の方法で、Security Cloud Control を使用して VPN トンネルを評価します。

- サイト間 VPN トンネルの接続性を確認する
- ピアが欠落している VPN トンネルを見つける
- 暗号化キーの問題がある VPN ピアを見つける
- トンネルに対して定義された不完全な、または誤った設定のアクセスリストを見つける
- トンネル設定の問題を見つける

管理されていないサイト間 VPN ピアの導入準備を行う

Security Cloud Control は、管理されていない VPN ピアも識別します。このようなデバイスを見つけたら、管理対象外サイト間 VPN ピアのオンボーディング を使用してデバイスの導入準備を行い、Security Cloud Control で同様に管理します。

ASA リモートアクセス VPN のサポート

Security Cloud Control を使用することで、リモートアクセス仮想プライベートネットワーク（RA VPN）構成を作成して、ユーザーが Cisco ASA 経由で接続中にエンタープライズリソースにセキュアにアクセスできるようになります。Cisco ASA の Security Cloud Control への導入準備が行われると、ASDM または Cisco Security Manager（CSM）を使用して設定済みのすべての RA VPN 設定が Security Cloud Control によって認識されるため、Security Cloud Control で管理できるようになります。

AnyConnect はエンドポイントデバイスでサポートされている唯一のクライアントで、RA VPN 接続が可能です。

Security Cloud Control は、Cisco ASA デバイスでの RA VPN 機能の次の側面をサポートします。

- SSL クライアントベースのリモートアクセス
- IPv4 および IPv6 のアドレッシング
- 複数の ASA デバイス間での共有 RA VPN 構成

詳細については、Cisco ASA のリモートアクセス仮想プライベートネットワークの設定を参照してください。

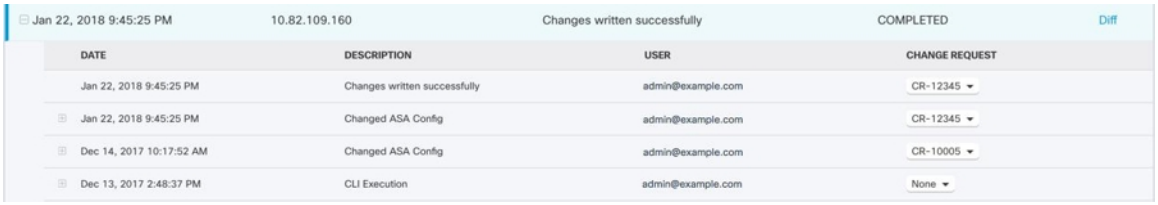
デバイス構成同期を監視する

Security Cloud Control は、データベースに保存したデバイス構成と、Cisco ASA にインストールされている構成を定期的に比較します。Security Cloud Control への導入準備がされた Cisco ASA は、引き続きデバイスの Adaptive Security Device Manager（ASDM）によって管理できます。そのため Security Cloud Control はその構成がデバイスの構成と同じであることを確認し、相違点があれば警告します。[同期済み（Synced）]、[非同期（Not Synced）]、[競合検出（Conflict Detected）] のデバイスステータスの詳細は、競合検出 を参照してください。

変更ログでの変更の追跡

デバイスの構成に加えた変更は、Security Cloud Control での変更ログの管理 に記録されます。変更ログには、Security Cloud Control からデバイスに展開された変更、デバイスから Security Cloud Control にインポートされた変更などの情報が表示されます。ここでは変更の「差分」、変更の時期、変更者といった変更内容も表示できます。

企業の追跡番号を使用するカスタムラベルを作成して、加えた変更に適用することもできます。変更ログでは、そのカスタムラベル、日付範囲、特定のユーザー、変更タイプで変更のリストをフィルタリングして、目的の変更を見つけることができます。



以前の構成を復元する

Cisco ASA に加えた変更を「元に戻す」必要がある場合、Security Cloud Control を使用してデバイスを以前の構成に復元できます。詳細については、ASA 設定の復元を参照してください。

コマンド ライン インターフェイスとコマンドマクロを使用してデバイスを管理する

Security Cloud Control は、グラフィック ユーザー インターフェイス（GUI）とコマンド ライン インターフェイス（CLI）の両方を提供する Web ベースの管理製品で、デバイスを 1 つずつまたは一括で管理できます。

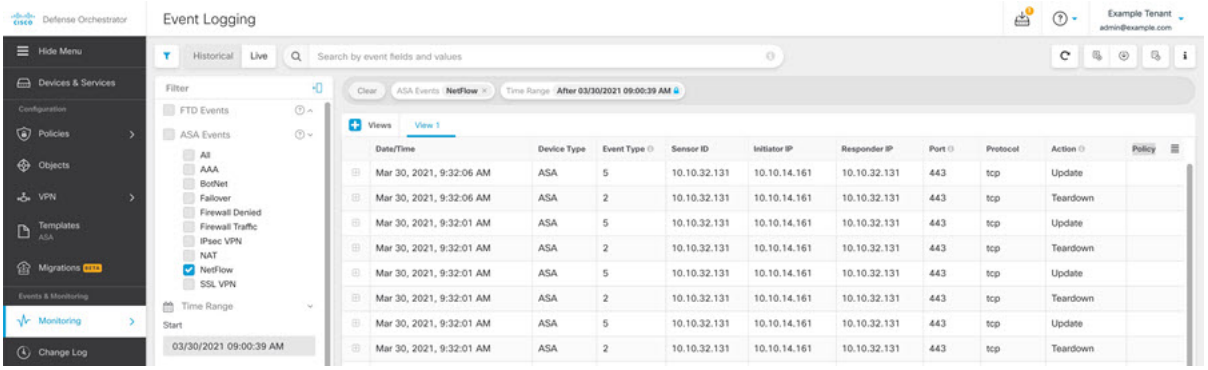
ASA CLI のユーザーは、シスコの CLI ツールの追加機能を活用できます。SSH セッションでデバイスに接続するのではなく、Security Cloud Control の CLI ツールを使用するべき理由は以下のとおりです。

- Security Cloud Control は、コマンドに必要なユーザーモードを認識します。コマンドを実行するために権限レベルを上げたり下げたりする必要はありません。また、コマンドを実行するために特定のコマンドコンテキストを入力する必要もありません。

- Security Cloud Control はコマンド履歴を保持しているため（）、リストから選択するだけで簡単にコマンドを再実行できます。
- CLI アクションは変更ログに記録されるため、送信されたコマンドと実行されたアクションを確認できます。
- コマンドは一括モードで実行できるため、オブジェクトまたはポリシーを複数のデバイスに同時に展開できます。
- Security Cloud Control は CLI マクロを提供します（）。. CLI マクロはすぐに実行可能なコマンドで、格納された状態からそのまま使用できます。または、CLI コマンドの「空白を埋めて」から実行することもできます。これらのコマンドを 1 つのデバイスで実行することも、コマンドを複数の ASA に同時に送信することもできます。
- CLI は、完全な ASA 構成ファイルを提供します。これを表示することも、上級ユーザーの場合は直接編集して変更を保存することもできます。CLI コマンドを実行して変更する必要はありません。

Cisco Security Analytics and Logging

追加のライセンスを使用すると、Syslog イベントと Netflow Secure Event Logging（NSEL）イベントを Cisco ASA から Secure Event Connector（SEC）に直接送信し、それから Cisco Cloud に転送できます。クラウドに転送されると、Security Cloud Control の [イベントログ（Event Logging）] ページでこれらのイベントを表示できます。そこでイベントをフィルタリングして確認することで、ネットワークでどのセキュリティルールがトリガーされているかを明確に把握できます。詳細情報は、「Cisco Security Cloud Control のイベント」を参照してください。



Cisco Security Analytics and Logging の導入方法の詳細は、ASA デバイスに安全なロギング分析（SaaS）を導入する を参照してください。

次の作業

これで、ASA の導入準備とポリシーのオーケストレーションを開始できます。

サポートが必要な場合

Security Cloud Control GUI のサポートメニューをクリックして、サポートに連絡して質問したり、製品ドキュメントを読んだりできます。

Security Cloud Control Firewall Management ダッシュボード

Security Cloud Control Firewall Management ダッシュボードは、さまざまなカテゴリにわたって組織レベルの詳細をモニタリングおよび管理するための中央ハブです。ログインすると、セキュリティと運用の効率を最適化するための重要なインサイトとアクションを提供するカスタマイズ可能なダッシュボードにアクセスできます。

ダッシュボードをカスタマイズする

表示されるウィジェットをカスタマイズして、特定のニーズに合わせてダッシュボードをカスタマイズします。

1. **[Home]** ページで、**[Customize]** をクリックします。
2. ダッシュボードウィジェットを選択または選択解除し、ドラッグアンドドロップして希望の順序に配置します。

上位情報

このセクションでは、さまざまなテナントレベルのメトリックに関する詳細なインサイトが提供されます。有効にすると、次のウィジェットが表示できます。

- **設定状態**：デバイス上の設定と、Security Cloud Control によって維持されているデバイス上の設定との不一致を示します。この比較は、存在する可能性のある不整合や競合を特定するのに役立ちます。

  詳細については、「デバイス管理」を参照してください。

- **変更ログ管理**： 変更ログを管理して、正確な運用管理を実現できます。ウィジェットには、**完了済み**の変更ログと**保留中**の変更ログが表示されます。

  詳細については、「ログの変更」を参照してください。

- **RA VPN セッション**：リモートアクセス VPN セッションをモニターするのに役立ちます。

  詳細については、「RA VPN セッション」を参照してください。

- **全体のインベントリ**：すべてのデバイスの正常性とステータスをモニターするのに役立ちます。ウィジェットには、**[Issues]**、**[Pending Actions]**、**[Other]**、**[Online]** に分類されたデバイス、およびハードウェアサポートの最終日に近づいているデバイス、またはすでにハードウェアサポートの最終日に達しているデバイスが表示されます。

  詳細については、「すべてのデバイス」を参照してください。

- **サイト間 VPN**： サイト間 VPN 接続を管理および評価するのに役立ちます。ウィジェットには、VPN トンネルの総数と、**アクティブ**および**アイドル**の割合が表示されます。

  詳細については、「サイト間 VPN」を参照してください。

- **アカウントとアセット**：

- マルチクラウドアカウントとリソースを効果的に追跡および管理できます。ここから Multicloud Defense Controller を起動できます。
- **[+Add Account]** をクリックして、新しいアカウントを追加します。

詳細については、「Multicloud Defense コントローラ」を参照してください。

- **トップリスク接続先**：アクセスが許可されている最も高リスクの接続先を特定してモニターするのに役立ちます。ウィジェットには、アプリケーションおよび URL カテゴリが一覧表示され、過去 90、60、または 30 日間のデータをフィルタ処理できます。**許可された**トラフィック（デフォルト）と**ブロックされた**トラフィックの間でフィルタ処理できます。
- **上位の侵入およびマルウェアイベント**：上位の侵入およびマルウェアイベントをモニターして対処するのに役立ちます。ウィジェットには、侵入イベントとマルウェアイベントが表示され、過去 90 日間、60 日間、および 30 日間のデータをフィルタ処理できます。**許可された**イベント（デフォルト）と**ブロックされた**イベントの間でフィルタ処理できます。

アナウンスメント

[Announcements] アイコンをクリックすると、最新の Security Cloud Control 機能と更新を確認できます。リストされている項目のいずれかについて詳細が必要な場合は、関連ドキュメントへのリンクが提供されます。

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。