オブジェクト

オブジェクトは、ポリシーまたはその他の設定で使用する基準を定義した再利用可能なコンテナです。たとえば、ネットワーク オブジェクトはホストとサブネットのアドレスを定義します。

オブジェクトを使用して基準を定義し、複数のポリシーでこの基準を簡単に再利用できます。オブジェクトを更新すると、そのオブジェクトを使用するすべてのポリシーが自動的に更新されます。

オブジェクト タイプ

次のタイプのオブジェクトを作成できます。ほとんどの場合、ポリシーまたは設定がオブジェクトを許可する場合、オブジェクトを使用する必要があります。

オブジェクト タイプ	主な用途	説明
セキュアクライアント プロファイル	リモート アクセス VPN	セキュアクライアントプロファイルは、セキュアクライアントソフトウェアとともにクライアントにダウンロードされます。これらのプロファイルでは、多くのクライアント関連オプション（スタートアップ時の自動接続、自動再接続など）や、エンドユーザーがセキュアクライアントの設定および詳細設定からオプションを変更することを許可するかどうかを定義します。 クライアント プロファイルの設定およびアップロードを参照してください。

オブジェクト タイプ	主な用途	説明
Application Filter	アクセス制御ルール	アプリケーション フィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネス関連性によってアプリケーションを定義するフィルタを定義します。ポート指定を使用する代わりに、ポリシーでこれらのオブジェクトを使用してトラフィックを制御できます。 アプリケーション フィルタ オブジェクトの設定 （11 ページ）を参照してください。
証明書	アイデンティティ ポリシー リモート アクセス VPN SSL 復号ルール。 管理 Web サーバ。	デジタル証明書は、認証に使用されるデジタル ID を保持しています。証明書は、HTTPS および LDAPS などの、SSL(Secure Socket Layer）、TLS（Transport Layer Security）、および DTLS（Datagram TLS）接続に使用されます。 「証明書の設定」を参照してください。
DNS グループ	管理インターフェイスとデータ インターフェイスの DNS 設定	DNS グループは、DNS サーバと一部の関連属性のリストを定義します。www.example.com などの完全修飾ドメイン名（FQDN）を IP アドレスに解決するには、DNS サーバが必要です。 DNS グループの設定を参照してください。
イベントリスト フィルタ	選択したログの宛先のシステムログ設定。	イベントリストフィルタは、syslog メッセージ用のカスタムフィルタリストを作成します。syslog サーバまたは内部ログ バッファなど、特定のログの場所に送信されるメッセージを制限するには、これらを使用できます。 イベント リスト フィルタの設定を参照してください。
位置情報	セキュリティ ポリシー	位置情報オブジェクトは、トラフィックの送信元または宛先となるデバイスをホストする国および大陸を定義します。IP アドレスを使用する代わりに、ポリシーでこれらのオブジェクトを使用してトラフィックを制御できます。 位置情報オブジェクトの設定 （16 ページ）を参照してください。

オブジェクト タイプ	主な用途	説明
アイデンティティ ソース	アイデンティティ ポリシー リモート アクセス VPN Device Manager アクセス	アイデンティティ ソースは、ユーザー アカウントを定義するサーバーとデータベースです。この情報は、IP アドレスに関連付けられているユーザー ID の提供や、Device Manager へのリモートアクセス VPN 接続またはアクセスを認証するなど、さまざまな方法で利用できます。 アイデンティティ ソースを参照してください。
IKE ポリシー	VPN	インターネット キー エクスチェンジ（IKE）ポリシー オブジェクトは、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動的な確立に使用される IKE プロポーザルを定義します。IKEv1 と IKEv2 には別個のオブジェクトがあります。 グローバル IKE ポリシーの設定を参照してください。
Ipsec プロポーザル	VPN	IPsec プロポーザル オブジェクトは IKE フェーズ 2 ネゴシエーション時に使用される IPsec プロポーザルを設定します。IPsec プロポーザルは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルとアルゴリズムの組み合わせを定義します。IKEv1 と IKEv2 には別個のオブジェクトがあります。 IPsec プロポーザルの設定を参照してください。
ネットワーク	セキュリティ ポリシーと多様なデバイス設定。	ネットワーク グループおよびネットワーク オブジェクト（まとめてネットワーク オブジェクトと呼ばれる）は、ホストまたはネットワークのアドレスを定義します。 ネットワーク オブジェクトとグループの設定 （6 ページ）を参照してください。
ポート	セキュリティ ポリシー	ポート グループおよびポート オブジェクト（まとめてポート オブジェクトと呼ばれる）は、トラフィックのプロトコル、ポート、または ICMP サービスを定義します。 ポート オブジェクトとグループの設定 （8 ページ）を参照してください。
秘密鍵	Smart CLI および FlexConfig ポリシー。	秘密鍵オブジェクトは、パスワードや、暗号化および非表示にするその他の認証文字列を定義します。 秘密キー オブジェクトの設定を参照してください。

オブジェクト タイプ	主な用途	説明
セキュリティ ゾーン	セキュリティ ポリシー	セキュリティ ゾーンは、複数のインターフェイスからなるグループです。ゾーンを使用するとネットワークがセグメントに分けられ、トラフィックの管理や分類に役立ちます。 セキュリティ ゾーンの設定 （9 ページ）を参照してください。
SGT グループ	アクセス制御ポリシー。	TrustSec セキュリティグループタグ（SGT）は、Cisco Identity Services Engine（ISE）で定義されたトラフィックのタグを定義します。これらのオブジェクトを作成するには ISE を設定する必要があります。その後、そのオブジェクトを、アクセス制御ルール内の送信元/宛先一致基準として使用できます。 セキュリティグループタグ（SGT）グループの設定 （18 ページ）を参照してください。
SLAモニタ	スタティック ルート	SLA モニタは、スタティックルートのモニタリングに使用するターゲットIPアドレスを定義します。ターゲット IP アドレスに到達できなくなったことをモニタが判断した場合、システムはバックアップ スタティック ルートをインストールできます。 SLA モニタ オブジェクトの設定を参照してください。
SSL 暗号	SSL設定。	SSL 暗号オブジェクトでは、Threat Defense への SSL 接続を確立するときに使用できるセキュリティレベル、TLS/DTLS プロトコルバージョン、および暗号化アルゴリズムの組み合わせを定義します。システム設定でこれらのオブジェクトを使用して、ボックスへのTLS/SSL接続を行うユーザのセキュリティ要件を定義します。 TLS/SSL暗号設定の設定を参照してください。

オブジェクト タイプ	主な用途	説明
Syslogサーバ	アクセス制御ルール 診断ロギング。 セキュリティ インテリジェンス ポリシー。 SSL復号ルール。 侵入ポリシー ファイル/マルウェアポリシー	Syslog サーバ オブジェクトは、コネクション型または診断システム ログ（syslog）メッセージを受信できるサーバを識別します。 syslog サーバの設定 （17 ページ）を参照してください。
URL	アクセス コントロール ルール セキュリティ インテリジェンス ポリシー。	Web リクエストの URL または IP アドレスを定義する URL オブジェクトおよびグループ（総称して URLオブジェクトと呼ばれます）。 URL オブジェクトとグループの設定 （13 ページ）を参照してください。
ユーザ	リモート アクセス VPN	リモートアクセス VPN とともに使用するために、デバイスでユーザ アカウントを直接作成できます。外部認証ソースの代わりに（または外部認証ソースに加えて）ローカル ユーザ アカウントを使用できます。 「ローカル ユーザの設定」を参照してください。

オブジェクトの管理

オブジェクトは、[オブジェクト（Objects）]ページから直接設定することも、ポリシーを編集するときに設定することもできます。どちらの方式でも同じ結果となり、新規または更新されたオブジェクトが作成されるので、その時点で適した方法を使用します。

次の手順では、[オブジェクト（Objects）]ページから直接オブジェクトを作成して管理する方法について説明します。

（注） ポリシーまたは設定を編集する際にプロパティにオブジェクトが必要な場合、すでに定義されたすべてのオブジェクトのリストが表示されるので、そこから適切なオブジェクトを選択します。必要なオブジェクトが存在しない場合は、リスト内に表示される [新しいオブジェクトの作成（Create New Object）] リンクをクリックします。

手順

ステップ 1 [オブジェクト（Objects）] を選択します。

[オブジェクト（Objects）]ページには目次があり、使用可能なタイプのオブジェクトがリストされます。オブジェクトタイプを選択すると、既存のオブジェクトのリストが表示され、そこから新しいオブジェクトを作成することができます。オブジェクトの内容とタイプも確認できます。

ステップ 2 目次からオブジェクト タイプを選択し、次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。オブジェクトのコンテンツはタイプによって異なります。具体的な情報については、各オブジェクトタイプの設定トピックを参照してください。
- グループ オブジェクトを作成するには、[グループの追加（Add Group）]（）ボタンをクリックします。グループ オブジェクトには複数の項目があります。
- オブジェクトを編集するには、そのオブジェクトの[編集（edit）]（）アイコンをクリックします。事前定義オブジェクトのコンテンツは編集できません。
- オブジェクトを削除するには、そのオブジェクトの [削除（delete）]（）アイコンをクリックします。ポリシーまたは別のオブジェクトで現在使用中のオブジェクトを削除することはできません。また、事前定義オブジェクトも削除できません。

ネットワーク オブジェクトとグループの設定

ネットワーク グループおよびネットワーク オブジェクト（まとめてネットワーク オブジェクトと呼ばれる）を使用して、ホストまたはネットワークのアドレスを定義します。その後、トラフィック一致基準を定義するためにセキュリティ ポリシーでオブジェクトを使用したり、サーバやその他のリソースのアドレスを定義する際に使用することができます。

ネットワーク オブジェクトは単一のホストまたはネットワーク アドレスを定義しますが、ネットワーク グループ オブジェクトは複数のアドレスを定義できます。

次の手順では、[オブジェクト（Objects）]ページからオブジェクトを直接作成および編集する方法を説明します。また、オブジェクトの一覧に表示される[新しいネットワークの作成（Create New Network）]リンクをクリックすることにより、アドレスプロパティの編集中にネットワーク オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [ネットワーク（Network）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- グループを作成するには、[グループの追加（Add Group）] ボタン（）をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前を入力し、オプションでオブジェクトの説明を入力してオブジェクトの内容を定義します。

オブジェクトの内容またはスタンドアロンIPアドレスからオブジェクト名を簡単に識別できるように、名前にIPアドレスだけを使用しないことを推奨します。名前にIPアドレスを使用する場合は、host-192.168.1.2やnetwork-192.168.1.0など、わかりやすいプレフィックスを付けてください。IP アドレスを名前として使用する場合は、縦線がプレフィックスとして追加されます（例：|192.168.1.2）。Device Manager ではオブジェクトセレクタに縦棒が表示されませんが、CLI で **show running-config** コマンドを使用して実行中の設定を調べると、この命名規則を確認できます。

ステップ 4 オブジェクトの内容を設定します。

ネットワークオブジェクト

オブジェクト [タイプ（Type）] を選択して、コンテンツを設定します。

- [ネットワーク（Network）]：次のいずれかの形式を使用してネットワーク アドレスを入力します。
  - サブネット マスクを含む IPv4 ネットワーク（例：10.100.10.0/24、10.100.10.0/255.255.255.0）。
  - プレフィックスを含む IPv6 ネットワーク（例：2001:DB8:0:CD30::/60 ）。
- [ホスト（Host）]：次のいずれかの形式を使用してホスト IP を入力します。
  - IPv4 ホスト アドレス（例：10.100.10.10）。
  - IPv6 ホスト アドレス（2001:DB8::0DB8:800:200C:417A または 2001:DB8:0:0:0DB8:800:200C:417A など）。
- [範囲]: 開始アドレスと終了アドレスをハイフンで区切ったアドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。たとえば、192.168.1.10-192.168.1.250 または 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100 とします。
- [FQDN]：www.example.com などの単一の完全修飾ドメイン名を入力します。ワイルドカードを使用することはできません。また、[DNS解決（DNS Resolution）] を選択して、IPv4 アドレス、IPv6 アドレス、または Ipv4 アドレスと IPv6 アドレスの両方を FQDN と関連付けるかどうかも決定します。デフォルトは、IPv4 と IPv6 の両方です。これらのオブジェ

クトは、アクセス制御ルールでのみ使用できます。ルールでは、DNSルックアップによって FQDN 用に取得された IP アドレスを照合します。

ネットワークグループ(Network Groups)

グループに追加するネットワークオブジェクトまたはグループを選択するには、[+] ボタンをクリックします。新しいオブジェクトを作成することもできます。

ステップ5 **[OK]** をクリックして変更を保存します。

ポート オブジェクトとグループの設定

ポート グループおよびポート オブジェクト（まとめてポート オブジェクトと呼ばれる）を使用して、トラフィックのプロトコル、ポート、ICMP サービスを定義します。その後、トラフィック一致基準を定義するためにセキュリティ ポリシーでオブジェクトを使用できます（たとえばアクセス ルールを使用して特定の TCP ポートへのトラフィックを許可する）。

ポート オブジェクトは単一のプロトコル、TCP/UDP ポートまたはポート範囲、ICMP サービスを定義しますが、ポート グループ オブジェクトは複数のサービスを定義できます。

システムには、一般的なサービス用の事前定義されたオブジェクトがいくつか用意されています。これらのオブジェクトをポリシーで使用できます。ただし、システム定義されたオブジェクトを編集/削除することはできません。

（注） ポート グループ オブジェクトを作成するときには、オブジェクトの組み合わせが適切であることを確認してください。たとえば、アクセスルールで送信元ポートと宛先ポートの両方を指定するために使用する目的で、1 つのオブジェクトにプロトコルを混在させることはできません。すでに使用されているオブジェクトを編集する場合は、そのオブジェクトを使用するポリシーを無効（使用不可）にしてしまわないよう、注意が必要です。

次の手順では、[オブジェクト（Objects）]ページからオブジェクトを直接作成および編集する方法を説明します。また、オブジェクトの一覧に表示される [新しいポートの作成（Create New Port）] リンクをクリックすることにより、サービス プロパティの編集中にポート オブジェクトを作成することもできます。

手順

ステップ1 [オブジェクト（Objects）] を選択し、次に目次から [ポート（Ports）] を選択します。

ステップ2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- グループを作成するには、[グループの追加（Add Group）] ボタン（  ）をクリックします。

- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力し、オブジェクトの内容を定義します。

ポート オブジェクト

[プロトコル（Protocol）] を選択し、そのプロトコルを次のように設定します。

- [TCP（TCP）]、[UDP（UDP）]：単一のポートまたはポート範囲を入力します。たとえば「80」（HTTP の場合）や「1 ～ 65535」（すべてのポートが対象）のように入力します。
- [ICMP]、[IPv6-ICMP]：[種類（Type）] で ICMP、任意で [コード（Code）] を選択します。タイプをすべての ICMP メッセージに適用するには、[任意（Any）] を選択します。タイプとコードについての詳細は、次のページを参照してください。
  - ICMP—http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6—http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- [その他（Other）]：適切なプロトコルを選択します。

Port Groups

グループに追加するポート オブジェクトを選択するには、[+] ボタンをクリックします。また、新しいオブジェクトを作成することもできます。

ステップ 4 **[OK]** をクリックして変更を保存します。

セキュリティ ゾーンの設定

セキュリティ ゾーンは、複数のインターフェイスからなるグループです。ゾーンを使用するとネットワークがセグメントに分けられ、トラフィックの管理や分類に役立ちます。複数のゾーンを定義できますが、1 つのインターフェイスは 1 つのゾーンにしか含めることができません。

システムは、初期設定時に次のゾーンを作成します。これらのゾーンを編集してインターフェイスを追加/削除できます。また、不要になったゾーンを削除することもできます。

- **inside_zone**：内部インターフェイスが含まれます。内部インターフェイスがブリッジグループである場合、このゾーンには内部ブリッジ仮想インターフェイス（BVI）ではなく、すべてのブリッジ グループ メンバー インターフェイスが含まれます。このゾーンは、内部ネットワークを表します。
- **outside_zone**：外部インターフェイスが含まれます。このゾーンは、インターネットなど、制御範囲の外にあるネットワークを表します。

通常は、ネットワーク内での役割に従ってインターフェイスをグループ化します。たとえば、インターネットに接続するインターフェイスを [outside_zone] セキュリティ ゾーンに配置し、内部ネットワーク用のすべてのインターフェイスを [inside_zone] セキュリティ ゾーンに配置します。その後、外部ゾーンから着信して内部ゾーンに向かうトラフィックにアクセス制御ルールを適用できます。

ゾーンを作成する前に、ネットワークに適用するアクセス ルールやその他のポリシーを検討してください。たとえば、すべての内部インターフェイスを同じゾーンに配置する必要はありません。内部ネットワークが 4 つ存在していて、その 1 つを他の 3 つとは別に扱う必要がある場合は、ゾーンを 1 つではなく 2 つ作成できます。パブリック Web サーバへの外部アクセスを許可すべきインターフェイスがある場合、そのインターフェイス用に別個のゾーンを使用できます。

次の手順では、[オブジェクト（Objects）] ページからオブジェクトを直接作成および編集する方法を説明します。また、オブジェクトの一覧に表示される [新しいセキュリティ ゾーンの作成（Create New Security Zone）] リンクをクリックすることにより、セキュリティ ゾーン プロパティの編集中にセキュリティ ゾーンを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、次に目次から [セキュリティゾーン（Security Zones）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前を入力し、任意で説明を入力します。

ステップ 4 ゾーンの [モード（Mode）] を選択します。

このモードはインターフェイスのモードに直接関係します。ゾーンには、1 つのタイプのインターフェイスを含めることができます。

- [ルーテッド（Routed）] : ルーテッドインターフェイスは、セキュリティポリシーを適用できる通過トラフィック用の通常のインターフェイスです。
- [パッシブ（Passive）] : パッシブインターフェイスは、デバイスを通過するトラフィックに影響を与えません。
- [インライン（Inline）] : インラインインターフェイスは、IPS 処理に使用されるインラインセットのメンバーです。

ステップ 5 [インターフェイス（Interfaces）] リストで、[+] をクリックし、ゾーンに追加するインターフェイスを選択します。

一覧には、その時点でゾーンに含まれていないすべての名前付きインターフェイスが表示されます。インターフェイスをゾーンに追加するには、その前にインターフェイスを設定して名前を付ける必要があります。

すべての名前付きインターフェイスがすでにゾーンに含まれている場合、この一覧には何も表示されません。あるインターフェイスを別のゾーンに移動するには、まず現在のゾーンから削除する必要があります。

（注）
□ブリッジグループインターフェイス（BVI）をゾーンに追加することはできません。代わりに、メンバーインターフェイスを追加してください。異なるゾーンにメンバーを配置することができます。

ステップ 6 **[OK]** をクリックして変更を保存します。

アプリケーション フィルタ オブジェクトの設定

アプリケーション フィルタ オブジェクトは、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネス関連性によってアプリケーションを定義するフィルタを定義します。ポート指定を使用する代わりに、ポリシーでこれらのオブジェクトを使用してトラフィックを制御できます。

個別のアプリケーションを指定することもできますが、アプリケーションフィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高くビジネス関連性が低いすべてのアプリケーションを識別してブロックするアクセス制御ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

アプリケーション フィルタ オブジェクトを使用せずに、アプリケーションやアプリケーションフィルタをポリシーで直接選択することもできます。しかし、同じグループに属するアプリケーションやフィルタに関して複数のポリシーを作成する必要がある場合は、オブジェクトが便利です。システムには事前定義されたアプリケーションフィルタが複数用意されています。これらを編集/削除することはできません。

（注） シスコは、システムや脆弱性データベース（VDB）の更新プログラムにより、追加のアプリケーション検出機能を頻繁に更新および追加しています。これにより、リスクの高いアプリケーションをブロックするルールが新しいアプリケーションに自動的に適用され、手動でルールを更新する必要がなくなります。

次の手順では、[オブジェクト（Objects）] ページからオブジェクトを直接作成および編集する方法を説明します。また、アプリケーション基準を [アプリケーション（Applications）] タブに追加してから [フィルタとして保存（Save As Filter）] リンクをクリックすることにより、ア

クセス制御ルールの編集中にアプリケーション フィルタ オブジェクトを作成することもできます。

始める前に

フィルタを編集するときに、選択したアプリケーションが VDB の更新によって削除された場合は、アプリケーション名の後に「Deprecated（廃止）」が表示されます。これらのアプリケーションはフィルタから削除する必要があります。それ以降の展開では、システム ソフトウェアのアップグレードがブロックされます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [アプリケーションフィルタ（Application Filters）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 [アプリケーション（Applications）] リストで [追加 +（Add +）] をクリックし、オブジェクトに追加するアプリケーションやフィルタを選択します。

最初のリストには、継続的にスクロールされる一覧形式でアプリケーションが表示されます。[高度なフィルタ（Advanced Filter）] をクリックすると、フィルタ オプションが表示され、アプリケーションを選択しやすくなります。選択が完了したら [追加（Add）] をクリックします。このプロセスを繰り返して、アプリケーションやフィルタを追加できます。

（注）
1 つのフィルタ条件内での複数の選択は OR 関係にあります。「リスクが高い OR 非常に高い」という具合です。フィルタ間の関係は AND であり、「リスクが高い OR 非常に高い AND ビジネスとの関連性は低い OR 非常に低い」となります。フィルタを選択するごとに、アプリケーションの一覧が更新され、条件に一致するものだけが表示されます。これらのフィルタを使用して、個別に追加するアプリケーションの検索や、フィルタ基準をルールに追加する際に目的のアプリケーションが対象となっているかを確認できます。

リスク

アプリケーションが、組織のセキュリティ ポリシーに違反して使用される可能性：非常に低い～非常に高い。

ビジネスとの関連性

アプリケーションが、娯楽としてではなく、組織のビジネス活動の範囲内で使用される可能性：非常に低い～非常に高い。

種類

アプリケーションのタイプ：

- **アプリケーション プロトコル**：HTTPやSSHなどのホスト間の通信を表すアプリケーション プロトコル。
- **クライアント プロトコル**：Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント。
- **Web アプリケーション**：HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

カテゴリ

アプリケーションの最も基本的な機能を表す一般的な分類。

タグ

アプリケーションに関する追加の情報。カテゴリに類似。

暗号化されたトラフィックの場合、システムがトラフィックを識別してフィルタ処理できるのは **SSL プロトコル**のタグが付けられたアプリケーションのみです。このタグが付いていないアプリケーションは、暗号化されていない、または復号されたトラフィックでのみ検出可能です。また、システムは**復号トラフィック**タグを、復号されたトラフィックでのみ検出できるアプリケーションに割り当てます。（暗号化されたトラフィックや暗号化されていないトラフィックで検出されるアプリケーションには割り当てない）

アプリケーション一覧（画面下部）

この一覧は、上部のフィルタ オプションを選択するごとに更新されるため、現在のフィルタに一致するアプリケーションのみを確認できます。この一覧を使用することで、フィルタ基準をルールに追加する際に目的のアプリケーションが対象となっているかを確認できます。特定のアプリケーションを追加しようとしている場合、このリストからそのアプリケーションを選択します。

ステップ 5 **[OK]** をクリックして変更を保存します。

URL オブジェクトとグループの設定

URL オブジェクトとグループ（URL オブジェクトと総称する）を使用して、Web リクエストの URL または IP アドレスを定義します。これらのオブジェクトを使用して、アクセス制御ポリシーに手動の URL フィルタリング、またはセキュリティ インテリジェンス ポリシーにブロッキングを実装できます。

URL オブジェクトは単一の URL または IP アドレスを定義するのに対して、URL グループ オブジェクトは複数の URL またはアドレスを定義できます。

URL オブジェクトを作成するときには、次の点に注意してください。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバーのホスト名のみに基づきます。1 つ以上の / を含める場合、文字列の部分一致には URL 文字列全体が使用されます。次に、次のいずれかに該当する場合、URL は一致と見なされます。
  - 文字列が URL の先頭にある。
  - 文字列がドットの後に続く。
  - 文字列の先頭にドットが含まれている。
  - 文字列が :// 文字の後に続く。

  たとえば、ign.com は ign.com および www.ign.com と一致するが、verisign.com とは一致しません。

（注） サーバーは再構成でき、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部（つまり / 文字を含む URL 文字列）をブロックまたは許可するために手動の URL フィルタリングは使用しないことをお勧めします。

- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成するときに、プロトコルを指定する必要はありません。たとえば、http://example.com ではなく example.com を使用します。
- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。また、システムはサブジェクト共通名に含まれるサブドメインを無視するので、サブドメイン情報を含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

  ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリング ルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。

（注） 証明書情報を利用できないためにブラウザがTLSセッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

次に、[オブジェクト（Objects）]ページで直接オブジェクトを作成および編集する方法について説明します。また、オブジェクトの一覧に表示される[新しいURL作成（CreateNewURL）]リンクをクリックすることにより、URL プロパティの編集中に URL オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、次に目次から [URL] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- グループを作成するには、[グループの追加（Add Group）] ボタン（）をクリックします。
- オブジェクトまたはグループを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトのごみ箱アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 オブジェクトのコンテンツを定義します。

URL オブジェクト

[URL] ボックスに URL または IP アドレスを入力します。[URL] ではワイルドカードを使用できません。

URL グループ

グループに追加する URL オブジェクトを選択するには、[+] ボタンをクリックします。また、新しいオブジェクトを作成することもできます。

ステップ 5 **[OK]** をクリックして変更を保存します。

位置情報オブジェクトの設定

位置情報オブジェクトは、トラフィックの送信元または宛先となるデバイスをホストする国および大陸を定義します。IPアドレスを使用する代わりに、ポリシーでこれらのオブジェクトを使用してトラフィックを制御できます。たとえば、地理的な場所を使用すると特定の国へのアクセスを簡単に制限できます。その際、その地域で使用される可能性のある IP アドレスをすべて把握する必要はありません。

通常は、位置情報オブジェクトを使用しなくても、地理的な場所をポリシーで直接選択することもできます。しかし、同じグループの国や大陸に対して複数のポリシーを作成する必要がある場合、オブジェクトは便利です。

（注） 地理的な場所の最新データをトラフィック フィルタリングに確実に使用するために、位置情報データベース（GeoDB）を定期的に更新することを強く推奨します。

次の手順では、[オブジェクト（Objects）]ページからオブジェクトを直接作成および編集する方法を説明します。また、オブジェクトの一覧に表示される [新しい位置情報の作成（Create New Geolocation）] リンクをクリックすることにより、ネットワーク プロパティの編集中に位置情報オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [地理位置情報（Geolocation）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 [大陸/国（Continents/Countries）] リストで、[追加＋（Add＋）] をクリックし、オブジェクトに追加する大陸や国を選択します。

大陸を選択すると、その大陸内のすべての国が選択されます。

ステップ 5 **[OK]** をクリックして変更を保存します。

syslog サーバの設定

Syslog サーバ オブジェクトはコネクション型または診断システム ログ（syslog）メッセージを受信可能なサーバを識別します。Syslog サーバにログ収集と分析のための設定がある場合は、オブジェクトを作成してそれらを定義し、関連ポリシーでこのオブジェクトを使用します。

以下のイベントタイプをsyslogサーバに送信できます。

- 接続イベント。次のポリシーのタイプで syslog サーバ オブジェクトを構成します：アクセス制御ルールとデフォルト アクション、SSL 復号ルールとデフォルト アクション、セキュリティ インテリジェンス ポリシー。
- 侵入イベント。侵入ポリシーで syslog サーバ オブジェクトを構成します。
- 診断イベント。リモート syslog サーバのロギングの設定を参照してください。
- ファイル/マルウェアイベント。**[デバイス]**>**[システム設定]**>**[ロギング設定]**でsyslogサーバを設定します。

次に、[オブジェクト（Objects）]ページで直接オブジェクトを作成および編集する方法について説明します。また、オブジェクトの一覧に表示される [syslog サーバの追加（Add Syslog Server）] リンクをクリックすることにより、syslog サーバ プロパティの編集中に syslog サーバ オブジェクトを作成することもできます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [Syslog サーバ（Syslog Servers）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 syslog サーバのプロパティを次のように設定します。

- [IP アドレス（IP Address）]：syslog サーバの IP アドレスを入力します。
- [プロトコルタイプ（Protocol Type）]、[ポート番号（Port Number）]：プロトコルを選択して、syslog に使用するポート番号を入力します。デフォルトは UDP/514 です。[TCP] を選択すると、システムはsyslogサーバが利用できない場合を認識して、サーバが再度利用可能になるまでイベントの送信を停止することができます。デフォルト UDP ポートは 514、デフォルト TCP ポートは 1470 です。デフォルトを変更する場合、ポートは 1025 ～ 65535 の範囲にする必要があります。

（注）

トランスポートプロトコルとして TCP を使用する場合、メッセージが失われないように syslog サーバーへの接続が 4 つ開きます。syslog サーバーを使用して非常に多数のデバイスからメッセージを収集する場合、接続オーバーヘッドの合計がサーバーに対して大きすぎる場合は、代わりに UDP を使用します。

- [デバイスログのインターフェイス（Interface for Device Logs）]：診断 syslog メッセージの送信に使用するインターフェイスを選択します。接続、侵入、ファイル、マルウェアの各イベントタイプでは、常に管理インターフェイスが使用されます。インターフェイスの選択によって、syslog メッセージに関連付けられる IP アドレスが決まります。次のオプションのいずれかを選択します。
  - [データインターフェイス（Data Interface）]：選択したデータ インターフェイスを診断 syslog メッセージに使用します。ブリッジ グループ メンバー インターフェイス経由でサーバにアクセス可能な場合は、代わりにブリッジグループインターフェイス（BVI）を選択してください。診断インターフェイス(物理的な管理インターフェイス)経由でアクセスできる場合は、このオプションではなく[管理インターフェイス]を選択することを推奨します。パッシブインターフェイスを選択することはできません。

    データインターフェイスで通信する場合、接続、侵入、ファイル、およびマルウェアの syslog メッセージでは、送信元 IP アドレスが管理インターフェイスかゲートウェイ インターフェイスで使用されます。前述のイベントタイプ用に選択したインターフェイスから syslog サーバにトラフィックを転送するための適切なルートが、ルーティングテーブルに存在する必要があることに注意してください。
  - [管理インターフェイス]: すべてのタイプのsyslogメッセージに仮想的な管理インターフェイスを使用します。データインターフェイス経由でルーティングする場合、送信元IPアドレスが管理インターフェイスまたはゲートウェイ インターフェイスで使用されます。

ステップ 4 **[OK]** をクリックして変更を保存します。

セキュリティグループタグ（SGT）グループの設定

セキュリティグループタグ（SGT）グループオブジェクトを使用して、Identity Services Engine（ISE）によって割り当てられた SGT に基づいて送信元アドレスまたは宛先アドレスを識別します。その後、トラフィックの一致基準を定義するためにアクセス制御ルールでオブジェクトを使用できます。

ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりに、ダウンロードした SGT 情報を参照する SGT グループを作成する必要があります。SGT グループは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションに基づいてポリシーを適用できます。

アクセス制御のために SGT を使用する方法の詳細については、TrustSec セキュリティ グループ タグを使用したネットワーク アクセスの制御方法 を参照してください。

始める前に

SGT グループを作成する前に、SXP マッピングをサブスクライブして変更を展開するように ISE アイデンティティソースを設定する必要があります。その後、システムは ISE サーバから SGT 情報を取得します。SGT をダウンロードした後にのみ、SGT グループを作成できます。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、目次から [SGTグループ（SGT Groups）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 3 オブジェクトの名前を入力し、任意で説明を入力します。

ステップ 4 [タグ（Tags）] で、[+] をクリックし、ダウンロードした SGT を選択してオブジェクトに含めます。

SGT を削除するには、タグ名の右横にある [x] をクリックします。

リストが空の場合、システムはSGTマッピングをダウンロードできませんでした。この場合、次のようになります。

- ISE アイデンティティ オブジェクトが SXP トピックをサブスクライブしていることを確認します。マッピングを取得するには、SXP をサブスクライブする必要があります。
- ISE で静的マッピングが定義されていることと、これらのマッピングをパブリッシュするように ISE が設定されていることを確認します。マッピングが存在しない場合は、単にダウンロードされるものはありません。ISE でのセキュリティグループと SXP パブリッシングの設定を参照してください。

ステップ 5 **[OK]** をクリックします。

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。