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内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 アドレスとサブネット アドレスを定義します。

オブジェクトでは基準を定義することができ、同じ基準を異なるポリシーで簡単に再利用できるようになります。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によって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
AnyConnect Client プロファイル	リモート アクセス VPN	AnyConnect Clientプロファイルは、AnyConnect Client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AnyConnect Client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
アプリケーション フィルタ	アクセス コントロール 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、またはビジネスとの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。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、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 を提供します。証明書は、SSL（セキュア ソケット レイヤ）、TLS（Transport Layer Security）、および DTLS（データグラム TLS）接続（HTTPS や LDAPS など）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 サーバーおよび関連付けられているいくつかの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のには、DNS サーバーが必要です。 「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 サーバーまたは内部ログ 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（GeoLocation）	セキュリティ ポリシー	地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IP アドレスを使用する代わりに、これらのオブジェクトをポリシーで使用してトラフィックを制御できます。 地理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 Firewall 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、Firewall 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（SAS）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 に対して、異なる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 プロポーザルでは、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 に対して、異なる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 ポリシーおよびさまざまなデバイス設定	ホストまたはネットワークのアドレスを定義するネットワーク グループおよびネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ばれます）。 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（Port）]	セキュリティ ポリシー	トラフィックのプロトコル、ポート、または ICMP サービスを定義するポート グループおよびポート オブジェクト（総称してポート オブジェクトと呼ばれます）。 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。
秘密キー	Smart CLI および FlexConfig ポリシー	秘密キー 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 ゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。 「セキュリティ ゾーンの設定 （10 ページ）」を参照してください。
SGT グループ	アクセス コントロール 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 モニター	スタティック ルート	SLA モニターは、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 モニター オブジェクトの設定」を参照してください。
SSL 暗号化	SSL 設定	SSL 暗号オブジェクトでは、Firewall 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 接続を行うユーザー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 コントロール 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 サーバーのオブジェクトはコネクション型メッセージ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ーを指定します。 Syslog サーバーの設定 （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 （14 ページ）を参照してください。
Users	リモート アクセス VPN	リモート アクセス VPN で使用するユーザー アカウントをデバイスで直接作成できます。外部認証ソースの代わりに、またはそれに加えて、ローカル ユーザー アカウントを使用できます。 ローカル ユーザーの設定 を参照してください。

オブジェクトに関するガイドラインと制限事項

- オブジェクトは、同じ名前スペースを共有します。異なるタイプのオブジェクトであっても、2 つのオブジェクトに同じ名前を使用することはできません。
- 次の名前はシステムにより予約済みと見なされます。これらの名前はオブジェクト名として使用できません：object、network、host、fqdn、no、range、subnet、description、nat、after-auto、source、destination、static、dynamic、any、dns、inactive、interface、service、pat-pool、round-robin、extended、flat、include-reserve、tcp、udp、no-proxy-arp、route-lookup、remark、rule-id、access-list、line、ip、icmp、icmp6、advanced、ifc、object-group、vlan、event-log、flow-start、flow-end、both、permit、trust、deny、group-object。

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、ポリシーの編集時に設定することもできます。いずれの方法でも同じく新規または更新されたオブジェクトが作成されるため、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および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と、プロパティにオブジェクトが必要な場合、すでに定義されているオブジェクトのリストが表示されるため、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まだ存在しない場合は、リストに表示される [新規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、使用可能なオブジェクトタイプが一覧表示される目次があります。オブジェクトタイプを選択すると、既存オブジェクトのリストが表示され、新しいオブジェクトを作成できます。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。オブジェクトの内容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含まれます。
- 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。定義済みオブジェクトの内容は編集できません。
- 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。ポリシーや別のオブジェクトで現在使用されているオブジェクト、または定義済みのオブジェクトは削除できません。

ネットワーク オブジェクトとグループの設定

ホストまたはネットワークのアドレスを定義するには、ネットワーク グループとネットワーク オブジェクト（ネットワーク オブジェクトと総称される）を使用します。これらのオブジェク

トは、トラフィックの一致条件を定義するためにセキュリティ ポリシーで使用するか、サーバーその他のリソースのアドレスを定義するために設定で使用できます。

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。アドレス プロパティの編集時に、オブジェクト リストに表示される [新しいネットワークの作成（Create New Network）] リンクをクリックして、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）。Firewall 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

オブジェクトの [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（10.100.10.0/24、10.100.10.0/255.255.255.0 など）。
  - プレフィックスを含む IPv6 ネットワーク（2001:DB8:0:CD30::/60 など）。

- [ホスト（Host）]：次のいずれかの形式を使用してホスト IP アドレスを入力します。
  - IPv4 ホスト アドレス（10.100.10.10 など）。
  - 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（Range）]：ハイフンで区切られた開始アドレスと終了アドレスを備えたアドレスの範囲。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のみで使用できます。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

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

トラフィックのプロトコル、ポート、またはICMPサービスを定義するには、ポート グループとポート オブジェクト（まとめてポート オブジェクトと呼ぶ）を使用します。その後、トラフィックの一致基準を定義するためのセキュリティ ポリシーのオブジェクトを使用して、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できます。

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、または 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、一般的なサービス向けの複数の事前定義されたオブジェクトが含まれています。これらのオブジェクトはポリシーで使用できます。ただし、システムで定義されたオブジェクトは、編集または削除ができません。

（注） ポート グループ オブジェクトを作成する場合、オブジェクトの組み合わせが有効であることを確認してください。たとえば、あるオブジェクトをアクセス ルールで送信元と宛先ポートの両方を指定するために使用する場合、そのオブジェクトに複数のプロトコルを組み合わ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注意してください。オブジェクトを使用するポリシーが無効（かつディセーブル）になる場合があります。

次に、オブジェクト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について説明します。オブジェクト リストに表示される [新規ポートの作成（Create New Port）] リンクをクリックすることで、サービスのプロパティを編集しながらポート 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、次のようにプロトコルを設定します。

- **TCP**、**UDP**：単一のポートまたはポート範囲の番号を入力します（たとえば80（HTTPの場合）または 1-65535（すべてのポートをカバー））。
- **ICMP**、**IPv6 ICMP**：ICMP の [タイプ（Type）] を選択し、オプションで [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）]：目的のプロトコルを選択します。

ポート グループ

[+] ボタンは、グループに追加するポート オブジェクトを選択するためにクリックします。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 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とはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。

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または削除したり、使用しなくなったゾーンを削除したりできます。

- **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の制御不可能な外部ネットワークを表すことを目的としています。

通常、ネットワーク内で果たす役割によって、インターフェイスをグループ化します。たとえば、インターフェイス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、内部ネットワークに接続するすべてのインターフェイスを **inside_zone** セキュリティ ゾーンに配置できます。次に、外部ゾーンから来て内部ゾーンへ向かうトラフィックにアクセス コントロール 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。4 つの内部ネットワークがあり、1 つだけ他の 3 つとは異なる処理をしたい場合、1 つではなく 2 つのゾーンを作成できます。パブリック Web サーバへの外部アクセスを許可するインターフェイスがある場合、そのインターフェイスに別のゾーンを使用できます。

次に、オブジェクト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について説明します。オブジェクト リストに表示される [新規セキュリティ ゾーンの作成（Create New Security Zone）] リンクをクリックすることで、セキュリティ ゾーンのプロパティを編集しながらセキュリティ 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、さらにオプション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。

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。

このリストは、現在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を表示します。インターフェイスをゾーンに追加するには、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ある場合、リストは空になります。別のゾーンにインターフェイスを移動しようとする場合、最初に現在のゾーンから削除する必要があります。

（注）
ゾーンにブリッジ グループ インターフェイス（BVI）を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ます。メンバーを異なるゾーンに配置できます。

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、またはビジネスとの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。ポートの仕様を使用する代わりに、これらのオブジェクトをポリシーで使用し、トラフィックを制御できます。

個々のアプリケーションを指定することはできますが、アプリケーションフィルタはポリシーの作成や管理を簡素化します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセス コントロール 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、ポリシーのアプリケーションとアプリケーション フィルタを直接選択できます。ただし、同じアプリケーションまたはフィルタ グループに対して複数のポリシーを作成する場合にはオブジェクトが便利です。システムには、事前に定義されたいくつかのアプリケーションフィルタが含まれていて、これらは編集または削除できません。

（注） シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーションディテクタを更新し追加しています。そのため、手動でルールを更新することなく、高リスクのアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

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および編集する方法について説明します。[アプリケーション（Applications）]タブにアプリケーション基準を追加した後、[フィルタとして保存（Save As Filter）]リンクをクリックして、アクセス コントロール ルールを編集しながら、アプリケーション フィルタ オブジェクトも作成できます。

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と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するリストでアプリケーションが表示されます。[フィルタの詳細設定（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容易に選択できます。選択したら、[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。たとえば、リスクが「高（High）」または（OR）「非常に高い（VeryHigh）」となります。フィルタ間の関係は「論理積（AND）」であるため、リスクが「高（High）」または（OR）「非常に高い（Very High）」であり、かつ（AND）ビジネスとの関連性が「低（Low）」または（OR）「非常に低い（Very Low）」

となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりできます。

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反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

ビジネスとの関連性

アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

タイプ

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（Application Protocol）]：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（Client Protocol）]：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（Web Application）]：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（**Categories**）

アプリケーションの最も重要な機能を説明する一般分類。

[タグ（Tags）]

カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは [SSLプロトコル（SSL Protocol）] とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグが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できます。また、システムは、復号されたトラフィック（暗号化された、または暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに [復号されたトラフィック（decrypted traffic）] タグを割り当てます。

アプリケーション リスト（ディスプレイ下部）

上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。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場合は、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場合は、オブジェクトの作成時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。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は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。オブジェクト リストに表示される [新規 URL の作成（Create New URL）] リンクをクリックすることで、URL のプロパティを編集しながら 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 オブジェクトの内容を定義します。

URL オブジェクト

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

URL グループ

[+] ボタンは、グループに追加する URL オブジェクトを選択するためにクリックします。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。

地理位置情報オブジェクトの設定

地理位置情報オブジェクトは、トラフィックの送信元または接続先であるデバイスをホストする国と大陸を定義します。IPアドレスを使用する代わりに、これらのオブジェクトをポリシーで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して、使用されている可能性のある IP アドレスすべてを把握する必要なしに、特定の国へのアクセスを簡単に制限できます。

通常は、地理位置情報オブジェクトを使用せずに、地理的な場所をポリシーで直接選択できます。とはいえ、同じ国や大陸のグループのために複数のポリシーを作成する場合、オブジェクトが便利です。

（注） 常に最新の地理位置情報データを使用してトラフィックをフィルタ処理できるように、地理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お勧めします。

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。ネットワークプロパティの編集時に、オブジェクトリストに表示される [新しい地理位置情報の作成（Create New Geolocation）] リンクをクリックして、地理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 [大陸または国（Continents/Countries）] リストで [追加＋（Add＋）] をクリックして、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、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 サーバーの設定

syslog サーバーのオブジェクトはコネクション型メッセージ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ーを指定します。syslog サーバー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 サーバー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（Device）]**>**[システム設定（System Settings）]**>**[ロギング設定（Logging Settings）]** で syslog サーバーを設定します。

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。オブジェクト リストに表示される [Syslogサーバーの追加（Add Syslog Server）] リンクをクリックすることで、syslog サーバーのプロパティを編集しながら syslog サーバー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 [Syslogサーバー（Syslog Server）] 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 サーバーのプロパティを設定します。

- [IPアドレス（IP Address）]：syslog サーバーの 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 サーバーが利用できない場合を認識して、サーバーが再度利用可能になるまでイベントの送信を停止できます。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は、1025 ～ 65535 の範囲のポートを使用してください。

（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。サーバーがブリッジグループのメンバーインターフェイスを介してアクセスできる場合、代わりにブリッジ グループ インターフェイス（BVI）を選択します。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（Management Interface）] 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サーバー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（Management Interface）]：すべてのタイプの syslog メッセージに仮想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 サーバーから 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、さらにオプション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 パブリッシングの構成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。

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。