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、ポリシーや設定によりオブジェクトが許可されている場合は、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
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 オブジェクトでは、IP 接続で使用されるアプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネス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、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，（8 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
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では、トラフィックの送信元または宛先であるデバイスをホストする国や大陸を定義します。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。 地理位置情報オブジェクトの設定, （12 ページ）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 オブジェクトでは、IPsec ピアの認証、IPsec 暗号化キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーションの自動確立に使用される IKE プロポーザルを定義します。IKEv1 と IKEv2 には個別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 の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 には個別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およびさまざまなデバイスの設定。	ネットワーク グループとネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ぶ）では、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, （4 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 グループとポート オブジェクト（総称してポート オブジェクトと呼ぶ）では、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, （5 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
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、インターフェイスのグループです。ゾーンでネットワークを複数のセグメントに分割することで、トラフィックの管理と分類が容易になります。 セキュリティ ゾーンの設定, （7 ページ）を参照してください。
syslog サーバ	アクセス コントロール ルール、診断ロギング。	syslog サーバ 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を特定します。 syslog サーバの設定, （13 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。	URL オブジェクトとグループ（総称して URL オブジェクトと呼ぶ）では、Web 要求の URL または IP アドレスを定義します。 URL オブジェクトとグループの設定, （11 ページ）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きにプロパティにオブジェクトが必要な場合は、すでに定義されているもののリストが表示されるため、適切なオブジェクトが選択してください。目的のオブジェクトがまだない場合は、リストに表示される [オブジェクトの新規作成（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 タイプを示すコンテンツ テーブルがあります。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ます。

ここから新しいオブジェクトを作成することもできます。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 コンテンツ テーブルからオブジェクト 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。固有の情報については、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アイテムが含まれます。
- オブジェクトを編集するには、そのオブジェクトの編集アイコン（）をクリックします。事前定義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 グループとネットワーク オブジェクト（総称してネットワーク オブジェクトと呼ぶ）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、オブジェクトは、トラフィックの一致基準を定義するためにセキュリティ ポリシーで使用したり、サーバやその他のリソースのアドレスを定義するための設定で使用したりできます。

ネットワーク オブジェクトで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 オブジェクトで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 プロパティを編集している間に、オブジェクト リストに表示される [新規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、[グループを追加（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、オブジェクトのゴミ箱アイコン（）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、任意で説明を入力して、オブジェクトの内容を定義します。

ネットワーク オブジェクト

オブジェクトの [タイプ（Type）]（[ネットワーク（Network）] または [ホスト（Host）]）を選択します。次に、ホストまたはネットワーク アドレスを入力します。次の形式を使用できます。

- IPv4 ホスト アドレス（10.100.10.10 など）。
- 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）。
- IPv6 ホスト アドレス（2001:DB8::0DB8:800:200C:417A、2001:DB8:0:0:0DB8:800:200C:417A 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）。

ネットワーク グループ

[+]ボタンをクリックして、グループに追加するネットワーク オブジェクトを選択します。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。

ポート オブジェクトとグループの設定

ポート グループとポート オブジェクト（総称してポート オブジェクトと呼ぶ）を使用して、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。その後、オブジェクトは、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 ポリシーで使用したり、特定の TCP ポートへのトラフィックを許可するアクセス ルールを使用するために使用したりできます。

ポート オブジェクトでは、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 オブジェクトでは複数のサービスを定義できます。

システムには共通サービスのための複数の定義済みオブジェクトが含まれています。それらのオブジェクトはユーザのポリシーで使用できます。ただし、システム定義オブジェクトの編集や削除はできません。

（注） ポート グループ オブジェクトを作成する場合は、意味のあるオブジェクトの組み合わせにしてください。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場合、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注意してください。そのオブジェクトを使用するポリシーを無効にしてしまう可能性があります。

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。サービス プロパティを編集している間に、オブジェクト リストに表示される [ポートの新規作成（Create New Port）]リンクをクリックして、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、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、[グループを追加（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、オブジェクトのゴミ箱アイコン（）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、任意で説明を入力して、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]：単一ポートの番号またはポート範囲の番号を入力します。例、80（HTTP の場合）、または 1 ～ 65535（全ポートを対象にする場合）
- [ICMP]、[IPv6-ICMP]：ICMP [タイプ（Type）] を選択し、任意で [コード（Code）]を選択します。すべての ICMP メッセージに適用するタイプの場合は、[すべて（Any）] を選択します。タイプとコードの詳細については、次の各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

[+]ボタンをクリックして、グループに追加するポート オブジェクトを選択します。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 ゾーンは、インターフェイスのグループです。ゾーンでネットワークを複数のセグメントに分割することで、トラフィックの管理と分類が容易になります。複数のゾーンを定義できますが、特定のインターフェイスは 1 つのゾーンにのみ定義できます。

初期設定時に次のゾーンが作成されます。それらのゾーンを編集して、インターフェイスの追加や削除ができます。また、不要になったゾーンは削除できます。

- [inside_zone]：内部インターフェイスが含まれています。内部インターフェイスがブリッジ グループの場合、このゾーンには、内部の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。これは、内部ネットワークを表すためのゾーンです。
- [outside_zone]：外部インターフェイスが含まれています。これは、ユーザの制御が及ばないネットワーク（インターネットなど）を表すためのゾーンです。

通常は、ネットワーク内での役割に応じ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は [outside_zone]セキュリティ ゾーンに設定し、内部ネットワークのインターフェイスはすべて [inside_zone]セキュリティ ゾーンに設定します。次に、外部ゾーンから内部ゾーンに移動するトラフィックに対してアクセス 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 ルールと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設定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 つのネットワークの扱いを他の 3 つのネットワークとは変えたい場合は、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必要があ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は別のゾーンを使用することができます。

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。セキュリティ ゾーン プロパティを編集している間に、オブジェクト リストに表示される [セキュリティ ゾーンの新規作成（Create New Security Zone）]リンクをクリックして、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、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、オブジェクトのゴミ箱アイコン（  ）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、任意で説明を入力します。

ステップ 4 [インターフェイス（Interfaces）]リストで [+] をクリックして、ゾーンに追加するインターフェイスを選択します。
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がリストに表示されます。インターフェイスはゾーンに追加する前に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、リストは空です。インターフェイスを別のゾーンに移動する場合は、まず現在のゾーンからそのインターフェイスを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ます。メンバーは異なるゾーンに含めることができます。

ステップ 5 [OK]をクリックして変更を保存します。

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、または、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。ポート仕様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。

個々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 フィルタを使用するとポリシーの作成と管理が簡素化されます。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。ユーザがそれらのアプリケーションの 1 つ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することなく、ポリシーで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、アプリケーションフィルタの同じグループに対して複数のポリシーを作成する場合は、オブジェクトを使用した方が便利です。システム

には、編集または削除できない複数の事前定義されたアプリケーション フィルタが含まれています。

（注） シスコでは、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、高リスクのアプリケーションをブロックするルールは、ルールを手動で更新する必要なく、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）] ページを通じて、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。[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）]をクリックすることで、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 [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、オブジェクトのゴミ箱アイコン（）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、任意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 +）] をクリックして、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。
初期リストでは、絶えずスクロールしているリストにアプリケーションが表示されます。[高度なフィルタ（Advanced Filter）]をクリックして、フィルタ オプションを表示し、アプリケーションを選択するための見やすいビューを表示します。選択したら、[追加（Add）]をクリックします。プロセスを繰り返して、アプリケーションまたはフィルタを追加します。

（注） 単一のフィルタ条件内で選択された複数の項目は、互いに「論理和（OR）」の関係となります。たとえば、リスクが「高（High）」または（OR）「非常に高い（Very High）」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、条件を満たすものだけが表示されるように、画面のアプリケーション リストが更新されます。これらのフィルタを使用すると、個別に追加しようとするアプリケーションを特定したり、ルールに追加する必要のあるフィルタが選択されているか確認する場合に役立ちます。

リスク

アプリケーションが、組織のセキュリティ ポリシーに反するおそれのある目的で使用される可能性。「非常に低い（Very Low）」～「非常に高い（Very High）」。

ビジネスとの関連性

娯楽としてではなく、組織の事業運営のコンテキスト内でアプリケーションが使用される可能性。「非常に低い（Very Low）」～「非常に高い（Very High）」。

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：HTTP や SSH など、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、ホスト上で実行され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：MPEG ビデオや Facebook など、HTTP トラフィックのコンテンツ、または要求された URL を表す Web アプリケーション。

カテゴリ

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

アプリケーションの補足情報。カテゴリに似ています。

暗号化トラフィックに対しては、SSL プロトコルのタグが付いたアプリケーションだけを使用するトラフィックが識別およびフィルタ処理されます。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（暗号化トラフィックまたは暗号化されていないトラフィックではなく）復号トラフィックのみで検出できるアプリケーションに対し、復号トラフィックタグを割り当てます。

アプリケーション リスト（画面下部）

このリストは、リスト上のオプションからフィルタを選択すると更新されます。したがって、現時点でフィルタに一致するアプリケーションを確認できます。このリストを使用すると、フィルタ条件をルールに追加する場合、必要なアプリケーションがフィルタのターゲットとなっているかどうかを確認できます。特定のアプリケーションを追加するには、このリストから選択します。

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 コントロール ポリシーで手動フィルタリングを実装することができます。

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。

- ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求された URL が文字列の一部に一致すると、URL が一致したと見なされます。したがって、example.com は、www.example.com や ads.example.com など、そのネットワーク上の任意のホストに一致します。また、badexample.com と一致します。
- URL 条件を含むアクセス コントロール ルールを使用して Web トラフィックを照合する場合、システムは暗号化プロトコル（HTTP 対 HTTPS）を無視します。つまり、アプリケーション条件を使用してルールを調整しない限り、Web サイトをブロックすると、その Web サイトへの HTTP と HTTPS の両方のトラフィック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。

（注） 特定のサイトをターゲットとする URL オブジェクトを設定する前に、アクセス コントロールの章に記載されている URL のフィルタリングに関する情報をよく確認してください。URL のマッチングは想定されるようには行われないため、意図せずにサイトをブロックしてしまう可能性があります。たとえば、ゲーム サイト ign.com を明示的にブロックしようとすると、verisign.com、およびその他の「ign」で終わる任意のサイトもブロックしてしまいます。

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 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、[グループを追加（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、オブジェクトのゴミ箱アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前、さらに任意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では、トラフィックの送信元または宛先であるデバイスをホストする国や大陸を定義します。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して、その国で使用される可能性があるすべての IP アドレスを知らなくても、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しなくても、ポリシーで地理的な場所を直接選択できます。ただし、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場合はオブジェクトの使用が便利です。

（注） 最新の地理的な場所のデータを使用してトラフィックをフィルタ処理するためには、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。ネットワークプロパティを編集している間に、オブジェクトリストに表示される [地理位置情報の新規作成（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、オブジェクトのゴミ箱アイコン（）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、任意で説明を入力します。

ステップ 4 [大陸と国（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と国を選択します。
大陸を選択すると、その大陸にある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を特定します。ログ収集と分析用の syslog サーバをセットアップしている場合は、ログ収集と分析を定義するためのオブジェクトを作成し、アクセス ルールまたは診断ロギング システムの設定でそれらのオブジェクトを使用します。システム ロギングの設定の詳細については、次のトピックを参照してください。

- ロギングの設定
- 診断ロギングの設定

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。syslog サーバ プロパティを編集している間に、オブジェクト リストに表示される [syslog サーバの追加（Add Syslog Server）]リンクをクリックして、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、オブジェクトのゴミ箱アイコン（  ）をクリックします。

ステップ 3 syslog サーバのプロパティを設定します。

- [デバイスインターフェイス（Device Interface）]：syslog サーバにアクセスするインターフェイスを選択します。ブリッジ グループ メンバー インターフェイスからサーバにアクセスできる場合は、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。
- [ポート（Port）]：サーバが syslog メッセージの受信に使用する UDP ポートを入力します。デフォルトは 514 です。

ステップ 4 [OK]をクリックして変更を保存します。