SCADA プリプロセッサ

以下のトピックでは、遠隔監視制御・情報取得（SCADA）プロトコルのプリプロセッサとその設定方法について説明します。

SCADA プリプロセッサの概要

Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。Firepower システムは、ネットワーク分析ポリシーの一部として設定できる Modbus および DNP3 SCADA プロトコル用のプリプロセッサを提供します。

対応する侵入ポリシーで Modbus または DNP3 キーワードを含むルールを有効にすると、Modbus または DNP3 プロセッサがその現在の設定で自動的に使用されます。ただし、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサは無効のままになります。

Modbus プリプロセッサ

Modbus プロトコルは 1979 年に Modicon が初めて発表した、広く利用されている SCADA プロトコルです。Modbus プリプロセッサは、Modbus トラフィックの異常を検出し、ルール エンジンによる処理のために Modbus プロトコルをデコードします。ルール エンジンは Modbus キーワードを使用して特定のプロトコル フィールドにアクセスします。

1 つの構成オプションで、プリプロセッサが Modbus トラフィックを検査するポートのデフォルト設定を変更できます。

関連トピック

SCADA キーワード

Modbus プリプロセッサ ポート オプション

ポート

プリプロセッサが Modbus トラフィックを検査するポートを指定します。複数のポートを指定する場合は、カンマで区切ります。

Modbus プリプロセッサの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

ネットワークに Modbus 対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [Modbus の構成（Modbus Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [Modbus の構成（Modbus Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 [ポート（Ports）] フィールドに値を入力します。
複数の値を指定する場合は、カンマで区切ります。

ステップ 7 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。

変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、Modbus プリプロセッサ ルール（GID 144）を有効にします。詳細については、侵入ルール状態の設定およびModbus プリプロセッサ ルール, （3 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入を参照してください。

関連トピック

レイヤの管理
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

Modbus プリプロセッサ ルール

次の表に示す Modbus プリプロセッサ ルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、これらのルールを有効にする必要があります。

表 *1*：*Modbus* プリプロセッサ ルール

プリプロセッサルール GID:SID	説明
144:1	Modbus の見出しの長さが、Modbus 機能コードに必要な長さと一致していない場合に、イベントが生成されます。 各 Modbus 機能の要求と応答には期待される形式があります。メッセージの長さが、期待される形式と一致しない場合に、このイベントが生成されます。
144:2	Modbus プロトコル ID がゼロ以外の場合に、イベントが生成されます。プロトコル ID フィールドは、Modbus と共にその他のプロトコルを多重伝送するために使用されます。プリプロセッサはこのような他のプロトコルを処理しないため、代わりにこのイベントが生成されます。
144:3	プリプロセッサが予約済み Modbus 機能コードを検出すると、イベントが生成されます。

DNP3 プリプロセッサ

Distributed Network Protocol（DNP3）は、当初は発電所間で一貫性のある通信を実現する目的で開発されたSCADAプロトコルです。DNP3も、水処理、廃棄物処理、輸送などさまざまな産業分野で幅広く利用されるようになっています。

DNP3 プリプロセッサは、DNP3 トラフィックの異常を検出し、ルール エンジンによる処理のために DNP3 プロトコルをデコードします。ルール エンジンは、DNP3 キーワードを使用して特定のプロトコル フィールドにアクセスします。

関連トピック

DNP3 キーワード

DNP3 プリプロセッサ オプション

ポート

指定された各ポートでの DNP3 トラフィックのインスペクションを有効にします。1 つのポートを指定するか、複数のポートをカンマで区切ったリストを指定できます。

無効な CRC を記録（Log bad CRCs）

DNP3 リンク層フレームに含まれているチェックサムを検証します。無効なチェックサムを含むフレームは無視されます。

ルール 145:1 を有効にすると、無効なチェックサムが検出されたときに イベントを生成し、インライン展開では、違反パケットをドロップします。 できます。

DNP3 プリプロセッサの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	任意（Any）	任意（Any）	Admin/Intrusion Admin

ネットワークにDNP3対応デバイスが含まれていない場合は、トラフィックに適用するネットワーク分析ポリシーでこのプリプロセッサを有効にしないでください。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 [ポリシー（Policies）] > [アクセス コントロール（Access Control）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。または[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [侵入（Intrusion）]、次に [ネットワーク分析ポリシー（Network Analysis Policy）] をクリックします。を選択します。

（注） カスタム ユーザ ロールに、ここにリストされている最初のパスへのアクセス制限がある場合は、2 番目のパスを使用してポリシーにアクセスします。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 ナビゲーション パネルで [設定（Settings）] をクリックします。

ステップ 4 [SCADA プリプロセッサ（SCADA Preprocessors）] の下の [DNP3 の構成（DNP3 Configuration）] が無効になっている場合は、[有効化（Enabled）] をクリックします。

ステップ 5 [DNP3 の構成（DNP3 Configuration）] の横にある編集アイコン（）をクリックします。

ステップ 6 ポートの値を入力します。
複数の値を指定する場合は、カンマで区切ります。

ステップ 7 [不良 CRC の記録（Log bad CRCs）] チェックボックスをオンまたはオフにします。

ステップ 8 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報（Policy Information）] をクリックして、[変更を確定（Commit Changes）] をクリックします。
変更を確定せずにポリシーをそのままにした場合、別のポリシーを編集すると、最後に確定してから加えたキャッシュされている変更は廃棄されます。

次の作業

- イベントを生成し、インライン展開では、違反パケットをドロップします。 を行うには、DNP3 プリプロセッサ ルール（GID 145）を有効にします。詳細については、侵入ルール状態の設定、DNP3 プリプロセッサ オプション，（4 ページ）、およびDNP3 プリプロセッサ ルール，（6 ページ）を参照してください。
- 設定変更を展開します。設定変更の導入を参照してください。

関連トピック

レイヤの管理
競合と変更：ネットワーク分析ポリシーと侵入ポリシー

DNP3 プリプロセッサ ルール

次の表に示すDNP3プリプロセッサルールによってイベントを生成し、インライン展開では、違反パケットをドロップします。 するには、これらのルールを有効にする必要があります。

表 *2* : *DNP3* プリプロセッサ ルール

プリプロセッサルール GID:SID	説明
145:1	[無効な CRC を記録（Log bad CRC）] が有効である場合に、無効なチェックサムを含むリンク層フレームがプリプロセッサにより検出されると、イベントが生成されます。
145:2	無効な長さの DNP3 リンク層フレームがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:3	再構成中に無効なシーケンス番号のトランスポート層セグメントがプリプロセッサにより検出されると、イベントが生成され、パケットがブロックされます。
145:4	完全なフラグメントを再構成する前に DNP3 再構成バッファがクリアされると、イベントが生成されます。このことは、FIR フラグを伝送するセグメントが、他のセグメントがキューに入れられた後で現れる場合に発生します。
145:5	予約済みアドレスを使用する DNP3 リンク層フレームをプリプロセッサが検出すると、イベントが生成されます。
145:6	予約済み機能コードを使用する DNP3 要求または応答をプリプロセッサが検出すると、イベントが生成されます。