Configuring SCADA Preprocessing

You configure Supervisory Control and Data Acquisition (SCADA) preprocessors in a network analysis policy, which prepares traffic for inspection using the rules enabled in an intrusion policy. See Understanding Network Analysis and Intrusion Policies, page 18-1 for more information.

SCADA protocols monitor, control, and acquire data from industrial, infrastructure, and facility processes such as manufacturing, production, water treatment, electric power distribution, airport and shipping systems, and so on. The ASA FirePOWER module provides preprocessors for the Modbus and DNP3 SCADA protocols that you can configure as part of your network analysis policy.

If you enable a rule containing Modbus or DNP3 keywords in the corresponding intrusion policy, the system automatically uses the Modbus or DNP3 processor, respectively, with its current settings, although the preprocessor remains disabled in the network analysis policy module interface. For more information, see Modbus Keywords, page 30-73 and DNP3 Keywords, page 30-74.

See the following sections for more information:

- Configuring the Modbus Preprocessor, page 23-1
- Configuring the DNP3 Preprocessor, page 23-3

Configuring the Modbus Preprocessor

License: Protection

The Modbus protocol, which was first published in 1979 by Modicon, is a widely used SCADA protocol. The Modbus preprocessor detects anomalies in Modbus traffic and decodes the Modbus protocol for processing by the rules engine, which uses Modbus keywords to access certain protocol fields. See Modbus Keywords, page 30-73 for more information.

A single configuration option allows you to modify the default setting for the port that the preprocessor inspects for Modbus traffic.

You must enable the Modbus preprocessor rules in the following table if you want these rules to generate events. See Setting Rule States, page 27-19 for information on enabling rules.

Table 23-1 Modbus Preprocessor Rules

Preprocessor Rule GID:SID	Description
144:1	Generates an event when the length in the Modbus header does not match the length required by the Modbus function code. Each Modbus function has an expected format for requests and responses. If the length of the message does not match the expected format, this event is generated.
144:2	Generates an event when the Modbus protocol ID is non-zero. The protocol ID field is used for multiplexing other protocols with Modbus. Because the preprocessor does not process these other protocols, this event is generated instead.
144:3	Generates an event when the preprocessor detects a reserved Modbus function code.

Note regarding the use of the Modbus preprocessor that if your network does not contain any Modbus-enabled devices, you should not enable this preprocessor in a network analysis policy that you apply to traffic.

You can use the following procedure to modify the ports the Modbus preprocessor monitors.

To configure the Modbus preprocessor:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to edit.

The access control policy editor appears.

Step 3 Select the **Advanced** tab.

The access control policy advanced settings page appears.

Step 4 Click the edit icon ( ) next to **Network Analysis and Intrusion Policies**.

The Network Analysis and Intrusion Policies pop-up window appears.

Step 5 Click **Network Analysis Policy List**.

The Network Analysis Policy List pop-up window appears.

Step 6 Click the edit icon ( ) next to the policy you want to edit.

If you have unsaved changes in another policy, click **OK** to discard those changes and continue. See Resolving Conflicts and Committing Policy Changes, page 18-15 for information on saving unsaved changes in another policy.

The Policy Information page appears.

Step 7 Click **Settings** in the navigation panel on the left.

The Settings page appears.

Step 8 You have two choices, depending on whether **Modbus Configuration** under **SCADA Preprocessors** is enabled:

- If the configuration is enabled, click **Edit**.
- If the configuration is disabled, click **Enabled**, then click **Edit**.

The Modbus Configuration page appears. A message at the bottom of the page identifies the network analysis policy layer that contains the configuration. See Using Layers in a Network Analysis or Intrusion Policy, page 19-1 for more information.

Step 9 Optionally, modify the **Ports** that the preprocessor inspects for Modbus traffic. You can specify an integer from 0 to 65535. Use commas to separate multiple ports.

Step 10 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. See Resolving Conflicts and Committing Policy Changes, page 18-15 for more information.

Configuring the DNP3 Preprocessor

License: Protection

The Distributed Network Protocol (DNP3) is a SCADA protocol that was originally developed to provide consistent communication between electrical stations. DNP3 has also become widely used in the water, waste, transportation, and many other industries.

The DNP3 preprocessor detects anomalies in DNP3 traffic and decodes the DNP3 protocol for processing by the rules engine, which uses DNP3 keywords to access certain protocol fields. See DNP3 Keywords, page 30-74 for more information.

You must enable the DNP3 preprocessor rules in the following table if you want these rules to generate events. See Setting Rule States, page 27-19 for information on enabling rules.

Table 23-2 DNP3 Preprocessor Rules

Preprocessor Rule GID:SID	Description
145:1	When **Log bad CRC** is enabled, generates an event when the preprocessor detects a link layer frame with an invalid checksum.
145:2	Generates an event and blocks the packet when the preprocessor detects a DNP3 link layer frame with an invalid length.
145:3	Generates an event and blocks the packet during reassembly when the preprocessor detects a transport layer segment with an invalid sequence number.
145:4	Generates an event when the DNP3 reassembly buffer is cleared before a complete fragment can be reassembled. This happens when a segment carrying the FIR flag appears after other segments have been queued.
145:5	Generates an event when the preprocessor detects a DNP3 link layer frame that uses a reserved address.
145:6	Generates an event when the preprocessor detects a DNP3 request or response that uses a reserved function code.

Note regarding the use of the DNP3 preprocessor that, if your network does not contain any DNP3-enabled devices, you should not enable this preprocessor in a network analysis policy that you apply to traffic. See Configuring TCP Stream Preprocessing, page 24-28 for more information.

The following list describes the DNP3 preprocessor options you can configure.

Ports

Enables inspection of DNP3 traffic on each specified port. You can specify a single port or a comma-separated list of ports. You can specify a value from 0 to 65535 for each port.

Log bad CRCs

When enabled, validates the checksums contained in DNP3 link layer frames. Frames with invalid checksums are ignored.

You can enable rule 145:1 to generate events when invalid checksums are detected.

To configure the DNP3 preprocessor:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to edit.

The access control policy editor appears.

Step 3 Select the **Advanced** tab.

The access control policy advanced settings page appears.

Step 4 Click the edit icon ( ) next to **Network Analysis and Intrusion Policies**.

The Network Analysis and Intrusion Policies pop-up window appears.

Step 5 Click **Network Analysis Policy List**.

The Network Analysis Policy List pop-up window appears.

Step 6 Click the edit icon ( ) next to the policy you want to edit.

If you have unsaved changes in another policy, click **OK** to discard those changes and continue. See Resolving Conflicts and Committing Policy Changes, page 18-15 for information on saving unsaved changes in another policy.

The Policy Information page appears.

Step 7 Click **Settings** in the navigation panel on the left.

The Settings page appears.

Step 8 You have two choices, depending on whether **DNP3 Configuration** under **SCADA Preprocessors** is enabled:

- If the configuration is enabled, click **Edit**.
- If the configuration is disabled, click **Enabled**, then click **Edit**.

The DNP3 Configuration page appears. A message at the bottom of the page identifies the network analysis policy layer that contains the configuration. See Using Layers in a Network Analysis or Intrusion Policy, page 19-1 for more information.

Step 9 Optionally, modify the **Ports** that the preprocessor inspects for DNP3 traffic. You can specify an integer from 0 to 65535. Use commas to separate multiple ports.

Step 10 Optionally, select or clear the **Log bad CRCs** check box to specify whether to validate the checksums contained in DNP3 link layer frames and ignore frames with invalid checksums.

Step 11 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. See the Network Analysis Policy Editing Actions table for more information.