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 11-1 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 23-73 and DNP3 Keywords, page 23-74.

See the following sections for more information:

- Configuring the Modbus Preprocessor, page 16-1
- Configuring the DNP3 Preprocessor, page 16-3
- Configuring the CIP Preprocessor, page 16-5

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 23-73 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 20-19 for information on enabling rules.

Table 16-1 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 11-15 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 12-1 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 11-15 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 23-74 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 20-19 for information on enabling rules.

Table 16-2 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 17-28 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 11-15 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 12-1 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.

Configuring the CIP Preprocessor

License: Protection

The Common Industrial Protocol (CIP) is a widely used application protocol that supports industrial automation applications. EtherNet/IP is an implementation of CIP that is used on Ethernet-based networks.

The CIP preprocessor detects CIP and ENIP traffic running on TCP or UDP and sends it to the intrusion rules engine. You can use CIP and ENIP keywords in custom intrusion rules to detect attacks in CIP and ENIP traffic. See CIP and ENIP Keywords, page 23-78. Additionally, you can control traffic by specifying CIP and ENIP application conditions in access control rules. See Controlling Application Traffic, page 8-2.

Note the following:

- To detect CIP and ENIP applications and use them in access control rules, intrusion rules and so on, you must manually enable the CIP preprocessor in the corresponding network analysis policy. See Setting the Default Network Analysis Policy for Access Control, page 13-3 and Specifying Traffic to Preprocess Using Network Analysis Rules, page 13-4.
- To drop traffic that triggers CIP preprocessor rules and CIP intrusion rules, ensure that the corresponding intrusion policy **Drop when Inline** option is enabled. See Setting Drop Behavior in an Inline Deployment, page 19-5.
- To block CIP or ENIP application traffic using access control rules, ensure that the inline normalization preprocessor and its **Inline Mode** option are enabled in the corresponding network analysis policy. See Normalizing Inline Traffic, page 17-6 and Allowing Preprocessors to Affect Traffic in Inline Deployments, page 14-5.
- Add the default CIP detection port 44818 and any other ports you list to the TCP stream **Perform Stream Reassembly on Both Ports** list. See Selecting Stream Reassembly Options, page 17-26.
- Event viewers give special handling to CIP applications. See Understanding CIP Events, page 16-7.

You must enable the CIP preprocessor rules listed in the following table if you want them to generate events. See Setting Rule States, page 20-19 for information on enabling rules.

Table 16-3 CIP Preprocessor Rules

Preprocessor Rule GID:SID	Rule Message
148:1	CIP_MALFORMED
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT
148:4	CIP_REQUEST_LIMIT

The following list describes CIP preprocessor options you can modify.

Ports

Specifies the ports to inspect for CIP and ENIP traffic. You can specify an integer from 0 to 65535. Separate multiple port numbers with commas.

Note You **must** add the default CIP detection port 44818 and any other ports you list to the TCP stream **Perform Stream Reassembly on Both Ports** list. See Selecting Stream Reassembly Options, page 17-26.

Default Unconnected Timeout (seconds)

When a CIP request message does not contain a protocol-specific timeout value and **Maximum number of concurrent unconnected requests per TCP connection** is reached, the system times the message for the number of seconds specified by this option. When the timer expires, the message is removed to make room for future requests. You can specify an integer from 0 to 360. When you specify 0, all traffic that does not have a protocol-specific timeout times out first.

Maximum number of concurrent unconnected requests per TCP connection

The number of concurrent requests that can go unanswered before the system closes the connection. You can specify an integer from 1 to 10000.

Maximum number of CIP connections per TCP connection

The maximum number of simultaneous CIP connections allowed by the system per TCP connection. You can specify an integer from 1 to 10000.

To configure the CIP preprocessor:

Step 1 Select **Configuration > ASA FirePOWER Configuration > 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 11-15 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 **CIP Configuration** under SCADA Preprocessors is enabled:

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

The CIP 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 12-1 for more information.

Step 9 You can modify any of the options described in this section.

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 11-15 for more information.

Understanding CIP Events

By design, application detectors detect and event viewers display the same application one time per session. A CIP session can include multiple applications in different packets, and a single CIP packet can contain multiple applications. The CIP preprocessor handles all CIP and ENIP traffic according to the corresponding rule and controls the display of CIP events as follows:

- Application Protocol: **CIP** or **ENIP**
- Client: **CIP Client** or **ENIP Client**
- Web Application: the specific application detected, which is:
  - For rules that allow or monitor traffic: the last application protocol detected in the session.

    Note that access control rules that you configure to log connections might not generate events for specified CIP applications, and access control rules that you do not configure to log connections might generate events for CIP applications.
  - For rules that block traffic: the application protocol that triggered the block.

    When an access control rule blocks a list of CIP applications, event viewers display the first application that is detected.

Note the following:

- Cisco recommends that you use an access control policy default action of **Intrusion Prevention**.
- The CIP preprocessor does not support an access control policy default action of **Access Control: Trust All Traffic** which may produce undesirable behavior, including not dropping traffic triggered by CIP applications specified in intrusion rules.
- The CIP preprocessor does not support an access control policy default action of **Access Control: Block All Traffic** which may produce undesirable behavior, including blocking CIP applications that you do not expect to be blocked.
- The CIP preprocessor does not support application visibility for CIP applications, including network discovery.