Implement Deep Packet Inspection of DNP3 Traffic with Cisco Catalyst IR8340 UTD IPS/IDS Functionality

Whitepaper

August 2025

Abstract

Operational Technology (OT) security is increasingly critical due to the flat network architecture and the vital nature of systems operating within these networks. Distributed Network Protocol 3 (DNP3) is widely adopted in North America and other regions for Supervisory Control and Data Acquisition (SCADA) systems, making it a prominent target for cyberattacks.

Intrusion Detection System (IDS) signatures for DNP3 are often generic and focus only on the standard protocol rather than the specific nuances of individual customer implementations. For example, a particular control command in one environment might be routine, while in another, it could trigger significant operational changes.

This whitepaper delves into the structure of DNP3 messages, providing insights into customizing Snort rules to align with customer-specific implementations.

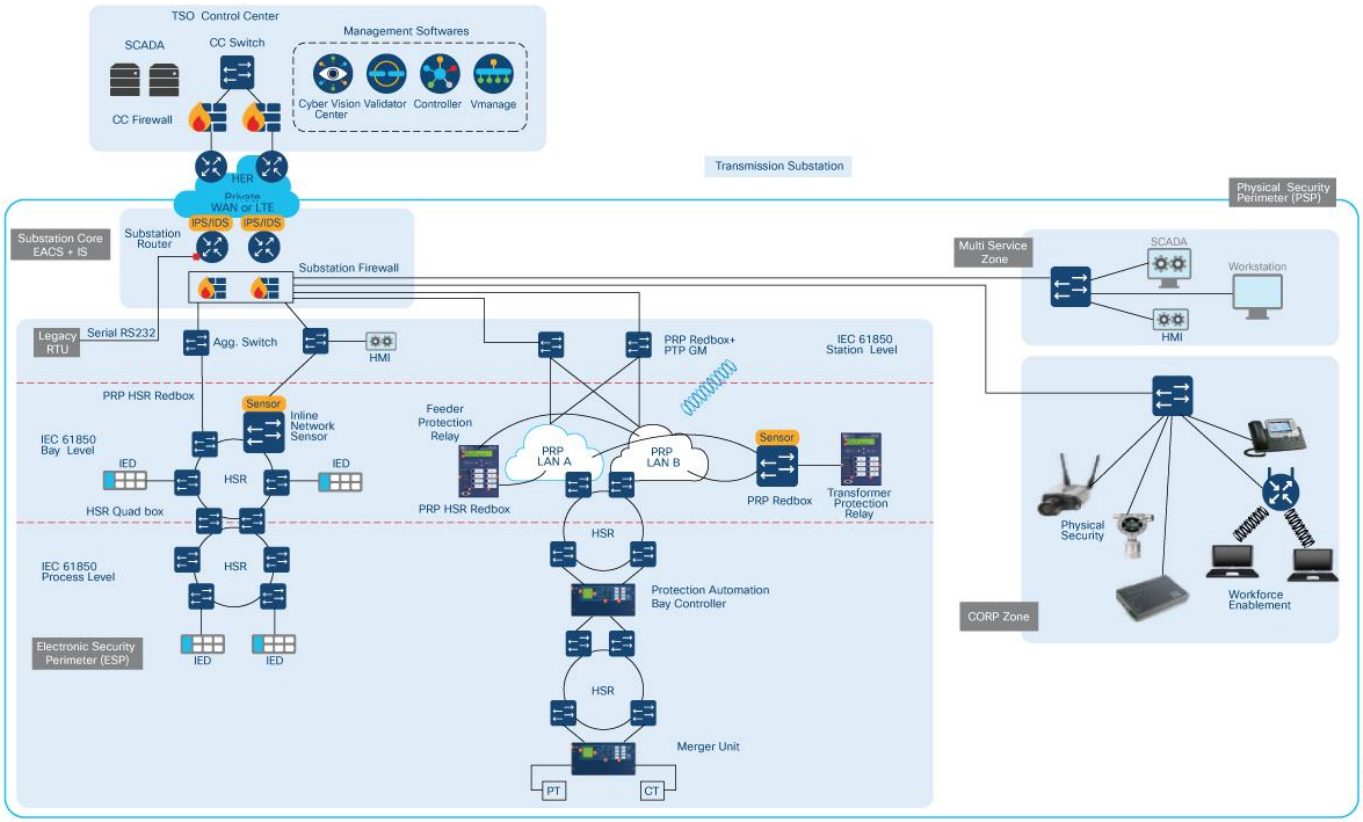
Snort is an open-source network intrusion detection and prevention system (NIDS/IPS) that analyzes network traffic in real-time to detect and prevent malicious activities. It uses a set of rules and signatures to identify threats such as exploits, malware, and suspicious behaviour. Snort is widely used in security solutions, including Cisco security products, to provide threat detection and network protection.

By tailoring IDS /IPS rules to recognize and interpret commands based on their context within a particular SCADA setup, organizations can achieve more precise monitoring and control, enabling granular decisions to permit, monitor, or deny specific SCADA actions.

Cisco Substation Automation Solution and Architecture

A modern electrical utility network is typically a distributed Cisco Catalyst IR8340 environment wherein the grid operators and controllers are not physically located within a substation. Utility operators often manage substations remotely from Operations and Control Centers. The centers are connected to the substations using a wide area network (WAN) infrastructure and use SCADA applications.

Figure 1. New Cisco Digital Substation Automation Reference Architecture



The new Cisco digital substation architecture comprises:

- An operations and control center
- A demilitarized zone
- A WAN tier
- A transmission substation Physical Security Perimeter (PSP)
- WAN connectivity for other Secondary substations, local multi-service, and corporate networks.

Further, the PSP is divided into substation core, Electronic Security Perimeter (ESP), and Multiservice and Corporate (CORP) zones.

Based on the IEC 61850 standard, ESP is further subdivided into station, bay, and process levels.

Components of Substation Automation

Cisco Catalyst IR8340 Rugged Series Router

The Cisco Catalyst IR8340 Rugged Series Router, as a substation router, enables secure, reliable, and scalable connectivity for utility environments. The device is crucial in substation automation and utilities processes. IR8340 functions as a substation automation gateway, acting as a SCADA proxy master station between the control center and RTUs. The device performs protocol translations to enable seamless communication within substation networks, such as:

- IEC 60870 T101 to IEC 60870 T104
- DNP3 serial to DNP3 IP

The IR8340 also serves as a ruggedized network infrastructure device at the substation edge and supports high-performance Layer 2 and Layer 3 services, including:

- MPLS and segment routing
- Precise timing protocols such as IEEE 1588 PTP Power profile
- Converting telecom PTP profiles to power profiles that are essential for synchronization, acting as a boundary clock.

For security and compliance, it includes zone-based firewalls (ZBFW) and next-generation firewall capabilities, helping users comply with NERC CIP and IEC 62443 standards. IR8340 also integrates with Cisco Cyber Vision for OT asset visibility and security posture monitoring.

The device supports high availability and resiliency through dual IR8340 HA designs, PRP/HSR redundancy for lossless network convergence, and high precision timing critical for substation applications.

Its use cases in utilities encompass substation automation, teleprotection, and power management applications such as the synchrophasor, also known as PMU, with secure and scalable connectivity.

In summary, the Cisco Catalyst IR8340 Rugged Series Router is a foundational component in modern substation automation architectures, enabling secure, high-performance communication, protocol translation, precise timing, and compliance with utility industry standards, thereby enhancing operational efficiency, reliability, and security in utility networks.

Cisco Catalyst SD-WAN Manager

Cisco Catalyst SD-WAN Manager enables centralized and scalable management of Cisco Catalyst IR8340 routers, providing unified control over routing, switching, and security features, including Next-Generation Firewall (NGFW).

It simplifies deployment and lifecycle management by integrating comprehensive security management, including NGFW, IPS/IDS, and zero-trust security policies to protect industrial and enterprise WAN environments.

The solution offers centralized policy and configuration capabilities, allowing consistent security and network policies across IR8340 devices at scale, supporting tens of thousands of devices.

It also facilitates simplified IT and OT collaboration through easy-to-deploy templates, remote updates, and application-aware routing, which optimize operational costs and network performance.

With a unified dashboard, the Cisco Catalyst SD-WAN Manager enhances visibility and control across data centers, branches, clouds, and industrial locations.

Additionally, the manager supports scalability and automation by enabling automated provisioning, configuration, and monitoring, which reduces operational complexity and allows rapid scaling of secure WAN deployments. This makes Cisco Catalyst SD-WAN Manager an essential tool for managing IR8340 routers with integrated NGFW features, delivering secure, efficient, and scalable WAN operations suitable for modern industrial and enterprise networks.

Unified Threat Defence

The Cisco Catalyst IR8340 supports the Unified Threat Defense (UTD) service, which includes Snort IPS/IDS as a virtual container service.

UTD provides comprehensive network security features, including firewalls, IPS/IDS, web filtering, and malware protection. On the IR8340, UTD requires a minimum of 1.8 GB of available memory to start the UTD container. UTD supports both Autonomous and Controller modes, but the IPS/IDS feature is necessary for Autonomous mode support.

The UTD configuration for IR8340 supports the Cloud-Low profile. The on-box web-filtering database is not supported.

The Cloud-Low profile for Cisco IOx app hosting refers to a resource profile that is used to allocate CPU, memory, and network resources for containerized applications running on Cisco IOx platforms. In IOx application packaging, resource profiles such as Cloud-Low define the amount of resources assigned to an application container, enabling efficient management of edge compute resources. These profiles help balance application performance and resource consumption on devices hosting IOx applications.

The Cloud-Low profile is a predefined resource allocation profile within Cisco IOx app hosting that defines a lower resource footprint for containerized applications, suitable for cloud or edge environments with constrained resources.

Snort IPS runs as a virtual container on the router, monitoring network traffic for intrusion detection and prevention. It analyzes traffic against signature sets that can be configured with different levels of security (Connectivity, Balanced, Security), each impacting system performance differently.

The Cisco Catalyst IR8340 router supports configurable core profiles tailored for service, data, and control planes, enabling optimized performance for high-speed WAN traffic.

The control plane manages routing and network control processes, the data plane handles packet forwarding, and the service plane supports additional services, all leveraging the IR8340's multicore Intel x86 CPU and integrated switching ASIC for efficient operation.

It is recommended to use the service plane core profile on the box to host edge computing applications such as UTD, Cisco Cyber Vision sensors, and Cisco Secure Equipment Access (SEA).

Cisco SD-WAN offers three primary security policy signature sets for intrusion prevention system (IPS) configurations, each balancing security and performance differently:

- **Connectivity**: This is the least restrictive setting with fewer IPS rules applied. It prioritizes better network performance and lower resource usage by applying a minimal set of IPS signatures. It is suitable when maintaining connectivity and performance is critical, and a less stringent security inspection is acceptable.
- **Balanced**: This setting provides a middle ground between security and performance. It applies a moderate number of IPS signatures to offer protection without significantly impacting system

performance. It is designed to provide effective threat protection while maintaining reasonable throughput.

- **Security**: This is the most restrictive setting with the highest number of IPS signatures enabled. It offers the most comprehensive protection by applying extensive rules to detect and prevent threats, but it may have a greater impact on system performance.

In summary, the Connectivity policy has the fewest IPS signatures for better performance, Balanced offers a compromise between protection and performance, and Security applies the most signatures for maximum protection. These signature sets are part of Cisco Talos-developed IPS rules, and administrators are advised to start with the Balanced set and then adjust based on network needs and performance considerations.

For more information, see Security Policy Design Guide for Cisco IOS-XE SD-WAN Devices.

Snort IPS can operate in IDS mode (alerts only) or IPS mode (actively blocks threats). Logs can be sent to external syslog servers or SIEM systems for analysis.

Implement and Deploy Snort IPS/IDS on Cisco Catalyst IR8340

In the operational technology (OT) field, ensuring secure communication in SCADA systems is critical. This use case focuses on leveraging Cisco's UTD on the IR8340 router, deployed via SD-WAN, to enhance security for the DNP3 SCADA protocol.

By integrating Snort IPS/IDS, the solution enables deep packet inspection (DPI) to enforce strict access control policies. Specifically, it allows only authorized read/write commands from trusted operators while blocking or denying all unauthorized or untrusted operators.

This approach ensures robust protection against potential threats, safeguarding critical infrastructure and maintaining operational integrity.

The configuration involves:

- Deploying UTD with Snort IPS/IDS for DPI on a Cisco Catalyst IR8340 router via Cisco SD-WAN
- Deploying the ZBFW rules to filter trusted and untrusted DNP3 operators
- Creating custom Snort rules to filter DNP3 commands based on operator trust levels
- Enforcing these rules through Cisco SD-WAN Manager policies
- Testing and validating the setup to ensure compliance and security

After the prerequisites are met, create custom rules that match the implementation requirements.

The official Snort documentation describes the rule syntax.

Load Custom Snort Rules in Catalyst SD-WAN Manager

Step 1. Log in to the Cisco Catalyst SD-WAN Manager GUI.

Step 2. **From the main menu, go to Administrator > Settings > UTD Snort Subscriber > Enable UTD and Custom Signature**.

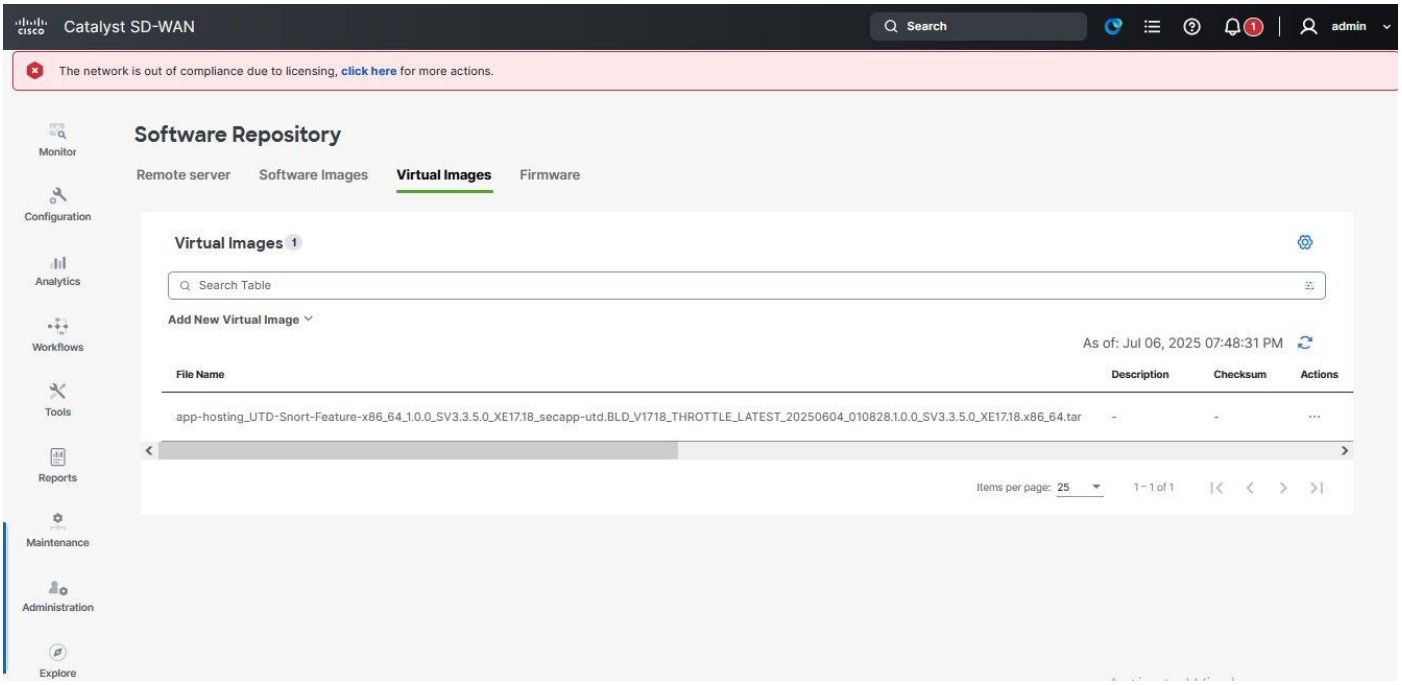
Step 3. Add the respective files and save the settings. (You can add files from remote servers, local, and more.)

UTD Deployment via Catalyst SD-WAN Manager

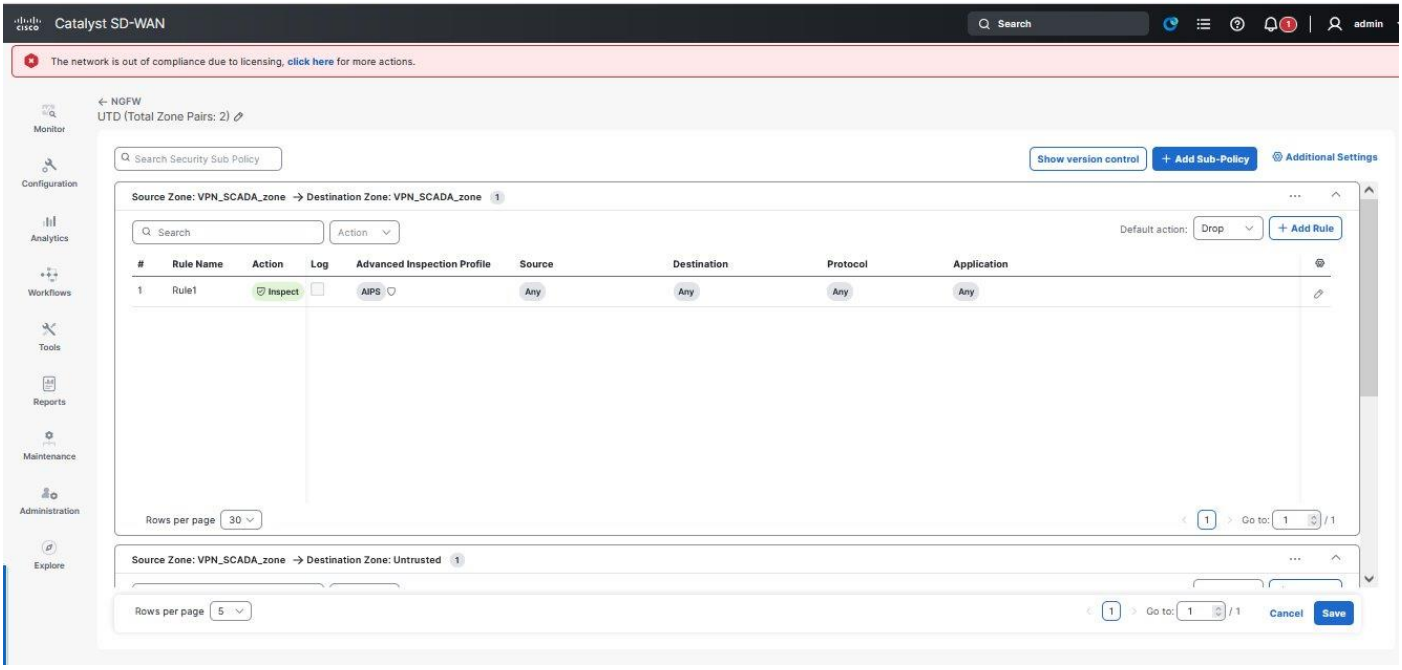
To deploy UTD on Cisco Catalyst IR8340:

Step 1. In the Cisco Catalyst SD-WAN Manager, go to **Maintenance > Software Repository > Virtual Images**.

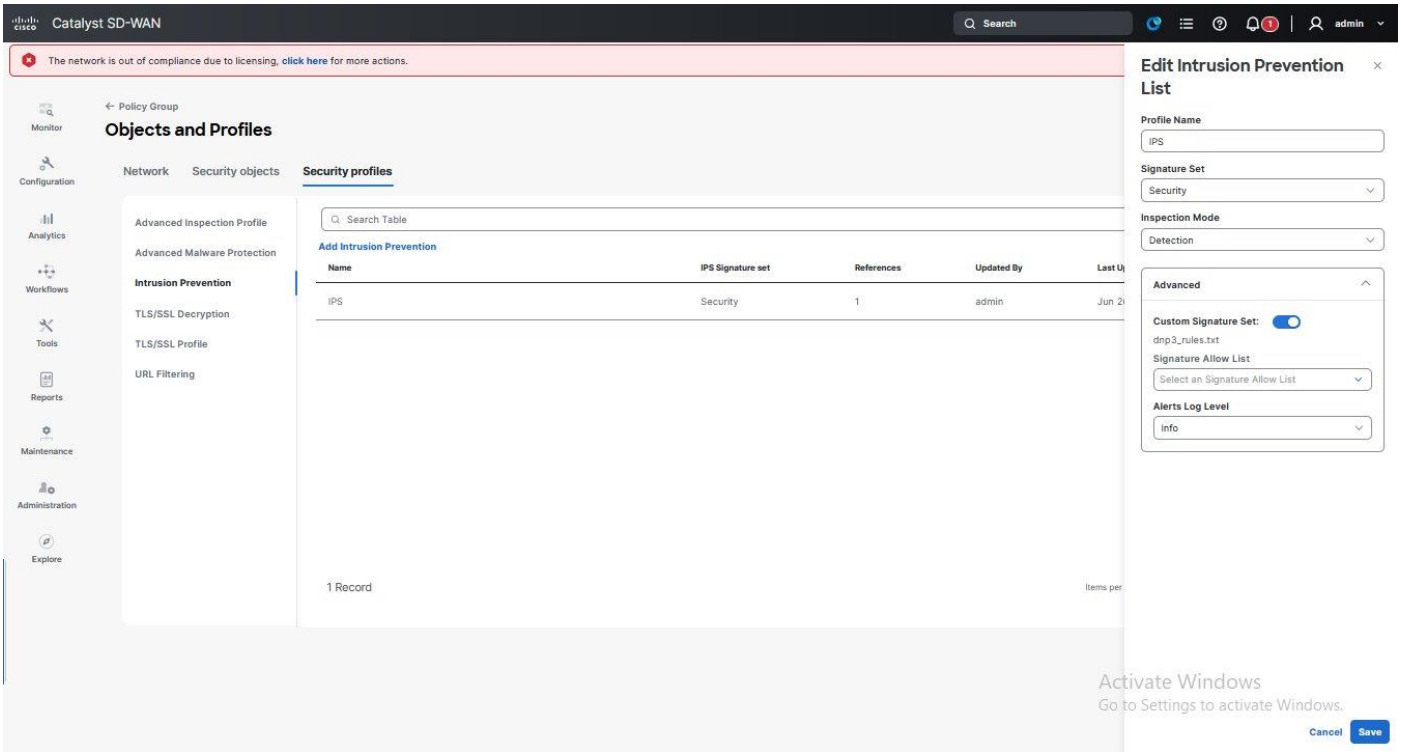
Step 2. Add a virtual image for the IR8340 UTD file (downloaded from software.cisco.com).



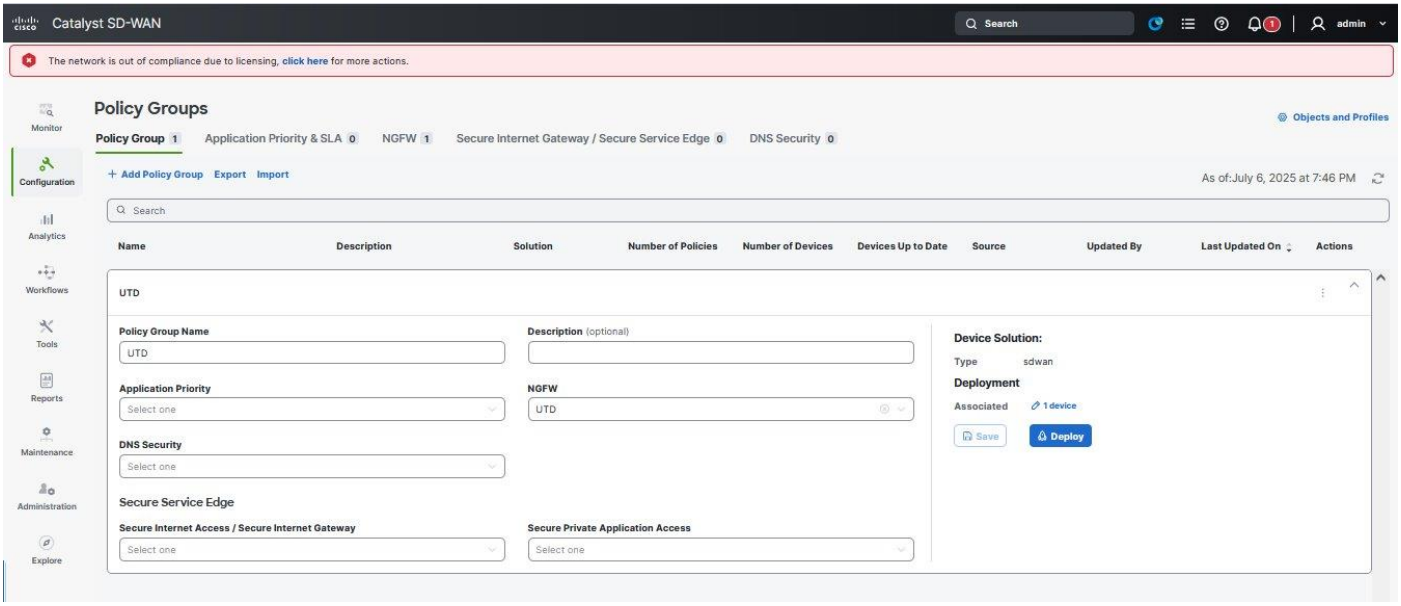
Step 3. Create a policy group with NGFW, and then create a subpolicy that includes FW rules with IPS inspection.



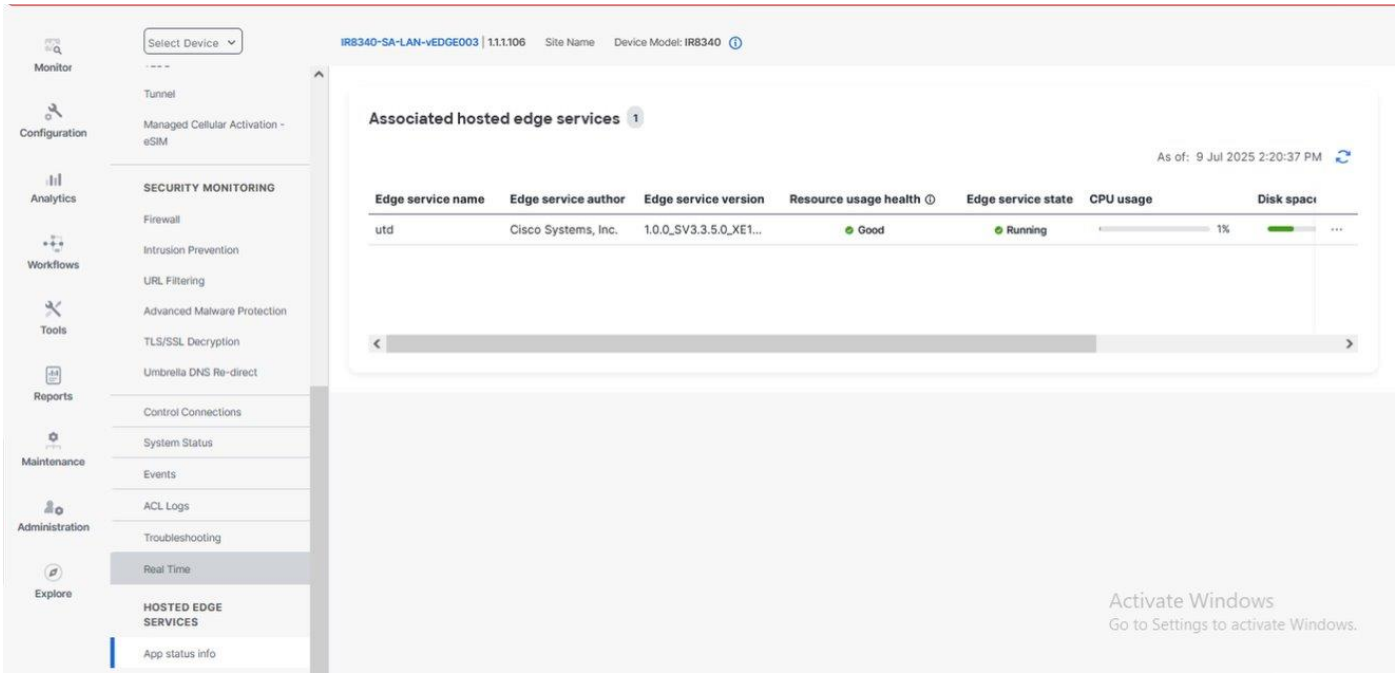
Step 4. Add IPS with custom rules enabled, and advanced IPS. Then, associate the IPS with the profile.



Step 5. Associate the device with the policy group.



Step 6. Deploy the policy group to install UTD as a virtual service on Cisco IR8340.



After you deploy the configuration, you can verify the app service status in the **Monitor > Device > Hosted Edge** Service page, in the **App status info** area.

Snort's Role in DNP3 Security

Snort includes a specialized DNP3 preprocessor that decodes and reassembles DNP3 traffic. This preprocessor not only validates the framing and layering of the protocol but also empowers security professionals to craft precise rules that monitor and alert on anomalies within DNP3 messages.

Key DNP3 Rule Options in Snort

Snort's integration with DNP3 is sophisticated, offering specific rule options that directly target the various components of a DNP3 message:

- `dnp3_func`: This option focuses on the function codes used within DNP3 messages. By inspecting these codes, you can differentiate between normal operational messages and those that might indicate malicious commands or control actions. For instance, if a command code that isn't typically used in your environment appears, it could trigger an alert.
- `dnp3_ind`: This option is designed to match indicator flags in DNP3 messages. These flags hint at various operational states or error conditions. Abnormal indicator flag values can signal disruptions or potential exploits that warrant further investigation.
- `dnp3_obj`: With this option, rules target the DNP3 object headers. This provides the ability to check for specific groups and variations within the data objects being transmitted. This option helps you detect unauthorized or unexpected data patterns that could be exploited by attackers.
- `dnp3_data`: Setting the cursor to the beginning of the DNP3 Application Layer data, this option allows subsequent rule options to evaluate the actual payload. This can be leveraged to search for suspicious strings or data injections within the DNP3 payload.

Using these dedicated rule options, Snort transforms what might be a complex protocol into a manageable and monitorable network asset. This targeted approach simplifies rule writing and greatly enhances the detection of anomalies, ultimately bolstering the security posture of Utility SCADA networks.

Scenario 1: Allow Read and Drop Write DNP3 Traffic on Trusted Ports and Operators

Alert the Read for DNP3 from Trusted Operators and Ports

Alert the read for DNP3 from trusted operators and ports using the following Snort rule:

```
alert tcp $trusted_operator any -> $trusted_IED 20000 (msg:"DNP3 Read"; dnp3_func: 1;
classtype:misc-activity; sid:1000000;)
```

Where,

Rule component	Defines	Description
`tcp $trusted_operator any -> $trusted_IED 20000`	Traffic direction and ports	The rule applies to TCP traffic where the source is defined by the variable `$trusted operator` (a group of trusted operator IP addresses) coming from any port, and the destination is defined by `$trusted IED` (the trusted Intelligent Electronic Device) on port 20000. Here, port 20000 is used for DNP3 communications.
`msg:"DNP3 Read"`	Alert message	If the rule conditions are met, Snort generates an alert with the message “DNP3 Read.” This informs the analyst that a DNP3 read command has been detected. All these events can be viewed in the router logs and can also be redirected to an external syslog server, such as Splunk, for further analysis. Additionally, these same messages are visible within the SD-WAN platform. The image at the end of this scenario section illustrates how the events are interpreted on the Cisco Catalyst SD-WAN Manager GUI.
`dnp3_func: 1`	DNP3 function code check	The DNP3 preprocessor built into Snort inspects the payload of the DNP3 message. In DNP3, function code 1 typically represents a read operation. This means that the rule checks if the DNP3 message’s function code matches 1. If the message is indeed a read command, it qualifies for this alert.
`classtype:misc-activity`	Classification	Assign a classification to the alert to help categorize or correlate alerts in larger incident response workflows.
`sid:1000000`	Signature ID	The signature ID uniquely identifies this rule for management and tracking in your Snort setup. Snort reserves SID values from 0 to 999999 because those are used in the rules included in Snort distribution. You must use local rules sid values that start at 1000000, incrementing the SID values by one for each additional local rule.

What Happens in Practice

When a TCP packet is sent from a trusted operator to a trusted IED on port 20000, the rule activates if the payload contains a DNP3 message with a function code of 1. In effect, this signifies that the sender (a trusted operator) is issuing a DNP3 read command to the IED. The system then logs this event and alerts the security team under the classification **DNP3 Read**.

Though the source is trusted, monitoring these operations is critical within a SCADA or industrial control system environment. Such alerts help ensure that even standard operations are logged and verified, establishing a baseline of activity for detecting anomalies in case of a system compromise or misconfiguration.

This focused rule helps maintain visibility over the operational commands within the network, a vital task in protecting critical infrastructure.

Drop DNP3 Control Commands From Trusted Operators

Drop DNP3 control commands from trusted operators using the following rule:

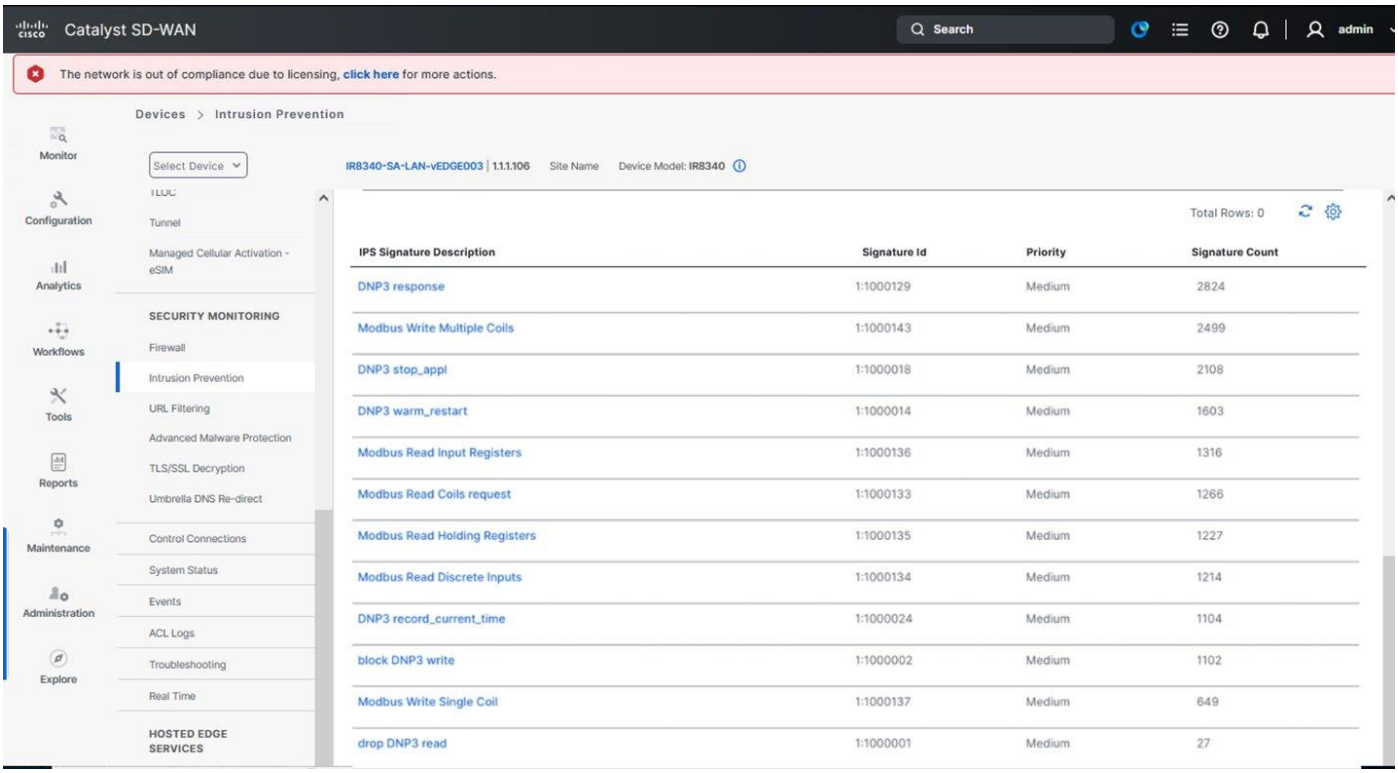
```
drop tcp $trusted_operator any -> $trusted_IED 20000 (msg:"Drop DNP3 write"; dnp3_func: 2;
classtype:misc-activity; sid:1000001;)
```

In practice, when a TCP packet is sent from an IP listed in `$trusted_operator` to an IP in `$trusted_IED` on port 20000, Snort inspects the DNP3 payload of that packet. The rule specifically checks for a DNP3 message with a function code of 2, which typically represents a write command within the DNP3 protocol.

If the payload contains this write command (`dnp3_func: 2`), Snort immediately triggers a drop with the message **Drop DNP3 Write**. The event is then uniquely identified by the signature ID (`sid:1000001`). This process ensures that any write commands, even from trusted operators, are monitored and dropped.

This is how the event is notified in the Cisco Catalyst IR8340 when UTD inspects the traffic for control command:

```
2024/09/09-07:28:13.942015 UTC [**] [Hostname: ir8340-sa-lan-vedge003] [**] [System_IP: 1.1.1.106] [**]
[Instance_ID: 1] [**] Drop[**] [1:100001:0] Snort Event [*Drop DNP3 Write*] [Classification: 1] [Priority:
0] [POLICY: ADVANCED_IPS] {TCP} 192.168.205.99:50333 -> 192.168.206.99:20000
```



Scenario 2: Block all DNP3 traffic on Untrusted Operators and Ports

Dual-Rule Setup for Strict Communication Policies

The following dual-rule setup is a practical way to enforce strict communication policies in an industrial control environment. It ensures that your trusted IEDs only communicate on their expected channels and with known, authorized operators—a critical step in defending such infrastructure.

```
drop tcp !$trusted_operator any -> $trusted_IED 20000 (msg:"Blocking DNP3 from untrusted operator"; dnp3; sid:1000002;)
```

Rule component	Defines	Description
`!$trusted_operator`	Source Check	The component causes the rule to match traffic coming from any IP that is not defined as a trusted operator.
`$trusted_IED 20000`	Destination Check	Traffic is only considered if it's destined for a trusted IED on port 20000.
`dnp3`	Protocol Content	This keyword tells Snort to inspect the payload for DNP3 protocol characteristics.
`drop`	Action	Using the drop action (in an inline deployment), the rule immediately discards any packet meeting these criteria.

```
drop tcp $trusted_operator any -> $trusted_IED !20000 (msg:"Blocking DNP3 traffic on unauthorized port"; dnp3; sid:1000003;)
```

Rule component	Defines	Description
`$trusted_operator`	Source Check	This rule matches traffic coming from a trusted operator (i.e., using the $trusted_operator variable).
`$trusted_IED !20000`	Destination Check	It specifically inspects packets aimed at a trusted IED but on any port other than 20000 (as indicated by the negation operator ! before the port).
`dnp3`	Protocol Content	Again, the DNP3 rule option ensures the rule only applies to DNP3 traffic.
`drop`	Action	Packets that meet these conditions are dropped, meaning that only traffic arriving on the authorized port is allowed.

What Happens in Practice

- **Legitimate Traffic**: If a DNP3 message is sent from an IP in `$trusted_operator` to a trusted IED on port 20000, neither rule is triggered. The packet is allowed to pass because both the operator IP and the port match your allowed list.
- **Untrusted Operator**: If a DNP3 packet is sent to a trusted IED on port 20000 but originates from an IP address not defined in $trusted_operator, the first rule matches and drops the packet.
- **Unauthorized Port**: Conversely, even if the packet originates from a trusted operator, if the DNP3 traffic is sent on any port other than 20000, the second rule will match and drop the packet.

- **Comprehensive Defense**: By deploying both rules, you permit only DNP3 traffic that contains both a trusted source and the correct destination port. This helps prevent potential spoofing or misconfiguration issues that could allow malicious commands to reach your trusted IEDs.

When the above rules match with an IPS inspection, then the event on the router is notified as follows.

```
2024/09/09-07:28:14.536610 UTC [**] [Hostname: ir8340-sa-lan-vedge003] [**] [System_IP: 1.1.1.106] [**]
[Instance_ID: 1] [**] Drop [**] [1:1000009:0] Snort Event [*Untrusted Operator*] [Classification: 0]
[Priority: 0][POLICY:ADVANCED_IPS] {TCP} 192.168.204.99:50359 -> 192.168.206.99:20000
```

Limitations

In Cisco Catalyst SD-WAN Manager, you can only upload one custom rule file at a time. This file is then applied to all edge routers. Therefore, you must include all rules in a single file, as you cannot configure separate custom rules for each edge router.

Conclusion

Cisco Catalyst IR8340, as a substation router and next-generation firewall (IDS/IPS), is flexible for deployment in OT environments. The standard ruleset is typically sufficient for most OT environments.

The benefits are substantial when the IT mindset is applied to detection mechanisms in OT networks. The participation of OT engineers is crucial in applying an IT solution for OT network visibility. OT teams are typically better aware of industrial processes than IT teams.By understanding the OT process, augmenting OT data with network detection by IT tools, you can:

- Increase visibility of process communication methods.
- Enhance the security posture of the OT network.

Using and customizing Snort in the OT environment as an IPS tool can also help you translate English alert messages to a native language alert message that is displayed on OT monitoring screens.

Customize alert text messages to:

- Speed up recovery processes.
- Detect who is doing what and from where based on the identity of accessed devices.
- Determine the importance of an event in OT networks.

SNORT custom rules provide significant value by allowing you to create tailored intrusion detection and prevention rules that address specific network security needs beyond the default rule sets. Custom rules are valuable for detecting attacks or behaviors not covered by standard rules, reducing false positives by disabling irrelevant rules, and enhancing detection capabilities tailored to your network environment.