Cisco IOS Intrusion Prevention System (IPS) for Connected Energy

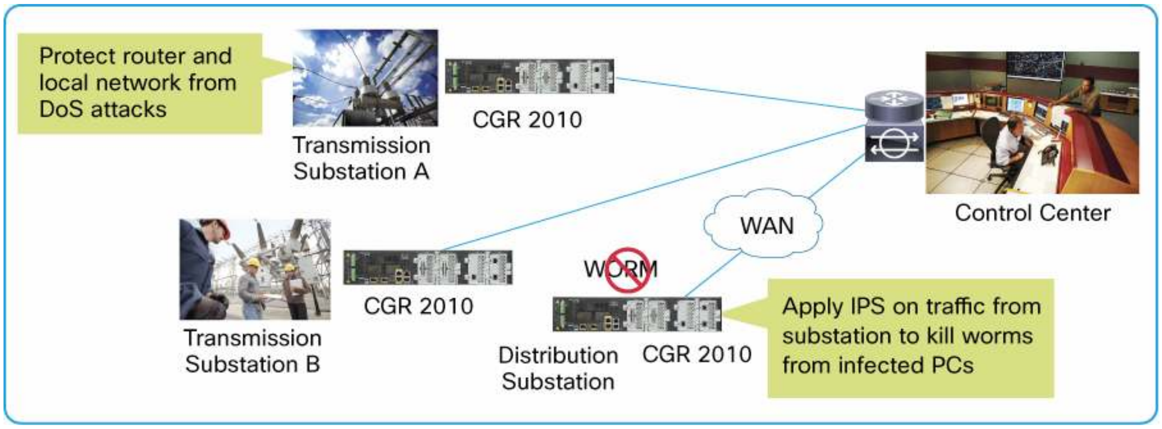
Product Overview

As more sophisticated communications technology is deployed in the energy infrastructure, security is top of mind for utilities and energy companies. Fortunately, the migration from legacy, proprietary systems to an IP standards-based technology platform provides many security capabilities that were not possible with older technology. Cisco®, the market leader in IP technology during the past 25 years, provides industry-leading network security in its routing and switching platforms.

For in-depth security, the Cisco 2010 Connected Grid Router (CGR 2010) offers an integrated Intrusion Prevention System (IPS). Cisco IPS solutions provide an inline, deep-packet inspection-based solution that enables Cisco IOS® Software to effectively mitigate a wide range of network attacks. The Cisco IOS IPS uses “signatures,” which are anticipated attack patterns, to monitor traffic flowing through the network. If a pattern of data matches a known attack outlined by the signature, the router can take user-defined action to prevent exploits or attacks. The system contains over 3000 general signatures used by customers worldwide.

Specifically for the energy industry, Cisco has implemented Supervisory Control and Data Acquisition (SCADA)-specific signatures on the CGR 2010. These SCADA signatures are based on anticipated attacks using Distributed Network Protocol 3 (DNP3) and Modbus protocols. By utilizing the CGR 2010 and providing this security down to the substation level, attacks can be countered right at the substation rather than back at the data center or central IT center. Figure 1 displays the Cisco IPS with the Cisco CGR 2010.

Figure 1. Cisco IOS IPS with the CGR 2010


Protect router and local network from DoS attacks
Transmission Substation A
CGR 2010
Control Center
WAN
Transmission Substation B
CGR 2010
WORM
Distribution Substation
CGR 2010
Apply IPS on traffic from substation to kill worms from infected PCs

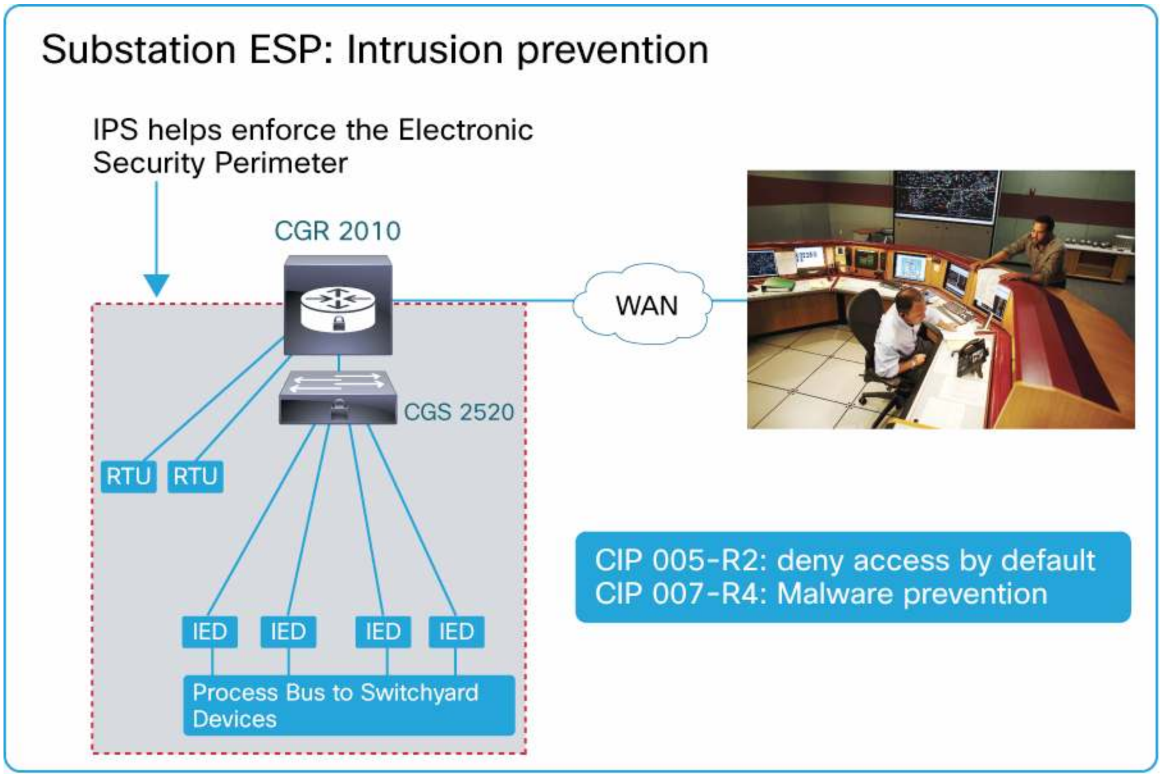
Primary Benefits

There are several benefits of the Cisco IOS IPS. The feature:

- Provides network-wide, distributed protection from many attacks, exploits, worms, and viruses that can exploit vulnerabilities in operating systems and applications

- Provides enhanced security down to the substation level and prevents attacks at the substation rather than waiting for information to travel back to the data center
- Offers a unique, risk-rating-based signature event action processor that dramatically improves the ease of management of IPS policies
- Offers field-customizable worm and attack signature sets and event actions
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions
- Works with Cisco IOS Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router
- Supports SCADA-specific signatures for monitoring SCADA traffic for vulnerabilities
- Help utilities meet North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) requirements (see figure 2)

Figure 2. Cisco Firewall and IOS IPS Help Meet NERC-CIP Requirements



Substation ESP: Intrusion prevention

IPS helps enforce the Electronic Security Perimeter

CIP 005-R2: deny access by default
CIP 007-R4: Malware prevention

SCADA-Specific Signatures: DNP3 and Modbus

Cisco IOS IPS on the CGR 2010 now supports SCADA-specific signatures that help identify attacks on the utility network. To develop these signatures, Cisco security experts worked with partners to develop anticipated attack scenarios using data with DNP3 and Modbus protocols. The CGR 2010 can reside in the substation and monitor traffic to and from Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs) for security vulnerabilities. Table 1 lists the currently supported signatures.

Table 1. SCADA Signature List

SCADA Sig ID	Description
5612/0	DNP3 - Unsolicited Response Storm
5613/0	DNP3 - Cold Restart Request
5614/0	DNP3 - Disable Unsolicited Responses
5615/0	DNP3 - Read Request to a PLC
5616/0	DNP3 - Stop Application
5617/0	DNP3 - Warm Restart
5618/0	DNP3 - Broadcast Request
5619/0	Non-DNP3 Communication on a DNP3 Port
5619/1	Non-DNP3 Communication on a DNP3 Port
5620/0	DNP3 - Write Request to a PLC
5621/0	DNP3 - Miscellaneous Request to a PLC
5622/0	Modbus TCP - Force Listen Only Mode
5623/0	Modbus TCP - Restart Communications Option
5624/0	Modbus TCP - Clear Counters and Diagnostic Registers
5625/0	Modbus TCP - Clear Counters and Diagnostic Registers
5626/0	Modbus TCP - Report Server Information
5627/0	Modbus TCP - Illegal Packet Size
5627/1	Modbus TCP - Illegal Packet Size
5628/0	Modbus Slave Device Busy Exception Code Delay
5629/0	Modbus Acknowledge Exception Code Delay
5630/0	Modbus TCP - Read Request to a PLC
5631/0	Modbus TCP - Read Request to a PLC
5632/0	Modbus TCP - Non-Modbus Communication
5632/1	Modbus TCP - Non-Modbus Communication

Signature Selection for Cisco IOS IPS

Cisco IOS IPS signature provisioning on the CGR 2010 is accomplished by selecting one of two signature categories—basic or default. Cisco IOS Basic and Default signature categories are pre-selected signature sets intended to serve as a good starting set for most users of Cisco IOS IPS. They contain the latest high-fidelity (low false-positives) worm, virus, instant messaging, or peer-to-peer blocking signatures for detecting security threat. This allows for easier deployment and signature management.

The SCADA IPS signatures are supported in Cisco IOS Software Release 15.2.(2)T and later releases of the CGR 2010 IOS Software. Users can add or remove individual SCADA signatures and can tune signature parameters using Cisco Configuration Professional (CCP). They can also do so through the command-line interface (CLI) which allows easy scripting to manage signature configuration for a large number of routers. CCP is a GUI-based device management tool for Cisco routers and switches. This tool simplifies routing, firewall, IPS, VPN, unified communications, WAN, and LAN configuration through GUI-based easy-to-use wizards. CCP is offered as a free tool with the purchase of the CGR 2010. Customers can find more information and download the CCP tool at http://www.cisco.com/en/US/products/ps9422/index.html.

Configuration and Signature Provisioning

The router CLI or CCP Version 2.4 or later can be used for configuration of Cisco IOS IPS as well as highly granular provisioning and tuning of IPS signatures on a single router running Cisco IOS Software Releases 15.2(2)M and 15.2(2)T and later releases.

Actions for Detected Signatures

Each individual signature or category of signatures selected can be configured to take any combination of the following five actions when triggered:

1. Send an alarm using a syslog message or log an alarm in Secure Device Event Exchange (SDEE) format
2. Drop malicious packet
3. Send TCP-reset packets to both ends of the connection to terminate the session
4. Deny all packets from the attacker (source address) temporarily
5. Deny further packets belonging to the same TCP session (connection) from the attacker (source address).

Note: Some actions are more CPU-intensive and have different effects on router throughput speeds.

Event Monitoring

Upon detecting an attack signature, Cisco IOS IPS can send a syslog message or log an alarm in SDEE format. CCP may be used to monitor events generated by a single router and Cisco IPS Manager Express (IME) may be used to monitor IPS events generated by up to five routers.

Signature Micro Engines

Cisco IOS IPS uses Signature Micro-Engines (SMEs) to load into the router's memory, and scan for a set of attack signatures. Each engine is customized for inspecting a Layer 4 or 7 protocol and its fields and arguments. Within each packet carrying data for that protocol, it looks for a set of legal parameters that have allowable ranges or sets of values. It also scans for malicious activity specific to that protocol using a parallel signature scanning technique to scan for multiple patterns within an SME at any given time.

SCADA Signatures on the Cisco 2010 Connected Grid Router

In order to have these SCADA-specific signatures on the CGR 2010, customers must purchase the security license for this router. The security license provides a wide set of firewall and security features for the platform. The 22 SCADA-specific DNP3 and Modbus signatures are included with the 3000 other signatures when purchasing the security license.

However, if customers would like to get signature updates, including new signatures as they are released, it is necessary to purchase a subscription to Cisco IPS services. The IPS subscription can be purchased for both Cisco Base and Cisco SMARTnet® services contracts. Table 2 lists the part numbers and descriptions.

Table 2. SKU Summary

SKU	Description
CGR-2010-SEC/K9	Cisco CGR2010 security bundle w/SEC license PAK
CON-SU1-C2010SEC	Cisco SMARTnet with IPS subscription
SP-SFSW-C2010SEC	SP Base with IPS subscription

For More Information

To learn more about the Cisco IOS IPS please visit http://www.cisco.com/en/US/products/ps6634/index.html

To learn more about the Cisco 2010 Connected Grid Router please visit http://www.cisco.com/go/cgr2010

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-696141-00 12/11