The bridge to possible

Cisco Catalyst Industrial Routers with Cisco Next-Generation Firewall

Across all industries, organizations need advanced, agile, and secure Wide Area Network (WAN) infrastructures to connect distributed Operational Technology (OT) assets to control centers and unlock the potential of digitization. Whether it's about connecting roadways assets, first responder or public transport vehicles, water, oil, or gas infrastructures, renewable energy resources, power substations, EV charging stations, or any critical remote assets, you need rugged routers with cutting-edge cybersecurity capabilities.

As we define the networking standards of the future, Cisco believes industrial routers must become a platform to easily deploy advanced OT security capabilities at scale. In addition to enabling smarter and simpler WAN infrastructures, Cisco industrial routers come with next generation firewall capabilities, malware protection, cloud security, and threat intelligence feeds to help you build secure distributed networks so you can run modern industrial operations with peace of mind.

Leveraging Cisco industrial routers to protect your critical infrastructure

Cisco® Catalyst Industrial Routers offer unconditional connectivity for all your remote assets. They can withstand extreme temperatures, humidity, and dust. They offer a variety of WAN connectivity options, including 5G/LTE cellular, MPLS, Ethernet, and fiber, through pluggable interface modules that can be easily replaced when needs or technologies evolve. In addition, Cisco Catalyst SD-WAN simplifies deploying and managing a large and complex WAN infrastructure from a central location.

Figure 1. Catalyst industrial routers are purpose built for industrial use cases

Catalyst industrial routers also come with comprehensive Next-Generation Firewall (NGFW) features and many more cybersecurity capabilities to block modern threats:

- Standard firewall capabilities like stateful inspection,
- Application awareness and control to block application-layer attacks,
- Integrated intrusion prevention (IDS/IPS),
- Continuously up-to-date threat intelligence,
- Malware protection and sandboxing,
- URL filtering,
- Integration with a Secure Services Edge (SSE).

Building a modern industrial WAN infrastructure requires advanced routing capabilities such as only Cisco can offer. Having state-of-the-art cybersecurity features built into your industrial routers not only is vital to keep the organization safe, but it's also key to simplify and scale deployment and management tasks. Converging industrial networking and cybersecurity helps ensure unified security policies are enforced across sites, eliminating gaps in defenses due to cost and complexity of integrating many point products together.

The bridge to possible

Benefits

- **Connect critical OT assets anywhere** with a wide range of modular rugged industrial routers that adapt to your needs.
- **Easily deploy and manage WAN infrastructures** of any size and complexity with powerful management tools.
- **Beat modern threats** by blocking malware intrusion, malicious traffic, and application-layer attacks.
- **Unify security policies** across all your remote industrial sites by centralizing policy definition to easily deploy at scale.
- **Secure access to cloud resources** by using secure DNS or centralizing policy enforcement toward the cloud.
- **Be always up to date** with Talos threat intelligence feeds that help your security infrastructure fight against the latest threats.

Stateful inspection with application awareness and control

All Cisco industrial routers offer stateful firewall inspection with application recognition for creating localized security policies to limit traffic between assets. Using Network Based Application Recognition (NBAR2), which can detect over 5,000 applications, Cisco industrial routers can recognize whether protocols are operating on standard network ports. In some cases, the presence of specific applications operating over nonstandard ports may indicate a policy violation or an attempt to evade firewall controls.

Additionally, application recognition can be used to create Quality-of-Service (QoS) policies, helping ensure that the most critical network traffic in the infrastructure always has priority and evading potential Denial-of-Service (DoS) attempts on the OT network.

Segment and protect critical infrastructure

Along with QoS, critical infrastructure can be further protected from noncritical assets that share the same physical infrastructure by segmenting traffic flows into separated virtual networks. Virtual Routing and Forwarding (VRF) allows a Cisco industrial router to run more than one routing table simultaneously. The routing tables are completely independent and fully segmented by default. For traffic originating in one domain to reach another domain, it must be explicitly routed through a firewall, reducing the possibility that an administrative error will lead to a wide-open network.

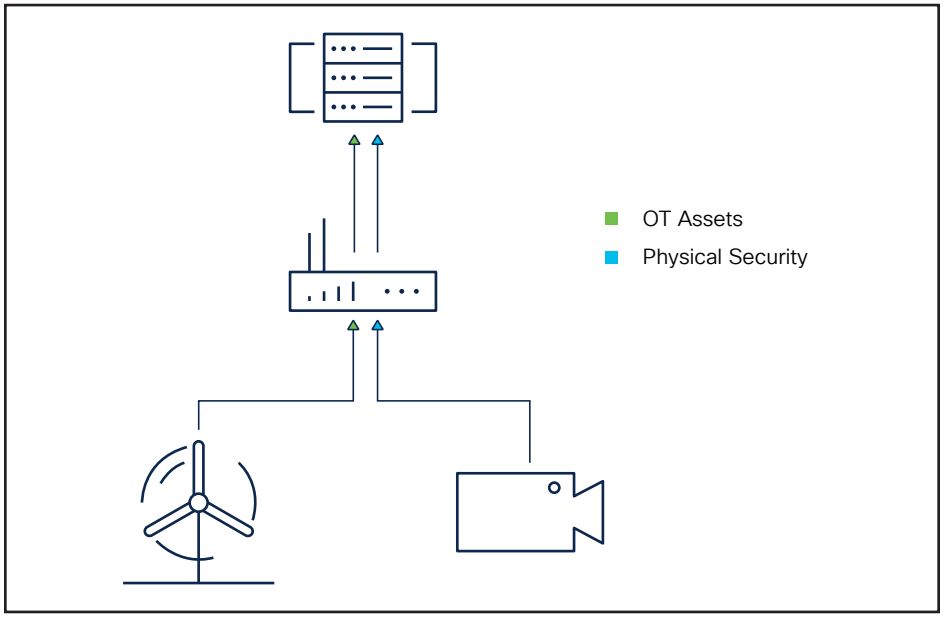

Figure 2. Traffic isolation

Whether it is a traffic cabinet, wind farm, or rail-side signaling, resources in the network infrastructure are often shared with physical security, technicians, IoT sensors, and more. Cisco industrial routers help ensure that the critical traffic that keeps our world moving remains protected.

Integrated intrusion detection and prevention system

An intrusion detection and prevention system (IDS/IPS) detects and blocks known network attacks. It uses signatures, which are a set of rules, to detect attacks originating from both external and internal sources.

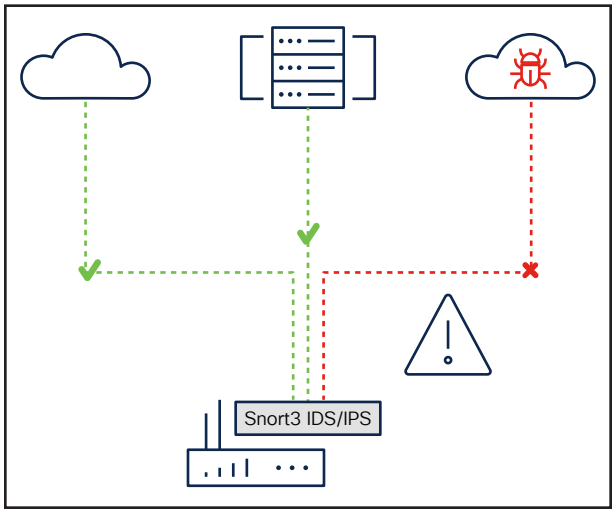

Figure 3. Intrusion detection and prevention

Snort®, the open-source IDS/IPS engine used across the Cisco portfolio, enables Cisco industrial routers to perform real-time traffic analysis to detect and prevent cyber threats. Cisco Talos®, the threat intelligence that powers Snort, leverages the world's largest threat detection network to bring security effectiveness to every Cisco security product. This industry-leading threat intelligence works as an early-warning system that constantly updates with new threats to help keep your infrastructure safe.

Rules can also be customized for OT deployments. Snort provides pre-processors for the Modbus, Distributed Network Protocol (DNP3), Common Industrial Protocol (CIP), and S7Commplus protocols so that network access policies can be easily customized for more granular application control.

Malware protection and sandboxing

Malware is one of the most common cyber threats. Detecting and removing malicious files before they enter your network is key to prevent breaches. Cisco Advanced Malware Protection (AMP) integrated into Cisco industrial routers equips the platform to provide protection and visibility from malware. Before letting a file enter the network, your Cisco industrial router generates a 256-bit Secure Hash Algorithm (SHA256) signature and compares it against a database curated by Cisco Talos, the industry's largest collection of file reputation intelligence.

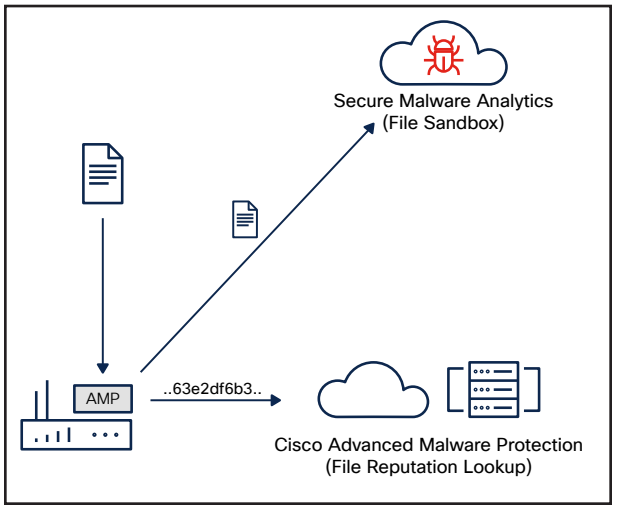

Figure 4. Sandboxing an unknown file

Files with an unknown disposition can be sent to the Cisco Secure Malware Analytics cloud for further analysis within a sandbox. During detonation, the sandbox captures artifacts and observes the behavior of the file, then gives the file an overall score of abnormal behaviors. Based on the observations and score, Secure Malware Analytics will define the file as clean or malicious so your Cisco industrial router will let it pass or block it.

URL filtering

Use cases such as predictive maintenance or IoT applications often require connections to cloud resources, increasing the attack surface. To enable such innovation, URL filtering in the Cisco industrial routers allows control access to trusted cloud resources by configuring domain-based or URL-based policies. Although we recommend that access to cloud and internet resources be disabled by default, and that you explicitly allow only trusted domains, security administrators have peace of mind that the network is protected by reputation-based filtering. Each URL has a web reputation score associated with it to help ensure that users or applications are not communicating with high-risk parts of the internet.

Integrating with a security service edge

Whether it is rail-side deployments spanning hundreds of miles or traffic intersections that are distributed across a whole city, critical infrastructure is often widely distributed. When deploying Cisco industrial routers, network architects have a choice of where advanced security policies will be deployed. A common deployment model is to centralize the most advanced policies in the network, alleviating the burden that may exist on edge nodes. Cisco industrial routers can leverage Cisco Secure Access or any third-party Security Service Edge (SSE) via IPsec tunnels to centralize policy enforcement across sites or toward the cloud.

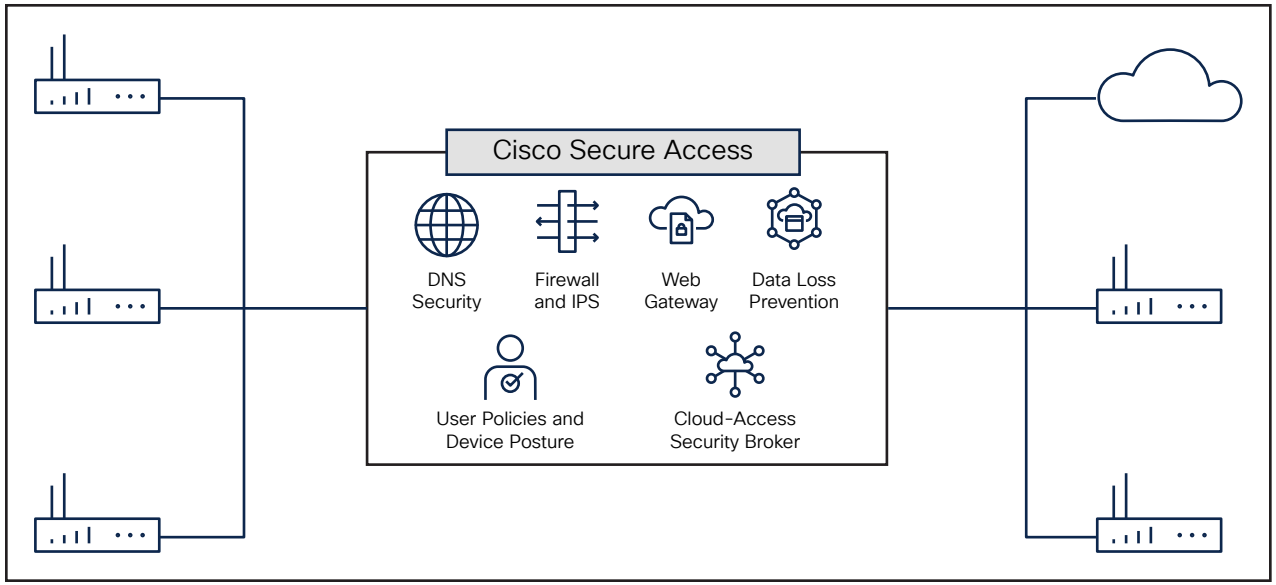

Figure 5. Cisco Secure Access

With Cisco Secure Access, network administrators enable segmentation and prioritization to the most critical traffic on the network, while security administrators maintain granular control of data that comes into and out of each remote site with a single set of policies, so that only known, trusted traffic flows throughout the infrastructure.

The bridge to possible

Centralized management with Catalyst SD-WAN Manager

As you connect distributed industrial sites together, it is essential to simplify and automate your WAN infrastructure deployment and management. Cisco Catalyst SD-WAN provides solutions for common challenges for industrial spaces by supporting multiple transports with configurable dynamic routing polices while leveraging the same security features and management tools for both the enterprise and industrial network extensions.

The Cisco Catalyst SD-WAN Manager provides both centralized policy creation for all Cisco industrial routers deployed in the infrastructure. By creating security policy templates, all existing devices, and any newly connected devices, will be subject to a consistent set of policies curated by the security team.

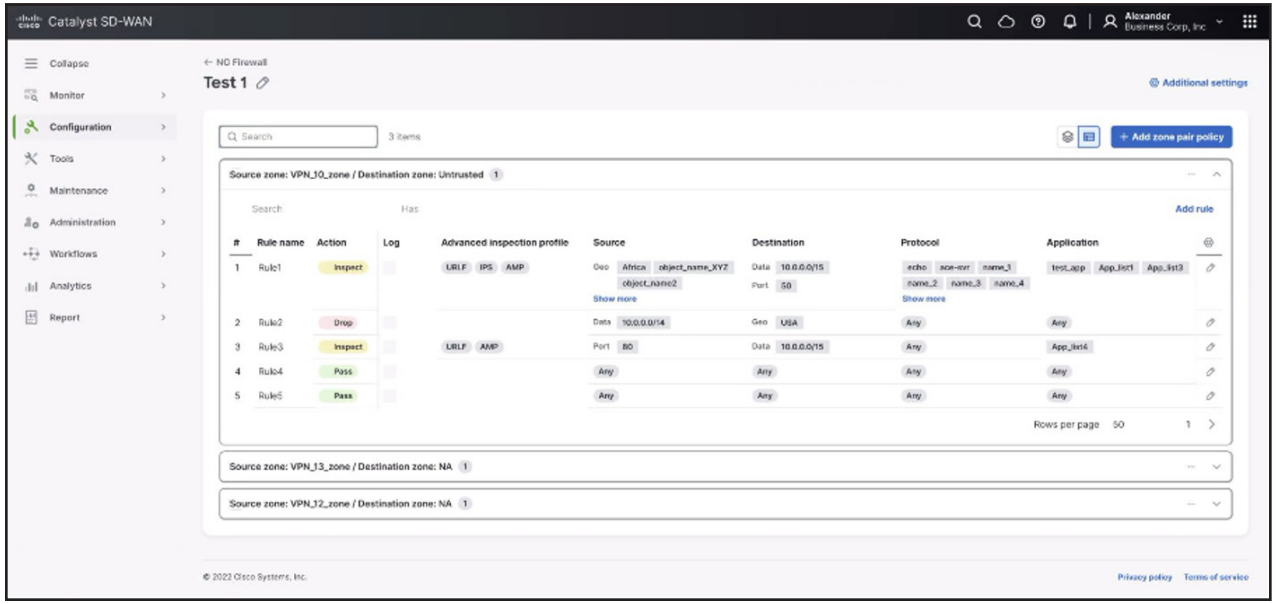

Figure 6. Cisco Catalyst SD-WAN Manager centralizes security policy definition

Cisco Catalyst SD-WAN Manager also offers centralized logging and reporting. It collects all events, alarms, and logs from your Cisco industrial routers, giving security teams visibility and understanding of any activity that is occurring within their critical infrastructure and helping them comply with cybersecurity mandates like NIS2.

Nevertheless, for deployments that are not leveraging centralized management, the NGFW features of the Cisco Catalyst industrial routers can be managed using the traditional command line interface.

The bridge to possible

The Cisco advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more.

Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. This rare combination makes Cisco an ideal partner to help industrial organizations secure their critical infrastructure from the ever-growing threat landscape.

Build your secure WAN infrastructure with Cisco

Talk to a Cisco sales representative or channel partner and visit these web pages to learn more:

- Catalyst Industrial Routers
- Cisco Validated Designs: SD-WAN for Industrial Markets
- Cisco Catalyst SD-WAN

Supported platforms

All Cisco Catalyst industrial routers have security built in. Cisco IOS® XE, the software that powers all Cisco networking infrastructure, provides stateful packet inspection, application visibility and control, VPN, segmentation, DoS mitigation, and FQDN matching.

For the remaining features, there is an NGFW add-on that can be deployed in devices with 8 GB of memory. The NGFW add-on for industrial routers provides Snort IDS/IPS, reputation-based URL filtering, and malware protection.

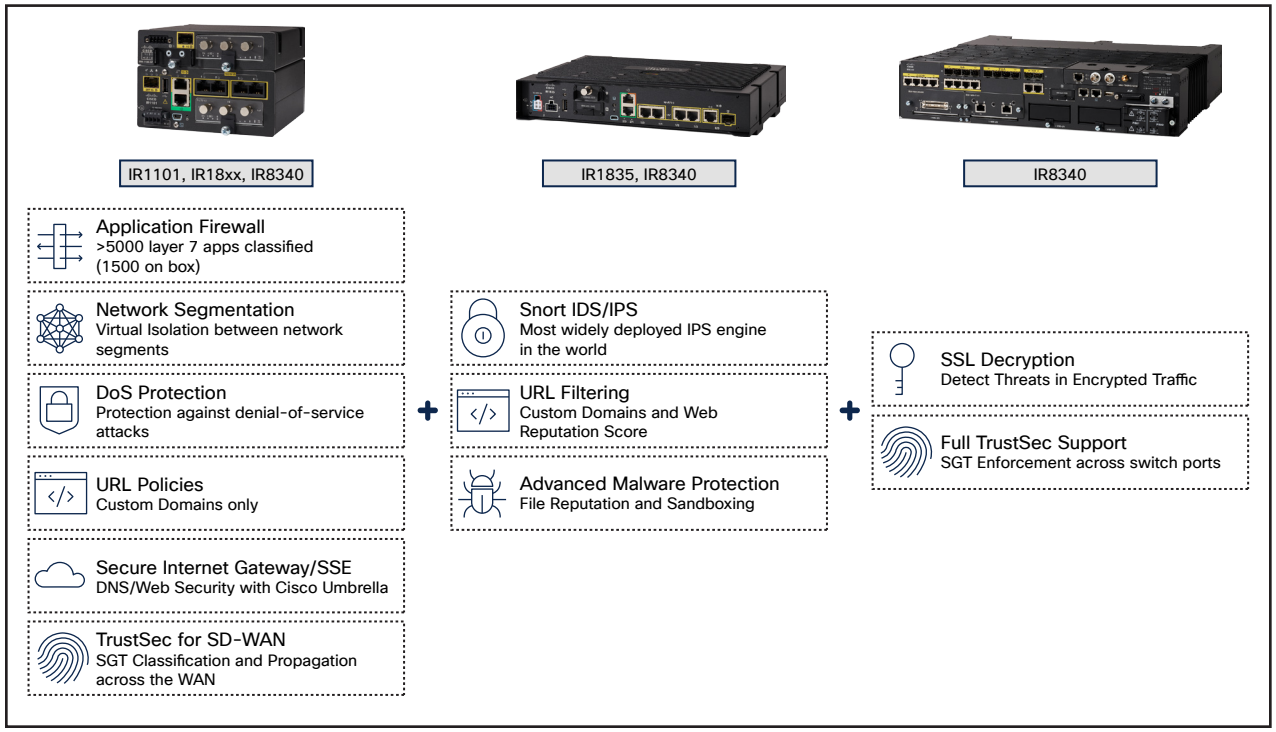

Figure 7. Catalyst Industrial Routers security features per platform