Securing Distributed Energy Infrastructures with SD-WAN

In contrast to traditional power generation plants, renewable energy sources such as solar and wind farms, biomass, hydropower, and geothermal installations number in the thousands, are distributed across large and remote areas, and are usually unmanned.

Connecting many highly distributed substations and renewable energy facilities requires purpose-built communication technologies that simplify network operations and meet the constraints of power utilities. Ensuring that sites are safe from cyberthreats is key to guaranteeing grid resilience and to complying with stringent cybersecurity regulations such as NERC CIP in North America and NIS2 in Europe.

By combining a comprehensive portfolio of rugged routers ideally suited for grid deployments, and a market-leading SD-WAN solution that embeds advanced cybersecurity features, Cisco offers a powerful network architecture that simplifies and secures grid operations at massive scale.

Build a unified WAN to easily connect field assets

The distributed nature of renewable energy resources requires a complex network infrastructure spanning multiple locations. Challenges such as latency and adequate bandwidth, redundancy and resiliency, scalability and flexibility, cybersecurity and more need to be addressed. These requirements are more stringent for critical resources, since any inadequacy could jeopardize grid stability and national security.

To meet these dynamic requirements, Software-Defined WAN (SD-WAN) is rapidly becoming the preferred connectivity choice for distributed assets. SD-WANs are more agile and flexible, can be deployed more quickly, and are easier to manage and scale. They offer improved performance, better security, and reduced costs.

The Cisco Catalyst™ SD-WAN solution with Cisco Catalyst Industrial Routers is ideally suited for these demanding grid requirements. It combines enterprise-grade performance and security with industrial-strength reliability and resilience.

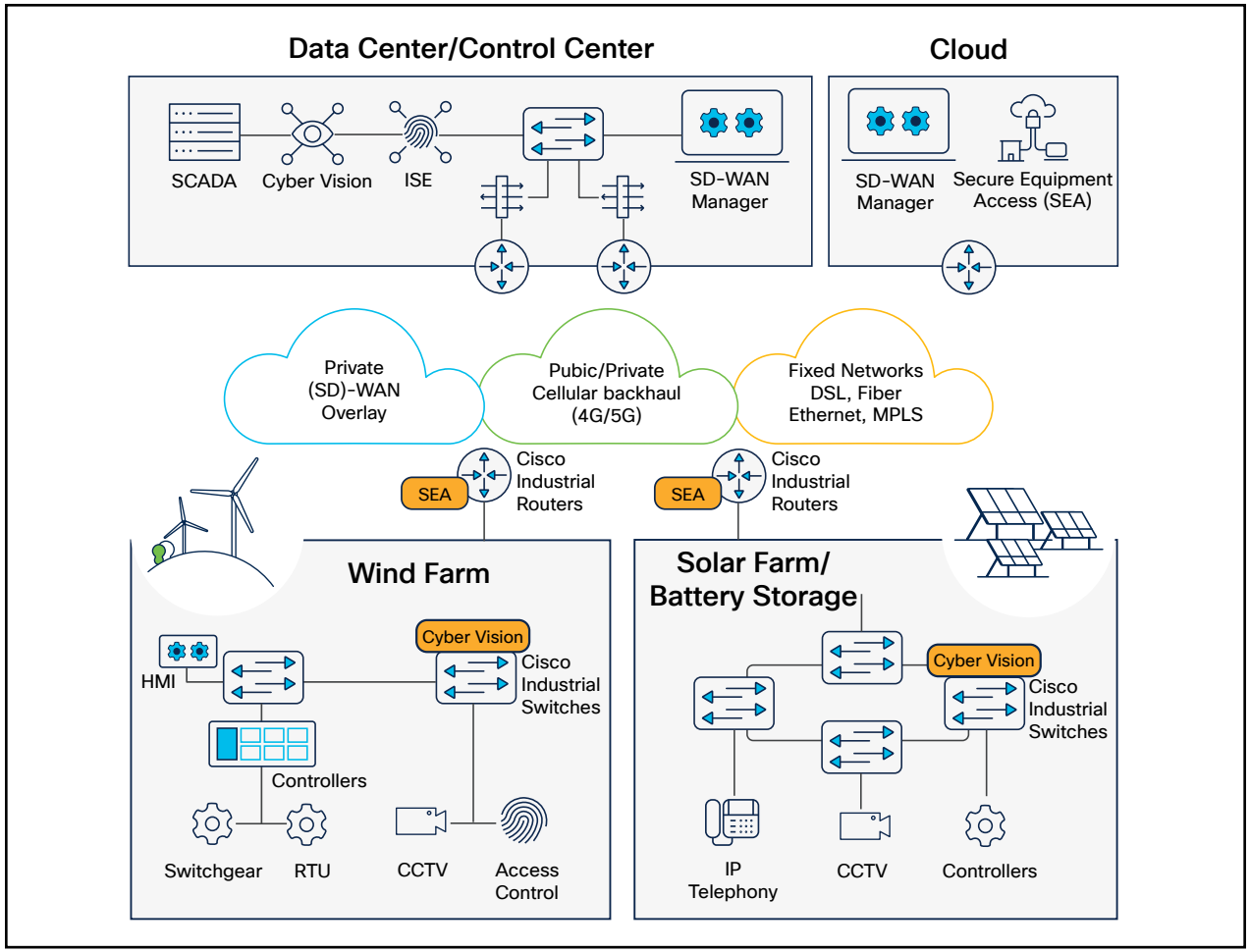

Figure 1. Cisco's secure SD-WAN architecture for distributed energy resources

Benefits

- Easily connect and secure distributed energy resources with a converged networking and security architecture.
- Streamline network operations at scale with automated provisioning and centralized management of rugged routers, purpose-built for your grid requirements.
- Simplify security operations and reduce costs by building security constructs within networking equipment instead of multiplying point products.
- Enforce advanced and consistent security across all facilities with centralized policy definitions.
- Take control over remote access to grid assets with zero-trust network access that's easy to manage and built into the network.

Purpose-built solutions to connect remote grid assets

The specific constraints of grid operations require purpose-built routers offering features such as high availability, support for industrial protocols, and specific certifications such as IEC 61850-3 and IEEE 1613 for safe deployment in utility infrastructures.

Cisco Catalyst Industrial Routers offer unconditional connectivity for all your power generation, transmission, and distribution assets. They can withstand extreme temperatures, humidity, dust, and water. They are certified for grid deployment and offer a variety of WAN connectivity options, including 4G/5G cellular, MPLS, Ethernet, and fiber, through pluggable interface modules that can be easily replaced when needs or technologies evolve.

Precision Timing Protocol (PTP) is supported to ensure clock synchronization across all grid assets. Some models also have GPS/GNSS clock inputs for time coordination across the network.

There's a grid router for every need

Cisco Catalyst IR1100 Rugged Series Routers

Ultra-compact, modular, and expandable router to securely connect substations to your SD-WAN.

Cisco Catalyst IR1800 Rugged Series Routers

This modular router offers multiple cellular interfaces, Wi-Fi 6, and advanced SD-WAN security capabilities.

Cisco Catalyst IR8100 Heavy Duty Series Routers

This fully modular router is IP67-rated for extending your SD-WAN to the outdoors and to the harshest environments.

Cisco Catalyst IR8300 Rugged Series Router

This all-in-one routing and switching platform provides outstanding performance, security, and modularity for connecting larger sites to your SD-WAN.

Simplify and automate your WAN operations

Configuring and managing a large number of routers connecting your distributed energy resources and substations to your control center can be a daunting task. Cisco Catalyst SD-WAN Manager (formerly vManage) provides a highly visualized dashboard that simplifies network operations. It enables automated provisioning and centralized configuration, management, and monitoring across the entire SD-WAN fabric, using any transport (internet, MPLS, or 4G/5G).

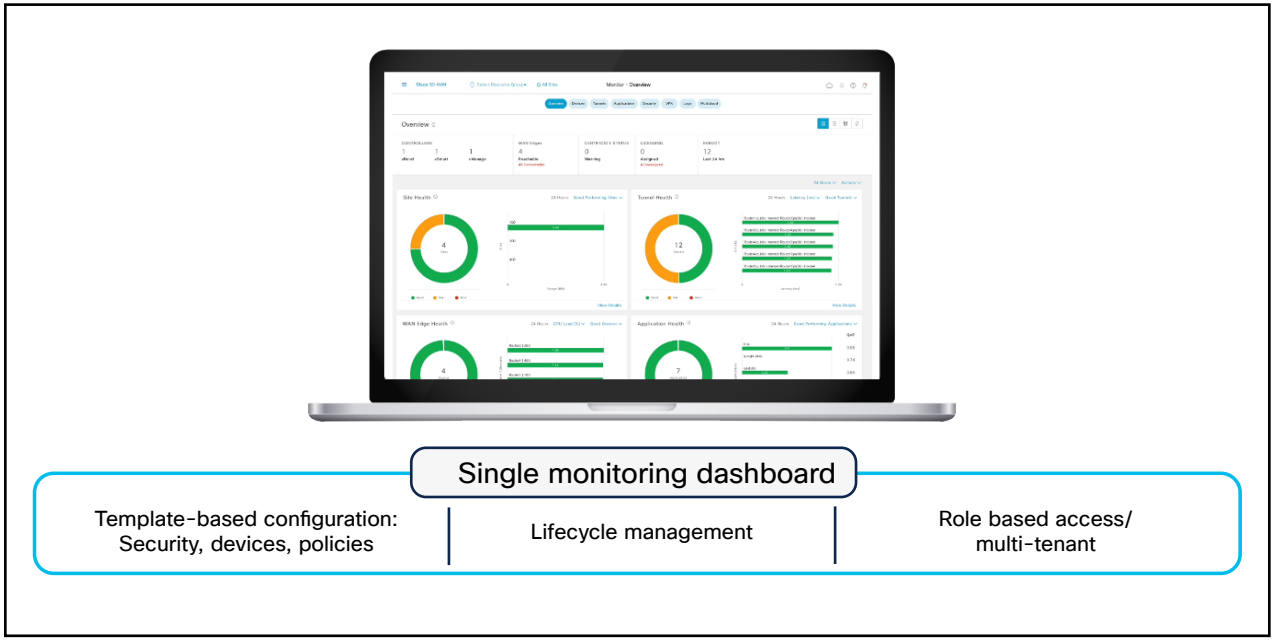

Figure 2. Cisco SD-WAN dashboard for managing and securing connection to distributed locations

One dashboard. Countless capabilities.

Catalyst SD-WAN Manager unifies security policies across all sites by centralizing configuration of your routers' integrated firewall, and by offering features such as URL filtering, Intrusion Prevention (IPS), malware protection, and more. It also helps with compliance by providing visibility into security events. It supports large-scale deployments, helping ensure consistent management capabilities even when operating thousands of units of remote network equipment.

Cisco Catalyst SD-WAN combines network management and cybersecurity capabilities into an easy-to-operate WAN infrastructure. It provides the foundation for a Secure Access Service Edge (SASE) architecture that converges advanced security and WAN management into a cloud-based service, making it even easier to implement a zero-trust security model and enforce strict access control policies wherever devices and users are connected and applications are located. Migrating to a SASE architecture is quite simple once Catalyst SD-WAN is in place.

Protect your grid operations with unified networking and security

Distributed energy resources and utility substations face constant threats to cyber and physical security. The Cisco Catalyst SD-WAN solution enables a broad set of cybersecurity capabilities enforced locally by Cisco Catalyst Industrial Routers but managed centrally by the Catalyst SD-WAN Manager.

Catalyst SD-WAN simplifies policy definition, helps ensure consistency across all sites, and offers a centralized view of security events, all within a single dashboard. The Catalyst SD-WAN security architecture eliminates the need to deploy multiple point products in cabinets where space is limited. It leverages the power of your Catalyst Industrial Routers to offer comprehensive threat detection and response capabilities across the SD-WAN.

Defend against threats with comprehensive security policies

Catalyst SD-WAN secures all your connected grid assets by empowering your Catalyst Industrial Routers with advanced security capabilities such as:

- **Firewall with application awareness (NGFW)** to filter traffic in real time and provide granular control capable of detecting thousands of applications.
- **Intrusion Detection and Prevention (IDS/IPS) with Talos® signatures** to identify and block known threats and malicious activities such as vulnerability exploits.
- **Advanced malware protection** techniques, including signature-based and behavior-based analysis, to identify and block known and unknown malware threats.
- **URL filtering** to block or allow users to access URLs based on more than 80 web categories covering millions of domains and billions of web pages.
- **Secure access to cloud and internet resources with Cisco Umbrella®** which combines secure web gateway, DNS security, cloud-delivered firewall, cloud access security broker functionality, and threat intelligence to protect against internet threats.

Identify connected assets and assess your security posture

As important as it is to secure outside connections to your grid operations, it is equally necessary to guard against threats from connected assets. One of the biggest challenges is knowing what is connected to the local network and monitoring communication activities. Regulations often require utilities to have comprehensive visibility into their asset inventory to reduce the attack surface and detect anomalous behaviors.

Cisco Cyber Vision uncovers the smallest details of your grid infrastructure. It automatically builds a detailed inventory of all grid assets, including their communication patterns, vulnerabilities, rack slot configurations, vendor references, serial numbers, and more. It calculates risk scores for each asset and any specific parts of your operations to highlight critical issues so you can prioritize what needs to be fixed.

Visibility you can easily deploy at scale

The Cyber Vision visibility capability is embedded into Cisco industrial routers and switches installed in substations, power generation, and control center facilities. There is no need for dedicated security appliances and the effort of installing them. Your network is the sensor and sees everything that connects to it, to save on WAN costs and enable deployment at scale.

Apply a zero-trust policy to your infrastructure

Securing every port of your field networking equipment is key. Cisco Identity Services Engine helps ensure that only the devices you specify are granted access. When combined with Cyber Vision, it automatically identifies the assets you trust, and all other devices are denied access by default. You can even create policies to ensure that assets can communicate only with the resources they need, giving you the control you need to enforce ISA/IEC-62443 zones and conduits.

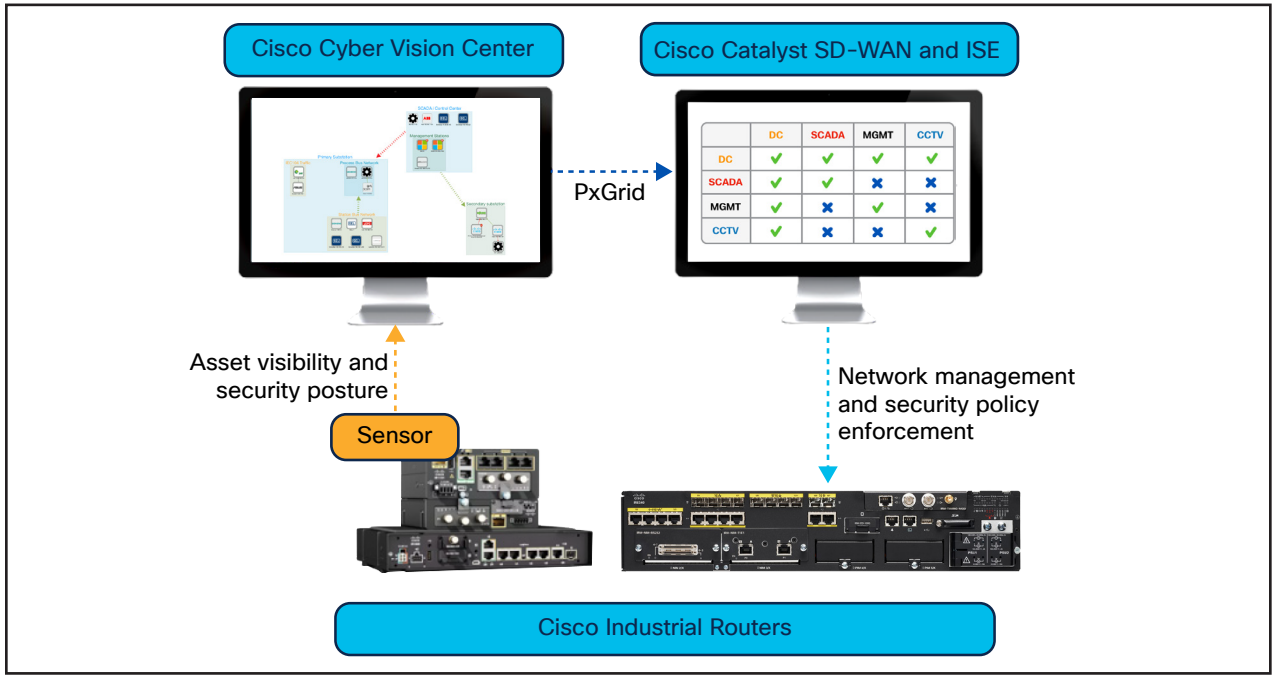

Figure 3. Using network equipment to gain visibility into connected assets and drive segmentation

Enable easy-to-use, secure remote access

Enabling remote access to highly distributed substations and renewable energy sites is key to reducing operational costs and minimizing downtime. Gateways installed by vendors or contractors make it very difficult to control who is connecting and what they can access. VPN-based solutions can be quite complex to manage at scale. Cisco Secure Equipment Access (SEA) gives you full control while empowering OT teams to manage remote accesses in order to run the business efficiently.

Remote access under total control

Cisco SEA is a Zero-Trust Network Access (ZTNA) solution specifically designed for OT workflows. It gives users access only to specific assets at specific times and using only protocols you choose. Assets are hidden from discovery, and lateral movement is restricted. User identity is verified using Multifactor

Authentication (MFA), and their security posture is checked. Sessions can be recorded for use in audit trails and compliance reports.

Remote access you can deploy at scale

With Cisco SEA, users connect to a cloud portal responsible for policy enforcement. It communicates with Cisco switches and routers deployed onsite to create a communication path to the OT assets. There is no point hardware solution to source, install, and manage. Enabling secure remote access is just a software feature to activate in network equipment. Policy management is centralized in an easy-to-use web portal to unify remote access control across all sites and empower OT administrators to allow remote access when needed.

Secure your distributed energy infrastructure with Cisco

Talk to a Cisco sales representative or channel partner and visit cisco.com/go/iotutilities or cisco.com/go/iotsecurity to learn more.

Browse the library of Cisco Validated Designs for power utilities and renewable energy for guidance and implementation guides on the best architecture for your specific needs.

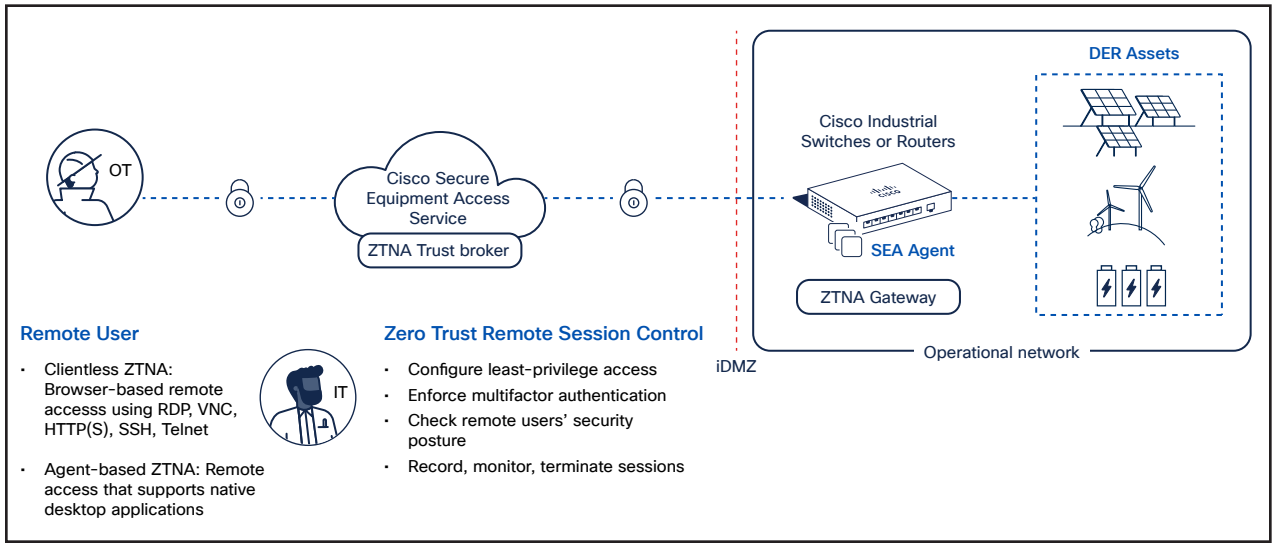

Figure 4. Zero-trust network access to grid assets with Cisco Secure Equipment Access

The Cisco advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe to 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. It's a rare combination.

By designing, developing, and testing products together, Cisco enables IT and OT teams to achieve advanced outcomes while reducing the complexity, time, and gaps incurred by the need to make point products work together. Our solutions come with comprehensive design and implementation guides that will help you reduce risk, accelerate implementation, and make the most of your technology stack.

C22-4149795-01 08/24