Cisco Connected Grid Security for Field Area Network

Introduction

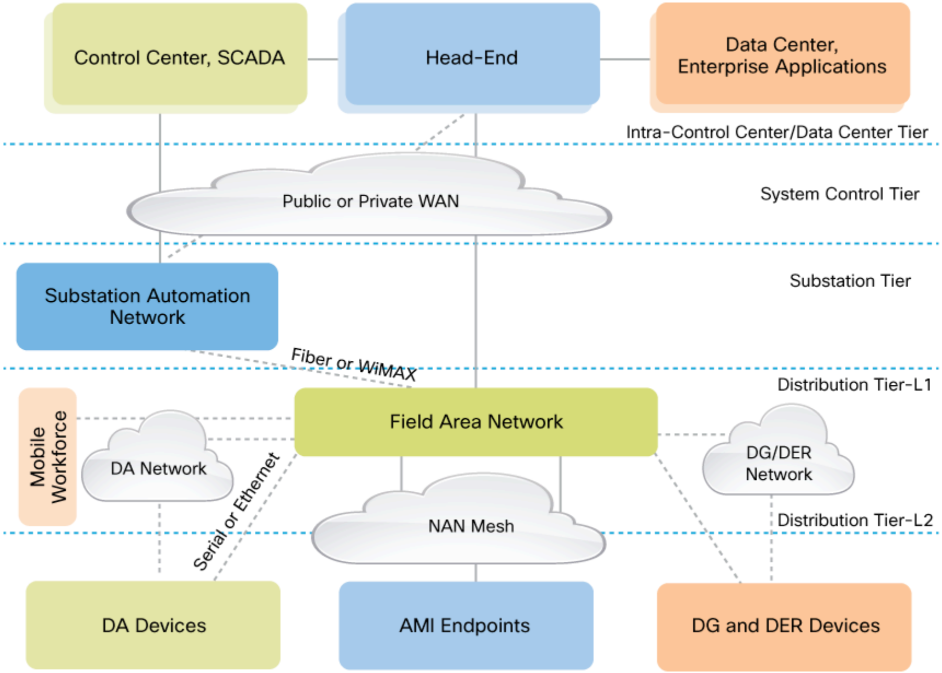
Utilities all over the world are undergoing significant transition in their grid—from transmission to consumption. Regulatory mandates are influencing initiatives around smart metering, grid reliability, and integration of solar and wind farms into the distribution grid. This in turn, imposes a unique set of challenges for utilities to build a bi-directional communications field area network (FAN) that enables these diverse applications and also scales across millions of endpoints.

The Cisco® Connected Grid FAN Solution has been specifically developed to meet these challenges, using design principles from industry-leading Cisco GridBlocks™ Reference Model. The solution offers the following benefits:

- Reduced system vulnerability to physical attack or cyber attack
- Operating resiliency against security disruptions
- Highly secure access and data privacy for smart grid information
- Establishment of a framework for meeting regulatory compliance requirements

In this white paper, we will focus on security for the field area network with smart meters and distribution automation devices connecting back to utility control centers through Cisco's Connected Grid solutions. Specifically, we will show how Cisco technology helps enable better security and reliability in the distribution grid of utilities and energy providers. Figure 1 displays a hierarchical layout of the utility communications network.

Figure 1. Tiered Communications Network for typical utilities



As illustrated above, a typical communications network for the distribution grid is a two-tier architecture with Neighborhood Area Network (NAN) and Wide Area Network (WAN).

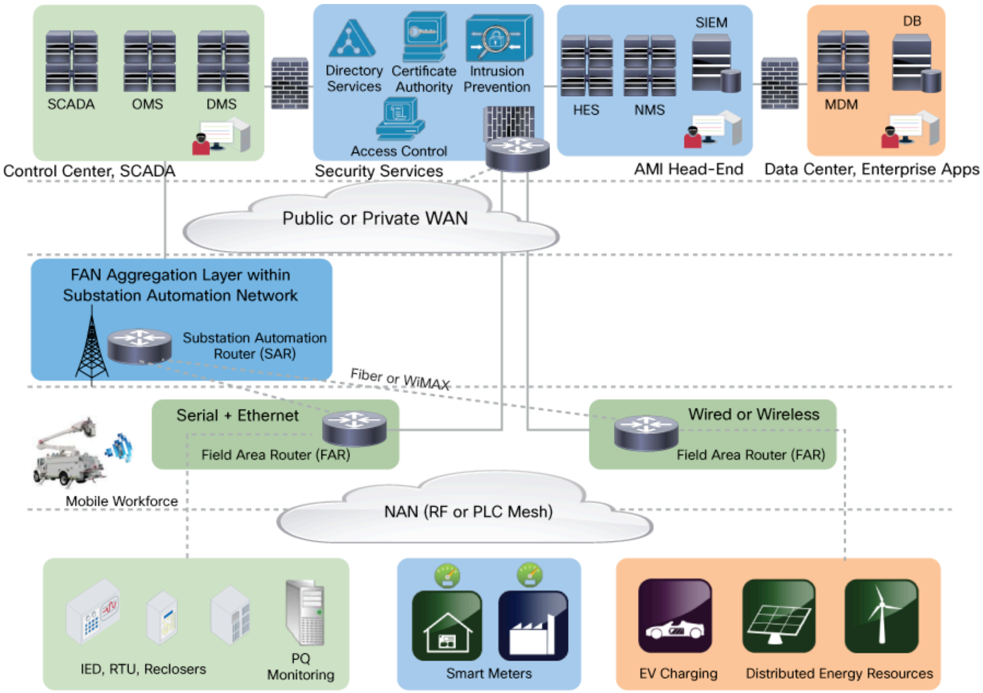
The NAN provides network connectivity to endpoints such as smart meters and distribution automation (DA) devices. These endpoints form a mesh network based on radio frequency (RF) or power-line communications (PLC) technologies. The WAN tier provides network connectivity to the utility's control center over either a service-provider network (cellular or fiber) or over a utility-owned network (private WiMAX or fiber),traversing the primary substations in many cases.

The NAN mesh network is aggregated at an intelligent device such as a field area router (FAR) mounted on pole-tops or in secondary substations. The FAR is a critical element of the architecture as it ties the NAN and WAN tier together. It also enables a multi-service network by offering ethernet, serial and wireless LAN connectivity for distribution automation and remote workforce-automation use cases.

Figure 2 provides a detailed view of the multi-service FAN with endpoints in the distribution grid, such as smart meters, DA devices, streetlights, public electric vehicle charging stations, and solar and wind farms. Such endpoints need to be embedded with a Cisco IPv6-based reference design (CG-Endpoint) to help enable superior communications and management to each node.

At the intra-control center tier, there can be many solution elements, ranging from Supervisory Control and Data Acquisition (SCADA) control, to data center, to the advanced metering infrastructure (AMI) head-end. Security services illustrated in Figure 2 form an important subsection of the head-end, for AMI as well as DA applications.

Figure 2. Tiered Communications Network with multi-service FAN and Head-End Components



Connected Grid Security Principles

Cisco integrates security as a fundamental building block of any network architecture—whether for the field area network, transmission and substation network, or the intra-control center tier. The primary principles behind Cisco Connected Grid security include:

- Access control
- Data integrity, confidentiality, and privacy
- Threat detection and mitigation
- Device and platform integrity

Access Control

The fundamental element of access control is to have strong identity mechanisms for all grid elements—users, devices, and applications. It is equally important to perform mutual authentication of both nodes involved in the communications for it to be considered secure.

The CGR 1000 Series, Cisco's Field Area Router (FAR), is manufactured with a X.509-based digital certificate that can be used to bootstrap the device and install utility's own digital certificate. Such an identity then forms the basis of authentication, authorization and accounting (AAA) services performed by the router with other entities, such as meters, aggregation routers, network management system, and authentication servers. Similarly, Cisco's recommendation is to use an X.509 certificate-based identity for meters since it is a highly secure method for authentication, as well as for scalable cryptographic key management.

Strong authentication of nodes can be achieved by taking full advantage of a set of open standards such as IEEE 802.1x, Extensible Authentication Protocol (EAP), and RADIUS. Every meter joining the mesh network needs to get authenticated before being allowed access to the AMI infrastructure. The FARs, along with intermediate meters, pass on the new meter's credentials to the centralized AAA server. Once authenticated, the meter is allowed to join the mesh and will be authorized to communicate with other nodes. Similarly, the IEEE 802.1x authentication mechanism can be used for locally-connected DA devices and can be combined with address allocation schemes such that only authenticated nodes can obtain an IP address.

For remote workforce automation, the Cisco 1000 Series Connected Grid Router (CGR 1000 Series) comes equipped with a Wi-Fi interface that can be accessed by field technicians for configuration. In order to gain access to the device, the technician will need to be authenticated and authorized by the authentication server in the head-end. For such role-based access control (RBAC), the technician's credentials could be a username and password or a X.509 digital certificate.

Data Integrity, Confidentiality, and Privacy

One of the critical security requirements in the FAN is to ensure data integrity and confidentiality for data from smart meters and distribution automation devices when it traverses any public or private network. Data confidentiality uses encryption mechanisms available at various layers of the communication stack. For example, an IPv6 node in the last mile (e.g. smart meter) can encrypt data using Advanced Encryption Standard (AES) at :

- Layer 2 (IEEE 802.15.4g or IEEE P1901.2)
- Layer 3 (IP Security [IPsec])
- Layer 4 (Datagram Transport Layer Settings [DTLS]), or
- Layer 7 (ANSI C12.22 or DLMS/COSEM)

The choice of a given layer for encryption is subject to the constraints on the node in terms of processing power, the network architecture, and scalability of deployment. For example, software upgrade or dynamic pricing can be efficiently sent to a select group of meters by use of Layer 3 IP Security (IPSec) and IP multicast on routers in the network infrastructure. The standards-based IPSec protocol suite ensures data integrity and confidentiality for all traffic—be it smart metering or distribution automation.

In the Cisco Connected Grid FAN architecture, the design recommendation is to use network-layer encryption (AES with IPSec) in the WAN and link-layer encryption in the mesh (AES on IEEE 802.15.4g or IEEE P1901.2). Such a design choice preserves network visibility into the traffic at the FAR and helps enables use of IP-based techniques of multicast, network segmentation, and quality of service (QoS). It also allows the smart meter and other endpoints to be a low-cost constrained node that only does link-layer encryption while the versatile FAR does both network-layer and link-layer encryption.

Network and link-layer encryption can be supplemented by use of application-layer techniques that verify message integrity and proof of origin (digitally signed firmware images or digitally signed commands as part of C12.22 or DLMS/COSEM).

If AMI or DA traffic traverses a public WAN of any kind, it is highly recommended that data be encrypted with standards-based IPSec. This approach is advisable even if the WAN backhaul is a private network. A site-to-site IPSec VPN can be built between the FAR and the WAN aggregation router in the control center. The Cisco Connected Grid solution implements a sophisticated key generation and exchange mechanism for both link-layer and network-layer encryption. This significantly simplifies cryptographic key management and ensures that the hub-and-spoke encryption domain not only scales across thousands of field area routers but also across millions of meters and grid endpoints.

Threat Detection and Mitigation

A simple but powerful network security technique is to logically separate different functional elements that should never be communicating with each other. For example, in the distribution grid, smart meters should not be communicating to DA devices and vice versa. Similarly, traffic originating from field technicians should be logically separated from AMI and DA traffic. The Cisco Connected Grid security architecture supports tools such as VLANs, Virtual Routing & Forwarding (VRFs), or Generic Routing Encapsulation (GRE) to achieve network segmentation. To build on top of that, access lists and firewall features can be configured on field area routers and substation routers respectively, to filter and control access in the distribution and substation part of the grid.

All traffic originating from the FAN is aggregated at the control-center tier and needs to be passed through a high-performance firewall, especially if it has traversed through a public network. This firewall should implement zone-based policies as well as intrusion prevention signatures to detect and mitigate threats. Different applications in the control center tier should be part of a layered design based on stricter restrictions with increasing security levels.

An important aspect of threat detection is the use of syslog and netflow information from network devices. Event logs from firewalls, routers, network management systems (NMS) and head-end systems, meters, and other end-points need to be collected and passed on to a security incident and event manager (SIEM) tool. Such an application can correlate events occurring in different parts of the grid to identify few security incidents, enabling a quicker and more coordinated response.

Device and Platform Integrity

A basic tenet of security design is to ensure that devices, endpoints, and applications cannot be compromised easily and are resistant to cyber attacks. With that goal in mind, the Cisco 1000 Series Connected Grid Routers are built with tamper-resistant mechanical designs. The Cisco 1240 Connected Grid Router (CGR 1240) is an outdoor model that is equipped with a physical lock and key mechanism. This makes it extremely difficult for any rogue entity to open or uninstall the device from the pole-top mounting. Both platforms generate software and NMS alerts if the router door or chassis is opened.

Additionally, each router motherboard is equipped with a dedicated security chip that provides:

- Secure unique device identifier (802.1AR)
- Immutable identity and certifiable cryptography
- Entropy source with true randomization
- Memory protection and image signing and validation
- Tamper-proof secure storage of configuration and data

CGR 1000 images are digitally signed to validate the authenticity and integrity of the software. That software is developed under Cisco Secure Development Lifecycle (CSDL) principles that aim to:

- Identify security threats and mitigations during design with threat modeling
- Use safe Java and C libraries, and Federal Information Processing Standards (FIPS) security library
- Provide a runtime defenses system and execution space protection
- Deploy static analysis tools with appropriate security rules
- Validate the system through security and penetration testing

For AMI deployments using the Cisco Connected Grid architecture, meters also have a tamper-resistant design, generate an alert on tampering, and maintain local audit trails for all sensitive events. Firmware images for meters are digitally signed. Similarly, to help ensure authenticity and integrity of commands delivered from the AMI head-end system (HES) to meters, the commands are digitally signed.

Vulnerability Management

Connected Grid products are backed by the Cisco Product Security Incident Response Team (PSIRT). Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks. This is a dedicated team available 24 hours a day, seven days a week, which manages all customer-sensitive information on a highly confidential basis.

Cisco also publishes security advisories for significant security issues that directly involve Cisco products and require an upgrade, fix, or other customer action. Cisco uses version 2.0 of the Common Vulnerability Scoring System (CVSS) to publish security advisories.

For more details on Cisco security advisories and PSIRT, visit http://www.cisco.com/go/psirt.

Summary

Cisco Connected Grid security solutions provide critical infrastructure-grade security to control access to critical utility assets, monitor the network, mitigate threats, and protect grid facilities. The solutions enhance overall network functionality while simultaneously making security easier and less costly to manage.

For More Information

For more information on the Cisco Connected Grid security solutions for Field Area Networks visit http://www.cisco.com/go/fan

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 C11-696279-00 01/12