E-REDES Secures-Critical Substation Environments with Next-Generation Security from Check Point

E-REDES

Customer Profile

E-REDES is mainland Portugal's energy distribution system operator.

Challenge

- Gain complete visibility into potential threats in substation network traffic
- Segment zones within each substation to separate engineering from critical grid operations traffic
- Detect and prevent threats from affecting either zone

Solution

- Check Point Rugged Security Gateways
- Check Point R80 Security Management

Benefits

- Achieved visibility to see exactly what is happening in traffic across diverse substation environments
- Assured controllability and enforcement through digital twinning of traffic and up-to-the-minute monitoring
- Managed 500 devices with a click through centralized firewall rules and substation profiles

> "With Check Point, we built security capabilities into our most important facilities, in a swift, agnostic way. Our project demonstrates the value of choosing the right partner."
>
> - Nuno Medeiros, CISO, E-REDES

Overview

E-REDES (formerly EDP Distribuição) operates and maintains more than 99% of Portugal's energy distribution power grid. Its critical infrastructure connects more than six million Portuguese customers through 220,000 kilometers of lines, approximately 500 substations, and 60,000 secondary substations. E-REDES has 3,000 employees dedicated to delivering high-quality services.

Business Challenge

Increased Digitalization Demands Heightened Security

In many areas of the world, critical energy infrastructure has been built and implemented over decades. Systems were designed with high resiliency in mind—not security—and systems were protected from operational threats by isolation from other networks. Today, digitalization is introducing new capabilities into these infrastructures. Smart meter, digital twinning, and intelligent power grid technologies promise to increase visibility and control. But they also open the door to heightened cybersecurity risk.

"Security has always focused on our data center infrastructure and mission-critical applications," said Nuno Medeiros, CISO at E-REDES. "Now, we needed to go deeper into the lower levels of our infrastructure—such as substations—to protect our facilities from cyber threats that could enter the network and take down operations."

"It was important to have a local system integrator helping us within these projects"

- Nuno Medeiros, CISO, E-REDES

The E-REDES team knew that it had to protect a large, highly heterogeneous infrastructure. Many existing substations had been built and deployed more than 20 years ago. New substations are planned for the future. It was clear that a one-size-fits-all approach could not succeed. The team began with a comprehensive assessment to identify primary risks at the physical and logical levels of its substations.

The risk assessment revealed three priorities. First, E-REDES needed detailed visibility of all network traffic within substations in order to identify and analyze abnormal behavior. Traffic aberrations could represent anything from a physical device malfunction or threat to employees' safety to a cybersecurity breach. Second, the team had to be able to segment zones at each substation. For example, the engineering zone is a network zone used by employees for remote access to systems. A second zone encompasses operational technologies dedicated to critical power distribution functions. Finally, the team needed security assets that could detect, identify, and prevent threats from affecting either zone.

SOLUTION

Next Step: Next-Gen Firewall

To Medeiros and his team, it was clear that a next-generation firewall was critical to the solution. But could security vendors deliver a solution that was as effective in a hostile, semi-outdoor substation environment as it was in a protected data center? After analysis and discussions with multiple vendors, E-REDES identified Check Point as the best solution for its requirements. The team also evaluated system integrators, looking for a partner up to the challenge of securing power distribution environments and mission-critical operational technologies.

"It was important to have a local system integrator helping us within these projects," said Medeiros. "We chose Warpcom, and they proved to be a flexible, dynamic partner for us and for Check Point."

Warpcom is a leading technology integrator that supports digital transformation initiatives, including cybersecurity and public safety solutions. Together, E-REDES, Check Point, and Warpcom performed a proof of concept, implementing Check Point 1200R Rugged Appliances in three substations—each with a different technology environment. The proof of concept was a success.

The Check Point Rugged Security Gateway delivers Next Generation Threat Prevention for critical infrastructure and industrial control systems. It secures Supervisory Control and Data Acquisition (SCADA) protocols and operational technology (OT) equipment with Firewall, IPS, Application

"With Check Point R80 SmartConsole, SmartView, and SmartEvent, we know exactly what is happening on any substation floor"

- Nuno Medeiros, CISO, E-REDES

Control, Antivirus, and Anti-Bot protection. Robust performance and powerful central management features provide unmatched value in a simple, all-in-one solution.

Gaining Additional Management Benefits

E-REDES initially deployed the rugged gateways in 68 of its most critical substations. Each rugged gateway controls traffic between the engineering control center and operational zones in a substation. Administrators use Check Point R80 Smart Console for integrated security management across all deployments. Check Point R80 Smart Console includes policy, logging, monitoring, event correlation and reporting in a single system, enabling administrators to easily identify security risks across the organization and apply security defenses to all traffic.

Check Point R80 SmartView centralizes viewing through a friendly interface. The E-REDES team can easily configure and monitor network activity and rugged gateway performance. Monitoring and logging data is delivered to the E-REDES Security Operations Center (SOC), where it is analyzed, correlated, and acted on if necessary.

Benefits

Visibility into Potential Threats

Because substation operations traffic is mission-critical, it cannot be jeopardized by any automated remediation actions. If a threat is detected, the SOC team needs immediate visibility. Check Point R80 SmartEvent provides full threat visibility with a single view into security risks. The E-REDES team can see all traffic, with R80 SmartEvent identifying and signaling any threat based on continuously updated signatures. Threat and logging data sent to the SOC is enables the team to quickly manage and respond to a security event.

"In the past, we had limited visibility into the substation networking traffic," said Medeiros. "With Check Point, we can quickly and easily create new rules or add capabilities without needing access to the devices themselves. With Check Point R80 SmartConsole, SmartView, and SmartEvent, we have increased visibility into what is happening on any substation floor."

Assuring Controllability

"Because of the mission-critical nature of substation traffic, we cannot implement security controls on all substation traffic," said Medeiros. "Instead, we mirror traffic, identify potential threats on the 'digital twin,' and apply controls as it leaves the substation and before it joins the main network."

With Check Point R80, the E-REDES team knows if anything suspicious is

"With Check Point, we built security capabilities into our most important facilities in a swift, agnostic way. Our partners not only helped design the project, they brought it to the table and made it happen. Our project demonstrates the value of choosing the right partner."

- Nuno Medeiros, CISO, E-REDES

occurring in substation traffic. They have detailed visibility into all traffic and can now control it—centrally implementing firewall rules and building profiles according to the different substation environments.

"If we want to add a new rule to 50 firewalls, we can do it with a click," said Medeiros. "It's simple. By mirroring the traffic we can secure it and proactively address any threats. Check Point R80 gives us enhanced visibility with controllability in a highly efficient way."

Effectively Mitigating Risk

The substation security initiative has become a flagship project for E-REDES, and the company is deploying the Check Point solution in 200 more substations. With first-time security visibility into all substations, the company gained peace of mind and significantly mitigated risk to mission-critical operations. In the event of a detected threat, the team can respond in seconds to prevent threats from entering critical zones.

"With Check Point, we built security capabilities into our most important facilities in a swift, agnostic way," said Medeiros. "Our partners not only helped design the project, they brought it to the table and made it happen. Our project demonstrates the value of choosing the right partner."