CASE STUDY

A Secure SD-Branch Brings Extended Protection To Industrial Networks

ENGIE is a global energy and services group based on four major activities: client solutions, renewable energy sources, networks, and thermal power generation. Driven by the aim of contributing to harmonious progress, ENGIE is facing up to major global challenges such as combating global warming, access to energy for all, and mobility, and is offering its customers—companies, the tertiary sector, cities, and regions—energy production solutions and services that bridge the gap between individual interests and collective challenges. Low in carbon, its integrated, effective, and sustainable offers rely on digital technology.

ENGIE has been operating in Italy for more than 20 years and is one of the main energy and services operators in the country. With more than 3,800 employees, 60 offices, and various energy plants, ENGIE is present in all segments, from residential to tertiary, public and private, to small and large industries.

Expanding the Network

Following a merger between two companies of the Group in 2015, ENGIE Italia's physical network grew exponentially. Remote sites were already an important asset to the business, but after the integration of the various regional networks, it became a national infrastructure with more than 120 remote branches.

With this growth came some pressing challenges. The existing multiprotocol label switching (MPLS) interconnections were not able to cope with the amount of traffic being routed from branch offices to central sites via the data centers, and the complexities around scaling up the network to accommodate the new branches were prohibitive. In order to keep pace with the amount of traffic between branch sites and the data centers, it was necessary to increase the size of the central MPLS connection, which in turn increased operating costs.

To also meet the redundancy and availability requirements, a parallel MPLS path was needed, increasing costs and management complexity: Those MPLS networks were seen as a technological constraint because every new site needed to be connected on those networks in order to function correctly, increasing time to go live and operational tasks to be managed, since the IT group was not directly in charge of the routing processes of the internet service providers (ISPs).

ENGIE also lacked the ability to have complete visibility over the new branch sites, meaning it could not ensure security of business-critical data transferred across the network or transitioning applications to the cloud. ENGIE therefore tasked Wellcomm

"Fortinet's solutions have reduced our connectivity costs and given us confidence that our network architecture is secure and robust enough to meet the demands of our growing business."

– *Giovanni Vismara, Network Special Projects Coordinator at ENGIE Italia*

Details

Customer: ENGIE

Industry: Energy

Location: Italy

Partner: Wellcomm Engineering S.p.A.

Business Impact

- Increased the security and visibility of branch offices and remote industrial networks
- Reduced geographical connectivity costs through a single MPLS network
- Simplified the hardware ecosystem with SD-Branch, centralized management and automation
- Improved collaboration between IT and OT teams

Engineering S.p.A. with an external evaluation of its IT environment, with the desired result of standardizing the network and security of these remote sites. It also required a network that could handle the shift of services to the cloud, reducing traffic backhauling to the data center in favor of local internet breakouts. These changes would also facilitate better collaboration between its IT and OT teams, which both are in charge of crucial tasks in the remote sites. They can be faster and more efficient, essential in an increasingly connected and centrally managed operational environment.

Solutions

- FortiGate
- FortiSwitch
- FortiAP
- FortiManager
- FortiAnalyzer

Extending Security Over the Network With SD-Branch

To solve those issues and increase the existing level of security and visibility of their remote branches and industrial networks, ENGIE relied on the skills of Wellcomm Engineering S.p.A., who developed the project with ENGIE Infrastructures & Architectures Team leveraging the Fortinet Security Fabric approach.

The FortiGate next-generation firewall (NGFW) was deployed at the central sites of Milan and Rome, at the main data center in Milan, and in the branch offices across other regions. The branch architecture consisted of:

- FortiGate NGFW
- FortiSwitch switches connected to and managed by a local FortiGate in every remote site
- FortiAP access point connected to the FortiSwitches and managed by a central FortiGate cluster in Milan that tunnels applications access through service set identifiers (SSIDs)

Local internet access on remote sites was provided through the FortiGate NGFW, leveraging its integrated software-defined wide-area networking (SD-WAN) capability and giving remote users the ability to directly access trusted cloud resources such as Microsoft 365 and Salesforce.

The Fortinet SD-Branch solution enabled ENGIE to simplify its hardware ecosystem. It also empowered ENGIE to centralize remote management and implement automation through the use of FortiManager and FortiAnalyzer: The Global Policy and address feature became a key component of the streamlined operation tasks and the centralized logging and reporting features of the FortiAnalyzer solution made the troubleshooting and analysis process much more easier and faster.

SD-Branch in Practice

As a result of its new deployment, ENGIE was able to balance traffic flows through the local firewall in the first pilot site in Bari and at both the branch office and call center. With more visibility across the remote branches, ENGIE can now separate out the guest network from its internal IT network, mitigating risk and allowing it to spot suspicious activities in real time. ENGIE was also able to dismantle the secondary MPLS carrier in late 2019 to reduce wide-area network (WAN) costs.

Furthermore, the OT team is also able to leverage the IT infrastructure, gaining more insights than ever before. Previously they had to configure a separate set of dedicated equipment, but by collaborating with the IT team, productivity has drastically improved. The teams are now able to identify devices on the network much faster and troubleshoot issues in seconds thanks to the perspective FortiManager/FortiAnalyzer has given them.

ENGIE realized that it was spending a lot of money on its WAN, and came up with a solution to remedy that. Information sharing and collaboration across the IT and OT teams has resulted in quicker response times to incoming threats and a seamless approach to network security across the branches in Italy and abroad.

September 24, 2020 3:07 PM

704050-0-0-EN

Sheldon:Fortinet:2020-06-704050-CS-Engie:cs-704050-Engie-red-A4-EN