SCADAfence and Barracuda CloudGen Firewall automate security for OT Networks

The joint solution provides visibility, detection, and automated incidence response to enforce security levels across OT and critical infrastructure networks.

Challenge

The digital transformation of industrial control system (ICS) environments, which include an extended adoption of advanced technologies and connection to regular IT networks, has led to new security challenges due to the lack of air gapping. The rising connectivity between manufacturing plants, critical infrastructure facilities, and smart buildings, and their corresponding external environments has exposed critical operational technology (OT) networks to a threat landscape ranging from targeted attacks to generic ransomware.
To ensure proper security control and risk management, organizations are deploying dedicated security solutions either within the OT network and on the perimeter between IT and OT, or between the internet and OT. SCADAfence and Barracuda Networks have joined forces to combine leading monitoring, segmentation, and secure remote access solutions so ICS owners can have the peace of mind that they are protected in the new digital era.

Joint Solution Overview

The SCADAfence Platform continuously monitors internal OT network traffic and, by analyzing the proprietary industrial protocols, specializes in asset discovery and inventory, vulnerability management, and threat detection. Combing SCADAfence's understanding of the internal OT network activities with Barracuda's CloudGen Firewall network protection and threat mitigation capabilities extends visibility and security enforcement capabilities from standard IT to specialized networks driving today's operational technology. Barracuda CloudGen Firewall products leverage the accurate data coming from the SCADAfence Platform to automate protection for each OT segment.

This improves policy enforcement, automatically remediates security violations, and increases overall network resilience.

Key Benefits:

- Add internal OT security and visibility to the existing IT security controls
- Combine OT threat detection with automatic enforcement capabilities to improve incident response
- Increase network resilience by ensuring proper enforcement of security policies
- Monitor remote access activities and ensure that only authorized changes are performed
- Block unwanted protocol usage
- Block unauthorized access

Flexible Staged Deployment Options

Secure connection between IT and OT

The Barracuda CloudGen Firewall is implemented between the IT network and the OT network and between the OT network and the internet. The SCADAfence Platform monitors the internal network communication and provides the CloudGen Firewall with detailed information on the industrial assets, alerts on anomalous network behavior, and warnings of risks and vulnerabilities. Once SCADAfence detects an anomaly, the Barracuda CloudGen Firewall automatically blocks the respective malicious source at the OT network ingress point.

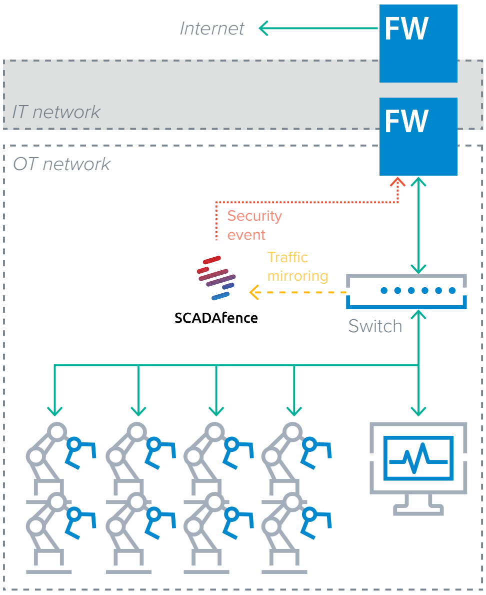

Figure 1 - Flexible Staged Deployment Options

Key Benefits:

- Most cost-effective integration: easy and quick to deploy
- Real-time network visibility
- Automated detection and response
- Does not affect critical internal network communications

OT network micro-segmentation

In this scenario, in addition to securing the outbound communications, the Barracuda CloudGen Firewall is also implemented in the internal OT network to create micro-segmentation between different zones. In this use case, OT production areas are divided into zones to create small network segments. Each segment has a designated purpose, and access between the segments is limited or blocked. Micro-segmentation in OT networks limits the potential damage caused by malicious attacks and non-malicious human errors. By leveraging SCADAfence's internal OT network visibility and asset management, the Barracuda CloudGen Firewall can be easily configured to limit communications between different zones based on actual network traffic analysis.

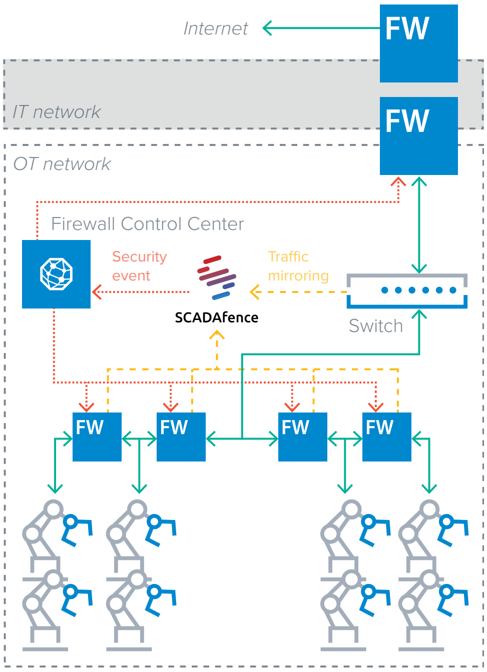

Figure 2 - OT network micro-segmentation

Key Benefits:

- Block internal OT network attack vectors
- Reduce attack surface by containing threats
- Improve network management and decrease errors

Virtual patching & OT device-specific security

Adding CloudGen Firewall units to protect specific OT devices allows administrators to enforce specific security policies for sensitive or vulnerable devices. This use case is especially powerful when there are specific devices that are more critical for the process and, therefore, require increased security control. In addition, if there are legacy devices with known vulnerabilities that are unpatchable, placing a firewall adjacent to them allows you to block unwanted communications and to significantly reduce the potential attack surface. The combination of SCADAfence and Barracuda enables you to identify the most critical or vulnerable devices according to their network activities and vulnerabilities. Once these devices are identified, the firewalls can be properly configured based on their actual role in the environment.

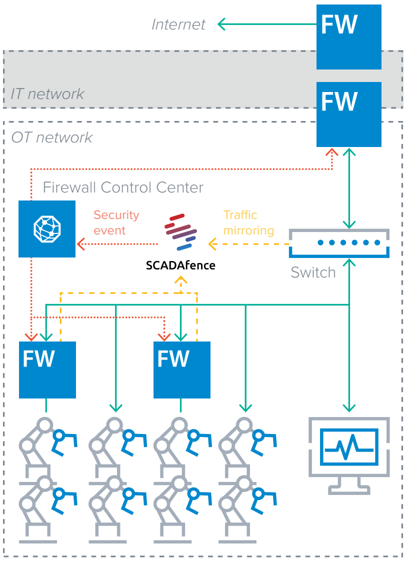

Figure 3 - Virtual patching & OT device-specific security

Key Benefits:

- Most secure coverage
- Capability of adding extra security for specific OT devices
- Securing vulnerable legacy devices

Barracuda
Your journey, secured.

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-enabled, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 150,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level.

For additional information, please visit www.barracuda.com.

Barracuda
Your journey, secured.

Bridged segmentation for every OT entity

Barracuda CloudGen Firewall devices are implemented between the IT network and the OT network. In addition, a rugged version protects every entity of the OT network in bridge mode. Every CloudGen Firewall is centrally managed by the Firewall Control Center. The SCADAfence Platform monitors the internal network communication and provides the Firewall Control Center with detailed information on the industrial assets, alerts on anomalous network behavior, and warnings of risks and vulnerabilities. Once SCADAfence detects an anomaly, it automatically notifies the Firewall Control Center. The Firewall Control Center automatically distributes the information to all deployed CloudGen Firewall instances, and the CloudGen Firewalls automatically block the respective malicious source.

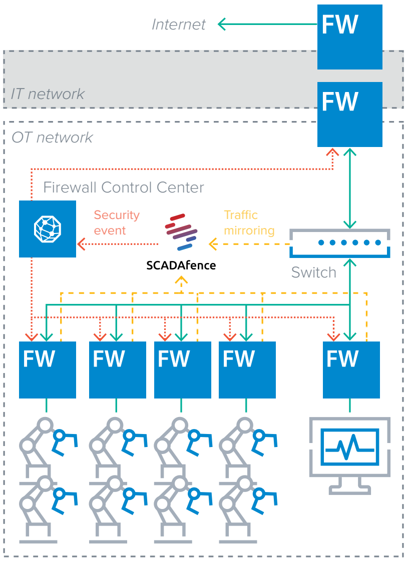

Figure 4 - Bridged segmentation for every OT entity

Key Benefits:

- Bridged connectivity unless a threat is detected
- Contains rogue or newly compromised OT devices
- Capability of adding extra security for specific OT devices
- Securing vulnerable legacy devices

SCADAfence

SCADAfence helps companies with large-scale operational technology (OT) networks embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. Our non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery, and user experience. SCADAfence seamlessly integrates OT security within existing security operations, bridging the IT/OT convergence gap. We deliver security and visibility for some of the world's most complex OT networks, including Europe's largest manufacturing facility. Thanks to SCADAfence, companies in manufacturing, building management, and critical infrastructure industries can operate securely, reliably, and efficiently as they go through the digital transformation journey.

For additional information, please visit www.scadafence.com.

SOLUTION BRIEF • UK 1.0 • Copyright 2018 Barracuda Networks, Inc. • barracuda.com