SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Technical Whitepaper

Simplifying Network Segmentation with SCADAfence

OT Network Segmentation Challenges

In the not-so-distant past, protecting mission-critical systems from external threats was mainly accomplished by means of "air-gapping" – that is, taking systems off the communications grid in order to prevent any interactions with other networks and the Internet.

Today, in the midst of the 4th industrial revolution, increased levels of connectivity are required to empower enterprises and to keep them competitive, making air-gapping completely irrelevant.

This trend towards increased connectivity exposes OT networks - making them vulnerable to an array of new attack vectors. In order to mitigate these risks, organizations are applying firewall technologies to implement network segmentation.

Segmentation in busy internal OT networks, differs from typical IT perimeter protection methods. The range and complexity of connections is much higher in OT networks, and the criticality of the production processes is much higher than daily office traffic crossing the organization perimeter. Especially when a large number of firewalls are deployed and micro-segmentation is targeted.

Although segmentation, when properly done, increases an OT networks' security posture, there are still major challenges and possible weaknesses that should be taken into consideration in order to make this investment effective.

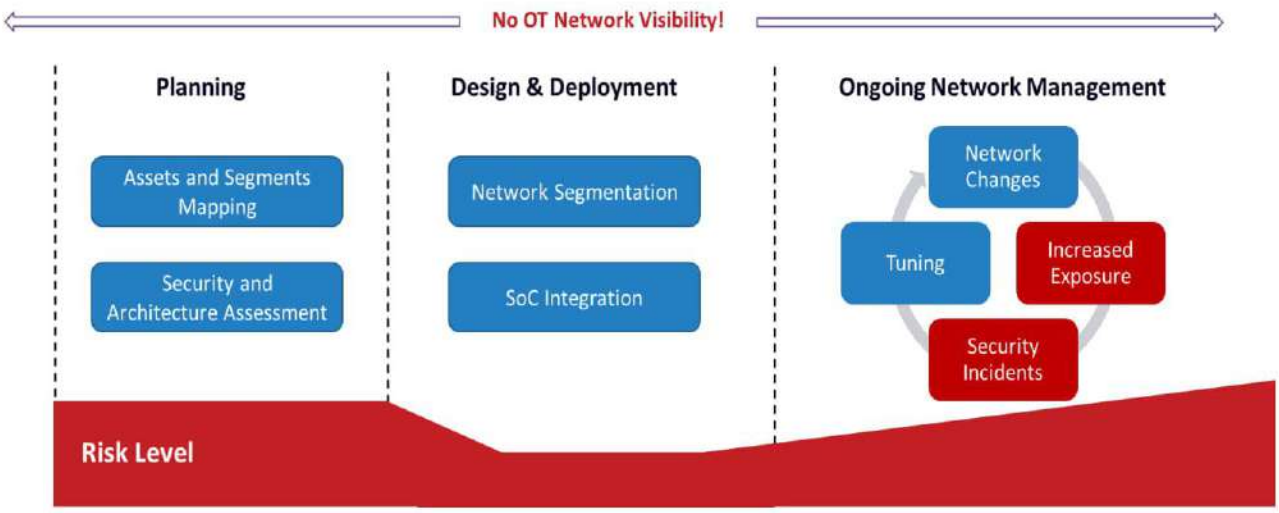

Diagram 1: Network Segmentation Without Proper Visibility and OT Process Correlation

These challenges mostly occur due to the lack of network visibility, reliance on manual processes and the lack of correlation of network devices to the OT processes running over the network.

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

MUNCHEN, Schellingstr. 109a80798 Munchen Germany +49-322-2109-7564

Contact: info@scadafence.com

The Challenges During the Deployment Process

- **High Risk Due to Lack of Visibility.** Segmentation projects typically take several months and even more. These projects typically include analysis, planning and deployment. During this time, the OT network does not have visibility and does not have proper security in place. In today's dynamic environment, this is a very long time that the network is exposed and can allow critical security incidents to occur.
- **Ineffective Deployment.** When deploying firewalls in internal busy networks, the firewalls do not "see" all of the dangerous traffic. Remote connections or rogue devices may exist and bypass the firewall, without appearing in the firewall logs. Sometimes, the deployment location is not chosen properly as a different network junction might be much more effective. These scenarios can give the security staff a false sense of security while lacking the required level of protection.
- **Lack of Correlation to the Business Process.** Firewalls do not correlate between the IP address that they see and the OT process roles of the devices. In internal networks, with many IPs and many types of application traffic, this can cause a lot of manual (and lengthy) work in understanding the traffic patterns. This lack of correlation can cause critical processes to be accidentally blocked, or on the other hand to open unnecessary ports and over-expose the network.

  This makes the investment in segmentation technologies ineffective, and eventually maintains the high-risk level.

Benefits Summary

- Effective segmentation, maximizing the return on investment (ROI).
- Coverage of additional non-firewall attack vectors, providing a holistic solution.
- Tight correlation & minimum interference with OT processes.
- Full visibility and risk reduction from day-1, and not having blind spots for long periods of time.
- Control the dynamic deterioration effect after the deployment phase, and reduce the risk of critical incidents.
- Monitor application traffic that is not segmented by firewalls.

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

MUNCHEN, Schellingstr. 109a80798 Munchen Germany +49-322-2109-7564

Contact: info@scadafence.com

The Challenges After the Deployment Process

- **Deterioration Over Time.** Network segmentation "deteriorates" over time, due to network changes, policy violations and human error. New systems are added to the network, and existing configurations and policies dynamically evolve, creating "holes" in the security policy.

  This means that the risk level that has been lowered by the segmentation project, rises back immediately on the first day after the firewall deployment ends.

  Going unnoticed, this deterioration poses high risk for severe security incidents.

- **Attack Vectors Bypassing the Perimeter.** Changes are often knowingly made to the network's infrastructure in order to bypass perimeter security. Backdoors are created for IT/OT or external vendors' staff members, thus leaving an opening for new attacks. New connections to/from the Internet can be established in an uncontrolled and unauthorized manner. Internal users, USB devices, wireless access, and malware infections over e-mail, are just some examples of attack vectors threatening the network.

  OT networks must be monitored by means additional to firewalls in order to keep the OT networks secure.

- **Application and Management Systems.** On the application level, the network is often viewed as "flat". Systems such as manufacturing execution systems (MESs) and domain controllers have access to all of the subnetworks in the organization, and are *not* protected by segmentation.

Continuous Monitoring & Automated Asset Discovery Addresses Network Segmentation Challenges

The SCADAfence Platform offers continuous network monitoring and automated asset discovery. It provides an extra layer of cyber defense that helps solve the aforementioned challenges and completes the security architecture.

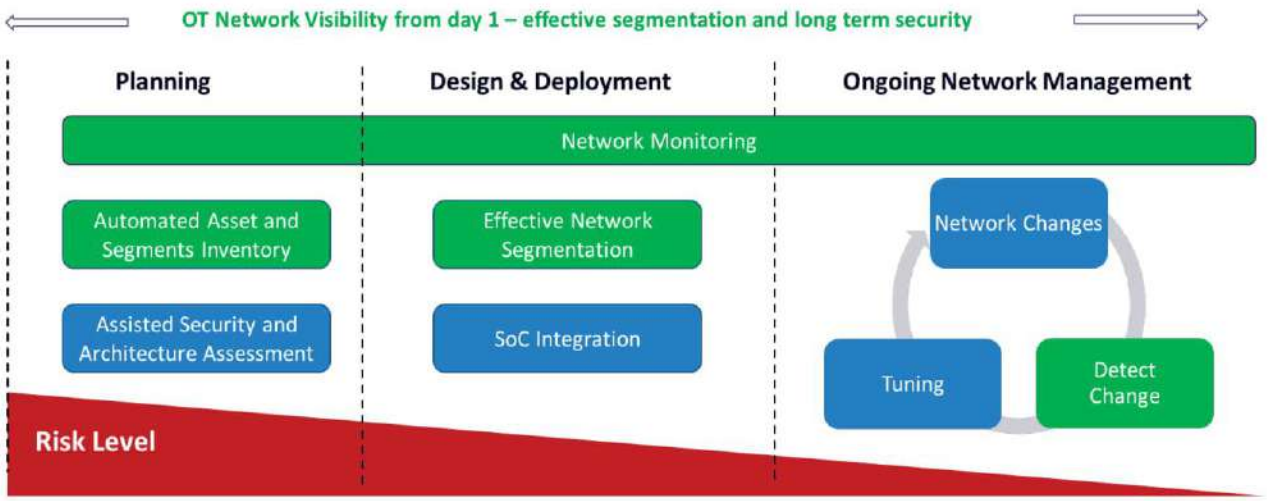

Diagram 2: Effective Segmentation and Long-Term Security

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

MUNCHEN, Schellingstr. 109a80798 Munchen Germany +49-322-2109-7564

Contact: info@scadafence.com

Addressing the Challenges During the Segmentation Project

- **Visualization of Traffic Between Segments.** The SCADAfence Platform provides a "Segments Map" that maps all network segments, and an "Exposure Map" that shows the traffic patterns between logical groups and different network parts. Additional automated traffic analysis views, provide insights into user and application behavior - as well as their requirements. This way, if any traffic attempts to bypass the perimeter / network, it gets detected instantly.

  This also ensures that all of the relevant network traffic is detected and the segmentation process is done effectively.

- **Automated Asset Inventory and Correlation to the OT Process.** The SCADAfence Platform discovers and maps all of the assets in the network, including their roles and their applicative activities using native industrial protocols. This makes the segmentation rules much more accurate and effective in internal OT networks - which have many assets, communication directions and critical industrial applications.

- **Automated Risk Assessment Report.** The SCADAfence Platform serves as a risk analysis tool and is used to identify critical communication patterns and detects security issues. It discovers exposures and vulnerabilities, allows mapping potential attack vectors, and helps to define security requirements based on real data - not by a manual investigation. Finally, a detailed report of findings and remedial recommendations is presented to the network administrator. This helps to ensure that the segmentation process addresses the critical network risks and does not oversee major security issues.

- **Reducing the Risk from Day One** – By monitoring the network, providing full visibility and alerting on any abnormal activities or deviations from policies, the SCADAfence Platform reduces risk immediately. Moreover, risk reduction is not postponed for months until all the security mechanisms are in place, ensuring that the network is not exposed to security incidents.

Keeping the Network Clean and Secure After the Deployment:

- **Detect Changes and Prevent Security Incidents.** Networks are dynamic: assets are being added, firewall rules can change to allow insecure actions, and remote connections are configured. Not all of these can be detected simply by segmentation technologies. The SCADAfence Platform offers a clear picture of the security health of the network, and provides alert notifications on any changes or deviation from the policy.

  Tuning can be made before the next security incident occurs, and not after. Monitoring also reduces the risk of cyber-attacks and malware infections, and it also minimizes the time required to handle potential incidents.

- **Eliminating Backdoors and Attack Vectors Bypassing the Firewall**. The SCADAfence Platform quickly discovers newly created connections and assets, even if they are not seen by segmentation gateways. This prevents bypassing the firewall and other backdoors before they can be penetrated by malicious actors.

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

MUNCHEN, Schellingstr. 109a80798 Munchen Germany +49-322-2109-7564

Contact: info@scadafence.com

- **Securing Unsegmented Systems.** The unsegmented management applications mentioned earlier are continuously monitored for anomalous activities, similar to systems that are unprotected by firewalls.

How to Use the SCADAfence Platform in a Network Segmentation Project

The SCADAfence Platform is used for segmentation project planning, which reduces both the length of the project and the cost, and also results in a tighter segmentation solution.

Follow these following steps for successful segmentation:

- Connect the system to the network to allow the network traffic to be analyzed – the asset inventory and network connectivity maps will be automatically populated.
- Use the Subnet Topology Map to see which subnets are currently in use. Make sure that you're aware of all the subnets.
- Use the Exposure map and drill down to the connection level between groups to understand the traffic between applications, OT processes, and sites.
- Use the automated asset inventory created (including the automatically detected device roles) to correlate between the OT process and the network traffic and quickly understand the communications nature.
- Use the Threat Assessment view, the exposure map and the security report to perform an automated risk assessment.
- Utilize the exposure map and the built-in alerts on internet connectivity to detect outbound connections. You should verify:

    A. If these are authorized connections.

    B. If they are bypassing the perimeter/firewall junctions.

Use the network map to identify connectivity between subnets. Subnets that don't require communication between them should be separated as part of the segmentation project.

- For each subnet, decide which subnets it should be able to communicate with. Try to limit connectivity as much as possible, and if you allow connectivity – try to limit what you allow.
- Use the result of the process as the guideline for your segmentation.
- After the segmentation project, use the same method to make sure that the segmentation has been successful and that the protection level is maintained over time.
- After the segmentation project, use the system's alerts of abnormal traffic, new devices and new connections to detect any deterioration in the security posture, and prevent

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cyber security. The SCADAfence platform enables organizations with complex OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and governance with minimal false-positives. SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in manufacturing, building management and critical infrastructure industries to operate securely, reliably and efficiently. To learn more, go to www.scadafence.com

NEW YORK, 462 W Broadway New York, NY 10012, ABD +1-646-475-2173

TOKYO, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Tokyo 103-0023, Japan +81-3-4588-5432

MUNCHEN, Schellingstr. 109a80798 Munchen Germany +49-322-2109-7564

Contact: info@scadafence.com