SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

SCADAfence Platform

How SCADAfence Platform Makes Network Segmentation Efficient and Effective

Introduction

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

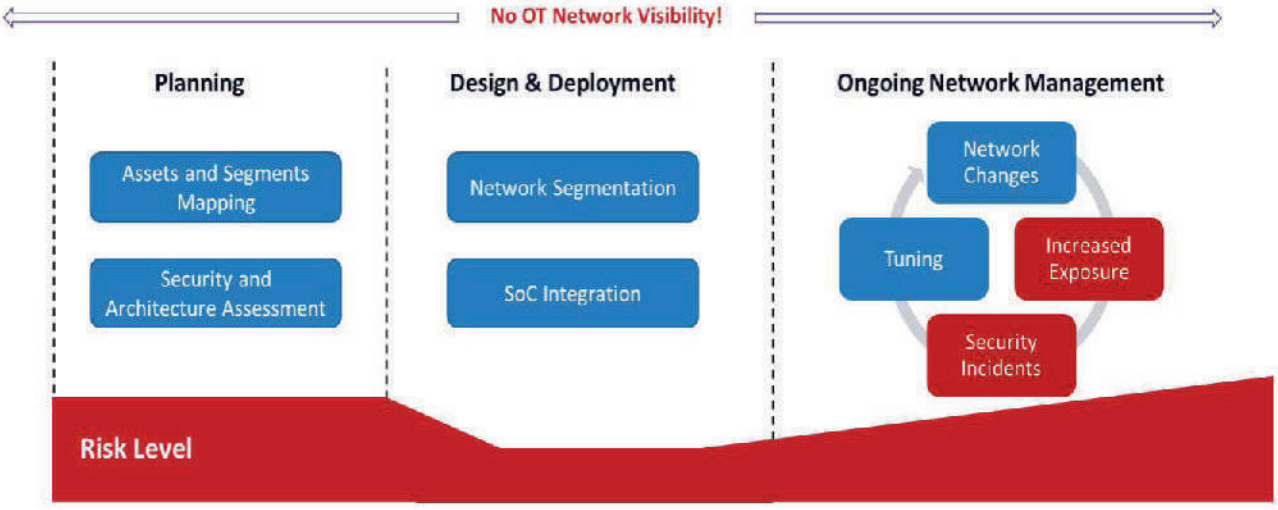
Today, in the midst of the 4th industrial revolution, increasing levels of connectivity are required to empower enterprises and keep them competitive, making air-gapping completely irrelevant.

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

Challenges of OT Network Segmentation Projects

Segmentation in busy internal OT networks, differs from typical IT Perimeter protection. The range and complexity of connections is much higher, 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 is deployed, and when micro-segmentation is targeted.

Therefore, although segmentation when properly done, increases the OT network security, there are still major challenges and possible weaknesses that should be taken into consideration to make this investment an effective one.



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

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

Challenges during the planning and deployment phase:

- **High Risk due to Lack of visibility**. Segmentation projects typically take several months and even more – of analysis, planning and deployment. During this time, the network remains without visibility and without proper security in place. In today's dynamic environment, this means a very long time for critical security incidents to occur.
- **Ineffective Deployment.** When deploying firewalls in internal busy networks, they might not "see" all the dangerous traffic. Remote connections or rogue devices might exist and bypass the firewall, without visibility in the firewall logs. Sometimes, the location itself is not chosen properly as a different network junction might be much more effective to segregate. In these cases, the security staff might have 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 they see and the role of the device. 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, blocking and interfering with critical industrial processes by mistake - or on the other hand - opening a lot of unnecessary ports in the firewall putting in risk the industrial network.

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

Challenges during the on-going management phase:

- **Deterioration over time.** Network segmentation "dissolves" with 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 is raising back immediately starting in 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 infrastructure in order to bypass perimeter security. Back doors are created for IT, OT or external vendors, thus leaving risky openings. New connections to/from the Internet can be established in an uncontrolled manner. Internal users, USB devices, wireless access, malware infection over e-mail, are just additional examples of attack vectors threatening the network.

  Therefore, OT networks have to be monitored by other means other than the firewall to keep the network secure.
- **Application and Management Systems.** On the application level the network is often viewed as "flat". Systems such as domain controllers or Manufacturing Execution Systems (MESs) have access to all the subnetworks in the organization, and are *not* protected by segmentation.

How Continuous Monitoring and Automated Asset Discovery Addresses the 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 challenges described above and completes the security architecture.

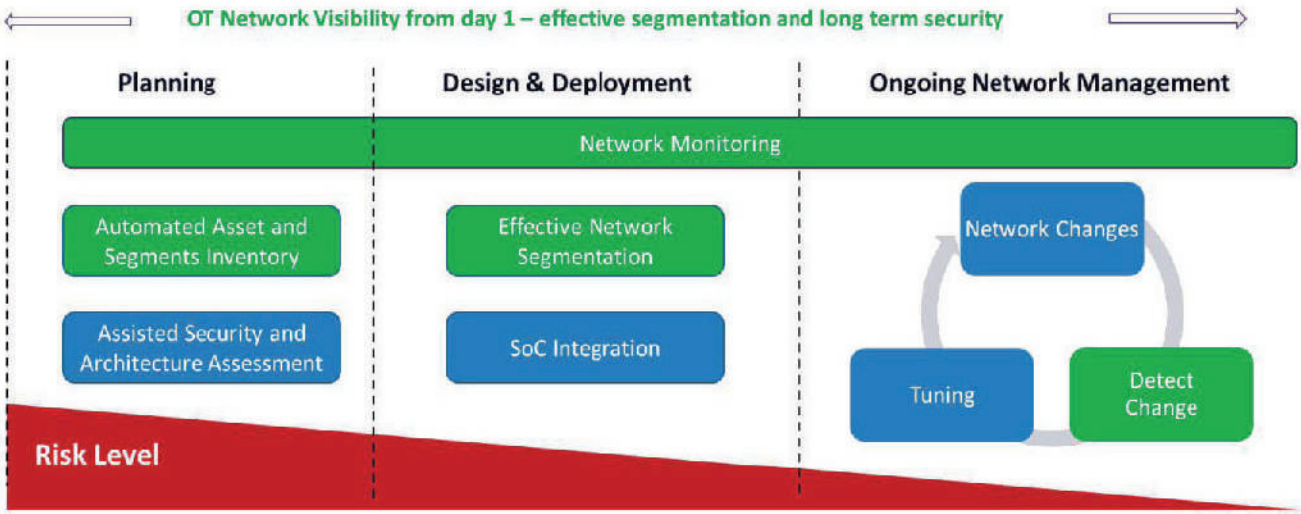


Diagram #2: Effective network segmentation with continuous monitoring and asset discovery

Addressing the challenges during the planning and deployment phases:

- **Analyzing traffic patterns between segments.** The SCADAfence Platform provides a "Segments Map" that maps all network segments, and an "Exposure Map" that shows the connections between logical groups and between different network parts, and alerts on abnormal or risky traffic. Additional automated traffic analysis views provide insight into user and application behavior and requirements, and avoids missing traffic that is bypassing the firewall.

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

- **Automated asset inventory and correlation to the OT process.** Discovers and maps all the assets in the network, including their roles and their applicative activities using native industrial protocols. This makes the segmentation rules much more precise and effective in internal OT networks, which have many assets, communication directions and critical industrial applications.

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

- **Reducing the risk from day 1** – by monitoring the network, having visibility and getting alerts on any abnormal activity or deviation from policies, immediate risk reduction is received, and this is not postponed for months till all the security mechanisms are in place, leaving the network open for security incidents.

Keeping the network clean and secure during the on-going management phase:

- **Detect changes and prevent security incidents.** Networks are dynamic: assets are being added, firewall rules may change to allow insecure actions, remote connections are configured and not all are being detected by the segmentation tool. The monitoring solution offers a clear picture of the network connectivity, and provides alert notifications on any changes or deterioration from the policy.

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

- **Elimination of back doors and attack vendors bypassing the firewall**. 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 back doors before they can be penetrated by malicious actors.

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

Benefits Summary:

- Effective segmentation maximizing the benefit of the investment
- Cover the additional, non-firewall attack vectors, providing a holistic solution
- Tight correlation and minimum interference with the OT processes
- Obtain visibility and reduce Risk Level from Day 1, instead of keeping the blind spots
- Controlling the dynamic deterioration effect after the deployment phase, and reducing risk for critical incidents
- Monitoring traffic of applications that are not segmented by the firewall

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

Steps to use the SCADAfence Platform in a Network Segmentation Project

As mentioned, the SCADAfence Platform is used for segmentation project planning, which both reduces the length of the project and therefore the cost, and also resulting in a tighter segmentation solution.

Follow the following steps as part of a segmentation project:

- 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 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 (including the automatically detected device roles) to correlate between the OT process and the network traffic and quickly understand communication nature.
- Use the Threat Assessment view, the Exposure Map and the Security Reports to perform a security risk assessment, based on real network traffic.
- Utilize the Exposure Map and the built-in alerts on Internet connectivity to detect outbound connections. Examine: A. if these are authorized connections. B. Detect connections that are bypassing perimeter/firewall junctions.
- Use the Network an Exposure Maps to identify connectivity between subnets. Subnets that don't require communication between them should be separated into different segments.
- Finally, for each subnet, decide which subnets it should be communicating with. Try to limit connectivity as much as possible, and if you allow connectivity – limit what is allowed.
- Use the result of the process as the guideline for segmentation.
- After the deployment phase, use the same method to make sure that the segmentation has been successful and that the protection level is kept improved.
- After the deployment phase, keep using the system's alerts of abnormal traffic, new devices and new connections to detect any deterioration in the security posture, and prevent security incidents.

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