Network Perimeter Defense

Best Practices in Network Segmentation

November 2014

EnergySec
8440 SE Sunnybrook Blvd., Suite 206
Clackamas, OR 97015
877-267-4732
energysec.org

This material is provided for general information purposes only. You should make your own judgment as regards use of this material and seek independent professional advice no your particular circumstances. Neither the publisher, nor the author, nor any contributors assume any liability to anyone for any loss or damage caused by any error or omission in the work, whether such error or omission is the result of negligence or any other cause.

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/4.0/.

© 2014 Energy Sector Security Consortium, Inc.

Executive Summary

Network segmentation is one of the best ways to protect your network and data.

Appropriate network segmentation is one of the key ways to protect a network. When network segmentation is used, traffic is not able to freely move between computers or devices on separate segments. This provides several benefits to the overall security of a network. First, if a device is compromised, the number of other devices or computers it can easily communicate with is limited. This can help prevent the malware or attacker from accessing other devices. Network segmentation can also limit the scope of compliance requirements, resulting in reduced costs of compliance to go along with a more secure network. Network segmentation can also be used to indirectly manage logging. Sensitive information can be segregated to high-level subnets, and then those subnets can be monitored more thoroughly.[1] In addition to the security benefits, using network segmentation can assist in lowering the bandwidth and processing power required for devices and networks since it limits the size of broadcast domains.

This paper will examine different ideas for how to effectively segment networks. It will examine the Zero Trust Model, which is based on the idea that it is no longer adequate to assume a network has a “trusted inside” and “untrusted outside.” It then examines a couple different models for how to segment a control systems network using a DMZ or the Purdue Model. The paper finishes with looking at how effective network segmentation helps lead to compliance with the NERC CIP requirements.

Zero Trust Approach

Never Trust, Always Verify.

The traditional approach to network segmentation is based on trust levels. The inside network is considered trusted and the outside network (Internet) is untrusted. Communications between devices inside the same trust-level would be allowed, while communications from outside networks are not trusted. Along with the idea of trust levels, any information which flows over a network with a lower trust level should use encryption to protect the data.

As an alternative to the traditional approach, Forrester Research first introduced the Zero Trust Model.[2] They took the approach that the idea of trusted and untrusted networks does not work. Partially due to the threat of the malicious insider, it is no longer adequate to assume that the internal network consists of safe traffic, while the external network is unsafe traffic. Instead, the Zero Trust Model takes the approach of “never trust, always verify.” Even if your network design doesn’t completely implement the Zero Trust Model as envisioned by Forrester Research, the idea of the model can be useful and lead to the use of defenses such as application and protocol whitelists rather than the use of blacklists for security.

© 2014 Energy Sector Security Consortium, Inc.

IT/OT Boundary

SCADA systems should be separate from the IT network, and should not be connected to the public Internet under normal operations. It should be documented where the SCADA networks connect to other networks, including connections to local and wide area networks, the Internet, wireless devices, satellite uplinks, modems, and connections to business partners or vendors.[3] The only way to successfully manage the connections between a SCADA network and other networks is if you know where those connections are. Once these connections are known, furthermore, you will be able to disconnect any unnecessary connections to the SCADA networks.

To configure the gateway device on the IT/OT boundary, you will need to inventory what services or information will have to cross the boundary. Then, the gateway device can be configured to only allow the applications and protocols which are required for those particular services.

A control room should be segmented from the enterprise network.

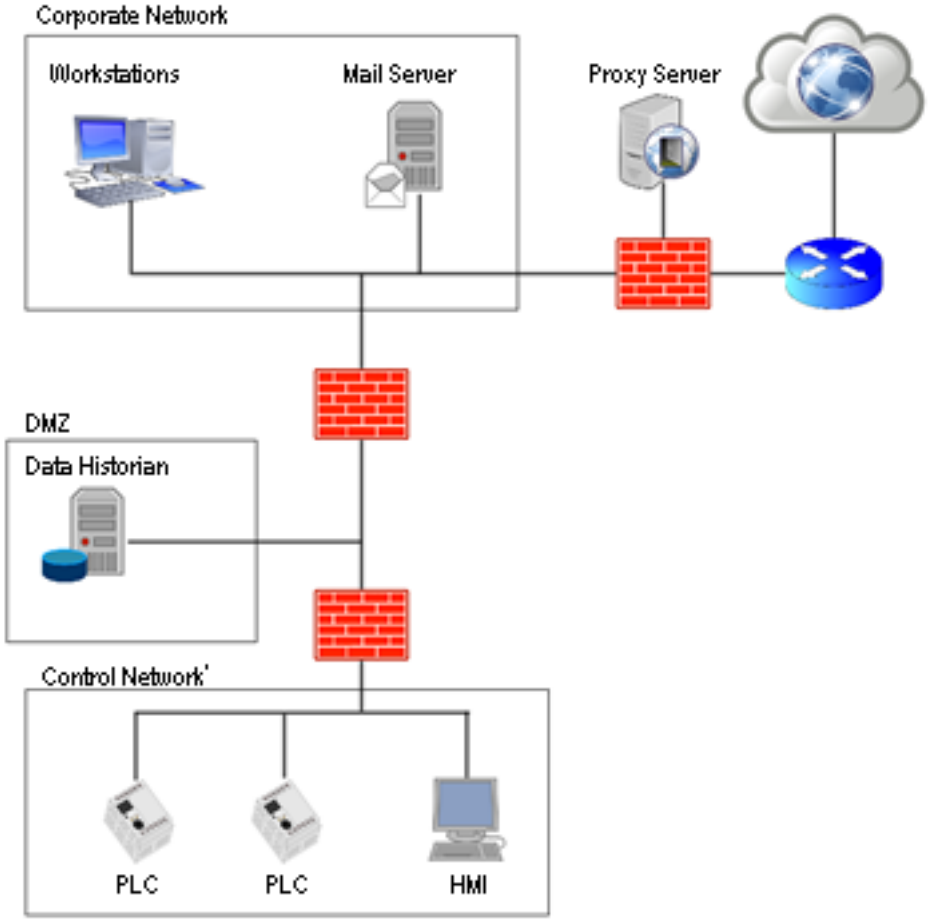
© 2014 Energy Sector Security Consortium, Inc.

Network Architectures for Segmentation

In segmenting networks, a traditional three-tier approach separates out the Information Technology (IT) network, the corporate network, and the Operations (OT) network. This approach should be expanded to include more granular controls. For example, human-machine interfaces (HMIs) could be considered as their own tier, as well as SCADA devices being on their own network segment.

As part of designing the network perimeter, a demilitarized zone (DMZ) should be implemented, so that access to the corporate network is not allowed from machines outside of the network. The outside machines should only be able to access the DMZ. The DMZ should not contain sensitive data, but rather should communicate with private network systems through an application proxy or application-aware firewall. The network perimeters should be designed so that all outgoing web, FTP, and SSH traffic to the Internet must pass through at least one proxy on a DMZ.

Control Network Segmented From A Corporate Network



© 2014 Energy Sector Security Consortium, Inc.

Purdue Model

One way this can be implemented is through the Purdue Model for Control Hierarchy. The Purdue Model has long been used in industry, and is incorporated into standards such as ISA-99[4] and IEC 62443.[5] It identifies levels of operations and is used to segment a network into zones.

Level 0

The physical processes which are monitored or controlled. For example, a temperature sensor would be a level 0 device.

Level 1

Intelligent devices which manipulate the physical processes. An example of a level 1 device would be a programmable logic controller (PLC).

Level 2

Level 2 is provides supervisory control of the controllers. Devices on this level would be the Human-Machine Interface (HMI) devices and SCADA software.

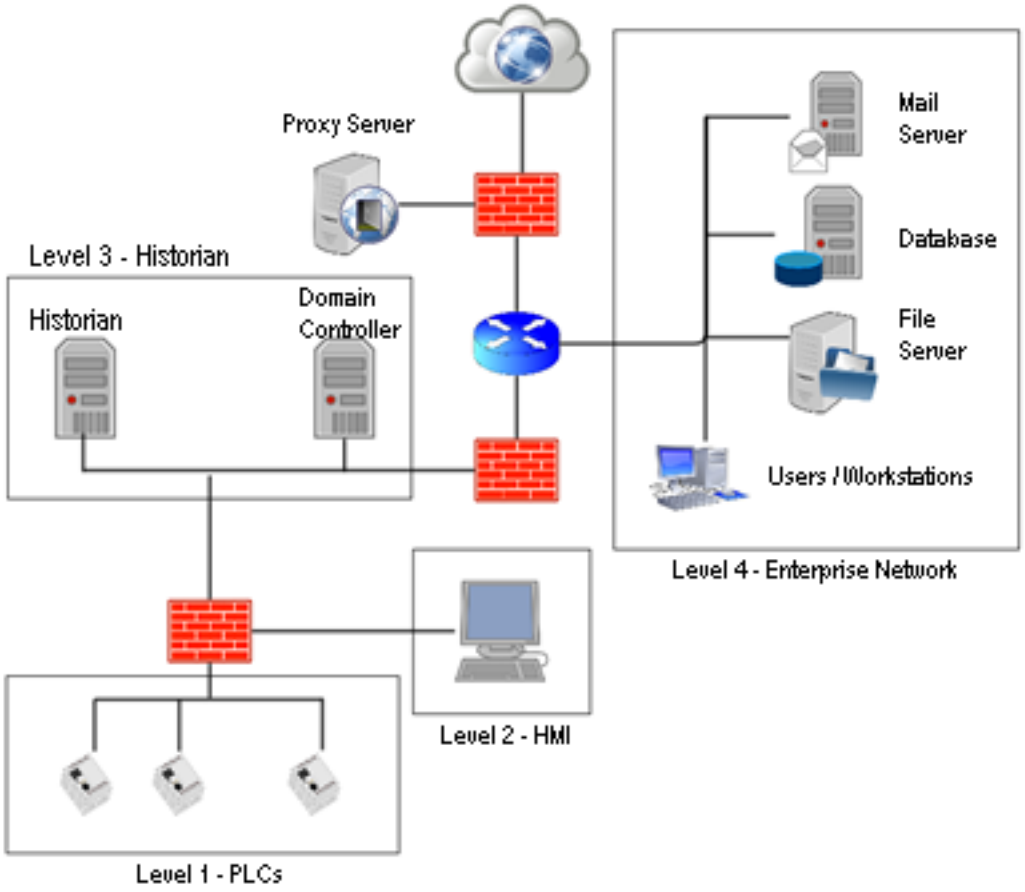
Level 3

Devices at the level 3 layer are for managing operations systems. An example is a data historian, which is used to collect and preserve information from devices at lower levels.

Level 4

Level 4 devices are used at the enterprise level, also commonly referred to as the Information Technology side of an organization. For example, email servers and end users would be at this level.

Example Network Diagram Using Purdue Model



© 2014 Energy Sector Security Consortium, Inc.

When designing a network, the Purdue Model allows us to control access to the SCADA controls. In general, level 2 devices are able to set or change values on level 1 devices. Level 3, however, is only able to read values from either level 1 or 2 devices. Then, combined with access controls such as firewalls between layers, segmentation can be used to help protect the ICS devices in the field or plant.

NERC CIP: Electronic Security Perimeters

Effective network segmentation leads to compliance with NERC CIP standards.

The NERC CIP-005-5 standard says that all Cyber Assets that are connected to a network via a routable protocol shall reside within a defined Electronic Security Perimeter (ESP) and the connection to the network must be through an Electronic Access Point (EAP). The standard also requires the use of an Intermediate Device to broker remote interactive access to an ESP. The regulations require the Intermediate Device to be outside the ESP, but it should also be situated in a DMZ.

Effective segmentation of a network will lead to compliance with the NERC CIP standards. The devices at the gateway of the network segment will be the EAP for that network. This is an example of good security leading to compliance with standards, which can often lead to better outcomes than a purely compliance-based approach.

Conclusion

Effective network segmentation is one of the best ways to protect your organization. By segmenting the networks, an attacker who gains access to a device on your network may still be blocked from being able to achieve his objectives or accessing more critical devices.

EnergySec
8440 SE Sunnybrook Blvd., Suite 206
Clackamas, OR 97015
877-267-4732
energysec.org

© 2014 Energy Sector Security Consortium, Inc.

[1] "Detecting and Deterring Data Exfiltration: Guide for Implementers," MWR Infosecurity, Feb. 2014.

[2] Kindervag, John. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. The Security Architecture and Operations Playbook. Forrester Research, Inc., November 15, 2012.

[3] U.S. Department of Energy, Infrastructure Security and Energy Restoration Committee, "21 Steps to Improve Cyber Security of SCADA Networks". 1-Jan-2007.

[4] http://isa99.isa.org/ISA99%20Wiki/Home.aspx

[5] https://www.isa.org/store/products/product-detail/?productId=116720

© 2014 Energy Sector Security Consortium, Inc.