Global Instrumentation and Control

Network Architecture and Cyber Security: Network Architecture

Background

Businesses, utilities, and people around the world use technology on a daily basis that requires the use of a data network. These networks have requirements and are designed to be as efficient, reliable, and secure as possible.

The scope of Network Architecture & Cyber Security includes the design of the physical and logical communications network. During the duration of work, the objective is to provide a network that meets the required reliability and security goals. This involves network device configuration, firewall implementation, use of unidirectional gateways, and defense in depth tactics.

Why Is This Important

A poorly designed network architecture leads to frustrations and problems, both operational and financial. The operational problems range from but are not limited to delayed traffic transmission, complete loss of data transmission, network loops, and lack of security. Some of the financial impacts associated with a poorly designed network involve time lost, and stolen information.

Westinghouse understands the consequences and is fully dedicated to mitigate these situations.

Description

The Westinghouse Network Architecture team has a primary focus involving the secure development and assessment of new and existing network topologies. The program analyzes all details including geographic location of devices, types of devices, security zones, IP scheme, and network vulnerability among many other variables. Westinghouse team members are qualified and committed to meet the requirements listed in 10 CFR 73.54.

Deliverables

The following are the services most directly involved with Network Architecture and will immediately improve network integrity.

Network Device Configuration

Network devices are devices used to connect computers together so that they can share information. This category includes switches, routers and firewalls. Each of these devices have the ability to be configured through an Internetwork Operating System.

- Evaluate IP scheme and modify device configuration to limit the amount of available hosts on a given network.
- Add and/or modify existing access control lists (ACLs) to block any data transmission that's not crucial to system functionality
- Password encryption
- Disabling unused ports
- Sending system logs to a SIEM
- Configuring SPAN ports for NIDS integration

Firewalls

Firewalls are network devices that monitor traffic. The device will block traffic specified by security rules implemented by the administrator.

- Provide custom configuration based upon customer requirements
- Configure firewalls for optimal protection based upon network vulnerability assessments as well as the Westinghouse team's strong understanding of each layer housed within the OSI model.

Unidirectional Gateways

Also called data-diodes, these appliances only allow data to travel in one direction. This is typically done through fiber optic links with transmit and receive removed in one direction.

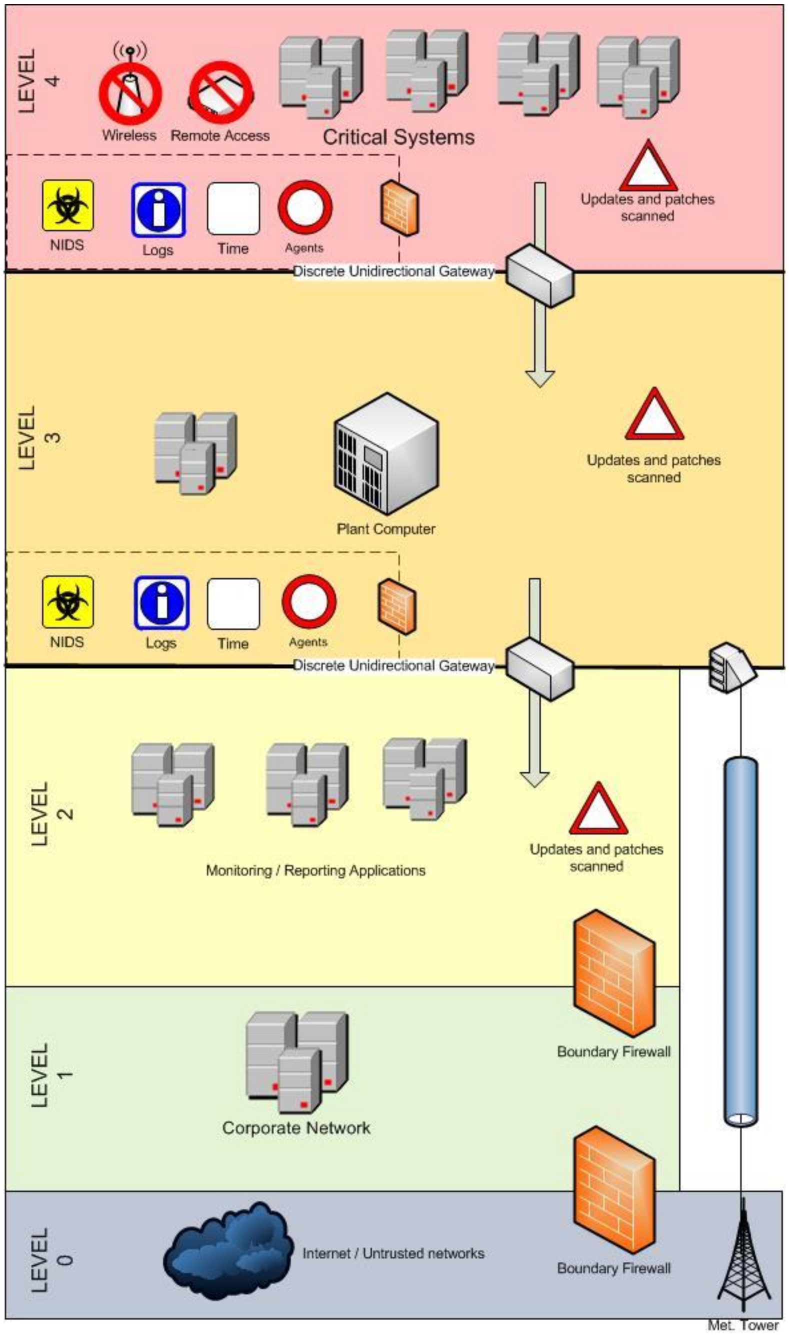
- Depending on network layout along with other variables, data-diodes will be included between networks with different security zones or remote locations to guarantee outside threats remain outside.

Westinghouse

Defense-in-Depth

Defense-in-Depth is the practice of having an independent and layered security based approach to network topologies. As a result, if one method of defense would fail then another layer would identify an incursion and limit any further exploitation.

- Westinghouse can provide and implement a layered defense strategy in order to provide the optimal approach to protecting systems and proprietary information.
- With the use of appropriate network device configuration, firewalls, unidirectional gateways, along with encryption and intrusion detection systems, Westinghouse will deliver a reliable and secure network.


LEVEL 4
Wireless
Remote Access
Critical Systems
Updates and patches scanned
NIDS
Logs
Time
Agents
Discrete Unidirectional Gateway
LEVEL 3
Plant Computer
Updates and patches scanned
NIDS
Logs
Time
Agents
Discrete Unidirectional Gateway
LEVEL 2
Monitoring / Reporting Applications
Updates and patches scanned
LEVEL 1
Corporate Network
Boundary Firewall
LEVEL 0
Internet / Untrusted networks
Boundary Firewall
Met. Tower

Benefits

Time Savings

Westinghouse engineers have the operational experience to deliver high quality results within the allocated schedules.

Experience

Westinghouse engineers have unparalleled expertise in analyzing network topologies while providing input to assist the licensee in meeting requirements.

Security

Having an optimally designed network architecture will make it easier to secure. While some level of residual risk will always remain, Westinghouse can provide the appropriate mitigation strategies to reduce the level of risk and vulnerabilities to the network.