Product Defense in Depth

Summary

Defense in depth is a layered security strategy that employs multiple measures to protect a network. Implementing these strategies helps establish defense system, that are capable to mitigate a wide range of threats.

Security Capabilities and Defense-in-Depth Strategy

Application layer:

- **Authentication and Authorization** - Ensures only authorized users can access devices administration and programming interfaces.
- **Access control mechanism** - prevents unauthorized access to the devices configurations and protects sensitive information.

Network layer:

- **NAC (Network Access Control)** - Network level DiD capability that restricts access the networks and sensitive resources.
- **Network encryption** - Utilizes encryption mechanisms for wireless communication and IPsec.
- **Network Firewall** - Firewalls control ingress and egress network traffic based on predetermined security rules to prevent unauthorized access and traffic.
- **Network Segmentation** - Divides the network into smaller, isolated segments. Reduces the attack surface by isolating critical systems.
- **VPN (Virtual Private Networks)** - Encrypts data transmitted over the network and ensures secure communication channel for remote access.
- **Network Failover System** - Ensures network availability in the event of failure.
- **Attack prevention** - Mitigates the risks of most common network layer attacks (e.g.: DoS, SYN Flood).

Defense-in-Depth recommendations

The following defense in depth measures are recommended:

- **Network Segmentation** - Segment network to isolate different types of traffic and devices.
- **Secure Access Controls** - Utilize strong authentication and authorization mechanisms to control access to the network and devices.
- **Regular Software Updates** - Keep all software and firmware up to date to protect against known vulnerabilities.
- **Change Default Configuration** - Change default usernames, passwords, and settings on the device.
- **Disable Unused Services** - Turn off unused services and ports on the device to reduce the attack surface.
- **Enable Security Features** - Activate built-in security features, such as SYN Flood protection,

HTTP attack prevention, port scan prevention.

- **Physical Security** - Restrict physical access to the device and other critical network hardware to authorized personnel only.