CYBER SECURITY IN NETWORKING

Harsini JP
(RA2211032010007)

S. Reshma
(RA2211032010008)

Hrishka Raj
(RA2211032010004)

ABSTRACT

As the digital age transforms power distribution, ensuring the security of smart grid networks is paramount. This case study explores a comprehensive approach to cyber defense, leveraging cutting-edge technologies and simulation to safeguard critical infrastructure.

INTRODUCTION

With the rise of smart grid technology, cybersecurity is critical due to the essential role of power infrastructure and its reliance on networked systems. Smart grids, while improving efficiency in power distribution and monitoring, are vulnerable to cyber threats because of their exposure to public networks. This project aims to strengthen smart grid security using Cisco Packet Tracer to simulate a Zero Trust model, where access is highly controlled and never assumed. Key measures like VLANs for traffic separation, Access Control Lists (ACLs), SSH for secure management, and Port Security are applied to establish a reliable cybersecurity framework for protecting this vital infrastructure.

IMPORTANCE OF SECURE GRID SYSTEMS IN THE DIGITAL AGE

Resilience against Attacks

Robust cyber security measures protect smart grid systems from malicious threats, ensuring uninterrupted power supply.

Data Integrity

Securing data transmission and storage across the grid prevents unauthorized access and data tampering.

Compliance and Regulations

Adherence to industry standards and government regulations reinforces the grid's security posture.

LEVERAGING ZERO TRUST ARCHITECTURE (ZTA) PRINCIPLES

Continuous Verification

ZTA requires users, devices, and applications to continuously verify their identity and authorization before accessing resources.

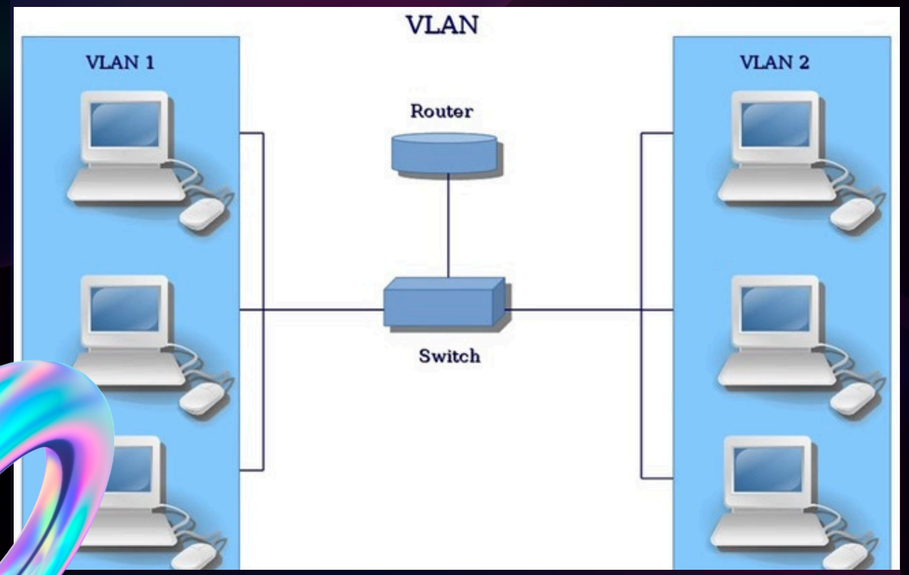
Granular Access Control

Micro-segmentation and least-privileged access policies limit the potential impact of security breaches.

Adaptive Security

ZTA leverages real-time monitoring and machine learning to detect and respond to evolving threats.

IMPLEMENTING VLANS FOR NETWORK SEGMENTATION



1. **Isolate Domains:**
   VLANs create logical network segments, isolating critical smart grid systems from other network traffic.

2. **Granular Access**
   VLAN-based access controls restrict communication between segments, limiting the spread of potential threats.

3. **Simplify Management**
   VLANs enable the centralized management and monitoring of network traffic, streamlining security operations.

CONFIGURING ACCESS CONTROL LISTS (ACLS) FOR ACCESS CONTROL

Perimeter Defense

ACLs filter inbound and outbound traffic, acting as a firewall to block unauthorized access.

Layered Security

ACLs complement other security measures, such as firewalls and intrusion detection systems.

Granular Rules

ACLs can be customized to permit or deny specific protocols, ports, and IP addresses.

Auditing and Logging

ACL logs provide valuable insights for security monitoring and incident response.

ENHANCING SECURITY WITH SSH AND PORT SECURITY

SSH

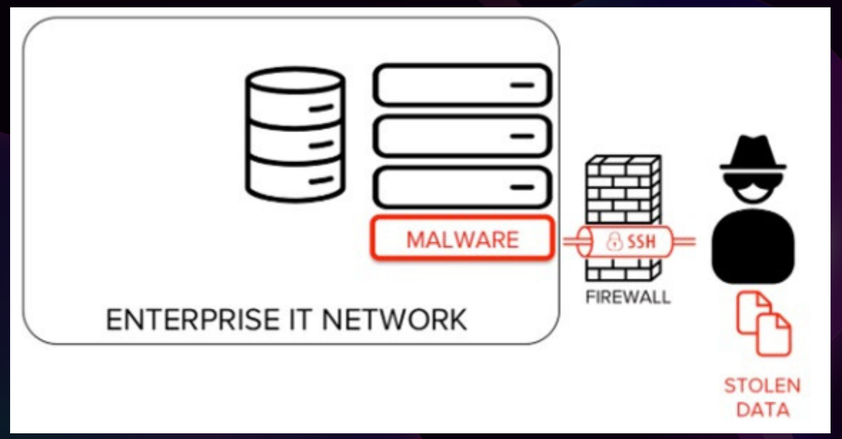
Secure Shell (SSH) encrypts remote access, preventing eavesdropping and man-in-the-middle attacks.

Port Security

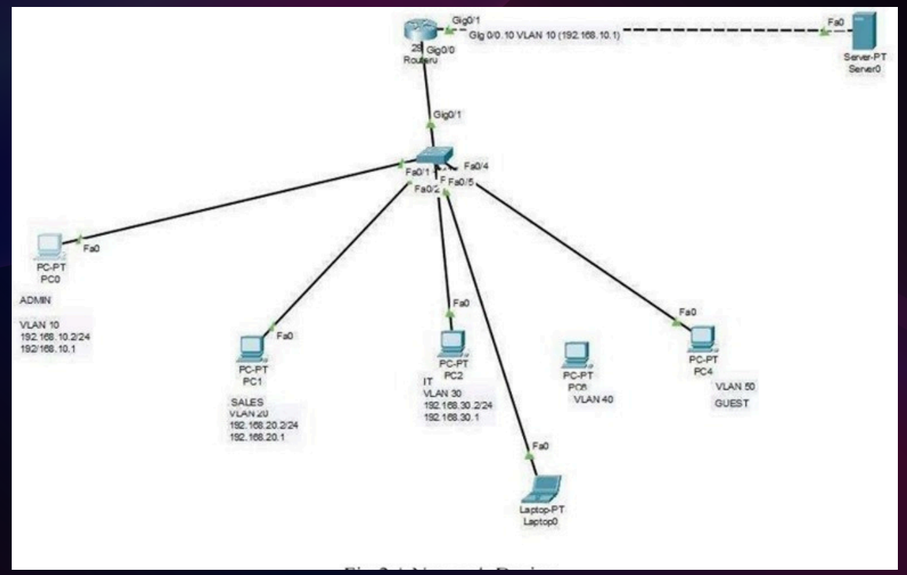
Restricting access to specific switch ports limits the attack surface and prevents unauthorized device connections.

Monitoring

Continuous monitoring of SSH sessions and port activities enables early detection of anomalies.



SIMULATING THE SECURITY SETUP IN CISCO PACKET TRACER



1. **Network Topology**
   Designing the smart grid network topology with appropriate segmentation and access controls.

2. **Security Configuration**
   Implementing ZTA principles, VLANs, ACLs, SSH, and port security across the simulated environment.

3. **Validation and Testing**
   Verifying the security posture through simulated attacks and monitoring the system's resilience.

KEY TAKEAWAYS AND RECOMMENDATIONS

1. **Holistic Approach**

   VLANs create logical network segments, isolating critical smart grid systems from other network traffic.

2. **Continuous Improvement**

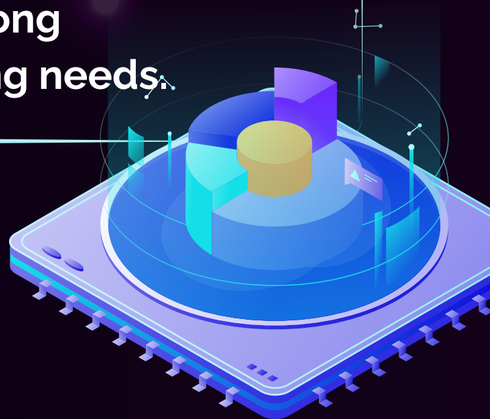
   Regular security assessments, updates, and employee training are essential to address evolving threats.

3. **Collaboration and Compliance**

   Coordinating with industry partners and adhering to regulations ensures the grid's overall security posture.

CONCLUSION

The Company Network Design project has been successfully implemented, achieving a robust, scalable, and secure network infrastructure. Key accomplishments include a hierarchical network model with redundancy to enhance reliability, VLAN-based segmentation for departments, and inter-VLAN routing for efficient communication. Security measures, NAT and PAT configurations, and Quality of Service (QoS) prioritization were meticulously applied to support secure and optimized performance. Testing with Cisco Packet Tracer validated the network's functionality, ensuring it meets the organization's requirements for scalability, security, and operational efficiency. This design provides a strong foundation for the company's evolving networking needs.



THANK YOU!