SECURING NETWORK DEVICES

WHAT IS SERURING NETWORK DEVICES

Securing network devices is an important topic in the world of internetworking and will remain so as long as the threat of intrusion, espionage, theft, or hacking exists.

ROUTER

Routers are the internet backbone, coordinating network traffic. They're vulnerable to theft, hacking, and attacks on routing protocols like RIP/OSPF. To protect them, focus on physical security, advanced configurations, secure routing protocols, and regular updates.

SW IC TH

Network switch security is important to protect against theft, hacking, and network attacks. Protective measures include physical security, advanced configuration, regular system updates, and use of port security features to limit valid MAC addresses

VLAN

VLANs group devices logically in a LAN, enabling segmentation for security. They isolate networks within a shared infrastructure, protecting sensitive data. However, they face vulnerabilities like protocol attacks. Countermeasures include monitoring, advanced configurations, and regular updates

FIREWALL

Firewalls filter traffic, using ACLs for control. They face threats like hacking, theft, and attacks on ACLs or performance. Security involves physical safeguards, advanced setups, secure access, and updates.

1 OPETORS CENTER

The Network Operation Center (NOC) is one or more locations containing the tools that provide administrators with a detailed status of the organization's network.

2 SWITCHES, ROUTERS, AND NETWORK APPLIANCES

The following sections discuss several measures that an administrator can take to protect various network devices.

3 WIRELESS AND MOBILE DEVICES

Wireless and mobile devices have become the predominant type of devices on most modern networks. They provide mobility and convenience but pose a host of vulnerabilities.

4 NETWORK AND ROUTING SERVICES

Wireless and mobile devices have become the predominant type of devices on most modern networks. They provide mobility and convenience but pose a host of vulnerabilities.

GROUP 5 BY SECURING NETWORK DEVICES

Network vulnerabilities, like open ports and service weaknesses (DHCP, DNS, ICMP, RIP, NTP), are exploited by cybercriminals. They target servers to disrupt access, redirect traffic, or manipulate time data. Security involves port filtering, service authentication, and regular updates.

Wireless devices dominate modern networks but carry vulnerabilities like theft, hacking, and unauthorized access. Securing wireless networks relies on authentication and encryption. Options like WEP, WPA, and WPA2 offer varying levels of security. For robust protection, 802.11i/WPA2 with AES encryption is the industry standard. Regular updates and physical security also bolster defenses.