

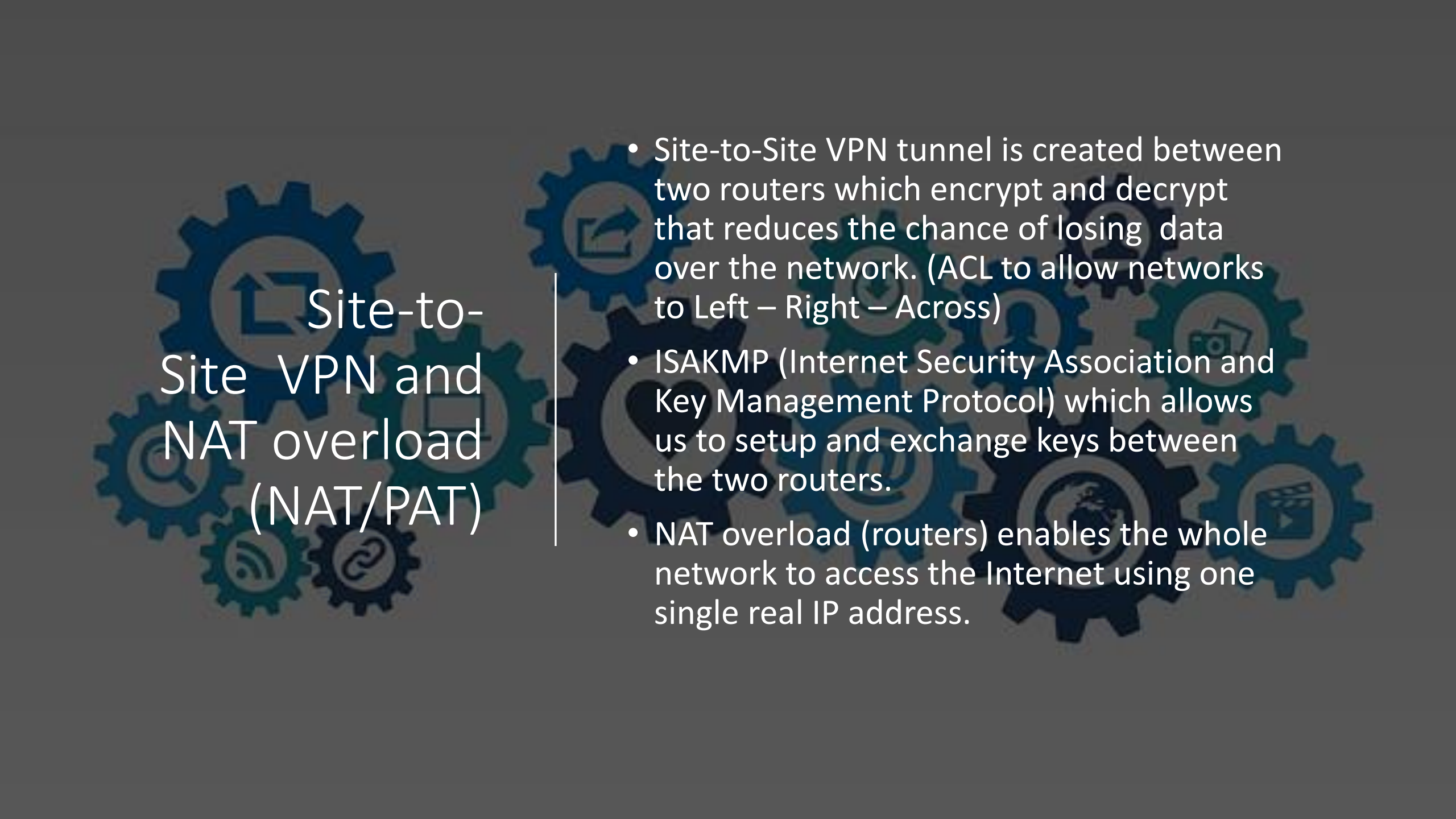


The Hospital network project

- Skylar York



West Office



Site-to-Site VPN and NAT overload (NAT/PAT)

- Site-to-Site VPN tunnel is created between two routers which encrypt and decrypt that reduces the chance of losing data over the network. (ACL to allow networks to Left – Right – Across)
- ISAKMP (Internet Security Association and Key Management Protocol) which allows us to setup and exchange keys between the two routers.
- NAT overload (routers) enables the whole network to access the Internet using one single real IP address.



Small Office |



Network Management on MLSW and Router

- **Configuration Management:** to monitor network and system configuration information (SNMP, Log Server and OSPF)
- **Fault Management:** is to detect, isolate, notify, and correct faults (SNMP)
- **Performance Management:** monitors and controls the network (Firewall, ACL's, and QoS)
- **Security Management:** is to control access to network resources (Radius Server, Username and password, SSH, encrypted all plain text password)
- **Accounting Management:** is the control of users' access to network resources (**AAA** Authentication, Authorization and Accounting , Logging Server)



East Office

Features



- Port security: We implemented port security on our switches by shutting down the ports and giving them a VLAN of 105 (unused ports). This will prevent hackers from getting a connection when trying to connect their devices into the switches and it'll tell us which ports are in use and which ones aren't being used
- DHCP server: We implemented DHCP servers on the West Office, East Office, and Accounting office to help the multi-layer switch provide the devices an IP address that are connected to the specific VLANs and to have a server provide our AAA for our username and passkey to connect to the router for Doctor, Employee, and Equipment, Syslog/NTP, and DNS
- Frame-relays: This is used to connect two or more LAN bridges over large distances we implemented this so that our network is pingable cross network accounting is connected to serial 0, west office is connected to serial 1, small office is connected to serial 2, east office is connected to serial 3, and the ISP router is connected to the serial 8 port

Accounting Office





Features

Access control:

- We implemented access control on the firewall this will prevent the guest (VLAN 20) from accessing any data that's on the accounting server using the **access-list OUTSIDE extended deny ip any 10.____.2.0 255.255.255.0** command on the firewalls

Ethernet channel:

- We implemented an Ethernet channel on the Multilayer switches on the gigabit 1/1/1 and gigabit 1/1/2 and putting them in group 1 on MLSW1 and group 2 on MLSW2 ports this will allow fault-tolerance and high-speed between the two switches

VLANs:

- Lastly, we used VLANs on our network to limit access of specific groups. The VLANs used are VLAN 10 (Equipment), 20 (Guest), 30 (Employee), 40 (Doctor), 77 and 99 (Management), and 105 (for unused ports)



Questions?



Sources

- W. (2020, September 21). *What is HIPAA*? Legend Networking. Retrieved December 1, 2021, from <https://legendnt.com/2019/11/21/what-is-hipaa/>
- Wright, J. (2018, Sept) *Five steps to HIPAA compliance for a doctor's office*;
 - [Five Steps to HIPAA Compliance for a Doctor's Office \(24by7security.com\)](https://24by7security.com/five-steps-to-hipaa-compliance-for-a-doctors-office/)
- HIPPA Journal (n.d.) HIPAA compliance checklist;
 - [Official 2021 HIPAA Compliance Checklist \(hippajournal.com\)](https://hippajournal.com/official-2021-hipaa-compliance-checklist/)