1. **VPN-Virtual Private Network and VPN Protocols**
2. A virtual Private Network is introduced to establish secured and reliable network connectivity on various cases. VPN is used to establish an isolated network for a community of computers.

Primarily VPN are used in three scenarios:

1. To manage a set of computers in a community and restricting their network usage and protocol usage.
2. To connect geographically divided MNC infrastructure. And enabling the enterprise employees to connect to enterprise network and work securely.
3. To establish secure and reliable connections to a set of servers for high throughput.
4. Protocols used in the VPN are
5. PPTP: Point to point tunneling protocol, this is the widely used VPN connection protocol. This protocol establishes a point-to-point tunnel between the devices and then pushes the data encapsulated packets.
6. IPSec: Internet protocol security, this uses regular IP protocol and used session authentication to approve devices and sends the encrypted data packets across network.
7. L2TP: Layer 2 Tunneling Protocol, this protocol connects to devices communicating via L2TP and usually transfers data packets using either PPTP or IPSec protocol.
8. SSL: Secure Sockets Layer, this is client friendly protocol usually deployed y web servers to isolate the users logging into their website to protect the content.
9. SSH: Secure Shell, this is to connect Unix based devices remotely. In an SSH the remote shell of the Unix machine is access securely with an encrypted tunnel.
10. We use VPN for making the networks secured and isolate from external connections. Enterprise employees connect to their office VPN to access the intranet websites and transfer data securely. Ticketing agents use VPN to establish a private network with the server so that the external load on the server will not affect their performance. Regular users use VPN to protect them when using public hotspots. this helps them to eliminate data capture by creating a secure tunnel.

We can use VPN for different purposes, most of the devices today will support VPN. We can just configure the VPN server in the device and the operating system will take of the tunneling. Some mobile applications will use VPN on Demand to connect to the secure servers there by eliminating the risk of fraud.

1. I learnt the basic functioning of VPN, how a VPN is used by different organizations and vendors to increase security and implement better communication. I learn how different protocols implement the VPN connectivity and their reliability. I learnt to use OpenVpn and configure to use with my personal devices.

References: Cisco Journal: What Is a VPN? - Part I - The Internet Protocol Journal - Volume 1, No. 1 *By Paul Ferguson, Cisco Systems and Geoff Huston, Telstra*

*https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-18/what-is-a-vpn.html*

1. **NIDS Network Intrusion Detection System**
2. Network intrusion detection system is a tool used to detect the malicious data packets running across the network. It is introduced by Inventec Corp., in 2009 and patented in 2010. The aim of the NIDS is to detect the rogue data packets usually before getting processed by the intended devices and to protect them. If a data packet contains the data that is not intended to be used in the community or if it does not comply with the policies, then the data packet should be dropped and alert should be sent to the administrators.
3. Usually and NIDS is implemented using several techniques like Signature Based algorithms, Anomaly based Algorithms and Using protocol scanning.
4. In signature based technique the system uses the set of signatures or patterns which are found to wrong in the history. If a new packet follows the same structure as one those in history then it will be detected as rogue data packet.
5. In anomaly based system the machine learning algorithms will predicts the rogue data packets based on the history. It is cognitive learning process and can be deployed on servers which require more security.
6. In protocol based NIDS, the technique is usually deployed at the server’s front end to analyze the HTTP and HTTPS data packets.
7. We use NIDS to detect the network flaws and to protect the network connected devices from attacks. This NIDS can be deployed at various levels of network. They can be even installed as a software at the terminal device and the software will analyze the packets before the corresponding application processes the data packet. This can be deployed at networking devices to eliminate the performance issues of the terminal devices.
8. From the research on NIDS, I understood the importance of network security and how the network flaws exploit the security of the connected devices in the network. Understood the underlying theory behind the network intrusion detection system. Analyzed how NIDS at different network levels is implemented and how they function at each level of network security implementation.

References: *Network intrusion detection system by Meng Sun, Tom Chen Inventec Corp*

*https://patentimages.storage.googleapis.com/8d/d2/c3/33174fa8b0aa19/US20100251370A1.pdf*

1. **Firewall**
2. A firewall could be devices or a software employed to monitor the incoming and outgoing traffic from a device. And depending upon the security levels and implemented filters this decides to allow or deny a particular activity on the network. Fire has been the most trusted implementation for the internet security from several years and has been performing exceptionally best at their service.
3. The firewalls are of several types and deployed for specific needs.
4. Proxy firewall: During the early days of Firewall implementation Proxy firewall techniques was used. A proxy firewall acts as the gate for the data exchange. The data loaded by the particular application is received by the proxy server and analyzed and then sent to application for usage. This used to be the best practice in those days where are end user computers are less powered. but this technique has a great impact on the network throughput.
5. Stateful inspection firewall: This type of firewall is used by all modern firewall software; this monitors the connections from beginning to termination. This firewall will use the administrative policies and history data to filter the network data.
6. Unified threat management firewall: This is designed particularly to avoid the attacks; it contains intrusion prevention as well as antivirus algorithms to ensure maximum safety.
7. Next-Generation firewalls: With increasing risks in the networks most of the companies started to deploy these firewalls. They contain all the conventional features along with advanced threat detection schemas. And they are application aware, they restrict the data to corrupted applications and protocols. They implement machine learning to learn the future risks.
8. The usage of these firewalls is simpler, they can be installed on the terminal consumer devices like any other software. Enterprise networks deploy firewalls on the networking devices to avoid regulations override by end users.
9. I leant the building blocks of firewall system. Studied how firewalls are developed and implemented in different scenarios. Learnt how administrators create firewall filters to maximize the security.

**References**: Cisco Journal, Firewalls and Internet Security - The Internet Protocol Journal - Volume 2, No. 2. Firewalls and Internet Security, the Second Hundred (Internet) Years by Frederic Avolio, Avolio Consulting

*https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-1/ipj-archive/ article09186a00800c85ae.html*