Active Directory

Windows Server introduction and installation
Active Directory (intro, hierarchy, installation, objects)
Files and folders permissions
Group Policy
DHCP and DNS
הספק הלימוד של הנושאים במודול זה ייקבע בהתאם לקצב ההתקדמות הקבוצה.

AWS

Cloud computing introduction
Account setup
Identity and access management
AWS Services and CLI
AWS EC2 – overview
Cloud Storage (EBS S3 EFS)

Fortinet

Intro & Basic Configuration
Routing
VDOMs
Firewall Policies and NAT
Firewall Authentication
FSSO
Certificate operations
SSL VPN
IPsec VPN
Antivirus
Web Filtering
IPS and Application Control
SD-WAN
Security fabric
HA
Diagnostics

Linux

1. Linux distributions

- Red Hat, CentOS, and Fedora
- Debian, Ubuntu, Mint

2. Text Editors

- Nano and Vi introduction
- Nano overview and shortcuts
- Interactive VIM Tutorial

3. Linux Fundamentals

- Root = power
- Linux Prompt Basics

4. File Systems

- Tree and directories

5. Files, Tools, Owners, Permission

- Help, man, grep, more and less
- Abbreviated and long arguments, owners, groups, and permissions
- Owners, groups, and basic permission example

CCNA

1. Network Access

- VLANs
- Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
- EtherChannel (LACP)
- Rapid PVST+ Spanning Tree Protocol
- Wireless Architectures and AP modes
- WLAN components (AP, WLC, access/trunk ports, and LAG)
- AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
- Wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

2. IP Connectivity

- Routing table
- Routing
- IPv4 and IPv6 static routing
- Single area OSPFv2
- First-hop redundancy protocol

3. IP Services

- NAT
- NTP
- DHCP and DNS
- SNMP
- Syslog
- Forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
- SSH
- TFTP/FTP

4. Security Fundamentals

- Key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Security program elements (user awareness, training, and physical access control)
- Access control using local passwords
- Security password policy elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
- Remote access and site-to-site VPNs
- Access control lists
- Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- AAA
- Wireless security protocols (WPA, WPA2, and WPA3)
- WLAN using WPA2 PSK using the GUI

5. Automation and Programmability

- Automation basics
- Controller-based and software-defined architectures (overlay, underlay, and fabric)
- Traditional campus device management with Cisco DNA Center-enabled device management
- REST-based APIs (CRUD, HTTP verbs, and data encoding)
- Capabilities of configuration management mechanisms Puppet, Chef, and Ansible
- Interpret JSON-encoded data