Admin GUID:
Sec : SID,
Last Logon time.

DC
AD.

Page No.:
Date:
YOUVA

Active directory.

↳ It is a set of database and services that connects users with the network resources they need to get work done.

↳ It stores each and every details

↳ LDAP, Kerbros, DNS.

↓

Lightweight Directory Access protocol

→ It will help to locate your data.

AD have three tier:

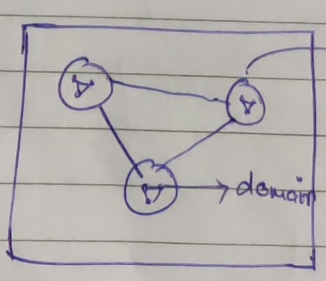
← Domain → trees → forest ⟶ Multiple trees.

It is ↓ ↳ Multiple domains.

Manage-ment Boundary

Domain is a group of related users, computers and other AD objects.

↳ forest is a security boundary, until Admin dont allow to connect you cant allow to joint forest.



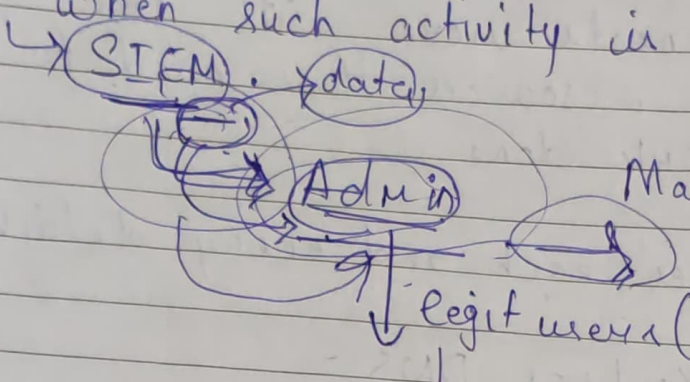
→ Tree.

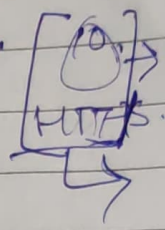
⟶ forest

IDS. Shikatagarai door → IDS → Firewall

↳ It is a system that monitors network traffic for suspicious activities and issues alerts when such activity is discovered.

↳ SIEM. data





1) NIDS, HIDS, PIDS, APIDS, Hybrid IDS

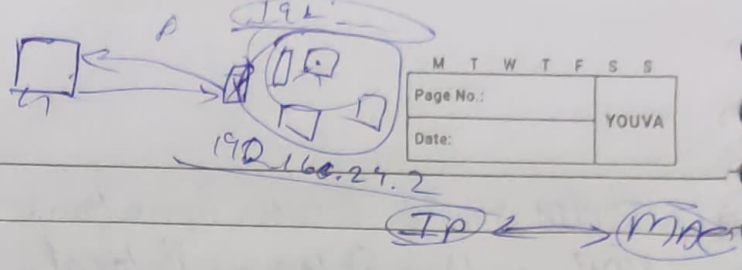
↑ Network ↑ Host ↑ protocal ↑ App Protocal.

Hybrid IDS → Host + Net.

Better than Other IDS.

IPS

- NIPS (Network)
- HIPS (Host)
- WIPS (Wireless)
- NBA (Network Behaviour Analyses)



M T W T F S S
Page No.:
Date:
YOUVA

* Network Protocols

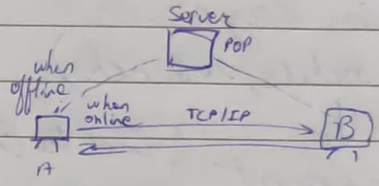
- Protocol ? :-

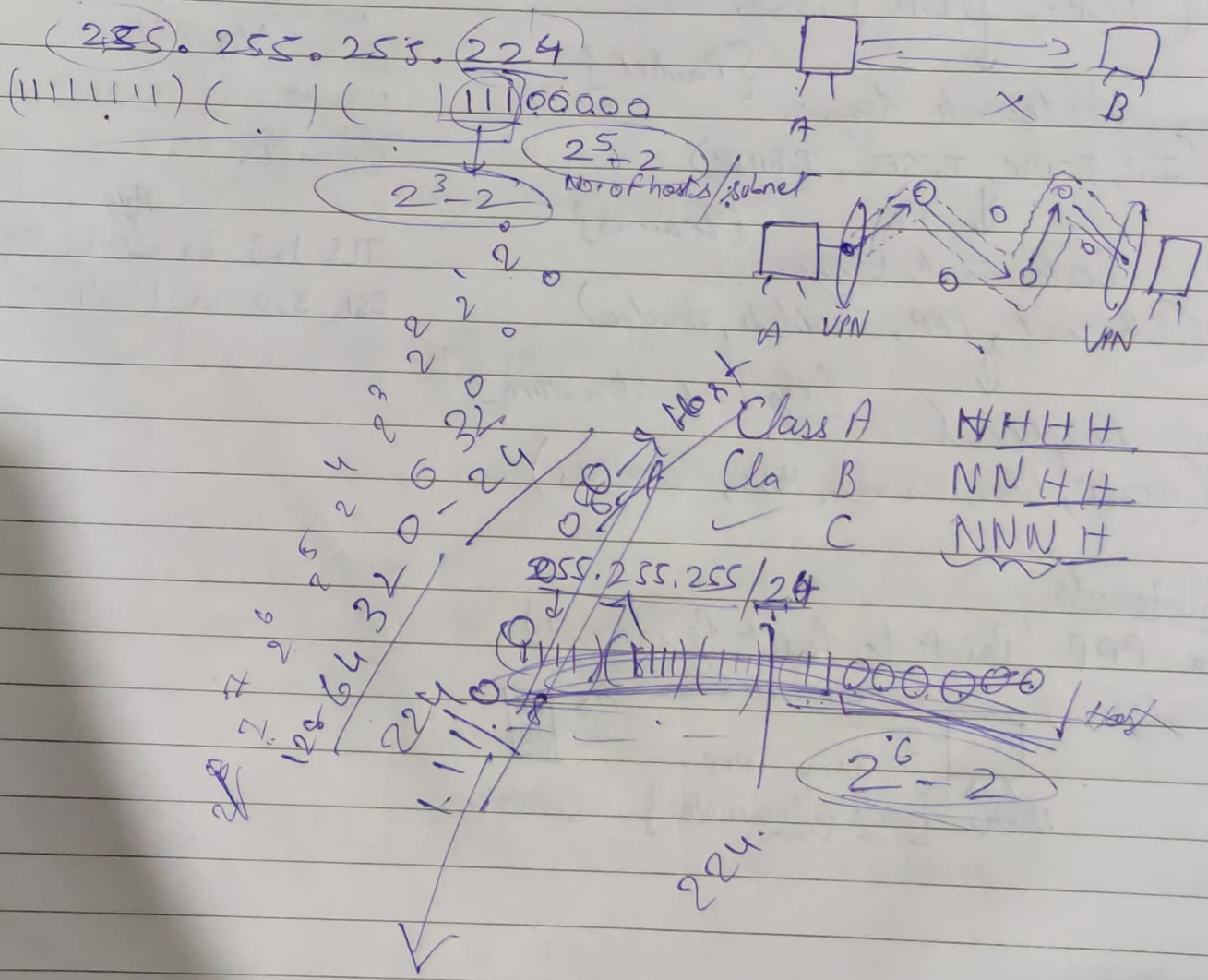
Sy

- It is set of Rules, used in Digital ~~Connection~~ Communication to connect network devices and exchange info. between them.

- Types: i) TCP/IP :- Three way handshake [Establish Connection]
  (Base Protocol)

ii) HTTP [Hypertext Transfer Protocol]
iii) SMTP [Simple Mail Transfer Protocol]
iv) POP [Post office Protocol]
v) PPP





TCP/IP :- To establish Connection..
UDP :- User Datagram Protocol.

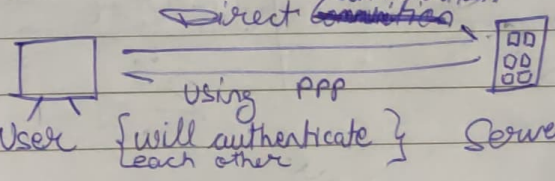
Application Layer {End User Layer}
(HTTP, FTP, IRC, SSH, DNS, SNMP)
↓
Presentation Layer {Sytax layer}
(SSL, SSH, IMAP, FTP, MPEG, JPEG)
↓
Session Layer. {Synch & Send to Port}
(APIs, Sockets, winsock)
↓
Transport {End to End Connection}
(TCP, UDP)
↓
Network Layer {Packet}.
(IP, ICMP, IPSEC, IGMP)
↓
Data Link Layer {Frames}.
(Ethernet, PPP, Switch, Bridge)
↓
Physical {Physical Structure}.
(Coax, Fiber, Wireless, Hubs, Repeaters)

Application
Presentation
Session.
Transport
Network.
Data Link.
Physical

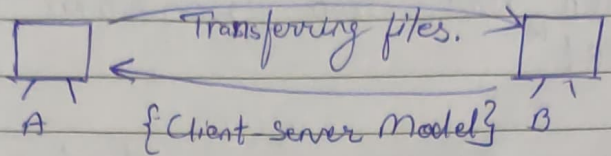
Firewall
Vig MR1
OS version of that firewall.
10.8.13.48

TLS 1.3 in 2018.
SSL 3.0 in 1999

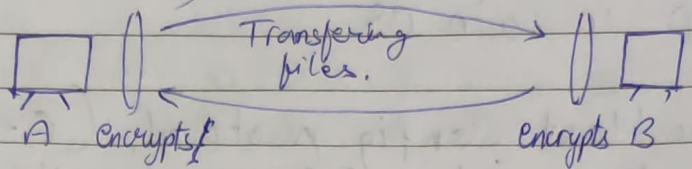
Protocols
- PPP (Point to Point Protocol)



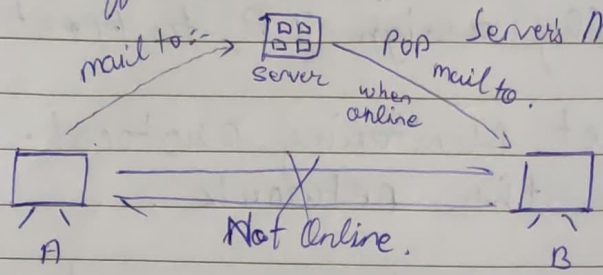
- FTP (File Transfer Protocol) :- → {authenticates using UserID & Password}



- SFTP (Secure FTP) :-



- POP 3 (Post office Protocol 3) :- → Client's MAA [Message Access Agent]



- IRC [Internet Relay Chat] :- ◦ Client-Server Model
  ◦ Used as a Chat Server.
- SSH [Secure Shell Protocol] :- {Cryptographic network Protocol.} It is used for operating network services, security over unsecure N/w.
- IMAP [Internet Message Access Protocol] :- Internet Standard Protocol used by clients to retrieve email messages from a mail server over a TCP/IP connection.
- ~~MPEG~~ E
- API (Application Programming Interfaces) :-
  ↳ It is a software allows two app to talk each other.

M T W T F S S

Page No.: YOUVA

Date:

Sockets: It is one endpoint of a two way communication betⁿ two programs running on netᵂ.

Winsock: It is a programming interface that handles I/O reqᵗˢ, for internet app in win OS.

DHCP: Dynamic Host Config protocol. (C-S) protocol that auto provides IP Host with its IP address
↳ Dynamically assign IP to Hosts on Net.

SNMP: Simple net Monitoring protocol: It monitors the network.

ICMP (Error Reporting Protocol): Internet Control Message protocol:
↳ To communicates problems with data transmission.

IGMP (To manage Membership of Host & Routing Devices): Internet Group Management Protocol:
↳ To transmit msg/diff data packets.

AD: LDAP → Lightweight Directory Access protocol.

↑

Domain trees forest

↑ ↑

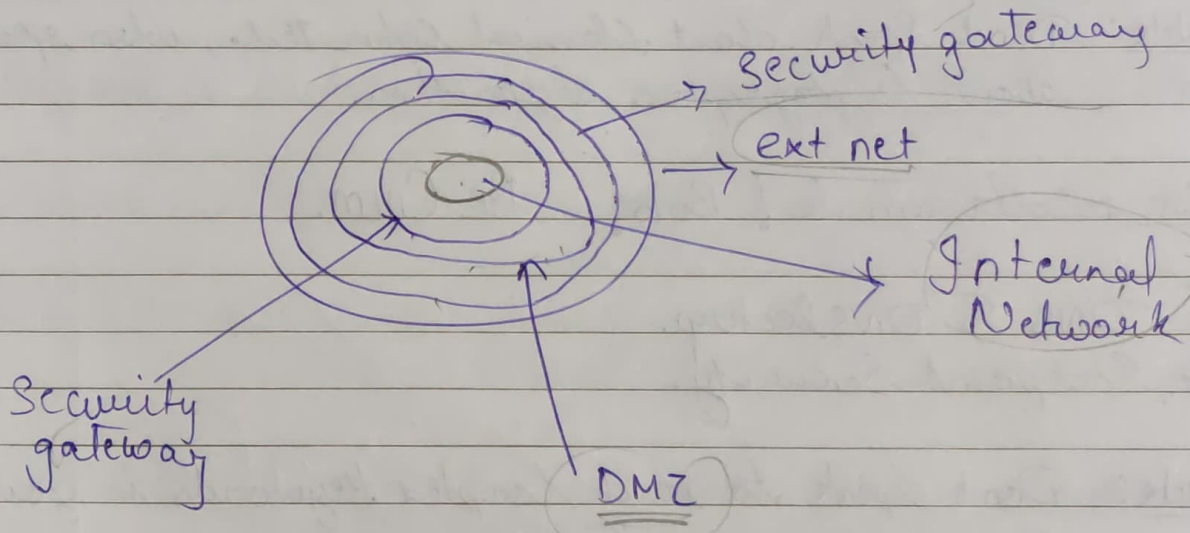
Management Security Boundary.

↳ Port Numbers :

20, 21 : FTP
22 : SSH
25 : SMTP
53 : DNS
80 : HTTP
123 : NTP → Net time protocol
179 : BGP → Border Gateway protocol.
443 : HTTPS
500 : ISAKMP, IPSec
3389 : RDP → Remote Desktop protocol (Anydesk)

DMZ : (Demilitarized Zone)

↳ Adds extra layer of Sec to Internal lan network from untrusted traffic.



Stateful → ~~HTTP~~ Telnet, FTP
~~F~~ Stateless → HTTP.

DC → Digital Certi
PKI → Pub key Infra.

* Application Security.
* Network Security
** Types of IDS & Firewall.
* Subnetting.
* OSI layer(s) & Protocols in each layer.
* DHCP.
** Cryptographic Algorithms & Practical Usage/uses. (might be in Hypothetical Situation)
[Book] TCP/IP Protocol Suite by Forozen.
* Ports (Most common.)
* How to Prevent the Virus/Trojans, if it has infected you.

Note:- Don't Speak about Classical Cipher Tech., when speaking about Cryptographic algorithm.

Note:- Aaram se! Bolo! BE CALM.

. DNS & DNS lookup.
* Endpoint Security.
.

Note:- Don't Speak to much Complex Keywords in your answer to every Question.

to Buy
Do we need, the Firewalls, IDS, IPS for the Endpoint Security OR is it okay without it?

- VPN. • Spyware • Proxies • Web-Proxy / Web Security
• SMB • Malware • Email-Security • SPAM Filtering

M T W T F S S
Page No.:
Date:
YOUVA

- MDR (Sophos Managed Detection & Response Service)
- Intercept X
- XDR (Extended Detection & Response)
- SASE
-

* Types of Virus:

i) Boot sector Vir.
ii) Direct Action Vir
iii) Resident Vir. ——→ Home
iv) Multi-Par-Tite Virus ——→ Boot Sector, Direct Action
v) Overwrite Virus ——→ Most Dangerous.
vi) Poly Morphic Virus ——→ Website.
vii) File Infector Virus
viii) Space filler Virus
ix) Macro Virus ——→ Email

* Types of Malware

- Trojans :- Tricks you, by acting as a legitimate software
- Spyware :- Attempts to steal your personal Information.
- Adware :- • Displays ads on your screen.
  • Collects Personal Info, to serve more Pers. ads.
- Root kits :- • Enables Unauthorized Users to gain access to your Computer without being Detected.
- Ransomware :- • Designed to Encrypt your files & blocks access to them. until Ransom is Paid.
- Virus

M T W T F S S

Page No.: YOUVA

Date:

- Worms :- • Replicates itself to consume network resources & spread/infect other Computers on the same network.
  - They are designed to consume Bandwidth & interrupt networks.
- Key-loggers :- Keep tracks of your keystrokes on your keyboard & record them on a log.

* Server Message Block (SMB)

- It is a Communication Protocol, developed in 1983 by Barry A. Feigenbaum at IBM
- It was intended to Provide Shared Access to files & Printers across nodes of a Network. ~~of Systems~~

* CMD Commands

i) Cron :- Job Scheduler
ii) df :- Avail. Disk Space
iii) Ping :- To test & Verify, If Add. is Corrut OR Not.
iv) nslookup:-

* Secure Access Service Edge Platform (SASE)

- Cloud Aritecture Model
- Bundles Networ & Securit as a Service
- Function Together, & delivery them as a single service.

M T W T F S S

Page No.: YOUVA

Date:

Extended Detection & Response :-

XDR :- Collects & Automatically correlates data across multiple Security layer.

- Email, Endpoint, Server, Cloud work load, Network.

Short! :- This allows faster Detection of threats & Better investigation & Response Time.

Intercept X with XDR :

- includes Anti-Ransome Technology
- Detects Malicious Encryption Processes & shuts them down.
- Prevents both [File Based] & [Master Boot] Record ransomeware.

Unix Commands

1) cron (Job Scheduler)
2) df (Avail Disk Spaces)
3) ping (IP Address is ✓/✗)
4) nslookup
5) ls
6) traceroute
7) grep
8) dd (Disk Destroyer)
9) vi
10) chmod
11) init
12) netstat (Display Active TCP Conn.)
13) kill (terminates any Processes)
14) gzip (General file Compression)
15) find (To find files & Directories)
16) wget (Retreve files using App. layer Protocols)
17) Netcat (R/w Data Net./Cmd line)
18) chown (change owner)
19) su (Super User)
20) mount (show Data in Big Tree Str.)
21) mkdir (Make Directory)
22) ifconfig (To check ip addresses)
23) fdisk (Fix & Defrag)
24) nohup (Run multi Comm. in bgd)
25) whoami (User Details)
26) tail (Reads some lines of i/p)
27) dpkg
28) xargs
29) pwd (Curr. Direc)
30) rmdir (Remove Directory)
31) chroot (change Root)
32) tty
33) fsck (Continuously Check)
34) env (Print Envir-nmtl Variables)
35) du (Disk Usage)
36) dmesg
37) cp (Copy)
38) useradd (Adds User file)
39) md5sum (File Integrity)
40) unix2dos (Convert)
41) sleep (Sleep)
42) tee (Std. I/O Reads & Write)

43) Modprobe (Add/Rem - Mod - Kernal)
44) bzip2 (File Compression Program)
45) cat (Concatenet)
46) echo (Print)
47) getotp
48) Mv (move)
49) passwd (Change Password)
50) UMOUNT (Detaches file from Heirarchy)
51) Hostname | Hostname -I

Windows powershell commands.

1) Get - Command
2) Get - Help
3) Set

Mar 2020 -> Thoma Bravo (Private Equity Firm)
$ 3.9 Billion.

CIO	Tony Young
CMO	Matt Fairbankes
CRO	Micheal Valentine
CEO	Kris Hagerman
CLO	Rashmi Garde.
Head H.R (IND)	Asha Poluru
MD (IND)	Sunil Sharma
Vice-Pre2 (IND)	Bibhuti Kar

~~SOPHOS~~ ->
Garima Maheshwari (Manager Talent Accusition)

Sophos : It is computer sec. developer it may also refered as agathos kai Sophos which is used by plato meaning good and wise sage. which is a philosophical term for someone who has attend wisdom.

- founded - 1985, 1989 - first virus scanning engine.

It is a world leader in IT Sec and data protection.

Sophos headquakers is in Oxford, UK

Sophos endpoint : Intercept X
" firewall : Nextgen
MDR : Managed Detection Response

Product : Sophos central management console. (SCMC)

A single web app for all your all sophos security connects and sync endpoints to the firewalls.

It provides on server, switch, CSPM (Cloud sec post. manage) mobile email, wireless, phish threat, encrypt^{n}, zero trust network access, cloud native sec, factory.

Endpoint : XDR, server, Mobile encryption.

Network : firewall, wireless, switch, ztna

Cloud : CNS, workload protection

Email : Antiphishing, Email protection

News :

1) On Jan 31, 2022 old sophos SSLVPN clients ends because before 1 year they launched new and greatly improved sophos connect v2 vpn client.

2) ~~Sph~~ sophos new firewall OS version v19MR1.

sophos antivirus is updated to 10.8.13.42

↳ Jan hruska and Peter Lammer founded sophos.

↳ SfOS is OS of Sophos XG firewall

Topic (geeksforgeeks)

1) AD ✓
2) IDS ✓
3) IPS ✓
4) Firewall ✓
5) Network Security ✓
6) Common Internet protocols. ✓
7) IPSec, Tunnelling ✓
8) Windows, Linux
9) Port Numbers ✓
10) DMZ ✓
11) Stateless, Stateful.
12) Virus ✓
13) OSI Model. ✓
14) Intercept X
15) XDR
16) SASE

(4) → accept/deny IP.

ACL → Active control list

cons.

↳ Dont know the nature of packets.
↳ Doesnot have the capacity to keep threats out of the network.

↳ firewall match the network traffic against the rule set defined in table.

↳ TCP, UDP and ICMP.

↑ ↑

↓ ↑

Source & Destination Address, Port No

~~Port~~ type code (identify the purpose of packets)

~~No.~~

If no rules are defined it will ~~you~~ use this.

↳ Every firewall have "default policies".

↑

Accept, Reject, drop

↳ firewall generations:

(1) first generation-Packet filtering firewall.

↳ first 3 layers are used.

(2) Second generation-Stateful Inspection Firewall:

↳ eg: TCP streams, filtering decisions would not only be based on defined rules but also on packet history in the state table.

They are used as NAT.
Network add. Translation,

(3) Thired generation - Application Layer:

↳ It Inspect and filter the packets on any OSI layer upto the application layer.

↳ It ables to block specific content, which protocals are being misused.

↳ These are hosts runs proxy server.

(4) Next Generation Firewall (NGFW):

↳ They are being deployed to stop Modern Security breaches.

↳ Contains Deep Packet Inspection, App Ins., SSL | SSH Ins., etc.

Firewall types:

1) Host-Based: Installs on each network nodes.

↳ It is a software APP, as a part of OS.

(2) Network based : It function on the network ~~layer~~.
↳ protect the internal network by filtering traffic using defined rules.

(6) Common Internet / Network protocol

TCP	FTP	ARP	RDP
IP	HTTP	DNS	SIP
UDP	HTTPS	FTP/S	SMB
POP	Telnet	HTTPS	SMTP
SMTP	Gopher	IMAP	SNMP
		POP3	SSH
		TELNET	VNC

(7)

IP Sec (IP Security):

↳ It is Internet Engineering Task force (IETF) between 2 communica - tion points across the IP network that gives CIA.

User:

↳ encrypt app layer data.

↳ Provides security for routers sendin routing data across the public internet.

↳ Protect network data by setting up circuit using IPsec tunnelling in which all data is being sent between two enpoints which are encrypted with VPN.

IP sec Components:

1) ESP (Encapsulating Security Payload):
2) Authentication Header (AH):
3) IKE (Internet key Exchange):

Page :
Date : / /

Network diagram :

↓

gives info about network and its architechture to an attecker

↳ It shows logical or physical path to a potential target.

Tools :

↳ Network Topology mapper

↳ It discovers a network and provide comprehensive network diagram.

↳ Op Manager
↳ Network view
↳ LAN State Pro
↳ nmap.

Proxy : → You can create a controlling environment.

↳ Proxy is the system that stands in between the attacker and the target.

↳ It play Imp role in the network.

↳ It helps the scanners to hide their Identity.

Page :
Date : / /

Proxy servers : It serves as an intermediary for connecting with other computers.

Proxy Chaining : It forwards traffic to the next proxy server.

Proxy Switcher
Proxy Workbench
Proxy TOR
Proxy Cyberghost

for Mobile

Proxy Droid
Net Shade

Anonymizers :

↳ It is a tool that completely hides or removes identity related information to make the activity untraceable.

↳ It Minimize Risk.
Identity theft prevention.
Bypass restrictions and censorship
Untraceable activity on the Internet.

Tails is a live OS that user can start on any computer for pendrive.