FIREWALL SIZING SHEET AND NOTES :

[A] INTERNET CONNECTIONS :

SR	ISP	CONNECTION TYPE[Static/ pppoe etc]	Download/ Upload Speed	Remarks – Please mention whether you require any policy routing, auto failover etc. [Applicable only if you have multiple internet connections]

[B] INTERNAL OFFICE CABLING

WHETHER YOU HAVE PERFECT INTERNAL CABLING IS COMPLETE ? YES / NO
[**IF THE ANSWER IS NO, WE ADVICE YOU TO COMPLETE THE TASK ON TOP PRIORITY**]

(PERFECT CABLING : PREFERRED MINIMUM STANDARD FOR CABLING IS CAT 6, ALL CONNECTOR LOCKS ARE INTACT, STANDARD RJ 45 CRIMPING IS DONE. ALL CABLES ARE NEAT AND TROUBLE FREE., NO CROSS-TALK ETC)

[C] PROPOSED DEVICES BEHIND FIREWALL

1. **DESKTOPS**

SR	SHORT CONFIG/ OS	MAC ID	USED BY/ PHYSICAL LOCATION	WHETHER YOU REQUIRE MAC BINDING? YES / NO	PROPOSED IP

2. **LAPTOPS / NOTEBOOKS**

SR	SHORT CONFIG/OS	ETHERNET MAC ID	WIFI MAC ID	USED BY	MAC BINDING Y/ N	PROPOSED IP

3. **SERVERS / VIRTUAL MACHINES**

SR	SHORT CONFIG / OS	ETHERNET MAC ID	ACCESSED BY# OF PEOPLE	VLAN REQD ? Y/ N	PHYSICAL LOCATION	SERVICE PORTS	ANY PORT FORWARDING / REVERSE PROXY REQD ? Y/N	STATIC PRIVATE IP

4. HAND HELD / MOBILE DEVICES

SR	SHORT – MAKE / MODEL	WIFI MAC ID	USED BY	PROPOSED IP	REMARKS

5. WIFI ROUTERS / ACCESS POINTS / CAMERA / NVR / BIO-MATRIC DEVICES

SR	SHORT – MAKE / MODEL	WIFI MAC ID	PHYSICAL LOCATION	STATIC PRIVATE IP	REMARKS

FIREWALL SIZING SHEET AND NOTES :

6. **ETHERNET SWITCHES**

SR	MAKE / MODEL	SWITCH TYPE UN-MANAGED / MANAGED / POE ETC	USER ID/ PASSWORD – WHETHER AVAILABLE OR NOT ? Y/N	# OF PORTS /SPEED	REMARKS

NOTES : IN CASE OF MULTIPLE WAN, AUTO FAIL OVER IS POSSIBLE. LOAD BALANCING IS ALSO POSSIBLE BUT NOT VERY ADVISABLE. INSTEAD, WE PROPOSE POLICY BASED ROUTING AS MANY SITES DO NOT WORK PROPERLY [ESPECIALLY GOVT, BANK SITES, RESERVATIONS SITES – AS THEY NOTICE CHANGE OF IP AND STOP FUNCTIONING]

CUSTOMER IS SUPPOSED TO BE READY WITH USER ID / PASSWORD ETC FOR WAN CONNECTIONS , IF TERMINATED THRU RJ45 CABLE ON WIFI.

IF CUSTOMER WANT TO CONTROL FILTERING, SPEED ETC, MAC BINDING + STATIC PRIVATE IP IS REQUIRED.

[D] VLAN

DO YOU NEED VLAN FACILITY ? Y / N [REQUIRES ALL SWITCHES ARE MANAGED – MINIMUM L2 LEVEL – MANAGED SWITCHES ARE COSTLY - CONFIGURING THESE SWITCHES REQUIRES EXPERTISE AND YOU MAY REQUIRE HELP FROM EXISTING VENDORS] VLAN IS GOOD FOR NETWORK BI-FURCATION.

VLAN DETAILS

SR	DEPARTMENT	VLAN NUMBER	# OF DEVICES FOR VLAN	ANY CROSS TRAFFIC REQUIRED BETWEEN VLAN	REMARKS

[E] VPN

DO YOU REQUIRE TO CONNECT INTERNAL ACCESS ? POSSIBLE THRU VPN SERVER – CONFIGURED IN FIREWALL. BASIC REQUIREMENT TO HAVE INCOMING VPN IS TO HAVE AT-LEAST ONE PUBLIC IP.

 # OF VPN CONNECTIONS REQUIRED =

NOTES : VPN USERS REQUIRES TO INSTALL VPN CLIENT + VPN CONFIGURATION ON THEIR DEVICES WHILE USING VPN.

SITE TO SITE CONNECTIVITY IS POSSIBLE IF YOU HAVE MULTIPLE OFFICES ACROSS GLOBE. [IPSEC] BUT YOU NEED TO HAVE 1. UNIQUE PRIVATE IP RANGE IN EACH OFFICE 2. YOU NEED TO HAVE FULL ACCESS 3. FIREWALL AT EACH PLACE SUPPORTING IPSEC. WITHOUT THESE DETAILS IPSEC VPN IS NOT POSSIBLE.

[F] YOU NEED CLASSIFY DEVICES WHERE YOU REQUIRED UNRESTRICTED INTERNET AND WHICH DEVICES ARE TO BE BLOCKED.

[G] USING FIREWALL CERTAINLY BLOCKS MOST OF THE INTERNET THREATS BUT NOT ALL.

[H] ONE NEED TO MONITOR OUTGOING TRAFFIC RATHER THAN INCOMING TRAFFIC AS INCOMING TRAFFIC IS BLOCKED UNLESS YOU OPEN A SPECIFIC PORT/S.

FIREWALL SIZING SHEET AND NOTES :

YOU CAN CHOOSE IP RANGES FROM FOLLOWING IP RANGES AVAILABLE IN PRIVATE IP RANGE SPACE.

Public IP Range	Private IP Range	Subnet Mask	# of Networks	# of Hosts per Network	
Class A	1.0.0.0 to 127.0.0.0	10.0.0.0 to 10.255.255.255	255.0.0.0	126	16,777,214
Class B	128.0.0.0 to 191.255.0.0	172.16.0.0 to 172.31.255.255	255.255.0.0	16,382	65,534
Class C	192.0.0.0 to 223.255.255.0	192.168.0.0 to 192.168.255.255	255.255.255.0	2,097,150	254

ALL OTHER IP'S ARE CONSIDERED TO BE PUBLIC IP EXCEPT 100.64. 0.0 to 100.127. 255.255 WHICH IS IS CGNAT NETWORK. - NON ROUTABLE [PLEASE CHECK WITH ISP REGARDING THIS . IF YOUR WAN CONNECTION IP FALLS IN CGNAT, YOU WILL NOT ABLE TO USE PORT FORWARDING , VPN, SITE TO SITE ETC - MOST OF THE RESIDENTIAL CONNECTIONS ARE ON CGNAT NETWORK. PLEASE BE AWARE OF THIS]

YOU WILL ALSO NEED TO DECIDE ADMIN USER ID + SECURED PASSWORD FOR FIREWALL MANAGEMENT.

ALL THESE INFORMATION IS NECESSARY FOR NEAT IMPLEMENTATION OF FIREWALL.

CUSTOMERS ARE ADVISED TO HAVE THIS INFORMATION READY AT THE TIME OF IMPLEMENTATION.

CAREFUL PLANNING IS MUST AT CUSTOMER'S END. THIS IS TO BE DONE BY CUSTOMER ONLY.

IF YOU INTEND TO USE WIFI, WE ADVISE TO USE ACCESS POINT OVER SIMPLE WIFI ROUTERS.

WIFI ROUTERS HAS A VERY LIMITED CAPACITY AND OFTEN FAIL.

IDS / IPS IMPLEMENTATION REQUIRES OBSERVATION/ ANALYSIS OF INTERNAL TRAFFIC BY THE CUSTOMER.

FIREWALL SIZING SHEET AND NOTES :

1. Open source – No additional licences required FOR UPDATES.
2. Unlimited Users / Groups.
3. Support 1 Gbps, 2.5 Gbps DEPENDING ON THE APPLIANCE.
4. Setup as you desire...
5. Multi Wan Support
6. Load Balancing of Wan connections
7. Auto switch over when one link is down.
8. Full blown Vlan Support
9. Supports Intel / AMD based processor
10. Low on Hardware requirements
11. Blocks all incoming ports out of box.
12. A stateful firewall is a network-based firewall that individually tracks sessions of network connections traversing it.
13. IP/DNS-based filtering can block web traffic from entire countries, one mechanism for stopping cyber criminals from attacking your business.
14. Anti spoofing detects packets with false addresses which leads to increased security.
15. Flexible Firewall rules. Custom rules supported.
16. Supports Link Aggregation.
17. Built on a specialised and hardened operating system.
18. Full support for VPN / IPSec / Wireguard [No limits] **
19. Captive Portal for WiFi / Authentication before user
20. Dynamic Routing.
21. Bandwidth Control
22. Data Privacy
23. Inbound and Outbound NAT **
24. Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) analyzes packets as well, but can also stop the packet from being delivered, helping to halt the attack.
25. Easy website / url blocking
26. Web based management.
27. Proxy and reverse proxy.
28. Full insite reports.
29. Auto Backup on cloud.
30 **World's most used firewall.**

**** SOME FEATURES COMES WITH PRE-REQUISITES.**