SLNo	Guidance	Compliance
	Firewalls	
1	Update the router to the latest firmware version.	
2	Enable stateful packet inspection (SPI).	
3	Disable ping (ICMP) response on WAN port.	
4	Disable UPnP (universal plug-and-play).	
5	Disable IDENT (port 113).	
6	Disable remote management of the router.	
7	Change the default administrator password.	
8	The settings for a firewall policy should be as specific as possible. Do not use 0.0.0.0 as an address.	
9	Check for incoming/outgoing traffic security policy	
10	Check for firewall firmware / OS updates	
11	Allow only HTTPS access to the GUI and SSH access to the CLI	
12	Re-direct HTTP GUI logins to HTTPS	
13	Change the HTTPS and SSH admin access ports to non-standard ports	
14	Restrict logins from trusted hosts	
15	Set up two-factor authentication for administrators	
16	Create multiple administrator accounts	
17	Modify administrator account lockout duration and threshold values	
18	Check if all management access from the Internet is turned off, if it does not have a clear business need. At most, HTTPS and PING should	

	be enabled.	
19	Ensure that your SNMP settings are using SNMPv3 with encryption and configure your UTM profiles	
20	All firewall policies should be reviewed every 3 months to verify the business purpose	

	Routers	
1	Do not use Default password for your router	
2	Check if the router block access to a modem by IP address	
3	Ensure that router admin gets an alert when a new device joins the network	
4	Most routers let you disable UPnP on the LAN side	
5	Enable port forwarding and IP filtering for your router	
LOCAL ADMINISTRATION		
6	Check if the router supports HTTPs, in some routers it is disabled by default	
7	If HTTPS is supported, can admin access be limited exclusively to HTTPS?	
8	Check if the TCP/IP port used for the web interface can be changed	
9	To really prevent local admin access, limit the LAN IP address to a single IP address that is both outside the DHCP range and not normally assigned.	
10	Check if the admin access can be limited to Ethernet only	
11	Check if the router access can be restricted by SSID and/or by VLAN	
12	The router should not allow multiple computers to logon at the same time using the same userid	

13	Check if there is some type of lockout after too many failed attempts to login to the web interface	
ROUTER		
17	**Inbound WAN:** What ports are open on the WAN/Internet side? The most secure answer is none and you should expect any router not provided by an ISP to have no open ports on the Internet side. One exception is old school Remote Administration, which requires an open port. Every open port on the WAN side needs to be accounted for, especially if the router was provided by an ISP; they often leave themselves a back door. The Test your Router page links to many websites that offer firewall tests. That said, none of them will scan all 65,535 TCP ports or all 65,535 UDP ports. The best time to test this is before placing a new router into service.	
18	**Inbound LAN:** What ports are open on the LAN side? Expect port 53 to be open for DNS (probably UDP, maybe TCP). If the router has a web interface, then that requires an open port. The classic/standard utility for testing the LAN side firewall is nmap. As with the WAN side, every port that is open needs to be accounted for.	
19	**Outbound:** Can the router create outgoing firewall rules? There are	

	all sorts of attacks that can be blocked with outgoing firewall rules. Generally, consumer routers do not offer outbound firewall rules while business class routers do. In addition to blocking, it would be nice if the blocks were logged for auditing purposes. Note however, that devices connected to Tor or a VPN will not obey the outbound firewall rules.	

	Switches	
1	Check if the latest firmware is used.	
2	Check the switch's user guide's for security features and see if the required ones have been implemented properly.	
3	Create an Enable Secret Password Encrypt Passwords on the device	
4	Use an external AAA server for User Authentication	
5	Create separate local accounts for User Authentication Configure Maximum Failed Authentication Attempts	
6	Restrict Management Access to the devices to specific IPs only	
7	Enable Logging for monitoring, incident response and auditing. You can enable logging to an internal buffer of the device or to an external Log server.	
8	Enable Network Time Protocol (NTP) - You must have accurate and uniform clock settings on all network devices in order for log data to be stamped with the correct time and timezone.This will help tremendously in incident handling and proper log monitoring and correlation.	
9	Use Secure Management Protocols if possible	

10	Restrict and Secure SNMP Access	

Reference: SANS & NIST & CIS Benchmarks