5 IT-NETWORKING POINTS TO REMEMBER FOR YOUR SOC ANALYST INTERVIEW
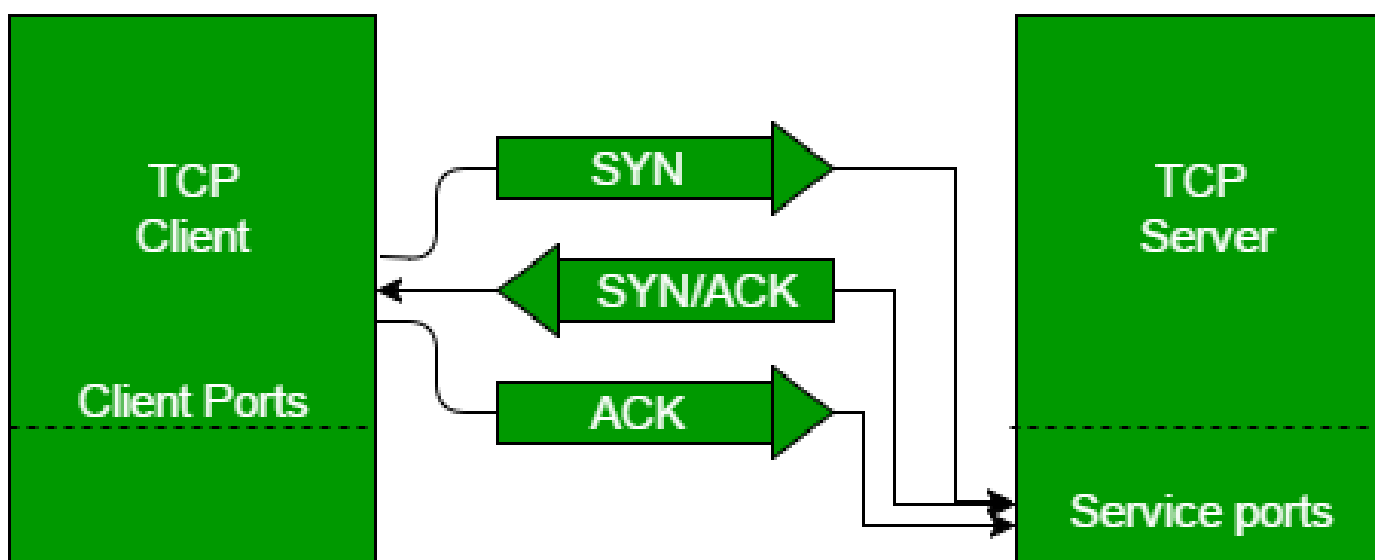
1
TCP/IP

- TCP/IP Flags
- TCP/IP 3-way handshake
- TCP vs UDP

WELL-KNOWN PORTS

- HTTP/HTTPS
- SSH
- DNS
- FTP

Common Ports

Top 100 TCP & UDP Ports

Port Number	Service	Protcol	Port Number	Service	Protcol
20-21	FTP	tcp	1337	menandmice-dns	tcp
22	SSH	tcp	1194	OpenVPN	tcp/udp
23	Telnet	tcp/udp	1433-1434	Microsoft SQL	tcp/udp
25	SMTP	tcp	1701	L2TP	udp
43	whois	tcp	1723	MS PPTP	tcp
49	TACACS	tcp/udp	1725	MS PPTP	tcp
53	DNS	tcp/udp	1741	cisco-net-mgmt	tcp
67-68	DHCP/BOOTP	udp	1812-1813	RADIUS	udp
69	TFTP	udp	1985	HSRP	tcp
79	Finger	tcp	2000	Cisco SCCP	tcp/udp
80	HTTP	tcp	2002	Cisco ACS	tcp
82	xfer	tcp	2049	NFS	tcp
83	mit-ml-dev	tcp	2082-2083	cPanel	tcp
88	Kerberos	tcp	2100	Oracle XDB	tcp
110	POP3	tcp	2087	eli	tcp

3
OSI LAYER

- OSI Layer
- Purpose of Each Layer

7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

STATEFUL FIREWALL

- What is a Stateful firewall?
- Stateful vs Stateless firewall
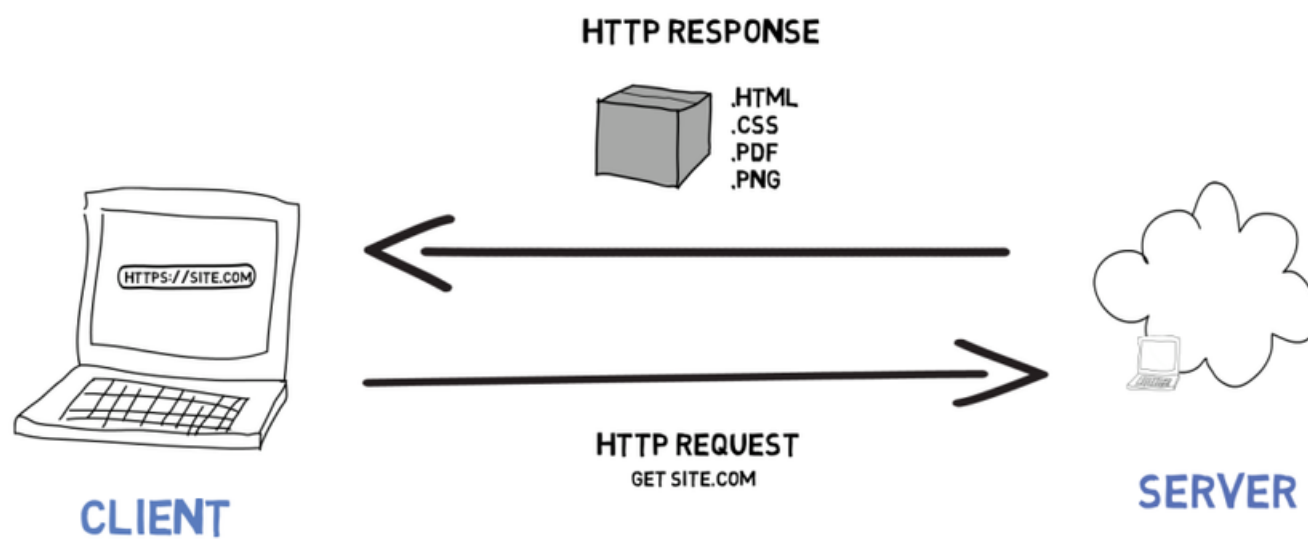- What is Next-gen Firewall?

STATE TABLES

STATE INSPECTION ENGINE

INTERNET

CLIENT

SERVER

STATEFUL INSPECTION FIREWALL
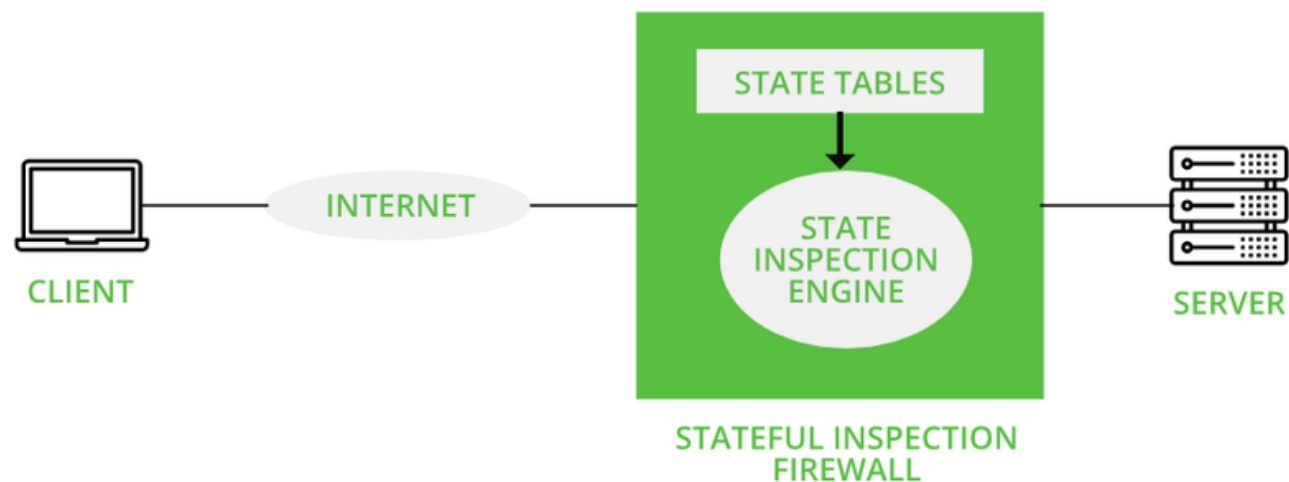
INTERNET

What happens when you type www.google.com on your browser?(Try to go as deep as possible)

HOW THE INTERNET WORKS