1. Co je to firewall a jaké jsou jeho hlavní funkce?

Firewall je bezpečnostní zařízení nebo program, který slouží k ochraně sítě a systémů před neoprávněným přístupem, útoky a škodlivým provozem. Jeho hlavní funkce zahrnují:

Filtrace síťového provozu: Firewall kontroluje a filtruje příchozí a odchozí síťový provoz na základě definovaných pravidel a politik. To umožňuje povolit nebo blokovat specifické typy provozu na základě různých kritérií, jako jsou zdrojová a cílová adresa, porty, protokoly apod.

Ochrana před útoky: Firewall detekuje a blokuje potenciálně škodlivý provoz, jako jsou DoS (Denial of Service) útoky, směrování falešných paketů, pokusy o prolomení zabezpečení apod.

NAT (Network Address Translation): Firewall může provádět překlad IP adres (NAT), což umožňuje sdílet veřejnou IP adresu mezi více zařízeními v privátní síti.

VPN (Virtual Private Network): Firewall může podporovat vytváření bezpečných VPN spojení pro vzdálený přístup nebo propojení vzdálených sítí.

2. Co je to proxy firewall a jaké jsou její funkce?

Proxy firewall je specifický typ firewallu, který slouží jako prostředník mezi interní sítí a vnějšími sítěmi. Jeho hlavní funkce zahrnují:

Filtrace síťového provozu: Proxy firewall provádí inspekci a filtraci příchozího a odchozího provozu na základě aplikací nebo protokolů. To znamená, že analyzuje obsah provozu a rozhoduje o povolení nebo blokování na základě aplikace nebo protokolu, které provoz využívá.

Cache a optimalizace: Proxy firewall může ukládat do mezipaměti (cache) často používané webové stránky nebo data, což umožňuje rychlejší a efektivnější přístup k nim.

Anonymizace a ochrana identity: Proxy firewall může skrývat interní adresy a informace o klientech, čímž zajišťuje vyšší anonymitu a bezpečnost.

3. Jak funguje VPN typu bod bod?

VPN (Virtual Private Network) typu bod-bod umožňuje vytvoření zabezpečeného spojení mezi dvěma bodovými uzly (např. mezi dvěma pobočkami nebo mezi dvěma síťmi). Při použití tohoto typu VPN jsou obě strany připojeny přes internet nebo jinou veřejnou síť, ale komunikace mezi nimi je šifrovaná a zabezpečená. VPN typu bod-bod zajišťuje soukromost a bezpečnost dat přenášených mezi těmito dvěma body.

4. Jak funguje VPN typu klient server?

VPN (Virtual Private Network) typu klient-server umožňuje klientovi (např. vzdálenému pracovníkovi nebo uživateli) připojit se do privátní sítě nebo intranetu pomocí veřejné sítě (např. internetu). Klient se připojuje na server VPN, který funguje jako brána do privátní sítě. Veškerá komunikace mezi klientem a serverem VPN je šifrovaná a zabezpečená, což zajišťuje soukromí a bezpečnost dat klienta v rámci privátní sítě.

5. Jak lze obejít NAT?

Obejítí NAT (Network Address Translation) je možné pomocí techniky nazvané "port forwarding" nebo "port mapping". Při použití NAT se veřejná IP adresa překládá na privátní IP adresu, což ztěžuje přímý přístup z venku do zařízení v privátní síti. Port forwarding umožňuje přesměrování specifických portů na interní IP adresu a port, což umožňuje externímu zařízení připojit se k určitému zařízení v privátní síti. Tímto způsobem lze překonat omezení NAT a umožnit komunikaci zvenčí s konkrétním zařízením v privátní síti.

6. Co je to SNMP (simple network management procol) a kdo s kým o čem komunikuje pomocí SNMP?

SNMP (Simple Network Management Protocol) je protokol používaný pro správu a monitorování síťových zařízení. Pomocí SNMP mohou správci sítě získávat informace o stavu zařízení, monitorovat provoz a provádět různé správné úkony. SNMP pracuje na základě komunikace mezi správcem a síťovými zařízeními, která jsou vybavena SNMP agentem. Správce pošle dotazy na zařízení pomocí SNMP protokolu a obdrží odpovědi obsahující požadované informace.

7. Jaké jsou důvody použití firewall a kde se vyplatí používat?

Důvody použití firewallu jsou:

Zajištění bezpečnosti sítě: Firewall pomáhá chránit síť a systémy před neoprávněným přístupem, útoky a škodlivým provozem.

Kontrola a filtrování síťového provozu: Firewall umožňuje správcům sítě definovat pravidla a politiky pro povolení nebo blokování specifického síťového provozu, což pomáhá omezit rizika a zabezpečit síť.

Monitorování síťového provozu: Firewall může sledovat a zaznamenávat síťový provoz, což umožňuje analýzu a detekci neobvyklých nebo podezřelých aktivit.

VPN a vzdálený přístup: Firewall může podporovat vytváření zabezpečených VPN spojení pro vzdálený přístup k síti nebo propojení vzdálených sítí.

Ochrana před škodlivým provozem: Firewall detekuje a blokuje škodlivý provoz, jako jsou viry, spyware, útoky DoS atd.

Firewall je vhodné používat na všech místech, kde je potřeba chránit síť a systémy před neoprávněným přístupem nebo škodlivým provozem, například v podnicích, organizacích, datových centrech, ale také u domácích uživatelů pro zajištění bezpečnosti jejich domácí sítě.

8. Jaké jsou úkoly transportní vrstvy?

Úkoly transportní vrstvy zahrnují:

Segmentace a reassemblování dat: Transportní vrstva rozděluje velká datová bloky na menší segmenty pro přenos po síti a na příjemné straně opět skládá segmenty do původních datových bloků.

Multiplexování: Transportní vrstva umožňuje více aplikacím sdílet síťové prostředky pomocí multiplexování. Každá aplikace je identifikována pomocí portu nebo socketu a transportní vrstva zajistí, že příslušné segmenty jsou správně doručeny do příslušných aplikací.

Řízení přenosu: Transportní vrstva reguluje přenos dat mezi zdrojovým a cílovým uzlem, aby zajistila spolehlivost a efektivitu přenosu. To zahrnuje mechanismy řízení toku, řízení přetížení a řízení chyb.

9. Jaká je koncepce transportní vrstvy v RM ISO/OSI?

Koncepce transportní vrstvy v RM ISO/OSI se zaměřuje na poskytování spolehlivého a transparentního přenosu dat mezi koncovými systémy. Transportní vrstva se stará o segmentaci a řízení přenosu dat, zajišťuje spolehlivost přenosu a správu chyb. Důležitými prvky transportní vrstvy v rámci RM ISO/OSI jsou transportní jednotky dat (TSDU), které představují datové bloky předané mezi koncovými systémy.

10. Jaká je koncepce transportní vrstvy v TCP/IP?

Koncepce transportní vrstvy v TCP/IP je založena na dvou hlavních protokolech: TCP (Transmission Control Protocol) a UDP (User Datagram Protocol). TCP poskytuje spolehlivý a spojovaný přenos dat, zatímco UDP poskytuje nespojovaný a nespolehlivý přenos dat. Transportní vrstva v TCP/IP se také stará o multiplexování pomocí portů a poskytuje mechanismy řízení toku a řízení přenosu.

11. K čemu slouží body SAP (RM ISO/OSI) a porty (TCP/IP)?

Body SAP (Service Access Point) v RM ISO/OSI slouží jako rozhraní mezi transportní a vyššími vrstvami. Porty v TCP/IP představují identifikátory konkrétních aplikací nebo služeb, které komunikují přes transportní vrstvu. Tyto porty se používají pro multiplexování a demultiplexování datového provozu mezi aplikacemi.

12. K čemu slouží konvence o době známých portech a jakou má podobu?

Konvence o době známých portech v TCP/IP je představena pomocí tzv. Well-Known Ports. Jedná se o standardizované číselné hodnoty portů od 0 do 1023, které jsou přiděleny určitým aplikacím nebo službám. Například port 80 je standardně používán pro HTTP (Hypertext Transfer Protocol), port 443 pro HTTPS (Hypertext Transfer Protocol Secure) atd. Tímto způsobem je umožněno jednoznačné identifikování specifických aplikací nebo služeb na základě použitého portu.

13. Jaký je vztah mezi porty a sockety (v TCP/IP)?

Porty a sockety v TCP/IP mají úzkou spojitost. Port je číselný identifikátor, který identifikuje konkrétní aplikaci nebo službu v rámci transportní vrstvy. Socket je kombinace IP adresy a portu, která představuje konkrétní koncový bod komunikace v síti. Socket je vytvořen na každé straně (odesílatel a příjemce) komunikace a umožňuje přenášet data mezi aplikacemi.

14. Naznačte příklad práce se sockety při spojované komunikaci (v TCP/IP)

Při spojované komunikaci v TCP/IP probíhá práce se sockety následovně:

Klient vytvoří socket a naváže spojení s určeným serverem pomocí jeho IP adresy a portu.

Server přijímá příchozí spojení a vytváří nový socket pro komunikaci s konkrétním klientem.

Klient a server vyměňují data přes své sockety a poté ukončí spojení.

Tento proces zajišťuje spojovanou a spolehlivou komunikaci mezi klientem a serverem.

15. Naznačte příklad práce se sockety při nespojované komunikaci (v TCP/IP)

Při nespojované komunikaci v TCP/IP se pracuje se sockety následovně:

Odesílatel vytvoří socket a přiřadí mu příslušnou IP adresu a port.

Odesílatel odešle datagram obsahující data a cílovou IP adresu a port příjemce.

Příjemce přijme datagram, získá data a identifikuje zdrojovou IP adresu a port.

Příjemce může vytvořit socket pro odpověď a poslat odpověď na danou IP adresu a port odesílatele.

Tímto způsobem je realizována nespojovaná komunikace mezi odesílatelem a příjemcem pomocí sockety.

16. Jakým způsobem (podle čeho) volí protokol TCP velikost časového limitu (timeout-u)

Velikost časového limitu (timeout-u) v protokolu TCP je volena na základě odhadu RTT (Round-Trip Time), což je doba potřebná pro odeslání paketu od odesílatele, přenos přes síť a doručení paketu zpět k odesílateli. Protokol TCP sleduje RTT a dynamicky upravuje timeout tak, aby byl dostatečně dlouhý na příjem odpovědi, ale zároveň dostatečně krátký na minimalizaci zpoždění v případě ztráty paketu nebo chybného doručení.

17. Jakým způsobem pracuje protokol TCP s bytovým proudem (při zajišťování spolehlivého přenosu)?

Protokol TCP pracuje s bytovým proudem při zajišťování spolehlivého přenosu tím, že rozděluje data na menší segmenty a přenáší je po síti. Odesílatel a příjemce používají číslování sekvencí bytů a potvrzování, aby zajistili správné a kompletní doručení dat. Pokud dojde k chybě v přenosu (např. ztráta paketu), protokol TCP automaticky znovu odesílá poškozené nebo ztracené segmenty, aby bylo zajištěno spolehlivé doručení dat.

18. Jakým způsobem předchází protokol TCP zahlcení?

Protokol TCP předchází zahlcení (congestion) tím, že používá mechanismy řízení toku a řízení přetížení. Řízení toku umožňuje odesílateli regulovat rychlost přenosu dat na základě kapacity sítě a schopností příjemce. Řízení přetížení zahrnuje sledování stavu sítě a zátěže, identifikaci příznaků zahlcení a přizpůsobení přenosové rychlosti tak, aby se zabránilo zahlcení sítě.

19. Jakým způsobem lze zajistit podporu QoS (nejen na úrovni transportní vrstvy)?

Podpora QoS (Quality of Service) může být zajištěna na různých úrovních sítě, včetně transportní vrstvy. K zajištění QoS na úrovni transportní vrstvy může protokol TCP využívat mechanismy řízení toku, řízení přetížení a prioritizace dat. Tyto mechanismy umožňují regulovat přenosovou rychlost, minimalizovat zpoždění a zajistit prioritu pro určité typy dat, jako jsou hlasová nebo videokonference.

20. Jaké jsou požadavky aplikací na QoS? Rozdělte alespoň na "datové" a "multimediální" aplikace.

Požadavky aplikací na QoS se liší v závislosti na jejich povaze a požadavcích. Datové aplikace (např. e-mail, webové prohlížeče) obvykle vyžadují spolehlivý a rychlý přenos dat s minimálním zpožděním a ztrátou. Multimediální aplikace (např. hlasové a videohovory, streamování) vyžadují nízké zpoždění, nízkou ztrátu a vyšší přenosovou rychlost pro zachování kvality a plynulosti přenosu multimediálních dat. Tyto aplikace také často vyžadují prioritu přenosu, aby bylo dosaženo co nejlepšího uživatelského zážitku.