

Snelgids Netwerken & Beveiliging: Kernarchitectuur, Protocollen en Verdedigingsmechanismen

Kernarchitectuur, Protocollen, Verkeersstromen en Verdedigingsmechanismen

Een compact en diepgaand Nederlandstalig naslagwerk voor IT- en cybersecurityprofessionals. Behandelt de fundamentele lagen van het OSI- en TCP/IP-model, subnettering, poortarchitecturen, dynamische netwerkdiensten (DNS, DHCP, NAT) en defensieve netwerktechnologieën inclusief firewalls, IDS/IPS, VPN-implementaties en draadloze beveiliging.

- | | |
|---|---|
| 01 Architectuurmodellen: OSI-model versus TCP/IP-stack | 02 IP-Adressering en Subnettering (IPv4 & IPv6) |
| 03 Cruciale Netwerkpporten & Transportprotocollen | 04 Kerndiensten: DNS Resolutie, DHCP DORA en NAT |
| 05 Netwerksegmentatie & Firewallarchitectuur | 06 Inbraakdetectie en -preventie (IDS vs. IPS) |
| 07 Versleutelde Verbindingen: VPN-Protocollen | 08 Draadloze Netwerkbeveiliging (Wi-Fi) |
| 09 Netwerkaudit & Segmentatie Verificatiechecklist | |



Architectuurmodellen: OSI-model versus TCP/IP-stack

Moderne datacommunicatie steunt op gelaagde referentiemodellen die bepalen hoe gegevens worden verpakt, gerouteerd en afgeleverd. Het theoretische OSI-model (7 lagen) biedt een conceptuele scheiding van taken, terwijl de praktische TCP/IP-stack (4 lagen) de operationele standaard van het internet vormt. Tijdens transmissie voegt elke laag eigen headerinformatie toe (encapsulatie), resulterend in een specifieke Protocol Data Unit (PDU) per laag.

- Laag 7 (Applicatie), Laag 6 (Presentatie) en Laag 5 (Sessie) vallen binnen TCP/IP samen onder de Toepassingslaag (PDU: Data). Protocollen: HTTP/HTTPS, DNS, SSH, DHCP.
- Laag 4 (Transport): Verantwoordelijk voor end-to-end communicatie en poortnummering (PDU: Segment voor TCP, Datagram voor UDP).
- Laag 3 (Netwerk/Internet): Verantwoordelijk voor logische adressering en routing over subnetten (PDU: Pakket/Package). Protocollen: IPv4, IPv6, ICMP.
- Laag 2 (Datalink): Fysieke adressering via MAC-adressen en framing binnen lokale netwerksegmenten (PDU: Frame). Protocollen: Ethernet (802.3), Wi-Fi (802.11), ARP.
- Laag 1 (Fysiek): Transmissie van ongeformatteerde binaire signalen via koper, glasvezel of radiogolven (PDU: Bits).

Encapsulatie & Decapsulatie

Bij verzending bouwt een host een frame op van boven naar beneden: Data -> Segment (L4 poort) -> Pakket (L3 IP) -> Frame (L2 MAC) -> Bits. Aan de ontvangende kant analyseert en verwijdert elke laag de bijbehorende header (decapsulatie).



IP-Adressering en Subnetting (IPv4 & IPv6)

Subnetting deelt grotere netwerken op in kleinere, geïsoleerde broadcast-domeinen om verkeersstromen te optimaliseren en beveiligingsgrenzen af te dwingen. Classless Inter-Domain Routing (CIDR) definieert het aantal bits dat gereserveerd is voor het netwerkgedeelte versus het hostgedeelte.

- /24 Subnetmasker (255.255.255.0): Biedt 256 totale adressen, waarvan 254 bruikbaar voor hosts (1 netwerkadres, 1 broadcastadres gereserveerd).
- /28 Subnetmasker (255.255.255.240): Biedt 16 adressen (14 bruikbaar voor hosts); ideaal voor kleine DMZ-segmenten of managementinterfaces.
- /30 Subnetmasker (255.255.255.252): Biedt 4 adressen (2 bruikbaar); standaard voor point-to-point routerverbindingen.
- IPv4 Privéreeksen (RFC 1918): 10.0.0.0/8 (grote ondernemingen), 172.16.0.0/12 (middelgroot) en 192.168.0.0/16 (thuis/kantoor). Niet direct routeerbaar over het openbare internet.
- IPv6 Architectuur: 128-bits adressen in hexadecimale notatie (bijv. 2001:db8::/32). Maakt NAT voor adrestekort overbodig en gebruikt gestructureerde prefixen (/64 per subnet).

Subnetgrootte Berekenen

Het aantal beschikbare hosts in een IPv4-subnet wordt berekend met $2^{(32 - \text{CIDR})} - 2$. Voor /26 geldt $32 - 26 = 6$ bits; $2^6 = 64$ min $2 = 62$ bruikbare hostadressen.

Cruciale Netwerkpooorten & Transportprotocollen

Poortnummers (0-65535) bepalen welke applicatie of dienst op een doelhost een inkomend transportsegment ontvangt. Beveiligingsanalisten moeten gevestigde standaardpoorten direct kunnen koppelen aan hun functie en risicoprofiel.

- ☐ Poort 22 (TCP) - SSH (Secure Shell): Versleuteld beheer op afstand en veilige bestandsoverdracht via SFTP.
- ☐ Poort 53 (TCP/UDP) - DNS (Domain Name System): Domeinnaamomzetting. UDP voor standaard queries; TCP voor zone-transfers en antwoorden groter dan 512 bytes.
- ☐ Poort 80 (TCP) - HTTP: Onversleuteld webverkeer; kwetsbaar voor af luisteren en manipulatie.
- ☐ Poort 443 (TCP) - HTTPS: Webverkeer beveiligd met TLS-encryptie.
- ☐ Poort 3389 (TCP/UDP) - RDP (Remote Desktop Protocol): Grafisch extern beheer voor Windows; frequent doelwit van brute-force aanvallen.
- ☐ Poort 25 (TCP) SMTP, 110 (TCP) POP3, 143 (TCP) IMAP: Klassieke e-mailprotocollen (beveiligd via 587/465 voor SMTP, 995 voor POP3S, 993 voor IMAPS).

Poortblootstelling Beperken

Sluit poort 3389 (RDP) en poort 22 (SSH) altijd af van directe blootstelling aan het openbare internet. Ontsluit beheerinterfaces uitsluitend via een beveiligde VPN of bastion host.

🎯 Kerndiensten: DNS Resolutie, DHCP DORA en NAT

Een betrouwbare netwerkinfrastructuur leunt op geautomatiseerde naamomzetting, dynamische configuratie en adrestranslatie. Onderstaande stroomschema's tonen de exacte interacties tussen clients en infrastructuurcomponenten.



- DNS Resolutieproces: Client consulteert lokale cache -> Recursive Resolver raadpleegt Root Server (.) -> TLD Server (.nl) -> Authoritative Nameserver -> IP-adres geretourneerd en gecachet.
- DHCP DORA-onderhandeling: Discover (broadcast client) -> Offer (unicast/broadcast server aanbod) -> Request (client vraagt specifiek IP aan) -> Acknowledge (server bevestigt lease en netwerkparameters).
- Source NAT (SNAT): Vertaalt private interne IP's naar één publiek IP bij uitgaand verkeer.
- Port Address Translation (PAT): Vertaalt meerdere interne hosts naar één publiek IP door unieke bronpoorten toe te wijzen.
- Destination NAT (DNAT / Port Forwarding): Vertaalt inkomend verkeer op een publieke poort naar het interne private IP van een specifieke server.



Netwerksegmentatie & Firewallarchitectuur

Firewalls vormen de scheiding tussen vertrouwde en onvertrouwde netwerkzones. Afhankelijk van de inspectie laag variëren de detectiecapaciteiten en overhead drastisch.



Welk type firewalltechnologie is vereist voor het inspecteren van verdacht verkeer?



Verkeer gebruikt dynamische poorten of camoufleert kwaadaardige payloads via standaard HTTP/HTTPS (poort 80/443).

Zet een Next-Generation Firewall (NGFW) in met TLS-decriptie en applicatielaaginspectie (L7 DPI).



Strikte scheiding tussen interne subnetten op basis van gevestigde TCP-verbindingen zonder diepe contentanalyse.

Gebruik een Stateful Inspection Firewall om sessiestatus en TCP SYN/ACK-flags op Layer 4 te valideren.



Eenvoudige router-ACL's voor bulk-verkeersfiltering met minimale latency op core-switches.

Implementeer Stateless Packet Filtering via hardwarematige Layer 3/4 Access Control Lists (ACL's).

- Stateless Packet Filtering (L3/L4): Beoordeelt pakketten individueel op basis van statische regels (bron/doel-IP, poort). Geen context of sessiestatus; kwetsbaar voor geavanceerde spoofing.
- Stateful Inspection (L3-L5): Houdt een actieve status-tabel (state table) bij van TCP-handshakes en UDP-sessies. Laat uitsluitend inkomend verkeer toe dat behoort tot een legitiem geïnitieerde uitgaande verbinding.
- Next-Generation Firewalls (NGFW, L7): Inspecteert data tot in de applicatielaag (Deep Packet Inspection). Herkent applicaties ongeacht poortnummer, integreert URL-filtering, TLS-decodering en malware-analyse.
- Demilitarized Zone (DMZ): Geïsoleerd netwerksegment voor publiek toegankelijke servers (web, mail), gescheiden van het interne vertrouwde LAN via dubbele of meerpoorts firewalls.

Architectuurprincipe: Bastion Host

Een bastion host is een speciaal geharde server die direct is blootgesteld aan vijandig verkeer (bijvoorbeeld in een DMZ). Alle overbodige software en services zijn uitgeschakeld om het aanvalsoppervlak tot een minimum te beperken.

🎯 Inbraakdetectie en -preventie (IDS vs. IPS)

Intrusion Detection Systems (IDS) en Intrusion Prevention Systems (IPS) analyseren netwerkstromen op handtekeningen van bekende aanvallen en afwijkend gedrag (anomalieën). De fysieke en logische positionering bepaalt de verdedigingskracht.

- ☐ IDS (Passief / Out-of-band): Ontvangt een kopie van het verkeer via SPAN/mirror-poorten of netwerk-TAPs. Signaleert incidenten en genereert alerts, maar kan kwaadaardig verkeer niet direct blokkeren.
- ☐ IPS (Actief / In-line): Het fysieke netwerkverkeer passeert direct door het apparaat. Kan kwaadaardige pakketten direct laten vallen (drop), verbindingen resetten (TCP RST) en firewallregels dynamisch bijwerken.
- ☐ Handtekening-gebaseerde detectie: Snelle herkenning van bekende exploits met lage foutmarge; blind voor zero-day kwetsbaarheden.
- ☐ Anomalie-gebaseerde detectie: Bouwt een baseline van normaal netwerkgedrag en slaat alarm bij afwijkingen; effectief tegen onbekende dreigingen maar vatbaar voor vals-positieven.

Risico van In-line IPS

Omdat een IPS in-line staat, veroorzaakt een softwarecrash of overbelasting directe netwerkuitval, tenzij hardwarematige bypass-switches (fail-open) zijn geconfigureerd.



Versleutelde Verbindingen: VPN-Protocollen

Virtual Private Networks (VPN's) creëren versleutelde tunnels over onveilige publieke infrastructuren. Afhankelijk van de use-case (site-to-site of remote-access) worden verschillende protocollen ingezet.

- IPsec Suite: Werkt op netwerklaag 3. Bestaat uit Authentication Header (AH) voor integriteit/authenticatie en Encapsulating Security Payload (ESP) voor dataversleuteling en integriteit. Gebruikt IKE/IKEv2 voor sleuteluitwisseling.
- IPsec Transportmodus: Versleutelt alleen de payload; originele IP-headers blijven zichtbaar (geschikt voor host-to-host communicatie).
- IPsec Tunnelmodus: Versleutelt het gehele originele IP-pakket en plaatst een nieuwe IP-header ervoor (standaard voor site-to-site VPN's tussen gateways).
- OpenVPN: Flexibel open-source protocol op transport-/applicatieniveau. Draait over TCP of UDP (poort 1194 standaard) via OpenSSL-cryptografie.
- WireGuard: Modern, gestroomlijnd cryptografisch protocol in de Linux-kernel. Werkt uitsluitend via UDP met vaste, bewezen cryptografische primitieven (ChaCha20, Curve25519) voor maximale doorvoersnelheid.

Draadloze Netwerkbeveiliging (Wi-Fi)

Wi-Fi-netwerken (IEEE 802.11) transporteren signalen door de vrije ruimte en vereisen robuuste cryptografische kaders om ongeautoriseerde toegang en af luisteren tegen te gaan.

- WEP & WPA: Verouderd en cryptografisch gekraakt (RC4-kwetsbaarheden, IV-zwaktes en TKIP-ontwerpfouten). Niet veilig voor productieomgevingen.
- WPA2 (Personal / Enterprise): Gebruikt CCMP met AES-128 voor versleuteling. Personal gebruikt een Pre-Shared Key (PSK) met 4-way handshake (kwetsbaar voor offline dictionary attacks bij zwakke wachtwoorden).
- WPA3-Personal: Vervangt de kwetsbare PSK-handshake door Simultaneous Authentication of Equals (SAE / Dragonfly-handshake). Biedt forward secrecy en immuniteit tegen offline woordenboekaanvallen.
- WPA2/WPA3-Enterprise (802.1X / EAP): Elimineert gedeelde wachtwoorden. Clients authenticeren zich individueel via een centrale RADIUS-server met certificaten of unieke gebruikersgegevens.

Configuratie-norm voor Bedrijfsnetwerken

Gebruik in zakelijke omgevingen altijd WPA3-Enterprise of WPA2-Enterprise met 802.1X (EAP-TLS). Vermijd Pre-Shared Keys om credential-sharing en ongecontroleerde hosttoegang te elimineren.

☒ Netwerkaudit & Segmentatie Verificatiechecklist

Gebruik onderstaande controlelijst en registratievelden tijdens periodieke netwerkaudits om te verifiëren of segmentatiecontroles, poortblokkades en veilige protocollen conform beleid functioneren.

- ☐ Zijn alle beheerpoorten (SSH 22, RDP 3389, Web GUI's) geblokkeerd op externe publieke interfaces?
- ☐ Zijn gastennetwerken, IoT-apparaten en kantoorwerkplekken gescheiden via geïsoleerde VLAN's met expliciete firewallregels?
- ☐ Is WPA3-Personal of 802.1X Enterprise actief op alle draadloze access points zonder actieve WEP/WPA fallback?
- ☐ Is DHCP-snooping geconfigureerd op Layer 2 switches om rogue DHCP-servers en man-in-the-middle aanvallen te voorkomen?
- ☐ Draait extern VPN-verkeer over moderne standaarden (IPsec IKEv2 of WireGuard/OpenVPN) met multi-factor authenticatie?

Geïnspecteerd netwerksegment / VLAN-ID en datum van evaluatie:

Gedetecteerde onbeveiligde poorten of overbodig openstaande diensten:

Vastgestelde tekortkomingen in firewallregels of segmentatiescheiding:

Vereiste herstelmaatregelen en toegewezen netwerkbeheerder: