A segurança em redes de comunicação assenta em vários pilares: software, hardware/firmware, pessoas, gestão e ambiente físico. Dentro de uma organização, o Centro de Operações de Rede (NOC) é responsável por garantir a resiliência da rede, segmentação de serviços, instalação e atualização de dispositivos e software, aplicação de políticas de segurança, e mitigação de ameaças. Já o Centro de Operações de Segurança (SOC) foca-se na prevenção e deteção de ataques, monitorização com ferramentas como SIEM, análise de comportamentos anómalos e resposta a incidentes com medidas de emergência ou playbooks conhecidos.

Os ataques podem ter motivações diversas - desde diversão até fins políticos ou económicos - e objetivos técnicos como a interrupção de operações ou a interceção de dados. Estes ataques incluem DoS, roubo de dados pessoais, técnicos ou comerciais, e podem ser combinados para maximizar impacto. Relatórios de segurança de entidades como Akamai, Cisco ou NSA ajudam a identificar ameaças e boas práticas, mas também revelam limitações devido a enviesamentos de observação, que ignoram ameaças invisíveis ou furtivas.

A segurança ciberfísica envolve medidas como controlo de acessos, sensores ambientais e redundância de energia. As defesas tradicionais - firewalls, antivírus, IDS/IPS - dependem de conhecimento prévio das ameaças. No entanto, ameaças persistentes avançadas (APT) usam métodos sofisticados, exploram vulnerabilidades desconhecidas e mantêm-se ativas por longos períodos, adaptando-se às defesas e utilizando canais alternativos como Bluetooth ou serviços legítimos para comunicação e exfiltração.

As defesas “inteligentes” tentam detetar ameaças desconhecidas em tempo útil, aplicando técnicas de Big Data e IA, embora ainda limitadas a soluções de fabricantes e dados locais. A deteção ideal requer conhecimento global da rede e sistemas - a chamada consciência situacional cibernética.

Os ataques seguem fases: infiltração (acesso inicial), aprendizagem (recolha de informação), propagação (acesso a zonas mais críticas), agregação (movimentação interna de dados) e exfiltração (envio de dados para fora). A infiltração pode ocorrer remotamente através de utilizadores legítimos (phishing, macros, software malicioso), por ações diretas do atacante (exploração de vulnerabilidades) ou localmente (acesso físico, dispositivos IoT inseguros). A propagação envolve exploração de credenciais e vulnerabilidades, muitas vezes em sistemas legados. A exfiltração pode ser direta ou disfarçada, usando técnicas como esteganografia.

Por fim, os cenários variam em complexidade, desde redes pequenas até redes distribuídas geograficamente, exigindo abordagens de segurança adaptadas à sua escala e estrutura.

O design de redes corporativas deve ser modular, resiliente e flexível. A modularidade permite escalar a rede com facilidade, a resiliência garante alta disponibilidade - essencial em setores críticos como finanças ou saúde - e a flexibilidade assegura adaptação a mudanças nos negócios. A escolha de equipamentos deve considerar tipo (switch L2, L3, router), fiabilidade (MTBF), preço, assistência, desempenho, número e tipo de portas, suporte a PoE, e funcionalidades de software.

A arquitetura hierárquica divide-se em três camadas: acesso, distribuição e núcleo. A camada de acesso conecta os utilizadores e dispositivos finais; a de distribuição agrega tráfego e aplica políticas; e a camada de núcleo assegura conectividade de alta velocidade e resiliência. Em redes pequenas, pode-se adotar uma arquitetura colapsada, fundindo núcleo e distribuição. A redundância é essencial, mas o excesso pode aumentar a complexidade e custos.

Os módulos de rede incluem campus (acesso principal), data center (com redundância e balanceamento de carga), filiais (acesso remoto seguro), WAN/MAN (com QoS e VPNs), e utilizadores remotos (acesso via VPN). A camada de acesso deve garantir alta disponibilidade, segurança (802.1X, DAI), QoS e suporte a multicast. A distribuição implementa políticas de roteamento, segmentação e balanceamento de carga. O núcleo deve ser rápido, escalável e evitar manipulação de pacotes.

VLANs permitem segmentar logicamente a rede, agrupando dispositivos com requisitos semelhantes. Podem ser locais ou fim-a-fim, e cada VLAN deve ter uma sub-rede IP única. A comunicação entre VLANs requer roteamento de camada 3, feito por routers ou switches L3. Trunks transportam múltiplas VLANs entre switches. A agregação de links aumenta a largura de banda entre dispositivos.

Protocolos como STP, RSTP e MST evitam loops em redes com redundância. Em redes sem fios, os APs devem integrar-se com a rede com VLANs mapeadas por SSID, garantindo mobilidade sem quebra de conectividade. A gestão eficiente do espectro e posicionamento dos APs é crucial.

O roteamento IP pode ser estático, dinâmico ou baseado em políticas. O roteamento dinâmico adapta-se automaticamente a mudanças na topologia. Protocolos como OSPF (link-state) e RIP (distance-vector) são usados para isso. OSPF utiliza LSAs para propagar mudanças e calcula os melhores caminhos com o algoritmo de Dijkstra. A hierarquia com áreas reduz o impacto de alterações e o tamanho das tabelas de roteamento.

Outros protocolos incluem IS-IS (semelhante ao OSPF), EIGRP (Cisco, híbrido), RIPng (para IPv6) e OSPFv3 (versão IPv6 do OSPF). A redistribuição de rotas permite

a interoperabilidade entre diferentes protocolos, mas deve ser cuidadosamente gerida para evitar loops e rotas subótimas. O roteamento baseado em políticas (PBR) permite definir regras específicas para o encaminhamento de tráfego com base em critérios como origem, destino ou tipo de aplicação.

O controlo de acesso em redes visa proteger portas Ethernet contra usos ilícitos, recorrendo a técnicas como separação por VLANs e autenticação 802.1X. Portas não utilizadas podem ser isoladas com VLANs ou 802.1X, mas continuam vulneráveis a ataques como MAC flooding. Portas em uso podem ser exploradas com dispositivos em linha que contornam a autenticação, permitindo escutas, injeção de tráfego e ataques man-in-the-middle.

A arquitetura AAA (Autenticação, Autorização e Contabilização) é essencial para segurança sistemática de acesso. A autenticação identifica o utilizador, a autorização define os seus privilégios e a contabilização regista a utilização da rede. Estes serviços são geralmente geridos por servidores externos, como RADIUS ou TACACS+.

O protocolo 802.1X, baseado em EAP (Extensible Authentication Protocol), é um padrão para controlo de acesso à rede, usado tanto em redes com fios como sem fios. O EAP permite autenticação extensível mesmo sem IP, sendo dividido em fases: descoberta, autenticação e associação segura. Em redes Wi-Fi, a descoberta é feita por beacons e probe requests, e a associação segura é estabelecida por um handshake de quatro vias.

TACACS+ separa claramente as funções AAA, usa TCP, encripta todos os pacotes e permite autenticação bidirecional. Já o RADIUS combina autenticação e autorização, usa UDP, encripta apenas a password e é menos robusto. O DIAMETER, sucessor do RADIUS, oferece autenticação bidirecional, segurança fim-a-fim e maior flexibilidade, sendo compatível com RADIUS para facilitar a migração.

Em redes Wi-Fi, o processo de ligação a um ponto de acesso (AP) envolve descoberta, autenticação e associação. A autenticação pode ser aberta (default) ou com chave partilhada (obsoleta). Após autenticação, a associação permite a troca de dados. O WPA (Wi-Fi Protected Access) e o WPA2 (802.11i) reforçam a segurança com autenticação baseada em 802.1X e cifragem com TKIP ou AES. O WPA2 introduz o protocolo RSN e suporte a AES, mas não protege quadros de controlo e gestão, exigindo hardware compatível.

Por fim, o processo de troca de chaves WPA ocorre após a associação, utilizando quadros de dados para estabelecer sessões seguras. A segurança em redes sem fios continua a evoluir, mas vulnerabilidades persistem, exigindo atenção contínua à configuração e atualização dos sistemas.

O controlo de fluxo em redes é um componente essencial da segurança, especialmente em arquiteturas Zero Trust, onde a microsegmentação divide a rede em zonas isoladas com diferentes níveis de segurança. Esta segmentação é reforçada por firewalls, que atuam como pontos de defesa entre redes, avaliando pacotes com base em políticas de segurança e podendo ser implementadas em hardware ou software.

As firewalls oferecem serviços como NAT, VPNs, análise de conteúdo, autenticação de utilizadores e deteção de ataques DoS/DDoS. Existem vários tipos: firewalls de nível de rede (L2/L3), de circuito (L4), de aplicação (L4+), stateful multilayer e firewalls pessoais. As firewalls podem ser **stateless**, aplicando regras a pacotes isolados, ou **stateful**, mantendo o estado das conexões em tabelas sincronizadas em cenários de alta disponibilidade.

A colocação das firewalls deve considerar redundância e segmentação, podendo ser organizadas em clusters ativos-passivos (com VRRP) ou ativos-ativos (com balanceamento de carga). O balanceamento pode ser feito por algoritmos como IP Hash, Round Robin ou Least Connections, e pode ser centralizado por um orquestrador. As firewalls podem ser **endereçadas** (com IPs) ou **stealth** (sem IPs), dependendo da função na rede.

As regras de firewall definem o tráfego permitido ou bloqueado com base em IPs, portas, protocolos e estado da conexão (NEW, ESTABLISHED, RELATED). A ordem das regras é crítica, e boas práticas incluem bloquear tudo por defeito e permitir apenas exceções específicas. A documentação e monitorização contínua das regras são essenciais para manter a segurança alinhada com as políticas da organização.

Ataques como IP spoofing e conexões TCP semiabertas podem ser mitigados com técnicas como verificação de caminho reverso e definição de timeouts. Ferramentas como **iptables** e **nftables** no Linux permitem configurar regras de filtragem e NAT, com suporte a cadeias e tabelas personalizadas. O **nftables** substitui o iptables com uma arquitetura mais eficiente e sintaxe unificada.

O controlo de tráfego com base em camadas superiores só é possível com tráfego não cifrado. Algumas firewalls conseguem inspecionar tráfego SSL/TLS ao atuar como autoridade certificadora, mas isso pode levantar questões legais e de privacidade. A avaliação de desempenho das firewalls inclui métricas como throughput, latência, taxa de estabelecimento e encerramento de conexões, e capacidade de transações a nível de aplicação.

As comunicações seguras em redes assentam em técnicas de criptografia e na criação de túneis virtuais para proteger dados em trânsito. A criptografia simétrica usa a mesma chave para encriptar e desencriptar, exigindo um canal seguro para partilha da chave. Já a criptografia assimétrica, como RSA, utiliza um par de chaves - pública e privada - permitindo confidencialidade e autenticação através de assinaturas digitais.

A infraestrutura de chave pública (PKI) gere certificados digitais emitidos por autoridades certificadoras (CA), que garantem a identidade dos intervenientes. Estes certificados seguem o padrão X.509 e podem ser revogados através de listas CRL. A verificação de validade inclui a confiança na CA, o período de validade e a não revogação.

Túneis de rede encapsulam pacotes com cabeçalhos adicionais, criando canais virtuais com características específicas de segurança e QoS. Interfaces de túnel virtuais (VTI) permitem tratar túneis como interfaces normais. Túneis podem ser ponto-a-ponto ou multiponto, com endereços de loopback usados para maior resiliência. O protocolo NHRP permite mapear endereços de rede sobrepostos, facilitando a criação de redes sobrepostas (overlays) como VPNs.

O IPsec é um conjunto de protocolos que protege dados ao nível da camada de rede. Usa os cabeçalhos AH (autenticação) e ESP (encriptação e integridade), podendo operar em modo túnel (gateway-to-gateway) ou transporte (host-to-host). As associações de segurança (SA) definem os parâmetros de proteção, sendo negociadas automaticamente com IKE/ISAKMP, que suporta autenticação por chave partilhada, assinaturas digitais ou encriptação assimétrica.

O IPsec pode coexistir com NAT através de encapsulamento em UDP (porta 4500). VPNs baseadas em IPsec podem ser configuradas estaticamente ou dinamicamente (como em DMVPN), permitindo conectividade entre múltiplos pontos com configuração simplificada. O GRE pode ser usado em conjunto com IPsec para suportar multicast.

As VPNs de acesso remoto permitem ligações seguras de utilizadores individuais a redes privadas. Podem usar protocolos como L2TP/IPsec, SSL/TLS, SSH ou OpenVPN. A autenticação pode ser feita por certificados, credenciais ou chaves partilhadas. A integração com firewalls e controlo de fluxo exige regras específicas para portas e protocolos usados por cada tipo de VPN.

Os sistemas de deteção e prevenção de intrusões (IDS/IPS) são fundamentais para a segurança das redes. O **IDS (Intrusion Detection System)** monitoriza e identifica acessos ou manipulações não autorizadas, analisando dados de múltiplas fontes como tráfego de rede, servidores e serviços. Deteta tanto intrusões externas como

comportamentos indevidos de utilizadores legítimos, mas não bloqueia o ataque - apenas gera alertas para análise humana ou resposta automática por firewalls ou sistemas de gestão centralizada.

O **IPS (Intrusion Prevention System)**, por outro lado, atua de forma proativa, bloqueando tráfego malicioso a nível de rede ou interrompendo processos e isolando ficheiros a nível de host. A proteção pode ser feita a nível de **host** (conhecido atualmente como EDR - Endpoint Detection and Response), monitorizando processos, acessos a ficheiros e dispositivos, ou a nível de **rede**, analisando pacotes e fluxos em pontos estratégicos como acessos à Internet, ligações entre zonas e redes sem fios.

A deteção pode ser baseada em **assinaturas**, comparando padrões conhecidos de ataque com os dados monitorizados, ou em **análise de anomalias**, que identifica desvios em relação a perfis de comportamento normais, podendo usar regras ou modelos de inteligência artificial.

O EDR oferece visibilidade contínua sobre as atividades nos dispositivos e permite resposta direta a incidentes. Pode funcionar de forma autónoma no dispositivo ou com apoio de análise externa.

A nível de rede, o tráfego pode ser espelhado para o IDS através de técnicas como **ERSPAN** (Encapsulated Remote Switched Port Analyzer), que encapsula o tráfego em túneis GRE para análise remota. O IPS pode ser integrado em linha com firewalls ou embutido nelas.

As ações dos IDS/IPS variam conforme a ferramenta. Por exemplo, o **Suricata** pode gerar alertas, bloquear pacotes, ou enviar mensagens de erro (ICMP ou TCP RST). O **Snort** oferece ações semelhantes, incluindo bloqueio silencioso (sdrop) ou rejeição com notificação.

A monitorização de redes é essencial para garantir a segurança e o desempenho dos sistemas. Pode ser feita através de acesso remoto via CLI (SSH, Telnet), leitura de ficheiros de log (via rsyslog, SCP, etc.) e recolha de métricas em tempo real. A monitorização pode ser feita ao nível do núcleo da rede (core), dos nós, dos utilizadores finais, dos serviços e da cloud, abrangendo parâmetros como largura de banda, perdas, jitter, desempenho de CPU/memória, e erros de serviço.

As fontes de dados incluem SNMP (para estados de nós e links), exportação de fluxos (NetFlow, IPFIX), captura de pacotes, logs de servidores e medições ativas. O SNMP permite recolher dados sobre desempenho e falhas, sendo estruturado em MIBs (Management Information Bases) com identificadores únicos (OIDs). NetFlow, por sua vez, caracteriza o tráfego IP com base em fluxos, sendo útil para análise de

utilização, destinos e padrões de tráfego. A versão 9 e o IPFIX (v10) introduzem maior flexibilidade e suporte a IPv6.

A monitorização passiva com sondas (probes) permite inferir dinâmicas detalhadas do tráfego, usando portas espelhadas, taps ou ERSPAN. Os dados podem ser armazenados e processados localmente ou enviados para um ponto central.

Os sistemas de gestão de logs (LMS) agregam e armazenam logs de múltiplas fontes, permitindo análise forense e deteção de indicadores de compromisso. Os sistemas SIEM (Security Information and Event Management) vão além, integrando gestão de eventos (SEM), gestão de informação (SIM) e correlação de eventos (SEC), permitindo deteção de ameaças, alertas em tempo real e resposta automatizada.

Exemplos de eventos SIEM incluem deteção de força bruta, falhas de login, acessos anómalos, transferências de dados suspeitas, ataques DDoS e alterações não autorizadas em ficheiros ou configurações. O SOC (Security Operations Center) utiliza SIEM para prevenir, detetar, investigar e responder a incidentes, devendo idealmente estar integrado com o NOC (Network Operations Center).

Por fim, métricas de segurança como MTBF, MTTR, MTTD, MTTA e MTTC ajudam a avaliar a eficácia da resposta a incidentes, enquanto indicadores como número de dispositivos não identificados, tempo médio para aplicar patches e tentativas de intrusão ajudam a medir o estado geral da segurança da organização.
