1.

A fase de **propagação** num ataque corresponde ao momento em que o atacante, já tendo um ponto de entrada na rede, procura **expandir o seu acesso a outros sistemas** ou segmentos mais críticos, explorando **vulnerabilidades internas**, **credenciais comprometidas** ou **configurações fracas**. Esta fase visa aumentar o controlo sobre a infraestrutura e facilitar a agregação e posterior exfiltração de dados. Para detetar tais atividades ilícitas, pode-se usar **sistemas IDS/IPS** com análise de tráfego lateral (leste-oeste), **SIEMs com regras de correlação** para acessos anómalos entre dispositivos, e monitorização de comportamentos fora do padrão, como múltiplas tentativas de login entre terminais, movimentação de ficheiros inesperada, ou ligações entre zonas da rede sem autorização. Técnicas como **NetFlow/IPFIX**, logs de autenticação e análise de pacotes espelhados também ajudam na deteção de propagação de worms ou trojans.

2.

Para proteger a rede contra DDoS e controlar o tráfego entre zonas, é necessário introduzir **segmentação lógica e física** através de zonas como: DMZ (serviços públicos), rede interna (usuários), zona de serviços críticos (bases de dados, intranet) e zona de gestão. As alterações envolvem:

- **Firewalls de perímetro** entre a Internet e a DMZ, com inspeção profunda de pacotes e mitigação de DDoS (ex. rate limiting, blacklists).
- **Firewalls internas** entre a rede de utilizadores, os datacenters e os servidores de base de dados, com políticas rigorosas de acesso.
- **Segmentação em VLANs** por tipo de serviço/usuário.
- **Sonda IDS/IPS** posicionada nas zonas críticas e entre segmentos.
- **Balanceadores de carga com capacidade de deteção de anomalias** para proteger serviços públicos.

Um possível desenho inclui: Internet → Firewall perimetral → DMZ com servidores web públicos. A rede interna comunica com os datacenters através de firewalls internas, e os servidores de base de dados estão em segmento isolado. Cada zona é protegida com regras específicas de controlo de tráfego.

3.

A arquitetura de rede deve prever a separação clara dos seguintes serviços:

(i) O servidor Web público (TCP 443) deve estar colocado na **DMZ**, acessível apenas a partir da Internet (via firewall de borda).

(ii) O servidor Web da intranet (TCP 443) deve estar alojado no **Datacenter B**, acessível **exclusivamente a partir da rede interna corporativa** (via firewall interna que bloqueie acessos externos).

(iii) Os três servidores MySQL (TCP 3306) devem estar num **segmento isolado**, acessível apenas pelos dois servidores HTTPS (DMZ e Intranet) e por um IP específico do servidor MySQL externo para sincronização.

As regras de firewall, a alto nível, seriam:

- **Firewall perimetral (Internet ↔ DMZ):** permitir TCP 443 para o servidor público apenas.
- **Firewall interna (rede interna ↔ Datacenter B):** permitir TCP 443 para a intranet.
- **Firewall entre DMZ/Datacenter ↔ rede de BD:** permitir TCP 3306 apenas de/para os servidores HTTPS.
- **Firewall perimetral (Datacenter ↔ Internet):** permitir TCP 3306 apenas do IP do servidor MySQL externo.

4.

A solução mais adequada para garantir confidencialidade no tráfego entre o **Datacenter A** e o **datacenter na Internet** é a implementação de uma **VPN IPsec em modo túnel**, utilizando cabeçalhos ESP para encriptação e integridade. As **associações de segurança (SA)** podem ser negociadas com IKEv2, usando **autenticação mútua por certificados digitais**.

As firewalls devem ser configuradas para permitir:

- **Tráfego UDP 500 e 4500** (negociação IPsec via IKE).
- **Protocolo ESP (número 50)** para dados encriptados.
- **Tráfego TCP 3306** encapsulado pela VPN, apenas entre os IPs dos servidores HTTPS e os servidores MySQL do outro datacenter.

Além disso, deve-se bloquear tráfego TCP 3306 direto para o exterior, garantindo que só circula dentro do túnel.

5.

Para acesso remoto por SSH (porta TCP 2222), a empresa deve criar uma **VPN de acesso remoto**, baseada em protocolos como **SSL VPN ou L2TP/IPsec**, com autenticação via credenciais seguras ou certificados. O acesso dos utilizadores à VPN deve ser autenticado por um servidor RADIUS ou LDAP integrado com a infraestrutura AAA.

As firewalls devem:

- **Permitir o tráfego VPN (ex: SSL na porta 443, IPsec em UDP 500/4500)** para o concentrador VPN.
- **Permitir TCP 2222** apenas para IPs dos clientes autenticados na VPN.
- **Bloquear TCP 2222** de quaisquer outras origens.
- Integrar com o SIEM para **detetar acessos anómalos ou tentativas de força bruta**.

6.a)
Para detetar tentativas de acesso ilegítimo aos servidores SSH, o SIEM deve recolher logs de autenticação (via Syslog ou agentes locais). Uma regra pode gerar alertas quando há mais de "n" tentativas falhadas por minuto, ou falhas repetidas de diferentes IPs para o mesmo utilizador.

6.b)
A deteção de tráfego P2P sobre HTTPS pode ser feita com análise de NetFlow/IPFIX e padrões de comunicação. O SIEM pode gerar alertas para:

- Ligações HTTPS com **frequência e volume elevado a múltiplos domínios suspeitos**.
- **Padrões de download/upload contínuo** em horas fora do normal, sem tráfego legítimo associado (por exemplo, sem DNS ou autenticação anteriores).

6.c)
Para identificar exfiltração de dados MySQL, o SIEM deve monitorizar:

- Conexões a servidores MySQL de IPs não autorizados.
- Transferência de dados fora do horário normal ou com volume atípico.
- Comandos SQL suspeitos (ex: SELECT * FROM, INTO OUTFILE) originados por utilizadores sem privilégios administrativos.

Estes eventos podem ser combinados para gerar alertas de possível acesso indevido e exfiltração.