Considerando a rede empresarial em anexo:

1. No contexto das fases de um ataque a uma rede empresarial:

a) Explique a fase de exfiltração de dados e apresente dois métodos usados por atacantes para ocultar a exfiltração perante mecanismos de deteção. (2.0 valores)

b) Indique dois tipos de indicadores de compromisso que podem ser monitorizados para detetar essa fase. Proponha ferramentas ou técnicas que permitam essa monitorização. (2.0 valores)

---

2. A empresa pretende implementar os seguintes serviços:

(i) Servidores Web HTTPS públicos na DMZ (portas TCP 443) com suporte a múltiplos domínios;
(ii) Servidores de email na DMZ (SMTP com STARTTLS – TCP 587 e IMAPS – TCP 993) acessíveis interna e externamente;
(iii) Servidores internos no Datacenter B acessíveis apenas a partir da VLAN 3 e VLAN 6 via SSH (porta TCP 22);
(iv) Servidor de replicação no Datacenter C acessível apenas pelos servidores Web e de email da DMZ, usando o protocolo TCP na porta 5000.

a) Proponha alterações de arquitetura e segmentação da rede que permitam aplicar controlo de fluxos eficaz e garantir mitigação de ataques volumétricos. Desenhe um diagrama da arquitetura proposta. (3.0 valores)

b) Apresente as regras de firewall de alto nível que devem ser aplicadas para garantir os requisitos descritos. Especifique a localização das regras. (3.0 valores)

---

3. A empresa deseja garantir que o tráfego entre os servidores internos no Datacenter B e uma infraestrutura privada na cloud da AWS (com servidores frequentemente criados/destruídos) é seguro e escalável, garantindo confidencialidade e integridade.

Proponha uma solução técnica de comunicação IPv4 e as respetivas alterações nas firewalls para atingir estes objetivos. (3.0 valores)

---

4. Proponha um sistema SIEM que permita detetar os seguintes cenários:

a) Acesso não autorizado a áreas administrativas dos servidores Web na DMZ. (1.5 valores)

b) Atividades de varrimento (scanning) interno iniciadas por terminais comprometidos. Apresente três regras. (2.0 valores)

c) Comunicação com domínios de comando e controlo (C&C) sobre HTTPS. (1.5 valores)

d) Tentativa de ataque man-in-the-middle por dispositivos ligados indevidamente em portas de acesso. (2.0 valores)

Rede empresarial em anexo:

Notas:

- Os edifícios 1 e 2 têm switches Layer 2 com VLANs 1 a 6 configuradas em portas de acesso.
- Ligações trunk ligam os switches L2 aos switches L3 (F1 a F4).
- Interfaces entre L3 e routers são IP routing.
- A empresa tem Datacenter B (interno) e Datacenter C (remoto via WAN).
- Roteamento OSPFv2 e OSPFv3 está ativo.
- Routers de borda anunciam rotas por omissão.
- Custo OSPF é 1 em todos os interfaces.