

1. A fase de exfiltração consiste na transferência de dados confidenciais da rede da organização para o exterior. Pode ser feita de forma direta ou dissimulada, usando canais alternativos como HTTPS, DNS, serviços cloud ou esteganografia. Para dificultar a detecção, os atacantes podem utilizar técnicas como fragmentação de pacotes, tunelamento sobre protocolos legítimos (ex: HTTPS, DNS), uso de horários fora do expediente e camuflagem no tráfego normal da organização.

2. Para proteger contra ataques DDoS com impacto mínimo, deve-se usar firewalls com capacidade de mitigação em linha na borda da rede, balanceadores de carga distribuídos por zonas críticas e serviços externos de limpeza de tráfego. A arquitetura deve incluir redundância com firewalls em alta disponibilidade, inspeção de tráfego com IDS/IPS em linha e uso de NetFlow/IPFIX para monitorizar fluxos em tempo real. O tráfego deve ser segmentado por zonas, com regras específicas por firewall.

3.a. A arquitetura deve ser segmentada em zonas distintas: zona interna (edifícios A e B), DMZ (servidores públicos), Datacenter (serviços internos) e zona externa. Deve-se criar VLANs e sub-redes específicas para os servidores de armazenamento e aplicar microsegmentação com controlo de fluxos. Firewalls entre zonas garantirão filtragem de tráfego com regras precisas. A DMZ deve estar isolada, acessível apenas pela firewall e interfaces dedicados.

3.b.

- **Firewall Edifícios ↔ Internet:** Permitir TCP 443 (destino) de terminais para exterior; bloquear outras saídas.
- **Firewall Edifícios ↔ Edifícios:** Permitir apenas TCP 3343 (origem e destino) entre terminais.
- **Firewall Internet ↔ DMZ:** Permitir TCP 443 (destino) para servidores HTTPS públicos.
- **Firewall Edifício A ↔ Datacenter A:** Permitir TCP 443 (destino) de terminais do edifício A para o servidor de intranet.
- **Firewall Datacenter ↔ Datacenter:** Permitir TCP 6800–6900 dos servidores HTTPS para os servidores de armazenamento.
- **Firewall Internet ↔ Datacenter A:** Permitir TCP 6800–6900 apenas do IP do servidor AWS para replicação. Bloquear tudo o resto.

4.a. Deve-se configurar túneis IPsec (modo túnel) entre o Datacenter A e os IPs conhecidos da AWS. As firewalls devem permitir tráfego UDP encapsulado (porta 4500) e ESP. A autenticação dos equipamentos deve usar certificados digitais

validados por uma infraestrutura de chave pública (PKI), garantindo integridade e confidencialidade do tráfego.

4.b. Para comunicação segura e dinâmica com máquinas virtuais na cloud da Microsoft, deve-se usar DMVPN com IPsec, permitindo criação dinâmica de túneis protegidos. A firewall deve permitir tráfego UDP (porta 4500) e ESP. A autenticação deve ser baseada em certificados ou chave pré-partilhada, e a negociação de túneis feita com IKEv2 para suportar mobilidade e rotação de endpoints.

5.a. O SIEM deve recolher logs dos servidores DNS, analisando requisições incomuns (domínios randômicos, volumetria fora do padrão). Deve correlacionar tentativas repetidas com padrões de exfiltração ou beaconing. Regras de alerta devem identificar consultas de domínios suspeitos ou taxas elevadas de resolução por terminais específicos.

5.b. Para deteção de comunicação C&C via serviços legítimos como Twitter, o SIEM deve correlacionar acessos HTTP/HTTPS com padrões anómalos, como frequências regulares, payloads incomuns ou tráfego gerado por processos não habituais. A integração com EDR pode ajudar a identificar processos maliciosos que acedem a APIs externas.

5.c. A exfiltração via HTTPS pelos terminais da administração pode ser detetada por análise de padrões de tráfego. O SIEM deve identificar uploads invulgares, sessões HTTPS prolongadas ou tráfego de saída com volume elevado fora do horário habitual. A análise contextual dos logs, incluindo destino, tamanho e frequência, permite configurar alertas adequados.