

1. A fase de infiltração corresponde ao acesso inicial à rede alvo. Pode ocorrer remotamente, através de utilizadores legítimos explorados via phishing, macros ou malware, ou diretamente, por exploração de vulnerabilidades e acessos físicos a dispositivos IoT inseguros. A sua deteção é difícil porque utiliza técnicas furtivas e disfarça-se de tráfego legítimo, evitando mecanismos tradicionais como antivírus ou firewalls.

2. Para mitigar ataques DDoS com impacto mínimo no desempenho, deve-se implementar balanceadores de carga e firewalls stateful na borda da rede com capacidades de mitigação DDoS, distribuindo o tráfego entre múltiplos pontos e filtrando anomalias. Pode-se usar serviços de mitigação na cloud, como scrubbing centers, que analisam e limpam o tráfego antes de entrar na rede. A monitorização contínua com NetFlow/IPFIX e sondas passivas também permite deteção precoce de padrões anómalos sem comprometer o desempenho da rede.

3.a. É necessário introduzir firewalls adicionais para segmentação entre a DMZ, Datacenter A e redes externas. A arquitetura deve permitir controlo de tráfego granular, isolando os servidores por função. Deve-se aplicar microsegmentação e criar ACLs em switches L3 para reforçar a política de Zero Trust, associando VLANs específicas aos serviços e permitindo controlo de fluxo orientado à aplicação.

3.b. As regras devem permitir tráfego HTTPS (TCP 443) da internet para os servidores web da DMZ. O servidor de intranet no Datacenter A deve aceitar apenas tráfego HTTPS vindo das VLANs 5 e 6. Os servidores de armazenamento no Datacenter A devem aceitar tráfego TCP nas portas 6800–6900 apenas a partir dos servidores web HTTPS e de um IP específico externo. Todo o outro tráfego deve ser bloqueado por defeito, seguindo a política de “deny all, allow by exception”.

4.a. Para garantir confidencialidade no tráfego UDP para servidores AWS, deve-se criar túneis IPsec em modo túnel entre o Datacenter A e os IPs conhecidos da AWS. As regras da firewall devem permitir tráfego UDP encapsulado (porta 4500) e ESP. A configuração IPsec deve ser baseada em SAs negociadas com IKE, utilizando autenticação forte com certificados digitais.

4.b. Como os destinos na cloud da Microsoft são altamente dinâmicos, a melhor solução é usar VPNs dinâmicas como DMVPN com IPsec, que suportam túneis multiponto e descoberta automática de endpoints. Isto garante confidencialidade sem a necessidade de configuração estática. As firewalls devem permitir tráfego IPsec com encapsulamento UDP e permitir controladamente os protocolos de gestão dinâmica como NHRP.

5.a. O SIEM deve recolher logs dos servidores da intranet no Datacenter A, filtrando eventos de login com falha. A regra de alerta deve disparar após três tentativas

consecutivas falhadas num curto intervalo de tempo (por exemplo, 5 minutos), indicando possível força bruta.

5.b. A comunicação de C&C via DNS pode ser identificada monitorando padrões de resolução DNS anómalos, como elevado número de domínios com baixa reputação ou domínios aleatórios (DGA). O SIEM deve correlacionar logs de DNS com destinos suspeitos, acionando alertas quando a frequência de consultas ou os destinos ultrapassarem um limiar definido.

5.c. A possível exfiltração de dados dos servidores HTTPS pode ser detetada com base em padrões de tráfego incomuns, como grandes volumes de saída, uso de métodos HTTP atípicos ou acesso massivo fora do horário normal. O SIEM deve analisar logs de acesso, tamanhos de payload e tempo de sessão, e gerar alertas sempre que for ultrapassado um limite predefinido, como 1 GB enviado por um servidor num curto intervalo.