

# Universidade de Aveiro

Exame Teórico – Segurança em Redes de Comunicações  
19 de junho de 2024

Duração: 2h00m. Sem consulta. Justifique cuidadosamente todas as respostas.

Considerando a rede empresarial em anexo:

1. No contexto das fases de um ataque a uma rede empresarial;
  - a) Explique o impacto do fator humano nas diferentes fases de um possível ataque externo. (2.0 valores)
  - b) Proponha soluções de segurança ao nível da rede passíveis de mitigar um ataque externo que use vetores de ataque focados em fatores humanos. (2.0 valores)
2. Assumindo que a empresa deseja implementar um conjunto de servidores para prestação de serviços, nomeadamente (i) vários servidores Web HTTPS na DMZ com vários sites/domínios (portas TCP 443) públicos que deverão estar disponíveis para o exterior, (ii) dois servidores de Email na DMZ (portas TCP 465 para clientes e servidores) públicos que deverão estar disponíveis para clientes internos e externos, (ii) um servidor Web HTTPS com a Intranet da empresa (porta TCP 443) no Datacenter B que deverá estar disponível apenas para os terminais internos das VLAN 5 e 6, e (iii) três servidores de *backup* de dados (portas TCP 5001 a 5002) no Datacenter C que apenas deverão estar acessíveis pelos servidores Web HTTPS e por um servidor pré-definido externo para sincronização/replicação dos dados.
  - a) Proponha as alterações de arquitetura de rede necessárias de modo a poder implementar o controlo de fluxos e proteção contra ataques DDoS. Defina as diferentes zonas da rede e desenhe um diagrama de rede com as alterações propostas. (3.0 valores)
  - b) Apresente uma lista das regras de *firewall*/controle de fluxo de tráfego (de alto nível) nos vários locais. (3.0 valores)
3. Proponha uma solução de comunicação e encaminhamento IPv4 ao nível da rede, e respetivas alterações nas regras das Firewalls, que garanta que o tráfego TCP para os servidores de *backup* no Datacenter C (via WAN) seja encaminhado de forma que garanta confidencialidade. (3.0 valores)
4. Proponha um sistema SIEM, incluindo o processo de coleta de dados e a definição de regras de alerta, capaz de alertar para:
  - a) Tentativas de acesso a objectos não autorizados nos servidores HTTPS. (1.5 valores)
  - b) Clientes externos a participar num ataque DDoS. Indique pelo menos 3 regras. (2.0 valores)
  - c) Possível atividade de uma botnet. (1.5 valores)
  - d) Possível exfiltração encoberta (stealth) de dados de terminais internos utilizando serviços externos legítimos e autorizados. (2.0 valores)



- Nos switches Layer 2 dos edifícios 1 e 2 estão configuradas portas de acesso para as VLANs 1,2,3,4,5 e 6.
- As ligações entre os switches Layer2 e os switches Layer3 F1 a F4 são feitas usando ligações trunk/inter-switch com permissão de transporte para todas as VLANs;
- Os interfaces entre os switches Layer 3 são portas Layer 3 (IP routing) e os interfaces entre os switches Layer 3 e os routers são portas Layer 3 (IP routing);
- A empresa possui um Datacenter interno para serviços internos (Datacenter B);
- A empresa possui um Datacenter externo para serviços backup remotos (Datacenter C) acessível por uma ligação WAN (proprietária) por satélite;
- Os switches Layer3, routers e firewalls têm os processos dos protocolos OSPFv2 e OSPFv3 ativos em todas as redes IP;
- Os routers de acesso à Internet (Routers 1 e 2), estão a anunciar (por OSPF) rotas por omissão;
- Todos os interfaces tem um custo OSPF de 1.

