Universidade de Aveiro

Exame Teórico – Segurança em Redes de Comunicações
13 de junho de 2025

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

Considerando a rede empresarial em anexo:

1. Considerando que se pretende tornar a rede empresarial mais resiliente a ataques distribuídos de negação de serviço (DDoS) e a ataques de personificação de endereços IP (IP Spoofing) com origem externa, explique as alterações a efetuar na infraestrutura para o efeito. (2.0 valores)

2. Assumindo que a empresa deseja implementar (entre outros) um conjunto de servidores/serviços para suporte à operação, nomeadamente:
   (i) um servidor de backup de dados (porta TCP 6001) no Datacenter C que recolhe dados dos servidores Web HTTPS (DMZ e Datacenter C) e envia-os para um servidor externo, e
   (ii) um servidor de OpenVPN na DMZ, onde os utilizadores remotos podem aceder a serviços no Datacenter B. A rede virtual alocada aos utilizadores remotos é a 192.168.10.0/24.

   a) Defina as diferentes zonas da rede que permitam a implementação dos requisitos de controlo de fluxos. (1.5 valores)
   b) Apresente as regras de *firewall*/controle de fluxo de tráfego (de alto nível) para os requisitos (i) e (ii). Indique as respetivas zonas e firewalls onde as regras devem ser implementadas. (3.5 valores)

3. Pretende-se criar uma ligação virtual segura que garanta a confidencialidade dos dados entre um conjunto pré-definido de servidores no Datacenter B e um duas redes externas (Cloud/Internet) para o serviço que usa as portas TCP/6002 (origem e destino).
   a) Proponha uma solução protocolar para a implementação desta ligação virtual segura e descreva como pode definir o tráfego encaminhado/protegido por esta ligação segura. (1.5 valores)
   b) Apresente as regras de *firewall*/controle de fluxo de tráfego (de alto nível) para que permita o estabelecimento e uso desta ligação virtual segura. Indique as respetivas zonas e Firewalls onde as regras devem ser implementadas. (1.5 valores)
   c) Pretende-se que a autenticação das máquinas para esta ligação segura seja feita com certificados fornecidos por uma entidade certificadora (CA) localizada no Datacenter B e sem acesso direto do exterior. Descreva como fazer a implementação inicial desta solução de autenticação. (2.5 valores)

4. Assumindo que a empresa possui um sistema SIEM. Indique como implementar alertas, incluindo a fonte de dados, processo de coleta desses dados e regras, para os seguintes casos:
   a) Identificar clientes externos a participar num ataque DDoS aos servidores da empresa. Assuma que todos os utilizadores geram poucos pedidos. Apresente pelo menos duas regras. (2.5 valores)
   b) Identificar terminais dos utilizadores comprometidos a efetuar ataques de exfiltração (com ritmo baixo) de dados para o exterior usando o serviço de DNS (servidor interno). Apresente pelo menos duas regras. (2.5 valores)
   c) Tentativas de propagação de Worms/Trojans entre terminais da empresa. (2.5 valores)

- Nos switches Layer 2 do edifício A estão configuradas portas de acesso para as VLANs 1, 2 e 3.
- Nos switches Layer 2 do edifício B estão configuradas portas de acesso para as VLANs 4, 5 e 6.
- As ligações entre os switches Layer2 e as Firewalls (Fw7 a Fw10) são feitas usando ligações trunk/inter-switch com permissão de transporte para todas as VLANS;
- A empresa possui dois Datacenters para serviços internos (Datacenter B e Datacenter C);
- Os switches Layer3, Routers e firewalls têm os processos dos protocolos OSPFv2 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;
- As firewalls são todas stateful.