

Universidade de Aveiro

Correção Simplificada do Exame Teórico – Segurança em Redes de Comunicações 6 de julho de 2022

As respostas apresentadas apenas indicam os aspetos importantes a referir.

Não são as respostas completas!

Existem respostas alternativas que foram consideradas totalmente ou parcialmente corretas.

1. A fase de **infiltração** depende muito de vetores de ataque a pessoas (social engineering, phishing, etc...) e o fator humano é **muito difícil de monitorizar**, definir regras de controlo e **detetar anomalias**. Igualmente, a rede e sistemas estão sujeitos a **vulnerabilidades desconhecidas (0-day)** impossíveis de controlar.
Durante as **fase de propagação e exfiltração** o atacante **terá sempre** de **quebrar algum padrão** de comunicação legítimo/aceitável (ainda que subtilmente) no que respeita a **quantidades de tráfego**, **rátios de tráfego**, **portos** e **protocolos usados**, **matrizes de tráfego**, **horas de comunicação**, **padrões temporais de comunicação**, etc....
2. Para proteger de ataques **DDoS** e **controlar fluxos** com origem na Internet, colocar na **zona de acesso 2 firewalls stateless** (mais no **exterior**), **2 load-balancers**, **2 firewalls stateful**, (opcionalmente) mais **2 load-balancers** na ligação ao **core**.
Internamente, colocar **2 firewall stateful** a **proteger/controlar** cada zona do edifício e cada datacenter. Colocar **sempre redundância** de equipamentos e ligações.
3. Primeiro para ter **serviços públicos** temos de criar uma **nova zona**, uma **DMZ**, ligada às **firewall stateful** do **acesso à Internet**. O tráfego destes serviços **nunca deverá passar no core da rede!**
Regras FW stateful do **acesso Internet**:
 - **Bloquear tudo por default.**
 - **IN → OUT:** Tráfego dos **terminais** com **endereços IP de terminais** para o **porto TCP 443**.
 - **OUT ou DMZ → IN:** Respostas de **sessões já estabelecidas**.
 - **IN ou OUT → DMZ:** Tráfego **para os endereços IP** e **portos TCP** (443, 465, e 993) dos **respetivos servidores**.
 - **DMZ → OUT:** Respostas de **sessões já estabelecidas**.
Tráfego **SMTP** dos **endereços IP** do **servidor SNMP** para **porto TCP** (465).
Poderia-se ter um método de validação dos **endereços externos** via **DNS**.
4. É necessário criar uma **VPN site-to-site** usando um **túnel IPsec ponto-a-ponto** (não é preciso multiponto) do tipo **ESP**, entre o **Router3** e o **Router 5**.
O tráfego deverá ser **encaminhado** usando **políticas de encaminhamento (PBR)**.
Exceções para as **firewall stateful** dos datacenters:
 - **Tráfego** de **negociação/estabelecimento** do **túnel** (IKE/ISAKMP, UDP 500 por default) **entre** os **endereços dos Routers 3 e 5**.
 - **Tráfego IPsec** (IP ESP – Protocolo 50 do IP) entre os **endereços dos Routers 3 e 5**. Ou com **NAT** Transversal UDP 4500, por exemplo.
5. É necessário criar uma **User VPN (client-to-site VPN)**. Colocar **um servidor** na **DMZ**.
Regras FW stateful do **acesso Internet** (assumindo que a rede da VPN pertence à DMZ ou a uma zona VPN):
 - **OUT → DMZ:** Tráfego **para os endereços IP** e **portos TCP/UDP** do **servidor VPN**.
 - **DMZ → OUT:** Respostas de **sessões já estabelecidas**.
 - **DMZ/VPN → IN:** Tráfego **dos endereços IP dos clientes VPN** para **para os endereços IP** e **portos TCP 443** dos **2 servidores no DCA**.
 - **IN → DMZ/VPN:** Respostas de **sessões já estabelecidas**.**Regras FW stateful** do **acesso DCA**:
 - **IN → DCA:** Tráfego **dos endereços IP** dos **clientes VPN** para **para os endereços IP** e **portos TCP 443** dos **2 servidores no DCA**.
 - **DCA → IN:** Respostas de **sessões já estabelecidas**.

6. a) Obter os logs dos servidores do DCB por rsyslog.
Alertar sempre que houver mais que N falhas de logins do mesmo endereço IP ou username.
- b) Obter os fluxos de tráfego HTTPS entre o interior e o exterior usando os logs das Firewalls (+rsyslog) ou Netflow.
Detetar sessões HTTPS com rácio up/down anormal, comunicação para endereços IP nunca contactados ou em países/localizações específicas (nunca usadas), padrões de comunicação temporal anormal, comunicações a horas anómalas, etc... Ou combinações de várias destas coisas.