Exame Teórico (recurso) – Segurança em Redes de Comunicações 28 de junho de 2023

1- Exfiltração de dados é a transferência de dados de máquina para máquina por um agente mal intencionado. Se as máquinas estiverem as duas na mesma empresa chama-se **Agregação**, se uma delas estiver fora tem o nome de exfiltração.

2-Poderiamos implementar load-balancers nas ligações com mais ligações de modo a se acontecer um ataque DDOS a carga ser distribuída de forma mais uniforme, a nossa recomendação inicial seria entre as Firewalls e os SWL3. Além disso poderíamos aumentar a redundância das ligações, acrescentados mais switches L3, mais firewalls router e servidores. Finalmente implementação de firewalls stateless em cada um dos edifícios e após do router 5 no acesso à firewall.

3- a) ![[Pasted image 20240618142308.png]] b)- i)-

Firewall 3/4 : Bloquear tudo por default Out/In->DMZ: Apenas para os sites públicos na porta 443 e protocolo TCP DMZ->OUT: Respostas a sessões estabelecidas DMZ->IN: Para os servidores WebHTTPs na Portas 6800 6900 por TCP OUT->IN: Resposta a sessões estabelecidas Datacenter -> OUT: Para IP do servidor pré-definido

Firewall Router 5 Buildings -> Datacenter: Tráfego dos endereços de IP das VLANS 5 e 6 para o servidor Web HTTPS por TCP na Porta 433 OUT-> Datacenter: para sessões já estabelecidas Datacenter ->OUT: Para IP do servidor pré-definido

Firewalls do edifício A:

4 a)- **VPN Site-to-Site com túneis IPsec com ESP**(Confere confidencialidade) e o trafego deverá ser encaminhado usando **politicas de encaminhamento PBR**
Exceções para as Firewalls dos edifícios:

- Tráfego de negociação e estabelecimento do túnel(IKE, UDP 500) entre os SWL3 dos edifícios

- Tráfego IPsec (IP ESP-Protocolo 50 do IP) entre os SWL3 ou NAT Transversal UDP 4500 b)- **Dynamic Multipoint VPN** com Túneis IPsec com ESP tráfego encaminhado por OSPF Exceções para firewall do Router 5 e Firewalls 3 e 4:
- Tráfego de negociação e estabelecimento do túnel(IKE, UDP 500) entre os Router 5 e Out
- Tráfego IPsec (IP ESP-Protocolo 50 do IP) entre os Router 5 e OUT ou NAT Transversal UDP 4500

5- a) Sistema de Logs como rsyslog Alerta sempre que houver mais que N falhas dos mesmo IP ou Username b) Obter fluxo de tráfego DNS entre o interior e exterior usando LOGS das firewalls Detetar tráfego irregular com servidores DNS não utilizados/whitelisted ou em países específicos. Detetar padrões de comunicação anormal , comunicação a horas anómalas c) Respostas dos servidores HTTPS serem incomumente longas e contínuas, se forem para países específicos. Detetar padrões de comunicação anormal como respostas com o mesmo tamanho, a horas anormais com algum tipo de repetição para o mesmo host ou hosts na mesma rede.