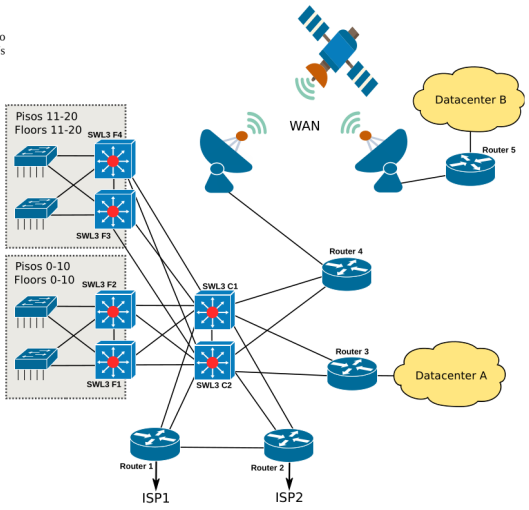
normal_6_julho_2022

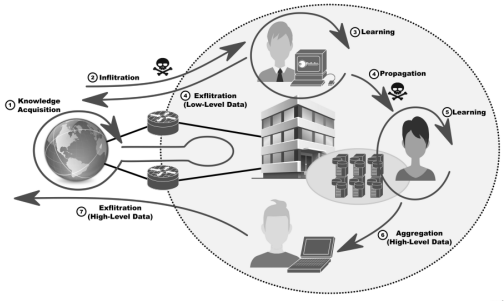
- Nos switches Layer 2 dos edifícios 1 e 2 estão configuradas portas de acesso para as VLANs 1,2,3,4,5 e 6.
- As ligações entre os switches Layer2 e os switches Layer3 F1 a F4 são feitas usando ligações trunk/inter-switch com permissão de transporte para todas as VLANS;
- Os interfaces entre os switches 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 dois Datacenters internos para serviços internos (Datacenters A e B);
- Existe uma ligação WAN via satélite que suporta ligações IPv4 entre a rede da empresa e um datacenter remoto (Datacenter B);
- Os switches Layer3 e routers 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.



Ex. 1

Question: No contexto das fases de um ataque como propósito de roubo de dados a uma rede empresarial, explique porque a deteção e mitigação do ataque é muito mais difícil durante a fase de infiltração do que durante as fases de propagação e exfiltração. (3.0 valores)
Prof. Answer:
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 sujeito 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 legitimo/aceitável (ainda que subtilmente) no que respeita a quantidades de tráfego, rácios de tráfego, portos e protocolos usados, matrizes de tráfego, horas de comunicação, padrões temporais de comunicação, etc.…
Answer:
Num ataque com o propósito de roubo de dados a uma rede empresarial, o processo geralmente envolve várias fases. Compreender essas fases é crucial para a implementação de estratégias eficazes de detecção e mitigação. As fases típicas de um ataque incluem:

1. **Reconhecimento (Reconnaissance)**: O atacante coleta informações sobre o alvo para identificar potenciais vulnerabilidades. Isso pode incluir sanning de portas, pesquisa de informações públicas e uso de engenharia social.
2. **Infiltração (Initial Compromise)**: O atacante ganha acesso inicial à rede. Isso pode ser feito por meio de phishing, exploração de vulnerabilidades de software, credenciais comprometidas, entre outros métodos.
3. **Estabelecimento de Persistência (Establishing Foothold)**: O atacante estabelece mecanismos para manter o acesso à rede, como a instalação de backdoors ou malwares persistentes.
4. **Escalação de Privilégios (Privilege Escalation)**: O atacante procura obter níveis mais altos de acesso para controlar mais recursos na rede.
5. **Movimentação Lateral (Lateral Movement)**: O atacante move-se através da rede, comprometendo outras máquinas e contas, expandindo seu controle sobre a rede.
6. **Exfiltração (Exfiltration)**: O atacante transfere dados valiosos da rede da empresa para fora, geralmente para servidores controlados pelo atacante.



Dificuldades de Detecção e Mitigação Durante a Fase de Infiltração

A detecção e mitigação durante a fase de infiltração são mais difíceis por várias razões:

- **Subtileza das Técnicas Utilizadas**: Técnicas de infiltração, como spear phishing e exploração de vulnerabilidades zero-day, são projetadas para serem difíceis de detectar. Essas técnicas podem parecer atividades normais ou benignas, dificultando a identificação por sistemas de segurança tradicionais.
- **Baixo Perfil de Atividade**: Durante a infiltração, o atacante geralmente tenta minimizar sua presença para evitar detecção. As atividades

podem ser espaçadas no tempo e integradas nas operações normais da rede, tornando-as menos suspeitas.

- **Falta de Assinaturas Conhecidas**: Ataques de infiltração podem envolver novas ameaças ou técnicas ainda não catalogadas em bases de dados de assinaturas de malware, como no caso de exploits de dia zero.
- **Necessidade de Contexto**: Detectar a infiltração pode exigir a correlação de eventos de baixa prioridade que, isoladamente, não indicam uma ameaça. Isso exige um contexto amplo e análises avançadas que nem sempre são viáveis em tempo real.

Fases de Propagação e Exfiltração

Em contraste, as fases de propagação (movimentação lateral e escalação de privilégios) e exfiltração tendem a ser mais ruidosas e mais fáceis de detectar:

- **Maior Atividade de Rede**: Movimentação lateral e exfiltração geralmente envolvem volumes maiores de tráfego de rede e acesso a múltiplos sistemas, o que pode ser mais facilmente detectado por anomalias nos padrões de tráfego.
  - Comunicações anomalas entre dispositivos (botnets), que podem ser analisadas pelo histórico da rede e construção de matriz de tráfego
- **Uso de Ferramentas Comuns**: Durante essas fases, os atacantes muitas vezes utilizam ferramentas de hacking conhecidas que podem ser identificadas por sistemas de detecção de intrusões (IDS) e antivírus.
- **Assinaturas e Indicadores de Comprometimento (IoCs)**: As ações realizadas durante essas fases frequentemente correspondem a padrões conhecidos e assinaturas que podem ser detectadas por soluções de segurança.
- **Comportamentos Anômalos**: A exfiltração de dados pode ser identificada através da detecção de comportamentos anômalos, como grandes volumes de dados sendo enviados para locais não habituais ou acessos a dados fora do horário normal de operação.
  - Analisar maquinas e seus níveis de permissões, a quem pertencem e com modelos de comportamento identificar o seu padrão. Ver a plataforma com quem estão a comunicar (é possivel ver mesmo com SSL) e analisar se se tráfego de tráfego benigno ou não (será mais fácil bloquear essas aplicações, pois a análise de plataformas externos é difícil)

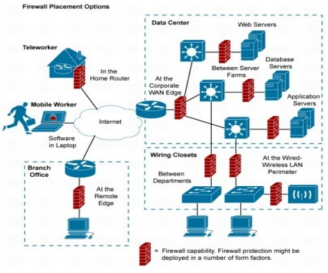
Conclusão

Em resumo, a fase de infiltração é mais difícil de detectar e mitigar devido à natureza subtil e sofisticada das técnicas utilizadas, a necessidade de um contexto amplo para correlacionar atividades aparentemente benignas, e a falta de assinaturas conhecidas para novos métodos de ataque. Em contrapartida, as fases de propagação e exfiltração são mais propensas a gerar comportamentos anômalos e atividades detectáveis devido ao aumento do volume de atividades e ao uso de ferramentas e técnicas mais ruidosas.

Ex. 2

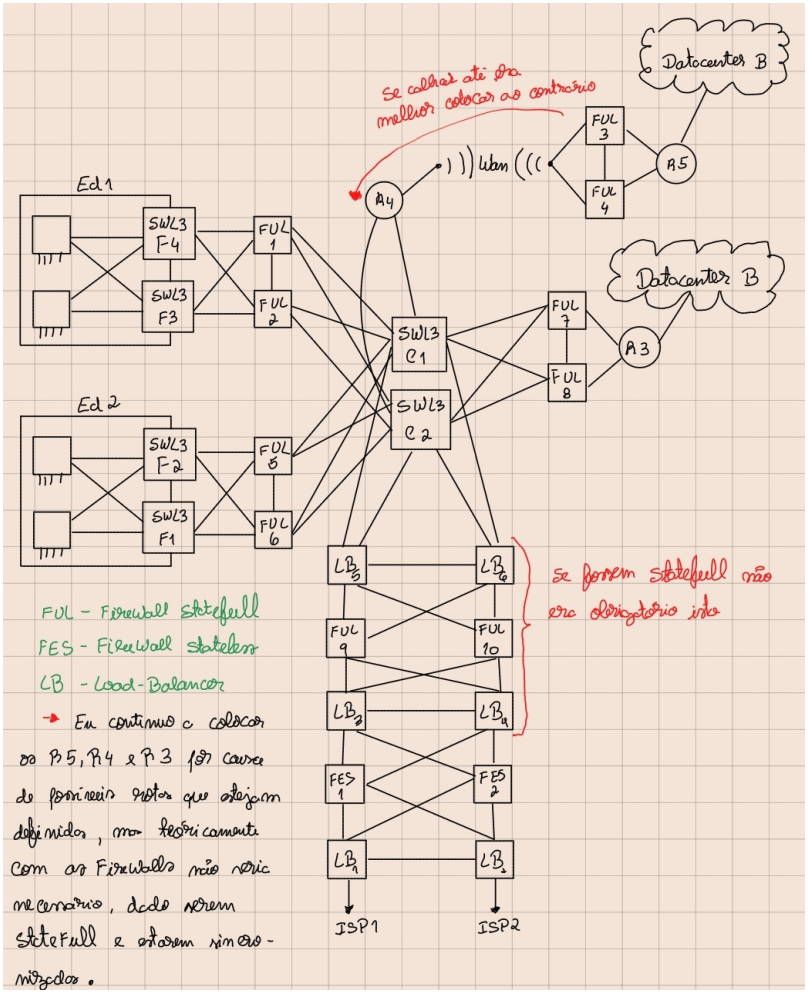
Question: Proponha um conjunto de alterações arquiteturais à rede empresarial de modo a protegê-la de ataques DDoS e permitir a implementação de múltiplos controles de fluxo de tráfego. Desenhe um novo diagrama de rede com as alterações/adições, indicando o tipo, funcionalidade e/ou modo de operação de cada equipamento. (4.0 valores)
Prof. Answer:
Para proteger de ataques DDoS e controlar fluxos com origem na Intenet, colocar na zona de acesso 2 firewals 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.

- Network must be protected at multiple levels and locations



Não é preciso LB para as novas FW nas áreas porque elas são state-full e sincronizadas, logo não precisando de um LB para encaminhar os

pacotes para a firewall correta, isto é pior em caso de DDOS, mas como ele já é tratado pelas firewalls iniciais...



Ex. 3

Question: Assumindo que a empresa deseja **permitir** que os terminais (não servidores) internos **apenas** acedam a serviços **HTTPS** na Internet (porta TCP 443). E em paralelo **implementar** um conjunto de servidores para prestação de serviços ao público (Internet), os novos serviços incluem:

- **(i):** um servidor Web HTTPS com vários sites/domínios (porta TCP 443)
- **(ii):** um servidor de e-mail (porta TCP 465 para comunicação SMTP segura entre servidores e porta TCP 993 para acesso de cliente via IMAPS)
  Proponha as alterações de arquitetura de rede necessárias e apresente uma lista das regras de firewall/ controle de fluxo de tráfego (de alto nível) nos vários locais. (4.0 valores)
  Answer:
  Dado que agora teremos um conjunto de servidores internos, acedíveis tanto por clientes internos como a internet, precisamos de criar uma DMZ (De-militarized Zone). A nível da rede, esta zona deve estar ligada às Firewalls Statefull de acesso à internet, possivelmente com um ou dois (redundancia) LB no meio, mas sincronizados, para garantir que enviam para a FW correta, dado estas serem statefull, mas não estarem sincronizadas. Atenção que o tráfego para a DMZ **nunca** deve passar pela rede do core!
  Colocar nas Firewalls Statefull as regras:
- Bloquear tudo por default -> everything is forbidden, until explicitly allowed
- IN → OUT: Tráfego dos terminais com endereços IP de terminais para o porto TCP 443.
- OUT ou DMZ → IN: Respostas de sessões já estabelecidas (estabished/related connections).
- 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 SMTP para porto TCP (465). Poderia-se ter um método de validação dos endereços externos via DNS.

Ex. 4

Question: Proponha uma solução de interligação utilizando a ligação WAN da empresa, entre um conjunto de servidores de base de dados no Datacenter A e Datacenter B, capaz de fornecer confidencialidade ao nível de rede para o tráfego de sincronização dos dados dos servidores (e somente esse tráfego). Apresente também as alterações necessárias às políticas de controlo de fluxo de tráfego nas firewalls para permitir o

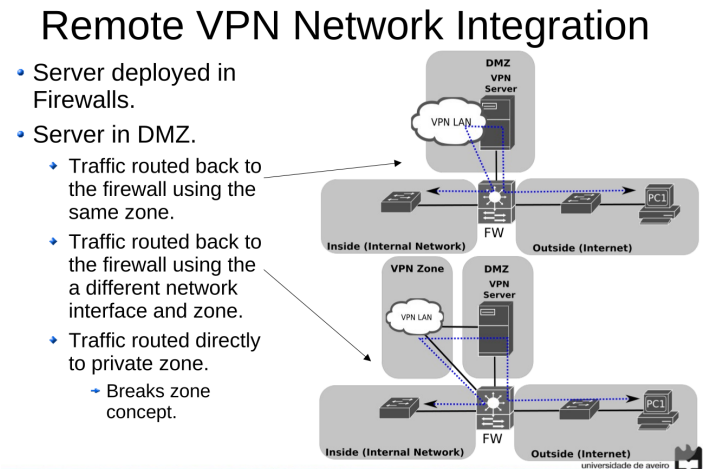
estabelecimento da ligação segura e transmissão de dados. (3.0 valores)
Answer:
Dado estes datacenters serem conhecidos e serem apenas dois, criamos uma VPN site-to-site usando um túnel IPsec ponto-a-ponto (não é preciso multiponto) do tipo ESP (Encapsulating Security Payload), entre o Router 3 e o Router 5. O ESP já permite autorização, autenticação das duas partes e encriptação dos pacotes trocados. O tráfego deverá ser encaminhado usando políticas de encaminhamento (PBR) nesses routers, possivelmente com base no IP de destino (gama reservada para cada conjunto de servidores), endereço do servidor que inicia a troca ou outro.Exceções para as firewall statefull 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.

Ex. 5

Question: Assumindo que a empresa deseja implementar tele-trabalho onde os utilizadores remotos terão acesso privilegiado a dois servidores HTTPS (porta TCP 443) no Datacenter A. Proponha uma solução integrada que permita o acesso dos utilizadores remotos e controlar o acesso aos serviços. Deverá incluir na sua proposta as alterações necessárias às políticas de controlo de fluxo de tráfego nas firewalls. (3.0 valores)
Answer:
É necessário criar uma User VPN (client-to-site VPN), OpenVPN, SSTP, L2TP, PPTP. Colocar um servidor na DMZ, onde os clientes possam estabelecer essa ligação VPN.
Regras FW statefull 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 (established/related connections).
- DMZ/VPN → IN: Tráfego dos endereços IP dos clientes VPN para para os endereços IP e portos TCP 443 dos 2 servidores no DCA (Datacenter A).
- IN → DMZ/VPN: Respostas de sessões já estabelecidas (established/related connections).
  Regras FW stateful do acesso Datacenter A:
- 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 (established/related connections).



A melhor opção seria mesmo colocar uma zona extra ou VLAN, invés de reutilizar diretamente a rede da DMZ, por causa de ser mais simples saber os clientes que acedem pela VPN ou não, na maneira que circulam pela rede e regras nas subsequentes FW.

Ex. 6

Question: Proponha um sistema SIEM, incluindo o processo de coleta de dados e a definição de regras de alerta, capaz de alertar para:

Ex. 6.a)

Question: Tentativas de acesso ilegítimo (com logins falhados) a servidores no Datacenter B com origem em terminais internos. (1.5 valores)
Answer:
Temos duas opções:

- A autenticação (situam-se ao nível do serviço), logo é preciso ir buscar os logs ao serviço (autenticação, BD, etc.). Usar o remote rsyslog, para descarregar os logs remotos (também pode ser feito por SFTP ou FTP, mas o rsyslog permite logo fazer operações e simplificação dos logs no cliente e é mais orientado para este caso). De seguida, caso haja N falhas de logins do mesmo endereço IP/username ou suspeitas de acesso ilegitimo (localização duvidosa do dispositivo, já existe uma conta com sessão iniciada, dispositivo não certificado...) alertar ou registar a informação.
- Sempre que o user falha o login, aparece uma página nova (não pode ser acedida em mais nenhum caso), que diz que o utilizador falhou o login e assim, é possível o SIEM identificar as tentativas de login falhado, sem precisar de acesso ao serviço (servidor) em si. No entanto

requer que tenha acesso à chave de desencriptação do tráfego, para podes verificar o URL, dado que este é encriptado em tráfego SSL TLS, apenas sendo possível visualizar o dominio de acesso. Dado isto, caso não seja possível visualizar o dominio, pode sempre recorrer ao rsyslog para obter a informação de acesso à página, sendo mais simples verificar as tentativas falhadas com esta abordagem.

Ex. 6.b)

Question: Possível comunicação de C&C (command and control) via HTTPS entre um atacante externo e máquinas internas comprometidas por agentes de uma Botnet. (1.5 valores)
Answer:
C&C (Command and Control). Quando uma máquina é comprometido, o virus pode tentar propagar-se para outras máquinas (botnet). Como detetar? -> Dados. A maneira mais simples é ver quem está a falar com quem (histórico e presente). Se for uma máquina que falava com uns utilizadores de vez em quando e de um momento começa a tentar falar com vários, na mesma rede... É preciso saber quem falou com quem. Usar o **netflow** nos routers, para ver quem está a falar com quem e criar uma matriz de flow (Não é trivial). Mais simples, é ter as firewalls entre os edifícios e saber quem comunicou com quem, entre VLANs (dentro da mesma vlan não dá). Se tiver acesso aos switches, é possível aceder às tabelas de Layer 2 e saber quem comunica com quem (Genérico, tráfego). Resumindo:

- Porta de mirroring no switch, onde o tráfico é redirecionado e permite fazer uma matriz de tráfego. É uma solução mais pesada e menos eficiente.
- Ter acesso ao switch, a nível da comunicação de Layer 2 e criar a matriz de tráfego a partir disso
- Usar as firewalls para analisar tráfego entre VLANs e construir a matriz de comunicação nela
  Em relação ao DNS (Mau uso de um serviço seguro. Máquinas a gerar tráfego IP em DNS), analisar os logs do DNS e ver os pedidos dos clientes, ou usar as firewalls. O rácio de tráfego dns de envio/receção, é mais ou menos constante. Se de repente, começa-se a efetuar muito DNS (ao nível da rede ou serviços), mas o tráfego não DNS tbm aumentou, então deve ser normal. Caso, então pode ser uma botnet a tentar comunicar. Se tiver acesso aos logs do servidor DNS, então podemos ver a resolução dos pedidos, gera bytes muito grandes e anómalos
  Em relação ao HTTPS, analisar tráfego interno e externo nas firewalls (saber qual usando distinção entre IPs privados e públicos), recorrendo a logs do rsyslog ou comunicação do netflow (para a parte de botnet). De seguida, detetar sessões HTTPS com rácio up/down anormal, comunicação para endereços IP nunca
  contactados ou em países/localizações especificas (nunca usadas), padrões de comunicação temporal
  anormal, comunicações a horas anómalas, etc… Ou combinações de várias destas coisas. O ideal é sempre ter um histórico de comparação e muitas vezes os problemas advêm de confusão com comportamento normal, por exemplo, se é permitido acesso ao google drive na empresa, eu posso fazer ex-fill de dados para ele, que o SIEM pode detetar como comportamento normal (ah, é só um user a fazer backup dos seus dados ou alguns ficheiros de sincronização), mas se esses serviços de transferência forem bloqueados, então é muito mais fácil detetar picos em upload de dados e agir logo.
  Categorizar utilizadores tbm ajuda (não pode ser individualmente por causa de leis de privacidade), em que colocamos perfis gerados por análise nas máquinas de cada user, de acordo com o histórico (power-user, regular-user, light user) e dps caso comece a haver muito overlap entre user, soar alarmes. Ter atenção a falsos positivos -> segunda-feira (primeiro dia de volta, mais tráfego), voltar de férias, fins de semana prolongados, férias, etc.