Resumão - Segurança em redes de computadores

Network Security

Fase dos ataques

Aquisição de conhecimento

Esta fase envolve a recolha de informação sobre a rede alvo, como por exemplo, endereços IP, portas abertas, etc.

Técnicas de aquisição de conhecimento:

- *Ping sweep*: envio de pacotes *ICMP* para descobrir endereços IP ativos;
- *Port scanning*: descobrir portas abertas num sistema;
- *OS fingerprinting*: descobrir o sistema operativo de um sistema.

Formas de mitigar essa aquisição:

- Bloqueio de portas;
- Restrição de protocolos (p/ portas específicas);
- Definição de regras de *firewall*;
- Não uso de banners.

Infiltração

Uma vez que o atacante tem informação suficiente, o próximo passo é a infiltração na rede, que envolve o uso do conhecimento público adquirido para ganhar acesso à parte privada da rede.

Nesta fase é muito **mais dificil** de detetar e mitigar o ataque, pois ele é feito com base em conhecimento da rede prévio, então estas mitigações deveriam ter sido feitas na fase anterior. Sendo então mais fácil de detetar e mitigar o ataque nas fases de propagação e filtragem.

> **Nota**: a infiltração pode ser feita de várias formas, como por exemplo, através de *phishing*, *malware*, etc.

Propagação

Uma vez infiltrado na rede, o atacante irá tentar propagar-se pela rede, de forma a ganhar acesso a mais recursos.

Esta fase é feita através de metodologias como:

- Exploração de credenciais;
- Exploração de vulnerabilidades;
- *Spoofing* de utilizadores e serviços.

Esta fase é **mais fácil** de detetar e mitigar

A deteção e mitigação pode ser feita através de técnicas como:

- *Honeypots*;
- Definição de regras de *firewall*;
- *Intrusion Detection Systems* (IDS);
- *Intrusion Prevention Systems* (IPS).

Porém esta fase é a fase mais perigosa, pois implica que o atacante já tenha acesso a recursos da rede.

Agregação e **Exfiltração**

Na fase de **agregação**, atacante irá tentar agregar (juntar) os recursos que conseguiu obter na fase de propagação, de forma a obter mais recursos.

Na fase de **exfiltração**, atacante irá tentar retirar informação da rede, de forma a obter informação sensível.

A fase de agregação e exfiltração podem ser feitas de maneira:

- **Interna**: através de canais existentes na rede (facilmente detetável);
- **Externa**: pode ser feito de duas formas:
    - **Usando canais existentes na rede**: copiar ficheiros, email, etc. Esta é mais fácil de detetar;
    - **Escondendo essa informação em canais permitidos através de comunicações licitas**: mais lentas e difíceis de detetar (e.g. dados incorporados em mensagens de texto e de voz).

Para mitigar a maneira **externa**, a melhor forma é a **monitorização de tráfego**. E isto é feito avaliando métricas como:

- Mean Time Between Failures (MTBF)
    - Average time between failures (hardware and/or software).
    - General or per device/service.
- Mean Time to Recovery (MTTR)
    - Average time between failure and recovery (hardware and/or software).
- Mean Time to Detect (MTTD) Average time between intrusion and detection.
- Mean Time to Acknowledge (MTTA)
    - Average time between detection and start of countermeasures deployment.
- Mean Time to Contain (MTTC)
    - Average time between start of countermeasures deployment and complete mitigation.
- Mean Time to Resolve (MTTR)
    - MTTA+MTTR

Network Access Control

DDOS

DDOS é a abreviatura de Distributed Denial of Service. É um ataque que tem como objetivo tornar um serviço indisponível para os utilizadores. Este ataque é feito através de um grande número de dispositivos, que enviam um grande volume de tráfego para o servidor alvo. Este tráfego é tão grande que o servidor não consegue processar todos os pedidos, tornando o serviço indisponível.

Segurança de Redes

- **Firewalls**: Barreira que protege uma rede interna contra acessos não autorizados.

- **IDS/IPS**: Intrusion Detection System/Intrusion Prevention System. Sistemas de deteção e prevenção de intrusões que monitorizam e analisam o tráfego de rede.

Tipos de Firewalls

Nível de Sessão(L4)

- **Circuit-level Gateways**: Monitorizam a handshakes do TCP(todo o flow do TCP) para assegurar que a sessão é legítima, ou seja, handshakes significa que a conexão foi estabelecida.
- **Vantagem**: Controle mais detalhado das sessões, ou seja, monitoriza o flow do TCP.
- **Desvantagem**: Mais consumo de recursos.

Nível de Aplicação(L7)

- **Proxies**: Inspecionam dados da aplicação para garantir que comportamentos corretos sejam seguidos.
- **Vantagem**: Alta granularidade e proteção contra ameaças específicas de aplicação.
- **Desvantagem**: Alto consumo de recursos.

Stateful

- **Stateful Inspection**: Monitoriza o estado da conexão e faz a filtragem de pacotes com base nas regras da sessão e não nas regras do pacote.
- **Vantagem**: Maior segurança e controle dinâmico, ou seja, regras bidirecionais automáticas.
- **Desvantagem**: Mais complexo e consome mais recursos.

> **Nota**: É inutil na **primeira** linha de defesa da rede.

Stateless

- **Packet Filtering**: Filtra pacotes com base em regras de filtragem de pacotes individuais.
- **Vantagem**: Mais simples e consome menos recursos.
- **Desvantagem**: Menos segurança e controle.

Aplicação de Load Balancers

Load Balancers são usados para distribuir o tráfego de rede ou aplicações entre vários servidores para garantir que nenhum único serviço fique sobrecarregado.

- **Benefícios**:
  - **Distribuição de carga**: Garante uma distribuição uniforme do tráfego, prevenindo sobrecarga num unico servidor.
  - **Alta Disponibilidade**: Melhora a disponibilidade dos serviços ao redirecionar o tráfego para servidores operacionais.
  - **Escalabilidade**: Facilita a adição de servidores para lidar com o aumento do tráfego.

Resposta

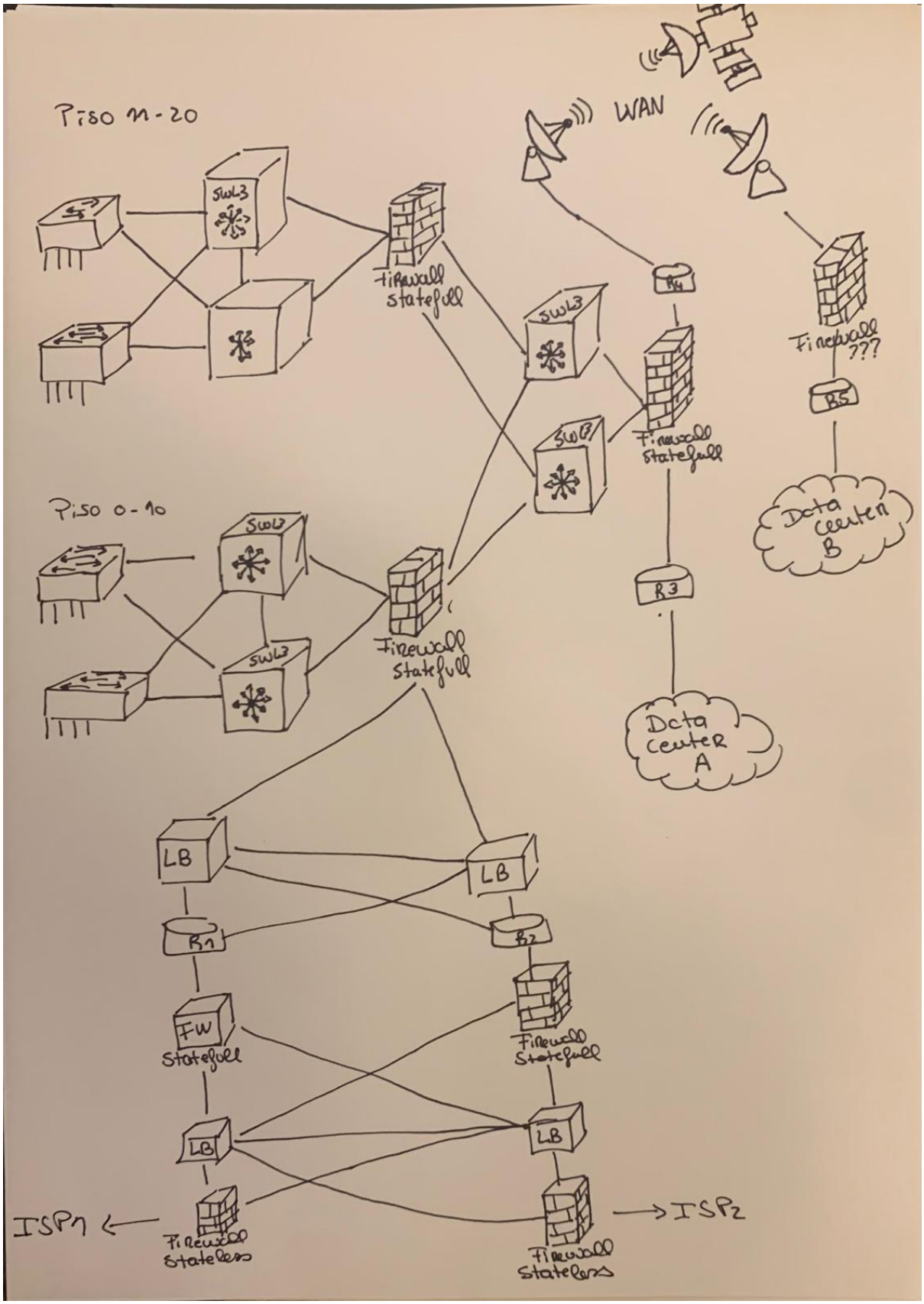
Exame 6 de julho de 2022

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)

R: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.

Alterações Arquiteturais

1. **Firewalls Stateless**:
    - Colocar dois firewalls stateless na zona de acesso à internet (antes dos routers de borda).
    - Função: Filtrar tráfego básico e mitigar ataques DDoS volumétricos na primeira linha de defesa.
2. **Load Balancers**:
    - Implementar dois load balancers logo após os firewalls stateless.
    - Função: Distribuir o tráfego de entrada uniformemente entre os servidores e reduzir a carga em qualquer ponto único.
3. **Firewalls Stateful**:
    - Colocar dois firewalls stateful após os load balancers.
    - Função: Inspecionar pacotes em profundidade, gerir estados de conexão e fornecer uma segunda camada de defesa.
4. **Load Balancers Internos (Opcional)**:
    - Adicionar dois load balancers na ligação ao core.
    - Função: Equilibrar o tráfego entre diferentes segmentos da rede interna.
5. **Firewalls Internos**:
    - Colocar firewalls stateful adicionais para proteger e controlar cada zona do edifício (pisos 0-10 e 11-20) e cada datacenter (A e B).
    - Função: Proteger segmentos internos da rede, controlar acesso entre diferentes zonas e segmentar o tráfego de forma granular.
6. **Redundância**:
    - Implementar redundância de equipamentos e ligações para garantir alta disponibilidade e resiliência contra falhas.



Network Flow Control

Demilitarized Zone (DMZ)

Uma DMZ é uma rede de perímetro entre a rede interna e a rede externa, onde se encontram os serviços que são acessíveis ao exterior.

É uma zona **semi-protegida**, onde se encontram os serviços que são acessíveis ao exterior, então deve-se sempre a assumir que qualquer máquina na DMZ encontra-se em risco.

Firewalls

Tipos de *firewall*

- **Stateful**: controla o tráfego com base em fluxos de tráfego/sessões. As regras definidas são por norma bidirecionais (entrada e saída).
- **Stateless**: análise a todos os pacotes individualmente e aplica regras de filtragem. As regras definidas são unidirecionais (entrada ou saída).

Posicionamento de *Firewall*

Firewall Stateless é ideal na primeira camada de defesa da rede de modo a prevenir de ataques *DoS* e *DDoS*, pois permite boa performance sobre altas taxas de tráfego.

Firewall Stateful é ideal na camada interna da rede de modo a prevenir de ataques mais sofisticados, como *IP Spoofing* e *Port Scanning*.

Tem dois tipos de posicionamento de *firewall*:

- *Exposed border router*: *firewall* antes do *router*.
- *Protected border router*: *firewall* depois do *router*.

Zonas/Grupos *Firewall*

Representa uma coleção de interfaces de rede que têm um nível de segurança comum, isto é usado para definir regras de origem e destino.

Secure IP Connections

Tuneis de tráfego

Tem como principal propósito garantir que o pacote de dados chega ao destino independentemente do caminho que ele percorre, mesmo que os intermediários não suportem o protocolo de rede do pacote.

Isto é feito adicionando um (ou mais) cabeçalho extra ao pacote original, que é usado para encapsular o pacote original.

Tipos de IP *tunnels*

- **IPv4-in-IPv4**: encapsula um pacote IPv4 dentro de outro pacote IPv4.
- **GRE (Generic Routing Encapsulation)-IPv4**: O protocolo original é encapsulado num pacote GRE e é entregue usando o protocolo IPv4.
- **IPv6-IPv6**: encapsula um pacote IPv6 dentro de outro pacote IPv6.
- **GRE-IPv6**: O protocolo original é encapsulado num pacote GRE e é entregue usando o protocolo IPv6.
- **IPv6-IPv4**: pacotes IPv6 são encapsulados em pacotes IPv4.
- **IPv4-IPv6**: pacotes IPv4 são encapsulados em pacotes IPv6.

IPsec

O IPsec não é um protocolo, mas um conjunto de protocolos.

Os seguintes protocolos compõem o conjunto do IPsec:

- **AH (Authentication Header)**: O protocolo AH garante que os pacotes de dados sejam de uma fonte confiável e que os dados não tenham sido adulterados, como um selo à prova de adulteração em um produto de consumo. Esses cabeçalhos não fornecem nenhuma criptografia; eles não ajudam a ocultar os dados dos invasores.
- **ESP (Encapsulating Security Payload)**: O ESP cifra o cabeçalho IP e o conteúdo para cada pacote — a menos que o modo de transporte seja usado, caso em que ele cifra apenas o conteúdo. O ESP adiciona seu próprio cabeçalho e um trailer a cada pacote de dados.

Qual é a diferença entre o modo de túnel IPsec e o modo de transporte IPsec?

O modo de túnel IPsec é usado entre dois routers dedicados, com cada router atuando como uma extremidade de um "túnel" virtual por meio de uma rede pública. No modo de túnel IPsec, o cabeçalho IP original que contém o destino final do pacote é cifrado, além do conteúdo do pacote. Para informar aos routers intermediários para onde encaminhar os pacotes, o IPsec adiciona um novo cabeçalho IP. Em cada extremidade do túnel, os routers decifram os cabeçalhos IP para entregar os pacotes aos seus destinos.

No modo de transporte, o conteúdo de cada pacote é cifrado, mas o cabeçalho IP original não. routers intermediários são, portanto, capazes de visualizar o destino final de cada pacote — a menos que um protocolo de encapsulamento separado (como o GRE) seja usado.

Security Associations (SA)

Uma *Security Association* (SA) é um acordo entre dois dispositivos de rede sobre como eles se comunicarão de forma segura. Uma SA é composta por um conjunto de parâmetros de segurança, como algoritmos de criptografia e autenticação, chaves e outros valores.

ISAKMP (Internet Security Association and Key Management Protocol)

O ISAKMP é um protocolo de gestão de chaves que permite que dois dispositivos de rede estabeleçam uma SA. O ISAKMP é usado para negociar os parâmetros de segurança que compõem uma SA.

IKE (Internet Key Exchange)

O IKE é um protocolo que usa o ISAKMP para estabelecer uma SA. O IKE é usado para autenticar os dispositivos de rede e negociar os parâmetros de segurança que compõem uma SA (Security Association).

Usa o H.A.G.L.E. (Hash, Authentication, Group, Lifetime, Encryption) para estabelecer a SA (Security Association).

O IKE/ISAKMP fornece um método para estabelecer uma SA entre dois dispositivos de rede. O IKE/ISAKMP é usado para negociar os parâmetros de segurança que compõem uma SA e autenticar os dispositivos de rede.

IPSec NAT Traversal

O NAT Traversal é um método que permite que dispositivos de rede estabeleçam uma conexão IPsec através de um dispositivo NAT (Network Address Translation, que traduz endereços IP privados em endereços IP públicos).

Regras de Firewall para IPsec

Para ter o IPsec a funcionar corretamente, é necessário configurar regras de firewall, aplicando as seguintes regras:

- Definir regras de firewall para permitir o tráfego de estabelecimento e negociação do tunel (IKE (Internet Key Exchange) e ISAKMP (Internet Security Association and Key Management Protocol)).
- Definir regras de firewall para permitir o tráfego IPsec (UDP 500, UDP 4500, protocolos ESP e AH).

Exemplo de pergunta de IPsec (Exame junho 2023)

Proponha uma solução de comunicação IPv4 ao nível da rede e respetivas alterações nas regras das Firewalls que:

- Garanta que o tráfego UDP das máquinas virtuais existentes no Datacenter A para um conjunto conhecido de servidores AWS da Amazon (a lista de redes IP são conhecidas) seja encaminhado de forma que garanta confidencialidade. (2.0 valores)
- Garanta que o tráfego UDP das máquinas virtuais existentes no Datacenter A para um conjunto de múltiplas máquinas virtuais em diversos servidores (em diferentes localizações geográficas) na Cloud da Microsoft seja transmitido de forma segura que garanta confidencialidade. Considere que as redes virtuais e servidores remotos são extremamente dinâmicos (são criados e destruídos frequentemente). (2.5 valores).

R: Para garantir a confidencialidade do tráfego UDP das máquinas virtuais no Datacenter A para os servidores AWS conhecidos e para as máquinas virtuais dinâmicas na Cloud da Microsoft, podemos seguir as seguintes abordagens:

Para propor uma solução de comunicação IPv4 ao nível da rede e as respetivas alterações nas regras das Firewalls que garantam a confidencialidade do tráfego UDP das máquinas virtuais existentes no Datacenter A, consideremos as seguintes abordagens:

Parte a: Tráfego UDP para servidores AWS conhecidos

Solução:

1. **Utilização de VPN (Virtual Private Network):**
    - **Configuração de VPNs Site-to-Site** entre o Datacenter A e os servidores AWS conhecidos. Utilizando IPsec para garantir a confidencialidade e a integridade dos dados transmitidos.
    - **Regras de Firewall:**
        - Permitir tráfego UDP entre o Datacenter A e as redes IP conhecidas dos servidores AWS, passando pela VPN.
        - Bloquear qualquer outro tráfego não autorizado que não passe pela VPN.
        - Exemplo de regra de firewall:
            - **Permitir:** UDP desde `192.168.96.0/20` para as redes IP conhecidas dos servidores AWS pela VPN (Portas UDP específicas que as aplicações utilizam).

- **Bloquear:** Qualquer outro tráfego UDP para as redes IP dos servidores AWS.

Parte b: Tráfego UDP para múltiplas máquinas virtuais na Cloud da Microsoft

Solução:

1. **Utilização de VPN Dinâmica com SD-WAN (Software-Defined Wide Area Network):**
    - **Configuração de VPNs Dinâmicas:** Utilizando soluções de SD-WAN que permitem a criação dinâmica de túneis VPN IPsec para diferentes localizações na Cloud da Microsoft.
    - **Integração com Azure Virtual WAN:** Configurar a rede para utilizar o serviço Azure Virtual WAN, que facilita a conectividade segura e escalável entre o Datacenter A e as máquinas virtuais na Cloud da Microsoft.
    - **Regras de Firewall:**
        - Permitir tráfego UDP para a Cloud da Microsoft através da VPN dinâmica configurada.
        - Utilizar listas de controle de acesso (ACLs) e regras de firewall dinâmicas que se atualizem conforme as mudanças nas redes virtuais da Cloud da Microsoft.
        - Exemplo de regra de firewall:
            - **Permitir:** UDP desde `192.168.96.0/20` para qualquer IP na Cloud da Microsoft pela VPN (portas UDP específicas que as aplicações utilizam).
            - **Bloquear:** Qualquer outro tráfego UDP não autorizado.

Remote Access

VPN-IPsec

Uma VPN (Virtual Private Network) é uma rede privada virtual que permite que os utilizadores acedam a rede de uma organização de forma segura pela Internet.

- **Site-to-Site VPN**: Conecta duas redes remotas, como filiais de uma empresa, através de uma conexão segura. Existem duas variantes que usam o IPsec:
    - IPsec VPN: With static or dynamic configuration
    - IPsec + GRE VPN: Dynamic Multipoint VPN
- **Client-to-Site VPN (Remote Access VPN)**: Permite que os utilizadores remotos se conectem à rede da organização a partir de qualquer local. Existem várias opções de VPN para acesso remoto, incluindo:
    - L2TP/IPsec: Combina o L2TP para criar túneis com o IPsec para autenticação e criptografia.
    - OpenVPN: Utiliza SSL/TLS para a cifragem das sessões VPN.
    - SSL/TLS VPN: Usado para acesso remoto a aplicações web.

Conceito Fundamental de Acesso Remoto

Acesso Remoto: Permite que utilizadores acedam a recursos de rede a partir de locais remotos, utilizando protocolos seguros e métodos de autenticação para garantir a integridade e segurança dos dados transmitidos.

Protocolos Comuns de Acesso Remoto

1. **L2TP/IPsec**:

- **L2TP** (Layer 2 Tunneling Protocol): Protocolo que cria túneis seguros para a transmissão de dados.
- **IPsec** (Internet Protocol Security): Protocolo que proporciona autenticação e criptografia dos pacotes transmitidos através do túnel L2TP.
- **Portas Utilizadas**:
  - UDP 500: Para o estabelecimento inicial da conexão (IKE).
  - IP protocolo 50: Encriptação ESP (Encapsulating Security Payload).
  - IP protocolo 51: Autenticação AH (Authentication Header).
  - UDP 4500: Para travessia NAT (NAT traversal).
  - UDP 1701: Para o próprio protocolo L2TP【32†source】.

2. **OpenVPN**:

   - Utiliza SSL/TLS para a encriptação das sessões VPN.
   - **Porta Utilizada**: UDP 1194 por defeito, mas pode ser configurado para usar TCP se necessário【32†source】.

3. **Autenticação**:

   - **Pre-shared keys**: Chaves partilhadas previamente entre o cliente e o servidor.
   - **RADIUS/LDAP**: Protocolos para autenticação centralizada.
   - **RSA com CA incorporada ou externa**: Autenticação baseada em certificados digitais.
   - **Distribuição Segura de Certificados/Credenciais**: A distribuição de certificados e credenciais deve ser feita de forma segura, através de serviços web, SSH, etc.【32†source】.

Implementação de VPNs para Acesso Remoto

Servidor VPN na DMZ: Para garantir a segurança das comunicações, é comum implementar o servidor VPN na DMZ (Demilitarized Zone), uma zona de rede segura que atua como uma camada de proteção adicional entre a rede interna e a externa.

Configuração das Firewalls: As firewalls devem ser configuradas para permitir e controlar o tráfego VPN de forma segura.

Regras de Firewall para Acesso VPN

- **De Fora para a DMZ (OUT → DMZ)**:
  - Permitir tráfego para os endereços IP e portas TCP/UDP do servidor VPN.
  - Exemplo: `permit ip any host <IP_Servidor_VPN>`

- **De Dentro para Fora (DMZ → OUT)**:
  - Permitir respostas de sessões já estabelecidas.
  - Exemplo: `permit established`

- **Da VPN para a Rede Interna (DMZ/VPN → IN)**:
  - Permitir tráfego dos endereços IP dos clientes VPN para os endereços IP e portas TCP 443 dos servidores no Datacenter A.
  - Exemplo: `permit tcp <IP_Clientes_VPN> any eq 443`

- **Da Rede Interna para a VPN (IN → DMZ/VPN)**:
    - Permitir respostas de sessões já estabelecidas.
    - Exemplo: `permit established`

Controlo de Fluxo de Tráfego

Tipos de Firewalls:

1. **Firewall Stateless**:
    - Filtra pacotes com base em regras simples, sem manter o estado das conexões.
    - Vantagem: Rápido e consome poucos recursos.
    - Utilização: Primeira linha de defesa contra DDoS.
2. **Firewall Stateful**:
    - Mantém o estado das conexões e inspeciona pacotes de forma mais detalhada.
    - Vantagem: Maior segurança e controlo sobre o tráfego.
    - Utilização: Segunda linha de defesa, inspecionando pacotes em profundidade.

Load Balancers:

- Distribuem o tráfego de rede entre múltiplos servidores para evitar sobrecarga e garantir alta disponibilidade.
- **Algoritmos de Balanceamento**:
    - **Round Robin**: Distribui solicitações sequencialmente.
    - **Least Connections**: Direciona solicitações para o servidor com menos conexões ativas.
    - **IP Hash**: Utiliza um hash do endereço IP do cliente para determinar o servidor.

Segmentação de Rede:

- **DMZ**: Zona intermediária para servidores que necessitam de acesso público, protegida por firewalls.
- **Rede Interna**: Segmento de rede para dispositivos e servidores internos.
- **Datacenter**: Segmento dedicado para servidores críticos e armazenamento de dados, com controlos rigorosos de acesso.

Políticas de Controlo de Acesso:

- **NAT/PAT**: Tradução de endereços de rede para permitir que múltiplos dispositivos utilizem um único endereço IP público.
- **Access Control Lists (ACLs)**: Regras que especificam o tráfego permitido ou bloqueado com base em critérios como endereços IP, portas e protocolos.
- **802.1X**: Protocolo de controlo de acesso à rede que fornece autenticação para dispositivos que desejam conectar-se à LAN.

Intrusion Detection and Prevention

Network Monitoring, SIEM and SOC

Regras SIEM (Security Information and Event Management)

Incorporam três tipos de regras:

- **SEM (Security Event Management)**: Sistemas que agregam e armazenam logs de eventos de segurança.
- **SIM (Security Information Management)**: Sistemas usados para identificar, coletar e analisar dados de logs de eventos.
- **SEC (Security Event Correlation)**: Sistemas que correlacionam eventos de segurança de várias fontes para identificar padrões e anomalias.

Exemplos de regras SIEM:

- Brute force detection
    - Excessive 404 errors (HTTP server Log) from a non-authenticated client (DB Log).
    - Excessive login failures (services or DB Logs) at one or multiple services.
        - From a specific IP address (or set of IP addresses).
        - From “strange” geographic regions or AS.
    - Non-matching credentials
        - From internal machines with non-matching user credentials (RADIUS/LDAP Logs).
- Impossible travel
    - Multiple logins from same user from different devices/locations.
    - Consecutive logins from same user from distant geographic regions within a small time window. VPN usage may trigger such an alarm.
- Anomalous data transference
    - Analyzing by individual source (IP or device group) and/or destination and/or by used protocol/port.
    - Excessive/Different data transference not compatible with past observations
        - Protocols and ports usage;
        - Usually firewall rules solve this!
        - Download/upload amounts, number of connections, ratio upload/download, ratio DNS/non-DNS, etc…;
        - Never contacted devices: external servers (unknown IP/ASN or country) or internal devices,;
        - Absolute time of day/week/month.
        - Relative time activity: mean or standard deviation of intervals between activity/flows/requests/etc...
    - Should be used to detect exfiltration (or propagation inside the network) and illicit C&C and data channels.
- DDoS attack
    - Excessive connection attempts from “never seen” devices/addresses/regions.
        - Ideal detection in the early phase of the attack.
    - Non-excessive attempts, but non-conformal behavior (time behavior, sequence of requests,etc...)
        - More difficult to define.
- Files/Configurations integrity fails
    - Specific device/service configuration file checksum failure, non justifiable by observed actions.
    - Generic file checksum failure, non justifiable by observed actions.