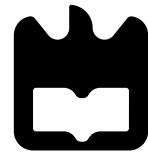


Segurança em Redes de Comunicações Apontamentos PARTE1

Universidade de Aveiro

Sebastian D. González



Segurança em Redes de Comunicações Apontamentos PARTE1

Dept. de Eletrónica, Telecomunicações e Informática
Universidade de Aveiro

sebastian.duque@ua.pt(103690)

18 de junho de 2024

Warning!!

Isto são apenas uns apontamentos realizados por uma pobre alma de MIECT, feitas a partir dos slides da disciplina e outras fontes . Por favor, não usem apenas estes apontamentos como material de estudo.

Dito isto, boa sorte a todos e ámen CT .

Agradecimentos ao Prof. Paulo Salvador salvador@ua.p e ao Prof. António Nogueira. nogueira@ua.pt por todo o material fornecido nas aulas.

Conteúdo

1	Introdução à segurança em Redes	1
1.1	Ataques disruptivos	2
1.2	Fases de Ataque	3
1.2.1	Vulnerabilidades técnicas em redes	3
1.2.2	Defesas tradicionais	4
1.2.3	Defensas “Inteligentes”	5
1.3	Security Metrics/KPI	5
2	Controlo de Acesso à Rede	6
2.1	Arquitetura AAA	6
2.2	802.1X	6
2.3	EAP	7
2.3.1	Fases do EAP	7
2.4	Protocolos AAA	8
2.4.1	TACACS+	8
2.4.2	RADIUS	8
2.4.2.1	Pacotes RADIUS	9
2.4.2.2	Vulnerabilidades do RADIUS	9
2.4.3	DIAMETER	9
2.5	802.1X - Ethernet vs. WiFi	10
2.6	Serviços IEEE 802.11	10
2.6.1	Aderir a uma BSS	11
2.6.1.1	Scanning	11
2.6.1.2	Authentication	12
2.6.1.3	Association	13
2.7	WPA e 802.11i (WPA2)	14
2.7.1	WPA	14
2.7.2	802.11i (WPA2)	15
3	Network Flow Control	16
3.1	FireWalls	16
3.1.1	Tipos de FireWalls	17
3.1.2	Stateful vs. Stateless Firewalls	18
3.1.2.1	Stateless firewalls	18

3.1.2.2	Stateful FireWall	19
3.1.3	Firewall Zones/Group	19
3.1.4	Firewall Virtual Instances	20
3.1.5	Firewall placement (with Redundancy)	20
3.1.6	Multi-Levels of Defense	21
3.1.7	Regras	21
3.1.8	Best Practices and Recommendations	22
3.1.9	High-Availability	22
3.1.9.1	Active-Backup Scenario	22
3.1.9.2	Active-Active Scenario	23
3.1.10	Load Balancing Firewall	23
3.1.10.1	Load Balancing Algorithms	24
3.1.11	Stealth Firewalls	24
3.1.12	Addressed Firewalls	25
3.1.13	Load-Balancers Instances	25
3.1.14	Redundant Load Balancers	26
3.1.15	Single Load Balancer	27
3.2	Ip Spoofing	27
3.2.1	Prevenir IP Spoofing at Layer 3	27
3.2.2	Prevenir IP Spoofing at Layer 2	28
3.3	Half-Open TCP Connection Problem	28
3.4	Firewall Performance Evaluation	28
3.5	Linux IPTables	29
3.6	Linux nftables	30
3.7	Control By Analysis of Higher Layers	30
3.8	Cisco's Access Control Lists (ACL)	30

Lista de Figuras

1.1	Ano de 2022 foi dos que registou maior número de ciberataques “de grande impacto”[1]	1
1.2	Jamming [2]	2
1.3	Attacks Phases	3
1.4	Vulnerabilidades	4
1.5	Print dos slides sobre Security Metrics/KPI	5
2.1	Implementação tradicional de um AAA	6
2.2	Enter Caption	7
2.3	Pacote RADIUS	8
2.4	RADIUS exchange involving just a username and user password:	9
2.5	Beacon Frame	11
2.6	Probe Request/Response Frames	12
2.7	Authentication Frame	13
2.8	Association Request/Response Frames	13
2.9	Data Frame	14
2.10	WPA* Key Exchange (EAP phase 2)	15
3.1	What is a FireWall [4]	16
3.2	Deploying FireWall	18
3.3	Demilitarized Zone	19
3.4	Firewall Virtual Instances	20
3.5	Enter Caption	20
3.6	Multi-Levels of Defense	21
3.7	Active-Backup Scenario	22
3.8	Active-Active Scenario	23
3.9	Load Balancer	23
3.10	Stealth Firewall	24
3.11	Addressed Firewalls	25
3.12	Load-Balancers Instances	25
3.13	Redundant Addressed Firewalls	26
3.14	Redundant Stealth Firewalls	26
3.15	Single Load Balancer	27
3.16	IP Spoofing at Layer 3	27

3.17 IP Spoofing at Layer 2	28
3.18 Linux IPTables	29

Glossário

BSS Basic Service Set.

DHCP Dynamic Host Configuration Protocol.

DMZ Demilitarized Zone.

EAP Extensible Authentication Protocol.

IEEE Institute of Electrical and Electronics Engineers.

IETF Internet Engineering Task Force.

NAC Network Access Control.

PSK Pre-Shared Key.

RADIUS Remote Authentication Dial-In User Service.

SSID Service Set Identifier.

TACACS+ Terminal Access Controller Access Control System Plus.

TKIP Temporal Key Integrity Protocol.

WNIC Wireless Network Interface Card.

WPA Wi-Fi Protected Access.

Introdução à segurança em Redes

Ciberataques são tentativas de obter acesso não autorizado a sistemas informáticos com o objetivo de roubar, modificar ou destruir dados.

Existem diversos tipos de ciberataques, com distintos objetivos:

Objetivos:

- Diversão e/ou reputação de hacking
- Propósitos políticos
- Propósitos militares
- Propósitos económicos

Objetivos técnicos:

- Disrupção de operações
- Para interceção de dados
- Ambos:
 - Disrupção para interceção!
 - Interceção para disrupção



Figura 1.1: Ano de 2022 foi dos que registou maior número de ciberataques ”de grande impacto”^[1]

1.1 Ataques disruptivos

Um ataque de negação de serviço distribuído (DDoS) é uma tentativa maliciosa de interromper o tráfego normal de um servidor, serviço ou rede sobrecarregando-o com um volume massivo de tráfego proveniente de várias fontes diferentes.

- **Soluções no alvo** geralmente envolvem a implementação de平衡adores de carga(Load-balancers) para distribuir efetivamente o tráfego recebido.
- **Para ataques TCP**, sobreviver pode envolver o reset ativo de sessões com validação de clientes legítimos, potencialmente utilizando soluções de lista branca para negociações de sessão concluídas.
- **Para ataques UDP ou DNS**, bloquear solicitações para servidores DNS de retransmissão/redirecionamento conhecidos (abordagem pode ser ineficaz contra grandes botnets ou solicitações diretas ao alvo).



Figura 1.2: Jamming [2]

O **Jamming** envolve a interrupção pura dos serviços ou a interrupção para ativar canais secundários mais facilmente comprometidos. A solução para este tipo de ataque envolve a detecção da fonte e a neutralização física da mesma.

1.2 Fases de Ataque

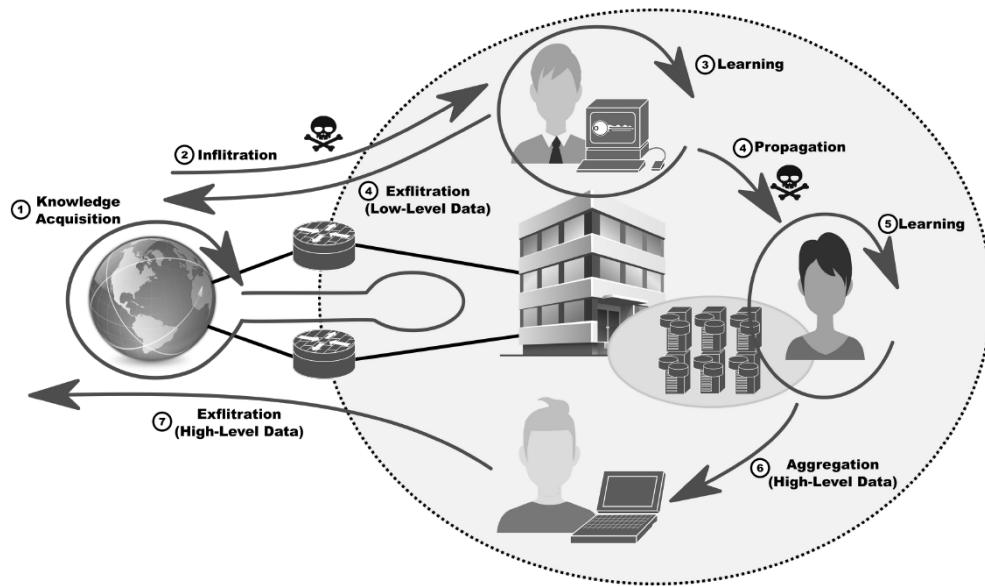


Figura 1.3: Attacks Phases

É muito importante descrever a escalada de metas e privilégios num contexto de cibersegurança. O atacante pode não obter um resultado relevante com o primeiro acesso ilícito a um domínio protegido, sendo necessário adquirir mais conhecimento [**Learning**] para acessar outras zonas/dispositivos/dados seguros com maior relevância [**Propagation**]. Em qualquer fase, o atacante pode precisar de conhecimento adicional.

Quando um resultado relevante é obtido, ele deve ser transferido para fora do domínio protegido [**Exfiltration**]. A exfiltração direta pode expor pontos relevantes dentro do domínio seguro, então o resultado relevante deve ser transferido primeiro para dentro do domínio protegido para um ponto menos importante [**Aggregation**], escolhendo um ponto que possa ser detetado e perdido sem causar danos.

1.2.1 Vulnerabilidades técnicas em redes

Technical Network Vulnerabilities Software referem-se a falhas no código ou design de tecnologia que criam potenciais pontos de comprometimento de segurança para um endpoint ou rede. Essas vulnerabilidades podem ser exploradas por invasores para executar código malicioso ou acessar a memória de dado sistema-alvo.

Software	Hardware	Known/unknown
<ul style="list-style-type: none"> Aplicações Frameworks/API Protocolos Sistemas operativos Configurações Código de baixo nível 	<ul style="list-style-type: none"> Physical tempering Physical emissions Electromagnetic emissions, sound, etc. Power instability, Electromagnetic Pulses (EMP), etc. 	<ul style="list-style-type: none"> CVE IDS/IPS and anti-virus databases



Figura 1.4: Vulnerabilidades

1.2.2 Defesas tradicionais

⇒ **Patch de Vulnerabilidades** - refere-se ao processo de desenvolver e aplicar correções ou atualizações em software, sistemas operacionais, aplicativos ou outros sistemas para corrigir falhas de segurança conhecidas, também chamadas de vulnerabilidades

⇒ **Firewalls**

- **Centralizados** - um único ponto de controlo é responsável por todas as decisões de filtragem do tráfego para toda a rede.
- **Distribuídos** - múltiplos firewalls são distribuídos pela rede, geralmente próximos aos pontos de entrada e saída de tráfego.

⇒ **Antivírus**

⇒ **Intrusion Prevention and Detection Systems (IDS/IPS)**

1.2.3 Defensas “Inteligentes”

- ⇒ Deteção de ameaças desconhecidas e/ou problemas para poder implementar as devidas contra medidas a tempo.
- ⇒ A aplicação de técnicas de Big Data e Data Science para monitorizar as redes e os sistemas.
- ⇒ Algumas soluções tradicionais já começam a incorporar inteligência artificial nos seus equipamentos.
 - Por exemplo, Firewalls da Palo Alto Networks, Cisco Appliances, ...
 - Ainda está limitado a **manufacturer based solutions**, dados localizados.
 - Limitadas em Scope
 - * Ameaças óbvias vs. Ameaças furtivas.
 - Implantação ideal requer conhecimento geral de rede e sistemas
 - * Consciência Situacional de Rede e Sistemas (Cibernética).

1.3 Security Metrics/KPI

- | | |
|---|--|
| <ul style="list-style-type: none">● Access management<ul style="list-style-type: none">◆ How many users have administrative access, and how often is used.◆ Shared passwords between staff.● Preparedness<ul style="list-style-type: none">◆ Percentage of devices fully patched and up to date.● Days to patch<ul style="list-style-type: none">◆ Average time between patch availability and deployment.● Unidentified devices<ul style="list-style-type: none">◆ Illicitly deployed devices.◆ BYoD policy, legacy devices, unlisted devices, IoT devices, etc...● Security devices average/maximum load per time period.● Intrusion attempts<ul style="list-style-type: none">◆ Amount of detected and undetected attempts (in real time or after off-line auditing).● Cost per incident<ul style="list-style-type: none">◆ Includes staff overtime, external support, investigation costs, employee productivity loss, loss of communication, service failure, etc... | <ul style="list-style-type: none">● Mean Time Between Failures (MTBF)<ul style="list-style-type: none">◆ Average time between failures (hardware and/or software).◆ General or per device/service.● Mean Time to Recovery (MTTR)<ul style="list-style-type: none">◆ Average time between failure and recovery (hardware and/or software).● Mean Time to Detect (MTTD)<ul style="list-style-type: none">◆ Average time between intrusion and detection.● Mean Time to Acknowledge (MTTA)<ul style="list-style-type: none">◆ Average time between detection and start of countermeasures deployment.● Mean Time to Contain (MTTC)<ul style="list-style-type: none">◆ Average time between start of countermeasures deployment and complete mitigation.● Mean Time to Resolve (MTTR)<ul style="list-style-type: none">◆ MTTA+MTTR |
|---|--|

Figura 1.5: Print dos slides sobre Security Metrics/KPI

Controlo de Acesso à Rede

2.1 Arquitetura AAA

A ideia é que a própria infraestrutura não permita qualquer pessoa ligar-se à rede (acesso não autorizado). É o primeiro passo do acesso a uma rede.

- **Authentication** - identifica o utilizador.
- **Authorization** - determina o que o utilizador pode fazer
- **Accounting** - monitoriza o tempo de utilização da rede para efeitos de faturação.

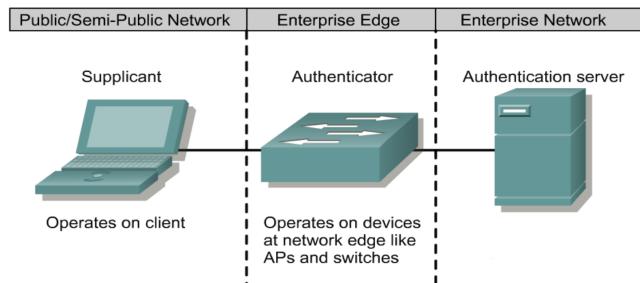


Figura 2.1: Implementação tradicional de um AAA

A implementação envolve, tipicamente, a utilização de um servidor de autenticação remoto (banco de dados externo) para facilitar a administração centralizada e a escalabilidade do sistema.

2.2 802.1X

IEEE 802.1X é um padrão para Controlo de Acesso à Rede [Network Access Control \(NAC\)](#). Este fornece um mecanismo de autenticação para dispositivos que desejam conectar-se a uma LAN, baseada no [Extensible Authentication Protocol \(EAP\)](#) 2.3.

2.3 EAP

O Protocolo de Autenticação Extensível **EAP**, definido no RFC 3748, foi projetado para possibilitar autenticação extensível para acesso à rede em situações em que o protocolo de Internet (IP) não está disponível. O EAP é um protocolo de duas partes falado entre um peer EAP e um servidor EAP.

- ⇒ No contexto do EAP, o material de chave é gerado por algoritmos de autenticação EAP, conhecidos como "métodos"
- ⇒ Parte desse material de chave pode ser usada pelos próprios métodos EAP, enquanto outra parte pode ser exportada.
- ⇒ O EAP é encapsulado em pacotes AAA falados entre o autenticador e o servidor de autenticação de back-end, com suporte para métodos como RADIUS e Diameter

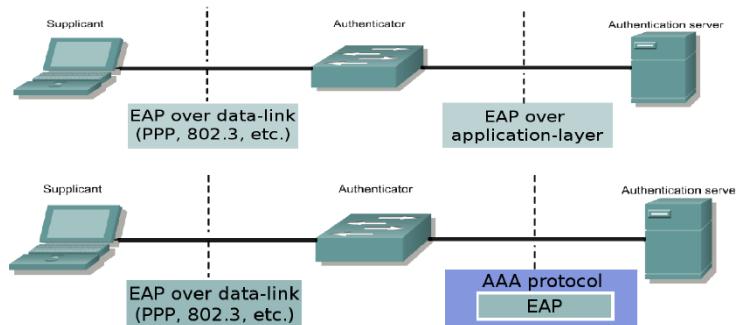


Figura 2.2: Enter Caption

2.3.1 Fases do EAP

1. **Discovery**
2. **Autentication**
 - 1a. Autenticação EAP.
 - 1b. Transporte de Chave AAA (opcional).
3. **Secure Association Protocol**
 - 2a. Associação Segura Unicast.
 - 2b. Associação Segura Multicast (opcional).

2.4 Protocolos AAA

2.4.1 TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) envolve o encaminhamento das informações de nome de utilizador e palavra-passe para um servidor de segurança centralizado. O servidor centralizado pode ser uma base de dados TACACS ou uma base de dados como o ficheiro de palavras-passe UNIX com suporte TACACS. Esta abordagem permite a gestão centralizada e segura das credenciais de acesso, garantindo um nível mais elevado de segurança e controlo sobre as informações mais sensíveis dos utilizadores.

Principais features:

- Separa todas as funcionalidades AAA
- Utiliza TCP
- Autenticação bidirecional
- Todos os pacotes são encriptados
- Personalização limitada da contabilização

2.4.2 RADIUS

O Remote Authentication Dial-In User Service (RADIUS) é um protocolo cujas funções incluem receber pedidos de ligação de utilizadores, autenticar os utilizadores e fornecer todas as informações de configuração necessárias para o cliente fornecer serviço ao utilizador. A autenticação e as transações entre o cliente e o servidor RADIUS são feitas usando um segredo partilhado, com suporte a vários métodos de autenticação como PAP, CHAP, MS-CHAP, login UNIX entre outros mecanismos.

O RADIUS combina Autenticação e Autorização, separando a Contabilidade (menos flexível que o TACACS+) e utiliza UDP para comunicação, sendo este menos robusto. Além disso, o RADIUS oferece autenticação unidirecional e criptografia apenas a senha, o que é menos seguro em comparação com outros métodos. A contabilidade do RADIUS pode armazenar mais informações sobre as sessões dos utilizadores.

Code (1 byte)	Identifier (1 byte)	Length (2 bytes)
Authenticator (16 bytes)		
Attributes		

Figura 2.3: Pacote RADIUS

2.4.2.1 Pacotes RADIUS

Existem 6 tipos de pacotes RADIUS:

- | | |
|--------------------|-------------------------|
| (1) Access-Request | (4) Accounting-Request |
| (2) Access-Accept | (5) Accounting-Response |
| (3) Access-Reject | (11) Access-Challenge |

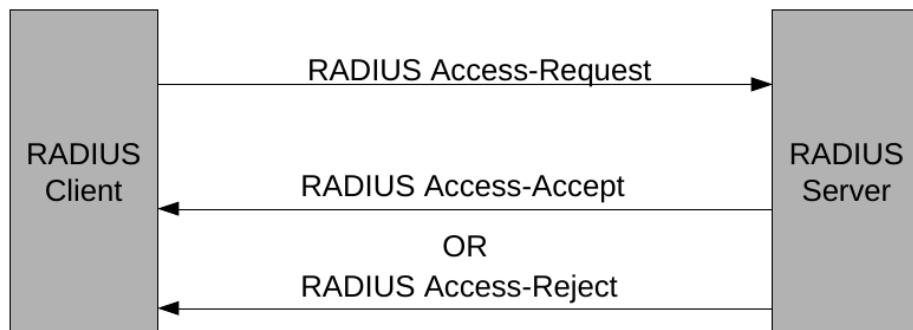


Figura 2.4: RADIUS exchange involving just a username and user password:

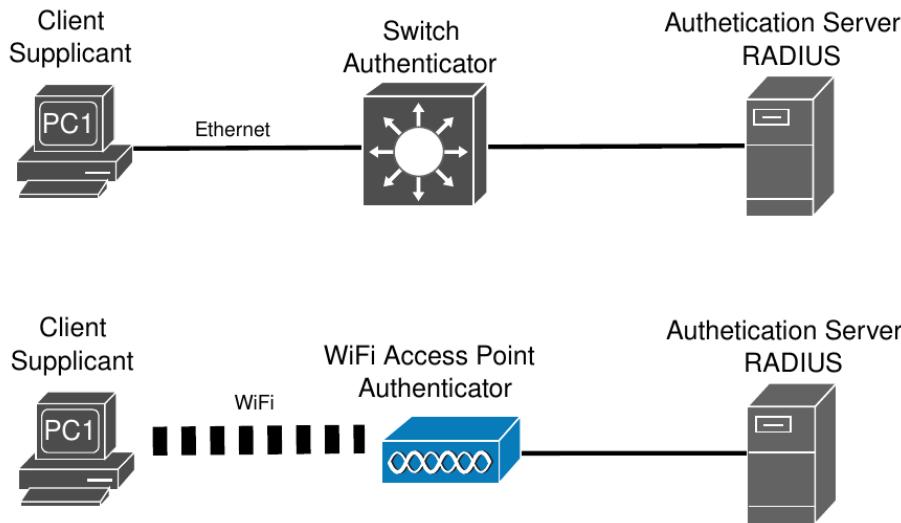
2.4.2.2 Vulnerabilidades do RADIUS

- ⇒ O pacote Access-Request não é autenticado de forma alguma.
- ⇒ Muitas implementações de clientes não criam Request Authenticators que sejam suficientemente aleatórios.
- ⇒ Muitos administradores escolhem segredos partilhados RADIUS com entropia de informação insuficiente e muitas implementações limitam o espaço da secret key partilhada.

2.4.3 DIAMETER

O DIAMETER é a mais recente framework no [IETF](#) para servidores AAA de próxima geração que fornece um framework AAA para Mobile-IP. Ele não utiliza a mesma unidade de dados do protocolo RADIUS [2.4.2](#), mas é compatível com o RADIUS para facilitar a migração. Oferece autenticação bidirecional, utiliza UDP, mas possui um esquema que regula o fluxo de pacotes e permite a segurança de atributos de desafio/resposta através de criptografia e autenticação ponta a ponta.

2.5 802.1X - Ethernet vs. WiFi



2.6 Serviços IEEE 802.11

- **Station services** (semelhante à rede com fios)
 - Autenticação (login)
 - Desautenticação (logout)
 - Privacidade
 - Entrega de dados
- **Distribution services**
 - **Associação**
 - * Estabelecer conexão lógica entre o AP e a estação - o AP não receberá dados de uma estação antes da associação
 - **Reassociação** (semelhante à associação)
 - * Enviado repetidamente para o AP.
 - * Auxiliar o AP a saber se a estação se moveu de/para outro **BSS**.
 - * **Após Economia de Energia**
 - **Desassociação**
 - * Desconexão manual (o PC é desligado ou o adaptador é ejetado manualmente)

2.6.1 Aderir a uma BSS

Quando uma estação deseja se juntar a um Basic Service Set (BSS) ou AP em uma rede sem fio, ela realiza essa conexão através de **Scanning** 2.6.1.1 para encontrar o BSS/AP disponível. No contexto de um BSS com um AP, tanto a **Authentication** 2.6.1.2 quanto **Association** 2.6.1.3 são necessárias para ingressar no BSS.

A estação envia uma solicitação de associação ao AP, que verifica se o cliente atende aos critérios necessários, como taxa de dados sem fio compatível e credenciais de autenticação. Após a associação bem-sucedida, todas as comunicações da estação passam pelo AP, que atua como intermediário encaminhando os quadros de dados para as estações de destino. Esse processo é essencial para estabelecer a conexão e permitir a comunicação eficaz em uma rede sem fio [3].

2.6.1.1 Scanning

1. **Passive scanning** - A estação procura nos canais por uma **Beacon frame** 2.5 que é enviada periodicamente por uma AP para anunciar sua presença e fornecer o **SSID** e outros parâmetros para as estações dentro do alcance
-> REDES PÚBLICAS

2. Active scanning

- I. A estação envia um **Probe Request frame** 2.6 para encontrar um AP.
- II. Todos os APs dentro do alcance respondem com um **Probe Response frame** 2.6, contendo informações de capacidade, taxas de dados suportadas, entre outros detalhes.

```
- IEEE 802.11 Beacon frame, Flags: .....
  Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ffff:ffff:ffff)
  Destination address: Broadcast (ffff:ffff:ffff:ff)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  ... 0000 0000 = Fragment number: 0
  1001 1000 1010 = Sequence number: 2442
  Frame check sequence: 0x6f0bb825c [unverified]
  [FCS Status: Unverified]

- IEEE 802.11 wireless LAN
  - Fixed parameters (12 bytes)
    Timestamp: 660070796
    Beacon Interval: 0.102400 [Seconds]
    Capabilities Information: 0x0421
  - Tagged parameters (123 bytes)
    - Tag: SSID parameter set: LABCOM
    - Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    - Tag: DS Parameter set: Current Channel: 13
    - Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    - Tag: ERP Information
    - Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    - Tag: Cisco CCX1 CKIP + Device Name
    - Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    - Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
    - Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
    - Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
    - Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
```

Figura 2.5: Beacon Frame

```

· IEEE 802.11 Probe Request, Flags: .......c
Type/Subtype: Probe Request (0x0004)
· Frame Control Field: 0x4000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Microsoft 0a:43:e3 (c0:33:5e:0a:43:e3)
Source address: Microsoft 0a:43:e3 (c0:33:5e:0a:43:e3)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
.... .... .... 0000 = Fragment number: 0
1100 1011 0001 .... = Sequence number: 3249
Frame check sequence: 0xc7056d0a [unverified]
[FCS Status: Unverified]

· IEEE 802.11 wireless LAN
· Tagged parameters (62 bytes)
· Tag: SSID parameter set: TD_WIFI_GUEST
· Tag: Supported Rates 1, 2, 5.5, 6, 9, 11, 12, 18, [Mbit/sec]
· Tag: DS Parameter set: Current Channel: 13
· Tag: HT Capabilities (802.11n D1.10)
· Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]

· IEEE 802.11 Probe Response, Flags: .......c
Type/Subtype: Probe Response (0x0005)
· Frame Control Field: 0x5000
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
Destination address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
.... .... .... 0000 = Fragment number: 0
1100 0010 1001 .... = Sequence number: 2601
Frame check sequence: 0x80831320 [unverified]
[FCS Status: Unverified]

· IEEE 802.11 wireless LAN
· Fixed parameters (12 bytes)
· Timestamp: 664064263
· Beacon Interval: 0.102400 [Seconds]
· Capabilities Information: 0x0421
· Tagged parameters (117 bytes)
· Tag: SSID parameter set: LABCOM
· Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
· Tag: DS Parameter set: Current Channel: 13
· Tag: HT Capabilities
· Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
· Tag: Cisco CCX1 CKIP + Device Name
· Tag: Vendor Specific: Microsoft Corp.: MMW/MME: Parameter Element
· Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
· Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
· Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
· Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled

```

Figura 2.6: Probe Request/Response Frames

2.6.1.2 Authentication

- Open system authentication

1. A estação envia um **Authentication Frame 2.7** com sua identidade para o AP.
2. O AP responde com um quadro de Ack / NACK.

- Shared Key Authentication

1. As estações recebem uma chave secreta compartilhada por meio de um canal seguro independente do padrão 802.11.
2. Após a **WNIC** enviar sua solicitação inicial de autenticação, ela recebe do AP um quadro de autenticação contendo um texto de desafio.
3. A **WNIC** envia de volta ao AP um **Authentication Frame 2.7** contendo a versão criptografada do texto de desafio.
4. O AP verifica se o texto foi criptografado corretamente com a chave correta, descriptografando-o com sua própria chave.
5. O resultado desse processo determina o status de autenticação da **WNIC**.

```

- IEEE 802.11 Authentication, Flags: .....
  Type/Subtype: Authentication (0x000b)
  Frame Control Field: 0xb000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... 0000 = Fragment number: 0
  0001 0100 1011 .... = Sequence number: 331
- IEEE 802.11 wireless LAN
- Fixed parameters (6 bytes)
  Authentication Algorithm: Open System (0)
  Authentication SEQ: 0x0001
  Status code: Successful (0x0000)

- IEEE 802.11 Authentication, Flags: .....
  Type/Subtype: Authentication (0x000b)
  Frame Control Field: 0xb000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... 0000 = Fragment number: 0
  1010 1001 0000 .... = Sequence number: 2704
  Frame check sequence: 0x9fb8350e1 [unverified]
  [FCS Status: Unverified]
- IEEE 802.11 wireless LAN
- Fixed parameters (6 bytes)
  Authentication Algorithm: Open System (0)
  Authentication SEQ: 0x0002
  Status code: Successful (0x0000)

From AP →

```

Figura 2.7: Authentication Frame

2.6.1.3 Association

1. A estação envia um **Associate Request frame** 2.6.1.3 contendo informações sobre o **WNIC**, como taxas de dados suportadas e o SSID da rede à qual deseja se associar.
2. O AP responde com **Association Response frame** 2.6.1.3, aceitando ou rejeitando a solicitação.

```

- IEEE 802.11 Association Request, Flags: .....
  Type/Subtype: Association Request (0x0000)
  Frame Control Field: 0x0000
  .000 0001 0011 1020 Duration: 314 microseconds
  Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... 0000 = Fragment number: 0
  0001 0100 1100 .... = Sequence number: 332
- IEEE 802.11 wireless LAN
- Fixed parameters (4 bytes)
  · Capability Information: 0x0421
  · Listen Interval: 0x0008
  - Tagged parameters (43 bytes)
    · Tag: SSID parameter set: LABCOM
    · Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    · Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    · Tag: Extended Capabilities (8 octets)
    · Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information E
- IEEE 802.11 Association Response, Flags: .....
  Type/Subtype: Association Response (0x0001)
  Frame Control Field: 0x0000
  .000 0001 0011 1010 Duration: 314 microseconds
  Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... 0000 = Sequence number: 2705
  1010 1001 0000 .... = Sequence number: 2705
  Frame check sequence: 0x7f103b15 [unverified]
  [FCS Status: Unverified]
- IEEE 802.11 wireless LAN
- Fixed parameters (6 bytes)
  · Capability Information: 0x0421
  · Status code: Success (0x0000)
  ..00 0000 0000 0001 = Association ID: 0x0001
  - Tagged parameters (42 bytes)
    · Tag: Supported Rates 1(8), 2(8), 5.5(8), 6, 9, 11(8), 12, 18, [Mbit/sec]
    · Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    · Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

From AP →

```

Figura 2.8: Association Request/Response Frames

Somente após a conclusão da associação, a estação pode transmitir e receber Data Frames [2.9](#).

```
- IEEE 802.11 QoS Data, Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8841
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)      ← Node that will receive frame (AP)
    Transmitter address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53) ← Node that send frame
    Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e) ← Station to receive data
    Source address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)      ← Station who sent data
    BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0011 .... = Sequence number: 3
    Frame check sequence: 0xc72771e8 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
  > CCMP parameters
- Data (1244 bytes)
  Data: f8002648417037bc923106ead1717d4821fde0989beb08b1...
  [Length: 1244]
```

Figura 2.9: Data Frame

2.7 WPA e 802.11i (WPA2)

2.7.1 WPA

[Wi-Fi Protected Access \(WPA\)](#) é um protocolo de segurança para redes sem fio que oferece autenticação e criptografia. Ele utiliza o 802.1X e o EAP (Extensible Authentication Protocol) como protocolos de transporte para sessões com e sem fio.

⇒ O EAP atua como um invólucro para o tráfego de autenticação específico, permitindo diferentes métodos de autenticação sem alterar os APs.

O WPA também define uma [Pre-Shared Key \(PSK\)](#) para redes locais e o [Temporal Key Integrity Protocol \(TKIP\)](#) para melhor proteção, garantindo maior privacidade e integridade dos dados. Após a associação bem-sucedida, uma estação pode transmitir e receber quadros de dados

2.7.2 802.11i (WPA2)

- Melhor que WPA

- Inclui também **TKIP**
- Autenticação IBSS (modo ad-hoc)?
- Protocolo RSN (Rede de Segurança Robusta)
 - * Autenticação e criptografia entre APs e estações
 - * Superta novos protocolos de cifra, recorrendo a 802.1x e EAP
 - * Suporta cifra AES

- Problemas

- Não cifra frames de controlo e gestão (Desassociar, potência de saída, etc).
- Requer hardware novo

```

208 595.669400767 IntelCor e8:14:53 Cisco 61:ee:d1          802.11 110 Association Request, SN=38, FN=0, Flags=....., SSID=LABCOM_SEC
208 595.671214291 Cisco 61:ee:d1 IntelCor e8:14:53          802.11 128 Association Response, SN=14, FN=0, Flags=.....
207 595.673042781 Cisco 61:ee:d1 IntelCor e8:14:53          EAPOL 211 Key (Message 1 of 4)
208 595.678333124 Cisco 61:ee:d1 IntelCor e8:14:53          EAPOL 168 Key (Message 2 of 4)
209 595.681795313 Cisco 61:ee:d1 IntelCor e8:14:53          EAPOL 269 Key (Message 3 of 4)
210 595.683690439 Cisco 61:ee:d1 IntelCor e8:14:53          EAPOL 146 Key (Message 4 of 4)

Frame 207: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface 0
Radio Tap Header: V0, Length 56
IEEE 802.11 wireless frame
Type/Subtype: QoS Data, Flags: .....F.
Type/Subtype: QoS Data (0x9028)
Frame Control Field: 0x8802
    0000 0001 0000 1000 = Duration: 314 microseconds
Recipient address: IntelCor e8:14:53 (08:0a:60:e8:14:53)
Transmitter address: Cisco 61:ee:d1 (00:1c:f6:61:ee:d1)
Destination address: IntelCor e8:14:53 (b8:0a:60:e8:14:53)
Source address: Cisco 61:ee:d1 (00:1c:f6:61:ee:d1)
BSS Id: Cisco 61:ee:d1 (00:1c:f6:61:ee:d1)
STA address: IntelCor e8:14:53 (b8:0a:60:e8:14:53)
    0000 0001 1100 ... = Fragment number: 9
    0000 0001 1100 ... = Sequence number: 28
QoS Control: 0x0007
Logical-Link Control
    802.11 Authentication
        Version: IEEE 802.1X-2004 (2)
        Type: Key (3)
        Length: 117
        Key Descriptor Type: EAPOL RSN Key (2)
        [Message number: 1]
        Key Identifier: 0x000a
        Key Length: 16
        Replay Counter: 1
WPA Key Nonce: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
Key IV: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
WPA MIC: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
WPA Key ID: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
WPA Key MIC: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
WPA Key Data Length: 22
WPA Key Data: dd14000fac046616ebb59b83e8cc1816ced0e542a935

```

Figura 2.10: WPA* Key Exchange (EAP phase 2)

Network Flow Control

3.1 FireWalls

Uma firewall fornece um único ponto de defesa entre as redes e protege uma rede das outras.

- É um sistema ou grupo de sistemas que aplica uma política de controlo sobre duas ou mais redes (controlo de acesso, controlo de fluxo e controlo de conteúdo)
- É uma gateway de rede que faz cumprir as regras de segurança da rede e minimiza vulnerabilidades locais.
- Avalia cada pacote de rede em relação às políticas de segurança da rede.
- Pode monitorizar todo o tráfego de rede e alertar sobre tentativas de contornar a segurança ou sobre padrões de uso inadequado.
- Pode ser baseado em hardware ou software.

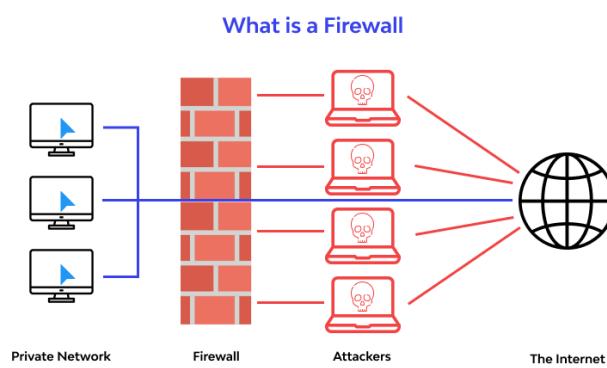


Figura 3.1: What is a FireWall [4]

3.1.1 Tipos de FireWalls

Firewalls de Rede (L2/L3)

- Filtragem de Pacotes
- Analisa headers de pacotes e filtra tráfego com base em endereços IP e MAC

Firewalls de Nível de Circuito (L4)

- Monitoriza a conexão TCP entre pacotes para garantir que uma sessão seja legítima
- O tráfego é filtrado com base em regras de sessão especificadas

Firewalls de Nível de Aplicação (L4+)

- Os firewalls de nível de aplicação são por vezes chamados de **Proxies**
- Análise mais aprofundada dos dados da aplicação
- Consideração do contexto das solicitações do cliente e das respostas da aplicação
- Tentativa de impor um comportamento correto da aplicação e bloquear atividades maliciosas

Firewalls Multinível Estatais (L*)

- Filtram pacotes ao nível da rede e reconhecem e processam dados ao nível da aplicação
- Como não empregam proxies mas têm um desempenho razoavelmente bom mesmo ao realizar análise profunda de pacotes

Firewalls de Nível de Host / Pessoais

- Atuam apenas dentro de um host específico
- Filtram todas as camadas de comunicação
- Controlam processos/aplicações do sistema operacional

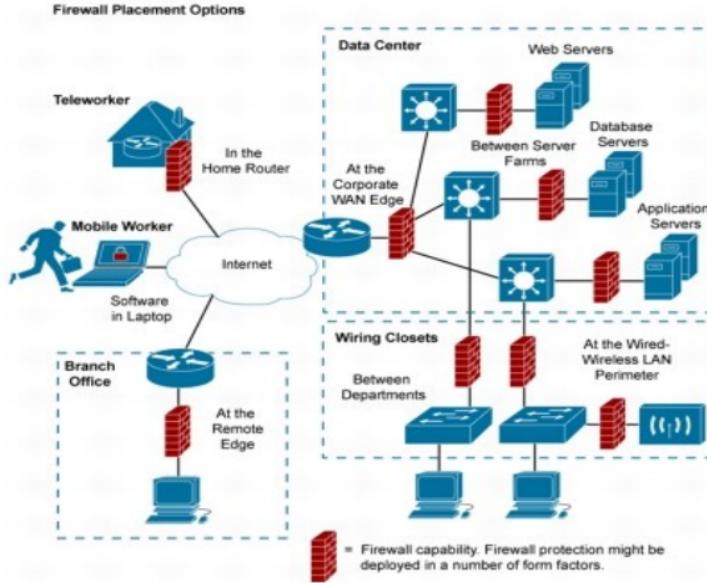


Figura 3.2: Deploying FireWall

3.1.2 Stateful vs. Stateless Firewalls

3.1.2.1 Stateless firewalls

Utilizam a origem, destino e outros parâmetros de um pacote de dados para determinar se os dados representam uma ameaça. Estas regras têm de ser introduzidos quer por um administrador quer pelo fabricante através de regras previamente definidas.

- Não precisa acompanhar fluxos/sessões de tráfego.
- As regras são baseadas em valores específicos nos cabeçalhos dos frames/pacotes disponíveis.
- Conjunto de ações básicas de permitir/negar para entrada e saída com base em endereços IP, portas UDP/TCP, etc.
- Geralmente chamado de ACL (Lista de Acesso).
- São rápidas e consomem baixos recursos computacionais.
- Apresentam bom desempenho sob carga de tráfego pesada.
- Ideais para defesa contra ataques DDoS na primeira linha de defesa da rede.

3.1.2.2 Stateful Firewall

Inspecionam tudo dentro dos pacotes de dados, as características dos dados e seus canais de comunicação. Eles examinam o comportamento dos pacotes de dados e, se algo parecer suspeito, podem filtrar os dados suspeitos. Além disso, um firewall stateful pode rastrear como os dados se comportam, catalogando padrões de comportamento e para isso utiliza uma memória.

	Stateless	Statefull
Rule-based Forward/Discard	Yes	No
Connection-based Forward/Discard	No	Yes
Robustness Against Spoofing Attacks	Low	High
Processing Performance	Typically outperforms stateful firewalls in heavy traffic scenarios	Can become a bottleneck faster than a stateless firewall in heavy traffic scenarios
Purchase Price	Typically cheaper than stateful firewalls	Typically more expensive than stateless firewalls

Tabela 3.1: Firewalls: Stateless vs. Stateful[5]

3.1.3 Firewall Zones/Group

As redes podem ser divididas em zonas ou grupos com diferentes níveis de segurança. Estes grupos consistem em coleções de endereços IP, redes ou portas que podem ser referenciados por regras de firewall como origem ou destino.

Existe um exemplo específico de uma **Demilitarized Zone (DMZ)** que é uma rede periférica usada para servidores/serviços públicos. A **DMZ** é considerada "semi-protegida" e qualquer máquina nela está em risco.

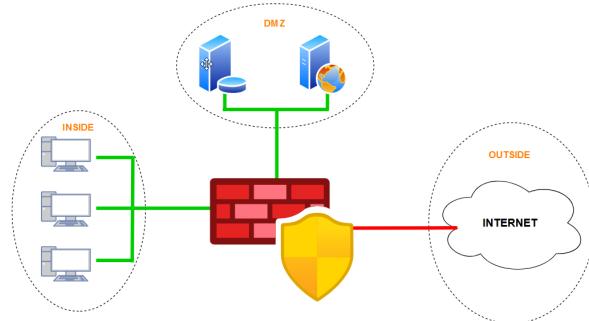


Figura 3.3: Demilitarized Zone

3.1.4 Firewall Virtual Instances

- Os firewalls podem ter instâncias (teoricamente) isoladas para lidar com diferentes zonas/grupos.
- Cada instância é um dispositivo virtual que pode realizar controle de fluxo, comutação e/ou roteamento.

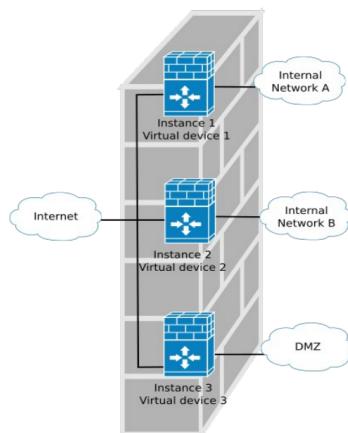


Figura 3.4: Firewall Virtual Instances

3.1.5 Firewall placement (with Redundancy)

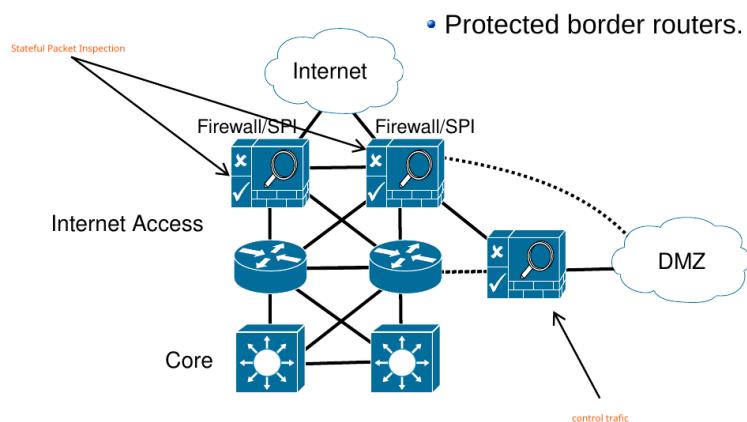


Figura 3.5: Enter Caption

3.1.6 Multi-Levels of Defense

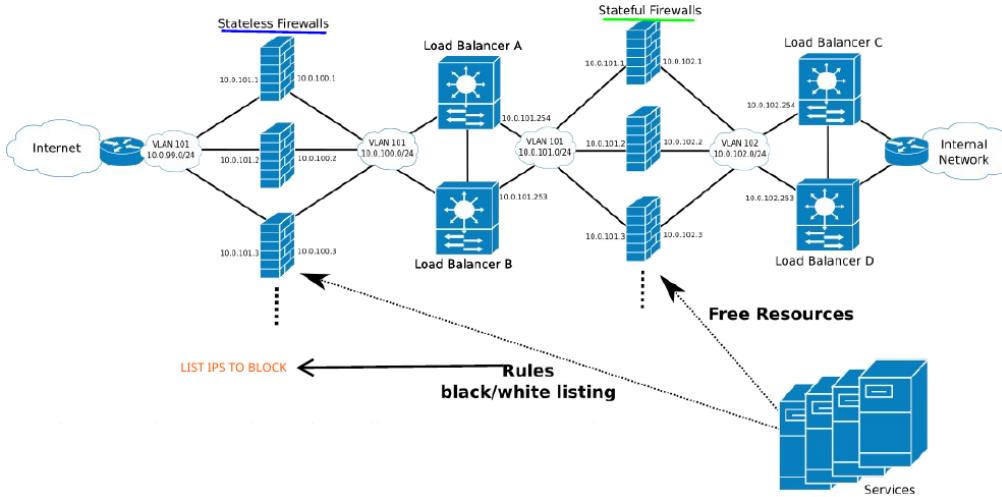


Figura 3.6: Multi-Levels of Defense

- **Primeiro nível** de Stateless firewalls para proteção contra DDoS.
- **Segundo(s) nível(is)** de Stateful firewalls para proteção geral.

3.1.7 Regras

- As regras do firewall devem ser especificadas com base na origem, destino e tipo de tráfego(portas, zonas, etc...).
- O tipo pode ser definido em termos de protocolo ou especificações de protocolo.
- As regras podem ser especificadas com base no estado de uma ligação (requer um firewall com estado) mediante a observação de um pacote:
 - **NOVA:** Para pacotes que iniciam uma nova comunicação ou estão ligados a uma comunicação onde ainda não houve troca de dados em ambas as direções
 - **ESTABELECIDA:** Para pacotes relacionados a comunicações que já foram estabelecidas, ou seja, onde houve troca de dados em ambas as direções. É necessário configurar regras específicas para permitir o retorno de tráfego em comunicações já estabelecidas.
 - **RELACIONADA:** Para casos especiais onde um pacote inicia uma nova comunicação, mas está de alguma forma vinculado a uma comunicação anterior, como erros ICMP relacionados a comunicações anteriores.

3.1.8 Best Practices and Recommendations

- Padronizar as políticas de segurança.
- Bloquear todo o tráfego por padrão.
 - Remover todas as regras de "Aceitar Tudo".
- Adicione exceções de "Accept".
- Documentar as regras do firewall.
- Manutenção e monitorização das regras.
- Verifique periodicamente a validade das regras.
- Integrar o controlo de fluxo com políticas existentes.

3.1.9 High-Availability

3.1.9.1 Active-Backup Scenario

É quando existem dois firewalls configurados num par redundante, com um firewall designado como a unidade ativa e o outro como a unidade de backup. Os firewalls ativo e de backup partilham uma conexão dedicada para sincronizar continuamente seu estado e configuração e também partilham um endereço IP virtual comum na interface LAN(Shared Virtual IP).

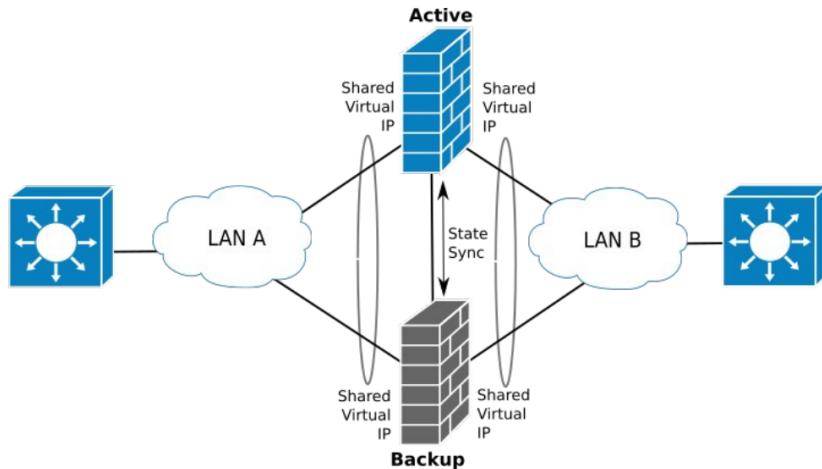


Figura 3.7: Active-Backup Scenario

Apenas uma firewall está a processar ativamente o tráfego por vez - a unidade ativa. O firewall de backup permanece em estado de espera, pronto para assumir em caso de falha da unidade ativa.

3.1.9.2 Active-Active Scenario

Possuem a capacidade de partilhar o estado através de uma ligação dedicada. Esta partilha de estado permite que os firewalls coordenem as suas ações e mantenham uma visão consistente do tráfego que passa pela rede. Além disso, cada firewall possui o seu próprio endereço IP, o que lhes permite operar de forma independente, mesmo quando trabalham em conjunto. Esta abordagem simultânea não só permite uma distribuição equitativa da carga de trabalho entre os firewalls, mas também resolve problemas de routing assimétrico, garantindo que o tráfego de entrada e saída siga caminhos consistentes.

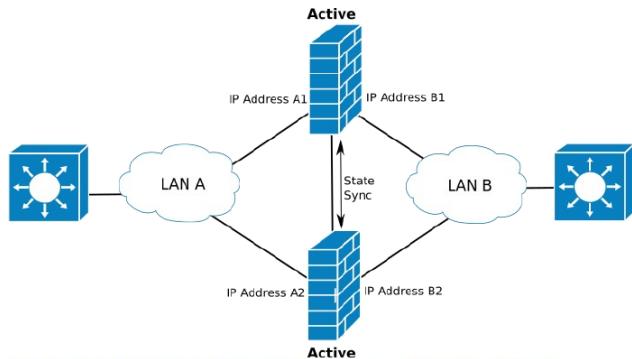


Figura 3.8: Active-Active Scenario

Os firewalls podem trabalhar em conjunto com平衡adores de carga para otimizar o desempenho da rede e garantir uma proteção eficaz contra ameaças

3.1.10 Load Balancing Firewall

O equipamento Load Balancer pode distribuir o tráfego por vários firewalls. O Load Balancer de carga roteia o tráfego do mesmo fluxo SEMPRE para o mesmo firewall (dependendo do algoritmo do balanceador de carga):

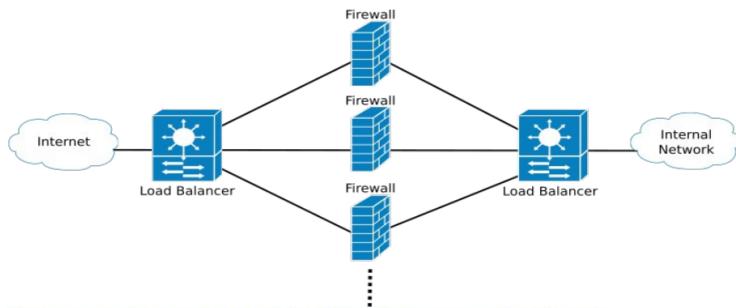


Figura 3.9: Load Balancer

3.1.10.1 Load Balancing Algorithms

- **IP Hash** - O endereço IP (ou um conjunto de identificadores de fluxo) do cliente é usado para determinar qual servidor/firewall recebe o fluxo ou pedido. Não requer sincronização de estado (FW ou LB). A saída da função hash determina o destino.
- **Round Robin** - Os pedidos são distribuídos sequencialmente pelo grupo de dispositivos. Se os firewalls não partilham estado, os平衡adores de carga devem "memorizar" a interface pela qual receberam o tráfego dos firewalls e usar a mesma interface para encaminhar o tráfego de resposta.
- **Least Connections** - Como o próprio nome diz um novo pedido é enviado para o servidor/firewall com menos conexões atuais. A capacidade computacional relativa de cada servidor/firewall é considerada para determinar qual tem menos conexões.
- **"Smart"** - Baseada numa fonte externa de informação.

3.1.11 Stealth Firewalls

- Firewalls stealth são conhecidos por serem "invisíveis" na rede, pois não possuem endereços IP nas interfaces em que operam. Isso os torna difíceis de serem detectados por atacantes.
- Esses firewalls podem ter várias regras de camada e são capazes de rotear o tráfego com base em interfaces ou VLANs específicas.
- Eles não oferecem serviços de roteamento ou NAT/PAT e não podem substituir routers.
- Os firewalls stealth atuam como pontes ou switches, conectando segmentos de rede e aplicando mecanismos de controle de acesso nesse ponto.

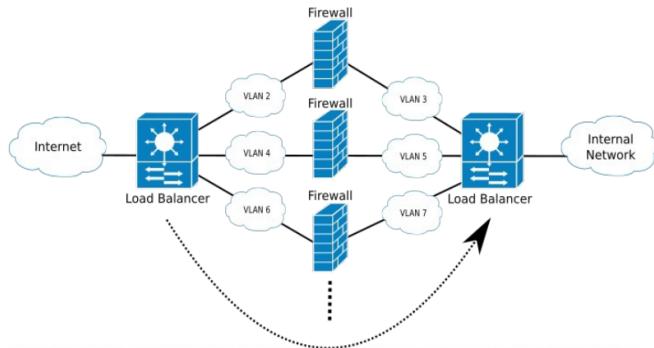


Figura 3.10: Stealth Firewall

3.1.12 Addressed Firewalls

- **Firewalls com Endereços IP**

- As interfaces nesses firewalls têm endereços IP atribuídos.
- Balanceadores de carga ou routers encaminham o tráfego para esses firewalls como o Next-Hop IP.
- Estes firewalls podem fornecer serviços de routing e potencialmente substituir routers tradicionais numa rede.
- Eles não são ”invisíveis” na rede como os **Stealth Firewalls 3.1.11**, uma vez que os seus endereços IP estão expostos.

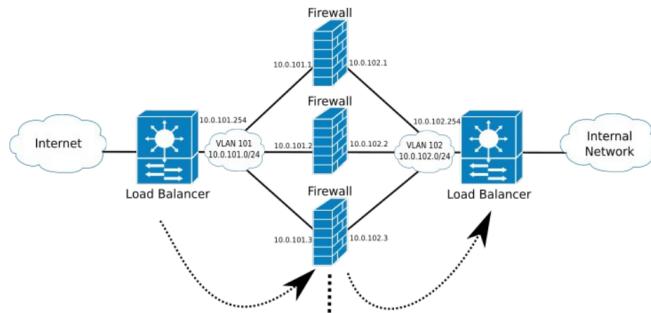


Figura 3.11: Addressed Firewalls

3.1.13 Load-Balancers Instances

Os LB podem ter instâncias isoladas (teoricamente) para lidar com diferentes zonas ou grupos.

⇒ Cada instância isolada pode ser designada para lidar com um conjunto específico de firewalls em uma determinada zona ou grupo

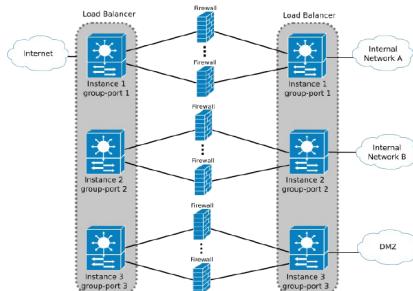


Figura 3.12: Load-Balancers Instances

Essas instâncias isoladas podem ser implementadas em partições físicas ou virtuais, permitindo uma separação clara e eficiente do tráfego e das tarefas de平衡amento de carga. Alguns fornecedores podem se referir a essas instâncias isoladas como "group-ports".

3.1.14 Redundant Load Balancers

- **Evitar a Sincronização de Estado dos Firewalls**

- Para evitar a necessidade de sincronização de estado dos firewalls, os balanceadores de carga devem garantir que os pacotes do mesmo fluxo sejam sempre enviados para o mesmo firewall.
- Isso ajuda a reduzir o risco de sobrecarga de memória nos firewalls, pois o firewall só precisa manter o estado para as conexões que está processando ativamente.

- **Balanceamento de Carga com Hash de IP**

- Os balanceadores de carga que utilizam algoritmos de IP Hash não requerem a sincronização do histórico de routing pois realizam um cálculo matemático no endereço IP do cliente para determinar qual servidor/firewall deve receber o tráfego, eliminando a necessidade de partilhar informações de roteamento.

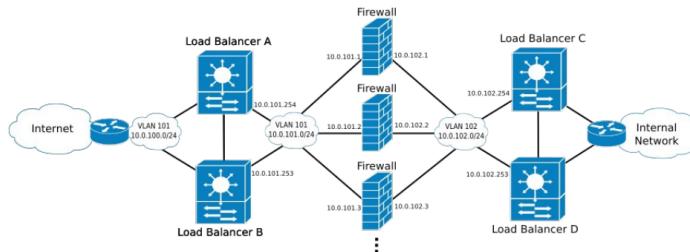


Figura 3.13: Redundant Addressed Firewalls

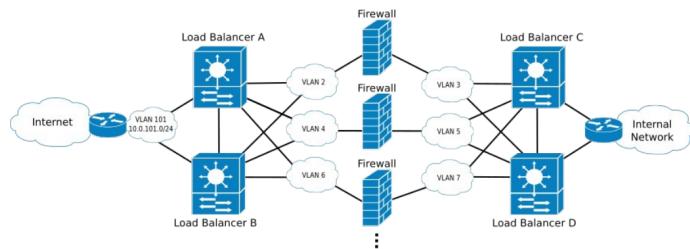


Figura 3.14: Redundant Stealth Firewalls

3.1.15 Single Load Balancer

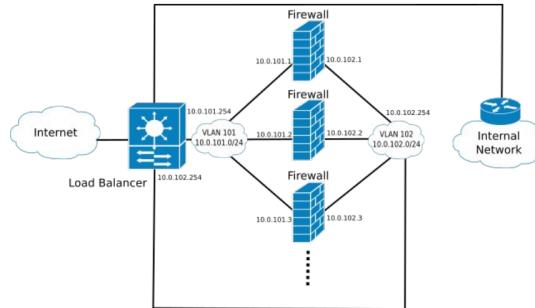


Figura 3.15: Single Load Balancer

3.2 Ip Spoofing

IP spoofing refere-se à criação de pacotes IP com um endereço IP de origem falsificado com o objetivo de esconder a identidade do remetente ou se passar por outro sistema de rede.

3.2.1 Prevenir IP Spoofing at Layer 3

- Uma medida eficaz para prevenir o IP spoofing é negar o tráfego externo a IP's de origem igual às redes protegidas ou aos intervalos de endereços IP privados.
- A **Reverse Path Verification** é uma técnica utilizada para negar o tráfego em que o IP de origem não é alcançável através da interface pela qual o pacote chegou.
- Além disso, é importante negar o tráfego com destinos de multicast para evitar possíveis ataques de spoofing.

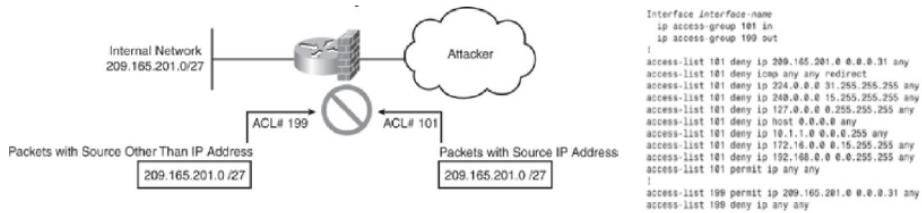


Figura 3.16: IP Spoofing at Layer 3

3.2.2 Prevenir IP Spoofing at Layer 2

- A restrição do tráfego IP em portas de Layer 2 não confiáveis para clientes com um endereço IP atribuído funciona filtrando o tráfego IP com um endereço IP de origem diferente daquele atribuído via **DHCP** ou configuração estática nas portas de Layer 2 não confiáveis.

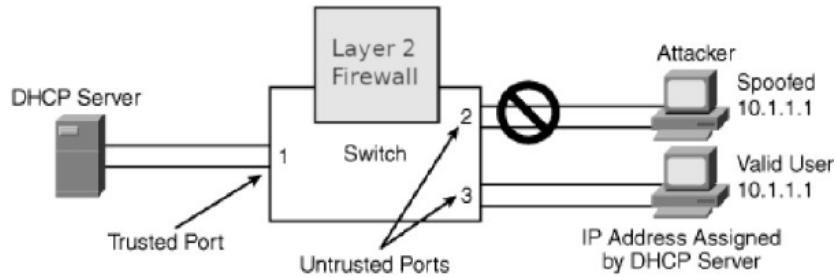


Figura 3.17: IP Spoofing at Layer 2

3.3 Half-Open TCP Connection Problem

O problema das conexões TCP meio-abertas envolve um tipo comum de ataque de negação de serviço (DoS) que explora o estado de conexão TCP meio-aberta, onde um lado encerrou a conexão enquanto o outro ainda espera dados. Os firewalls mantêm o estado das sessões TCP em memória, e múltiplas conexões TCP meio-abertas podem sobrecarregar o firewall, levando a um DoS.

Para mitigar, é crucial definir timeouts apropriados para as conexões TCP meio-abertas, com valores menores em situações de ataque. Em casos extremos, pode ser necessário limpar essas conexões do firewall externamente. A configuração correta dos timeouts é essencial para lidar com esse tipo de ataque e garantir a proteção contra DoS.

3.4 Firewall Performance Evaluation

⇒ Basic Firewall

- **IP Throughput:** Capacidade bruta do firewall de passar tráfego de interface para interface.
- **Latency:** Tempo de atraso do tráfego no firewall. Deve ser medido e relatado quando o firewall está em sua carga operacional.

⇒ Firewall Empresarial Tradicional

- **Taxa de Estabelecimento de Conexão:** Velocidade com que os firewalls podem estabelecer conexões.

- **Capacidade de Conexão Concorrente:** Número total de conexões abertas através do firewall em qualquer momento dado.
- **Taxa de Desmontagem de Conexão:** Velocidade com que os firewalls podem encerrar conexões e liberar recursos.

⇒ **Firewall de Próxima Geração**

- **Taxa de Transação de Aplicativo:** Capacidade do firewall de garantir transações de camada de aplicativo discretas contidas em uma conexão aberta.
- Pode incluir gateways de camada de aplicativo, prevenção de intrusões ou tecnologia de inspeção profunda.
- As taxas de transação de aplicativo são altamente dependentes de dados.

3.5 Linux IPTables

As Linux IPTables são ferramenta de espaço do utilizador pela qual os administradores criam regras para os módulos de filtragem de pacotes e NAT, usada para configurar, manter e inspecionar as tabelas de regras de filtragem de pacotes IP no kernel do Linux 🚧.

O iptables possui 5 cadeias padrão:

- INPUT
- OUTPUT
- FORWARD
- PREROUTING
- POSTROUTING

Além de 3 tabelas padrão: Filter, nat e mangle. As decisões básicas no iptables incluem ACCEPT, DROP, QUEUE e RETURN, enquanto as decisões estendidas envolvem LOG, MARK, REJECT, TOS, SNAT, DNAT, MASQUERADE, REDIRECT, entre outras. O iptables também possui múltiplas máquinas de estado, como o Conntrack (rastreador de conexão).

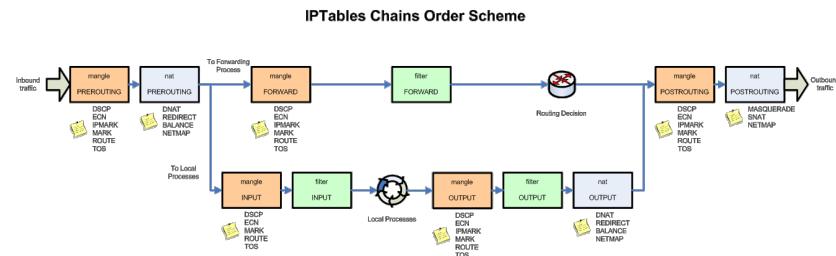


Figura 3.18: Linux IPTables

3.6 Linux nftables

As nftables são uma estrutura do Linux que substitui partes do iptables, oferecendo filtragem e classificação de pacotes de rede. O nftables fornecem uma nova framework de classificação de pacotes no kernel, baseado numa Máquina Virtual (VM) específica de rede, e utiliza um novo comando de utilizador nft no espaço do usuário. Ele oferece alto desempenho por meio de mapas e concatenações, possui um código de kernel menor e coloca a inteligência no comando nft no espaço do utilizador. Além disso, as nftables apresenta uma sintaxe unificada e consistente para todas as famílias de protocolos suportadas, facilitando a transição e as alterações nas regras do firewall.

3.7 Control By Analysis of Higher Layers

O controlo do fluxo de tráfego através da análise das camadas superiores de dados/protocolos é viável apenas em tráfego não criptografado. Alguns firewalls oferecem a capacidade de desencriptar e inspecionar o tráfego SSL/TLS. Isso é realizado através da instalação de um certificado raiz nos dispositivos dos clientes, permitindo que atuem como Autoridade de Certificação para os pedidos SSL. Os firewalls emitem certificados aos clientes em nome dos servidores web aos quais estão se estão a conectar, intercetando o handshake SSL/TLS.

No entanto, essa abordagem requer modificações nos dispositivos dos clientes e é intensiva em termos de processamento, levando a uma degradação no desempenho. Uma maneira de mitigar isto é utilizando dispositivos dedicados para descarregar a descriptografia SSL/TLS. É importante notar que esta prática pode violar leis e direitos de privacidade e confidencialidade nalguns países.

3.8 Cisco's Access Control Lists (ACL)

Uma Access Control Lists é uma coleção sequencial de condições de permitir e negar. O software testa pacotes contra as condições em uma lista de acesso uma por uma. A primeira correspondência determina se o software aceita ou rejeita o pacote. Como o software para de testar as condições após a primeira correspondência, a ordem das condições é crítica. Se nenhuma condição corresponder, o software rejeita o pacote. Pode ser aplicado ao tráfego de entrada ou saída.

Tipos de ACL's

- **Standard**

Controla o tráfego pela análise do endereço de origem dos pacotes IP. Numerados de 1 a 99.

– Exemplo: `access-list 1 permit 10.1.1.0 0.0.0.255`

- **Extended**

Controla o tráfego pela análise dos endereços de origem e destino e do protocolo dos pacotes IP. Numerados de 100 a 199.

– Exemplo: `access-list 101 permit ip any 10.1.1.0 0.0.0.255`

- **Named**

Permite que ACLs padrão e estendidas recebam nomes em vez de números. Identifique intuitivamente uma ACL usando um nome alfanumérico. Elimina os limites de números que existem em ACLs padrão e estendidas. As ACLs nomeadas fornecem a capacidade de modificar ACLs sem excluí-las e reconfigurá-las.

– Exemplo: `ip access-list {extended | standard} name`

- **Reflexive**

Permite que pacotes IP sejam filtrados com base em informações de sessão de camada superior. A comunicação em uma direção abre portas na direção oposta. Geralmente usado para permitir tráfego de saída e limitar tráfego de entrada em resposta a sessões que se originam de ZW:0. Inspecciona o tráfego para descobrir e gerenciar informações de estado 21311313 para sessões TCP e UDP. Essas informações de estado são usadas para criar aberturas temporárias na lista de acesso do firewall. - 3221

Bibliografia

- [1] L. e Sic Notícias, *Ano de 2022 foi dos que registou maior número de ciberataques*, <https://sicnoticias.pt/pais/2023-06-25-Ano-de-2022-foi-dos-que-registou-maior-numero-de-ciberataques-de-grande-impacto-4ec8ba92>.
- [2] everythingRF, *What is GPS Jamming?*, <https://www.everythingrf.com/community/what-is-gps-jamming/>.
- [3] geeksforgeeks, *Introduction of Basic Service Set (BSS)*, <https://www.geeksforgeeks.org/introduction-of-basic-service-set-bss/>.
- [4] M. Beschokov, *What Is A Firewall And How Does It Work?*, <https://www.wallarm.com/what/the-concept-of-a-firewall>.
- [5] V. Fulber-Garcia, *Firewalls: Stateless vs. Stateful*, <https://www.baeldung.com/cs/firewalls-stateless-vs-statefull>.