SÃO
PAULO
TECH
SCHOOL

Infraestrutura em Nuvem

Aula 05

Professor Marcio Santana

marcio.santana@sptech.school

Agenda da Aula

- Segurança em Redes
- Lab - Security Groups
- Atividade - Case de Segurança

Malware

É um **termo amplo que engloba todos os tipos de software malicioso**.

O objetivo do malware pode variar, desde **danificar sistemas** e dados até **roubar informações pessoais**, espionar atividades do usuário ou assumir o controle de dispositivos.

Vírus

É um tipo de **malware que se anexa a arquivos ou programas** existentes e se espalha quando esses arquivos ou programas são executados.

O objetivo principal de um vírus é **causar danos ao sistema** ou aos **dados do usuário**, como **corromper arquivos ou tornar o sistema inoperável.**

Phishing

É uma **técnica de engenharia social** usada para **enganar os usuários**, fazendo-os revelar informações confidenciais, como senhas ou números de cartão de crédito.

Normalmente, os phishers **usam e-mails, sites falsos ou mensagens falsas** para parecerem legítimos e **enganar as vítimas.**

Spyware

Projetado para **coletar informações pessoais** e atividades do usuário sem o seu conhecimento ou consentimento.

Ele pode **rastrear a navegação na web**, registros de teclas digitadas e outras atividades, e geralmente é usado para fins maliciosos, como roubo de identidade ou espionagem.

Trojans (Cavalos de Troia):

Malware que se disfarça de **software legítimo.**

Não se replica sozinho, mas **realiza ações maliciosas quando executado.**

Worms

Malware autônomo que se **espalha automaticamente** por redes e sistemas.

Explora vulnerabilidades de software para replicação e propagação.

Como proteger a Rede?

- Conceito antigo, começou na década de 80 com a popularização da internet

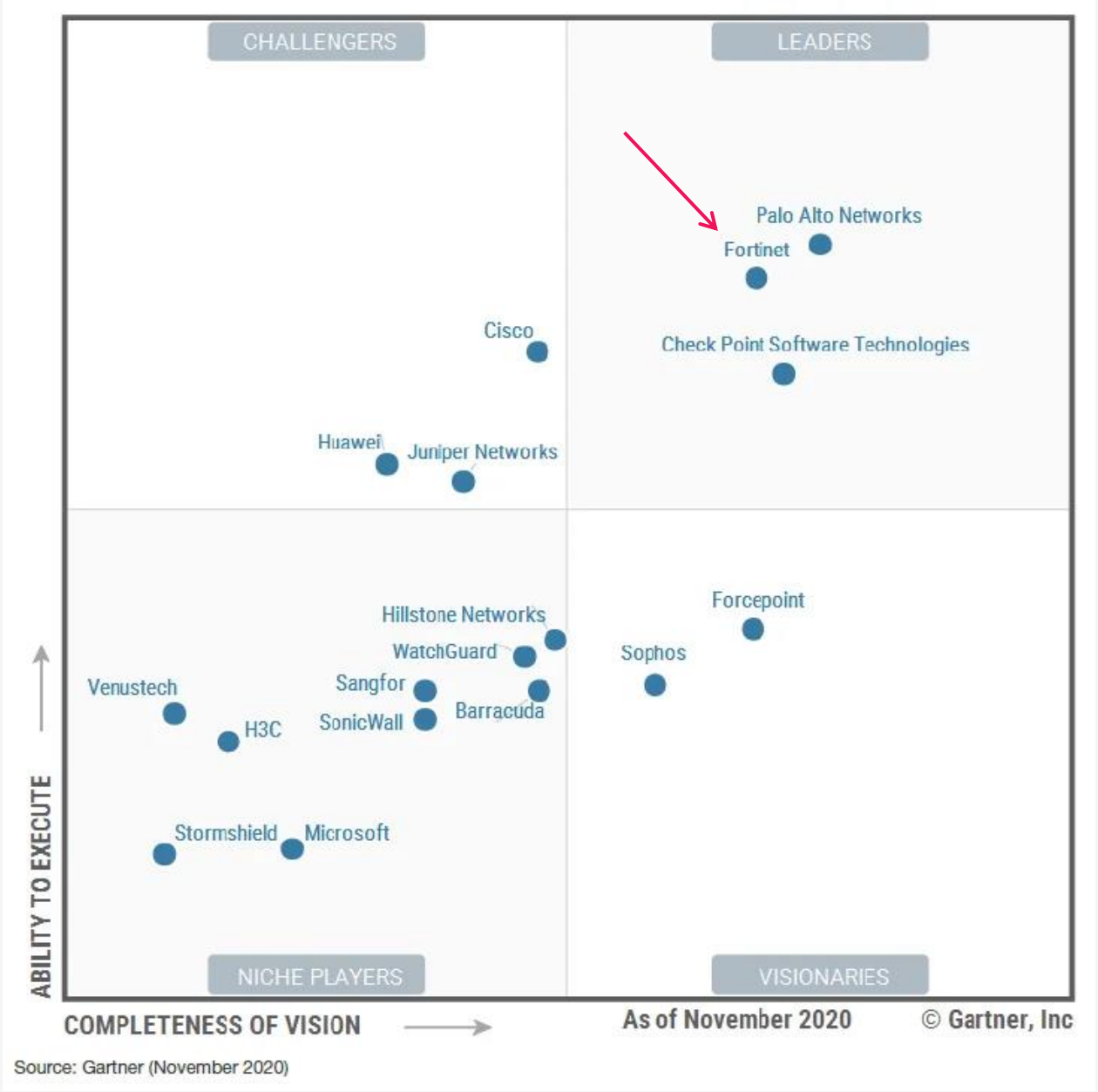
- Novas funcionalidade foram sendo agregadas aos Firewall assim surgiu o:

Firewall UTM (Unified Threat Management – Gerenciamento Unificado de Ameaças)

Esses equipamentos acumula alguns serviços:

- ✓ **Firewall:** Controla o tráfego de entrada e saída com base em regras de segurança;
- ✓ **Antivírus:** Inspeciona o tráfego de dados em busca de vírus e malwares;
- ✓ **Controle de Aplicações:** Monitora e controla o uso de aplicativos, permitindo ou bloqueando o uso.
- ✓ **Balanceamento de Links:** Permite conectar mais de um provedor de internet;
- ✓ **VPN:** Oferece suporte para conexões seguras por meio de VPNs (redes privadas virtuais);
- ✓ **Filtro de Conteúdo:** Bloqueia o acesso a sites maliciosos ou inadequados, usando filtros baseados em categorias.
- ✓ **Controle de acesso Wireless:** Centralizar a gestão de Aps
- ✓ **Relatórios:** Permite visualizar e gerar relatórios sobre o tráfego de rede

Quadrante Mágico da Gartner para Firewalls



AWS Security Groups

- Um security group atua como um **firewall virtual** para sua instância para **controlar o tráfego de entrada e saída;**
- Quando você executa uma instância na VPC, é possível atribuir até **cinco grupos de segurança à instância;**
- Os grupos de segurança atuam no **nível da instância** e não no nível da sub-rede;
- **Cada instância** em uma sub-rede em sua VPC pode ser **atribuída a um conjunto** diferente de grupos de segurança.

AWS Security Groups

Se você executar uma instância EC2 e não especificar um grupo de segurança, a instância será atribuída automaticamente ao **grupo de segurança padrão da VPC;**

Se você executar uma instância usando o console do Amazon EC2, terá a **opção de criar um grupo de segurança** para a instância.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

AWS Security Groups e Router Tables

As configurações são complementares:

- Um Security Group **aceita protocolos** de rede como TCP, UDP, ICMP com base em portas.

- As **tabelas de roteamento devem ser associadas às suas sub-redes** para que o tráfego de rede (TCP) saiba para onde ir.

Como o Modelo OSI surgiu

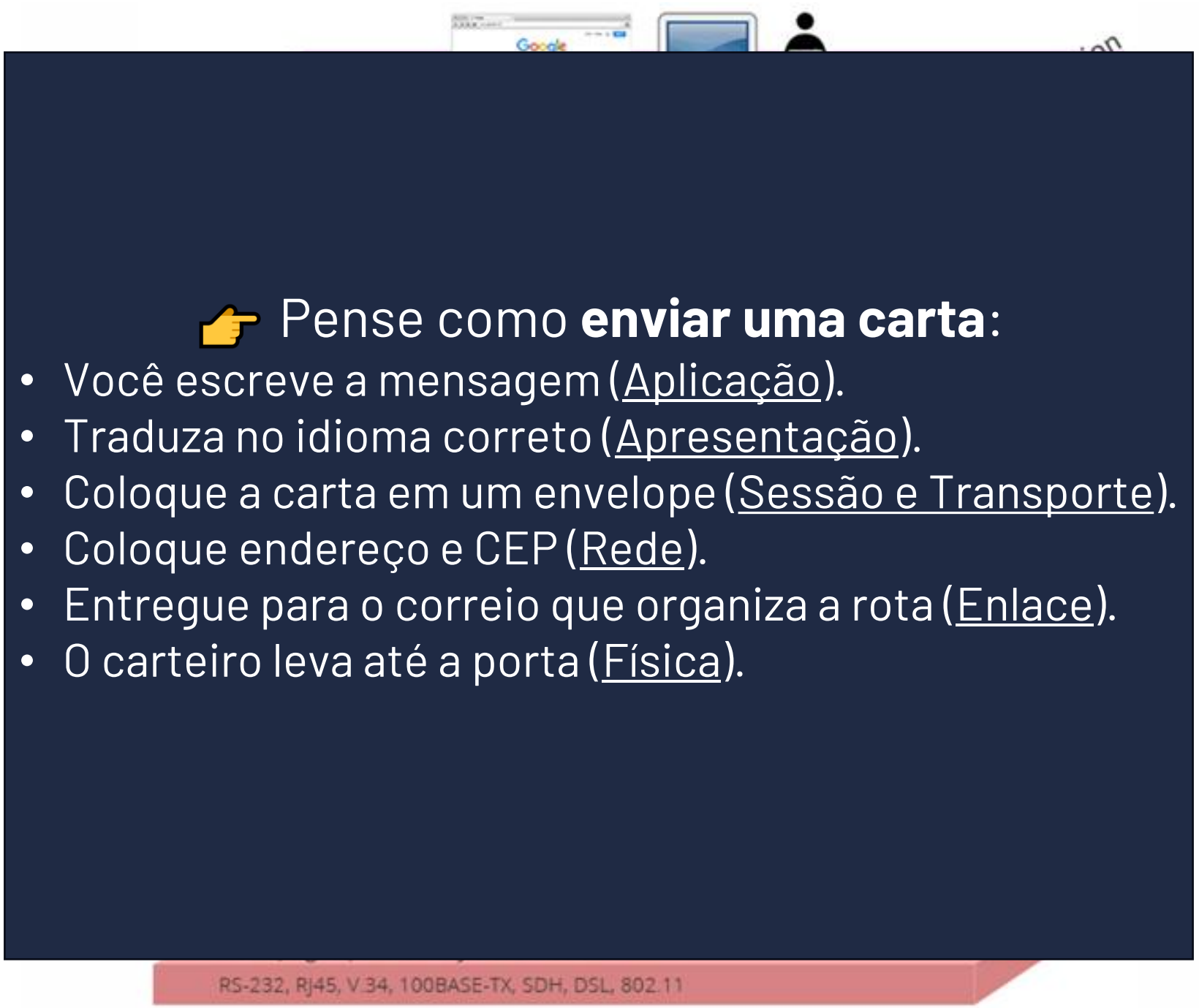
- Nos anos 70 e 80, cada fabricante de computador (IBM, Xerox, etc.) criava sua própria forma de comunicação de rede.
- **O problema: esses sistemas não conseguiam conversar entre si.**
- Por exemplo: uma rede IBM não conseguia se comunicar facilmente com uma rede de outro fabricante.
- Para resolver isso, a **ISO** (International Organization for Standardization) começou a trabalhar em um modelo padronizado.
- Em 1984, a ISO publicou o **Modelo OSI (Open Systems Interconnection).**
- O objetivo era criar **uma linguagem comum** para que diferentes equipamentos e softwares pudessem se comunicar.

Modelo OSI

Open System Interconnection

Interconexão de Sistemas Abertos

7xCamadas de Rede



👉 Pense como **enviar uma carta**:

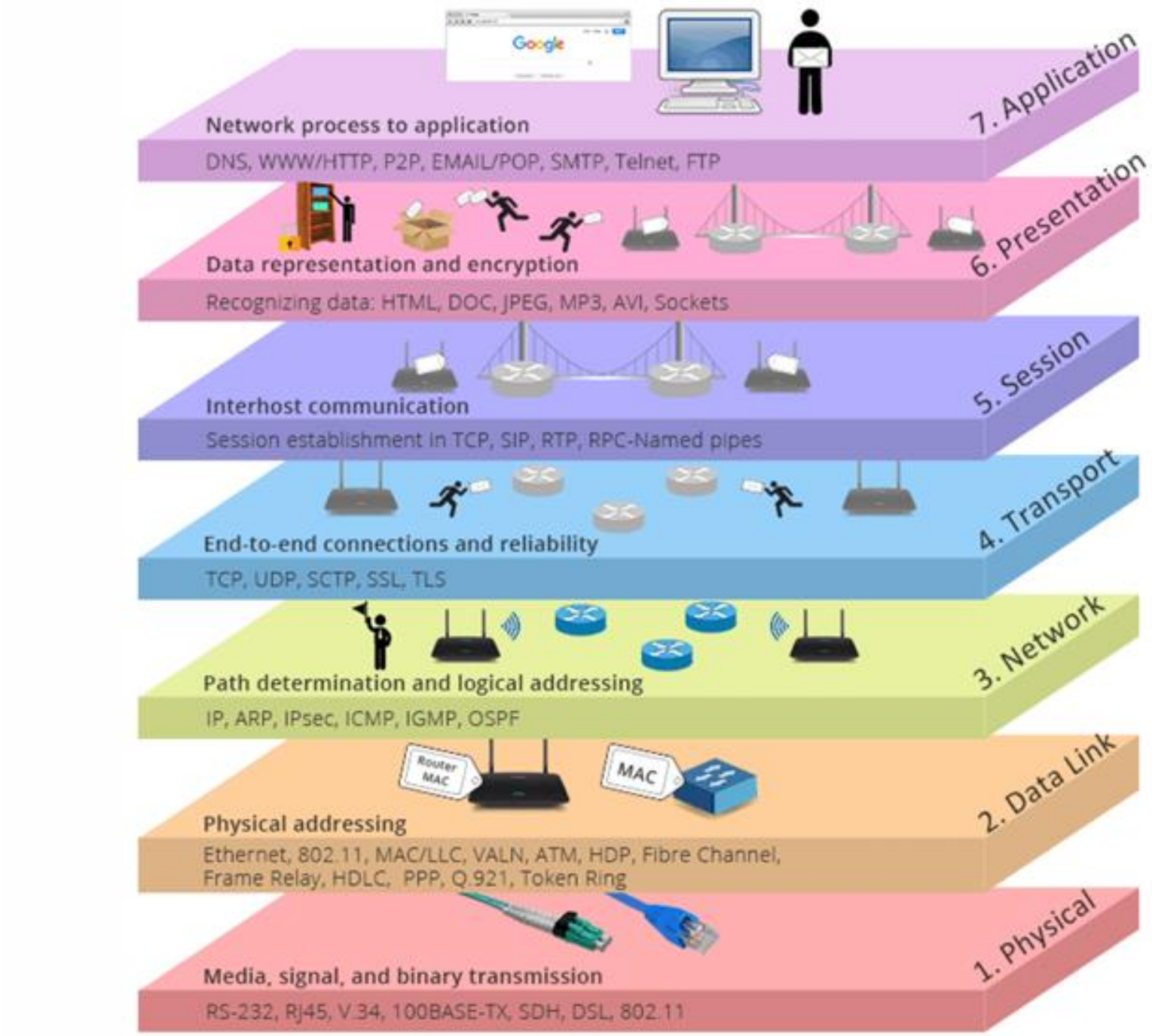
- Você escreve a mensagem (Aplicação).
- Traduza no idioma correto (Apresentação).
- Coloque a carta em um envelope (Sessão e Transporte).
- Coloque endereço e CEP (Rede).
- Entregue para o correio que organiza a rota (Enlace).
- O carteiro leva até a porta (Física).

Modelo OSI

Open System Interconnection

Interconexão de Sistemas Abertos

7xCamadas de Rede



Camada 1 ao 3

Camada 1: **Física (Physical Layer)** Responsável pela **transmissão de dados brutos por meios físicos**, como cabos ou sinais sem fio. Trata de aspectos como voltagem, frequência e modulação dos sinais.

Exemplos: cabos de rede, conectores, repetidores, hubs.

Camada 2: **Enlace de Dados (Data Link Layer)** Garante a **transferência de dados confiável** entre dois nós diretamente conectados. Gerencia a detecção de erros e o controle de fluxo.

Exemplos: switches, MAC (Media Access Control), protocolos como Ethernet.

Camada 3: **Rede (Network Layer)** Responsável pelo **roteamento dos pacotes de dados** entre diferentes redes. Gerencia endereçamento lógico e determina o melhor caminho para o envio dos dados.

Exemplos: roteadores, IP (Internet Protocol), ICMP (Internet Control Message Protocol)

Camada 4 ao 5

Camada 4: Transporte (Transport Layer) Assegura a **transferência confiável** de dados de ponta a ponta.

Gerencia a segmentação dos dados, controle de fluxo e correção de erros.

Exemplos: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

Camada 5: Sessão (Session Layer) Gerencia e **controla as conexões (sessões)** entre dois dispositivos.

Estabelece, mantém e encerra sessões de comunicação.

Exemplos: protocolos de gerenciamento de sessão, como NetBIOS e RPC (Remote Procedure Call)

Camada 6 ao 7

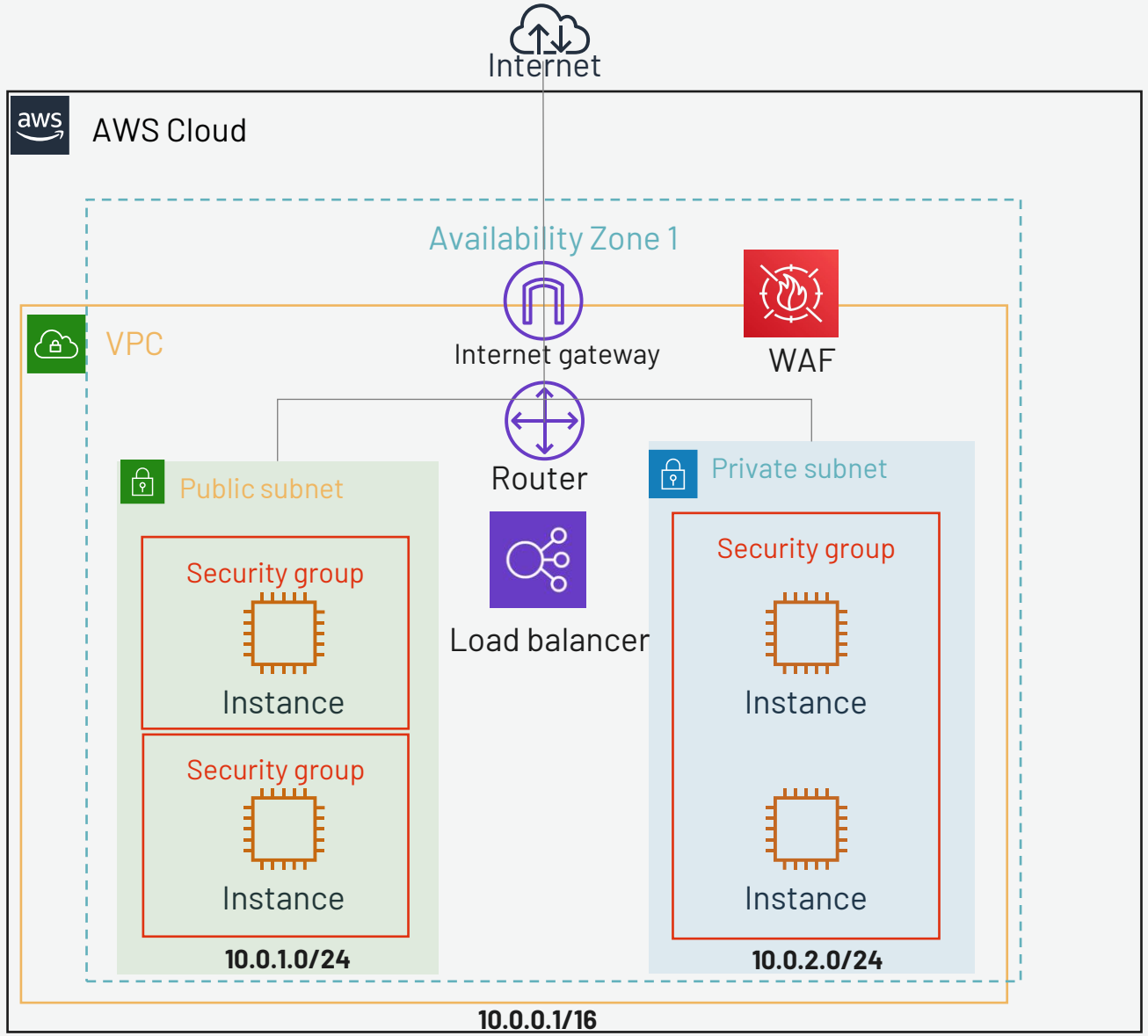
Camada 6: **Apresentação (Presentation Layer)** **Tradução dos dados entre o formato** utilizado pela rede e o formato compreensível pelo aplicativo. Inclui criptografia, compressão e conversão de dados.

Exemplos: SSL/TLS (para criptografia), JPEG (para imagens), MPEG (para vídeos).

Camada 7: **Aplicação (Application Layer)** **Fornece interfaces para que os aplicativos utilizem a rede**. É a camada mais próxima do usuário final e engloba protocolos de comunicação usados por aplicativos.

Exemplos: HTTP (para navegação web), FTP (para transferência de arquivos), SMTP (para envio de e-mails).

Arquitetura de Referência



Public SubNet Router Table

Destination	Target
10.0.0.1/16	10.0.1.0/24
0.0.0.0	Igw-id

Private SubNet - Router Table

Destination	Target
10.0.0.1/16	10.0.2.0/24

Serviços Cloud AWS – WAF (Web Application Firewall)

- Esse serviço **inspeciona o tráfego HTTP** antes que ele chegue ao seu aplicativo da Web para **bloquear o tráfego** da Web mal-intencionado.
- O WAF pode ser **usado na frente de um aplicativo** executado no EC2 ou na frente de um aplicativo em contêiner executando no ECS, por exemplo.
- Pode também usar um Application Load Balancer na frente dos servidores de aplicativos e **associar o WAF a esse Load balancer.**
- Se seu aplicativo for executado em um **Serveless**, como por exemplo um Lambda, você poderá fazer o mesmo, mas usando o API Gateway.
- Um WAF **mitiga os ataques** antes que eles atinjam seu aplicativo.

Podemos minimizar o risco em nossa infraestrutura

1. **Separando as redes em Private e Public VPC**
2. **Adicionando regras de Security Group**
3. **Criando ACL**
4. **Implementando Politicas no serviço WAF**

Agradeço
a sua atenção!

Marcio Santana

marcio.santana@sptech.school

SÃO PAULO TECH SCHOOL