# FUNDAMENTOS DE FIREWALL PT-BR

Joas Antonio

# Detalhes

- Apenas um overview sobre os conceitos fundamentais sobre um firewall;
- O pdf tem como objetivo ajudar aqueles que querem entender o funcionamento da ferramenta fundamental em uma rede;

Meu LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos

# O que é Firewall e como funciona?

- Um firewall é um dispositivo de **segurança de rede** que monitora o tráfego de entrada e saída da rede e permite ou bloqueia **pacotes de** dados com base em um conjunto de regras de segurança. Seu objetivo é estabelecer uma barreira entre sua rede interna e o tráfego de entrada de fontes externas (como a Internet) para bloquear o tráfego malicioso, como vírus e hackers.
- Os firewalls analisam cuidadosamente o tráfego de entrada com base em regras pré-estabelecidas e filtram o tráfego proveniente de fontes não seguras ou suspeitas para evitar ataques. Os firewalls protegem o tráfego em um ponto de entrada do computador, chamado portas, que é onde as informações são trocadas com dispositivos externos. Por exemplo, “O endereço de origem 172.18.1.1 tem permissão para alcançar o destino 172.18.2.1 pela porta 22."
- Pense nos endereços IP como casas e nos números das portas como cômodos dentro da casa. Apenas pessoas confiáveis (endereços de origem) têm permissão para entrar na casa (endereço de destino) - então é filtrado ainda mais para que as pessoas dentro da casa tenham permissão para acessar apenas determinados quartos (portas de destino), dependendo se são os proprietários , uma criança ou um convidado. O proprietário pode entrar em qualquer sala (qualquer porta), enquanto as crianças e hóspedes podem entrar em um determinado conjunto de salas (portas específicas).
- https://www.forcepoint.com/pt-br/cyber-edu/firewall

# Tipos de Firewall

- Os firewalls podem ser software ou hardware, embora seja melhor ter os dois. Um firewall de software é um programa instalado em cada computador e regula o tráfego por meio de números de portas e aplicativos, enquanto um firewall físico é um equipamento instalado entre a rede e o gateway.

**Os firewalls de filtragem de pacotes**

- O tipo mais comum de firewall, examinam os pacotes e os proíbem de passar se eles não corresponderem a um conjunto de regras de segurança estabelecido. Este tipo de firewall verifica os endereços IP de origem e destino do pacote. Se os pacotes corresponderem a uma regra “permitida” no firewall, ele é confiável para entrar na rede.
- Os firewalls de filtragem de pacotes são divididos em duas categorias: com estado e sem estado. Os firewalls sem estado examinam os pacotes independentemente uns dos outros e não têm contexto, tornando-os alvos fáceis para hackers. Em contraste, os firewalls com monitoração de estado lembram informações sobre pacotes passados anteriormente e são considerados muito mais seguros.
- Embora os firewalls de filtragem de pacotes possam ser eficazes, eles fornecem uma proteção muito básica e podem ser muito limitados - por exemplo, eles não podem determinar se o conteúdo da solicitação que está sendo enviada afetará adversamente o aplicativo que está alcançando. Se uma solicitação mal-intencionada permitida de um endereço de origem confiável resultasse, digamos, na exclusão de um banco de dados, o firewall não teria como saber disso. Firewalls de próxima geração e firewalls de proxy são mais equipados para detectar tais ameaças.

# Tipos de Firewall

- Os firewalls de filtragem de pacotes operam em linha em pontos de junção onde dispositivos como roteadores e switches fazem seu trabalho. No entanto, esses firewalls não roteiam pacotes; em vez disso, eles comparam cada pacote recebido a um conjunto de critérios estabelecidos, como os endereços IP permitidos, tipo de pacote, número de porta e outros aspectos dos cabeçalhos de protocolo de pacote. Os pacotes sinalizados como problemáticos são, em geral, descartados sem cerimônia - ou seja, eles não são encaminhados e, portanto, deixam de existir.

**Vantagens do firewall de filtragem de pacotes**

- Um único dispositivo pode filtrar o tráfego de toda a rede
- Extremamente rápido e eficiente na verificação do tráfego
- Barato
- Efeito mínimo em outros recursos, desempenho de rede e experiência do usuário final

**Desvantagens do firewall de filtragem de pacotes**

- Como a filtragem de tráfego é baseada inteiramente no endereço IP ou nas informações da porta, a filtragem de pacotes carece de um contexto mais amplo que informa outros tipos de firewalls
- Não verifica a carga útil e pode ser facilmente falsificado
- Não é uma opção ideal para todas as redes
- As listas de controle de acesso podem ser difíceis de configurar e gerenciar

# Tipos de Firewall

- Usando outra maneira relativamente rápida de identificar conteúdo malicioso, os Circuit-level gateway monitoram handshakes TCP e outras mensagens de inicialização de sessão de protocolo de rede à medida que são estabelecidas entre os hosts locais e remotos para determinar se a sessão iniciada é legítima - se o o sistema remoto é considerado confiável. Eles não inspecionam os pacotes sozinhos, no entanto.

**Vantagens do Circuit-level gateway**

- Apenas processa transações solicitadas; todo o outro tráfego é rejeitado
- Fácil de configurar e gerenciar
- Baixo custo e impacto mínimo na experiência do usuário final

**Desvantagens do Circuit-level gateway**

- Se não forem usados em conjunto com outra tecnologia de segurança, os Circuit-level gateway não oferecem proteção contra vazamento de dados de dispositivos dentro do firewall
- Sem monitoramento de camada de aplicativo
- Requer atualizações contínuas para manter as regras atualizadas
- Embora os gateways em nível de circuito forneçam um nível mais alto de segurança do que firewalls de filtragem de pacotes, eles devem ser usados em conjunto com outros sistemas. Por exemplo, os gateways no nível do circuito são normalmente usados junto com os gateways no nível do aplicativo. Essa estratégia combina atributos de firewalls de gateway em nível de pacote e circuito com filtragem de conteúdo.

# Tipos de Firewall

**Application-level gateway**

- Esse tipo de dispositivo - tecnicamente um proxy e às vezes chamado de *firewall proxy* - funciona como o único ponto de entrada e saída da rede. Os gateways no nível do aplicativo filtram os pacotes não apenas de acordo com o serviço ao qual se destinam - conforme especificado pela porta de destino - mas também por outras características, como a string de solicitação HTTP.
- Embora os gateways que filtram na camada do aplicativo forneçam segurança de dados considerável, eles podem afetar drasticamente o desempenho da rede e podem ser difíceis de gerenciar.

**Vantagens do Application-level gateway**

- Examina todas as comunicações entre fontes externas e dispositivos atrás do firewall, verificando não apenas as informações de endereço, porta e cabeçalho TCP, mas o próprio conteúdo antes de permitir que qualquer tráfego passe pelo proxy
- Fornece controles de segurança refinados que podem, por exemplo, permitir o acesso a um site, mas restringir quais páginas desse site o usuário pode abrir
- Protege o anonimato do usuário

**Desvantagens do Application-level gateway**

- Pode inibir o desempenho da rede
- Mais caro do que algumas outras opções de firewall
- Requer um alto grau de esforço para obter o máximo benefício do gateway
- Não funciona com todos os protocolos de rede
- Os firewalls de camada de aplicativo são mais usados para proteger os recursos da empresa contra ameaças de aplicativos da web . Eles podem bloquear o acesso a sites perigosos e evitar que informações confidenciais vazem de dentro do firewall. Eles podem, no entanto, causar um atraso nas comunicações.

# Tipos de Firewall

## Stateful inspection firewall

- Os dispositivos com reconhecimento de estado não apenas examinam cada pacote, mas também controlam se o pacote faz ou não parte de um TCP estabelecido ou de outra sessão de rede. Isso oferece mais segurança do que a filtragem de pacotes ou o monitoramento de circuito sozinho, mas tem um impacto maior no desempenho da rede.
- Uma outra variante da inspeção stateful é o firewall de inspeção multicamadas, que considera o fluxo de transações em processo em várias camadas de protocolo do modelo Open Systems Interconnection (OSI) de sete camadas .

**Vantagens do Stateful inspection firewall**

- Monitora toda a sessão para o estado da conexão, ao mesmo tempo que verifica os endereços IP e cargas para uma segurança mais completa
- Oferece um alto grau de controle sobre o conteúdo que pode entrar ou sair da rede
- Não precisa abrir várias portas para permitir o tráfego de entrada ou saída
- Oferece recursos de registro substantivos

**Desvantagens do Stateful inspection firewall**

- Consome muitos recursos e interfere na velocidade das comunicações da rede
- Mais caro do que outras opções de firewall
- Não fornece recursos de autenticação para validar que as fontes de tráfego não são falsificadas
- A maioria das organizações se beneficia do uso de um firewall de inspeção com monitoração de estado. Esses dispositivos servem como um gateway mais completo entre computadores e outros ativos dentro do firewall e recursos fora da empresa. Eles também podem ser altamente eficazes na defesa de dispositivos de rede contra ataques específicos, como DoS.

# Tipos de Firewall

**Os firewalls de última geração (NGFW)**

- Um NGFW típico combina inspeção de pacote com inspeção de estado e também inclui alguma variedade de inspeção profunda de pacote ( DPI ), bem como outros sistemas de segurança de rede, como IDS / IPS, filtragem de malware e antivírus.
- Enquanto a inspeção de pacotes em firewalls tradicionais olha exclusivamente para o cabeçalho do protocolo do pacote, o DPI analisa os dados reais que o pacote está transportando. Um firewall DPI rastreia o progresso de uma sessão de navegação na web e pode notar se uma carga útil de pacote, quando montada com outros pacotes em uma resposta de servidor HTTP, constitui uma resposta formatada em HTML legítima.

**Vantagens do NGFW**

- Combina DPI com filtragem de malware e outros controles para fornecer um nível ideal de filtragem
- Rastreia todo o tráfego da camada 2 para a camada de aplicativo para obter insights mais precisos do que outros métodos
- Pode ser atualizado automaticamente para fornecer o contexto atual

**Desvantagens do NGFW**

- Para obter o maior benefício, as organizações precisam integrar NGFWs com outros sistemas de segurança, o que pode ser um processo complexo
- Mais caro do que outros tipos de firewall

https://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls

# Tipos de Firewall

**Os Proxy-Firewall**

- filtram o tráfego de rede no nível do aplicativo. Ao contrário dos firewalls básicos, o proxy atua como um intermediário entre dois sistemas finais. O cliente deve enviar uma solicitação ao firewall, onde é avaliada em relação a um conjunto de regras de segurança e, em seguida, é permitida ou bloqueada. Mais notavelmente, os firewalls de proxy monitoram o tráfego de protocolos da camada 7, como HTTP e FTP, e usam a inspeção de pacotes com estado e profunda para detectar tráfego malicioso.

**Os Network address translation (NAT) firewalls**

- permitem que vários dispositivos com endereços de rede independentes se conectem à Internet usando um único endereço IP, mantendo os endereços IP individuais ocultos. Como resultado, os invasores que varrem uma rede em busca de endereços IP não podem capturar detalhes específicos, proporcionando maior segurança contra ataques. Os firewalls NAT são semelhantes aos firewalls de proxy, pois atuam como intermediários entre um grupo de computadores e o tráfego externo.

**Stateful multilayer inspection (SMLI) firewalls**

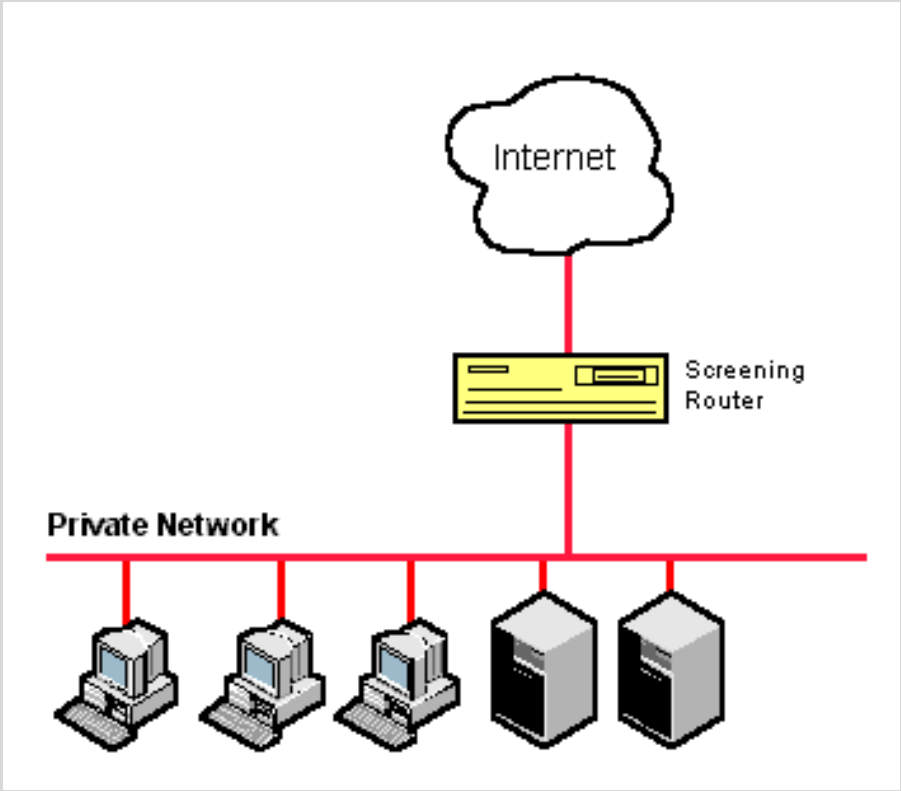
- filtram pacotes nas camadas de rede, transporte e aplicativo, comparando-os com pacotes confiáveis conhecidos. Como os firewalls NGFW, o SMLI também examina o pacote inteiro e só permite que eles passem se passarem por cada camada individualmente. Esses firewalls examinam os pacotes para determinar o estado da comunicação (portanto, o nome) para garantir que todas as comunicações iniciadas ocorram apenas com fontes confiáveis.

# Modelos de Entrega

- **Firewalls baseados em hardware**
- Um firewall baseado em hardware é um dispositivo que atua como um gateway seguro entre os dispositivos dentro do perímetro da rede e aqueles fora dele. Por serem dispositivos autocontidos, os firewalls baseados em hardware não consomem energia de processamento ou outros recursos dos dispositivos host.
- Às vezes chamados *de firewalls baseados em rede* , esses dispositivos são ideais para organizações de médio e grande porte que buscam proteger muitos dispositivos. Firewalls baseados em hardware requerem mais conhecimento para configurar e gerenciar do que seus equivalentes baseados em host.
- **Firewalls baseados em software**
- Um firewall baseado em software, ou *firewall host* , é executado em um servidor ou outro dispositivo. O software de firewall do host precisa ser instalado em cada dispositivo que requer proteção. Assim, os firewalls baseados em software consomem alguns dos recursos de CPU e RAM do dispositivo host.
- Os firewalls baseados em software fornecem aos dispositivos individuais proteção significativa contra vírus e outros conteúdos maliciosos. Eles podem discernir diferentes programas em execução no host, enquanto filtram o tráfego de entrada e saída. Isso fornece um nível de controle refinado, tornando possível habilitar as comunicações de / para um programa, mas impedi-las de / para outro.
- **Firewalls hospedados em nuvem /**
- Os provedores de serviços de segurança gerenciados (MSSPs) oferecem firewalls baseados em nuvem. Este serviço hospedado pode ser configurado para rastrear a atividade de rede interna e ambientes sob demanda de terceiros. Também conhecido como *firewall como serviço* , os firewalls baseados em nuvem podem ser totalmente gerenciados por um MSSP, o que os torna uma boa opção para empresas grandes ou altamente distribuídas com lacunas nos recursos de segurança. Os firewalls baseados em nuvem também podem ser benéficos para organizações menores com equipe e experiência limitada.

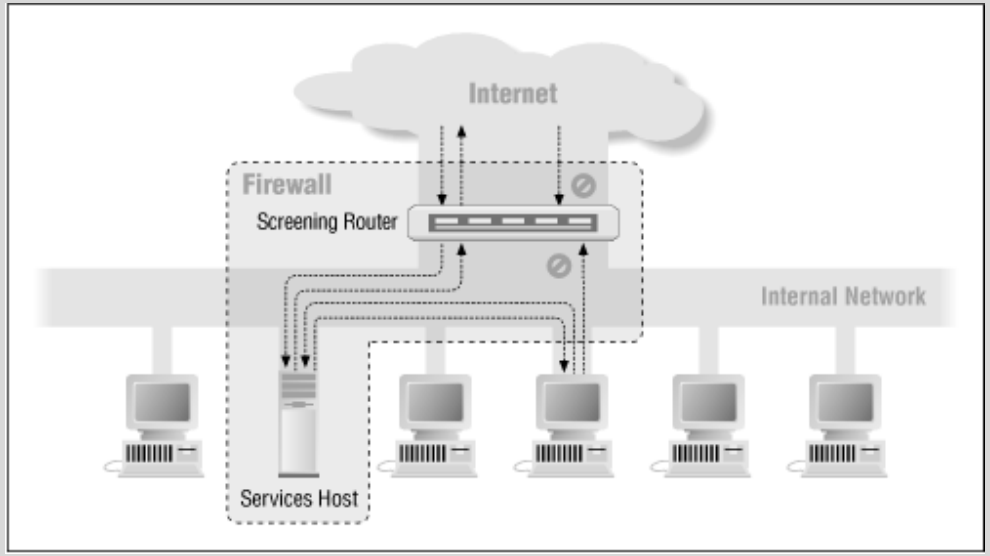
# Arquitetura de Firewall

- **Screening Router:**
- É a arquitetura mais simples utilizada, caracteriza-se pela presença de um roteador de filtro de pacotes entre a rede interna e a internet. Nessa arquitetura existe comunicação direta entre múltiplos servidores internos e múltiplos servidores externos. A sua zona de risco é proporcional ao número de servidores na rede interna e os tipos de serviço de tráfego permitidos pelo roteador. Para cada tipo de serviço permitido a zona de risco aumenta consideravelmente. Controle de danos é igualmente difícil, já que o administrador da rede teria que verificar cada servidor a procura de traços de invasão regularmente. No caso de destruição do firewall tende a ficar muito complicado rastrear ou até mesmo notar a invasão. Já a facilidade de uso entretando é bem alta, já que o usuário pode acessar diretamente os serviços da internet. Essa configuração é um caso de "Aquilo que não é expressamente proibido é permitido".



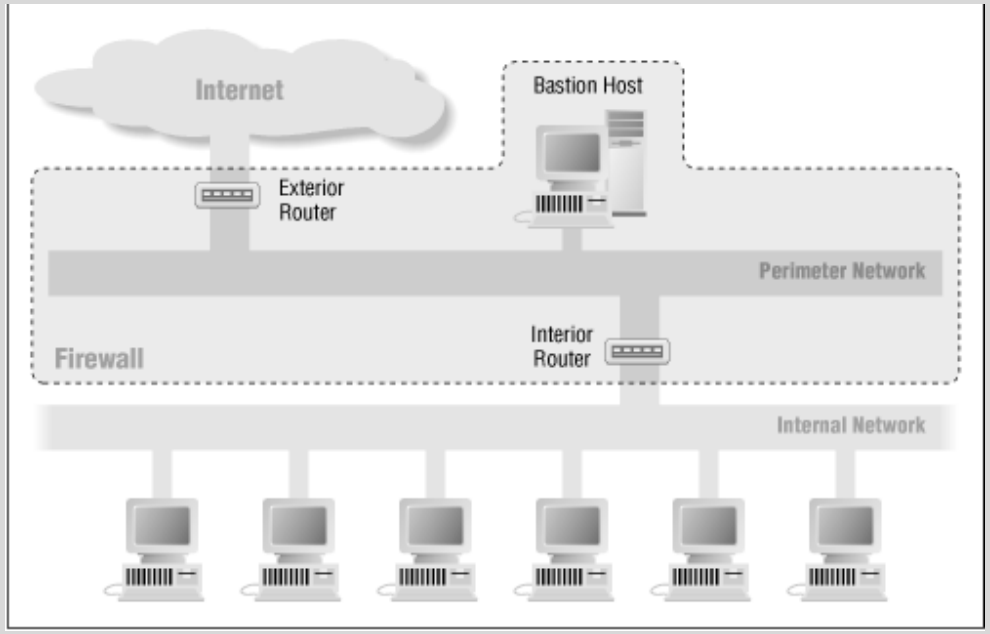
# Arquitetura de Firewall

- **<u>Screened Host:</u>**
- Em geral, arquiteturas desse tipo são altamente seguras. porém não muito simples de se implementar. Tipicamente, configura-se um servidor principal com segurança reforçada, sendo ele o único ponto de comunicação entre a rede interna e a internet, esse servidor é chamado de *Bastion Host.* Entre o *Bastion Host* e a internet, utiliza-se a arquitetura do *Screening router.* A zona de risco é restrita somente ao *Bastion Host* e o roteador. A estância básica dos *Screened Hosts* é determinada pelo *software* utilizado no *Bastion Host.*



# Arquitetura de Firewall

- **Screened Subnet:**
- É considerada a mais segura, pois adiciona uma nova camada de segurança à arquitetura *Screened Host*. Baseia-se na criação de uma sub-rede, geralmente chamada de *Perimiter Network* ou DMZ (*Demilitarized Zone*), que isola a rede interna da externa, sendo ela a responsável por toda a comunicação entre as redes, além da criação do *Bastion Host*. Sendo asssim, uma *Screened Subnet* é formada por um Bastion Host isolado pela sub-rede, um roteador responsável pela comunicação entre a rede interna e o bastion host e outro responsável pela comunicação entre o bastion host e a rede externa(internet). Para invadi-lo o ataque teria que passar por ambos os roteadores.Sendo assim, a zona de risco é reduzida drasticamente. A estância básica pode variar, porém como na maioria dos casos necessita-se alto nível de segurança utiliza-se a estância "Aquilo que não é expressamente permitido é proibido".




https://www.gta.ufrj.br/grad/08_1/firewall/architectures.html

# Alta disponibilidade

- A interrupção de sistemas é uma das maiores dores de cabeça que a uma equipe de TI pode experimentar. As empresas precisam de tecnologia para manter a produtividade de seus funcionários, e no momento em que um sistema fica indisponível, o desempenho das equipes cai, enquanto o número de chamados para a equipe de TI aumenta.
- E em tempo de ameaças cibernéticas frequentes, os sistemas de segurança do perímetro não podem deixar de funcionar, sob pena de expor usuários e informações confidenciais a potenciais ataques.

**O que é alta disponibilidade**

- Direto ao ponto: alta disponibilidade (H.A – high availability) é a capacidade de garantir a continuidade de serviços utilizados, mesmo em ocasiões de falhas (por exemplo, de hardware, software, interrupção de energia etc.). Ou seja, as funcionalidades do sistema não podem ser interrompidas.
- Esse é o caso do uso das soluções de segurança de redes.
- Aplicando este conceito à implementação de seu firewall, significa que caso ocorra uma falha (por exemplo, seu hardware sofre perda de funções por causa de uma interrupção de energia), haverá um sistema paralelo, com configurações idênticas ao firewall original, pronto para assumir a operação de filtragem de tráfego dentro do perímetro de sua empresa.

# Alta disponibilidade

**É aqui que entra o conceito de Failover**

- São configurados dispositivos de firewall independentes, mas que podem trabalhar em conjunto e se comunicar durante a operação. Quando uma falha é identificada, seja no software, seja na conexão física, o dispositivo alternativo pode passar a operar, assumindo todas as funções do equipamento inoperante.
- Duas formas de implementações são possíveis para dar continuidade aos serviços: **Ativo-Passivo** e **Ativo-Ativo**.
- No caso da implementação de firewall, nos dois modelos um dispositivo trabalha ativamente nas funções de monitoramento da rede, enquanto o segundo está em *stand by* e só irá operar caso o "titular" deixe de funcionar. Contudo, no **Ativo-Ativo**, as conexões e sessões de autenticação são replicadas entre as instâncias de equipamentos, enquanto no **Ativo-Passivo** todas as conexões precisam ser restabelecidas pelo usuário.
- A operação do failover pode ser configurada em **implementações de hardware ou virtuais**. Há possibilidade de operar de forma híbrida: o firewall primário pode ser implementado em appliance físico e o redundante em appliance virtual, desde de que as características de hardware sejam idênticas.
- Em todos os casos, a opção de failover é crucial para manter a segurança do ambiente, protegendo usuários, dispositivos e dados.

# Alta disponibilidade

**O que é redundância**

- O conceito de redundância está vinculado às implementações de alta disponibilidade. Basicamente, refere-se à presença do dispositivo adicional a ser adotado como back up (no caso ativo-passivo) ou balanceador (no caso ativo-ativo).

**Por que a minha empresa precisa de alta disponibilidade?**

- Essa é uma questão simples de responder:
- Se sua empresa precisa estar conectada a uma rede pública (internet) para operar, então há dois cenários que justificam a alta disponibilidade do firewall:

- **Produtividade:** É claro que a sua equipe utiliza aplicações web e na nuvem. O firewall pode ser adotado para filtrar conteúdos e permitir/bloquear o acesso a aplicações utilizadas pela sua equipe, garantindo mais produtividade e aderência à política de segurança da empresa. Contudo, normalmente um firewall está implementado entre a rede local e a Internet; caso o dispositivo falhe, seus usuários não terão acesso à rede externa, o que criará prejuízos financeiros em função da indisponibilidade de serviços e trabalho de restabelecimento dos serviços.
- **Segurança:** A internet é por onde todas as ameaças cibernéticas circulam. Sem a proteção de um firewall redundante, em caso de falha, o seu ambiente estará exposto a diversas ameaças frequentes (como vírus, malware, ransomware, trojans etc.) que são barradas pela proteção do firewall. Além disso, nos casos de adoção de serviços integrados, diversos recursos ficarão indisponíveis, como criptografia, proteção contra ameaças avançadas, prevenção contra intrusos etc.

https://www.blockbit.com/pt/blog/o-que-e-alta-disponibilidade/

# Modelo OSI

- Em meados da década de 80, os fabricantes de equipamentos chegaram a conclusão que o caminho a ser seguido deveria basear-se em normas (Padrões ou Standards). Surgiu então, o modelo que veio para solucionar o problema de incompatibilidades entre as tecnologias de diferentes fabricantes dando início ao surgimento do Modelo de Referência ISO (International Standards Organization) "OSI" (Open System Interconnection), isto devido esse modelo basear-se em uma proposta desenvolvida pela ISO. Este modelo propiciou às empresas e fabricantes uma padronização a fim de garantir compatibilidade coerente e ininterrupta entre as diversas tecnologias de rede construídas por diversas empresas em todo o mundo e garantindo a comunicação end-to-end (fim-a-fim).
- O modelo de camadas OSI foi desenvolvido para acabar com o bloqueio de comunicação entre redes de diferentes propriedades, permitindo a interoperabilidade independentemente de qual seja o fabricante de um ou outro dispositivo que compõe uma mesma rede ou, de um sistema que esteja sendo utilizado (FILIPPETTI, 2002).
- O "Modelo OSI", como chamaremos deste ponto em diante, é composto por 7 camadas, onde cada camada realiza funções específicas. Vale ressaltar que:
- o "Modelo OSI" propriamente dito não é uma arquitetura de rede, pois não especifica os serviços e os protocolos exatos que devem ser usados em cada camada. Ele apenas informa o que cada camada deve fazer. No entanto, a ISO também produziu padrões para todas as camadas, embora esses padrões não façam parte do próprio modelo de referência. Cada um foi publicado como um padrão internacional distinto. (TANENBAUM, 2003).

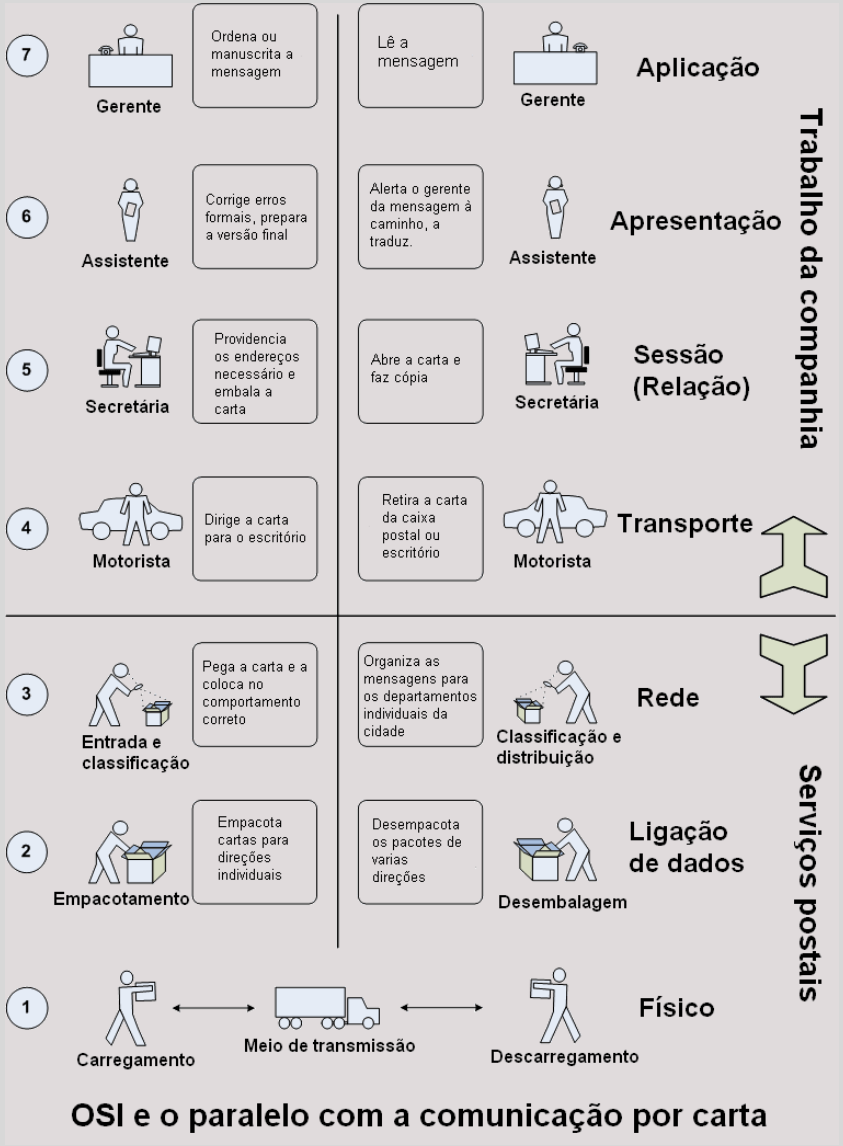
# Modelo OSI - Camadas

- **Aplicação** *(Application)*
- **Apresentação** *(Presentation)*
- **Sessão** *(Session)*
- **Transporte** *(Transport)*
- **Rede** *(Network)*
- **Dados / Enlace** *(Data Link)*
- **Física** *(Physical)*

# Modelo OSI - Camadas

**Camada de Aplicação (Application Layer)**

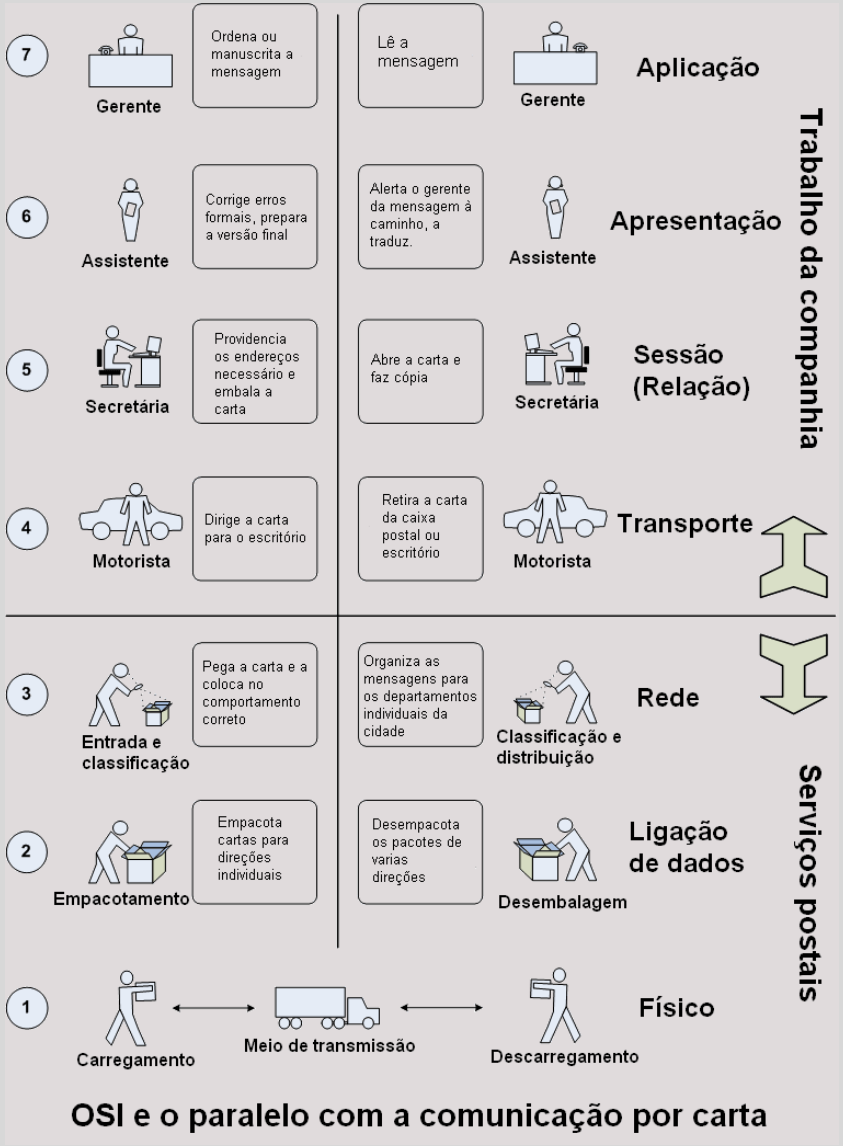
- Fornece serviços às aplicações do usuário.
- Possibilita que o usuário possa obter informações de sua rede através de um aplicativo, como navegador, também conhecido browser (Ex.: Mozilla Firefox, Google Chromium, Google Chrome...), Clientes de E-mail (Ex.: Thunderbird e Outlook Express), além de muitos outros.
- Esta camada é responsável diretamente pela interface entre o usuário do computador e a rede. Acesso a softwares que transmitem e recebem dados da rede, como softwares de e-mail e navegadores (FILIPPETTI, 2002).



# Modelo OSI - Camadas

**Camada de Apresentação** (Presentation Layer)

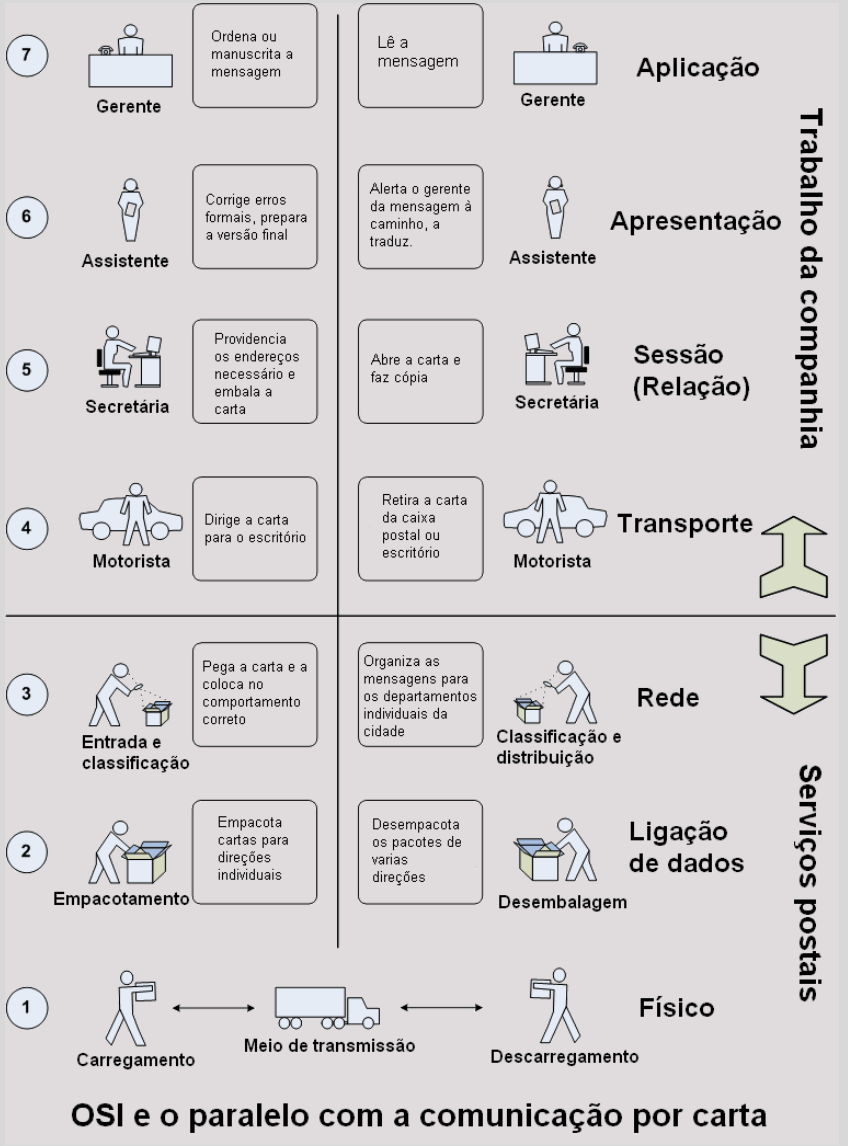
- Encriptação e compressão de dados.
- Cuida da tradução dos dados da camada de aplicação em dados legíveis (que sejam entendidos) pelos protocolos. Cuida também da formatação dos dados, e da representação destes.
- Assegura a compatibilidade entre camadas de aplicação de sistemas diferentes, ou seja, é responsável por fazer com que duas redes diferentes se comuniquem, transformando os dados no processo de comunicação.
- Camada responsável por apresentar os dados à camada de aplicação. Ela é encarregada de codificar e decodificar os dados, de maneira que se tornem legíveis na camada de aplicação, assim como criptografia e descompressão. Esta camada pode ser conhecida também como “camada tradutora” (DIOGENES, 2004).



# Modelo OSI - Camadas

**Camada de Sessão (Session Layer)**

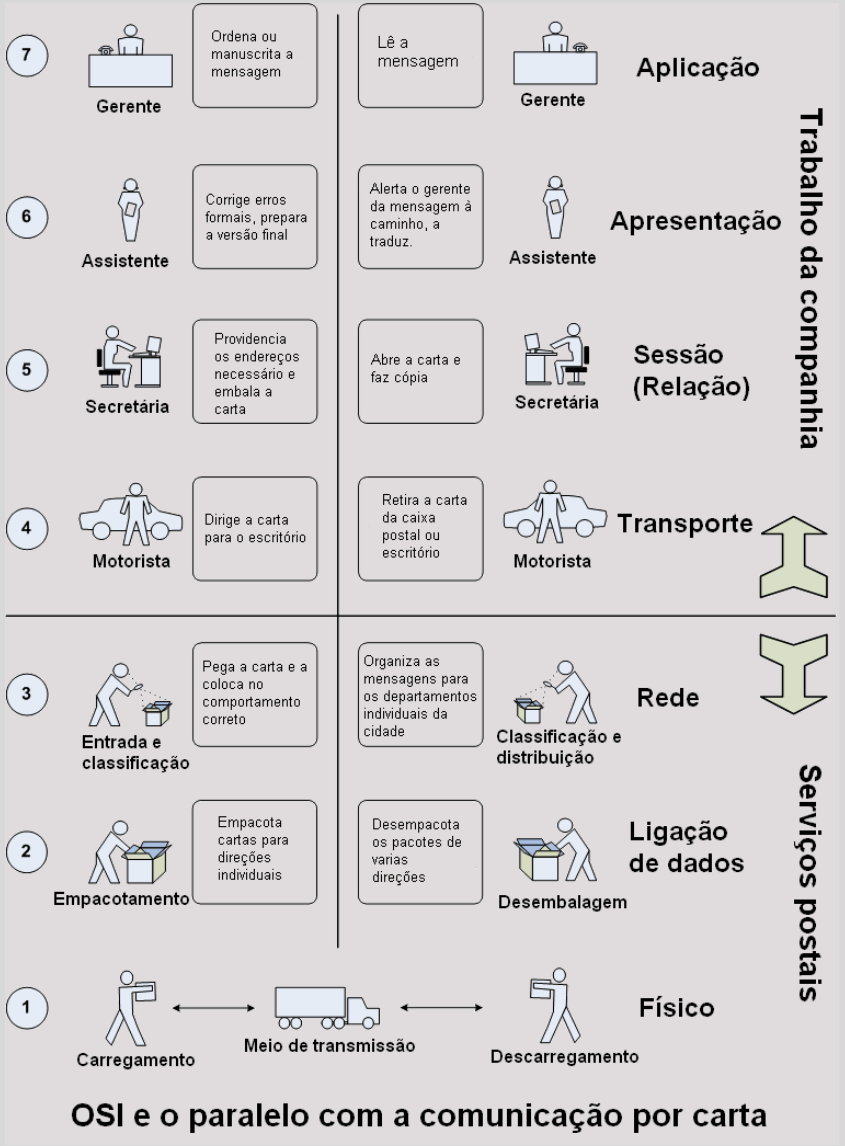
- Controla (estabelece, faz a gestão e termina), as sessões entre aplicações.
- Responsável por controlar a comunicação entre dois computadores. A camada de sessão gerencia o estabelecimento e finalização de uma conexão entre dois computadores, assim como as formas em que uma conexão pode ser feita: simplex (um computador apenas transmite, o outro apenas recebe), half duplex (somente um computador por vez transmite dados) ou full duplex (ambos os computadores podem transmitir e receber dados ao mesmo tempo) (FILIPPETTI, 2002).



# Modelo OSI - Camadas

**Camada de Transporte (Transport Layer)**

- Controle de fluxo de informação, segmentação e controle de erros.
- Garante a comunicação fim-a-fim (end-to-end).
- Se responsabiliza pela entrega e recebimento dos dados.
- O protocolo de transporte pode operar em 2 modos, Orientados à Conexão ou Não.
- Modo Não Orientado a Conexão: serviço de transporte não confiável. A camada de transporte somente mapeia o pedido de transmissão de dados em pacotes para a transmissão pela camada de rede. Um exemplo de um protocolo não orientado a conexão é o protocolo UDP (User Datagram Protocol).
- Modo Orientado a Conexão: serviço de transporte confiável. O transporte orientado a conexões consiste em ocultar as imperfeições do serviço de rede, de modo que os processos do usuário possam simplesmente supor a existência de um fluxo de bits livre de erros. Um exemplo de um protocolo orientado a conexão é o TCP (Transmission Control Protocol).
- É responsável por agrupar os dados em seguimentos e fragmentar estes seguimentos de forma que se encaixem na tecnologia física de redes da qual está sendo utilizada. Algumas características fazem parte desta camada, como garantir que os seguimentos foram entregues ao destino, controlar se houve erro na transmissão, controlar o fluxo de seguimentos em transmissão, garantir a seqüência correta destes seguimentos e, caso haja em algum momento, erro na transmissão ou, algum seguimento não seja entregue, a camada de transporte se encarrega de re-transmitir o seguimento perdido e/ou corrompido (DIOGENES, 2004).



# Modelo OSI - Camadas

**Camada de Rede (Network Layer)**

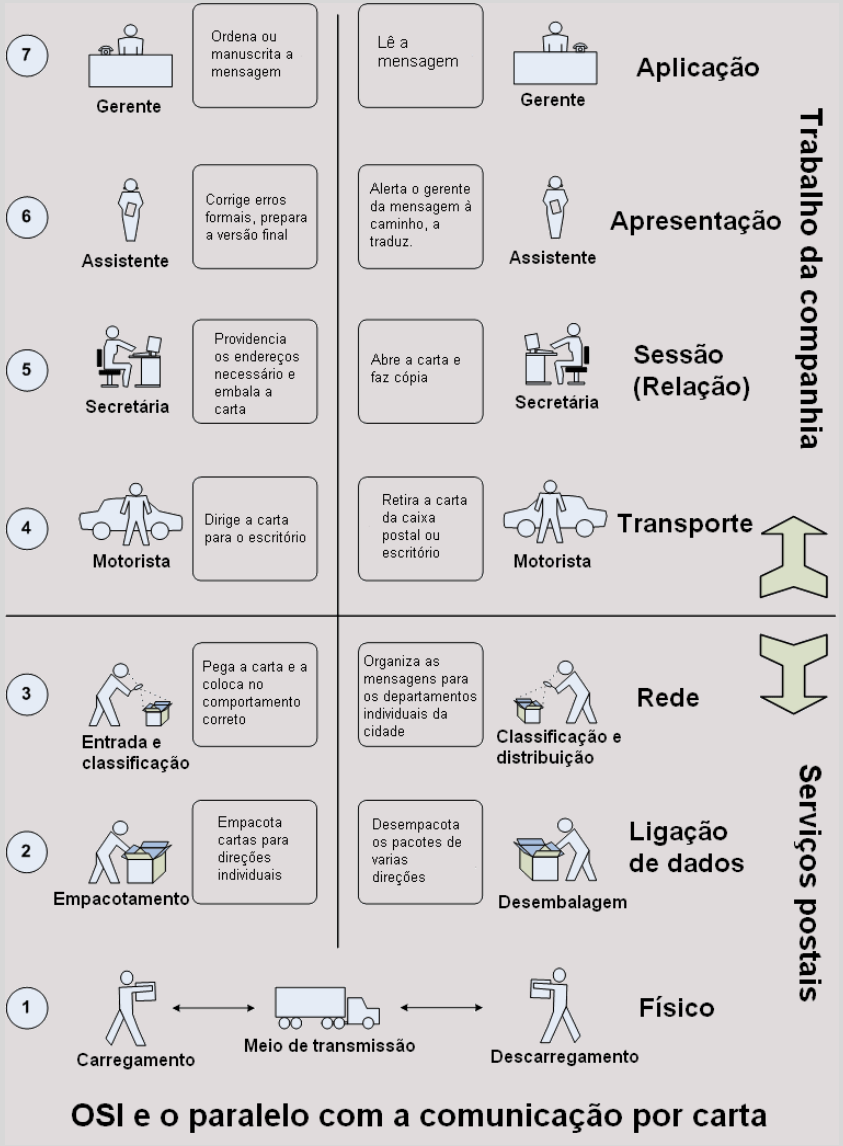
- Encaminhamento (routing) de pacotes e fragmentação.
- Esquema de endereçamento lógico dos pacotes, convertendo endereços lógicos em físicos (IP Address em MAC Address), fazendo com que os pacotes cheguem corretamente ao seu destino.
- Interconexão de Redes.
- Tratamento de Erros.
- Fragmentação de Pacotes.
- Controle de Congestionamento.
- Sequenciamento de Pacotes.
- Trata-se de uma camada onde, são encaminhados os dados na rede, verificando a melhor rota a ser seguida. É nesta camada que o endereçamento IP é atribuído ao pacote de dados (FILIPPETTI, 2002).

**Camada de Enlace ou Link de Dados (Data Link Layer)**

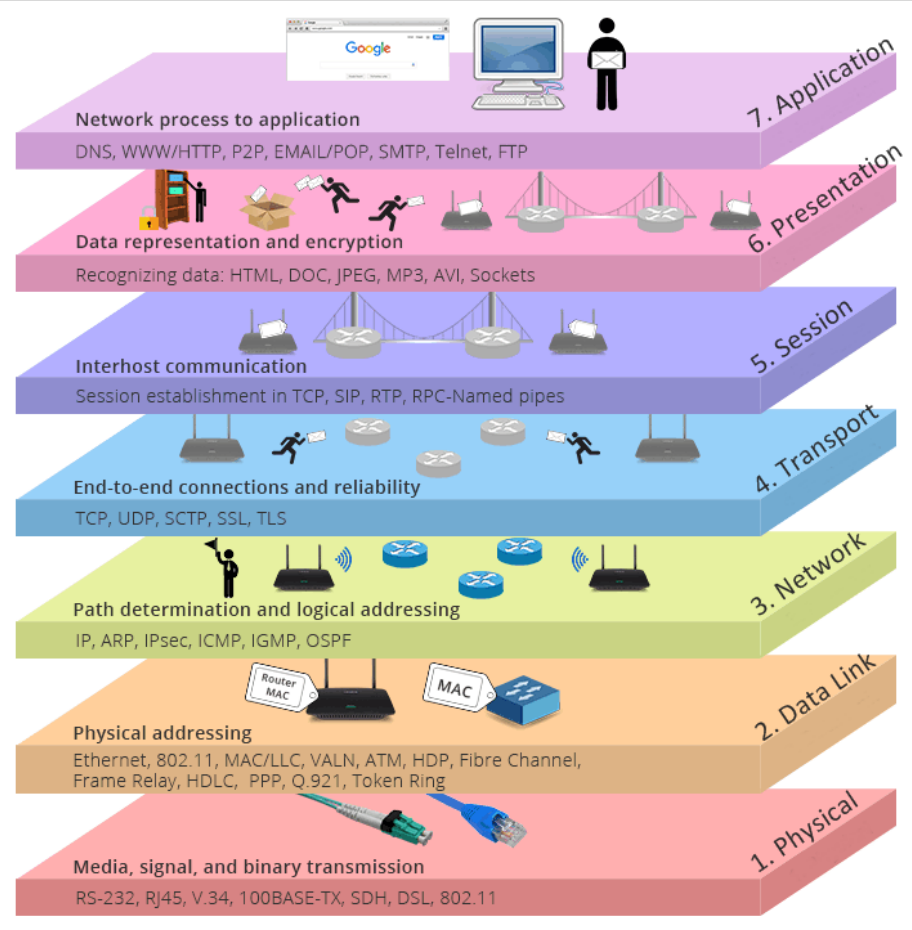
- Controla o acesso ao meio físico de transmissão.
- Controlo de erros da camada física.
- É responsável por fornecer meios funcionais para a transferência de dados entre os dispositivos da rede.
- O exemplo mais conhecido desta camada é a Ethernet. Outros são 802.11 (WiFi), Frame Relay e ATM. Na família TCP/IP temos o PPP e o SLIP.
- Esta camada é responsável por traduzir os dados vindos da camada anterior (Rede) em bits e prover a transferência dos dados no meio (DIOGENES, 2004).

**Camada Física (Physical Layer)**

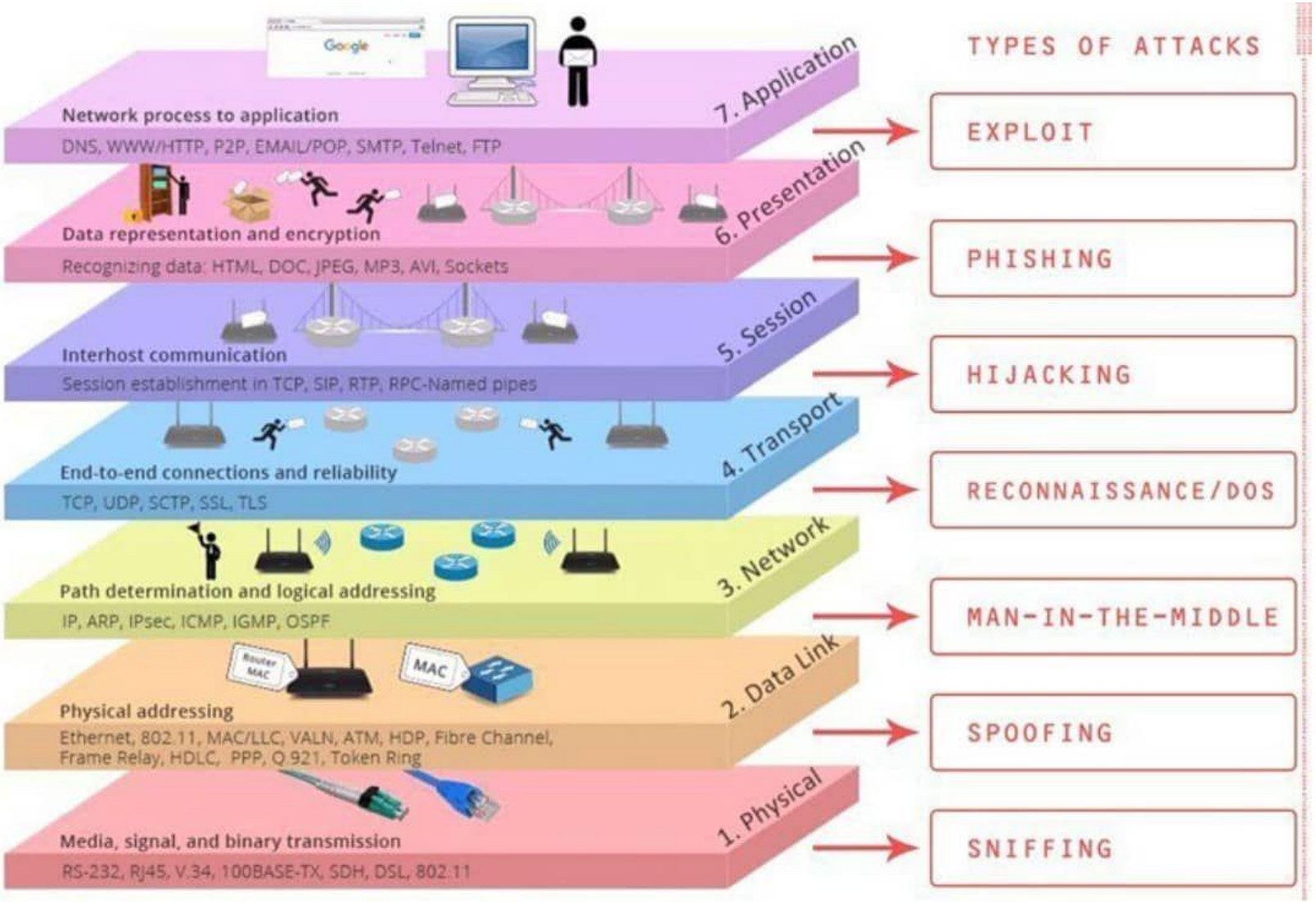
- Define as todas as características técnicas do meio físico de transmissão da rede, conectores, interfaces, codificação ou modulação de sinais, incluindo o layout de pinos, voltagens e especificações de cabos.
- Está é a camada do meio em si. Fazem parte desta camada o cabeamento, os conectores, voltagem, bits, entre outros dispositivos (DIOGENES, 2004).



# Modelo OSI - Protocolos




| Camada | Protocolo |
|---|---|
| 7.Aplicação | HTTP, RTP, SMTP, FTP, SSH, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS, Ping ... |
| 6.Apresentação | XDR, TLS ... |
| 5.Sessão | NetBIOS ... |
| 4.Transporte | NetBEUI, TCP, UDP, SCTP, DCCP, RIP ... |
| 3.Rede | IP (IPv4, IPv6), IPsec, ICMP, ARP, RARP, NAT ... |
| 2.Enlace<br>• Subcamada LLC<br>• Subcamada MAC | Ethernet, IEEE 802.1Q, HDLC, Token ring, FDDI, PPP, Switch, Frame relay, ATM ... |
| 1.Física | Modem, , 802.11 Wi-Fi RDIS, RS-232, EIA-422, RS-449, Bluetooth, USB, 10BASE-T, 100BASE-TX, ISDN, SONET, DSL ... |




# Modelo OSI - PenTest

# Modelo TCP/IP

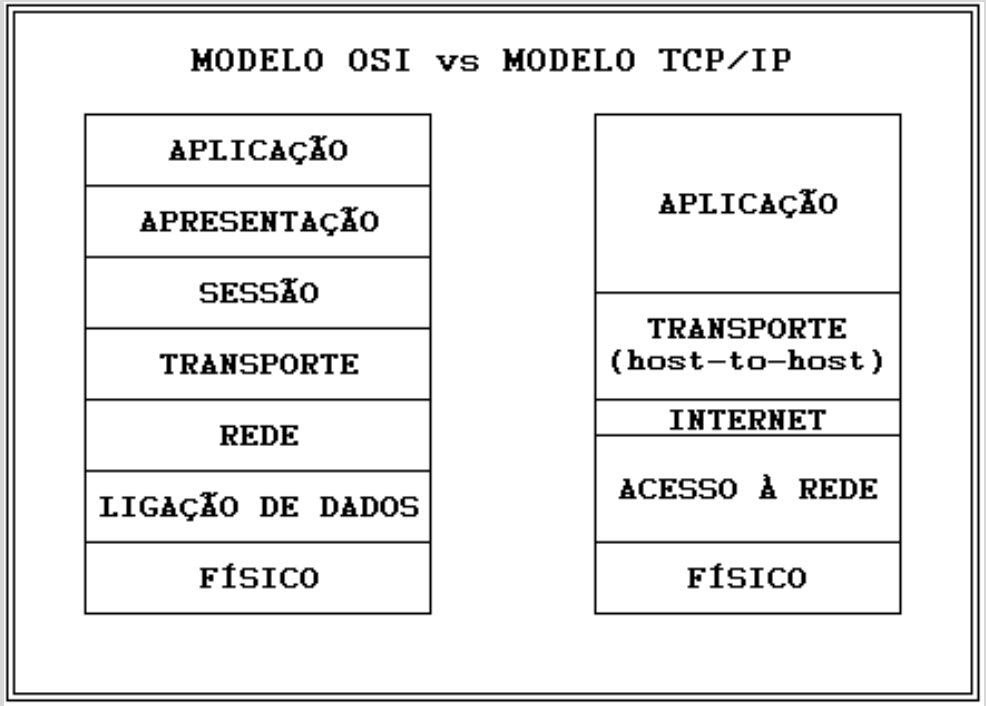
- Antes da internet se tornar tão popular os protocolos de comunicação mais importantes eram o TCP/IP, NETBEUI, IPX/SPX, Xerox Network System (XNS) e o Apple Talk. De salientar que para dois equipamentos de rede poderem comunicar entre si é essencial que ambos entendam as mesmas regras ou seja, ambos têm de usar o mesmo protocolo de comunicação.

- Com o acesso crescimento e vulgarização da Internet e com a necessidade de as redes internas das empresas se ligarem cada vez com mais frequência à Internet e de serem obrigadas a utilizar o protocolo já usado na internet, o protocolo TCP/IP expandiu-se também a estas redes empresariais tornando-se actualmente no protocolo padrão de comunicação.

- O TCP/IP (Transmission Control Protocol/Internet Protocol) representa um conjunto de protocolos que permitem que diversos equipamentos que constituem uma rede possam comunicar entre si. É um protocolo estruturado por camadas na qual cada camada utiliza e presta serviços às camadas adjacentes. Cada camada apenas trata das informações que correspondem à sua função.

- O modelo TCP/IP quando comparado com o modelo OSI, tem duas camadas que se formam a partir da fusão de algumas camadas do modelo OSI, elas são: as camadas de Aplicação (Aplicação, Apresentação e Sessão) e Acesso à Rede (Ligação de dados e Física).

- Existem 5 camadas distintas que formam o TCP/IP:



# Modelo TCP/IP

- **APLICAÇÃO:** Esta camada é formada por um vasto conjunto de protocolos os quais permitem o correcto funcionamento dos diversos Serviços/Aplicações do modelo TCP/IP. Esta camada não possui um padrão comum para todas as aplicações, ou seja, consoante o serviço em questão irá depender também o protocolo que o vai atender. Por exemplo o serviço e-mail utiliza o protocolo SMTP, sempre que este serviço é solicitado ao TCP/IP (envio ou recepção de e-mail), é este protocolo que se encarrega do atender. De igual modo sempre que é solicitado ao TCP/IP o serviço www o protocolo que se encarrega de o atender é o HTTP. Ou seja, por trás de cada aplicação existe um protocolo específico seja ele o FTP,TELNET, HTTP, SMTP, POP3, DNS, etc.
- **TRANSPORTE:** Pela figura, pode-se verificar que a Camada TCP do Modelo TCP/IP corresponde à Camada de Transporte do Modelo OSI. Desta forma, o TCP é responsável pelas funções de transporte nas quais se incluem os mecanismos necessários que garantem a entrega sequencial de dados, sem erros e sem falhas. O acesso das diversas Aplicações a esta camada é feito através de portas as quais têm associados números inteiros distintos para cada tipo de Aplicação. Podem ser utilizados dois protocolos distintos para o transporte, o TCP e o UDP. O TCP é orientado à conexão enquanto que o UDP não. O UDP funciona como segunda opção da camada de transporte uma vez que não oferece garantias de entrega de pacotes, nem da sua correcta sequência de envio. Normalmente o UDP só é utilizado em aplicações que geram elevados volumes de tráfego na Internet.
- **CAMADA IP ou INTERNET:** As Funções da Camada de Rede do Modelo OSI, são aqui realizadas pela Camada IP e pela consequente utilização do Protocolo IP. A Camada IP é uma camada normalizada em que o único protocolo utilizado é o protocolo IP. Esta camada é responsável pelo endereçamento, roteamento e controlo de envio e recepção dos dados. A comunicação é realizada por datagramas. O protocolo IP é não orientado à conexão, não garantindo que os pacotes IP cheguem ao seu destino nem se chegam pela ordem com que foram enviados. O IP é o protocolo responsável por definir o caminho que um pacote de dados deverá percorrer desde o host de origem até ao host destino, passando por uma ou várias redes onde poderá encontrar protocolos de conexão como o IP, o ICMP, o ARP e o RARP.
- **ACESSO À REDE:** Esta camada tem como principal função a adaptação do Modelo TCP/IP aos diversos tipos de redes (X.25, ATM, FDDI, Ethernet, Token Ring, Frame Relay, PPP e SLIP). É a camada de abstracção de hardware e devido à enorme variedade de tecnologias de rede possíveis, é uma camada não normalizada pelo modelo TCP/IP. É possível a interligação e interoperação com redes heterogéneas. Nesta camada são utilizados gateways ou routers.
- **FÍSICO:** Esta camada descreve as características físicas da comunicação tais como a natureza do meio usado para a comunicação (cobre, fibra-óptica ou links de rádio) e todos os detalhes relacionados com os sinais (modulações, comprimentos de onda, níveis de sinal, sincronizações, distâncias máximas, etc)

# PROTOCOLO TCP/IP

- O TCP é um protocolo da camada de transporte confiável em que existe a garantia que os dados são integralmente transmitidos para os hosts de destino correctos na sequência pelo qual foram enviados. O TCP segmenta a informação proveniente da Camada Aplicação em pequenos blocos de informação (datagramas) inserindo-lhes um cabeçalho de forma a que seja possível no hoste de destino fazer a reassemblagem dos dados. Este cabeçalho contém um conjunto de bits (checksum) que permite tanto a validação dos dados como do próprio cabeçalho. A utilização do checksum permite muitas vezes no hoste de destino recuperar informação em caso de erros simples na transmissão (nos casos da rede corrómper o pacote). Caso a informação seja impossível de recuperar ou o pacote TCP/IP se tenha perdido durante a transmissão, é tarefa do TCP voltar a transmitir o pacote. Para que o hoste de origem tenha a garantia que o pacote chegou isento de erros é necessário que o hoste de destino o informe através do envio de uma mensagem de "acknowledgement".

- O TCP corresponde a um conjunto de rotinas instaladas nos hosts de origem e destino as quais são utilizadas pelas várias aplicações (e-mail, http, FTP, telnet, etc) quando necessitam de executar o transporte de dados entre hosts.

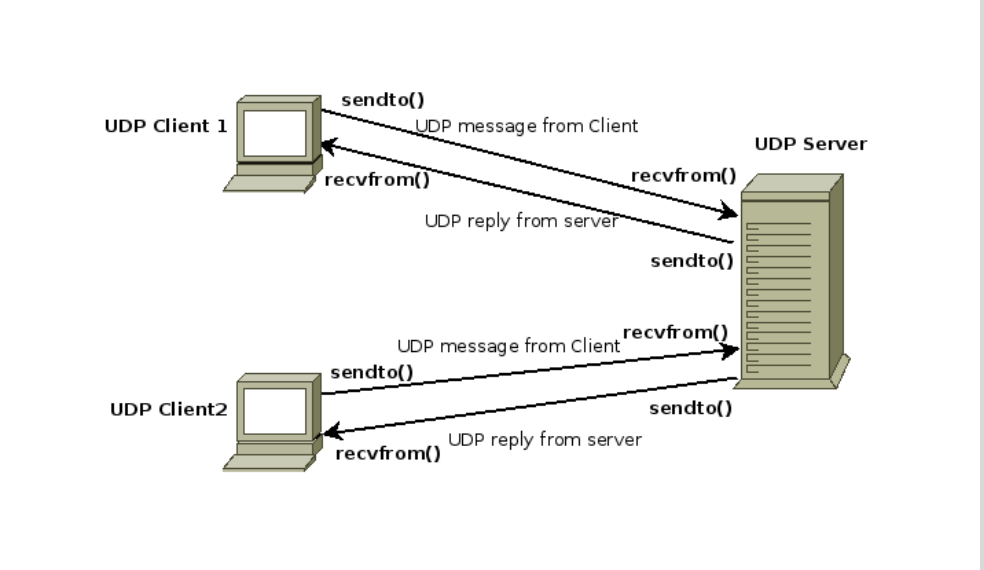
- Para que seja possível identificar a que serviço um determinado datagrama pertence, o TCP utiliza o conceito de portas. A cada porta está associado um serviço. Após determinada a porta, toda a comunicação com a aplicação é realizada e endereçada através dela.

- **Características do protocolo TCP:**

- ·Transferência de dados: transmissão ponto-a-ponto de blocos de dados no modo full-duplex.
- ·Transferência de dados com diferentes prioridades: transmite em primeiro lugar os datagramas que contenham sinalização de prioridade superior.
- ·Estabelecimento e libertação de conexões
- ·Sequenciação: Ordenação dos pacotes recebidos.
- ·Segmentação e reassemblagem: O TCP divide os dados a serem transmitidos em pequenos blocos de dados, identificando-os de forma a que no host de destino seja possível reagrupá-los.
- Controle de fluxo: o TCP é capaz de adaptar a transmissão dos datagramas às condições de transmissões ( velocidade , tráfego ... ) entre os diversos sistemas envolvidos.
- Controle de erros: A utilização de checksum permite verificar se os dados transmitidos estão livres de erros. É possível, para além da detecção a sua correcção.
- ·Multiplexagem de IP: Uma vez que é utilizado o conceito de portas, é possível enviar dados de diferentes tipos de serviços (portas diferentes) para o mesmo hoste de destino.

# Protocolo UDP

- O UDP (**U**ser **D**atagram **P**rotocol) é tido como um protocolo "irmão" do TCP, mas é mais simples e também menos confiável. Isso acontece porque o funcionamento do TCP é, como já dito, baseado em conexões, o que não ocorre com o UDP. Como conseqüência, não há procedimentos de verificação no envio e recebimento de dados (todavia, pode haver checagem de integridade) e se algum pacote não for recebido, o computador de destino não faz uma nova solicitação, como acontece com o TCP. Tudo isso faz do UDP um pouco mais rápido, porém inutilizável em certas aplicações.
- Por essas características, pode parecer que o UDP é inútil, mas não é. Há aplicações em que é preferível entregar os dados o mais rapidamente possível, mesmo que algumas informações se percam no caminho. É o caso, por exemplo, das transmissões de vídeo pela internet (streaming), onde a perda de um pacote de dados não interromperá a transmissão. Por outro lado, se os pacotes não chegarem ou demorarem a chegar, haverá congelamentos na imagem, causando irritação no usuário.



# Portas TCP e UDP

- Agora que você já conhece algumas características dos protocolos TCP e UDP, já está apto a entender o conceito de portas. Para uma compreensão mais fácil, usaremos o seguinte exemplo: suponha que, neste momento, você esteja usando um navegador de internet, um cliente de e-mail e um software de comunicação instantânea. Todas essas aplicações fazem uso da sua conexão à internet, mas como o computador faz para saber quais os dados que pertencem a cada programa? Simples, pelo número da porta que cada um utiliza. Por exemplo, se você está usando um programa de FTP (File Transfer Protocol), a conexão à internet é feita pela porta TCP 21, que é uma porta convencionada a este protocolo. Se estiver baixando arquivos pelo BitTorrent, uma das portas que vão de 6881 à 6889 estará sendo utilizada para tal atividade.
- Compare seu computador a um prédio. Ao chegar uma correspondência, é necessário saber a qual apartamento entregá-la. Se no envelope estiver escrito que o destino é o apartamento número 123, onde reside Fulano, basta fazer a entrega. Em seu computador, o conceito é o mesmo: basta substituir a correspondência pelo pacote de dados, o apartamento pela porta e o Fulano pelo programa. No entanto, é importante frisar que um aplicativo pode utilizar mais de uma porta.
- Ilustração de uso de portas TCP
- Ao todo, é possível usar 65536 portas TCP e UDP, começando em 1. Tanto no protocolo TCP como no UDP, é comum o uso das portas de 1 a 1024, já que a aplicação destas é padronizada pela IANA (Internet Assigned Numbers Authority). De acordo com essa entidade, eis algumas das portas TCP mais utilizadas:
- :: 21 - FTP;
- :: 23 - Telnet;
- :: 25 - SMTP;
- :: 80 - HTTP;
- :: 110 - POP3;
- :: 143 - IMAP;
- :: 443 - HTTPS.

https://www.infowester.com/portastcpudp.php

# Portas TCP e UDP

- Agora que você já conhece algumas características dos protocolos TCP e UDP, já está apto a entender o conceito de portas. Para uma compreensão mais fácil, usaremos o seguinte exemplo: suponha que, neste momento, você esteja usando um navegador de internet, um cliente de e-mail e um software de comunicação instantânea. Todas essas aplicações fazem uso da sua conexão à internet, mas como o computador faz para saber quais os dados que pertencem a cada programa? Simples, pelo número da porta que cada um utiliza. Por exemplo, se você está usando um programa de FTP (File Transfer Protocol), a conexão à internet é feita pela porta TCP 21, que é uma porta convencionada a este protocolo. Se estiver baixando arquivos pelo BitTorrent, uma das portas que vão de 6881 à 6889 estará sendo utilizada para tal atividade.
- Compare seu computador a um prédio. Ao chegar uma correspondência, é necessário saber a qual apartamento entregá-la. Se no envelope estiver escrito que o destino é o apartamento número 123, onde reside Fulano, basta fazer a entrega. Em seu computador, o conceito é o mesmo: basta substituir a correspondência pelo pacote de dados, o apartamento pela porta e o Fulano pelo programa. No entanto, é importante frisar que um aplicativo pode utilizar mais de uma porta.
- Ilustração de uso de portas TCP
- Ao todo, é possível usar 65536 portas TCP e UDP, começando em 1. Tanto no protocolo TCP como no UDP, é comum o uso das portas de 1 a 1024, já que a aplicação destas é padronizada pela IANA (Internet Assigned Numbers Authority). De acordo com essa entidade, eis algumas das portas TCP mais utilizadas:
- :: 21 - FTP;
- :: 23 - Telnet;
- :: 25 - SMTP;
- :: 80 - HTTP;
- :: 110 - POP3;
- :: 143 - IMAP;
- :: 443 - HTTPS.

https://www.infowester.com/portastcpudp.php

# SDWAN

- Os tempos mudaram. À medida que as empresas começam a usar aplicações SaaS e IaaS (infraestrutura como serviço) em várias nuvens com maior frequência, a experiência de aplicação do usuário se torna cada vez mais insatisfatória. Isso ocorre porque as WANs que foram projetadas para uma outra época não estão prontas para absorver o aumento considerável de tráfego da WAN, que foi gerado pela adoção da nuvem. Esse tráfego gera complexidade no gerenciamento, imprevisibilidade do desempenho das aplicações e vulnerabilidade dos dados.
- Além disso, expor a empresa ao ambiente da Internet e da nuvem traz à tona os principais riscos de ameaças e problemas de conformidade. É extremamente desafiador proteger os ativos mais importantes de uma empresa, quando as aplicações são acessadas por uma força de trabalho bastante diversificada, que inclui funcionários, parceiros, terceirizados, fornecedores e convidados. A ativação da banda larga na WAN torna os requisitos de segurança ainda mais importantes, fazendo com que seja um desafio para a TI encontrar um equilíbrio entre a experiência do usuário, a segurança e a complexidade.
- A SD-WAN resolve os atuais desafios de TI. Essa nova abordagem de conectividade de rede pode reduzir os custos operacionais e melhorar a utilização dos recursos em implantações multisite. Os administradores de rede podem usar a largura de banda de maneira mais eficiente e ajudar a garantir altos níveis de desempenho para aplicações essenciais, sem sacrificar a segurança ou a privacidade dos dados.

# SDWAN

A arquitetura de WAN tradicional limitada-se à empresa, filial e ao data center. Depois que uma empresa adota aplicações em nuvem na forma de SaaS e IaaS, a arquitetura de WAN passa por uma explosão do tráfego de acesso às aplicações distribuídas em todo o mundo.
Essas alterações têm várias implicações para a TI. A produtividade do funcionário pode ficar comprometida por problemas de desempenho da aplicação de SaaS. As despesas com a WAN aumentam com o uso ineficiente de circuitos dedicados e de backup. A TI enfrenta a batalha diária e complexa de conectar diferentes tipos de usuários, com diversos tipos de dispositivo, a vários ambientes de nuvem.
Com a SD-WAN, a TI pode fornecer roteamento e proteção contra ameaças, além de economizar custos com circuitos caros e simplificar o gerenciamento das redes WAN. Os benefícios comerciais incluem:

**Melhor experiência de aplicação**

•Alta disponibilidade, com serviço previsível, de todas as principais aplicações empresariais
•Vários links ativos-ativos para todos os cenários de rede
•Tráfego de aplicações com roteamento dinâmico, que reconhece aplicações para oferecer ótimos resultados e a melhor experiência de usuário
•OpEx aprimorado, substituindo os serviços de MPLS (Multiprotocol Label Switching) por uma banda larga mais econômica e flexível (incluindo conexões VPN seguras)

**Mais segurança**

•Políticas de reconhecimento de aplicações com segmentação de ponta a ponta e controle de acesso em tempo real
•Proteção integrada contra ameaças aplicada no lugar certo
•Tráfego seguro no ambiente de Internet de banda larga e na nuvem
•Segurança distribuída para a filial e os endpoints remotos com NGFW, segurança DNS e NGAV

Conectividade de nuvem otimizada

•Fácil ampliação da WAN para várias nuvens públicas
•Desempenho otimizado em tempo real no Microsoft Office 365, Salesforce e outras aplicações importantes de SaaS
•Fluxos de trabalho otimizados para plataformas de nuvem, como serviços Web da Amazon (AWS) e Microsoft Azure

Gerenciamento simplificado

•Um painel de gerenciamento único e centralizado, oferecido na nuvem para configuração e gerenciamento de WAN, nuvem e segurança
•Provisionamento automatizado e baseado em modelo em todos os locais: filial, campus e nuvem
•Relatório detalhado de aplicações e desempenho de WAN para análise de negócios e antecipação da largura de banda necessária

14/07/2021

# Load Balance

- O Load Balance é um componente que tem como principal função manter o equilíbrio entre a carga de trabalho e o direcionamento das requisições de uma aplicação, de um site, ou o que estiver em operação no momento.
- Basicamente, o balanceamento de cargas pode ser implementado para hardware, software ou até mesmo uma combinação entre os dois. O Load Balance pode trabalhar de maneiras diferentes.

**Round-Robin**

- Nesse modelo, há uma distribuição por igual entre todos os componentes do cluster. Isso significa que todas as requisições que chegam ao balanceador de cargas são encaminhadas igualmente entre todos os players da composição do servidor. Dessa forma, ele alterna entre os componentes e as requisições.
- Quando se trabalha com um servidor Round-Robin, todos os seus componentes são masters. Ou seja, eles estão nos servidores principais. Portanto, todos recebem igualmente as requisições. Além disso, normalmente, todos os players têm exatamente a mesma configuração.
- Nesse cenário, caso ocorra alguma falha e algum desses componentes caia, o Load Balance identifica, retira da distribuição e continua a encaminhar as requisições entre os componentes ativos, que estão no ar.

**Master/slave**

- Nesse modelo, as composições master/slave enviam todas as requisições para um servidor master e somente se ocorrer algum problema com esse servidor principal — como uma queda de serviço — ele encaminhará as requisições para um servidor slave, que é um servidor intermediário.

# Link Dedicado

- Link de internet dedicado é um serviço desenvolvido para o setor corporativo, projetado para garantir uma maior estabilidade e segurança na transmissão de dados. Por meio dele, as empresas podem realizar suas atividades digitais sem precisar compartilhá-lo.
- É como se a internet toda fosse um conjunto de estradas e, ao aderir ao serviço de link dedicado, a empresa pegasse um atalho sem curvas, obstáculos e paradas.

**Qual a diferença entre link dedicado e internet dedicada?**

- Ok, agora que entendemos o que é link dedicado, talvez você esteja se perguntando: qual a diferença entre link dedicado e internet dedicada? A resposta pode ser mais simples do que você pensa: são apenas variações de nomes para o mesmo conceito.
- O que acontece é que, com o volume de propagações de informações sobre o tema, variações do termo vão se criando. Não vai ser incomum você ler por aí nomes como "IP dedicado" ou até "internet dedicado". Isso mesmo, com "o".

**Link dedicado X Internet compartilhada: quais as diferenças?**

- Internet compartilhada, banda larga ou internet convencional. Vários nomes, mesmo conceito: é aquele serviço que, provavelmente, você usa em casa. Além da velocidade e estabilidade, os dois "modos" de internet diferem no que diz respeito à manutenção: o link dedicado não precisa de tanto tempo quanto a internet compartilhada para ser reparado em casos de interrupção.

**Vantagens do link dedicado da Copel Telecom à sua empresa**

- Sua empresa é de pequeno, médio ou grande porte? Seja qual for, a Copel Telecom tem a solução em link dedicado para impulsionar suas conexões. Listamos, então, algumas vantagens do serviço da nossa internet dedicada:
- 1 – Total disponibilidade de conexão
- Com nosso serviço, sua empresa não perde prazos importantes para o dia a dia, como o envio de documentos, notas fiscais ou pedidos de compra, por exemplo.
- 2 – Atendimento diferenciado
- Temos uma equipe à disposição 24h para atender as demandas da sua empresa.
- 3 – Fibra óptica de ponta a ponta
- Se a internet dedicada já é veloz por si só, imagine quando ela é transmitida via fibra óptica.

# Web Application Firewall

- O WAF é um software desenvolvido para filtrar, monitorar e bloquear pacotes de dados que são passados para um aplicativo online. Com inspeções personalizadas, ele é capaz de proteger contra DDoS, Serviços Seguros de Gateway para Web, Inteligência de IP, aplicações entregues pela nuvem e também aplicações híbridas.
- Os ataques de cross-site scripting (XSS) e injeção de SQL, bem comuns no ambiente digital, são outros essenciais que o Web Application Firewall consegue manter sua rede protegida. Portanto, o WAF previne de possíveis invasões, visto que monitora tudo que acontece nos servidores da WEB entre um cliente e servidores.

**Como funciona o Web Application Firewall**

- Implantado através de um proxy, ele se baseia em uma rede, um host ou em uma nuvem. Uma das suas principais funções é filtrar o tráfego danoso por meio de um inspecionamento de cada pacote de dado e usando uma base de regra para análise da lógica de aplicativos da Web. Ele permite que o ambiente de TI consiga ter uma ampla visualização das ameças que travam os procedimentos das empresas no ambiente digital.
- Instalado localmente, basta que para seu funcionamento sejam reaplicadas regras e configurações nos appliances. Hospedados em host, ele é integrado no código do aplicativo. Na nuvem é implantado em uma base de assinatura e requer uma alteração de DNS para desviar o tráfego.

https://en.wikipedia.org/wiki/Web_application_firewall

# Tipos de Protocolos de Roteamento

- https://en.wikipedia.org/wiki/Routing_protocol
- https://www.guru99.com/routing-protocol-types.html
- https://www.comparitech.com/net-admin/routing-protocol-types-guide/
- https://www.youtube.com/watch?v=rA0p0ouD3aE
- https://www.youtube.com/watch?v=LYE8Y-zDQa8
- https://www.youtube.com/watch?v=RNYronaK-oI
- https://www.youtube.com/watch?v=Icd5AxDCxRE
- https://www.youtube.com/watch?v=y9Vx5I-th9Y
- https://www.youtube.com/watch?v=VJLI41ht2pQ
- https://www.youtube.com/watch?v=viB-qNUj-zI
- https://www.youtube.com/watch?v=EZc4xUtfd6Y
- https://study-ccna.com/routing-protocols/
- https://www.ibm.com/docs/en/zos-basic-skills?topic=layer-routing-tables-protocols

14/07/2021

# FIREWALL NA PRÁTICA

OVERVIEW DE CONFIGURAÇÃO E BOAS PRÁTICAS

# Configurando Firewall e suas boas práticas

1. Documentar todas as mudanças de regras de firewall
2. Instale todas as regras de acesso com direitos de acesso mínimos
3. Verifique cada mudança de firewall em relação às políticas de conformidade e solicitações de mudança
4. Remova as regras não utilizadas das bases de regras do firewall quando os serviços forem desativados
5. Realize uma revisão completa das regras de firewall pelo menos duas vezes por ano

# Configurando Firewall e suas boas práticas

- https://www.securitymetrics.com/blog/how-configure-firewall-5-steps
- https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-9.7
- https://blog.icorps.com/bid/138231/3-steps-to-a-successful-firewall-implementation
- https://www.dummies.com/programming/networking/cisco/network-firewall-implementation/
- https://about.usps.com/handbooks/as805/as805c11_028.htm
- https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-firewall.html
- https://community.jisc.ac.uk/library/advisory-services/firewall-implementation
- https://www.securityskeptic.com/2010/06/5-best-firewall-practices-and-how-to-implement-them.html

# Configurando Firewall e suas boas práticas

- https://www.securityskeptic.com/2010/06/5-best-firewall-practices-and-how-to-implement-them.html
- https://tools.cisco.com/security/center/resources/firewall_best_practices
- https://www.manageengine.com/products/firewall/firewall-best-practices.html
- https://ostec.blog/en/perimeter/deploying-firewalls-best-practices/
- https://docs.netgate.com/pfsense/en/latest/firewall/best-practices.html
- https://www.esecurityplanet.com/networks/fine-tuning-firewall-rules-best-practices/

# Hardening Firewall

- O processo de **hardening** nos firewalls envolve muito mais do que manter senhas fortes e políticas de segurança complexas. São o conjunto de pequenas ações de segurança que visem incrementar gradativamente, e em camadas, o nível geral de segurança no uso diário dos equipamentos.
- https://repositorio.uniceub.br/jspui/bitstream/235/12391/1/51307251.pdf
- https://perspectiverisk.com/top-5-tips-hardening-firewalls/
- https://www.beyondtrust.com/resources/glossary/systems-hardening
- https://wikisites.cityu.edu.hk/sites/netcomp/articles/Pages/HardeningStepsforFirewall.aspx
- https://www.sans.org/media/score/checklists/FirewallChecklist.pdf
- https://security.uconn.edu/firewall-standards/

# Hardening Firewall

- O processo de **hardening** nos firewalls envolve muito mais do que manter senhas fortes e políticas de segurança complexas. São o conjunto de pequenas ações de segurança que visem incrementar gradativamente, e em camadas, o nível geral de segurança no uso diário dos equipamentos.
- https://repositorio.uniceub.br/jspui/bitstream/235/12391/1/51307251.pdf
- https://perspectiverisk.com/top-5-tips-hardening-firewalls/
- https://www.beyondtrust.com/resources/glossary/systems-hardening
- https://wikisites.cityu.edu.hk/sites/netcomp/articles/Pages/HardeningStepsforFirewall.aspx
- https://www.sans.org/media/score/checklists/FirewallChecklist.pdf
- https://security.uconn.edu/firewall-standards/
- https://www.chmag.in/articles/techgyan/firewall-hardening-checklist/
- https://www.process.st/checklist/firewall-audit-checklist/

# Padrões para o Firewall

- https://www.luc.edu/its/aboutits/itspoliciesguidelines/network_firewall_standard.shtml
- https://www.pcisecuritystandards.org/pdfs/Small-Merchant-Firewall-Basics.pdf
- https://www.algosec.com/what-are-firewall-rules/
- https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901083
- https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final
- https://brocku.ca/policies/wp-content/uploads/sites/94/Standards-for-Firewall-Deployment-Management.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/882768/dwp-ss013-security-standard-firewall-security-v1.5.pdf
- https://www.usmd.edu/usm/adminfinance/itcc/firewallpolicynis.pdf

# Regras e Politicas de Firewall

- As **Regras** de **firewall** definem que tipo de tráfego Internet é permitido ou bloqueado. Cada perfil da **firewall** possui um conjunto de **regras** da **firewall** predefinido que não podem ser alteradas. Apenas pode adicionar novas **regras** a alguns dos perfis. Pode não conseguir adicionar as suas próprias **regras** a alguns perfis.
- https://docs.rackspace.com/support/how-to/best-practices-for-firewall-rules-configuration/
- https://www.real-sec.com/2020/01/7-firewall-best-practices-for-securing-your-network/
- https://www.liquidweb.com/kb/best-practices-for-firewall-rules/
- https://www.youtube.com/watch?v=r5yiJYpNPJc
- https://www.youtube.com/watch?v=_HF99sTLPUI
- https://www.youtube.com/watch?v=x_EKqRZrkTc
- https://totalcompliancetracking.com/firewall-rules-best-practices/
- https://www.pcidssguide.com/firewall-rule-configuration-best-practices-for-pci-compliance/
- https://www.juniper.net/documentation/en_US/junos-space18.1/topics/concept/junos-space-firewall-policy-best-practice.html
- https://help.f-secure.com/product.html?business/client-security/13.10/pt/concept_F980D184D74D4FF0A795622315481 78C-13.10-pt#:~:text=As%20Regras%20de%20firewall%20definem,pr%C3%B3prias%20regras%20a%20alguns%20perfis.
- https://www.gta.ufrj.br/grad/13_1/firewall/regras.html

# Firewall - Iptables

- O **iptables** é, a princípio, um *firewall* em nível de pacotes, mas dispõe de módulos que o permitem atuar na camada de aplicação. Ele vem instalado por padrão na maioria das distribuições Linux, incluindo o Linux Kamarada e o openSUSE. Isso significa que podemos simplesmente começar a usar o **iptables**: não precisamos instalar nada antes.
- https://e-tinet.com/linux/firewall-iptables/
- https://www.digitalocean.com/community/tutorials/how-to-list-and-delete-iptables-firewall-rules-pt
- https://linuxkamarada.com/pt/2019/11/18/proteja-se-com-o-firewall-iptables/
- https://www.guiafoca.org/guiaonline/seguranca/ch05.html
- https://docente.ifrn.edu.br/filiperaulino/disciplinas/gerencia-e-seguranca-de-redes/aulas/Firewall%20-%20IPTables%20exemplos.pdf
- https://www.drawerhost.com.br/blog/2018/01/30/10-regras-do-firewall-iptables-que-todo-sysadmin-linux-deve-conhecer/
- https://www.youtube.com/watch?v=LJlJlLgkNxg

# Firewall - Pfsense

- O pfSense é open source, licenciado sob BSD license, baseado no sistema operacional FreeBSD e adaptado para assumir o papel de um firewall e/ou roteador de redes. O nome deriva do fato que o software utiliza a tecnologia packet-filtering.
- https://4linux.com.br/o-que-e-pfsense/
- https://indicca.com.br/firewall-pfsense/
- https://www.youtube.com/watch?v=b-DSK6vSHM4
- https://www.youtube.com/watch?v=I2yF5NQcRuI
- https://e-tinet.com/linux/pfsense-vantagens/
- http://professor.prochnow.com.br/artigo/criando-regras-de-firewall-no-pfsense
- https://www.youtube.com/watch?v=YxIoRKH2ERQ

# Firewall – Fortigate

- https://fortigate.fortidemo.com/
- https://www.youtube.com/watch?v=BvPfvuuNcFw
- https://www.youtube.com/watch?v=3ELl7f4QUQI
- https://www.youtube.com/watch?v=l62_-hh39jw
- https://tndbrasil.com.br/fortinet-online-demo/
- https://www.firewall-singapore.com/fortinet-live-demo/
- https://blog.router-switch.com/2021/03/7-basic-commands-of-fortinet-fortigate-firewalls-configuration/
- https://www.youtube.com/watch?v=mC3xvZWFMtY
- https://docs.fortinet.com/document/fortigate/6.0.0/handbook/31043/basic-configuration-steps
- https://techencyclopedia.wordpress.com/2017/08/13/how-to-setup-fortigate-firewall-to-access-the-internet/

# Firewall – Fortigate

- https://fortigate.fortidemo.com/
- https://www.youtube.com/watch?v=BvPfvuuNcFw
- https://www.youtube.com/watch?v=3ELl7f4QUQI
- https://www.youtube.com/watch?v=l62_-hh39jw
- https://tndbrasil.com.br/fortinet-online-demo/
- https://www.firewall-singapore.com/fortinet-live-demo/
- https://blog.router-switch.com/2021/03/7-basic-commands-of-fortinet-fortigate-firewalls-configuration/
- https://www.youtube.com/watch?v=mC3xvZWFMtY
- https://docs.fortinet.com/document/fortigate/6.0.0/handbook/31043/basic-configuration-steps
- https://techencyclopedia.wordpress.com/2017/08/13/how-to-setup-fortigate-firewall-to-access-the-internet/

# Laboratórios

- https://www.youtube.com/watch?v=q-cxDKxwy_M
- https://www.youtube.com/watch?v=BNAD9h3dAH8
- https://www.class365.com.br/linux/lab-complexo-virtualbox/
- https://tiparaleigo.wordpress.com/2019/09/06/laboratorio-de-configuracao-de-firewall-baseado-em-zona-de-palo-alto/
- https://www.lsec.icmc.usp.br/gurgel/tutorial05.pdf
- https://forum.netgate.com/topic/82784/criar-laborat%C3%B3rio-pfsense-win-para-testes-n%C3%A3o-funciona
- http://linuxfirewall.com.br/linuxwp/sdn-criando-uma-rede-openflow-com-multiplos-pcsnetfpgas/
- https://blueteamlabs.online/
- https://cyberdefenders.org/

# Firewall and Graylog

- https://www.scip.ch/en/?labs.20180719
- https://marketplace.graylog.org/addons?tag=Firewall+Syslog
- https://www.reddit.com/r/graylog/comments/njgtz2/using_graylog_with_palo_alto_networks_firewall/
- https://www.graylog.org/post/vpn-and-firewall-log-management
- https://marketplace.graylog.org/addons?tag=iptables
- https://www.graylog.org/post/how-to-use-graylog-as-a-syslog-server
- https://marketplace.graylog.org/addons?tag=pfsense
- https://www.youtube.com/watch?v=rtfj6W5X0YA
- https://www.youtube.com/watch?v=YkeN7AFs2XQ
- https://github.com/opc40772/pfsense-graylog

# Detectando Ataques no Firewall


- https://smallbusiness.chron.com/identify-potential-malicious-attacks-firewalls-71361.html
- https://www.watchguard.com/training/fireware/82/defense2.htm
- https://www.compuquip.com/blog/firewall-threats-vulnerabilities
- https://www.manageengine.com/products/firewall/firewall-virus-report.html
- https://www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/concept/attack-detection-prevention-overview.html
- https://www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/concept/denial-of-service-attack-overview.html
- https://purplesec.us/firewall-penetration-testing/
- https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/why-a-firewall-is-the-first-line-of-defense-against-cyber-attacks/
- https://www.vmware.com/topics/glossary/content/internal-firewall
- https://www.fortinet.com/content/dam/fortinet/assets/white-papers/DDoS-Attack-Mitigation-Demystified.pdf
- https://sobrelinux.info/questions/650580/how-can-i-detect-a-ddos-attack-using-pfsense-so-i-can-tell-my-isp-who-to-block

# Configurando IDS/IPS no Pfsense

- https://www.youtube.com/watch?v=icHj0Qo8aAM
- https://www.youtube.com/watch?v=HFeCftNKBS8
- https://www.youtube.com/watch?v=8Pq_LIhOUbU
- https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html
- https://techexpert.tips/pt-br/pfsense-pt-br/instalacao-de-snort-em-pfsense/
- https://dataunique.com.br/blog/pfsense-ids-e-ips/
- https://turbofuture.com/internet/How-to-Set-Up-an-Intrusion-Detection-System-Using-Snort-on-pfSense-20

# IDS e IPS

- https://cybersecurity.att.com/blogs/security-essentials/intrusion-detection-techniques-methods-best-practices
- https://cybersecurity.att.com/resource-center/videos/ids-best-practices
- https://www.darkreading.com/vulnerabilities---threats/7-ways-to-get-the-most-from-your-ids-ips/d/d-id/1334487
- https://silo.tips/download/e-guide-sponsored-by-3
- https://ostec.blog/en/perimeter/ids-positioning-network-architecture/
- https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/

# Lab Infosec

- http://www.sis.pitt.edu/lersais/education/labs/firewall_config.php
- https://web.ecs.syr.edu/~wedu/seed/network_security.html
- http://web.csulb.edu/projects/security-ia/sidemenu/lab/experiment/
- http://webpages.eng.wayne.edu/~fy8421/16sp-csc5991/labs/lab8-instruction.pdf
- https://techcommunity.microsoft.com/t5/azure-network-security/tutorial-overview-azure-web-application-firewall-security/ba-p/2030423
- https://seedsecuritylabs.org/Labs_16.04/Networking/
- https://www.coursehero.com/file/22460986/Lab-13-Infosec-Learning-Attacking-the-Firewall-and-Stealing-Data-Over-an-Encrypted-Channel-201/
- http://osou.ac.in/eresources/DCS-05-Block-04-LabManual.pdf
- https://www.researchgate.net/publication/220094496_Laboratory_experiments_for_network_security_instruction
- https://dl.acm.org/doi/abs/10.5555/2527148.2527180

# SIEM + Firewall

- https://blog.corserva.com/why-siem-if-already-have-a-firewall
- https://www.intrinsicamerica.com/siem-vs-firewall-why-do-you-need-a-siem-when-you-already-have-a-firewall/
- https://www.diariodeti.com.br/siem-gestao-de-eventos-de-seguranca/
- https://www.newnettechnologies.com/firewalls-siem-fear-and-loathing-of-log-savers.html
- https://www.manageengine.com/products/firewall/Analyzing-Logs-for-SIEM-Whitepaper.html
- https://www.exabeam.com/siem-guide/siem-concepts/firewall-logs/
- https://www.itfacil.com.br/como-o-siem-funciona
- https://www.netsurion.com/knowledge-packs/fortinet-firewall
- https://www.forcepoint.com/cyber-edu/siem
- https://download.manageengine.com/products/firewall/Analyzing-Logs-for-SIEM-Whitepaper.pdf
- https://github.com/decay/alienvault-pfsense
- https://success.alienvault.com/s/question/0D50Z00008oGrUSSA0/pfsensesnort-and-ossim-deployment
- https://success.alienvault.com/s/question/0D50Z00008oGtYrSAK/pfsense-suricata-and-ossim
- https://diegocananea.files.wordpress.com/2014/03/tcc_diego_cananea_redes-corrigido.pdf

# WAF Lab

- https://techcommunity.microsoft.com/t5/azure-network-security/part-1-lab-setup-azure-waf-security-protection-and-detection-lab/ba-p/2030469
- https://www.youtube.com/watch?v=8G97_8id-NI
- https://www.imperva.com/products/web-application-firewall-waf/
- https://gcsec.org/introduction-to-the-waf-security-laboratory-for-web-applications/
- https://cloudacademy.com/blog/aws-waf-web-application-firewall/
- https://www.cloudflare.com/pt-br/waf/
- https://blog.cloudflare.com/new-cloudflare-waf/
- https://www.cloudflare.com/pt-br/learning/ddos/glossary/web-application-firewall-waf/

# WAF Bypass

- https://github.com/0xInfection/Awesome-WAF
- http://139.162.22.237/waf/
- https://owasp.org/www-pdf-archive/OWASP_Stammtisch_Frankfurt_WAF_Profiling_and_Evasion.pdf
- https://kali-linuxtr.net/tag/sql-injection-waf-bypass-lab
- https://attackdefense.com/challengedetailsnoauth?cid=2296
- https://f5-agility-labs-waf.readthedocs.io/en/latest/class5/module1/lab3/lab3.html
- https://lab.wallarm.com/xxe-that-can-bypass-waf-protection-98f679452ce0/
- https://owasp.org/www-pdf-archive/OWASP_Stammtisch_Frankfurt_-_Web_Application_Firewall_Bypassing_-_how_to_defeat_the_blue_team_-_2015.10.29.pdf
- https://hacken.io/researches-and-investigations/how-to-bypass-waf-hackenproof-cheat-sheet/
- https://www.youtube.com/watch?v=zhkCf8tldbk
- https://www.youtube.com/watch?v=iQqwQXHwQk0
- https://www.youtube.com/watch?v=tSf_IXfuzXk

# Referências


- https://www.uniaogeek.com.br/voce-sabe-o-que-e-o-modelo-osi/
- https://www.cisco.com/c/pt_br/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html#~benefits
- https://www.eveo.com.br/blog/load-balance/
- http://eadccna.com.br/
- https://www.softwall.com.br/blog/waf-como-funciona-para-quem-e-indicado/
- https://www.dltec.com.br/
- https://www.udemy.com/topic/firewall/
- https://www.youtube.com/watch?v=QeuVVlmY4sQ&list=PLFf4J8oI5tSPSnzgXDyDxh0QjH6gzQzWe
- https://www.youtube.com/watch?v=k-voNrQXv0A&list=PLQ7gVTPc8Kmij4-2RpiQMAQjkj3XkoIGI
- https://www.youtube.com/watch?v=igJku9tHcNo&list=PLozhsZB1ILUN7vHnCDA2NF6rMfTBs-vAs
- https://www.youtube.com/watch?v=8vnc4CtRRYA&list=PLg5bzqpFBvElqxlVFNIn4yK0hoVlmz8Vp