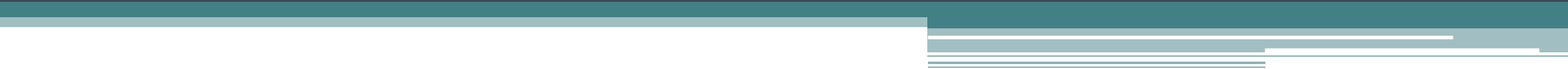


# Aula 7 – Segurança de Telecomunicações e Redes de Computadores

A decorative graphic element consisting of several horizontal lines of varying lengths and colors (teal, light blue, and white) extending across the width of the slide.

# Definição de segurança de telecomunicações e redes

- A segurança de telecomunicações e redes é um campo da segurança da informação que se concentra em proteger as informações, os sistemas e as comunicações transmitidas por meio de redes de computadores de telecomunicações. Ela abrange uma ampla gama de medidas e práticas destinadas a garantir a **confidencialidade, integridade e disponibilidade dos dados e serviços** que são transmitidos por meio de redes de comunicação, como a internet, redes locais (LANs), redes sem fio e redes móveis.



A segurança de telecomunicações e redes lida com a prevenção, detecção e resposta a ameaças cibernéticas que visam explorar vulnerabilidades em sistemas de comunicação e redes. Isso inclui a proteção contra ataques maliciosos, como invasões, infecções por malware, ataques de negação de serviço (DDoS), interceptação de dados, entre outros.



Com o aumento do compartilhamento de informações, transações online e o crescente número de dispositivos interconectados (Redes Sem Fio e Internet das Coisas), a necessidade de garantir a segurança dessas comunicações se tornou crucial para proteger a privacidade, os dados confidenciais e a infraestrutura crítica.



A segurança de telecomunicações e redes é fundamental para garantir que as informações sejam transmitidas com segurança, que os sistemas de comunicação estejam protegidos contra ameaças e que as redes permaneçam resilientes diante de ataques potenciais.

# Importância da segurança cibernética na era da conectividade

- Proteção dos Dados Pessoais e Privacidade
- Prevenção de Ataques Cibernéticos
- Continuidade dos Negócios e Serviços Críticos
- Proteção de Infraestruturas Críticas
- Confiança no Digital
- Evolução das Ameaças
- Cumprimento de Regulamentações
- Inovação e Desenvolvimento Tecnológico

# Ameaças e Ataques em Redes de Computadores

- **Malware:**

- **Vírus:** Programas maliciosos que se anexam a arquivos legítimos e se espalham quando esses arquivos são abertos.
- **Worms:** Malwares que se propagam automaticamente pela rede, explorando vulnerabilidades em sistemas.
- **Trojans:** Malwares disfarçados de programas legítimos que realizam ações maliciosas quando executados.

- **Ataques de Phishing:**
  - E-mails ou mensagens enganosas que tentam convencer os destinatários a fornecer informações confidenciais, como senhas ou dados bancários.
- **Ataques de Engenharia Social:**
  - Manipulação psicológica de pessoas para obter informações confidenciais ou acesso a sistemas.
- **Ataques de Negociação de Credenciais:**
  - Tentativas de obter ou usar indevidamente credenciais de autenticação, como senhas, para ganhar acesso não autorizado a sistemas.

- **Ataques de Força Bruta:**
  - Tentativas repetidas e automatizadas de adivinhar senhas ou chaves de criptografia até que a combinação correta seja encontrada.
- **Ataques de Negação de Serviço (DDoS):**
  - Sobrecarregam um sistema alvo com tráfego de rede malicioso para torná-lo inacessível a usuários legítimos.
- **Injeção de SQL:**
  - Exploração de vulnerabilidades em aplicativos da web para injetar comandos SQL maliciosos e obter acesso a bancos de dados.

- **Exploração de Vulnerabilidades:**
  - Aproveitamento de vulnerabilidades de softwares não corrigidas ou mal configuradas para ganhar acesso a sistemas.
- **Ransomware:**
  - Criptografa dados em sistemas e exige resgate em troca da chave de descriptografia.
- **Ataques de Man-in-the-Middle (MitM):**
  - Interceptam comunicações entre duas partes, muitas vezes para espionagem ou manipulação de dados.



- **Ataques de Spoofing:**
  - Falsificação de endereços IP ou outros identificadores para mascarar a origem de um ataque.
- **Botnets:**
  - Redes de computadores comprometidos controlados por um atacante para realizar tarefas maliciosas, como ataques DDoS.
- **Ataques de Zero-Day:**
  - Exploração de vulnerabilidades de software antes que os desenvolvedores tenham a chance de lançar correções.

- **Ataques a Dispositivos IoT (Internet das Coisas):**
  - Aproveitamento de vulnerabilidades em dispositivos IoT mal protegidos para acessar redes maiores.
- **Ataques a Redes sem Fio (Wi-Fi):**
  - Tentativas de acessar redes Wi-Fi sem autorização, que podem resultar em espionagem ou invasão de dispositivos conectados.
- **Ataques de Injeção de Código:**
  - Inserção de código malicioso em aplicativos ou sites para executar ações não autorizadas.

- **Ataques de Engenharia Reversa:**
  - Tentativas de descompilar ou analisar o código de um programa para encontrar vulnerabilidades.
- Para proteger eficazmente as redes de computadores contra essas ameaças, é crucial adotar uma abordagem em camadas, que inclua medidas de segurança cibernética, como firewalls, antivírus, atualizações regulares de software, monitoramento de tráfego de rede e treinamento de conscientização para os usuários.
- A constante vigilância e adaptação às novas ameaças cibernéticas também são fundamentais para manter a segurança da rede.

Educação do usuário,  
Atualizações e Patchs

Segurança Wireless

Antivírus

Backup de Dados

## Defesa em camadas

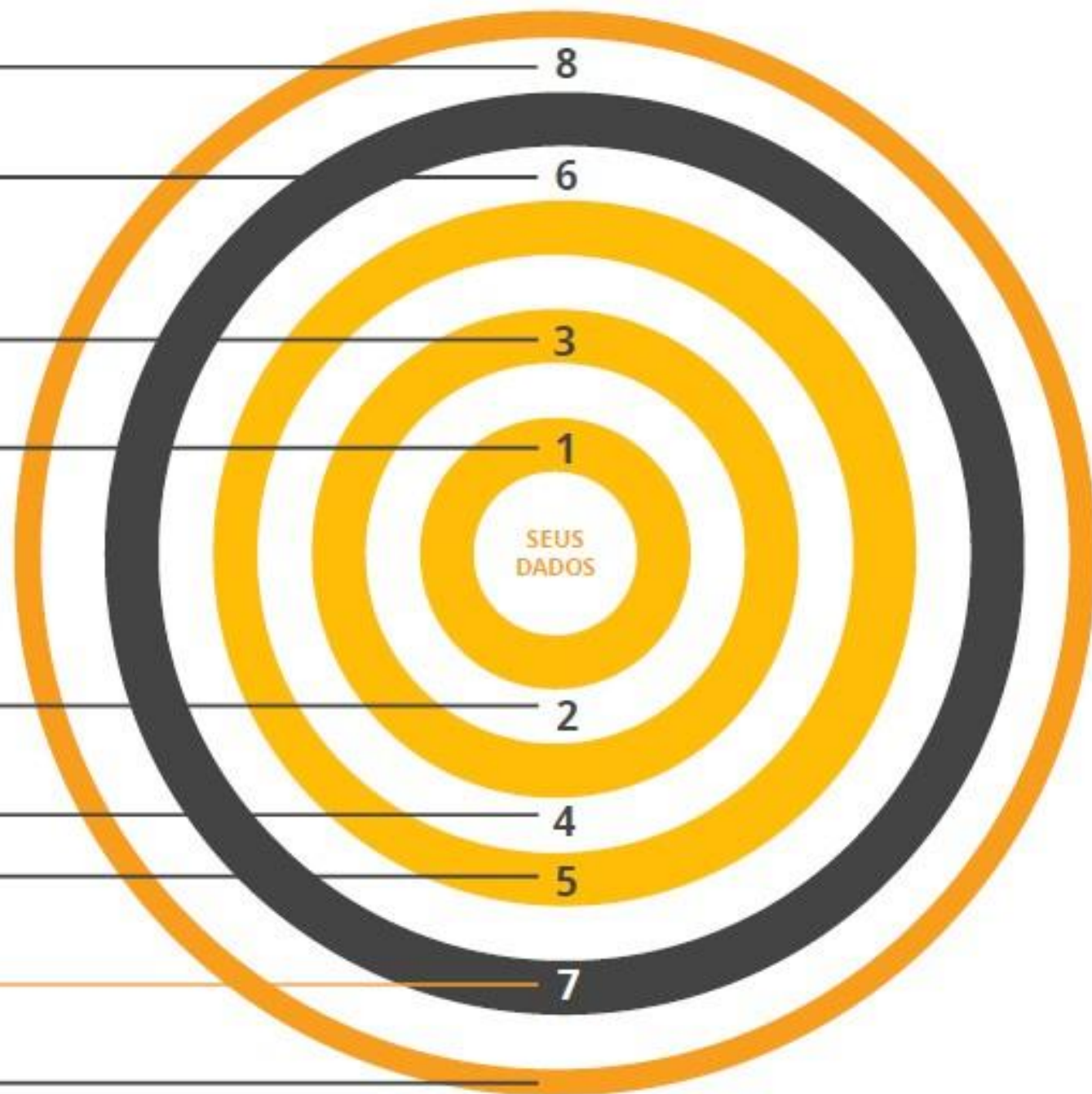
Recuperação de desastres

Firewall

Segurança e filtragem de e-mail

Segurança e filtragem na Web

Política de Segurança



# Criptografia e segurança da informação

- **Criptografia e Decodificação:**

- A criptografia é o processo de transformar dados legíveis em um formato ilegível, enquanto a decodificação é o processo de reverter essa transformação para recuperar os dados originais.

- **Chaves:**

- As chaves são peças essenciais da criptografia. Uma chave é um valor único que é usado para criptografar ou decodificar dados. Existem dois tipos principais de criptografia com base em chaves.



**Criptografia Simétrica:** Usa a **mesma chave** para criptografar e decodificar dados. Exemplos incluem AES (Advanced Encryption Standard) e DES (Data Encryption Standard).



**Criptografia Assimétrica:** Usa um **par de chaves**, uma pública e outra privada, onde a chave pública é usada para criptografar e a chave privada é usada para decodificar. Exemplos incluem RSA e ECC (Elliptic Curve Cryptography).

- **Algoritmos de Criptografia:**

- São conjuntos de regras matemáticas que determinam como a criptografia e a decodificação são realizadas. Alguns algoritmos populares incluem AES, RSA, e SHA (Secure Hash Algorithm).

- **Autenticação e Integridade:**

- A criptografia não apenas oculta o conteúdo dos dados, mas também pode ser usada para verificar a autenticidade dos dados (garantindo que não tenham sido alterados) e a identidade do remetente.

- **Uso em Comunicações Seguras:**

- A criptografia é amplamente utilizada para proteger a comunicação na Internet, como em transações bancárias online, e-mails e navegação segura (SSL/TLS), VPNs (Virtual Private Networks) e mensagens criptografadas (como o WhatsApp).

- **Criptografia de Armazenamento:**

- Além de proteger comunicações, a criptografia também é usada para proteger dados armazenados em dispositivos, como discos rígidos, smartphones e pendrives. Isso evita que pessoas não autorizadas acessem os dados em caso de perda ou roubo.



- **Algoritmos e Tamanho de Chave:**

- A segurança da criptografia depende do algoritmo utilizado e do tamanho da chave. Algoritmos mais avançados e chaves mais longas oferecem maior segurança, mas também podem ser mais computacionalmente intensivos.

- **Quebra de Criptografia:**

- A quebra de criptografia é a tentativa de descriptografar dados sem a chave adequada. Isso pode ser feito por força bruta (tentando todas as combinações possíveis) ou por meio de ataques mais sofisticados, como ataques de criptoanálise.

- **Importância da Gestão de Chaves:**

- A segurança da criptografia depende da gestão adequada das chaves. Isso inclui a geração segura de chaves, a distribuição segura das chaves para partes autorizadas e a revogação de chaves comprometidas.

# Protocolos de Segurança

- Protocolos de segurança como **SSL/TLS** e **IPSec** são fundamentais para proteger a confidencialidade e a integridade dos dados transmitidos pela Internet e em redes privadas. Vamos explorar esses dois protocolos em detalhes:
- **SSL/TLS (Secure Sockets Layer/Transport Layer Security):**
  - O SSL (Secure Sockets Layer) e seu sucessor, o TLS (Transport Layer Security), são protocolos de criptografia e segurança que garantem a privacidade e a integridade das comunicações na Internet. Eles são amplamente utilizados em navegadores da web, aplicativos móveis e muitos outros serviços online.

- **Aqui estão os principais pontos relacionados ao SSL/TLS:**
  - **Criptografia de Comunicações:** O SSL/TLS protege os dados transmitidos entre um cliente (por exemplo, um navegador da web) e um servidor (por exemplo, um site) por meio da criptografia. Ele garante que terceiros não possam interceptar ou entender as informações transmitidas.
  - **Certificados Digitais:** O SSL/TLS usa certificados digitais para autenticar os servidores e, às vezes, os clientes. Isso assegura que você está se comunicando com o site ou serviço real, não com um impostor.
  - **Protocolos e Versões:** TLS é a versão mais recente e segura do protocolo, com várias versões (TLS 1.0, 1.1, 1.2, 1.3) lançadas ao longo do tempo. O uso de versões mais antigas, como SSL 2.0 e SSL 3.0, é desencorajado devido a vulnerabilidades conhecidas.

- **Handshake TLS:** Quando um cliente e um servidor iniciam uma comunicação segura, eles realizam um processo chamado handshake TLS para estabelecer uma sessão segura. Isso inclui negociação de parâmetros de criptografia e autenticação mútua.
- **Compatibilidade:** O suporte ao TLS é amplamente adotado, e os sites que desejam manter a segurança devem habilitar pelo menos o TLS 1.2 ou posterior. Isso também é importante para atender aos requisitos de conformidade, como o **PCI DSS** para transações financeiras online.

- **IPSec (Internet Protocol Security):**

- O IPSec é um conjunto de protocolos usado para proteger o tráfego de rede em redes privadas ou virtuais. Diferentemente do SSL/TLS, que opera no nível de aplicativo, o IPSec opera no nível de rede e é frequentemente usado em conexões VPN (Virtual Private Network). Aqui estão os principais aspectos relacionados ao IPSec:

- **Túneis VPN:** O IPSec é comumente usado para criar túneis VPN seguros que permitem que o tráfego de rede seja criptografado e autenticado enquanto passa por redes não confiáveis, como a Internet pública.

- **Modos de Funcionamento:** O IPSec opera em dois modos principais: modo de transporte e modo de túnel. O modo de transporte protege o tráfego entre dois hosts, enquanto o modo de túnel protege o tráfego entre redes inteiras.
- **Protocolos IPSec:** O IPSec utiliza uma combinação de protocolos para fornecer segurança, incluindo o ESP (Encapsulating Security Payload) para criptografia e autenticação, e o protocolo AH (Authentication Header) para autenticação de pacotes.
- **Chaves e Certificados:** O IPSec requer a configuração de chaves de criptografia e autenticação para garantir que somente dispositivos autorizados possam estabelecer túneis VPN e acessar recursos de rede protegidos.

- **Suporte em Roteadores e Firewalls:** Muitos dispositivos de rede, como roteadores e firewalls, oferecem suporte nativo ao IPSec, facilitando sua implementação em infraestruturas de rede.
- Tanto o SSL/TLS quanto o IPSec desempenham papéis importantes na segurança de dados em trânsito. A escolha entre eles depende do cenário específico de uso e dos requisitos de segurança.
  - O **SSL/TLS** é mais comumente usado para proteger comunicações entre navegadores e servidores web
  - O **IPSec** é ideal para estabelecer conexões seguras entre redes ou para criar túneis VPN para acesso remoto seguro.
- Ambos são ferramentas valiosas para garantir a privacidade e a integridade dos dados em ambientes de rede.



# VPN – Virtual Private Network

- **Sigla VPN: Rede Privada Virtual**
- **Definição:** Transporte de dados através de redes públicas com confidencialidade. São túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos.
- Segurança é o ponto mais importante de uma VPN: prevenir a interceptação ou corrupção dos dados quando transmitidos através da Internet (meio inseguro).
- Conexões de corporações (Extranets) através da internet, conexões criptografadas.

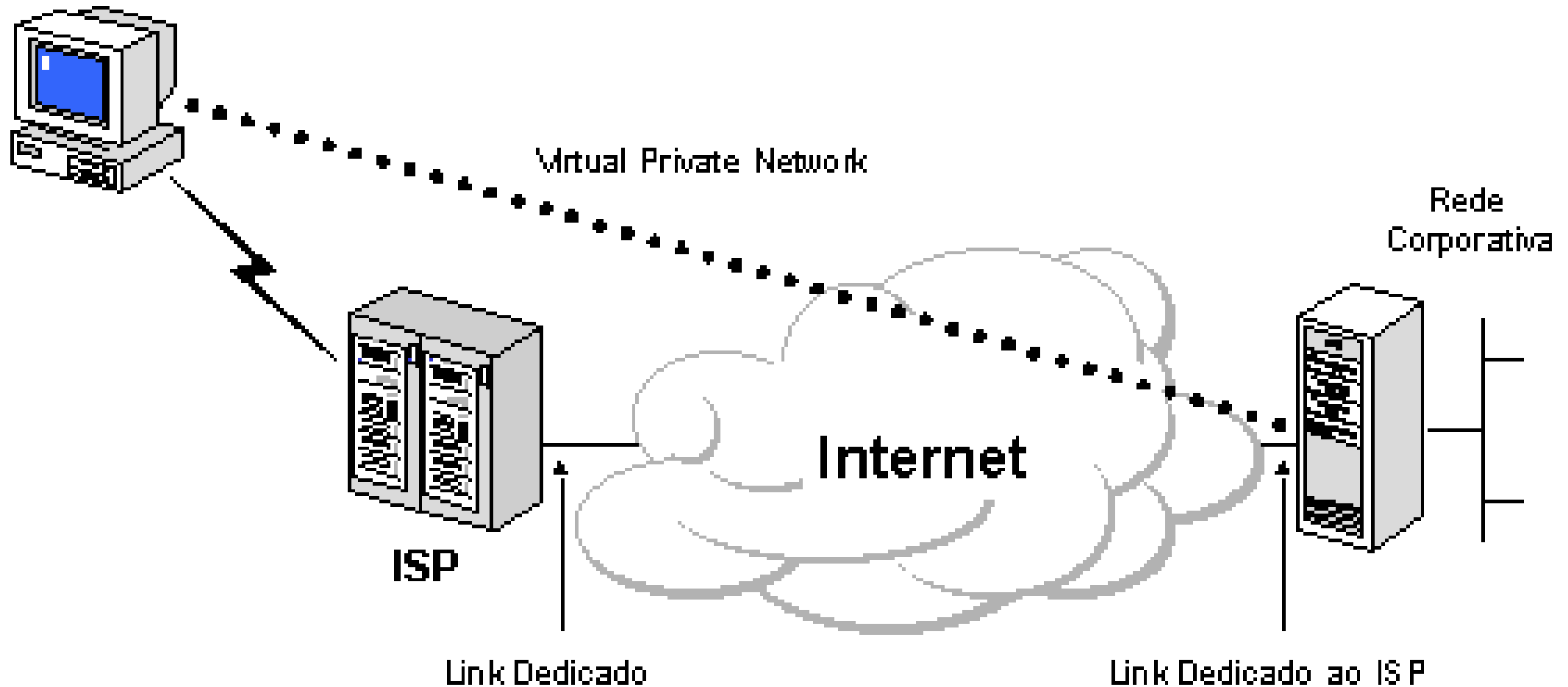
# Aplicações para as VPNs

- Três aplicações são ditas mais importantes para as VPNs:
  - Acesso remoto via Internet
  - Conexão de LANs via Internet
  - Conexão de computadores numa Intranet

# Acesso Remoto via Internet

- O acesso remoto a redes corporativas através da Internet pode ser viabilizado com a VPN através da conexão a algum provedor de acesso (Internet Service Provider - ISP). A estação remota se conecta com o provedor de acesso, conectando-se à Internet e o software de VPN cria uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet.

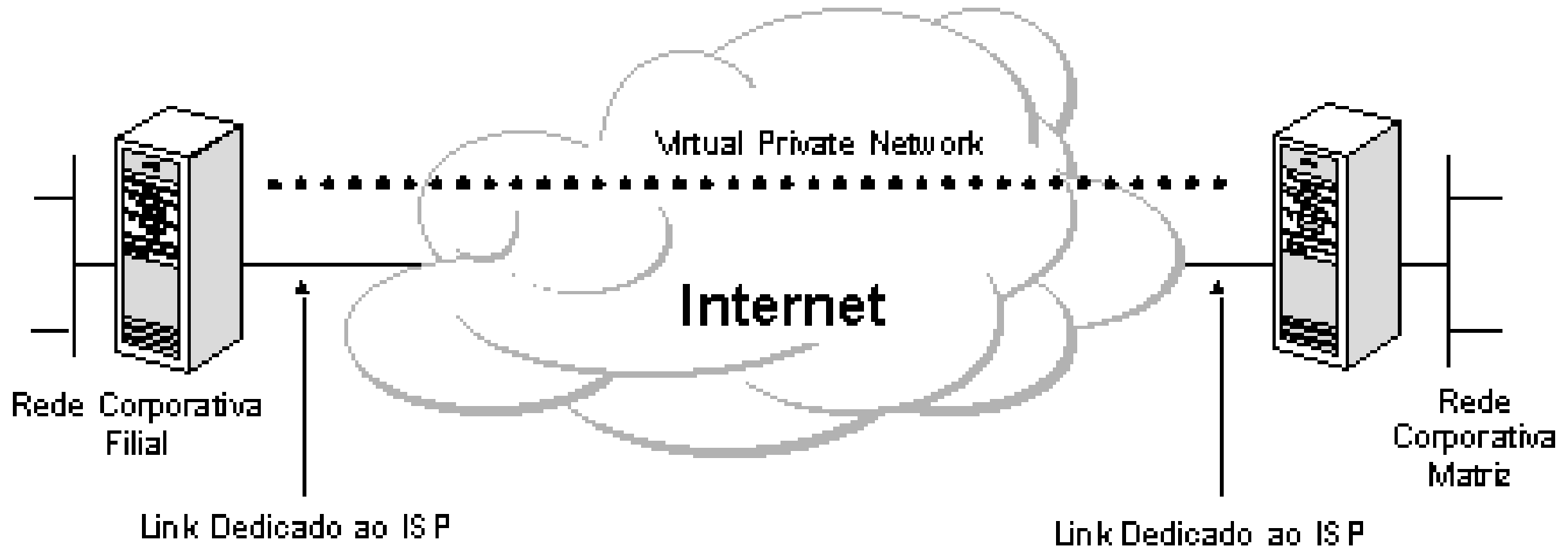
# Acesso Remoto via Internet



# Conexão de LANs via Internet

- Uma solução que substitui as conexões entre LANs através de circuitos dedicados de longa distância é a utilização de circuitos dedicados locais interligando-as à Internet. O software de VPN assegura esta interconexão formando a WAN corporativa. A depender das aplicações também, pode-se optar pela utilização de circuitos discados em uma das pontas.

# Conexão de LANs via Internet



# Conexão de Computadores numa Intranet



As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados através da inserção de um servidor VPN entre elas.

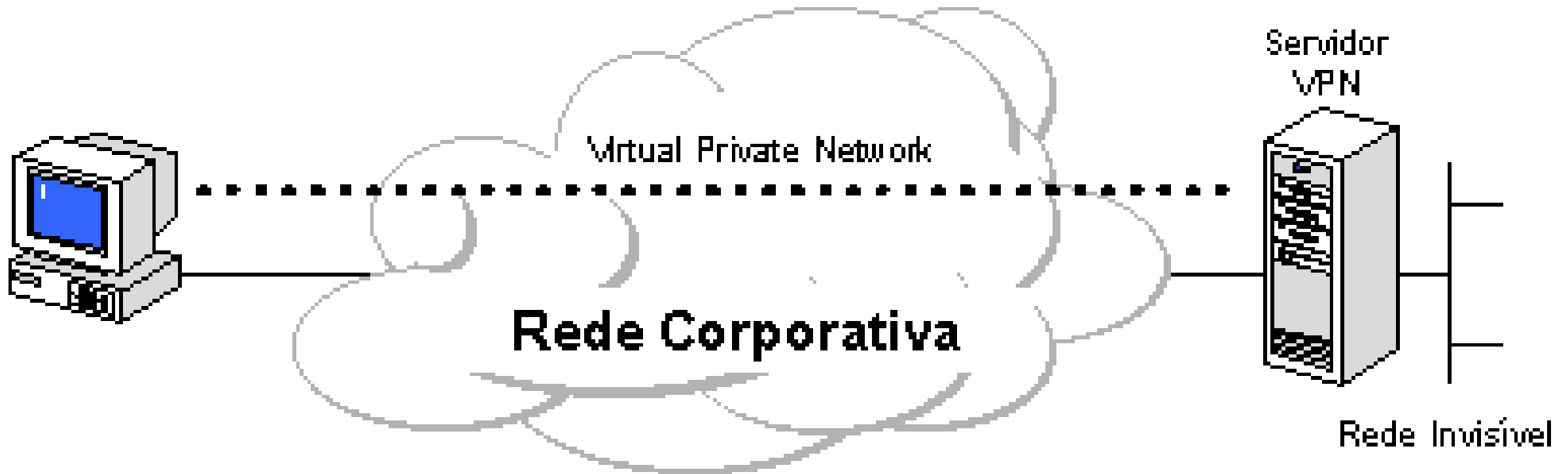


Com o uso da VPN o Administrador da Rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede restritos.



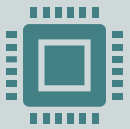
Adicionalmente, toda comunicação ao longo da VPN pode ser criptografada assegurando a "confidencialidade" das informações.

# Conexão de Computadores numa Intranet





# Características básicas



É bastante desejável que sejam implementadas facilidades de controle de acesso a informações restritas.



A VPN deve dispor de recursos para permitir o acesso de clientes remotos autorizados aos recursos restritos da LAN.



Ela deve também assegurar privacidade e integridade de dados ao atravessar a Internet bem como a própria rede corporativa.

# Características básicas



Autenticação de Usuários



Gerenciamento de Endereço



Criptografia de Dados



Gerenciamento de Chaves



Suporte a Múltiplos Protocolos

# Tunelamento



O tunelamento em VPNs é como enviar uma carta dentro de outra carta, para que ninguém possa ler o que está dentro da carta interna, exceto o destinatário.

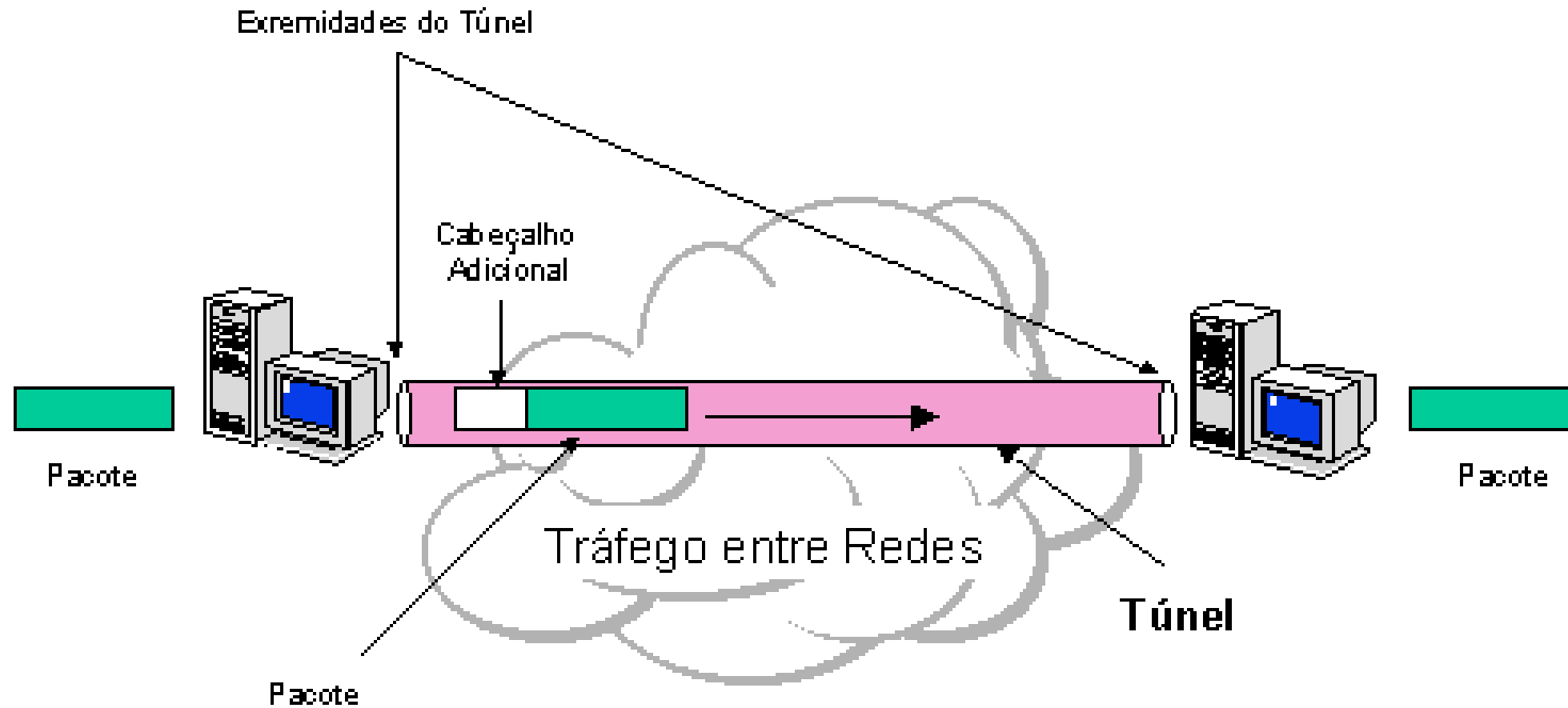


Simplificando, é como colocar uma mensagem secreta em uma caixa e, em seguida, colocar essa caixa dentro de outra caixa. Assim, mesmo se alguém pegar a caixa externa, eles não poderão ver o que está dentro da caixa interna, a menos que tenham a chave certa para abri-la.



Isso é exatamente o que o tunelamento faz em uma VPN: protege seus dados, criptografando-os e enviando-os de forma segura através de uma rede pública, como a internet, para que somente o destinatário final possa lê-los.

# Tunelamento



# Protocolos de Tunelamento

**Tunelamento em Nível 2 - Enlace - (PPP sobre IP). Exemplos:**

- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- L2F (Layer 2 Forwarding)

**Tunelamento em Nível 3 - Rede - (IP sobre IP). Exemplo:**

- O IP Security Tunnel Mode (IPSec) da IETF

# Tipos de Túneis

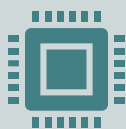


**Túnel Voluntário** - um cliente emite uma solicitação VPN para configurar e criar um túnel voluntário. Neste caso, o computador do usuário funciona como uma das extremidades do túnel e, também, como cliente do túnel.



**Túnel Compulsório** - um servidor de acesso VPN configura e cria um túnel compulsório. Neste caso, o computador do cliente não funciona como extremidade do túnel. Outro dispositivo, o servidor de acesso remoto, localizado entre o computador do usuário e o servidor do túnel, funciona como uma das extremidades e atua como o cliente do túnel.

# Túnel GRE



O **GRE – Generic Routing Encapsulation** é um protocolo de tunelamento sugerido pela Cisco em 1994 que permite o encapsulamento de uma variedade de outros protocolos.

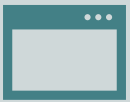


No entanto ele só foi “padronizado” em 2000, inclusive com a participação de outros fabricantes. Com ele é possível criar um link ponto a ponto virtual entre roteadores Cisco.



A grande vantagem do tunelamento GRE é permitir o tráfego de protocolos em cenários onde normalmente não seria possível. Justamente por esta propriedade o GRE é muito utilizado em conjunto com protocolos de roteamento.

# VPN SSL/TSL



Uma VPN SSL/TSL funciona com quase todos os navegadores da Web padrão.



Ao contrário das VPNs Internet Protocol Security (IPSec), a VPN SSL/TSL não precisa de software especializado no computador do usuário final o que aumenta bastante a flexibilidade desse tipo de VPN.



Os usuários móveis podem também se conectar à rede através da VPN SSL/TSL , proporcionando maior segurança, a administração do sistema é menos complexo.



- O principal benefício de uma VPN SSL é que ele oferece uma maneira segura e flexível para os indivíduos , como colaboradores remotos , viajantes, parceiros de negócios e prestadores de serviços podem se conectar a partir de qualquer computador com um navegador e uma conexão à Internet para uma rede interna. Isto permite um trabalho mais eficiente e produtivo.

# Diferenças



Existem tecnologias diferentes de VPN com forças diferentes de criptografia.



Por exemplo, o PPTP (Point-to-Point Tunneling Protocol) é rápido, mas muito menos seguro do que outros protocolos como o IPSec ou o OpenVPN, que usa SSL/TLS.



Além disso, o tipo de algoritmo de criptografia e o tamanho da chave usados também são importantes nas VPNs baseadas em SSL/TLS.



Vale notar que quanto mais forte a criptografia, maior será o impacto na velocidade de conexão

# Segurança em redes sem fio (Wi-Fi)

- **Vulnerabilidades em Redes Wi-Fi:**

- **Ataques de Quebra de Senha:** Os ataques de quebra de senha são uma das ameaças mais comuns em redes Wi-Fi. Os invasores tentam adivinhar ou quebrar a senha da rede usando força bruta, dicionários de senhas ou técnicas avançadas de craqueamento. O uso de senhas fracas torna as redes mais suscetíveis a esse tipo de ataque.
- **Ataques de Desautenticação (Deauthentication Attacks):** Os ataques de desautenticação visam desconectar dispositivos legítimos de uma rede Wi-Fi, forçando-os a se reconectar e possivelmente revelar informações confidenciais durante o processo de autenticação.

- **Roubo de Identidade (Identity Theft):** Se a autenticação em uma rede sem fio não for suficientemente segura, os invasores podem falsificar identidades e se passar por dispositivos legítimos para obter acesso à rede.
- **Roubo de Tráfego (Traffic Snooping):** Se a comunicação na rede sem fio não for criptografada adequadamente, os invasores podem interceptar e bisbilhotar o tráfego, expondo informações confidenciais.

# Métodos de Segurança em Redes Sem Fio

- **WPA (Wi-Fi Protected Access):** é um conjunto de protocolos de segurança desenvolvido para melhorar a segurança das redes sem fio em comparação com seu antecessor, o **WEP (Wired Equivalent Privacy)**.
  - O WEP era notoriamente vulnerável a ataques, o que levou ao desenvolvimento do WPA como uma alternativa mais robusta. Posteriormente, o WPA foi substituído pelo WPA2 e, mais recentemente, pelo WPA3.

- **WPA melhorias em relação ao WEP:**

- O WPA foi desenvolvido em 2003 para corrigir as vulnerabilidades de segurança inerentes ao WEP, que era suscetível a ataques de quebra de chave e fácil de comprometer.
- Uma das principais melhorias do WPA foi a introdução do **TKIP (Temporal Key Integrity Protocol)**, que fornecia chaves dinâmicas para cada pacote de dados, dificultando a decifração do tráfego por parte de invasores.

- **Autenticação por PSK e EAP:**

- O WPA suporta dois métodos de autenticação principais: **PSK (Pre-Shared Key)** e **EAP (Extensible Authentication Protocol)**.
- **PSK** envolve a configuração de uma senha compartilhada (também conhecida como chave de pré-compartilhamento) entre os dispositivos e o ponto de acesso. Essa senha é usada para autenticação e geração de chaves de criptografia.
- **EAP** é uma autenticação mais segura, geralmente usada em ambientes empresariais, que envolve a autenticação de dispositivos em um servidor de autenticação usando certificados digitais.

- **WPA2 e WPA3:**

- O **WPA2**, lançado em 2004, é a evolução do WPA e oferece maior segurança. Ele usa **criptografia AES** (Advanced Encryption Standard) em vez do TKIP, tornando as redes WPA2 mais seguras.
- O **WPA3**, lançado em 2018, introduz melhorias significativas na segurança, incluindo **autenticação individualizada**, que dificulta a adivinhação de senhas, e proteção contra ataques de força bruta.
- O WPA e suas variantes (WPA2 e WPA3) são amplamente usados em redes domésticas, empresariais e públicas para proteger a confidencialidade e a integridade das comunicações sem fio.



- **Migração para WPA2/WPA3:**

- Devido às vulnerabilidades do WEP e às melhorias de segurança oferecidas pelo WPA2 e WPA3, é altamente recomendável que as redes sem fio migrem para esses protocolos mais recentes para garantir a proteção adequada.

- **Vulnerabilidades Anteriores:**

- O WPA e o WPA2 tiveram suas próprias vulnerabilidades ao longo do tempo, como o **ataque WPS (Wi-Fi Protected Setup)** e as **vulnerabilidades KRACK (Key Reinstallation Attacks)**. No entanto, essas vulnerabilidades foram abordadas por meio de atualizações e patches de segurança.

- **Outros Métodos de Segurança em Redes Sem Fio:**

- **Filtragem de Endereços MAC (MAC Address Filtering):** Essa técnica permite que o administrador da rede especifique quais dispositivos podem se conectar à rede com base nos endereços MAC dos dispositivos. No entanto, essa abordagem pode ser contornada por invasores que clonam endereços MAC.
- **VPN (Virtual Private Network):** O uso de uma VPN em uma rede Wi-Fi pode adicionar uma camada adicional de segurança, criptografando todo o tráfego entre o dispositivo e um servidor VPN remoto, protegendo-o contra bisbilhotagem e interceptação de tráfego.

- **Atualizações de Firmware e Patching:** Manter os dispositivos de rede, como roteadores e pontos de acesso, atualizados com as últimas correções de segurança é essencial para proteger a rede contra vulnerabilidades conhecidas.
- **Autenticação de Dois Fatores (2FA):** O uso de autenticação de dois fatores em dispositivos e contas de rede adiciona uma camada adicional de segurança, exigindo uma segunda forma de autenticação além das senhas.

# Desafios de Segurança em Redes Móveis

- A segurança em redes móveis é uma preocupação crítica, uma vez que os dispositivos móveis estão se tornando o principal meio de comunicação e acesso à internet para muitas pessoas. Vamos explorar os desafios de segurança em redes móveis, a proteção de dados em redes 4G e 5G, e as ameaças específicas para dispositivos móveis.

# Desafios de Segurança em Redes Móveis



**Conectividade Pública:** As redes móveis frequentemente operam em ambientes públicos, onde a segurança não pode ser totalmente controlada. Isso torna os dispositivos móveis vulneráveis a ataques, como ataques de interceptação de tráfego em redes Wi-Fi públicas.



**Roubo ou Perda de Dispositivos:** A perda ou o roubo de dispositivos móveis é uma ameaça significativa. Se um dispositivo for comprometido, os dados armazenados nele podem ser acessados e explorados por invasores.



**Malware e Aplicativos Maliciosos:** A distribuição de malware e aplicativos maliciosos é uma preocupação constante em dispositivos móveis. Aplicativos não confiáveis podem roubar informações pessoais, infectar dispositivos com ransomware ou spyware e explorar vulnerabilidades.



**SMS Phishing (Smishing):** Smishing é uma forma de phishing que ocorre por meio de mensagens SMS. Os atacantes enviam mensagens falsas solicitando informações confidenciais ou induzindo os usuários a clicar em links maliciosos.

- **Ataques de Engenharia Social:** Os ataques de engenharia social visam enganar os usuários para que revelem informações pessoais ou instalem malware. Isso pode ocorrer por meio de chamadas telefônicas falsas, mensagens de texto ou e-mails enganosos.

# Proteção de Dados em Redes 4G e 5G



**Criptografia de Dados:** As redes 4G e 5G usam criptografia para proteger a confidencialidade dos dados em trânsito. O 4G utiliza criptografia AES (Advanced Encryption Standard), enquanto o 5G aprimora ainda mais a segurança, incluindo a autenticação individualizada dos dispositivos.



**Proteção de Identidade:** O 5G introduz a autenticação individualizada, que torna mais difícil para os invasores falsificarem a identidade de dispositivos. Cada dispositivo recebe uma identidade única, tornando a rede mais segura.



**Rede de Acesso Fixo Sem Fio (FWA):** O 5G também é usado para fornecer conectividade de banda larga em residências e empresas por meio de redes FWA. Essas redes usam protocolos seguros para proteger os dados em trânsito.



# Ameaças Específicas para Dispositivos Móveis



**Aplicativos Maliciosos:** Os dispositivos móveis são vulneráveis a aplicativos maliciosos que podem roubar informações pessoais, controlar o dispositivo ou espionar o usuário. É fundamental apenas baixar aplicativos de fontes confiáveis.



**Phishing Móvel:** Os ataques de phishing móvel podem ocorrer por meio de mensagens SMS, aplicativos falsos ou sites móveis. Os usuários devem ser cautelosos ao clicar em links ou fornecer informações pessoais por meio de dispositivos móveis.

# Ameaças Específicas para Dispositivos Móveis

## **Jailbreaking e Rooting:**

Jailbreaking (iOS) e rooting (Android) são processos que removem as restrições de segurança impostas pelos fabricantes. Isso pode abrir o dispositivo para vulnerabilidades e torná-lo mais suscetível a malware.

## **Redes Wi-Fi não Seguras:**

Conectar-se a redes Wi-Fi não seguras em locais públicos pode expor os dispositivos móveis a ataques de interceptação de tráfego e outros riscos.

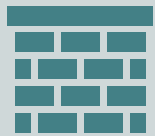


Para garantir a segurança em redes móveis, os usuários devem adotar práticas de segurança, como manter sistemas operacionais e aplicativos atualizados, usar senhas fortes, evitar redes Wi-Fi públicas não seguras e serem cuidadosos em relação a mensagens e aplicativos suspeitos.

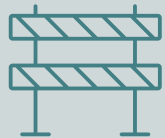


As organizações também devem implementar políticas de segurança móvel e fornecer treinamento de conscientização para os funcionários.

# Sistemas de Proteção em Redes de Computadores (Firewall, IDS, IPS)



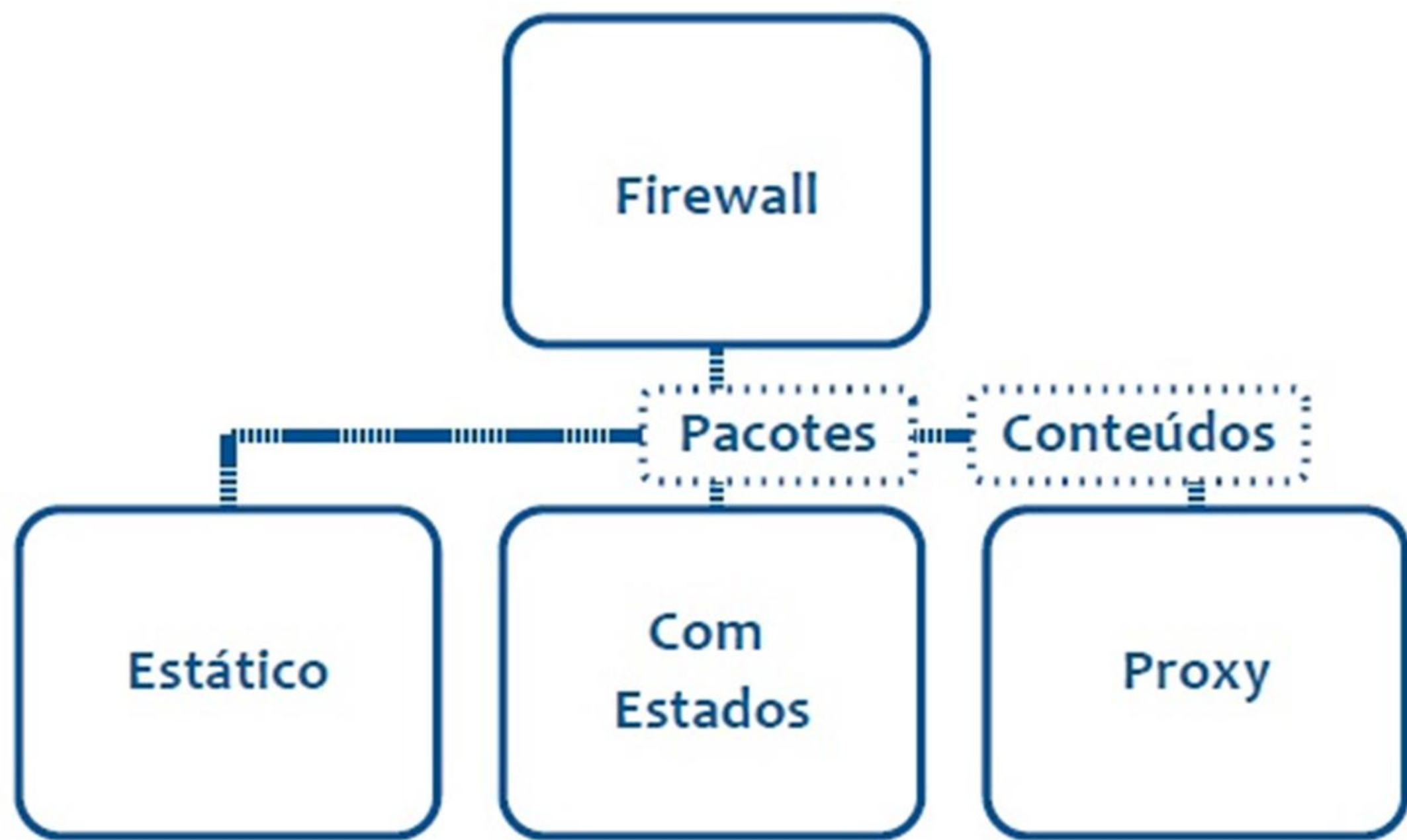
Um sistema de Firewall pode ser definido como um dispositivo que combina hardware e software para segmentar e controlar o acesso entre redes de computadores distintas.



Os sistemas de firewall são a primeira barreira contra os possíveis atacantes de um sistema computacional ou redes de computadores, devido a seu histórico de utilização e eficácia no cumprimento de sua função.

# O que é um Appliance?

- Um Appliance é uma combinação de hardware e software, ou seja, você adquire tudo junto com um objetivo específico, dentre as principais vantagens podemos citar:
  - Ter um sistema operacional totalmente customizado para o hardware e o software.
  - Ter uma função específica não permitindo com que seja agregadas funções e sistemas extras.
  - Ter uma estabilidade maior, uma vez que tudo foi customizado e a empresa sabe qual o hardware e sistema operacional.
  - Basicamente podemos ter qualquer serviço em um appliance, principalmente recursos de segurança como alguns que veremos a seguir.



# Firewall Filtro de Pacotes



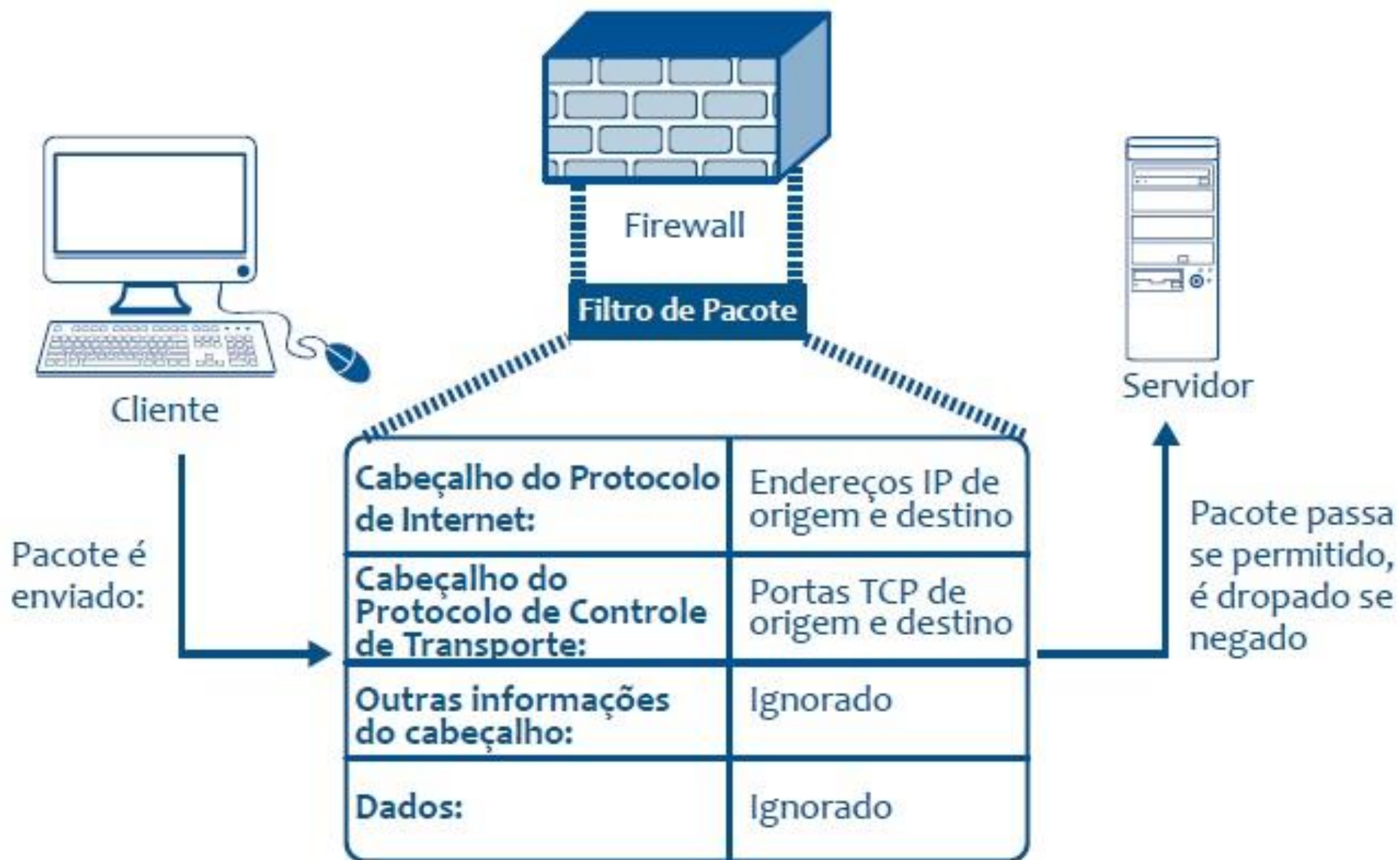
Conhecidos também por **static packet filtering**, devido à utilização de regras estáticas para filtragem de pacotes, são o tipo de firewall mais simples existente, sendo fácil, barato e flexível de serem implementados.



A análise é feita baseada nas camadas de rede e de transporte da pilha TCP/IP.



Normalmente esse tipo de firewall possui um maior desempenho em relação aos outros tipos existentes, justamente pela análise simples, fácil e rápida, fato que contribui para que esse tipo de firewall fossem incorporados a alguns roteadores.





# Firewall Filtro de Pacotes

- As regras dos filtros são baseadas em:
  - Endereço IP de origem;
  - Endereço IP de destino;
  - Protocolos TCP, UDP, ICMP;
  - Portas TCP ou UDP origem;
  - Portas TCP ou UDP destino;
  - Tipo de mensagens ICMP.

## Vantagens:

- Simples e flexível;
- Baixo Custo;
- Desempenho melhor se comparado a outros tipos de firewall;
- É bom para o gerenciamento de tráfego;
- É transparente ao usuário;
- Regras utilizadas são simples de serem criadas.

## Desvantagens:

- Muito vulnerável aos ataques que exploram as deficiências do protocolo TCP/IP;
- Não possui autenticação de usuários;
- Impossibilidade de bloqueio de ataques que exploram serviços das camadas superiores;
- Permite conexão direta entre hosts internos e externos;
- É difícil de gerenciar em ambientes complexo;
- Dificuldade de filtrar serviços que utilizam portas dinâmicas.

# Firewall Filtro de Pacotes Baseados em Estados



**Stateful Packet Filter.** As conexões são monitoradas o tempo todo, o que significa que os pacotes só podem passar pelo firewall se fizerem parte de uma sessão registrada na tabela de estados.

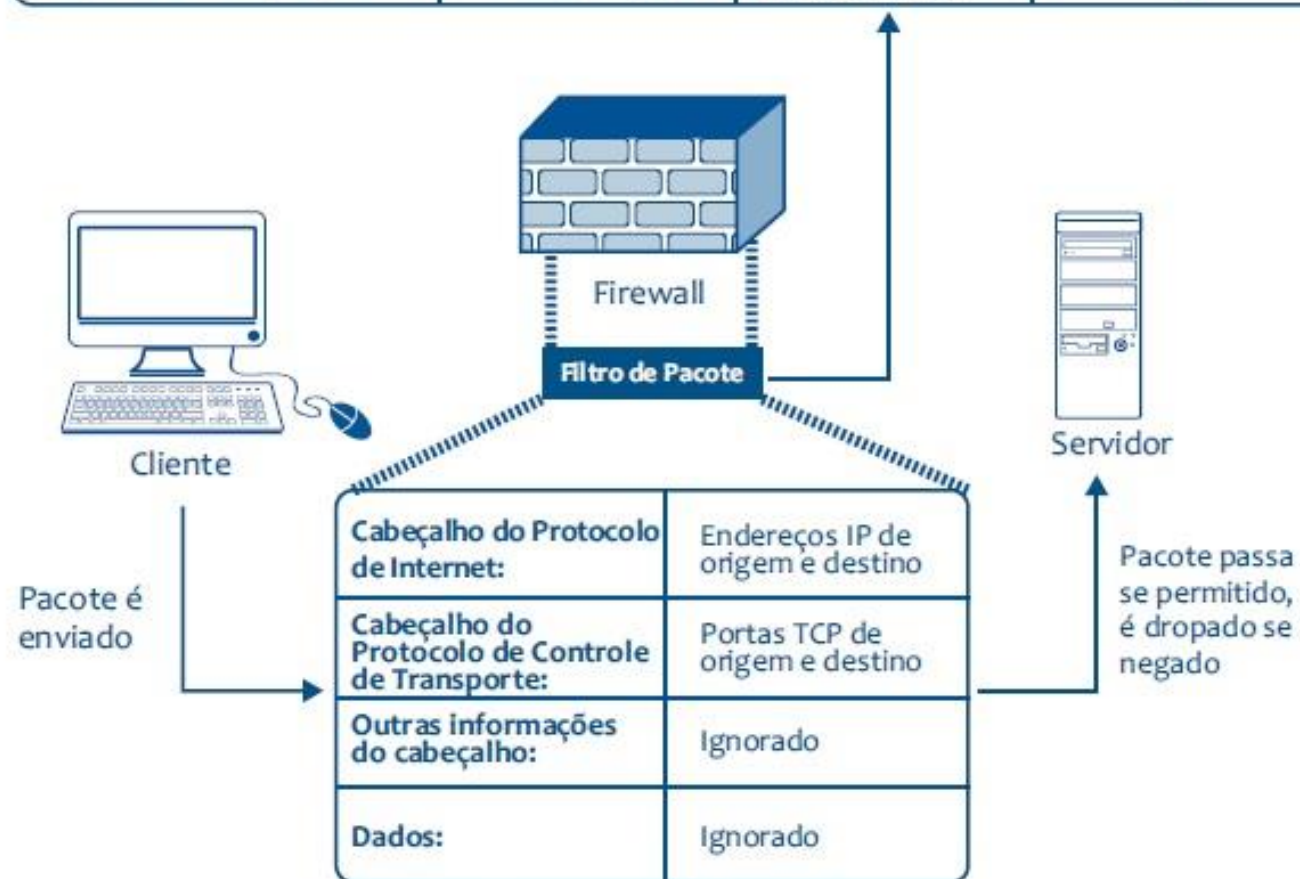


Também são conhecidos como **Dynamic Packet Filter.**



São uma evolução dos filtros de pacotes, pois, associados à tabela de regras, eles possuem uma tabela de estados, que auxiliam na tomada de decisões de filtragem.

Porta do IP de Origem (no caso porta 10033 UDP):	Porta do IP de destino (no caso, UDP 53):	Estado:	Segundos antes de expirar:
192.168.1.1: udp 10033	10.1.1.5: udp53	Não enviada resposta à origem	17
10.1.1.7: tcp 20113	192.168.1.5: tcp80	Fluxo UDP ou conexão TCP estabelecidas	66
192.168.1.1: udp 11412	10.1.15: udp53	Fluxo UDP ou conexão TCP estabelecidas	29



Pacote é comparado com as regras de filtragem e tabela de estado

# Proxy – Firewall de Aplicação



Fazem a intermediação entre um host cliente e um servidor externo, não permitindo conexões diretas entre os mesmos.



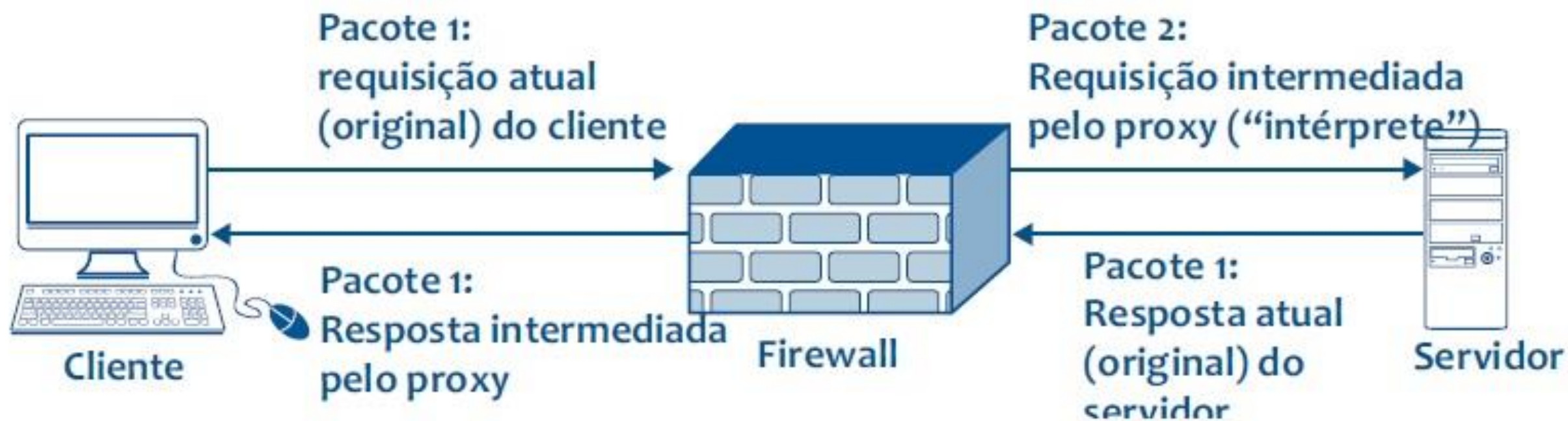
O cliente se conecta a uma porta TCP do firewall e este abre uma conexão com o servidor externo.



**Circuit Level Gateway:** trabalham nas camadas de sessão ou transporte.



**Application Level Gateway:** trabalham na camada de aplicação.



# Vantagens dos Proxies

Não permissão de conexões diretas entre servidores externos e hosts internos;



Capacidade de manter logs detalhados sobre o tráfego de atividades específicas;



Possibilidade de autenticação de usuários;



Possibilidade de análise de comandos de aplicação.

# Desvantagens dos Proxies

Não tratamento de pacotes ICMP.

Maior lentidão em relação aos firewalls de filtro de pacotes.



# Sistemas de Detecção de Intrusão IDS/IPS



O **IDS (Intrusion detection System)** tem por finalidade detectar uma ameaça ou intrusão na rede. Pode se dizer por analogia que o IDS é como se fosse um alarme de um carro que soa quando alguém abre sua porta.




A monitoração e a detecção de intrusos eficientes são tão importantes quanto chaves e cadeados em nossas casas, assim como firewalls em nossas redes.

O **IPS (Intrusion Prevention System)** complementa um IDS bloqueando a intrusão e impedindo um dano maior para a rede.



É uma ferramenta que detecta e bloqueia o invasor. Como foi dito o IDS é como se fosse um alarme de um carro que somente soa quando alguém abre sua porta.



Já o IPS dispara o alarme e também trava as rodas para que o invasor não leve o carro.

# Tipos de IDS

- **IDS de Assinatura (Signature-Based IDS):**
  - Os IDS de assinatura examinam o tráfego da rede em busca de padrões conhecidos de ataques ou atividades maliciosas.
  - Eles usam bases de dados de assinaturas, que contêm descrições detalhadas de ataques conhecidos.
  - Eficientes na detecção de ameaças conhecidas, mas podem ser ineficazes contra ataques novos ou variantes de malware.

- **IDS de Anomalia (Anomaly-Based IDS):**

- Os IDS de anomalia monitoram o tráfego de rede e estabelecem um perfil do comportamento normal da rede.
- Eles detectam atividades que se desviam significativamente do comportamento esperado como possíveis intrusões.
- São eficazes na detecção de ataques desconhecidos, mas podem gerar falsos positivos se o perfil de comportamento normal não estiver bem definido.

- **IDS Híbridos (Hybrid IDS):**

- Os IDS híbridos combinam características de IDS de assinatura e IDS de anomalia.
- Isso permite uma detecção mais abrangente, combinando a detecção de ameaças conhecidas com a detecção de atividades anômalas.
- Pode reduzir os falsos positivos em relação aos IDS de anomalia pura.

- **IDS de Host (Host-Based IDS - HIDS):**

- Os HIDS monitoram a atividade em sistemas e dispositivos individuais, como servidores e estações de trabalho.
- Eles podem identificar intrusões em nível de sistema, como tentativas de acesso não autorizado ou atividades suspeitas em arquivos ou registros de sistema.
- São especialmente úteis para proteger sistemas críticos e servidores.

- **IDS de Rede (Network-Based IDS - NIDS):**
  - Os NIDS monitoram o tráfego da rede em tempo real, examinando os pacotes que circulam na rede.
  - São eficazes na detecção de atividades suspeitas em toda a rede, como escaneamento de portas, tráfego malicioso e ataques de negação de serviço (DDoS).
- **IDS Distribuídos (Distributed IDS - DIDS):**
  - Os DIDS são sistemas que distribuem a funcionalidade de detecção de intrusões em vários pontos da rede, compartilhando informações e coordenando a detecção.
  - São úteis em redes maiores ou complexas, onde um único IDS pode não ser suficiente.

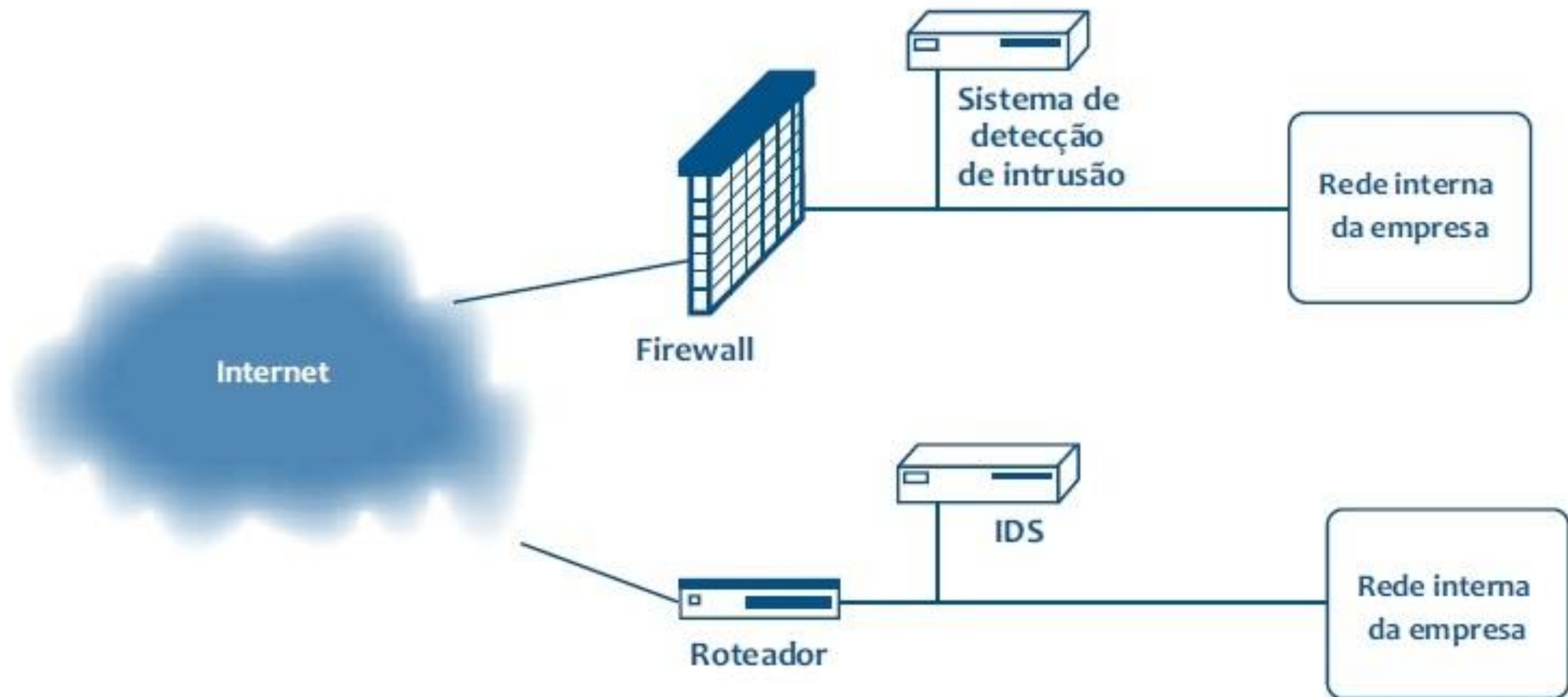
- **IDS Baseado em Comportamento (Behavior-Based IDS):**

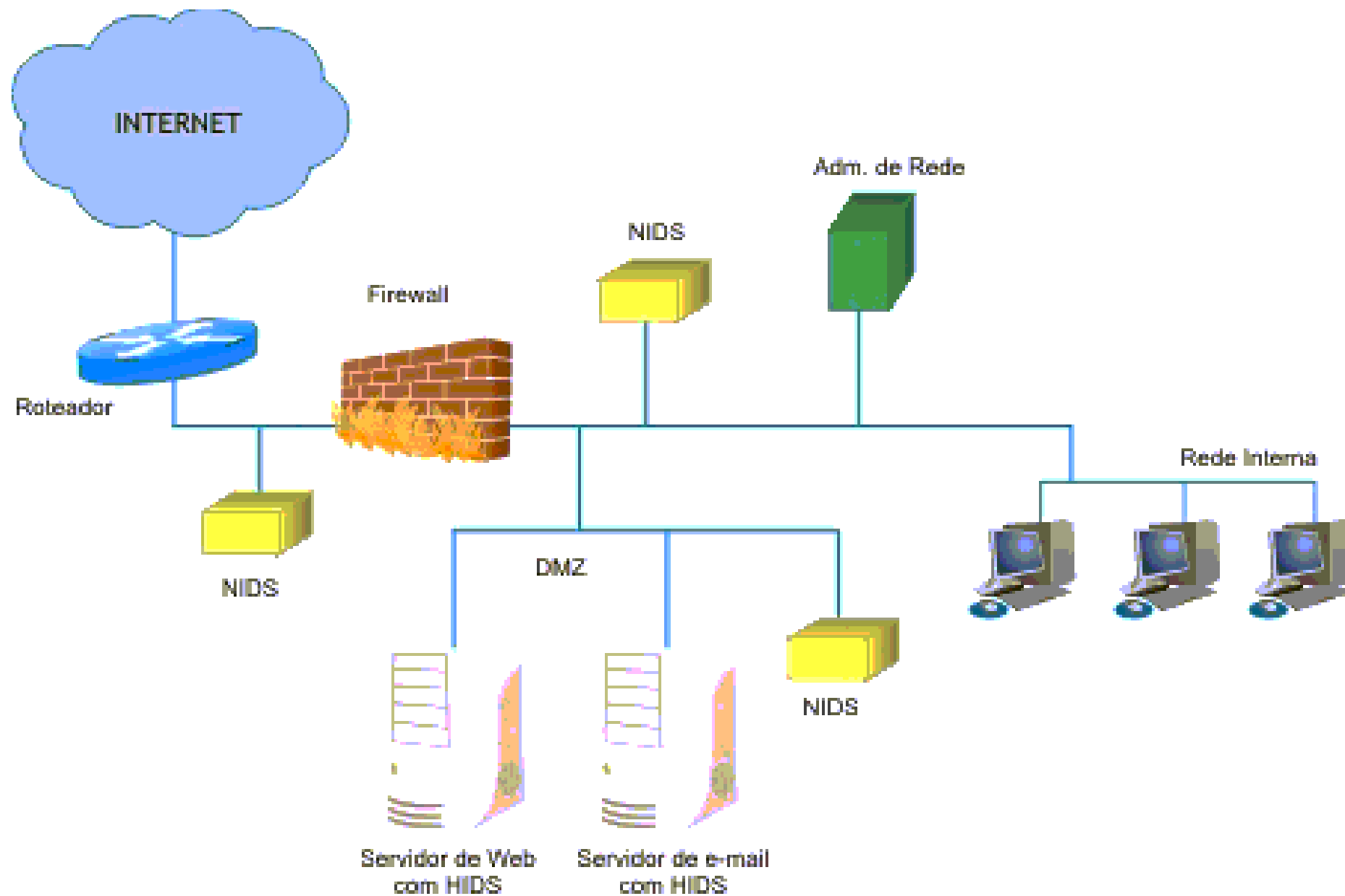
- Os IDS baseados em comportamento se concentram na detecção de atividades suspeitas com base no comportamento dos usuários e dispositivos.
- Eles monitoram as ações de usuários e dispositivos para identificar atividades anômalas ou comportamento suspeito.

- **IDS de Protocolo (Protocol-Based IDS):**

- Os IDS de protocolo analisam o tráfego da rede em busca de violações das regras de protocolo, como tentativas de explorar vulnerabilidades em protocolos específicos.







# Unified Threat Management (UTM)

## "Central Unificada de Gerenciamento de Ameaças"



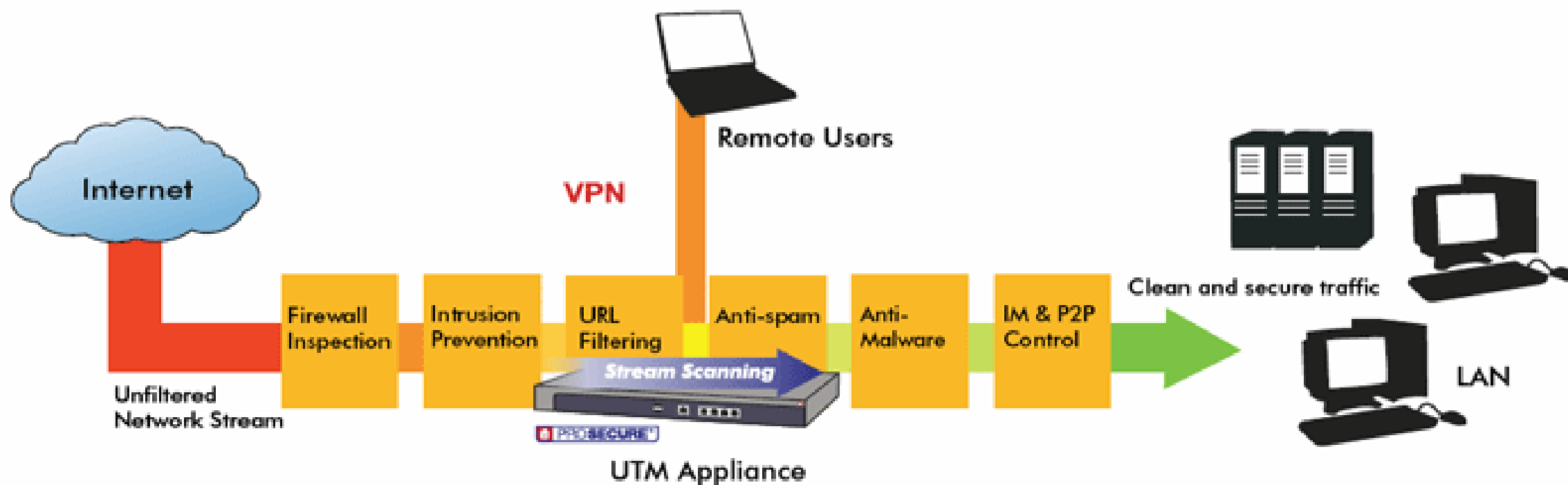
A sigla UTM teve origem no IDC, instituto de pesquisa de mercado, e esta linha de produto tem a vantagem de fundir em um único appliance ( hardware + software) os serviços que antes eram feitos por vários softwares dentro do servidor ou então por vários outros appliances individuais.



Esta unificação das funções permite o gerenciamento da segurança em um único painel, facilitando a prevenção, detecção e ação contra ameaças de variadas fontes. O UTM também garante que as soluções de segurança encontradas nele sejam compatíveis e complementares, diminuindo brechas ou falhas de segurança.

# Unified Threat Management (UTM)

"Central Unificada de Gerenciamento de Ameaças"



O **UTM** é teoricamente uma evolução do firewall tradicional, unindo a execução de várias funções de segurança em um único dispositivo: firewall, prevenção de intrusões de rede, antivírus, VPN, filtragem de conteúdo, balanceamento de carga e geração de relatórios informativos e gerenciais sobre a rede.

# Honey Pots e Honey Nets



As Honey Pots e Honey Nets são estratégias de segurança cibernética que visam atrair e identificar invasores cibernéticos, fornecendo alvos falsos e controlados.



Elas desempenham um papel fundamental na defesa de redes e sistemas, permitindo que as organizações estudem táticas de ataque, identifiquem ameaças e fortaleçam suas medidas de segurança.

# Honey Pot

---

Uma **Honey Pot** é um sistema ou dispositivo de rede que simula ser uma entidade legítima, mas na verdade é um alvo falso projetado para atrair invasores. As Honey Pots podem ser implantadas de várias formas.

---

**Honey Pot de Baixa Interatividade:** Este tipo de Honey Pot emula serviços de rede, como um servidor web ou FTP, com interações limitadas. São mais fáceis de configurar e menos arriscados, mas oferecem menos informações detalhadas sobre os atacantes.

---

**Honey Pot de Alta Interatividade:** Estes Honey Pots são sistemas completos que imitam sistemas operacionais e aplicativos reais. Eles oferecem interações mais sofisticadas, permitindo que os administradores coletem informações detalhadas sobre táticas de ataque e ameaças em potencial.

As Honey Pots são valiosas porque:



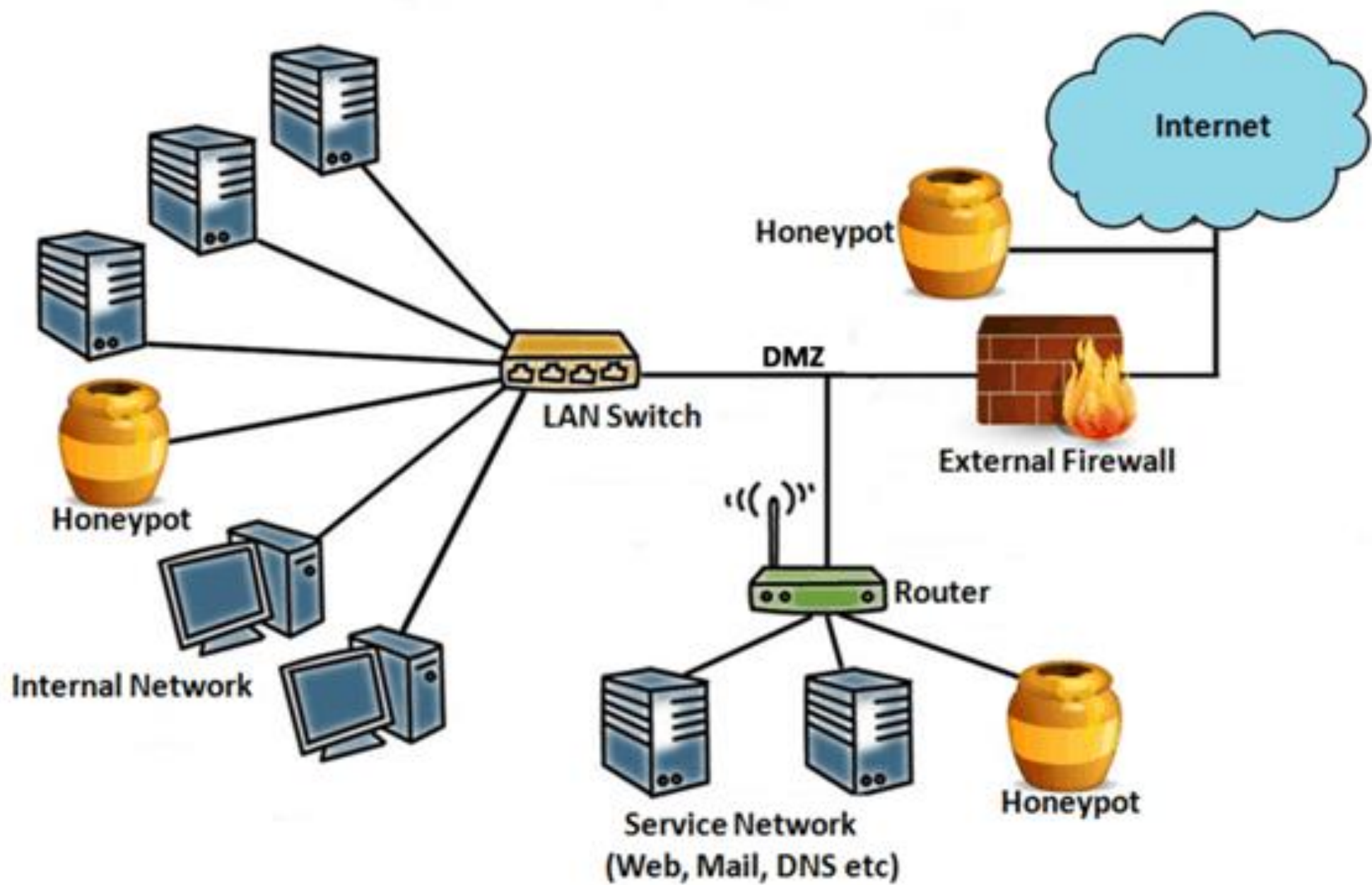
```
graph TD; A[As Honey Pots são valiosas porque:] --> B[Permitem a coleta de informações detalhadas sobre táticas de ataque e ameaças em potencial.]; B --> C[Atraem invasores antes que eles alcancem sistemas e dados reais.]; C --> D[Podem ajudar a distrair e atrasar invasores, dando mais tempo para as equipes de segurança responderem.]; D --> E[Facilitam o aprendizado sobre as vulnerabilidades e os métodos de ataque específicos direcionados à organização.];
```

Permitem a coleta de informações detalhadas sobre táticas de ataque e ameaças em potencial.

Atraem invasores antes que eles alcancem sistemas e dados reais.

Podem ajudar a distrair e atrasar invasores, dando mais tempo para as equipes de segurança responderem.

Facilitam o aprendizado sobre as vulnerabilidades e os métodos de ataque específicos direcionados à organização.





# Honey Net

---

Uma Honey Net é uma rede de Honey Pots interconectados e distribuídos em uma rede ou segmento de rede. Essa abordagem cria um ambiente mais realista para atrair invasores e estudar suas atividades. Além dos benefícios das Honey Pots, as Honey Nets também oferecem:

---

Maior visibilidade das ameaças, pois capturam informações de múltiplos Honey Pots em uma rede.

---

Capacidade de detectar ataques em várias camadas de uma infraestrutura, proporcionando uma visão mais abrangente das táticas de ataque.

---

No entanto, as Honey Nets também requerem mais recursos e planejamento de implementação do que as Honey Pots individuais.

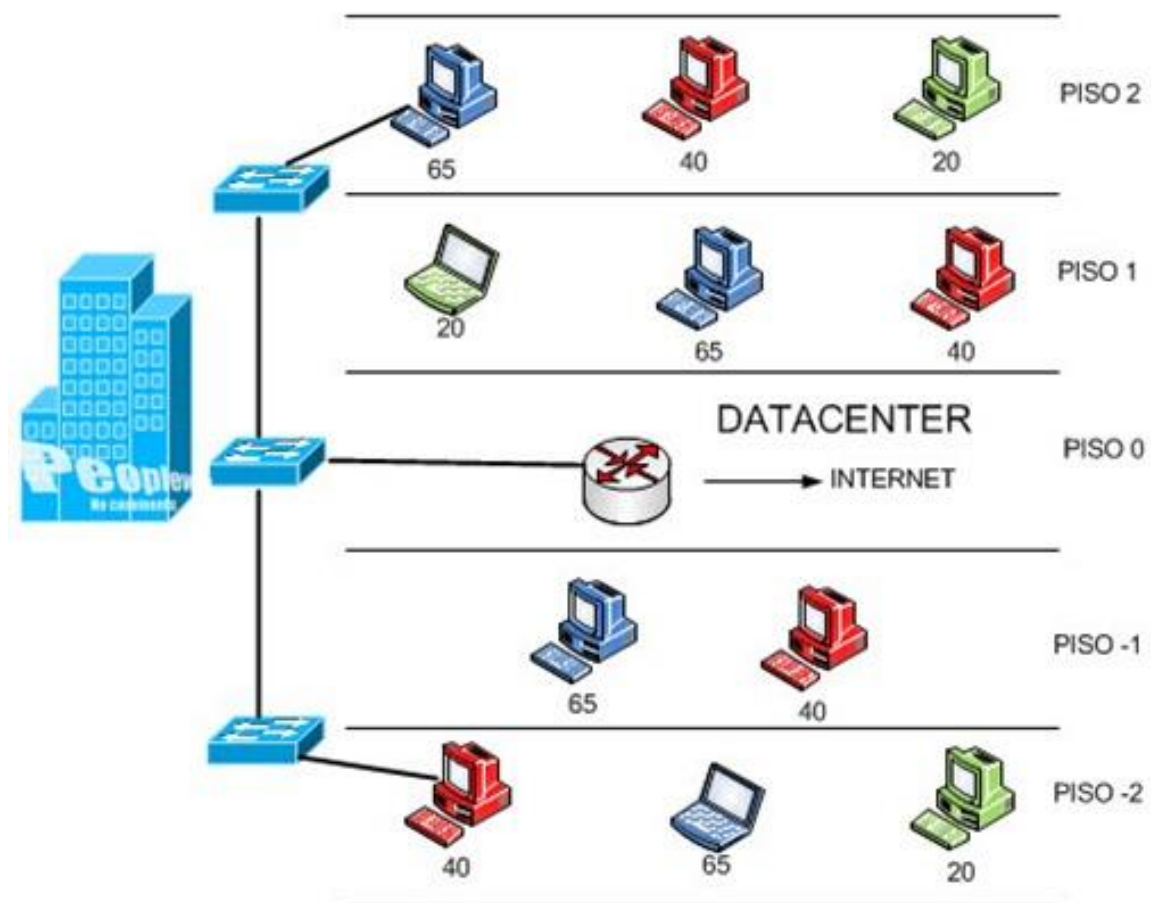
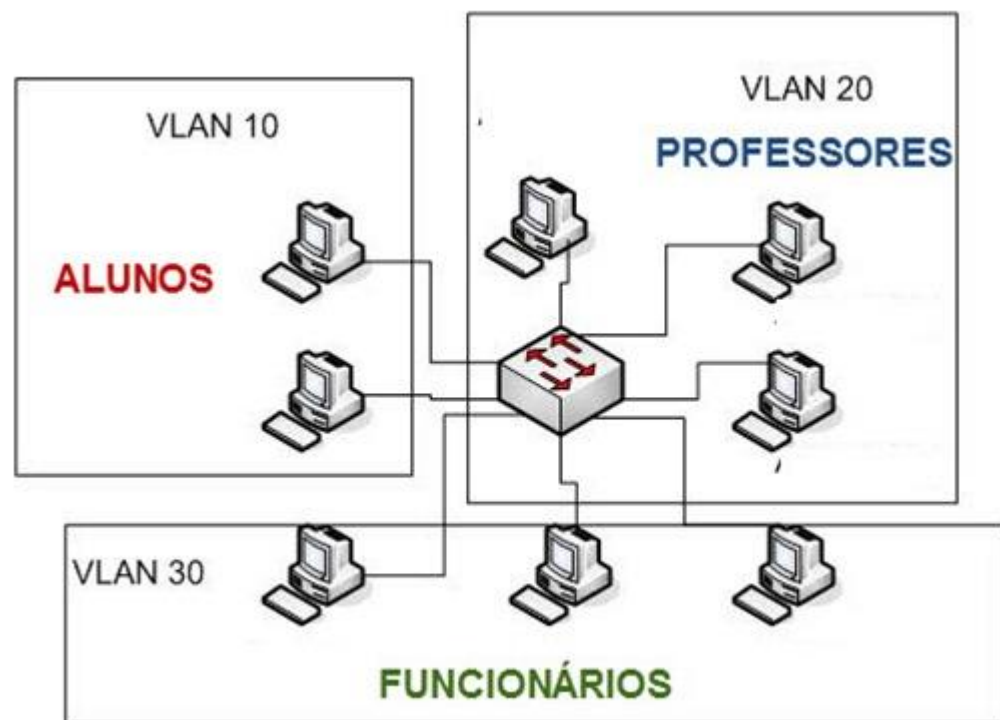
- **Considerações de Segurança:**

- Enquanto Honey Pots e Honey Nets são ferramentas valiosas para melhorar a segurança cibernética, elas também apresentam riscos:
  - **Risco de Ataque às Honey Pots:** Se não forem adequadamente protegidas, as Honey Pots podem se tornar alvos reais para invasores. Portanto, é essencial implementar medidas de segurança robustas.
  - **Coleta e Armazenamento de Dados Sensíveis:** As informações coletadas pelas Honey Pots e Honey Nets podem incluir dados sensíveis dos invasores. É fundamental manter esses dados de forma segura e em conformidade com regulamentos de privacidade.
  - **Falsos Positivos:** As atividades legítimas podem ser erroneamente interpretadas como ameaças, levando a falsos positivos. É importante interpretar os resultados com cuidado.

# VLANs (Virtual Local Area Networks) e DMZ (Demilitarized Zone)

- **VLANs (Virtual Local Area Networks):**
  - As VLANs são uma técnica que permite segmentar uma rede física em várias redes lógicas, isolando grupos de dispositivos em sub-redes virtuais. Aqui estão alguns pontos-chave sobre as VLANs:
  - **Segmentação de Rede:** As VLANs permitem dividir uma rede física em várias redes lógicas separadas. Isso é útil para melhorar o desempenho, a segurança e a gestão da rede.

- **Isolamento de Tráfego:** Dispositivos em VLANs diferentes não podem se comunicar diretamente, a menos que haja um roteador entre elas. Isso aumenta a segurança, isolando o tráfego entre departamentos ou funções diferentes.
- **Melhoria de Desempenho:** Ao dividir uma rede em VLANs, é possível reduzir o tráfego de broadcast, o que ajuda a melhorar o desempenho e a eficiência da rede.
- **Gestão Simples:** VLANs facilitam a gestão de dispositivos, permitindo que os administradores atribuam políticas de rede e segurança a grupos específicos de dispositivos.
- **Tráfego Separado:** As VLANs permitem a segmentação de tráfego de voz, dados, vídeo, entre outros, melhorando a qualidade de serviço (QoS).



-  Serviços de **Contabilidade** (VLAN 40)
-  Serviços **Gestão de Pessoal** (VLAN 65)
-  Serviços de **Apoio a Direcção** (VLAN 20)

- **DMZ (Demilitarized Zone):**

- Uma DMZ é uma área de rede separada e desprotegida localizada entre a rede interna de uma organização e a rede externa (normalmente a internet). Aqui estão alguns pontos-chave sobre DMZ:

- **Camada Intermediária de Segurança:** A DMZ atua como uma camada intermediária entre a rede interna (confiável) e a rede externa (não confiável). Ela é projetada para hospedar serviços acessíveis ao público, como servidores web, de e-mail ou DNS.
- **Isolamento Controlado:** Os servidores na DMZ são isolados da rede interna e têm acesso limitado apenas aos serviços necessários. Isso impede que intrusos acessem diretamente a rede interna em caso de comprometimento.

- **Políticas de Segurança:** As políticas de segurança são rigorosas na DMZ, com regras de firewall que controlam o tráfego de entrada e saída. Isso ajuda a proteger a rede interna contra ameaças externas.
- **Monitoramento e Registro:** A DMZ é frequentemente monitorada de perto para detectar atividades suspeitas ou tentativas de intrusão. Os registros de eventos são mantidos para fins de auditoria e investigação.
- **Balanceamento de Carga e Redundância:** A DMZ pode ser usada para implementar balanceamento de carga e redundância para serviços de alto tráfego, como servidores web.

