

**Engenharia de Controle e Automação – 9º Período**  
**Disciplina: Aspectos de Segurança em Automação**  
**Professor: José Maurício S. Pinheiro**

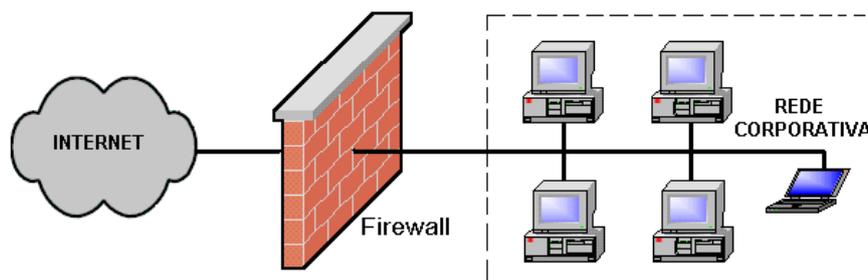
**AULA 6: Sistemas de Proteção e Prevenção de Intrusão**

A segurança é inversamente proporcional à simplicidade e facilidade de uso / configuração da rede. Por exemplo, um servidor da rede pode centralizar diversos serviços para atender a rede externa (Internet) e a rede privada (interna). Esta configuração gera problemas de segurança como:

- **Exposição da rede interna à Internet** - Os serviços da rede interna (e-mail, por exemplo) estando localizados na mesma máquina que provê os serviços externos (web, por exemplo), deixarão os dados do usuário expostos em caso de uma invasão;
- **Maior fragilidade a vulnerabilidades** - O fato de concentrar muitos serviços em uma única máquina gera esse tipo de problema, pois quanto mais serviços disponíveis, mais vulnerabilidades podem ser exploradas e, conseqüentemente, existe um maior grau de exposição e risco de invasão;

**1. Firewall**

O Firewall opera nas camadas de transporte e de rede do modelo TCP/IP, tendo como principal finalidade a filtragem de pacotes. Ele analisa todos os pacotes que entram ou saem de todas as interfaces de rede a ele conectadas, ou seja, tanto pacotes destinados diretamente ao Firewall, quanto destinados a qualquer host conectado a ele por meio de alguma de suas interfaces de rede. Outra função do firewall é bloquear todas as portas quem não estejam sendo utilizadas (Figura 1).



**Figura 1 - Firewall implementado no perímetro da rede local**

O firewall é uma passagem (“gateway”) que restringe e controla o fluxo de dados entre redes, mais comumente entre uma rede interna e a Internet e também pode estabelecer passagens seguras entre redes internas. Algumas máquinas da rede precisam receber acessos externos, é o caso de servidores SMTP e servidores Web, por exemplo. Para permitir que estas máquinas possam desempenhar suas funções, mas que ao mesmo tempo o restante da rede continue protegida, muitos firewalls oferecem a opção de criar uma zona

onde a vigilância é mais fraca, conhecida como DMZ (Figura 2). Nesse caso, o controle de acesso à Internet pode ser feito através de DMZ permitindo que todo o tráfego entre os servidores da empresa, a rede interna e a Internet, passe por um firewall e pelas regras de segurança criadas para a proteção da rede interna. Assim, o firewall se torna um único ponto de acesso à rede em que o tráfego poderá ser analisado e controlado por meio de scripts no firewall que definem o aplicativo, o endereço e os parâmetros de usuário. Esses scripts ajudam a proteger os caminhos de conectividade para redes e centros de dados externos.

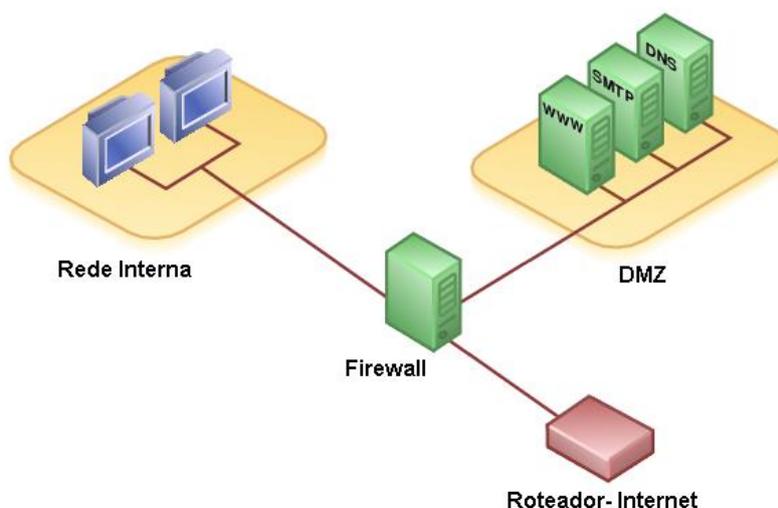


Figura 2 - Rede com firewall e DMZ

### 1.1. Funções de Firewall

- **Filtro de Pacotes** - Tem a capacidade de analisar os cabeçalhos (Headers) dos pacotes, a função principal e mais usada no Firewall;
- **NAT (Network Address Translator)** - Controla a origem ou destino dos pacotes, alterando no cabeçalho a porta e/ou endereço IP do pacote, seja de origem ou de destino, conforme a necessidade;
- **Híbridos** - São soluções que associam, além da função de filtragem de pacotes, a função NAT, onde, além de alterar a origem e destino dos pacotes, podemos também analisá-los.

### 1.2. Tipos de Firewall

Temos três tipos básicos de Firewall: Roteador de Barreira, Gateway Servidor de Proxy e Inspeção de Estado:

#### 1.2.1. Roteador de Barreira

Este roteador pode ser um equipamento específico ou um computador com duas placas de rede, filtrando os pacotes baseando-se no endereço IP e, às vezes, no tipo de conexão (nível transporte). O Roteador conecta duas redes implementando filtragem de pacotes e controle do tráfego entre elas (Figura 3).

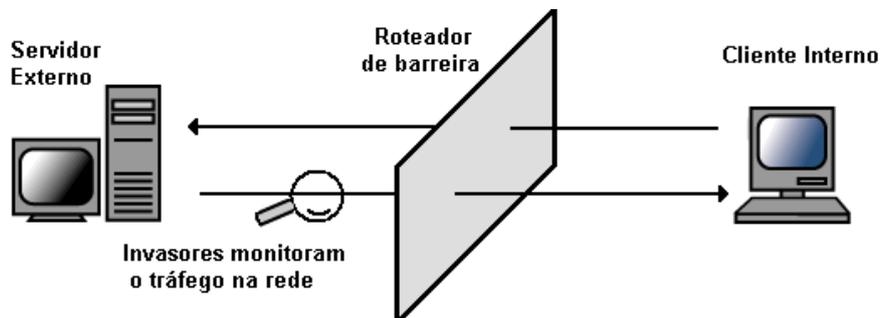


Figura 3 - Roteador de barreira

### 1.2.2. Gateway Servidor de Proxy

Gateways funcionam em um nível mais elevado na pilha de protocolos permitindo maiores possibilidades de monitorar e controlar a comunicação entre redes. O Gateway de Servidor Proxy, ou simplesmente Proxy, age como um intermediário entregando mensagens de um cliente interno a um serviço externo. O serviço de Proxy altera o endereço IP dos pacotes do cliente para protegê-lo da Internet, agindo em seu nome na Internet. O único endereço que vai para a Internet é o do Proxy.

Usando um servidor Proxy diminui a possibilidade de invasão pelo monitoramento do tráfego de rede, bloqueando a obtenção de informações sobre os computadores da rede interna. Existem dois tipos de Servidores Proxy: Gateway de Nível Circuito e Gateway de Nível Aplicação.

#### 1.2.2.1. Gateway de Nível Circuito

Este tipo de servidor Proxy provê uma conexão controlada de rede entre sistemas internos e externos. Existe um circuito virtual entre os clientes e o Proxy. As requisições para a Internet passam por este circuito até o servidor Proxy que altera o endereço IP e encaminha a mensagem à Internet. Os usuários externos só veem o endereço IP do Servidor. As respostas são recebidas pelo Servidor Proxy e enviadas de volta pelo circuito ao cliente. O sistema interno e o externo nunca se conectam, senão através do Proxy (Figura 4).

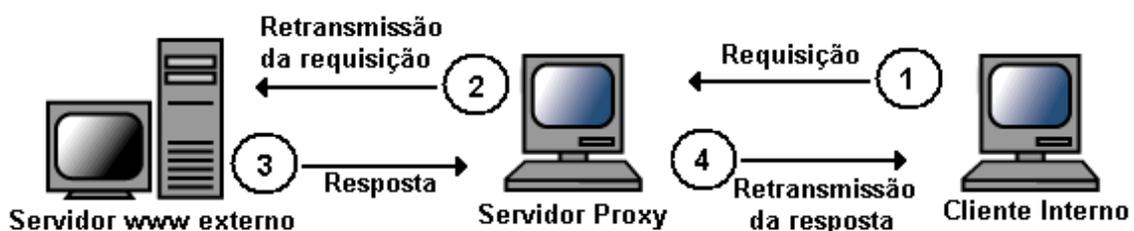


Figura 4 - Gateway de nível de circuito

### 1.2.2.2. Gateway de Nível Aplicação

Este tipo de Servidor Proxy fornece, além dos serviços básicos citados acima, um serviço de análise dos pacotes. Quando o pacote que vem da rede externa é examinado e avaliado para determinar se, a política de segurança permite que este pacote entre na rede interna. O Gateway não avalia somente o endereço IP, verifica também os dados contidos no pacote para bloquear malwares que escondem informações nos pacotes (Figura 5).

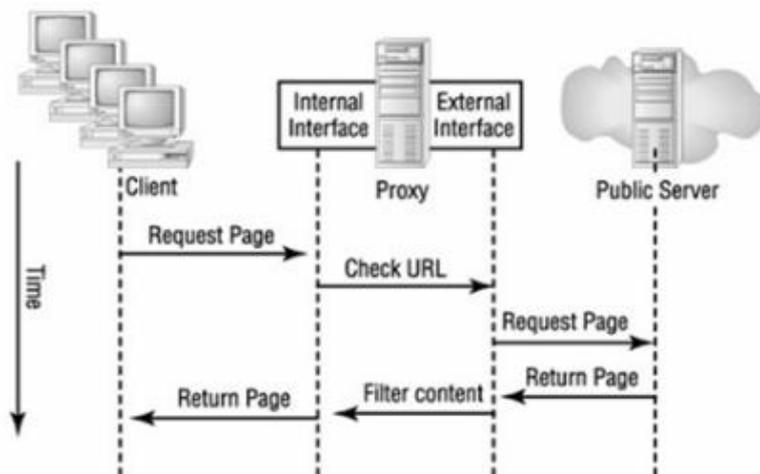


Figura 5 - Gateway de nível aplicação

Um Gateway de Nível Aplicação típico pode prover serviços para aplicações e protocolos como: Telnet, FTP, HTTP e SMTP. Estes serviços podem ser aplicados em um servidor único ou em um conjunto de servidores dedicados a uma aplicação.

### 1.2.3. Gateway de Técnicas de Inspeção de Estado

O Gateway de Técnicas de Inspeção de Estado, em vez de examinar cada pacote, compara o padrão de bits do pacote com um padrão conhecido como confiável. Por exemplo, quando o cliente acessa um serviço externo, o servidor salva dados da requisição como número da porta, endereço de origem e de destino. Esta memória é chamada: salvar o estado. Quando o sistema externo responde à requisição, o Firewall compara o pacote recebido com o estado salvo para definir se ele está autorizado a entrar. Enquanto esta técnica fornece velocidade e transparência, uma das grandes desvantagens é que os pacotes internos acessam a rede externa com os seus próprios endereços IP, expondo os endereços internos ao ataque de hackers (Figura 6).

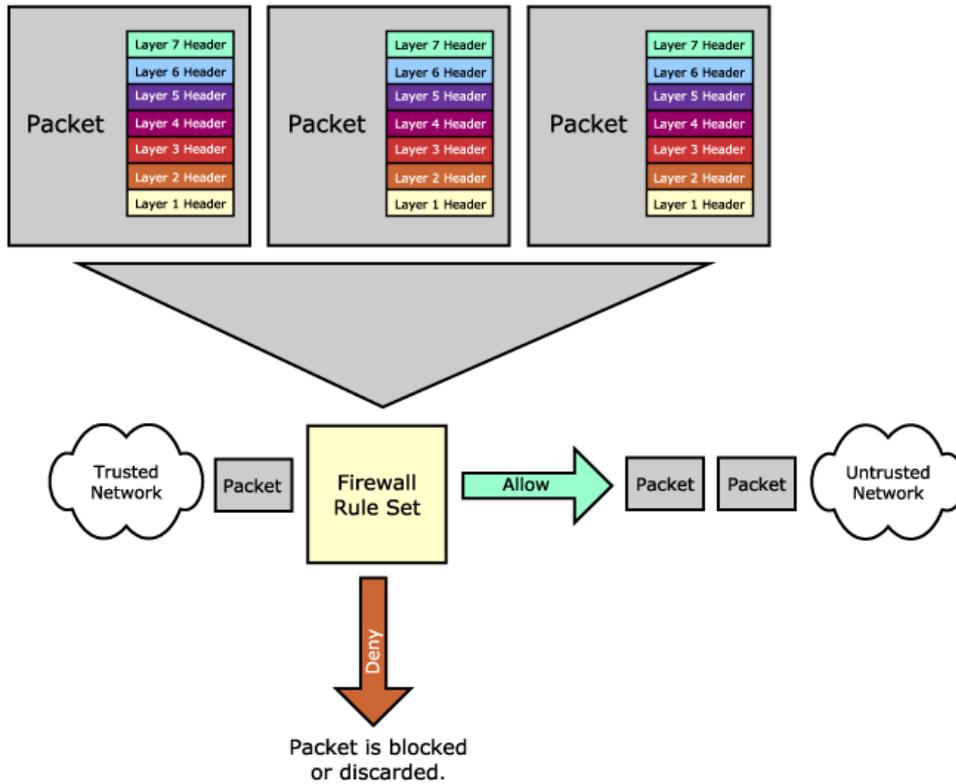


Figura 6 – Gateway de Inspeção de Estado

### 1.3. Proxy

O Proxy normalmente é um computador que funciona como intermediário entre um navegador da Web e a Internet. Os servidores proxy ajudam a melhorar o desempenho na Web armazenando uma cópia das páginas utilizadas com mais frequência. Quando um navegador solicita uma página que está armazenada no servidor proxy (o cache), ela é disponibilizada pelo servidor proxy, o que é mais rápido do que acessar a Web. Os servidores proxy também ajudam a melhorar a segurança porque filtram alguns tipos de conteúdo da Web e softwares mal-intencionados. Eles são mais usados por redes de organizações e empresas. Normalmente, as pessoas que se conectam à Internet de suas casas não usam um servidor proxy.

O Proxy tem como função principal analisar os pacotes de internet, FTP e http, por exemplo. Os Proxies também têm a função de prover controle de acesso por meio de autenticação. Grande parte das redes corporativas os utiliza para o controle e monitoramento do acesso à Internet, por exemplo, o Linux apresenta o SQUID.

O Servidor Proxy é, em essência, um equipamento que presta um serviço de procurador de um computador de uma rede em outra rede, evitando que o endereço IP do computador seja conhecido na outra rede. O Serviço de Proxy age como representante de um usuário que precise acessar um sistema do outro lado do Servidor Proxy (Figura 7).

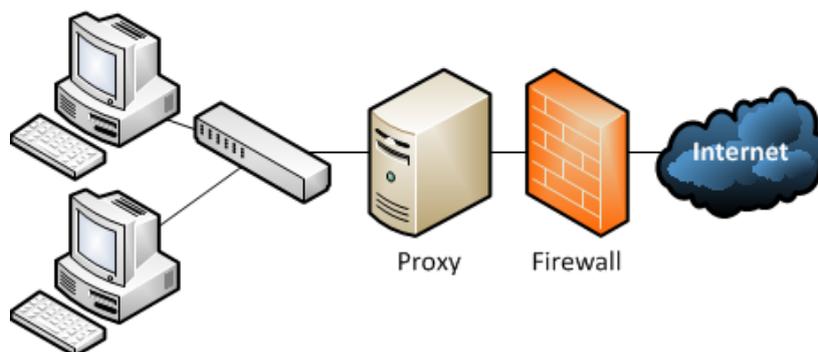


Figura 7 - Proxy na rede de computadores

Um dos maiores problemas dos servidores Proxy é que eles têm de avaliar muitas informações em muitos pacotes. Além disso, com o crescimento da demanda pelos serviços a adoção de múltiplos Servidores Proxy especializados é natural. Isto afeta a performance e implica em custos.

#### 1.4. Rede de Perímetro

O termo refere-se a um segmento de rede isolado no ponto em que uma rede corporativa alcança a Internet. As redes de perímetro destinam-se a criar um limite que permite a separação do tráfego entre redes internas e externas. Com este limite, é possível categorizar, colocar em quarentena e controlar o tráfego da rede de uma empresa. A segurança de perímetro é proporcionada por um dispositivo como um firewall, por exemplo, que inspeciona os pacotes e as sessões para determinar se devem ser transmitidos para a rede protegida ou a partir dela ou ser abandonados (Figura 8).

Os serviços e servidores que devem interagir com a Internet externa desprotegida são colocados na rede de perímetro e na sub-rede filtrada. Isto ocorre para que, caso invasores consigam explorar vulnerabilidades em serviços expostos, possam avançar apenas uma etapa no acesso à rede interna confiável.

A rede de perímetro, também conhecida como Zona Desmilitarizada, DMZ ou ainda “Zona Neutra”, também pode incluir regras de acesso específico e sistemas de defesa de perímetro para que simule uma rede protegida e induzindo os possíveis invasores para armadilhas virtuais (honeyPots) de modo a se tentar localizar a origem do ataque. Um HoneyPot (pote de mel), é uma ferramenta de segurança que tem a função simular falhas de segurança de um sistema e colher informações sobre o invasor, funcionando como uma espécie de armadilha.

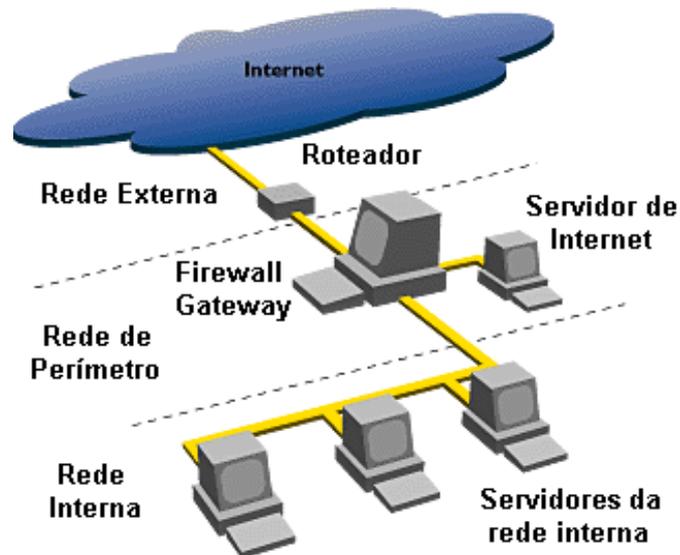


Figura 8 - Rede de perímetro

Podemos ter dois tipos de DMZ: a interna, só acessada pelo usuário da rede interna e a DMZ externa, acessada por qualquer usuário da Internet. Este conceito aliado ao de VLAN também permite a implantação de DMZ privadas, ou seja, a possibilidade de DMZ específicas para cada cliente ou para a hospedagem de servidores. As DMZ são sub-redes onde se hospedam os servidores / serviços de um provedor, protegidos contra ataques da Internet por um firewall. Em geral é necessário especificar uma faixa de endereços IP, ou informar diretamente os endereços das máquinas que devem ser incluídas nessa zona.

#### 1.4.1.1. Bastion Host

Por definição, bastion host é qualquer máquina configurada para desempenhar algum papel crítico na segurança da rede interna e provendo os serviços permitidos segundo a política de segurança da empresa. Trata-se de uma máquina segura que está localizada no lado público da rede de perímetro (acessível publicamente), mas que não se encontra protegida por um firewall ou roteador de filtragem, expondo-se totalmente a ataques (Figura 9). Este tipo de máquina também recebe a denominação de “*application gateway*” porque funciona como um gateway ao nível de aplicação. Os servidores disponíveis nos bastion host são denominados de proxy servers, ou seja, servidores por procuração que atuam como intermediários entre o cliente e o servidor.

Um bastion host deve ter uma estrutura simples, de forma que seja fácil de garantir a segurança. São normalmente usados como servidores Web, DNS, FTP, SMTP. Como é mais fácil proteger um único serviço em um único bastion host, o ideal é que eles sejam dedicados a executar apenas uma das funções citadas, pois quanto mais funções cada um desempenha, maior a probabilidade de uma brecha de segurança passar despercebida.

Os bastion hosts são configurados de uma maneira bem diferente dos hosts comuns. Todos os serviços, protocolos, programas e interfaces de rede desnecessárias são desabilitados ou removidos e cada bastion host é, normalmente, configurado para desempenhar uma função específica. A

proteção de bastion hosts dessa maneira limita os métodos potenciais de ataque. Por esse motivo os bastion hosts são um ponto crítico na segurança de uma rede, geralmente necessitando de cuidados extras como auditorias regulares.

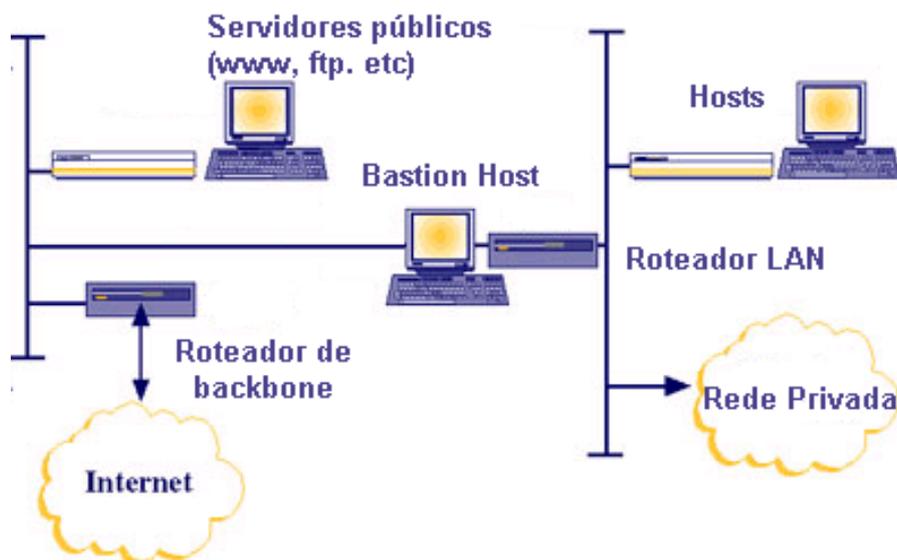


Figura 9 - Bastion Host

#### 1.4.2. Implantação da DMZ

O projeto lógico de uma rede que visa conexões com a Internet deve envolver a criação de uma DMZ. Esta DMZ será protegida por um sistema de defesa de perímetro, onde os usuários de Internet podem entrar livremente para acessar os servidores web públicos, enquanto que os dispositivos localizados nos pontos de acesso (firewall, switch e servidor de perímetro) filtram todo o tráfego não permitido, como por exemplo, pacotes de dados que tentam prejudicar o funcionamento do sistema. Ao mesmo tempo a rede interna privada está protegida por um outro firewall (Figura 10).

A zona desmilitarizada comporta-se como uma outra sub-rede, atrás de um firewall, onde temos uma máquina segura na rede externa que não executa nenhum serviço, mas apenas avalia as requisições feitas a ela e encaminha cada serviço para a máquina destino na rede interna. No caso de uma invasão de primeiro nível, o atacante terá acesso apenas ao firewall, não causando problema algum para a rede da empresa. Já em invasões de segundo nível, o atacante conseguirá passar do firewall para a sub-rede interna, mas ficará preso na máquina do serviço que ele explorar.

Em todos os casos, devem-se analisar com cuidado quais serviços podem ser colocados dentro da DMZ. Por exemplo, na maioria das situações, o servidor de e-mail é inserido na DMZ. Nesse caso, em uma invasão ao servidor de e-mail, os únicos dados que poderão ser comprometidos são os e-mails e mais nenhum outro. Já a colocação de um servidor de DNS em uma DMZ não é recomendável para a segurança da rede. Como uma DMZ permite acesso menos seguro para alguns segmentos da rede, a colocação desse servidor

nesta situação poderia comprometer a segurança dos endereços de todos os servidores da rede local e roteadores.

Convém salientar que durante a elaboração do projeto da rede, é recomendável se manter os serviços separados uns dos outros. Assim, será possível adotar as medidas de segurança mais adequadas para cada serviço.

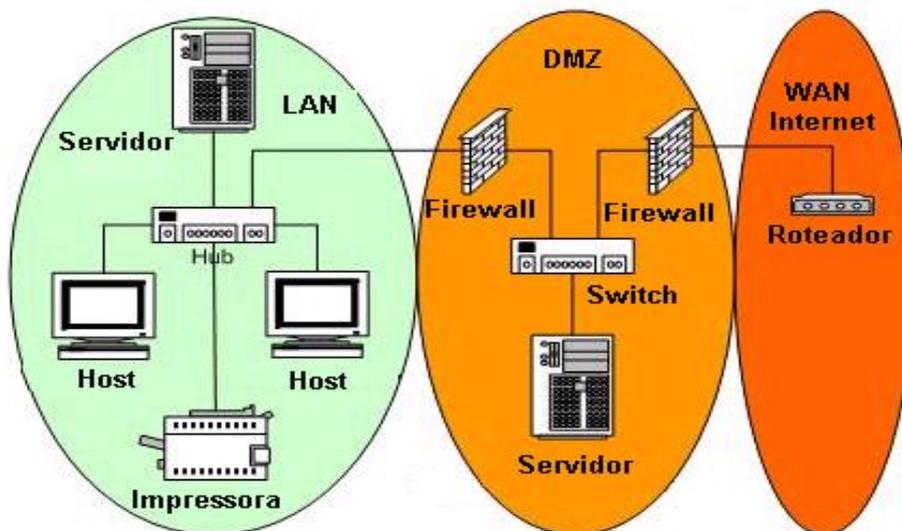


Figura 10 - Exemplo de rede com DMZ

## 2. Sistemas de Detecção de Intrusão (IDS)

Uma infraestrutura de segurança mais simples consiste em um firewall implementado no perímetro da rede local de computadores (LAN). Esta estrutura funciona bem quando há uma interação limitada entre as redes externa e interna, quando os usuários internos são confiáveis e quando o valor das informações na rede é limitado. Os sistemas de detecção de intrusão (*Intrusion Detection System - IDS*), são sistemas automáticos que funcionam em tempo real, analisando o tráfego na rede e detectam tentativas não autorizadas de acesso à rede lógica. O grande objetivo é proporcionar uma reação efetiva aos ataques que um segmento de rede possa vir a sofrer.

Os IDS baseiam seu funcionamento nos tipos conhecidos de ataques e também verificando alterações de comportamento no tráfego de dados. Sempre que é detectada alguma alteração no comportamento desse tráfego ou identificado algum padrão de ataque, o sistema pode enviar um alerta aos administradores da rede, contra-atacar ou simplesmente se defender baseado em alguma configuração predefinida.

### 2.1. Tipos de IDS

Os IDS podem ser divididos em dois grandes grupos:

- Baseados em host (*Host-based Intrusion Detection System – HIDS*);
- Baseados em rede (*Network-based Intrusion Detection System - NIDS*);
- Híbridos - (Hybrid IDS), aproveitam as melhores características do HIDS e do NIDS.

### 2.1.1. HIDS

Os sistemas baseados em host (HIDS) são programas dedicados a sistemas individuais, afinados às suas características e que detectam sinais de intrusão nas comunicações (de entrada ou de saída) dos sistemas que protegem. Esses sistemas fazem o monitoramento da rede com base em informações de arquivos de logs ou de agentes de auditoria.

No caso de se tratar de um servidor de banco de dados, por exemplo, o HIDS poderá analisar, além das transações do sistema operacional e do protocolo de comunicação, operações específicas dos aplicativos em utilização.

### 2.1.2. NIDS

Os sistemas baseados em rede (NIDS) monitoram o tráfego do segmento da rede em tempo real, com a interface de rede atuando em modo promíscuo. Desse modo é possível capturar os pacotes referentes ao ataque, analisar e responder praticamente ao mesmo tempo em que o segmento da rede é atacado. Os NIDS podem ser divididos em duas partes que atuam em conjunto: sensores (sondas) e um gerenciador (ou console) como mostrado na Figura 11.

- Os sensores são colocados em pontos estratégicos da infraestrutura, analisando todo o tráfego do segmento de rede onde estão inseridos, comparando-o com uma base de dados de padrões e assinaturas de ataques para identificar atividades suspeitas. A detecção é realizada pela captura e análise dos cabeçalhos e conteúdo dos pacotes, que são comparados com esses padrões e assinaturas;
- O gerenciador é responsável pela administração integrada dos sensores, com a definição dos tipos de resposta a serem utilizados para cada evento de comportamento suspeito detectado. A comunicação entre gerenciador e sensores utiliza na maioria das vezes criptografia assimétrica para a formação de um canal seguro.

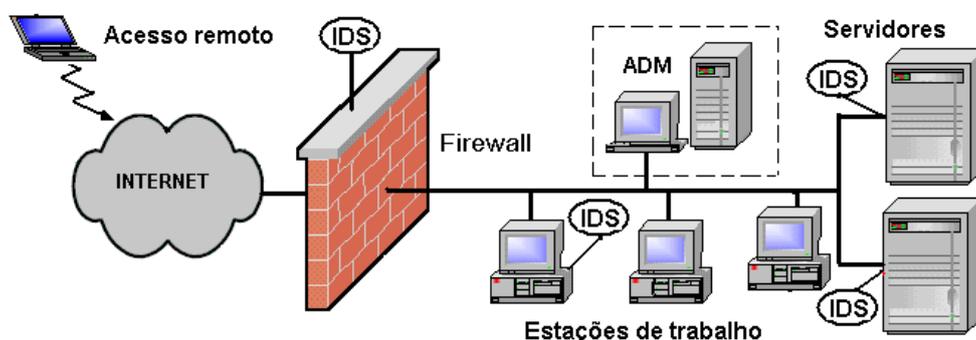


Figura 11 – Posicionamento da estação de gerenciamento central na rede

### 2.1.3. Sistemas Híbridos

Um sistema IDS híbrido tem como objetivo combinar as vantagens do HIDS e do NIDS, a fim de proporcionar uma melhor capacidade de detecção de intrusões. O IDS híbrido funciona como o NIDS coletando o tráfego de pacotes

da rede, processando as informações e detectando e respondendo a ataques do mesmo modo como ocorre no HIDS. Com relação ao gerenciamento, alguns sistemas podem ter uma centralização dos IDS, pois alguns sensores, baseados em rede, são localizados em diversos segmentos de rede e outros IDS, baseados em host, são usados em servidores. O gerenciador pode controlar as regras dos dois tipos, formando o IDS híbrido. No caso dos servidores da DMZ, o uso de IDS híbrido é vantajoso uma vez que ataques específicos a cada servidor podem ser identificados com maior precisão.

#### **2.1.4. Deficiências nos IDS**

Uma deficiência nos IDS é o fato do seu funcionamento se basear no mesmo princípio dos sistemas antivírus, ou seja, utilizam bases de dados com assinaturas de ataques: se ataques conhecidos são detectados, as tentativas são bloqueadas com relativa facilidade, caso contrário, podem passar impunemente. Outra questão tem a ver com o volume de dados gerado. Numa rede com elevados índices de atividade, os dados registados pelos sensores podem atingir proporções significativas, o que implica dificuldades na capacidade de detecção e de gestão.

A instalação de um IDS deve ser cuidadosamente avaliada. Regra geral, não são sistemas simples e seu custo cresce proporcionalmente com a capacidade de proteção desejada. Os sensores de rede deverão ser instalados em máquinas dedicadas, nos pontos de entrada da infraestrutura de comunicação e os sensores de host nos sistemas que se pretende proteger. Todos os sensores se comunicam com uma estação de gerenciamento central (ADM), onde são armazenados todos os dados coletados. Esta estação, que também deverá ser dedicada a esta tarefa, é o ponto da rede no qual se faz a gestão centralizada dos recursos IDS disponíveis.

#### **2.1.5. Metodologias de Detecção**

Idealmente, a infraestrutura IDS deve pertencer numa rede dedicada, separada do restante da rede corporativa, não devendo os computadores com sensores de rede ser visíveis nesta última, ou seja, as suas placas de rede não devem possuir qualquer endereçamento, ou seja, devem operar em modo promíscuo. Os dados relativos à atividade maliciosa registados pelo IDS podem ocasionar várias reações: alertas administrativos (incluindo chamadas para celulares) e reações automáticas (interrupção da conexão ou bloqueio do IP de origem, por exemplo).

As metodologias utilizadas pelos IDS para a detecção de um ataque são o *Knowledge-Based Intrusion Detection*, também conhecido como *Misuse Detection System* e o *Behavior-Based Intrusion Detection*, também conhecido como *Anomaly Detection System*.

##### **2.1.5.1. Knowledge-Based Intrusion Detection**

A abordagem Knowledge-Based Intrusion Detection, na qual as detecções são realizadas segundo uma base de dados com informações sobre ataques conhecidos, é a mais utilizada pelos IDS. O funcionamento, neste caso, é

semelhante ao antivírus, pois o IDS procura por um padrão ou uma assinatura de ataque que esteja na sua base de dados. Todos os eventos que não são reconhecidos pelo conjunto de assinaturas são considerados aceitáveis. Conseqüentemente, a precisão desse tipo de IDS depende das atualizações da base de dados, do sistema operacional, da versão de IDS em uso, da plataforma e da aplicação.

### 2.1.5.2. Behavior-Based Intrusion Detection

O Behavior-Based Intrusion Detection considera que as tentativas de intrusão podem ser descobertas através de desvios no comportamento dos usuários ou dos sistemas. Um modelo de normalidade é estabelecido em condições adequadas de uso dos recursos (quando este não está sob ataque) e comparado com a atividade em andamento. Qualquer comportamento suspeito dos pacotes que trafegam pela rede passa por uma análise estatística ou heurística com o objetivo de encontrar possíveis indícios de alterações de padrão, como súbito aumento de tráfego, utilização maciça da CPU, atividade anormal do disco rígido, entre outros. O que for diferente do padrão armazenado na base de dados será considerado suspeito.

### 2.1.6. Posicionamento dos Sensores

Um dos problemas para a utilização de IDS, especificamente do NIDS, é a segmentação cada vez maior das redes pela utilização de switches, o que faz com que o NIDS tenha limitações quanto ao seu desempenho, uma vez que ele funciona no modo promíscuo, analisando todos os pacotes que passam pelo segmento da rede. É possível utilizar o NIDS em redes segmentadas por switches usando sensores HIDS em conjunto com o NIDS, nos IDS híbridos. Os sensores podem ser usados de diversas formas, as quais irão refletir o grau de monitoramento do ambiente de rede (Figura 12):

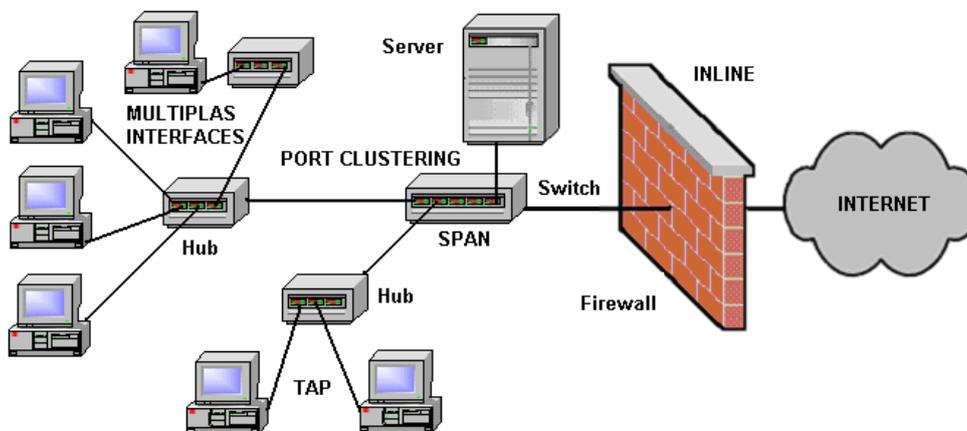


Figura 12 - Posicionamento dos sensores na rede

- **Switched Port Analyzer (SPAN) e hubs** – portas SPAN de switches ou portas de hubs podem ser usadas para que os sensores sejam habilitados;

- **Modo Tap** – os sensores são inseridos como uma extensão da rede (modo Tap);
- **Modo Inline** – ou modo ativo. O IDS é posicionado fisicamente no fluxo da informação, com o tráfego dos pacotes passando ativamente pelo sistema;
- **Port Clustering** – permite a monitoração dos segmentos da rede, com todos os tráfegos sendo agregados em um único fluxo de dados;
- **Múltiplas interfaces** – um sensor atuando em diferentes segmentos de rede.

### 2.1.7. Localização do IDS na Rede

O IDS pode ser utilizado em diversas posições na rede e cada posição significa um tipo de proteção específico (Figura 13). Outra consideração importante é quanto ao posicionamento do IDS em relação ao firewall da rede:

- Posicionado antes do firewall, a detecção é considerada simultânea aos ataques (detecção de ataques);
- Posicionado após o firewall, a detecção passa a ser de intrusões (detecção de intrusões) ou de erros cometidos pelos usuários internos.

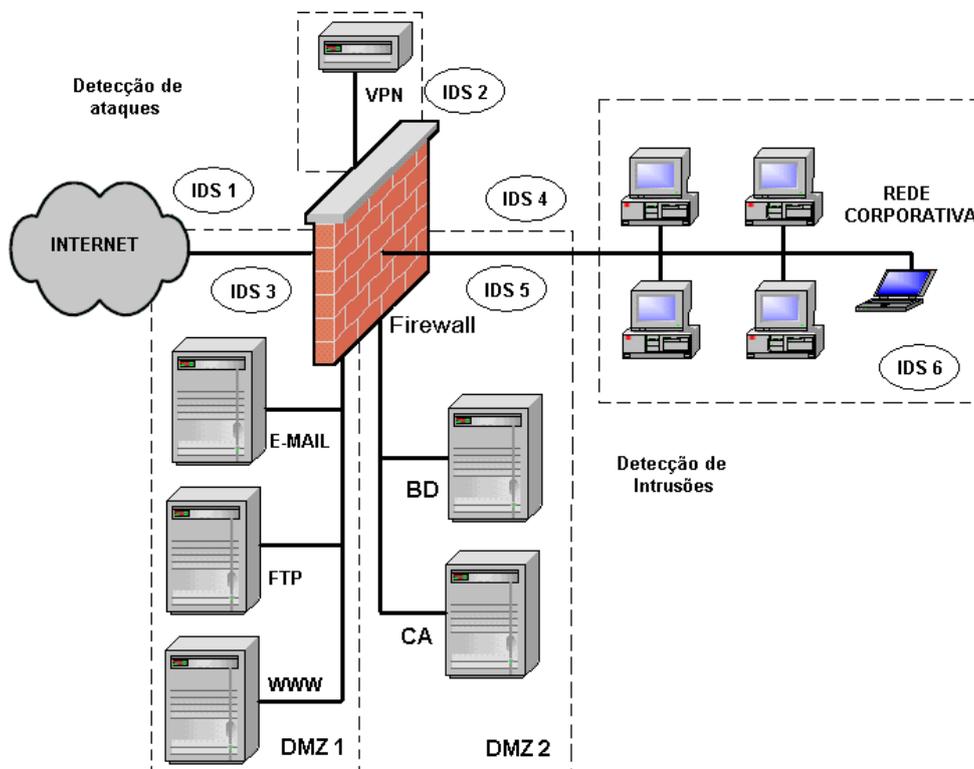


Figura 13 - Localização de IDS na rede

- **IDS 1** – detecta tentativas de ataques externos, oferecendo uma fonte de informações sobre os tipos de ameaças de intrusão para a rede corporativa;
- **IDS 2** – funciona no próprio firewall, detectando tentativas de ataque contra este;
- **IDS 3** – detecta tentativas de ataque contra os servidores localizados na DMZ 1, que conseguem passar pelo firewall;
- **IDS 4** – detecta tentativas de ataque contra recursos internos da rede que passaram pelo firewall e que podem ocorrer via VPN, por exemplo;
- **IDS 5** – detecta tentativas de ataque contra os servidores localizados na DMZ 2, que passaram pelo firewall, pela VPN ou por algum outro serviço na DMZ 1;
- **IDS 6** – detecta tentativas de ataques internos na rede corporativa.

### 3. Sistemas de Prevenção de Intrusões

O funcionamento do IDS como *sniffer*, interceptando e analisando o tráfego da rede, apresenta alguns problemas, como o fluxo de pacotes fragmentados, não confiáveis e que chegam fora de ordem. Os sistemas funcionam em modo passivo, apenas escutando o tráfego, não sendo capazes de controlar esse tráfego, seja ignorando, modificando, atrasando ou injetando pacotes para defender a rede.

A identificação desses pontos fracos, relacionados a determinados tipos de IDS, levou ao desenvolvimento de novos sistemas que buscam detectar e prevenir ataques contra a rede de comunicação. Operando de forma ativa na prevenção de intrusões, eles são conhecidos como Sistemas de Prevenção de Intrusões (*Intrusion Prevention System – IPS*).

A operação ativa difere da operação passiva na forma de capturar os pacotes dos segmentos de rede. Enquanto o IDS que opera no modo passivo capturando o tráfego do segmento de rede, o IDS que opera no modo ativo assumindo uma posição como um firewall, onde todo o tráfego da rede passa por ele (Figura 14). Essa característica permite que o IDS seja capaz de detectar os ataques e também de preveni-los, pois, os pacotes dos atacantes não chegam aos servidores da rede. A diferença entre os dois modos de operação (passivo e ativo) torna-se clara: no modo passivo, o IDS é capaz de detectar ataques, mas não é capaz de preveni-los; no modo ativo, o IDS é capaz de detectar ataques e evitá-los utilizando recursos semelhantes aos de um firewall.

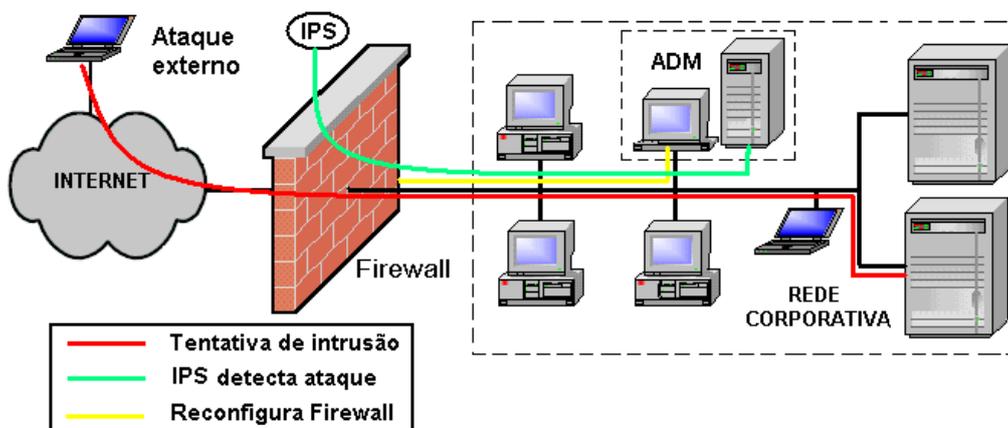


Figura 14 - Funcionamento do IPS na rede

### 3.1. Detecção de Anomalias

Uma anomalia é definida como algo diferente, anormal, peculiar ou que não seja facilmente classificado. Aplicada à segurança de computadores, uma anomalia pode ser definida como ações ou dados que não sejam considerados normais por um determinado sistema, usuário ou rede. Essa definição abrange ainda uma grande variedade de itens e pode incluir tópicos como padrões de tráfego, atividades dos usuários e comportamento de aplicativos.

#### 3.1.1. Anomalias em Padrões de Comportamento

Os sistemas que procuram por anomalias em padrões de comportamento (normalmente o comportamento de usuários) são considerados sistemas de anomalias comportamentais. Esses sistemas são normalmente de características, porém eles podem abranger também alguns critérios de estatísticas, como os tipos de aplicativos e protocolos usados em várias horas do dia, a relação entre a origem e o destino das atividades da rede ou até mesmo os tipos de anexos de e-mail que são enviados através de um sistema. A maioria dos sistemas de detecção de anomalias que se concentram em segurança normalmente se enquadra em três categorias gerais: comportamental, padrão de tráfego ou protocolo.

#### 3.1.2. Anomalias em Padrões de Tráfego

Os sistemas que procuram por anomalias em padrões de tráfego da rede são considerados sistemas de anomalias no padrão de tráfego. Esses normalmente são de natureza estatística, apesar de incluírem algumas características como volume de tráfego, mistura de protocolos e várias distribuições na origem e no destino. Pode-se considerar como vantagem o gerenciamento de uma rede que pode operar em um domínio muito maior e variado. A desvantagem é que esses sistemas frequentemente não são capazes de detectar a maioria das anomalias qualitativas ou quantitativas sutis. Eles apresentam também

algumas dificuldades na definição de uma base confiável para o desempenho da análise de estatísticas.

### 3.1.3. Anomalias em Padrões de Protocolos

Os sistemas que procuram por anomalias em padrões protocolos são considerados sistemas de anomalias de protocolos. Normalmente sistemas de características, esses tendem a variar um pouco de acordo com a implementação, mas os mais eficientes são frequentemente implementados como sistemas de modelo rígido. Esse tipo de sistema tira proveito do fato de que os protocolos sozinhos são geralmente muito restritos. Eles tendem a limitar muito a natureza e ordem das transações e são geralmente muito bem descritos por alguma implementação ou documento de referência.

Outra vantagem desse sistema é que ele pode detectar uma grande variedade de anomalias dentro do espaço do protocolo, podendo ser construído com muita eficiência. A desvantagem, porém, é que pode ser difícil de estimar o efeito da anomalia observada de forma acurada, uma vez que alguns tipos de transações de protocolo problemáticas (como ataques, por exemplo) não se manifestam como anomalias.

## 4. Segurança Integrada

Através da combinação de várias funções, a segurança integrada pode proteger com mais eficiência contra uma variedade de ameaças em cada nível para minimizar os efeitos dos ataques de rede. As tecnologias de segurança principais que podem ser integradas incluem:

- **Firewall** - Controla todo o tráfego de rede através da verificação das informações;
- **Detecção de Intrusão** - Detecta o acesso não autorizado e fornece diferentes alertas e relatórios que podem ser analisados para políticas e planejamento da segurança;
- **Filtragem de Conteúdo** - Identifica e elimina o tráfego não desejado de informação;
- **Redes Privadas Virtuais (VPN)** - Assegura as conexões além do perímetro, permitindo que organizações se comuniquem com segurança com outras redes através da Internet;
- **Gerenciamento de Vulnerabilidade** - Permite a avaliação da segurança da rede sobre falhas de segurança e sugerindo melhorias;
- **Proteção com Programas Antivírus** - Protege contra vírus, Cavalos de Tróia e outras pragas virtuais.