Análise de Firewalls

Rodrigo Rubira Branco
rodrigo@firewalls.com.br

O que é a Firewalls?

- **Empresa Especializada em Segurança.**
- **Profissionais Certificados.**
- **Atenta a Padrões Internacionais.**
- **Parceira das maiores empresas de Segurança do Mundo.**
- **Visão de Negócios e Ética Empresarial.**
- **Soluções Personalizadas para a Realidade das Empresas.**

O que a Firewalls tem?

- **Treinamentos em Segurança.**
- **Implementação de Infra-Estrutura de Redes.**
- **Implementação de Análises de Risco e Vulnerabilidades.**
- **Implementação de Detectores de Intrusão e Politicas de Segurança.**
- **Consultoria em E-commerce e Desenvolvimento.**
- **Divisão de Alta Disponibilidade e Disponibilidade Continua.**
- **HOMOLOGAÇÃO de FIREWALLS.**

Objetivos da Palestra

- **Palestra Técnica visando o público corporativo.**
- **Visa demonstrar os tipos de Firewalls existentes e as necessidades das empresas neste segmento.**
- **Auxilia na escolha de uma solução de Firewall eficiente.**
- **Demonstra o grau de perigo que as empresas correm ao adquirir soluções de empresas "não-especializadas".**

OBS: Esta palestra não ira falar sobre tipos de Hackers, Politicas de Segurança nem como invadir e sim demonstrará um paradigma da realidade atual em soluções de Firewall.

O que é Segurança?

CIDAL =

Confidencialidade
Integridade
Disponibilidade
Autenticidade
Legalidade

LEMBRAR-SE SEMPRE DISTO NO DECORRER DA PALESTRA!

Ambiente em Questão

Trabalhamos em um mundo real de sistemas mal configurados

* **Bugs de Software.**
* **Empregados Insatisfeitos.**
* **Administradores de Sistemas Sobrecarregados.**
* **Acomodação de necessidades empresariais.**
* **Falta de Educação em Segurança.**
* **B2B,B2C,B2E,C2C,X2X?**

Para que serve um Firewall

- Controlar Tráfego que entra em sua rede.
- Controlar Tráfego que sai de sua rede.
- Garantir o cumprimento de uma política de segurança.
- Melhorar o desempenho de sua rede.

Em termos gerais: Aumentar o nível de segurança de sua rede.

Onde um Firewall Atua

Perímetro

Borda fortificada de nossa rede, que pode conter:

- **Roteadores de borda.**
- **Firewalls.**
- **IDS.**
- **Dispositivos de VPN.**
- **Software.**
- **DMZ e Screened Subnets.**

Defense In-Depth

- Um Firewall apenas aumenta o nível de segurança.
- O conceito de seguranca em camadas garante que as falhas existentes em um Firewall sejam supridas por outros tipos de defesa e segurança.
- Através de diversas camadas cria-se um modelo de segurança robusto e capaz de suportar falhas.

Quando pensar em Segurança pense em uma CEBOLA.

Quem precisa de Firewall

TODOS

- Grandes Empresas.
- Médias Empresas.
- Pequenas Empresas.
- Micro Empresas.
- Faculdades, Governos, ONGs.
- Pessoas Físicas!

Tipos de Firewall

- **FirewallConnection Less (filtro de pacotes).**
- **Firewall Proxy (Firewall de aplicação).**
- **Firewall Gateway.**
- **Firewall com Estado (Stateful).**

OBS: Um equipamento pode possuir diversas destas características.

Firewall Connection Less

- Connection Less (filtro de pacotes):

Este tipo de Firewall é comumente encontrado em roteadores e tem uma utilidade na rede muito maior do que a ele geralmente atribuída.

Firewalls Stateful como veremos adiante são muito lentos em seu processamento, não devendo portanto serem deixadas regras de nível de rede simples para estes processarem.

Firewall Proxy

- Proxy (Firewall de aplicação):

Grande utilidade no controle de conteúdo, são Firewalls de camada 7 que abrem os pacotes que por ele passam para checar se cumprem determinados itens.

Considerando-se que a segurança da informação deve contemplar não apenas a entrada da rede, como também sua saída, possuem valor inestimável em um projeto de segurança.

Firewall Gateway

- **Firewall Gateway:**

Máquinas que podem possuir um antivírus e seu único objetivo é receber os pacotes em uma interface entrante, passar antivírus e encaminhá-lo a outra interface, não fazendo filtragens de outro tipo.

Firewall Stateful

- **Firewall Stateful:**

Podereso sistema Firewall que se "lembra" das conexões entrantes, evitando os chamados "Stealth Scans".

Stealth Scan

- Tipo de ataque que visa passar por Firewalls que não sejam Stateful.
- Utiliza-se de algumas características inerentes a conexões TCP:

Flags:

SYN – Iniciar conexão.
FIN – Terminar conexão normalmente.
URG – Campo URG possui dados.
ACK – Aceitar conexão.
PSH – Dar prioridade a este pacote.
RST – Terminar conexão caso haja erros.

O ataque Stealth simplesmente envia um pacote com o Flag ACK ativo sem haver enviado um pacote com o flag SYN (iniciar conexão).

Com isto, alguns Firewalls creem ser este um pacote de retorno e permitem que passe.

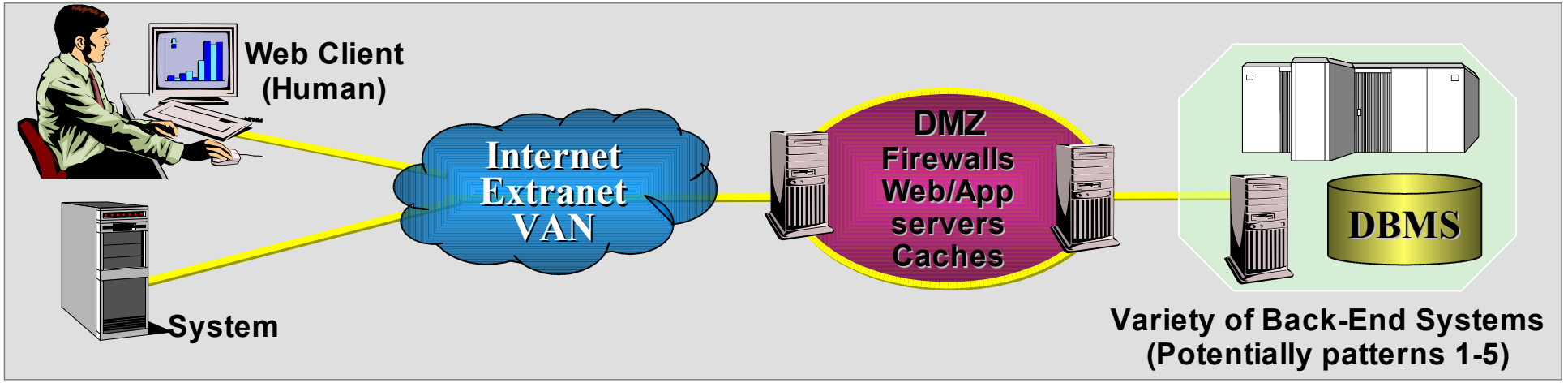
E nossos servidores?

Servidores são equipamentos que provem algum tipo de informação a usuários externos (sejam da própria empresa ou de outras empresas).

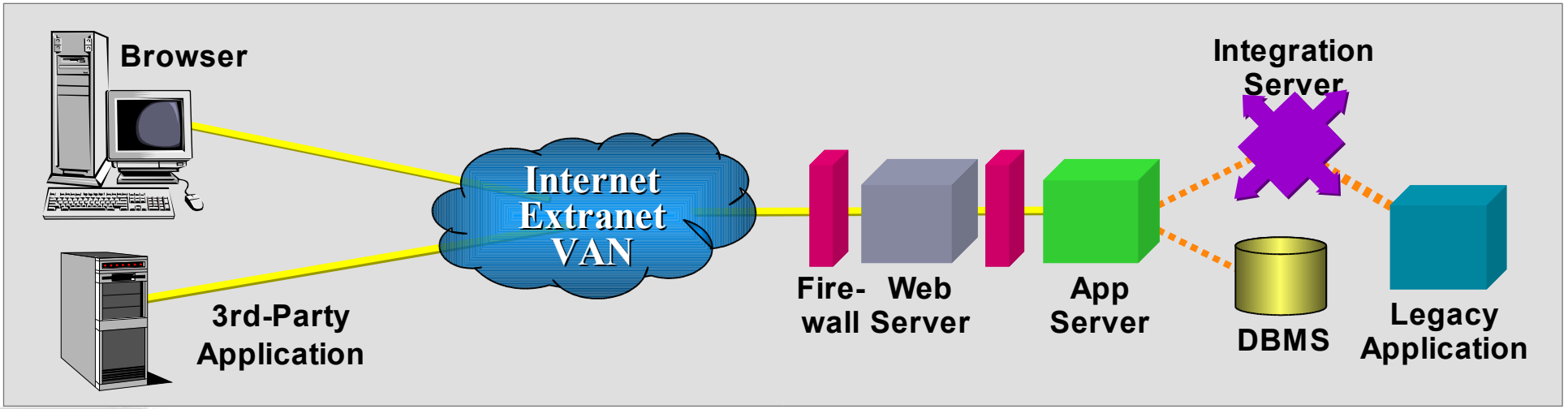
Podem e devem ser protegidos pelo Firewall e isolados da Rede Interna!

DMZ x Screened

DMZ



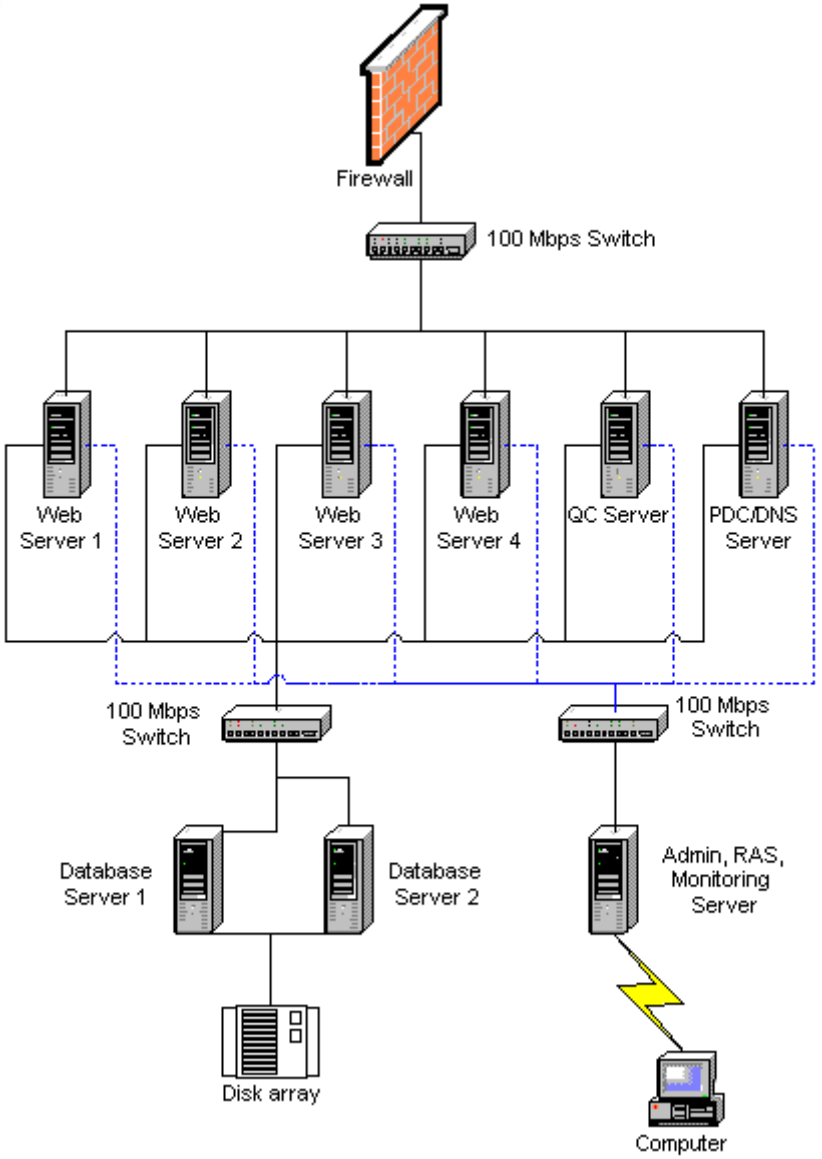
Screened Subnet



Screened Subnet

- Confunde-se com DMZ!

- Isola-se através do Firewall uma rede protegida.



Fornecedores de Firewall

Fornecedores de Firewalls:

* **CheckPoint.**
* **NetScreen.**
* **NetFilter (linux).**
* **Ipf (FreeBSD/Linux).**
* **Microsoft (ISA Server).**
* **Securepoint.**
* **Cisco.**
* **Symantec.**
* **CA.**

Limitações de um Firewall

ENORMES!

- Códigos Maliciosos.
- Vírus.
- Roubos de Informações.
- Explorações em Serviços Permitidos.
- DoS e DdoS.

Outras Soluções

Adiantando-se ao ataque!

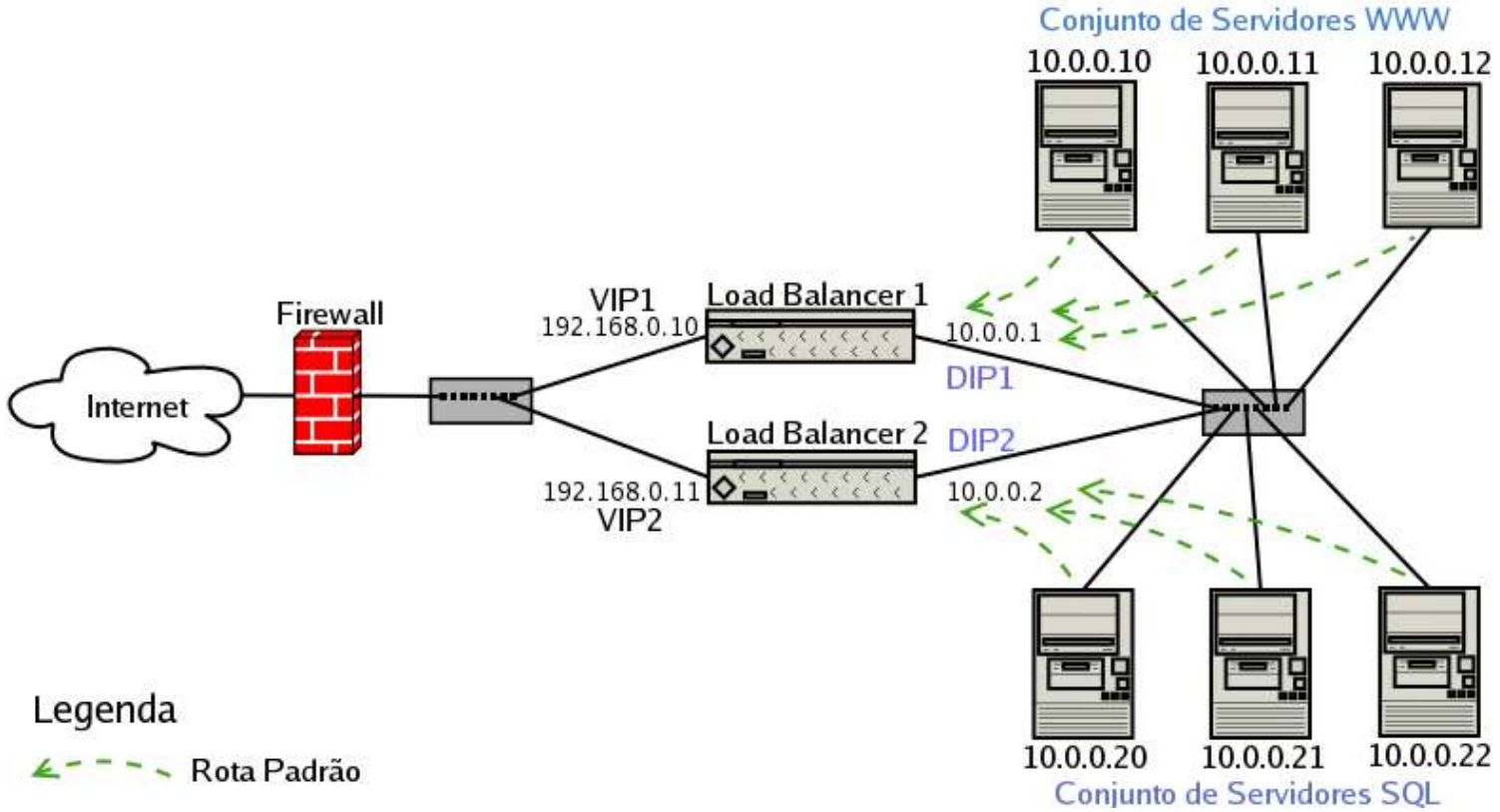
- **IDS (Intrusion Detection System).**
- **Análises de Vulnerabilidades.**
- **Honeynets.**
- **Fortificação de Hosts.**
- **(re)Estruturação da Rede.**

Firewall Redundante

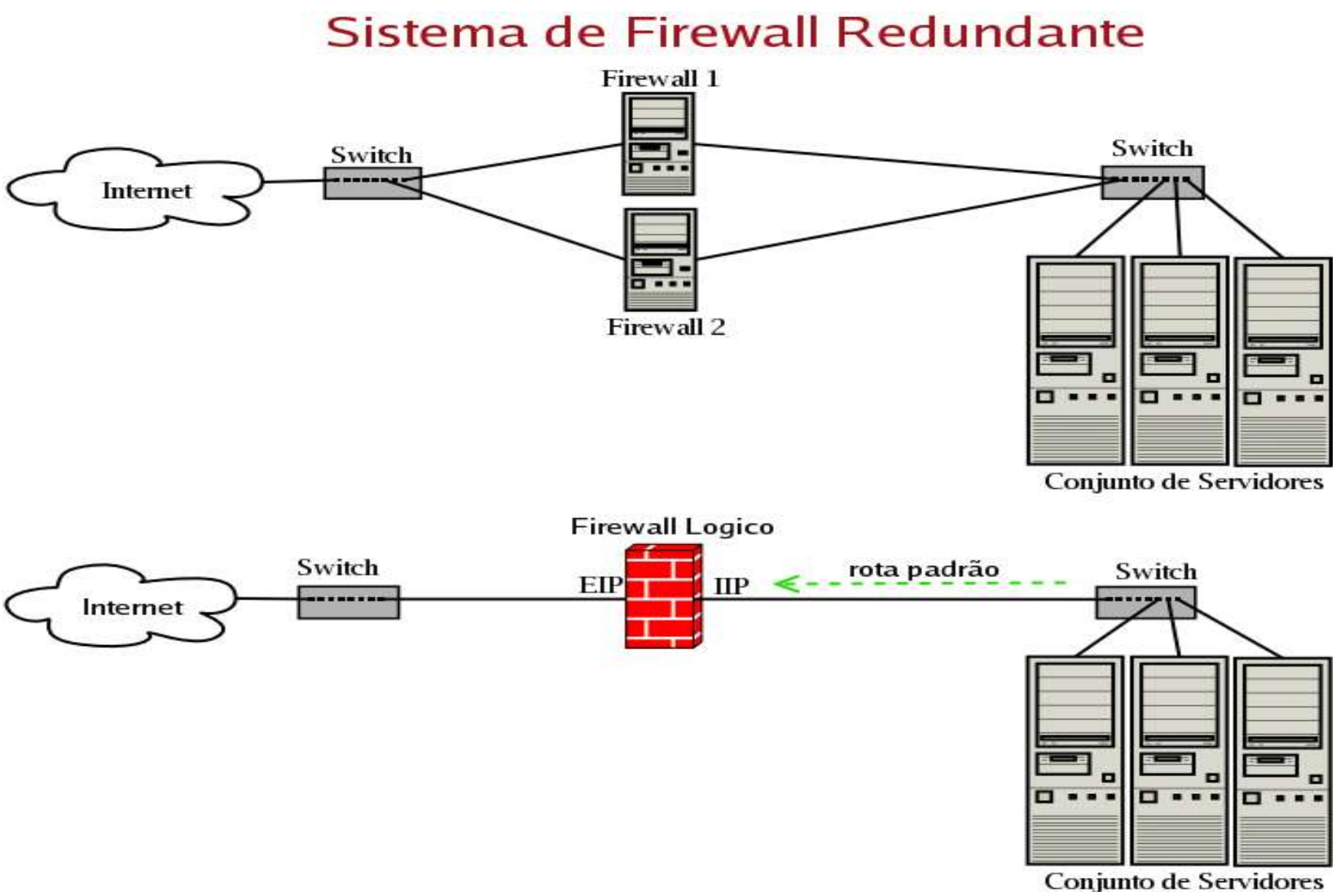
- **Evitar o número de quedas do sistema.**
- **Aumentar a resistência a ataques DoS e DdoS.**
- **Garantir maior desempenho da rede.**
- **Aumentar o ponto de gargalo.**
- **Dividir links e balancear carga.**

Firewall Redundante

Sistema com Balanceamento de Conexões



Firewall Redundante



Homologação de Firewalls

- Garante que a solução de Firewall possui o desempenho necessário.

- Garante a melhor prática de implementação do serviço contratado.

- Oferecido por uma empresa independente da solução contratada.

- Segue normas internacionais e RFCs como padrão.

- Pode ser contratado pelo cliente final, exigido pelo mesmo ou obtido por prestadores de serviço.

FIM! Será mesmo?

DÚVIDAS?!?

Rodrigo Rubira Branco
rodrigo@firewalls.com.br