

**Só Firewall  
Não Resolve!**

# Bem Vindos!

Palestrante:

**Rodrigo Ribeiro Montoro**

*Analista de Segurança da BRconnection®*



**POR GENTILEZA, MANTENHAM SEUS CELULARES  
DESLIGADOS DURANTE A APRESENTAÇÃO.  
OBRIGADO!**

# Gerenciando Riscos em Comunicação de Dados



### → **Analista de Segurança**

- Testes de Invasão
- Auditoria dos Produtos BRconnection®

### → **Certificados**

- RHCE
- LPI
- SnortCP

# **Só Firewall Não Resolve!**

- ***Empresa***
- ***Camadas de Segurança***
- ***Ataques***
- ***Infra-estrutura***
- ***Firewall***
- ***Proteção / Monitoramento de Rede***
- ***Proteção / Monitoramento de Hosts***



# Só Firewall Não Resolve!

BRconnection®

- **BRMA®**
- **messengerPOLICY®**
- **smartWEB®**
- **Servidores Demo no Stand da BRconnection®**

# Só Firewall Não Resolve!

## Camadas de Segurança

- Física
- Lógica
- Humana

## → **Acessos**

- Empresa
- Sala de Servidores

## → **Controles**

- Entrada / Saída de Pessoas
- Entrada / Saída de Materiais

→ ***Celulares, Pen Drives, Modems e etc.***

## → *Servidores*

- WEB / SMTP / FTP
- Arquivos
- Banco de Dados

## → *Desktop*

- Browser
- Sistema Operacional

→ *IPSEC, HTTPS, IMAPS, SSL, Tunelamentos, SMTPS e etc.*

# **Só Firewall Não Resolve!**

*Humana*

- **Telefone**
- **E-Mail**
- **Instant Messaging**
- **Anotações**
- **Funcionários Externos**
- **Lixo**



**BRCONNECTION<sup>®</sup>**  
INTERNET CONTROLADA

# Só Firewall Não Resolve!

Ataques

- **Funcionários Internos**
- **Worms**
- **Phishing**
- **Trojans**
- **Engenharia Social**
- **Vulnerabilidades**



**BRCONNECTION**<sup>®</sup>  
INTERNET CONTROLADA

# **Só Firewall Não Resolve!**

*Quanto vale o conhecimento?*

- **Trojan (Shell) - US\$ 350,00 - US\$700,00**
- **Trojan (Roubo de Senhas) - US\$600,00**
- **Listagem E-mail (32 milhões) - US\$1.500,00**
- **Milhões de Usuários do ICQ - US\$150,00**
- **Proteção Contra Detecção do Trojan - US\$20,00**
- **Suporte**

- **Auto Propagação**
- **Code Red (2001) - US\$ 2,6 bilhões**
- **Slammer (2003) - US\$ 950 milhões a US\$ 2 bilhões**
- **Blaster (2003) - US\$ 2 bilhões a US\$ 10 bilhões**
- **Sasser (2004) - US\$ 18 bilhões**

# **Só Firewall Não Resolve!**

*Phishing*

- ***E-mail***
- ***Links para Sites Falsos***
- ***Roubo de Identidade***
- ***Mercado Milionário***



**BRCONNECTION<sup>®</sup>**  
INTERNET CONTROLADA

[http://www.GRANDESEARCH.com/pagead/iclck?sa=l&ai=Br3ycNQz5Q=fXBJGSiQLU0eDSAueHkArnhtWZAu=FmQWgjlKQAxgFKAg4AEDKEUiFOVD=4r2f=P\\_\\_\\_\\_\\_8BoAGyqor\\_A8gBAZUCCapCCqkCxU7NLQH0sz4&num=5&adurl=%68%74%74%70%3a%2f%2f%77%77%77%2e%68%61%63%6b%65%72%2e%63%6f%6d%2f%74%72%6f%6a%61%6e%2e%65%78%65](http://www.GRANDESEARCH.com/pagead/iclck?sa=l&ai=Br3ycNQz5Q=fXBJGSiQLU0eDSAueHkArnhtWZAu=FmQWgjlKQAxgFKAg4AEDKEUiFOVD=4r2f=P_____8BoAGyqor_A8gBAZUCCapCCqkCxU7NLQH0sz4&num=5&adurl=%68%74%74%70%3a%2f%2f%77%77%77%2e%68%61%63%6b%65%72%2e%63%6f%6d%2f%74%72%6f%6a%61%6e%2e%65%78%65)

**Só Firewall  
Não Resolve!**

*Onde fui parar?*

**Vale um Brinde !**

<http://www.hacker.com/trojan.exe>

[http://www.GRANDESEARCH.com/pagead/iclck?sa=l&ai=Br3ycNQz5Q=fXBJGSiQLU0eDSAueHkArnhtWZAu=FmQWgjl kQAxgFKAg4AEDKEUiFOVD=4r2f=P\\_\\_\\_\\_8BoAGyqor\\_A8gB AZUCCapCCqkCxU7NLQH0sz4&num=5&adurl=%68%74%74%70%3a%2f%2f%77%77%77%2e%68%61%63%6b%65%72%2e%63%6f%6d%2f%74%72%6f%6a%61%6e%2e%65%78%65](http://www.GRANDESEARCH.com/pagead/iclck?sa=l&ai=Br3ycNQz5Q=fXBJGSiQLU0eDSAueHkArnhtWZAu=FmQWgjl kQAxgFKAg4AEDKEUiFOVD=4r2f=P____8BoAGyqor_A8gB AZUCCapCCqkCxU7NLQH0sz4&num=5&adurl=%68%74%74%70%3a%2f%2f%77%77%77%2e%68%61%63%6b%65%72%2e%63%6f%6d%2f%74%72%6f%6a%61%6e%2e%65%78%65)

<http://grandeportalnacional.com.br/Redirector.aspx?bstat=terrastats01&type=CK&source=buscador.terra.com.br&id=sponsored&partner=google&query=nike&position=1&target=%68%74%74%70%3a%2f%2f%77%77%77%2e%62%72%63%2e%63%6f%6d%2e%62%72%2f%76%69%72%75%73%33%2e%65%78%65>

[http://outrograndesearch.com/\\_ylt=A0geum1Mv9RGw4EB6FXz6Qt./SIG=129lovkbd/EXP=1188434124/\\*\\*%68%74%74%70%3a%2f%2f%77%77%77%2e%62%72%63%2e%63%6f%6d%2e%62%72%2f%68%61%63%6b%65%72%32%2e%65%78%65](http://outrograndesearch.com/_ylt=A0geum1Mv9RGw4EB6FXz6Qt./SIG=129lovkbd/EXP=1188434124/**%68%74%74%70%3a%2f%2f%77%77%77%2e%62%72%63%2e%63%6f%6d%2e%62%72%2f%68%61%63%6b%65%72%32%2e%65%78%65)

- **Acesso Posterior / Shell Reverso**
- **Roubo de Dados / Controle do Computador**
- **Exemplos**
  - Netbus / BackOrifice
  - Específicos (Difícil Detecção)
  - Key Logger
  - Servidores DNS Falsos
- **Kits faça você mesmo!**



- **O lado mais Vulnerável**
  
- **Interesse em Sempre ser Prestativo (especialmente funcionários novos)**
  
- **Vazamento de Senhas / Informações**
  - **Senhas de E-mails / Sistemas (acesso remoto)**
  - **Softwares Utilizados**
  
- **Falta de Metodologia Transmitir as Informações**
  
- **Sites de Networking (Orkut , Via6 e etc.)**

- **Updates de Softwares**
  - Servidores
  - Estações
- **Acesso à Empresa**
  - Sala de Servidores
  - Senhas / Anotações Esquecidas Sobre as Mesas
- **Erros de configurações**
  - Complexidade de Softwares e/ou da Rede
  - Senhas Fracas

- **Posicionamento**
  - Firewall / NIDS / NIPS
- **Perímetro**
- **Controles**
  - Autenticação
  - Switches
- **Hardwares**



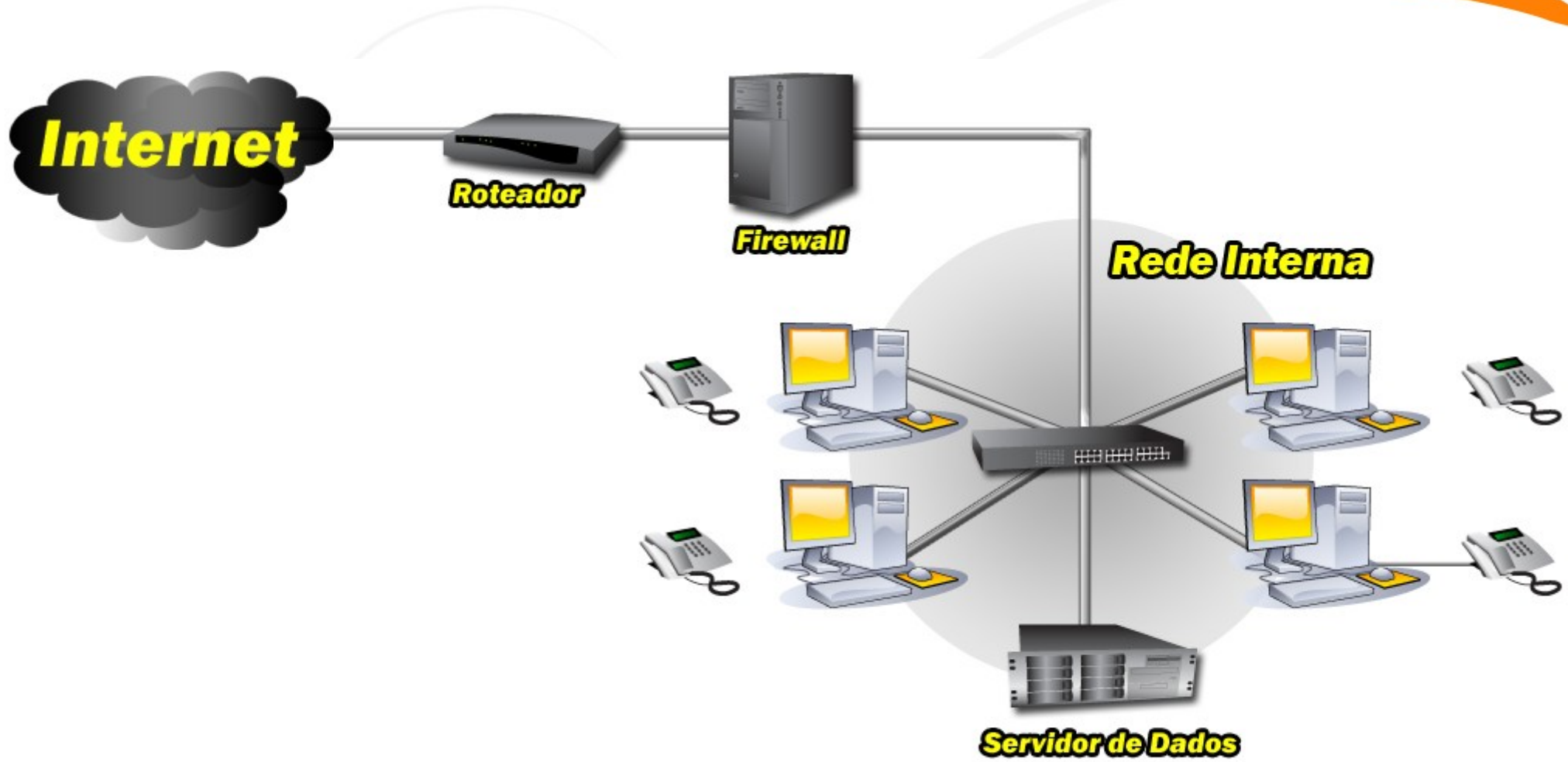
# Só Firewall Não Resolve!

Você conhece seu Hardware?



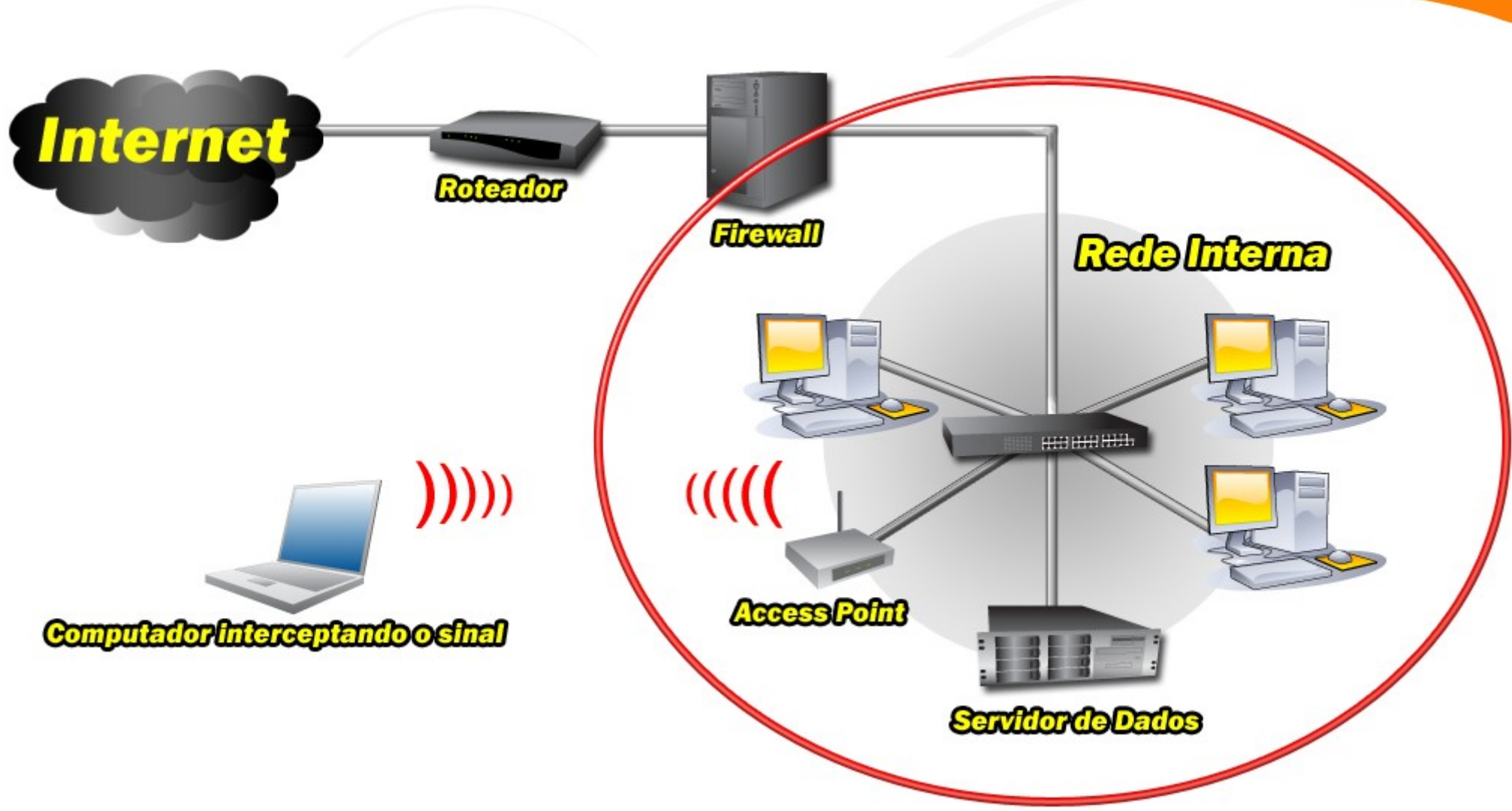
# Só Firewall Não Resolve!

Onde está a falha?



# Só Firewall Não Resolve!

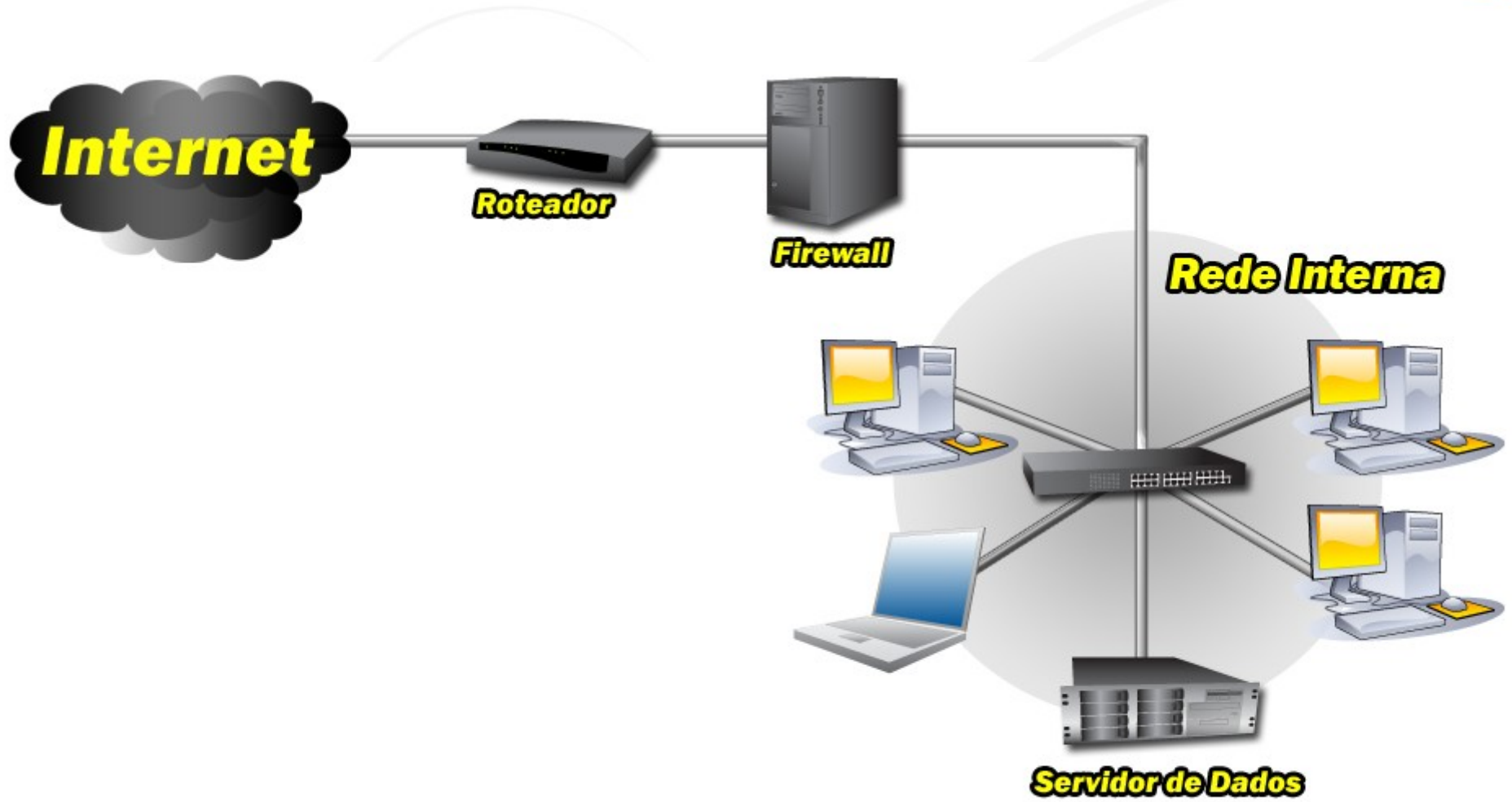
Wireless



- **Segundo Informações o Motivo Inicial da Invasão (wireless)**
- **Prejuízo de US\$150 milhões**
- **Fora do Compliance PCI DSS**
- **Aproximadamente 46 milhões de números de cartões de crédito roubados**
- **Falhas de Infra-estrutura e Monitoramento**

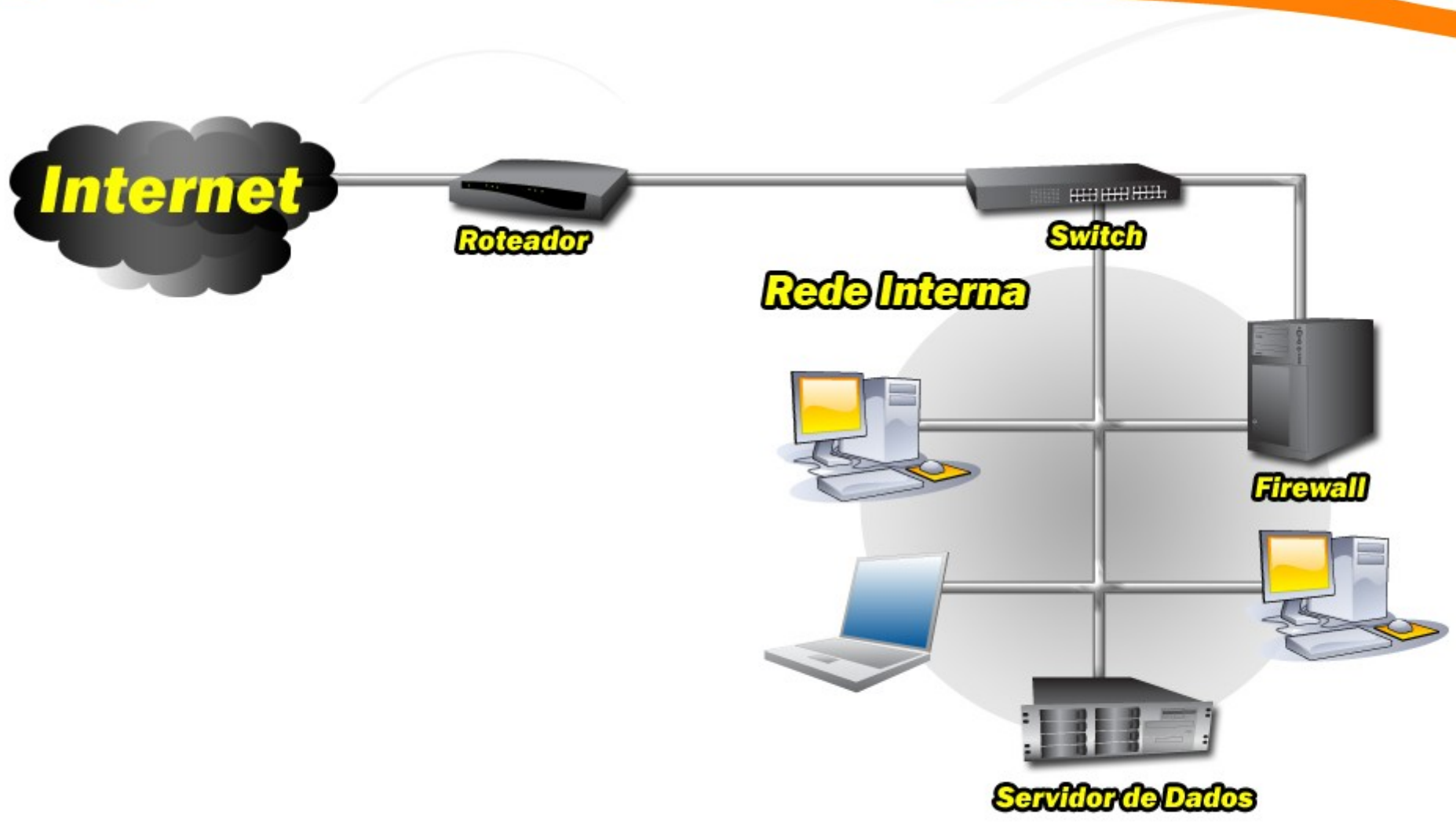
# Só Firewall Não Resolve!

Laptop: Entrada ou saída de problemas?



# Só Firewall Não Resolve!

Link direto no switch?



### → **Fotos**

- Senhas
- Telas

### → **Filmagens**

- Senhas
- Conversas entre Funcionários / Conversas Telefônicas

### → **Internet Via Celular**

# Como minimizar os impactos?

- ***NIDS (Network Intrusion Detection System)***
- ***NIPS (Network Intrusion Prevention System)***
- ***NSM (Network Security Monitoring)***

- **Sistema Passivo**
- **Análise de “Malwares”**
  - Vírus
  - Worms
  - Trojans
  - Necessidades Específicas
- **Alertas**
  - Tentativas de Invasão
  - Reconhecimento da Rede
  - Tráfego Suspeito

# Só Firewall Não Resolve!

NIPS (Network Intrusion Prevention System)

- **Analisar / Detectar / Reportar**
- **Sistema Ativo**
  - Bloqueia
  - Redireciona
- **Camada de Aplicação**
- **“Proxy”**

- **Coleta de Dados**
  - IDS
  - IPS
  - Routers / Switches / Wireless
- **Tráfego Interno**
- **Gerenciamento de Logs**

- **HIDS (Host Intrusion Detection System)**
- **HIPS (Host Intrusion Prevention System)**
- **HSM (Host Security Monitoring)**

### → *Atividades do Host*

- Keyloggers
- Spywares
- Botnets
- Rootkits

### → *Monitoramento do Sistema de Arquivos (HIMS)*

### → *Registro do Sistema*

- **Local**
- **Tráfego Criptografado / Não Criptografado**
- **Políticas**
  - **Quarentena**
  - **Bloqueio do Computador**

### → **Inventários**

- **Softwares (Acrobat®, Flash®, browsers, plugins e etc.)**
  - Atualizações
  - Utilização
- **Hardwares (modems , USB's, gravadores de CD e etc.)**

### → **Análise de Logs**

- **Local (real-time)**
- **Direcionar para um Servidor de Logs Centralizado**

- **Educação dos Funcionários**
- **NIDS / NIPS / HIDS / HIMS / HIPS**
- **Controle de Acessos (físico / lógico)**
- **Gerenciamento de Patches (atualizações)**
- **Câmeras, Telefones (fixo / celulares), Laptops e outros Dispositivos Portáteis**
- **Logs Servem para Serem Analisados!**



**Rodrigo Montoro**

***rodrigo@brc.com.br***

***www.brc.com.br***

***Visite-nos no Stand da BRconnection®***

BRconnection®, BRMA®, messengerPOLICY® e smartWEB® são marcas registradas da BRconnection.  
Qualquer outra marca ou nome de empresa citado aqui deve ser registrado pelos seus respectivos proprietários.