

Sistemas de Firewall



João Eriberto Mota Filho

Campinas, SP, 06 mai. 2014

Sistemas de Firewall

1. Introdução

2. Conceitos

- > O modelo OSI
- > Roteamento de rede x bridges
- > Sistemas de firewall
- > Criptografia x firewalls

3. Conclusão

Sistemas de Firewall

1. Introdução

2. Conceitos

- > O modelo OSI
- > Roteamento de rede x bridges
- > Sistemas de firewall
- > Criptografia x firewalls

3. Conclusão

Sistemas de Firewall

Introdução



A quem pertence esta mão? Ela está fechando ou está abrindo?

Sistemas de Firewall

1. Introdução

2. Conceitos

- > **O modelo OSI**

- > Roteamento de rede x bridges

- > Sistemas de firewall

- > Criptografia x firewalls

3. Conclusão

Sistemas de Firewall

O modelo OSI

Camada 7 - Aplicação

Camada 6 - Apresentação

Camada 5 - Sessão

Camada 4 - Transporte

Camada 3 - Rede

Camada 2 - Enlace

Camada 1 - Física

- ✓ Open Systems Interconnection.
- ✓ Possui 7 camadas, numeradas de baixo para cima.
- ✓ Criado para prover compatibilidade entre produtos de rede de fabricantes diferentes.
- ✓ O seu entendimento é fundamental para o estudo dos sistemas de firewall.
- ✓ Um tráfego de rede nem sempre atingirá as camadas superiores.

Sistemas de Firewall

O modelo OSI

Camada 7 - Aplicação

→ http, ftp, smtp, pop-3 etc.

Camada 6 - Apresentação

Camada 5 - Sessão

Camada 4 - Transporte

→ Protocolos TCP e UDP.

Camada 3 - Rede

→ Endereço IP e roteamento rede.

Camada 2 - Enlace

→ Endereço MAC, bridge, switch.

Camada 1 - Física

Sistemas de Firewall

1. Introdução

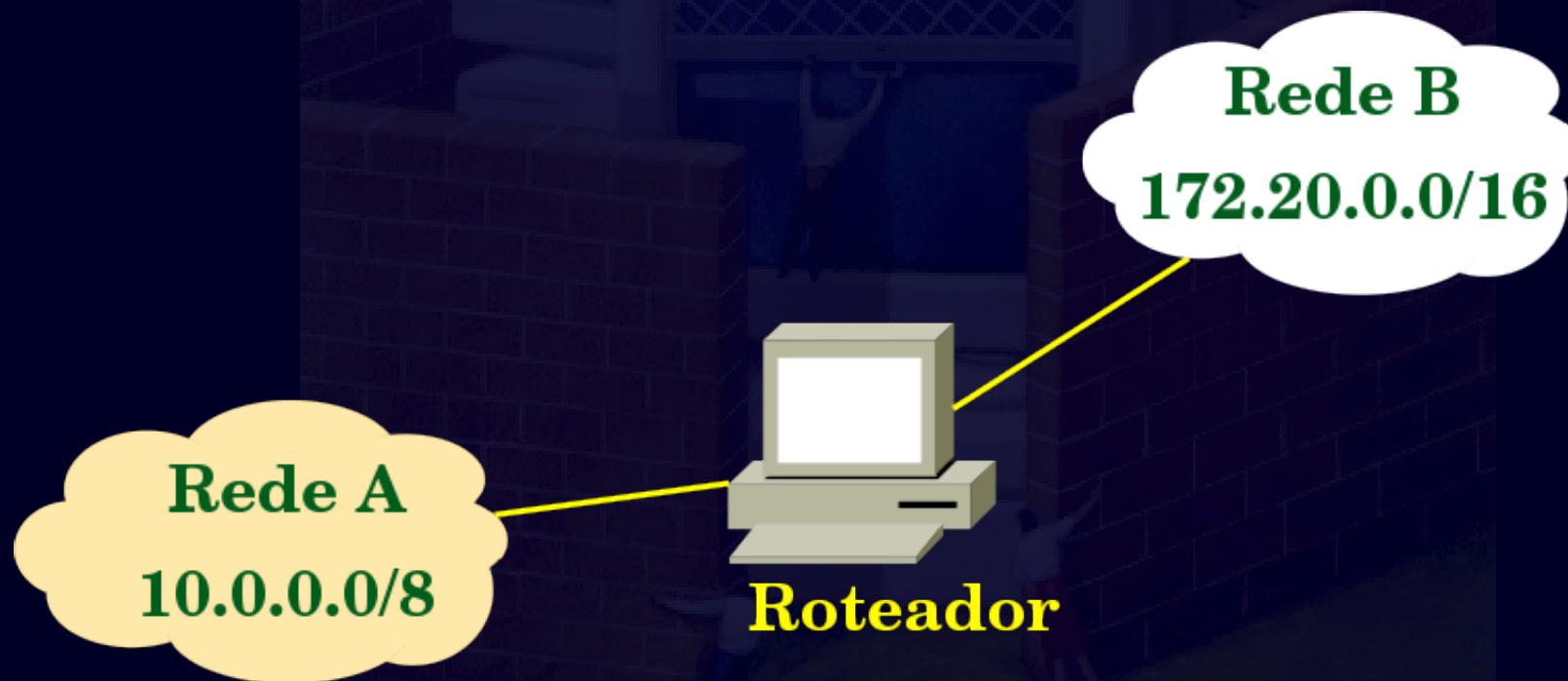
2. Conceitos

- > O modelo OSI
- > **Roteamento de rede x bridges**
- > Sistemas de firewall
- > Criptografia x firewalls

3. Conclusão

Roteamento de rede

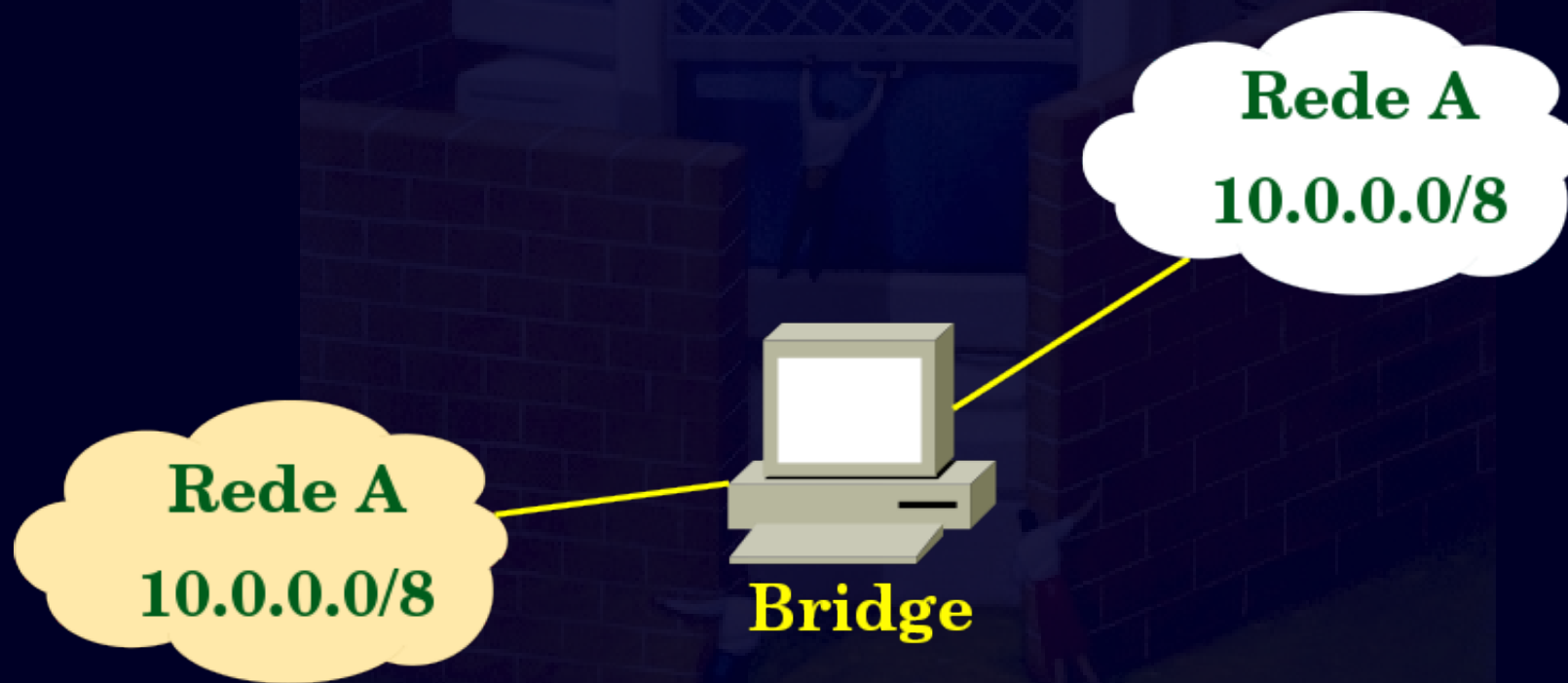
- ✓ O roteamento é utilizado para interligar segmentos de rede diferentes, via camada de rede do modelo OSI (camada 3).



Sistemas de Firewall

As bridges

- ✓ As bridges possuem diversas funções, dentre elas, interligar porções diferentes da mesma rede, de forma transparente, via camada de enlace do modelo OSI (camada 2).



Sistemas de Firewall

1. Introdução

2. Conceitos

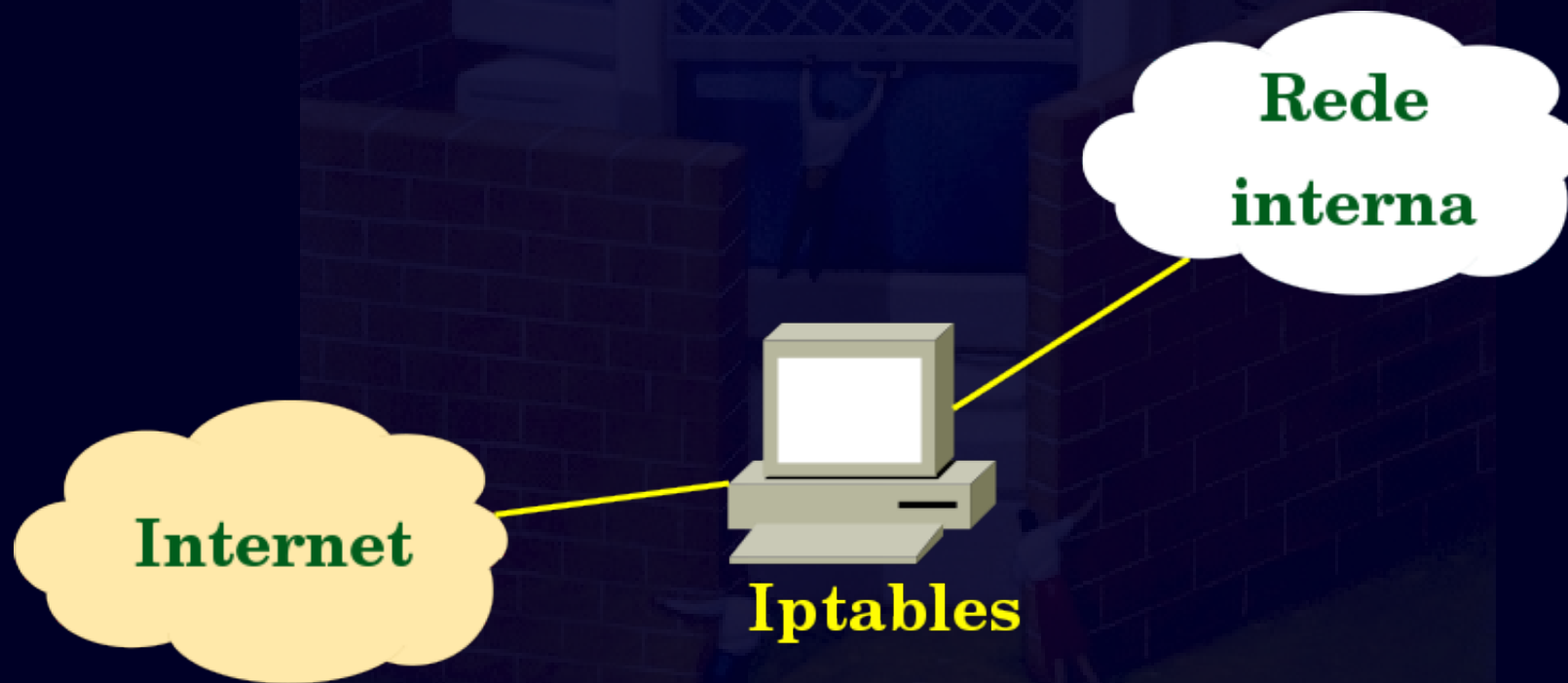
- > O modelo OSI
- > Roteamento de rede x bridges
- > **Sistemas de firewall**
- > Criptografia x firewalls

3. Conclusão

Sistemas de Firewall

Um simples exemplo...

Esta rede possui um firewall???



Sistemas de firewall

- ✓ Firewall é um sistema. É todo o esforço físico e lógico voltado para a segurança da rede.
- ✓ Os sistemas de firewall podem ser compostos por diversos elementos, como filtros de pacotes, filtros de estados, proxies (forward e reverso), IDS, IPS, HIDS, antivírus de rede, verificadores de integridade etc.
- ✓ A segurança em profundidade é fundamental em sistemas de firewall (teoria da cebola).
- ✓ Não é possível ter um sistema de firewall apenas com uma máquina.
- ✓ **IMPORTANTE:** segurança é inversamente proporcional ao conforto. Exemplo: sites de bancos.

Elementos de firewall

- ✓ **Filtros de pacotes:** atuam nas camadas 2, 3 e 4 do modelo OSI, filtrando endereços IP, portas, protocolos IP etc.
- ✓ **Filtros de estados:** entendem estados de conexão (camada 4).
- ✓ **Proxy:** entende protocolos da camada 7 e atua como intermediário em conexões cliente – servidor, evitando o contato direto entre eles. Podem ser dos tipos forward ou reverso.
- ✓ **IDS (Intrusion Detection System):** entendem o payload da camada 7. Criam logs de ações suspeitas. São detalhistas e consomem muitos recursos computacionais. Costumam gerar falsos positivos.
- ✓ **IPS (Intrusion Prevention System):** similares aos IDS mas bloqueiam tráfego. São mais precisos. Falsos não devem ocorrer.
- ✓ **HIDS:** IDS que funciona em máquinas finalísticas.
- ✓ **Verificador de integridade:** aponta mudanças no filesystem.

Alguns exemplos de elementos de firewall

- ✓ Filtros de pacotes: Netfilter (Iptables), ebtables e PF.
- ✓ Filtros de estados: Netfilter (Iptables) e PF.
- ✓ IDS: Snort, Suricata e Labrea.
- ✓ IPS: HLBR (extinto) e Snort In-Line.
- ✓ Proxy: Squid, totd, qpsmtpd, apt-cache search proxy :-)
- ✓ Port scan detector: psad e PortSentry.
- ✓ Monitor de login: fail2ban.
- ✓ Antivírus: Clamav.
- ✓ Verificadores de integridade: Fcheck, iwatch, Samhain e AIDE.
- ✓ Outros: apt-cache search firewall / apt-cache search honey.

Sistemas de Firewall

Elementos de firewall x modelo OSI

Camada 7 - Aplicação

→ proxies, (H)IDS, IPS, antivírus etc.

Camada 6 - Apresentação

Camada 5 - Sessão

Camada 4 - Transporte

→ filtros, proxies, IDS, IPS etc.

Camada 3 - Rede

→ filtros, proxies, IDS, IPS etc.

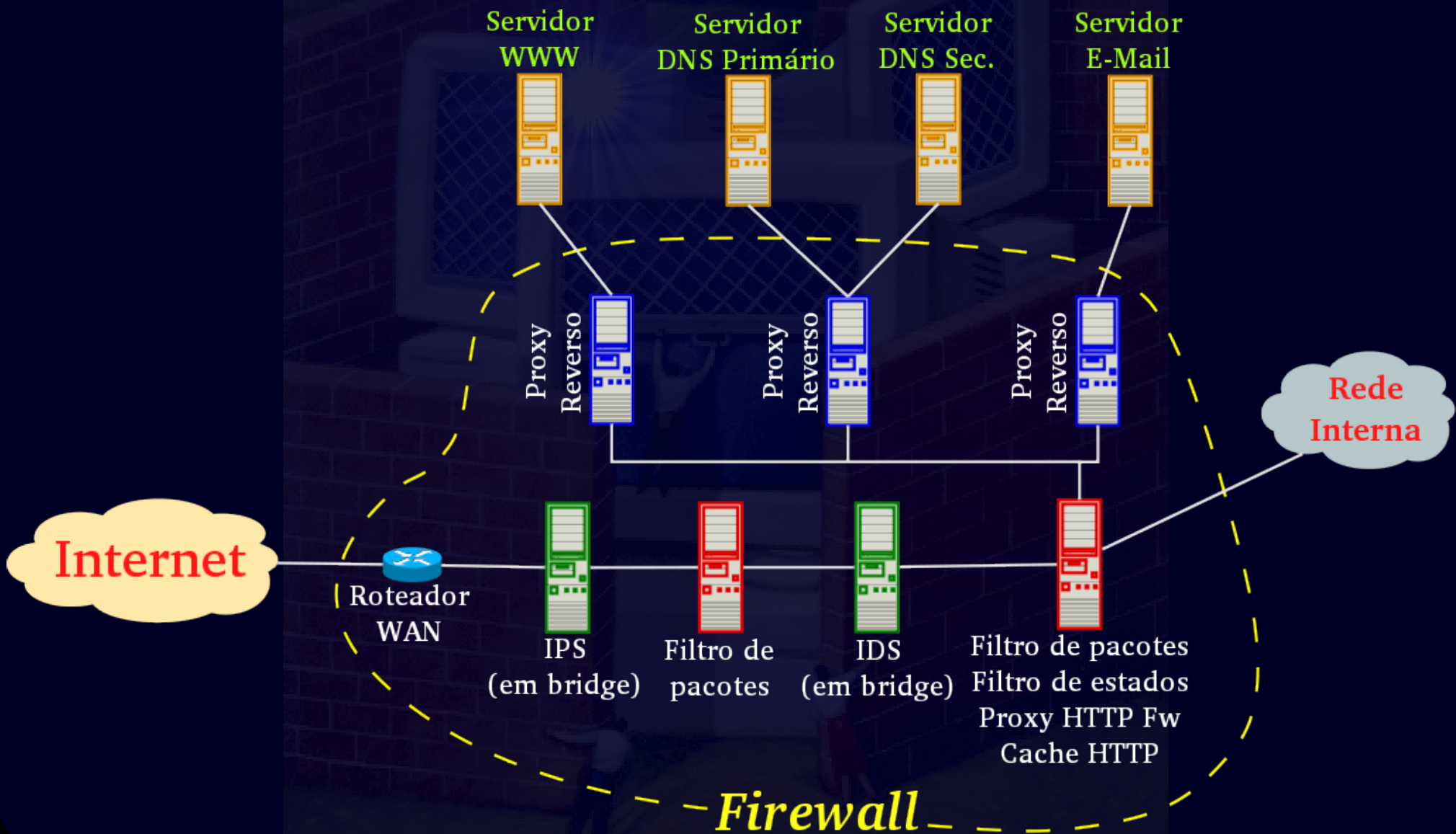
Camada 2 - Enlace

→ filtros, IPS (scrubbers).

Camada 1 - Física

Sistemas de Firewall

Um exemplo simples de sistema de firewall



Sistemas de Firewall

Sistemas de firewall

- ✓ Única solução 100% confiável e eficiente para a segurança em redes de computadores:

DEUS

Sistemas de Firewall

1. Introdução

2. Conceitos

- > O modelo OSI
- > Roteamento de rede x bridges
- > Sistemas de firewall
- > **Criptografia x firewalls**

3. Conclusão

Criptografia x firewalls

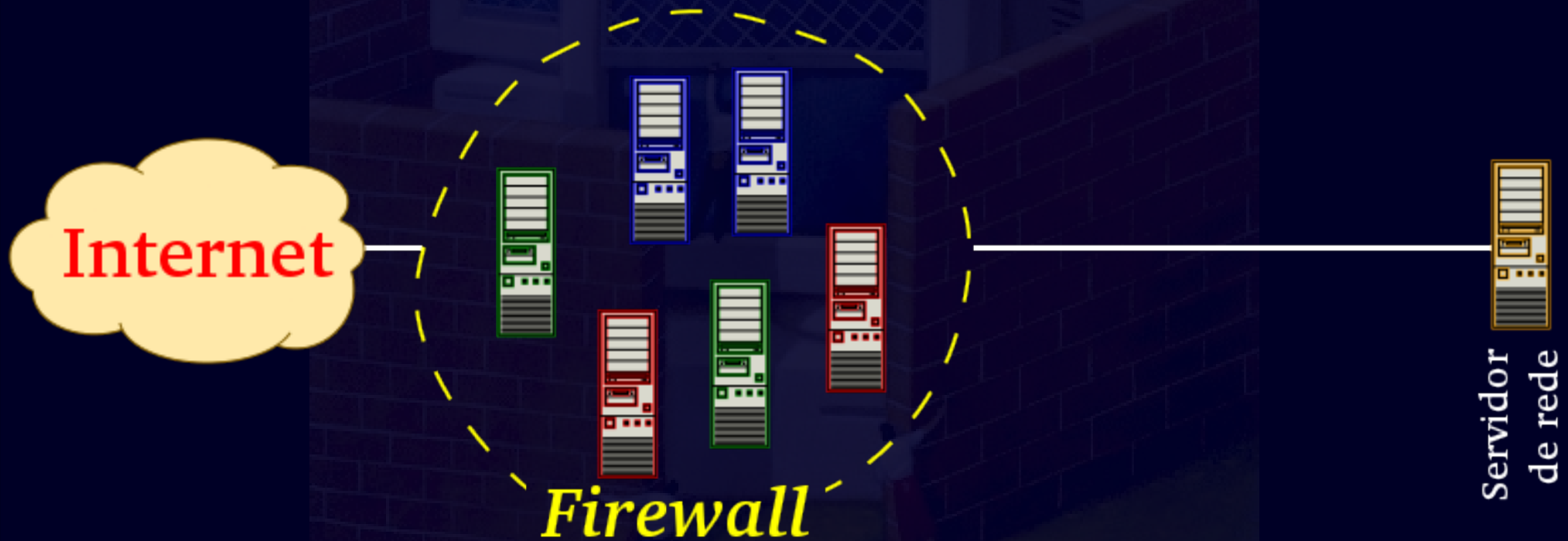
Criptografia é uma boa solução
para a segurança?

Criptografia x firewalls

- ✓ A criptografia cria um canal cliente - servidor. Esse canal não pode ser entendido por quem está no meio do caminho.
- ✓ A criptografia CEGA o sistema de firewall.
- ✓ A criptografia provê segurança para o usuário.
- ✓ A criptografia em servidores poderá causar insegurança na rede e o seu uso deverá ser feito mediante extrema necessidade.
- ✓ Uma solução: criptografia até os proxies reversos e elementos de firewall entre os reversos e os servidores.

Sistemas de Firewall

Criptografia x firewalls



Sistemas de Firewall

Criptografia x firewalls



Sistemas de Firewall

Criptografia x firewalls

Solução

=

proxy reverso

Internet



Firewall



Servidor
de rede

Sistemas de Firewall

Criptografia x firewalls

Solução

=

proxy reverso



Sistemas de Firewall

Criptografia x firewalls

Solução

=

proxy reverso



Sistemas de Firewall

1. Introdução

2. Conceitos

- > O modelo OSI
- > Roteamento de rede x bridges
- > Sistemas de firewall
- > Criptografia x firewalls

3. Conclusão

Conclusão

- ✓ Firewall é um sistema e não uma máquina.
- ✓ É um esforço integrado para prover segurança em uma rede de computadores.
- ✓ A defesa em profundidade é essencial para garantir a segurança do próprio sistema de firewall.
- ✓ Não existe rede 100% segura.
- ✓ Criptografia só deve ser utilizada quando for extremamente necessário e a sua adoção requer cuidados especiais.

Esta palestra está disponível em:

<http://eriberto.pro.br>

Siga-me no Twitter @eribertomota