Sistemas de Firewall

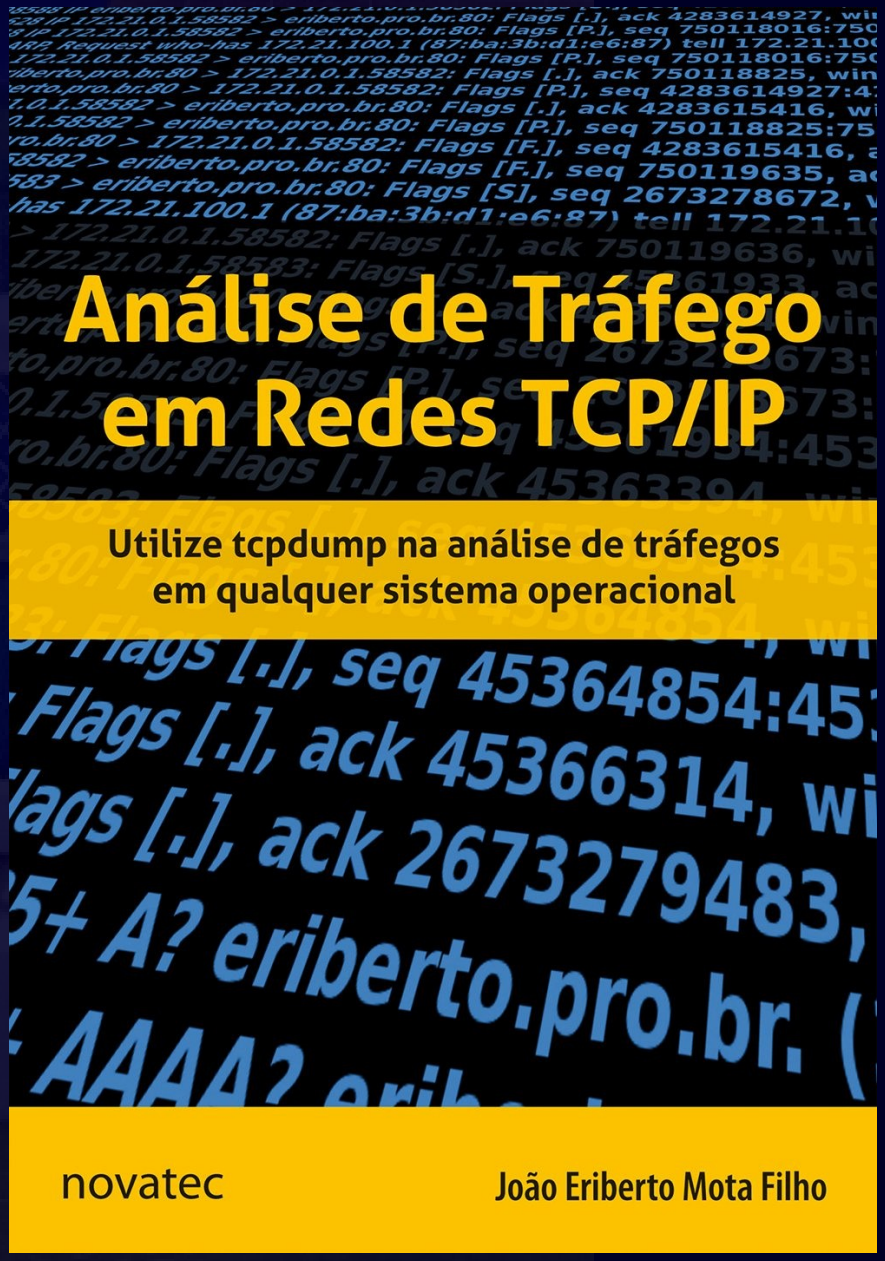
João Eriberto Mota Filho

Brasília, DF, 29 set. 2022

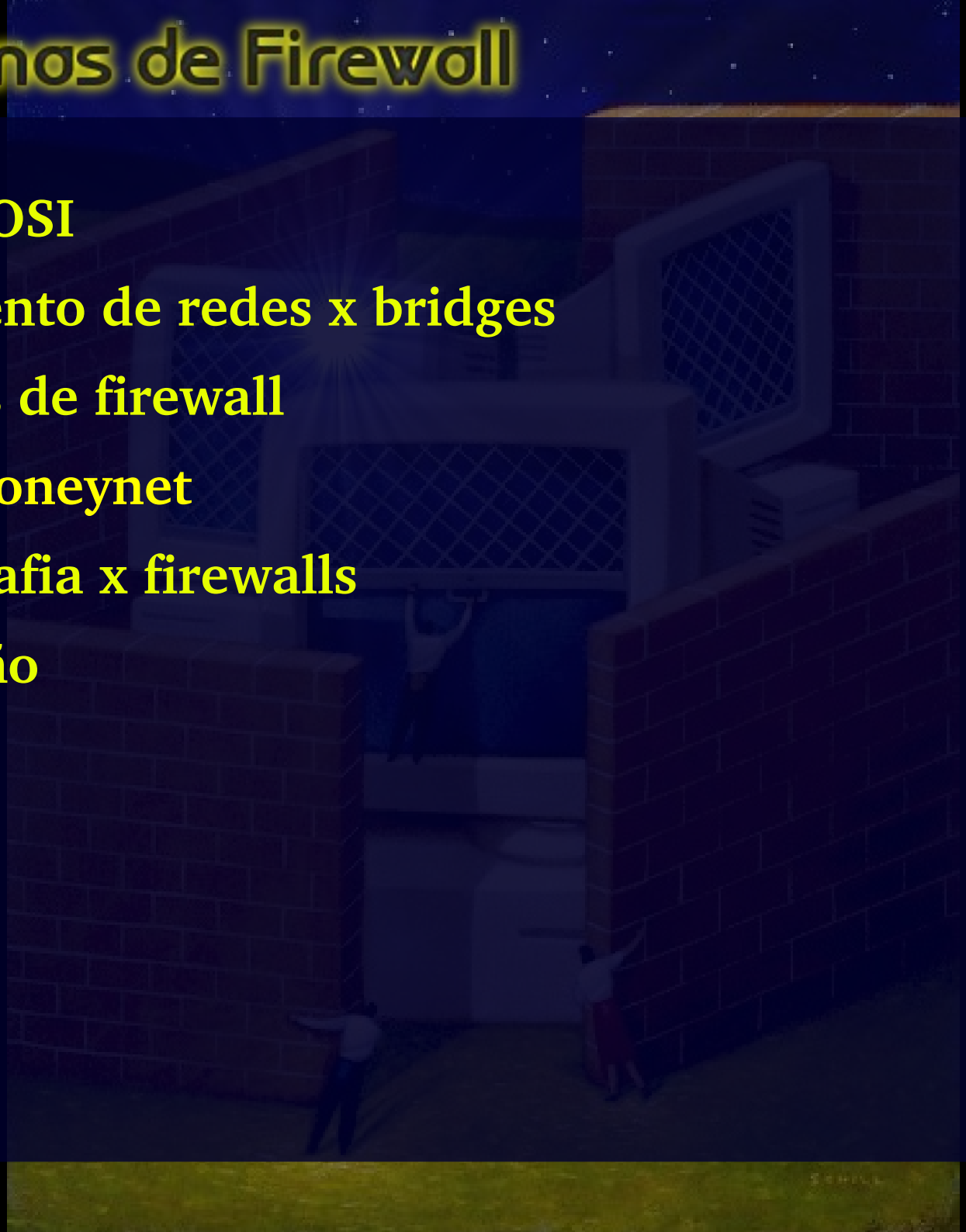
SEMANA DE CAPACITAÇÃO
26 a 30 de Setembro de 2022
Edição Online 5
nic.br

Sistemas de Firewall

Esta palestra está baseada no Cap. 17 do livro Análise de Tráfego em Redes TCP/IP, da Novatec Editora.

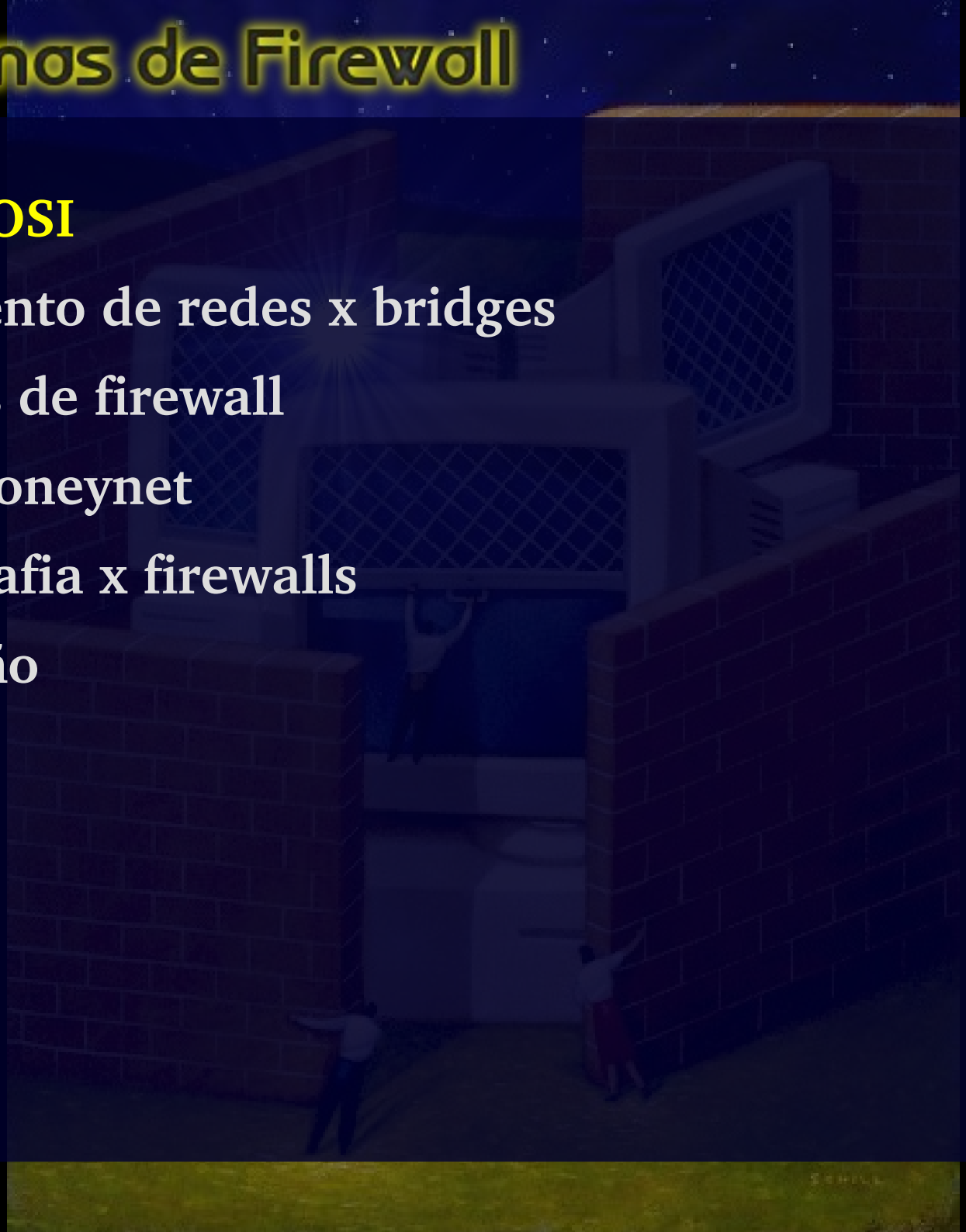


Sistemas de Firewall



- Modelo OSI
- Roteamento de redes x bridges
- Sistemas de firewall
- DMZ e honeynet
- Criptografia x firewalls
- Conclusão

Sistemas de Firewall



- **Modelo OSI**
- Roteamento de redes x bridges
- Sistemas de firewall
- DMZ e honeynet
- Criptografia x firewalls
- Conclusão

Eriberto - set. 2022

O modelo OSI

- Camada 7 - Aplicação
- Camada 6 - Apresentação
- Camada 5 - Sessão
- Camada 4 - Transporte
- Camada 3 - Rede
- Camada 2 - Enlace
- Camada 1 - Física

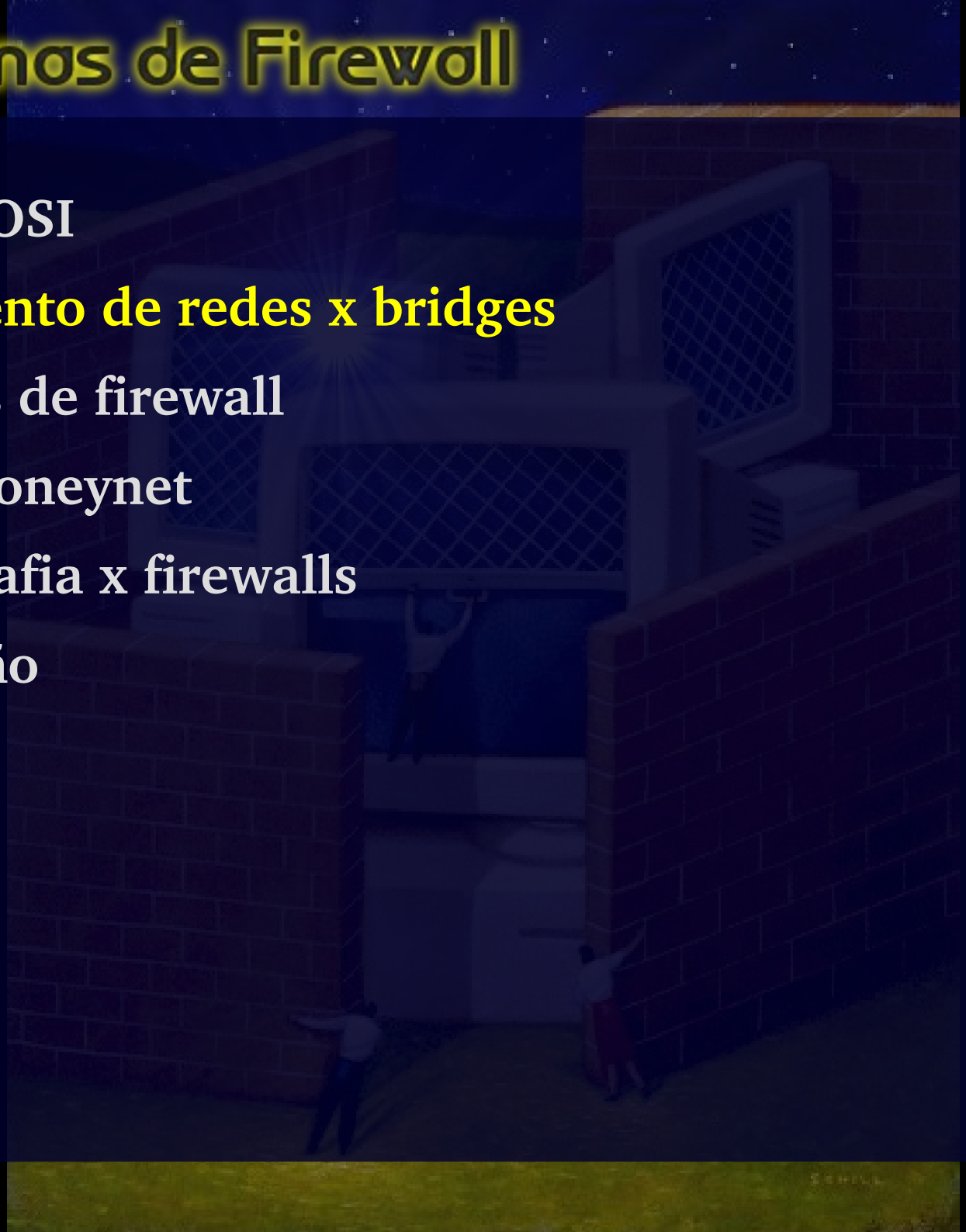
- ✔ Open Systems Interconnection.
- ✔ Possui 7 camadas, numeradas de baixo para cima.
- ✔ Criado para prover compatibilidade entre produtos de rede de fabricantes diferentes.
- ✔ O seu entendimento é fundamental para o estudo dos sistemas de firewall.
- ✔ Um tráfego de rede nem sempre atingirá as camadas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

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

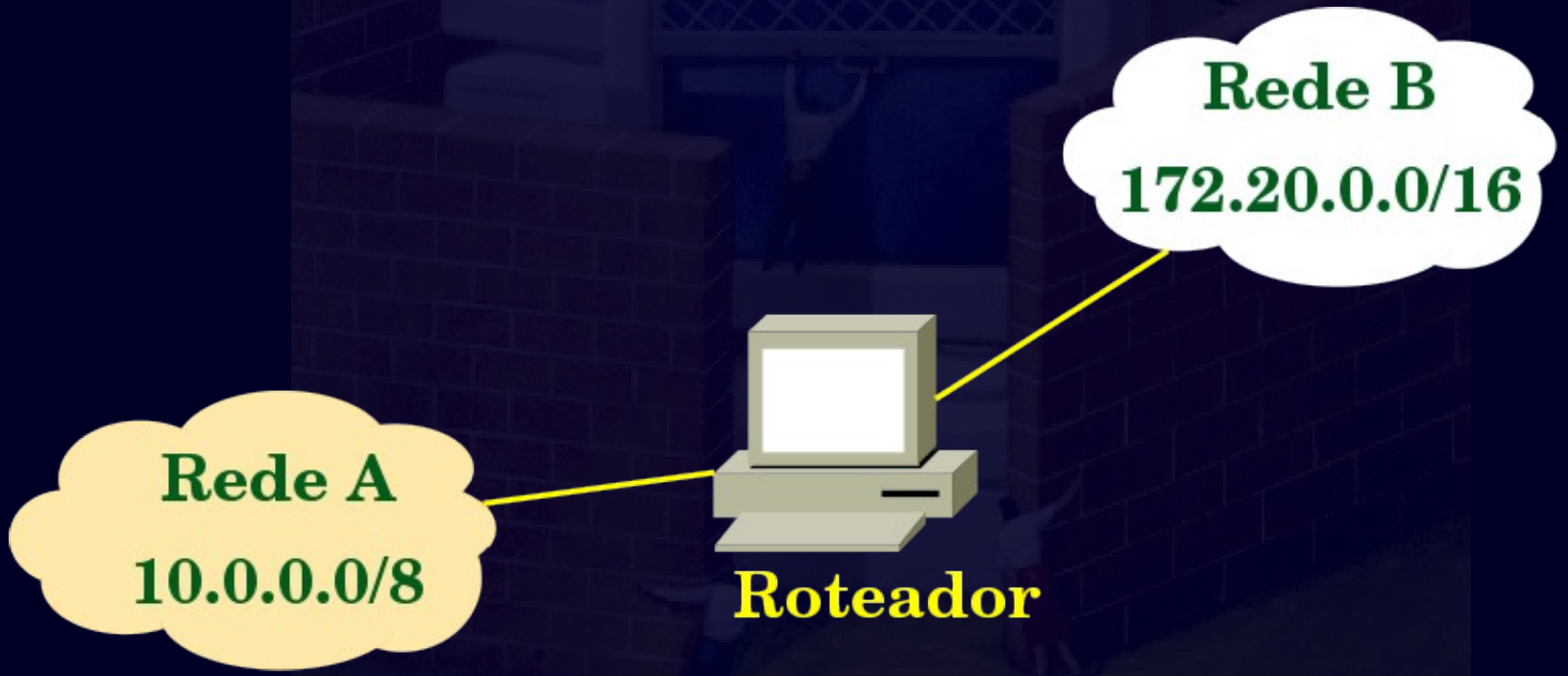
- Modelo OSI
- **Roteamento de redes x bridges**
- Sistemas de firewall
- DMZ e honeynet
- Criptografia x firewalls
- Conclusão



Eriberto - set. 2022

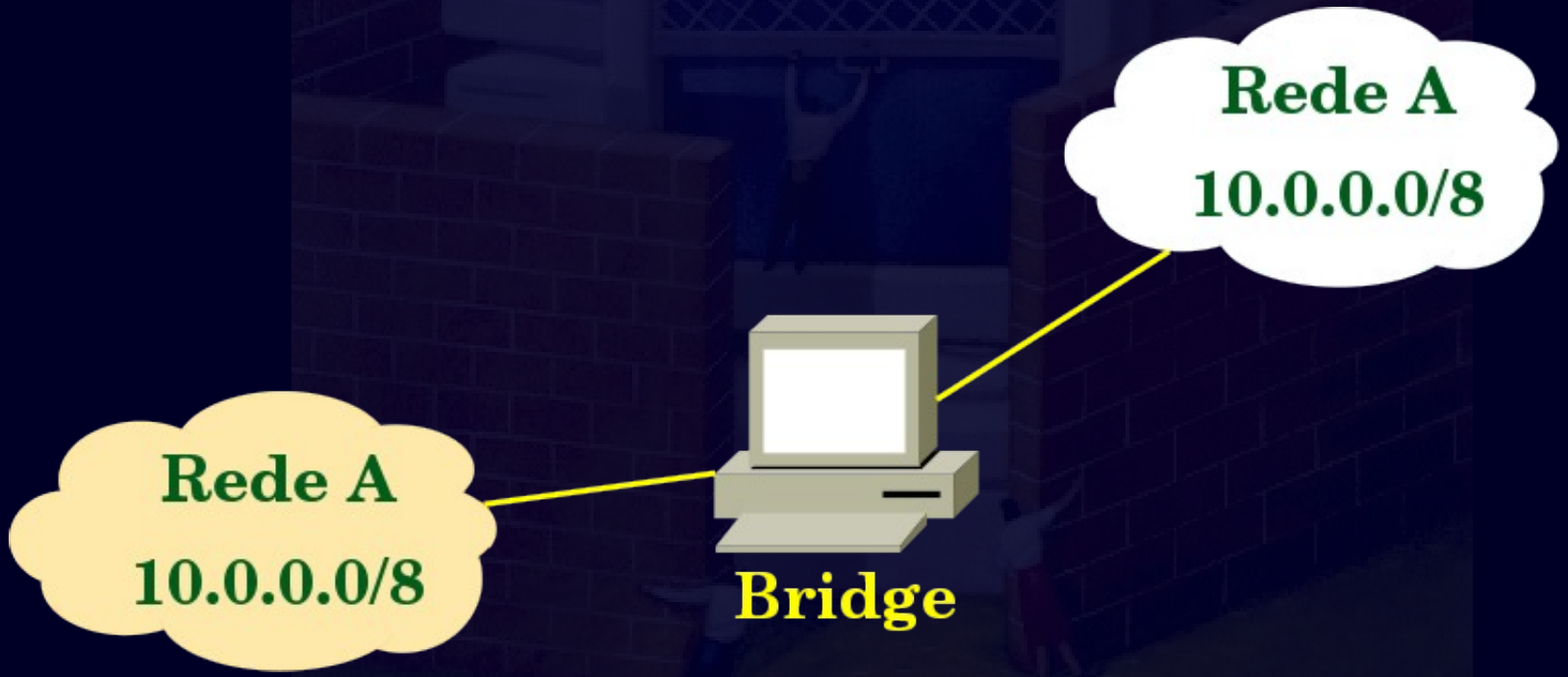
Roteamento de rede

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

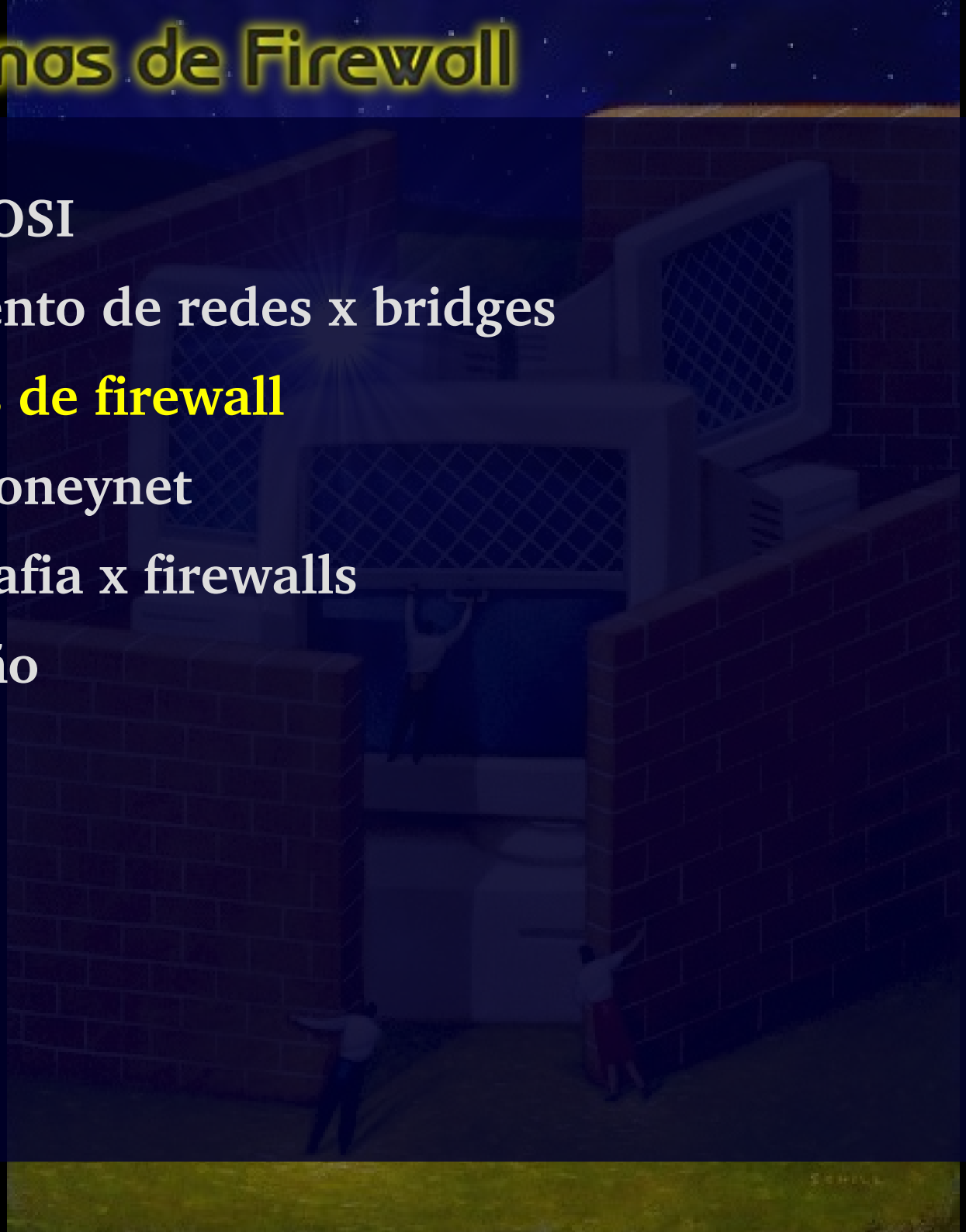


As bridges

- ✔ 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

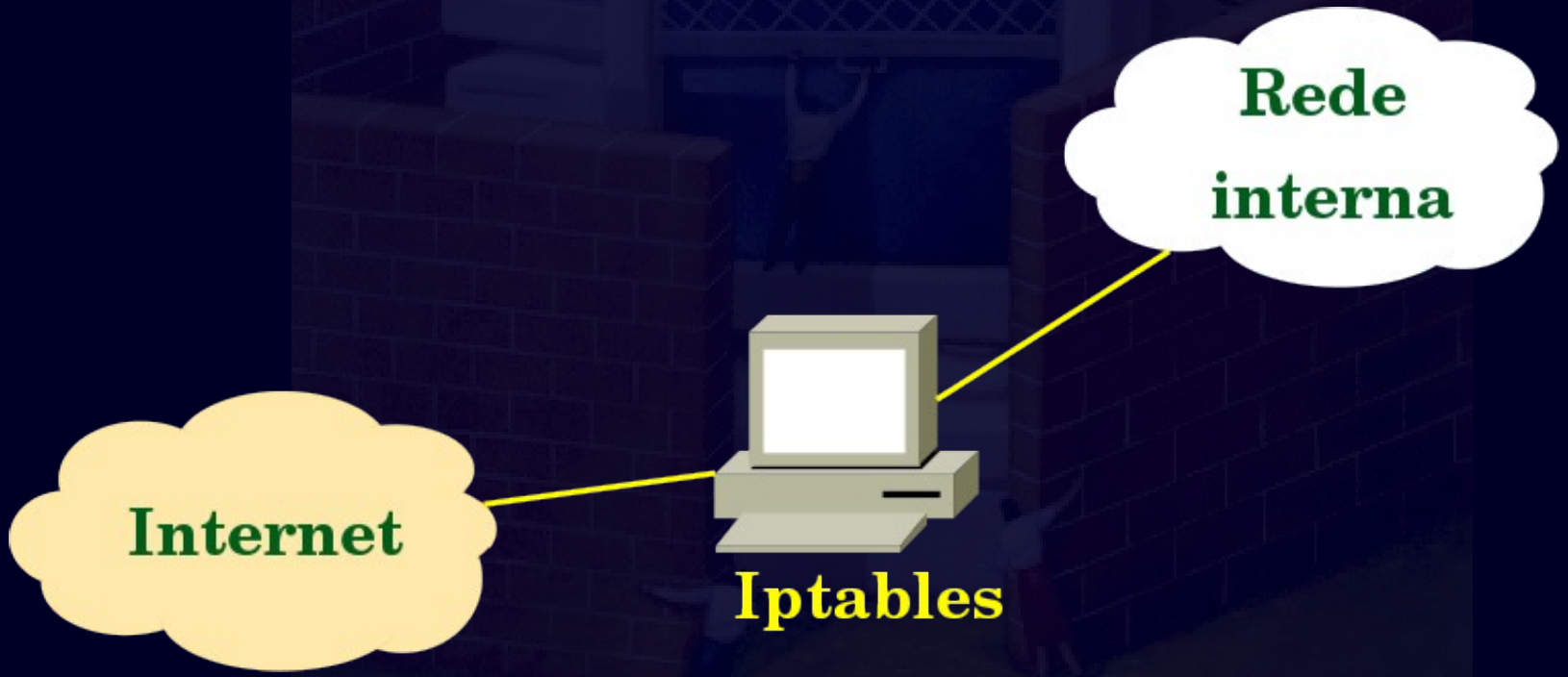


- Modelo OSI
- Roteamento de redes x bridges
- **Sistemas de firewall**
- DMZ e honeynet
- Criptografia x firewalls
- Conclusão

Eriberto - set. 2022

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 frames, 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.

Sistemas de Firewall

Elementos de firewall

- ✔ Filtros de frames: atuam na camada 2 do modelo OSI.
- ✔ Filtros de pacotes: atuam nas camadas 3 e 4 do modelo OSI, filtrando endereços IP, portas, protocolos IP etc.
- ✔ Filtros de estados: entendem estados de conexão (camadas 3 e 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 positivos não devem ocorrer.
- ✔ HIDS: IDS que funciona em máquinas finalísticas.
- ✔ Verificador de integridade: detecta mudanças em filesystems.

Alguns exemplos de elementos de firewall

- ✔ Filtros de frames: ebtables, Netfilter (Iptables, parcialmente)
- ✔ Filtros de pacotes: Netfilter (Iptables) e PF.
- ✔ Filtros de estados: Netfilter (Iptables) e PF.
- ✔ IDS: Snort e Suricata.
- ✔ IPS: Suricata e Snort In-Line.
- ✔ Proxy: Squid, dnsproxy, qpsmtpd, apt-cache search proxy :-)
- ✔ Port scan detector: Netfilter, psad e PortSentry.
- ✔ Monitor de falhas em logs e de logins: fail2ban.
- ✔ Antivírus: Clamav.
- ✔ Verificadores de integridade: Fcheck, iwatch, Samhain e AIDE.
- ✔ Log de pacotes: daemonlogger.
- ✔ Outros: apt-cache search firewall / apt-cache search honey.

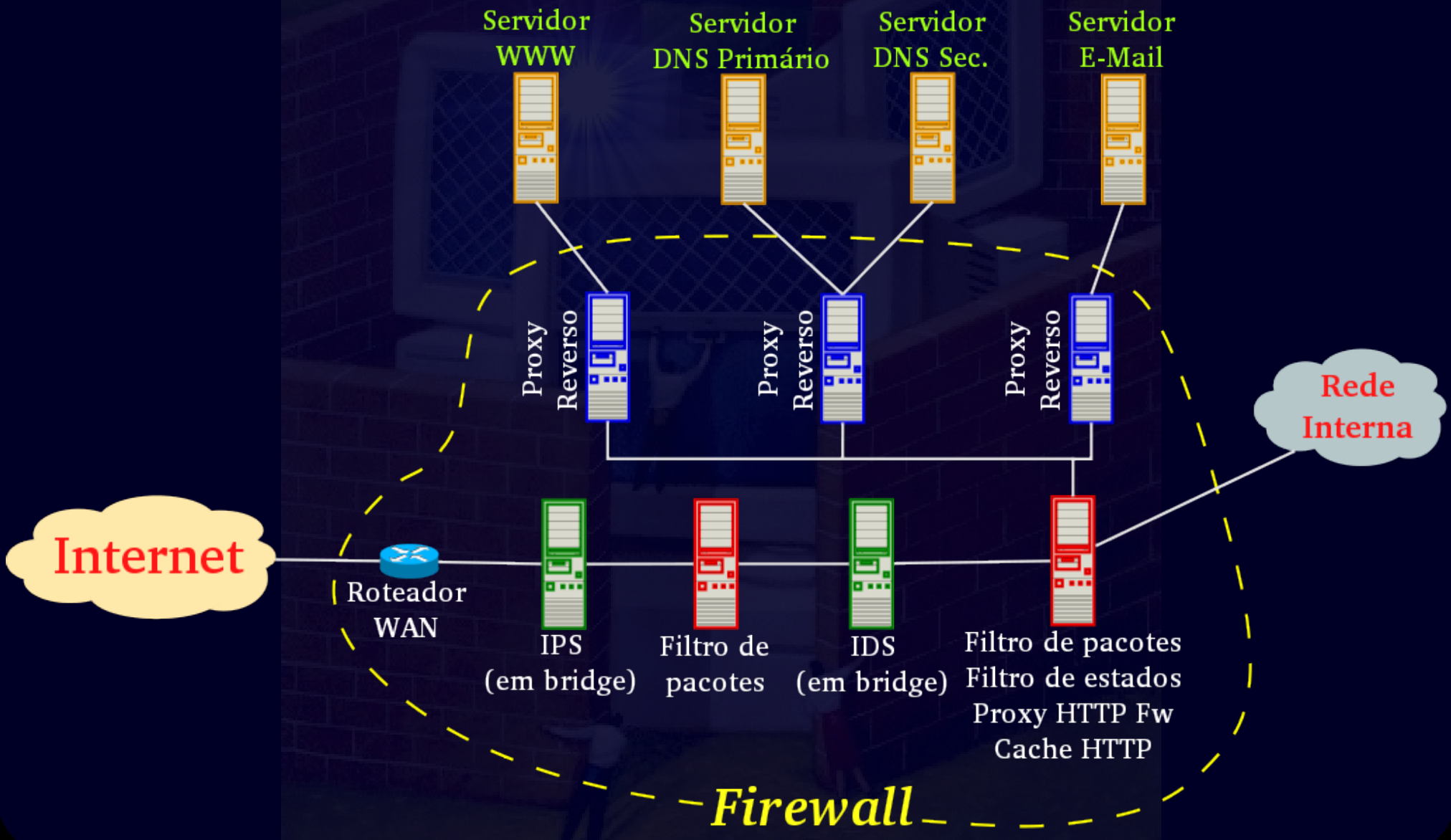
Elementos de firewall x modelo OSI

Camada 7 - Aplicação	→ proxies, (H)IDS, IPS, antivírus etc.
Camada 6 - Apresentação	
Camada 5 - Sessão	
Camada 4 - Transporte	→ filtros. (proxies, IDS, IPS etc)[1]
Camada 3 - Rede	→ filtros. (proxies, IDS, IPS etc)[1]
Camada 2 - Enlace	→ filtros. (IPS [scrubbers])[1]
Camada 1 - Física	

[1] Atuam na camada 7; entendem as camadas 2, 3 e 4.

Sistemas de Firewall

Um exemplo simples de sistema de firewall



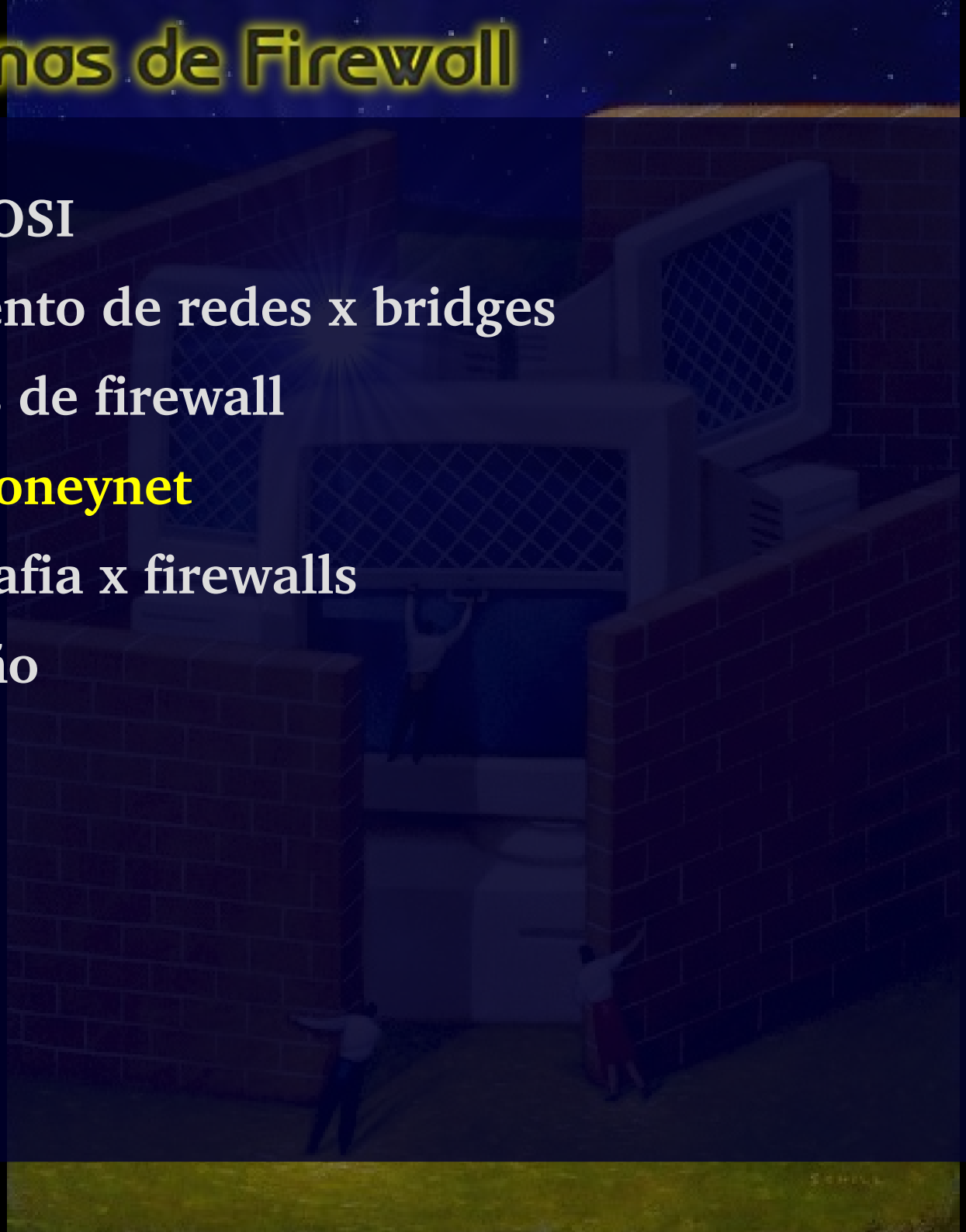
Eriberto - set. 2022

Sistemas de firewall

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

D E U S

Sistemas de Firewall

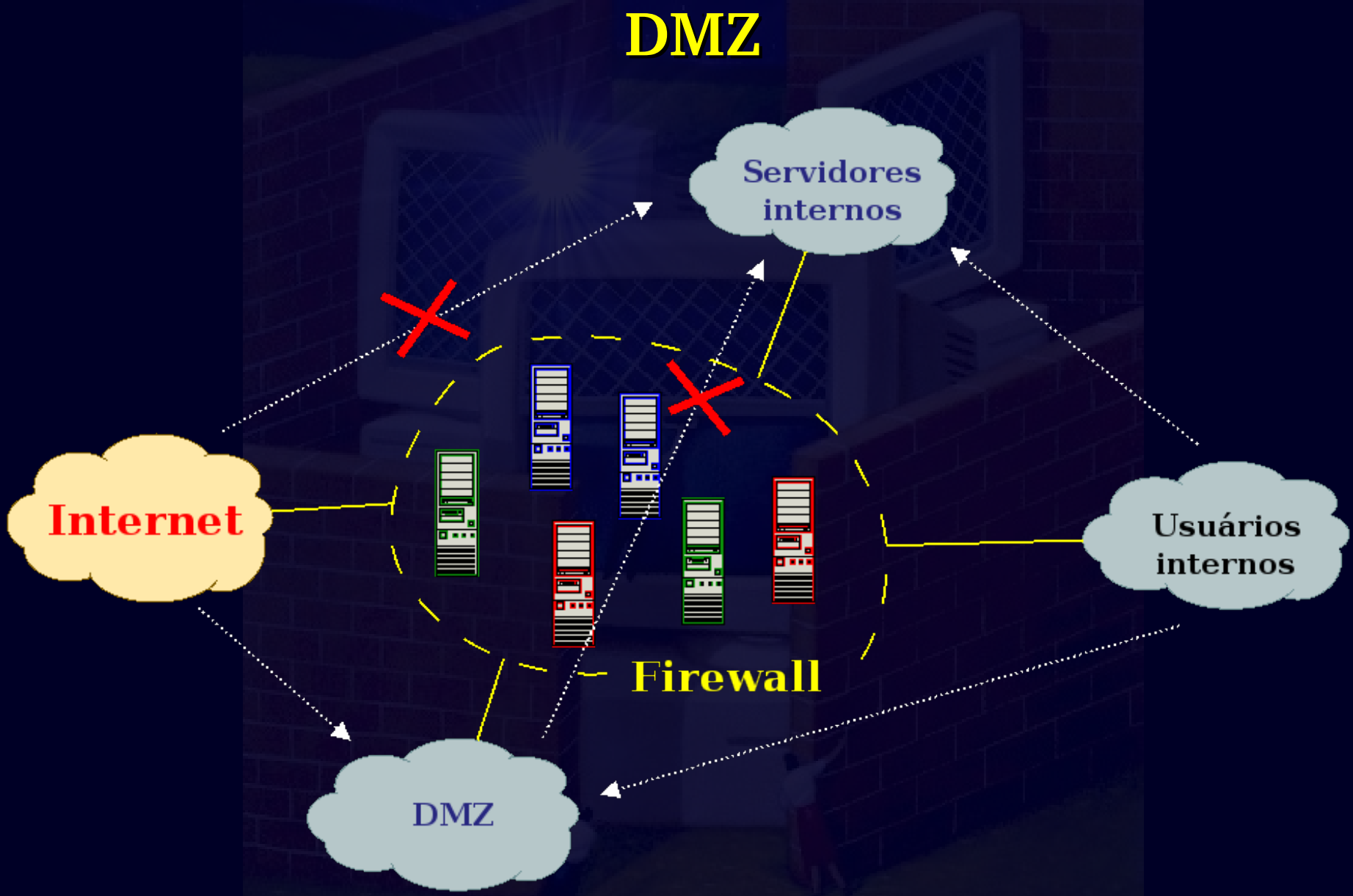


- Modelo OSI
- Roteamento de redes x bridges
- Sistemas de firewall
- **DMZ e honeynet**
- Criptografia x firewalls
- Conclusão

DMZ

- ✔ DMZ (demilitarized zone) ou rede de perímetro serve para concentrar servidores que possibilitam acesso externo, podendo também receber acessos de usuários internos.
- ✔ A ideia é criar um bolsão onde um possível invasor ficará retido.
- ✔ Em princípio, a DMZ não deve ter contato com servidores da rede interna. Caso isso seja necessário, deverá haver um rígido controle e restrições.

Sistemas de Firewall

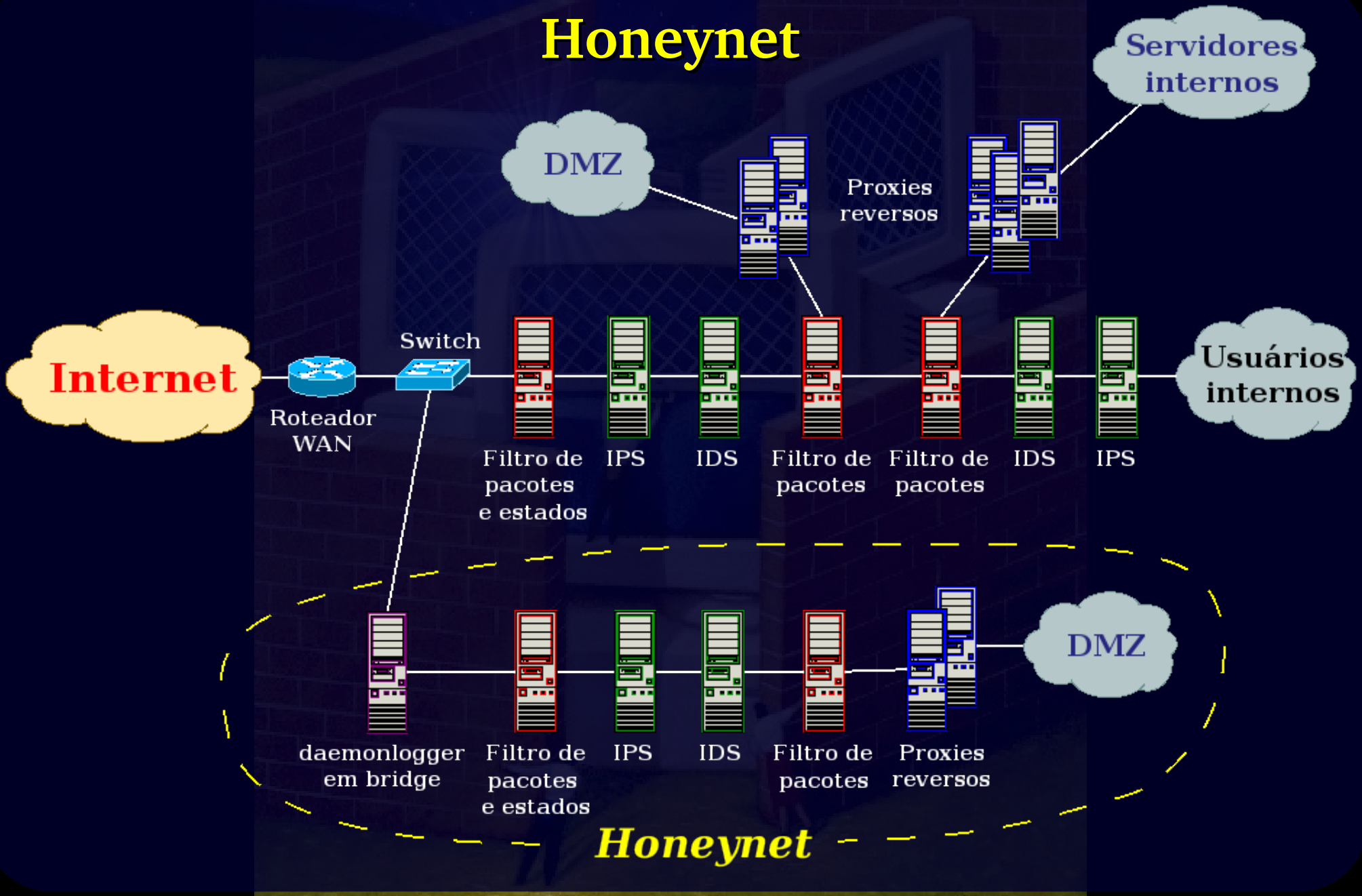


Eriberto - set. 2022

Honeynet

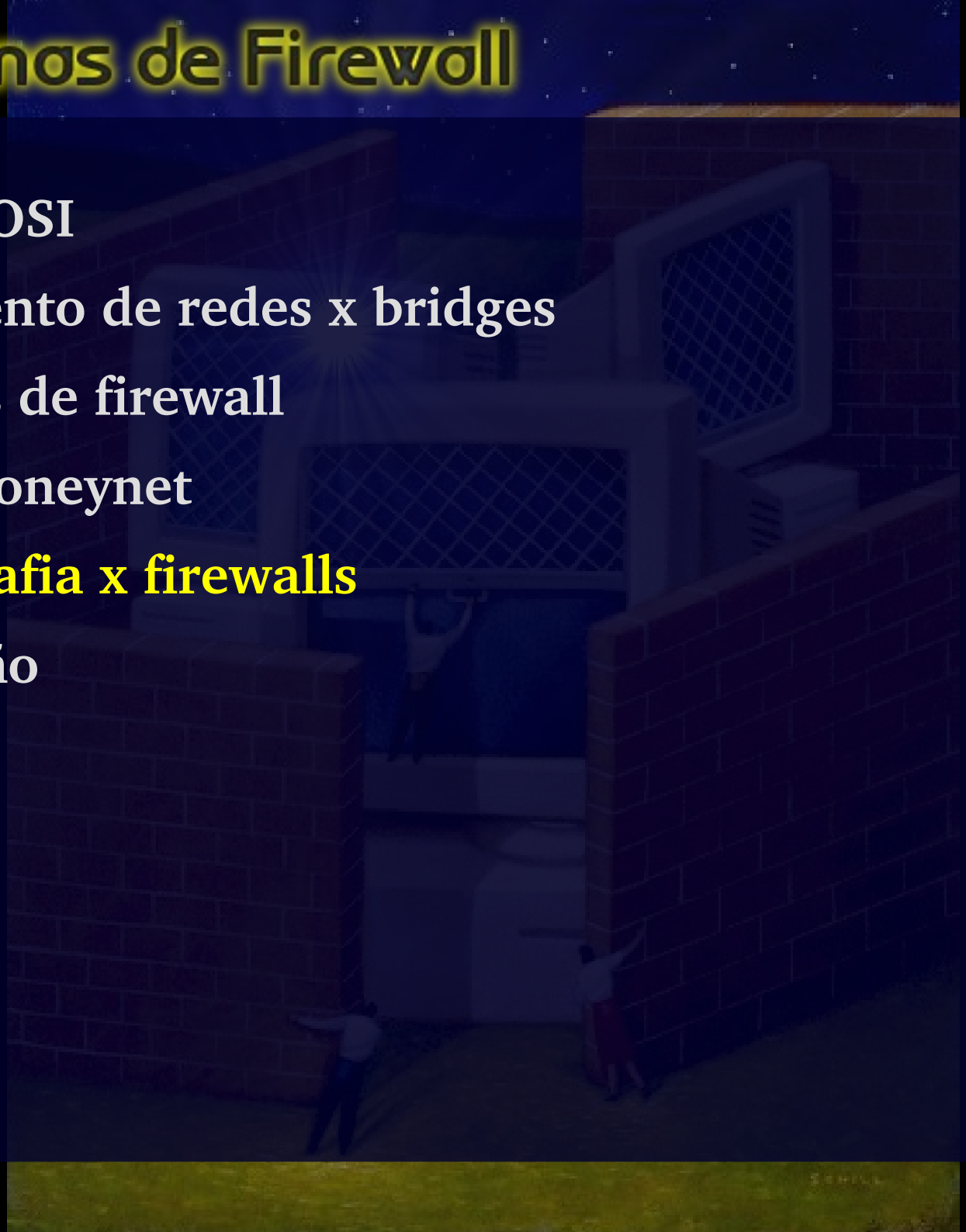
- ✔ Dentro de uma rede corporativa, uma honeynet servirá para estudarmos ações danosas sobre a topologia.
- ✔ A estrutura de uma honeynet deverá imitar a estrutura da rede real, no que tange aos acessos vindos do exterior.
- ✔ A existência da honeynet não deverá ser divulgada em DNS ou por outro meio qualquer. Assim, quem chegar à mesma o fará por scaneamento ou outro método similar.
- ✔ Dentro de uma rede corporativa, uma honeynet NUNCA deverá ser objeto de invasão. Então, a rede principal e a honeynet deverão estar sempre atualizadas e em segurança.

Sistemas de Firewall



Eriberto - set. 2022

Sistemas de Firewall



- Modelo OSI
- Roteamento de redes x bridges
- Sistemas de firewall
- DMZ e honeynet
- **Criptografia x firewalls**
- Conclusão

Criptografia x firewalls

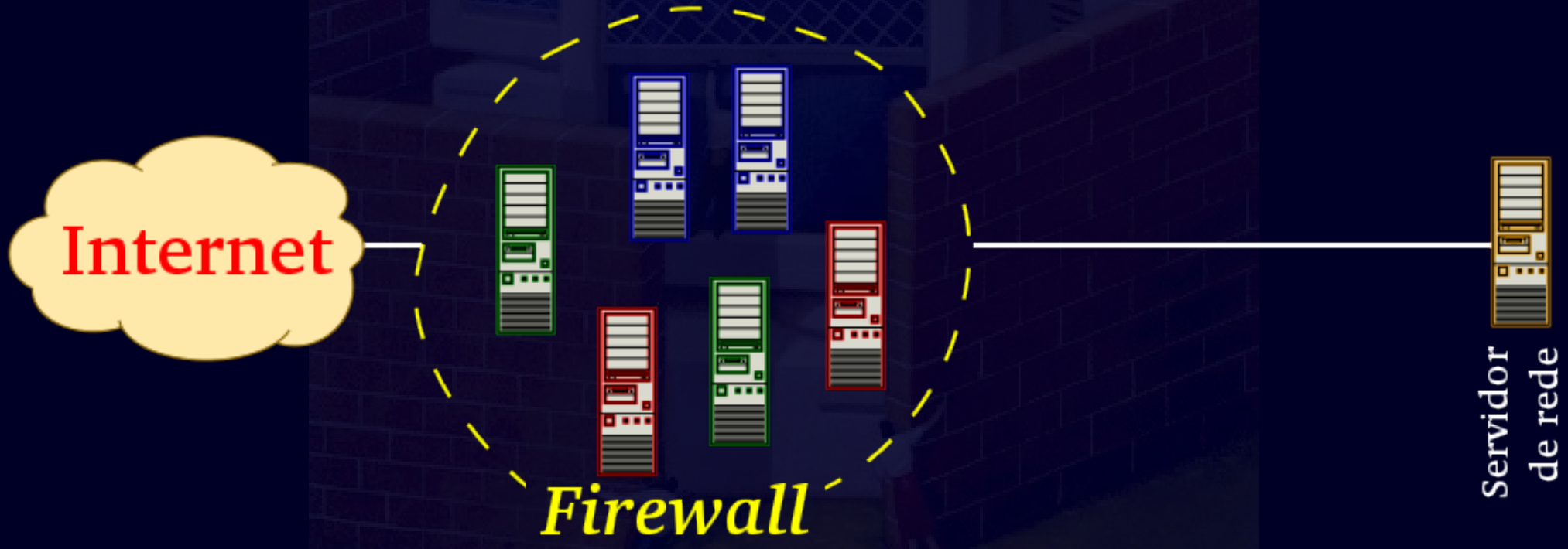
Criptografia é uma boa solução para a segurança?

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



Eriberto - set. 2022

Sistemas de Firewall

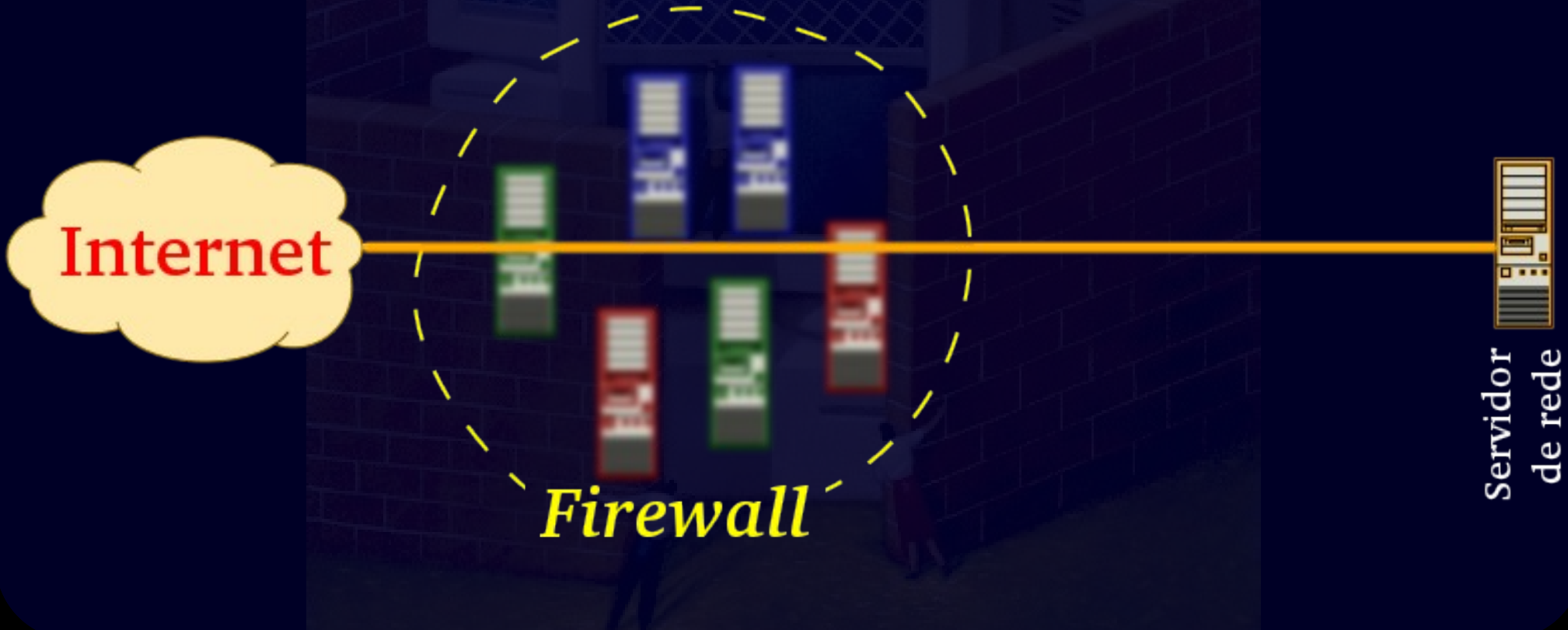
Criptografia x firewalls

Eriberto - set. 2022

Sistemas de Firewall

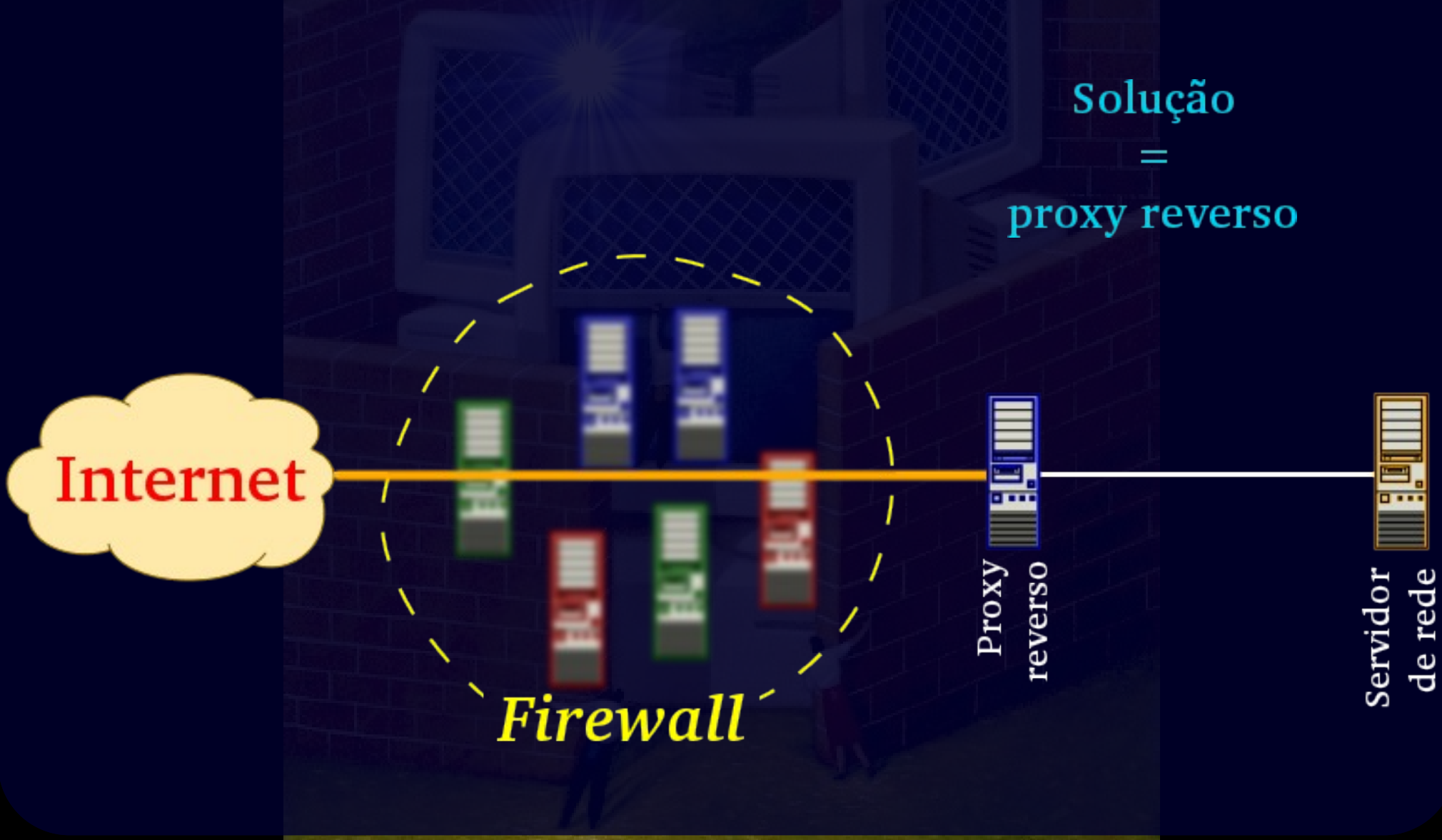
Criptografia x firewalls

Solução
=
proxy reverso



Sistemas de Firewall

Criptografia x firewalls

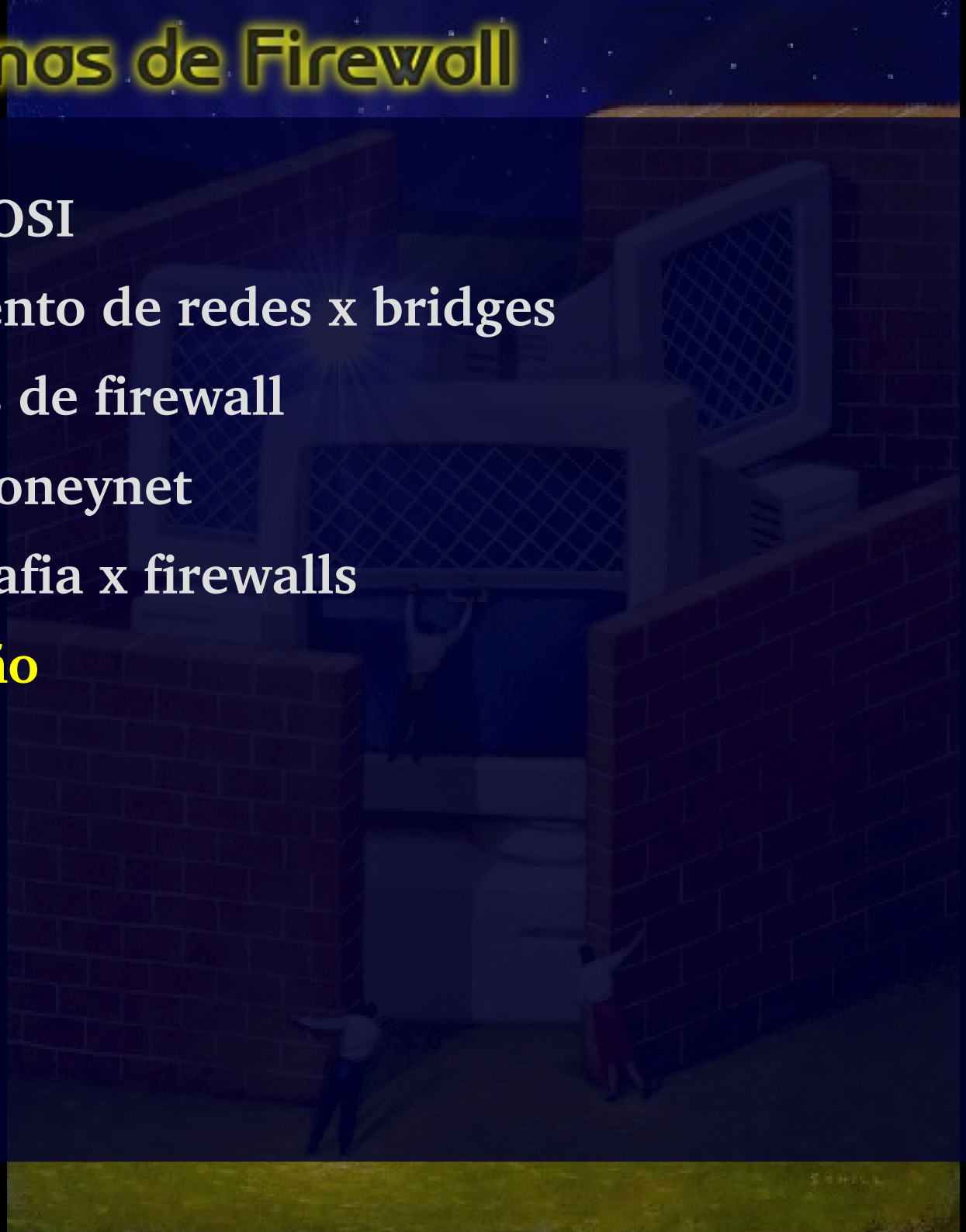


Sistemas de Firewall

Criptografia x firewalls

Eriberto - set. 2022

Sistemas de Firewall



- Modelo OSI
- Roteamento de redes x bridges
- Sistemas de firewall
- DMZ e honeynet
- Criptografia x firewalls
- **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