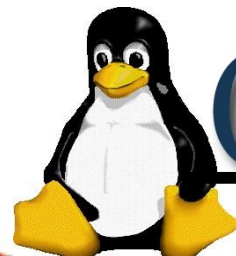


Palestrante: Flávio Cunha

www.clublinux.com.br



Club Linux

Linux sem segredos



FIREWALLS EM AMBIENTE LINUX

O que é um FIREWALL?

- **Firewall** é o nome dado ao dispositivo de rede, que tem por função, regular o tráfego de rede entre redes distintas e impedir a transmissão de dados nocivos ou não autorizados de uma rede a outra.

Definição: wikipedia.org

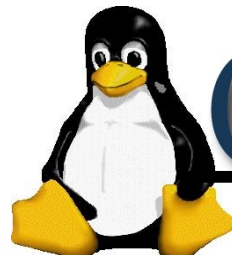


Club Linux

Linux sem segredos

Filtro de Pacotes

- Um **filtro de pacotes** é um programa que analisa o cabeçalho (Header) dos pacotes, enquanto eles passam, e decide o que fazer com eles.



Club Linux

Linux sem segredos

netfilter

firewalling, NAT, and packet mangling for Linux

- O **Netfilter** é um framework que foi inserido nos kernels **2.4 e 2.6** para realizar filtragem de pacotes. O programa associado ao netfilter é o **iptables**.



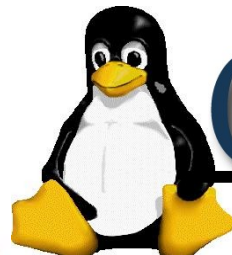
Club Linux

Linux sem segredos

**Kernel 2.0
Ipfwadm**

**Kernel 2.2
Ipchains**

**Kernel 2.4 e 2.6
Iptables**

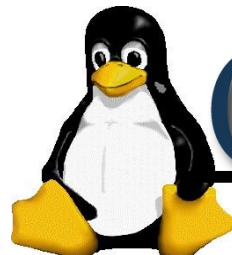


Club Linux

Linux sem segredos

Principais características do Netfiler/Iptables

- Filtro de pacotes **STATELESS**
- Filtro de pacotes **STATEFULL**
- NAT/NAPT
- Arquitetura Flexível e expansível
- Firewall **OPEN SOURCE** (Eu posso mexer no código :)



Club Linux

Linux sem segredos

O que eu posso fazer com o Netfilter/Iptables?

- Implementar Firewalls de Internet baseados em filtragem STATELESS E STATEFULL
- Usar NAT para compartilhar o acesso a Internet
- Implementar serviço de Proxy transparente em conjunto com o Proxy SQUID
- Pode ser utilizado com o pacote iproute2 para implementação de regras de roteamento avançado e controle de banda



Club Linux

Linux sem segredos

O que eu posso fazer com o Netfilter/Iptables?

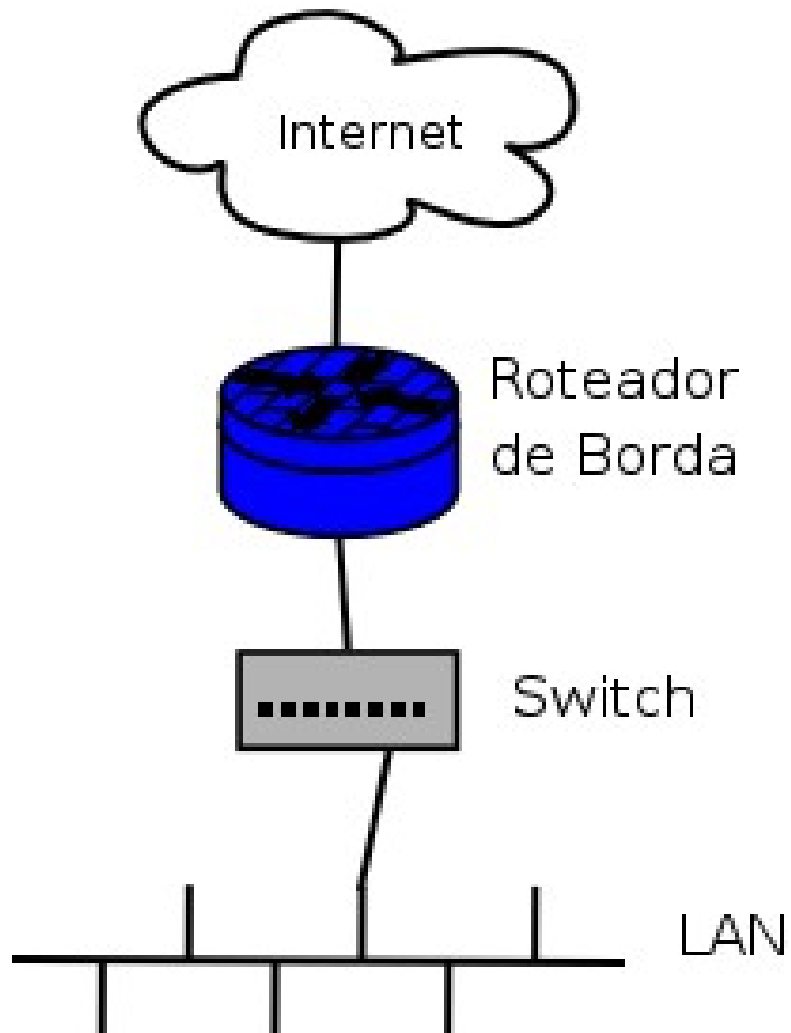
- Interação com o pacote através da manipulação do campo TOS do cabeçalho IP
- Implementação de regras que tratam até o Layer 4 do modelo ISO-OSI
- Firewall que pode atuar em nível de aplicação para vários protocolos, com o projeto **I7-filter**
- Usar o proxy **SQUID**, para trabalhar em conjunto com o Iptables e fazer filtragens em nível de aplicação para o protocolo **HTTP**.



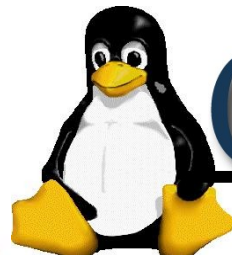
Club Linux

Linux sem segredos

Arquiteturas de Firewall



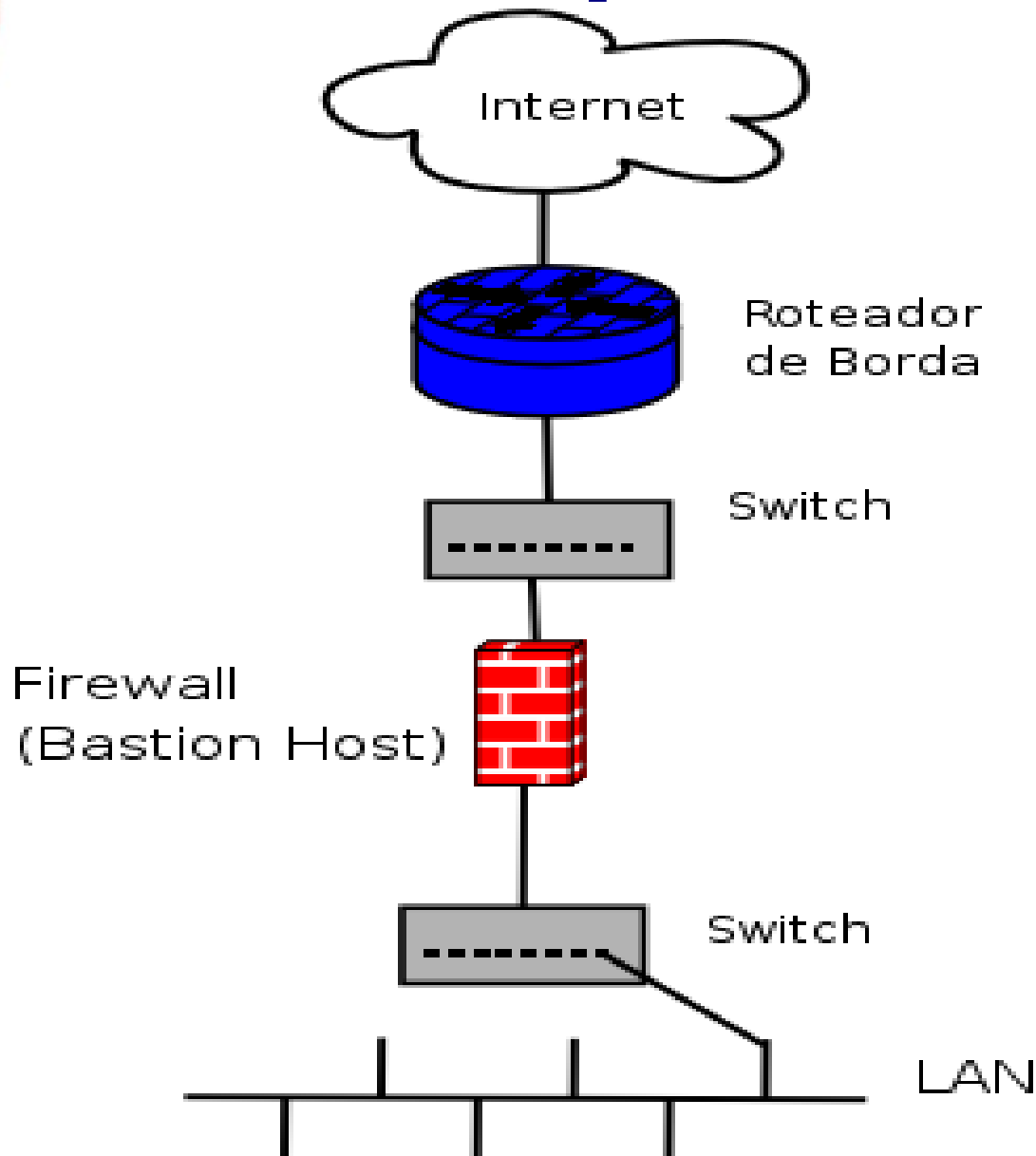
**SCREENED
ROUTER**



Club Linux

Linux sem segredos

Arquiteturas de Firewall



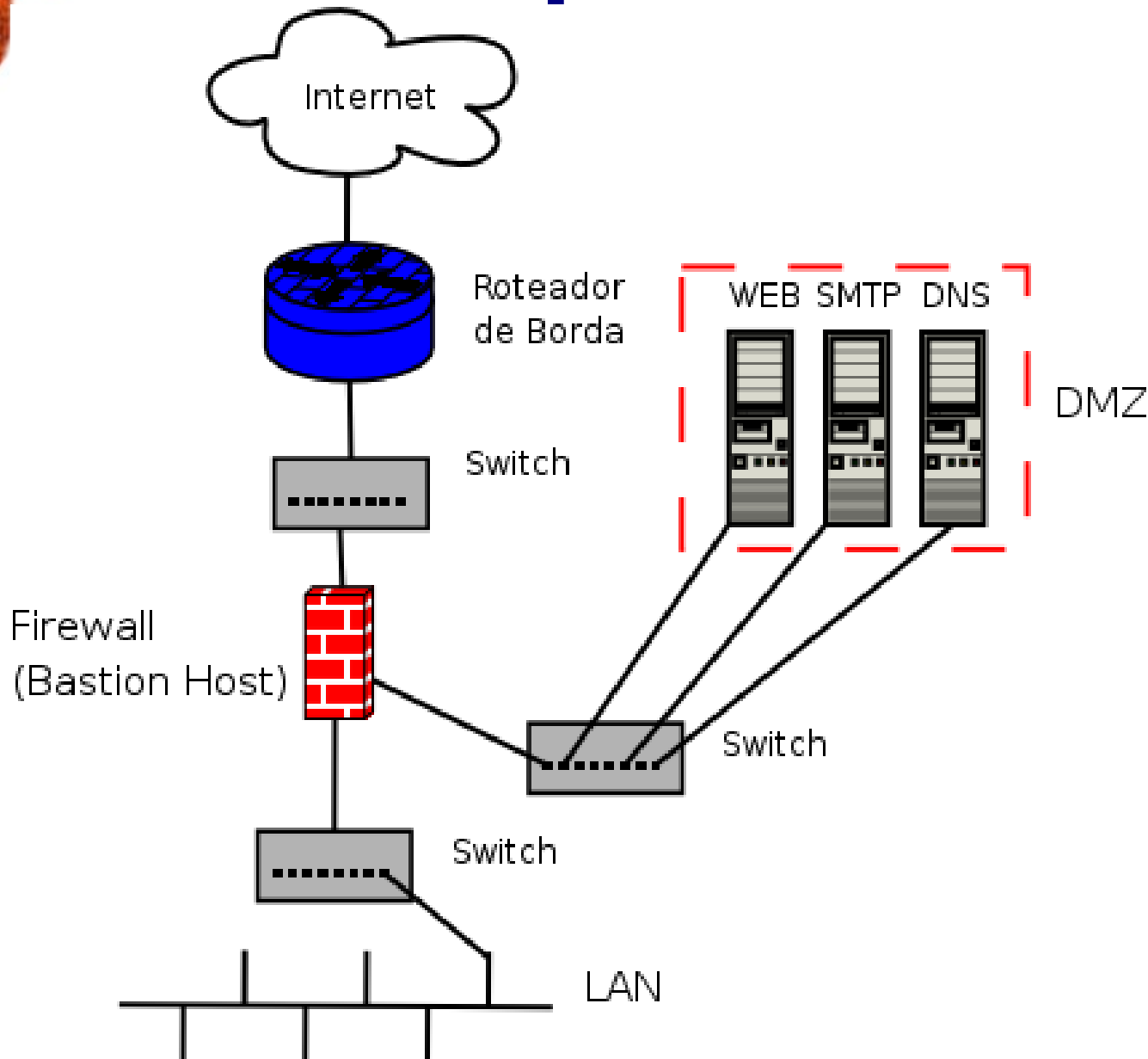
DUAL HOMED GATEWAY



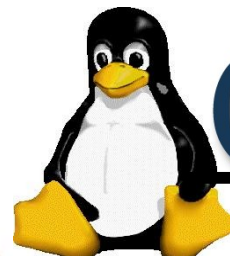
Club Linux

Linux sem segredos

Arquiteturas de Firewall



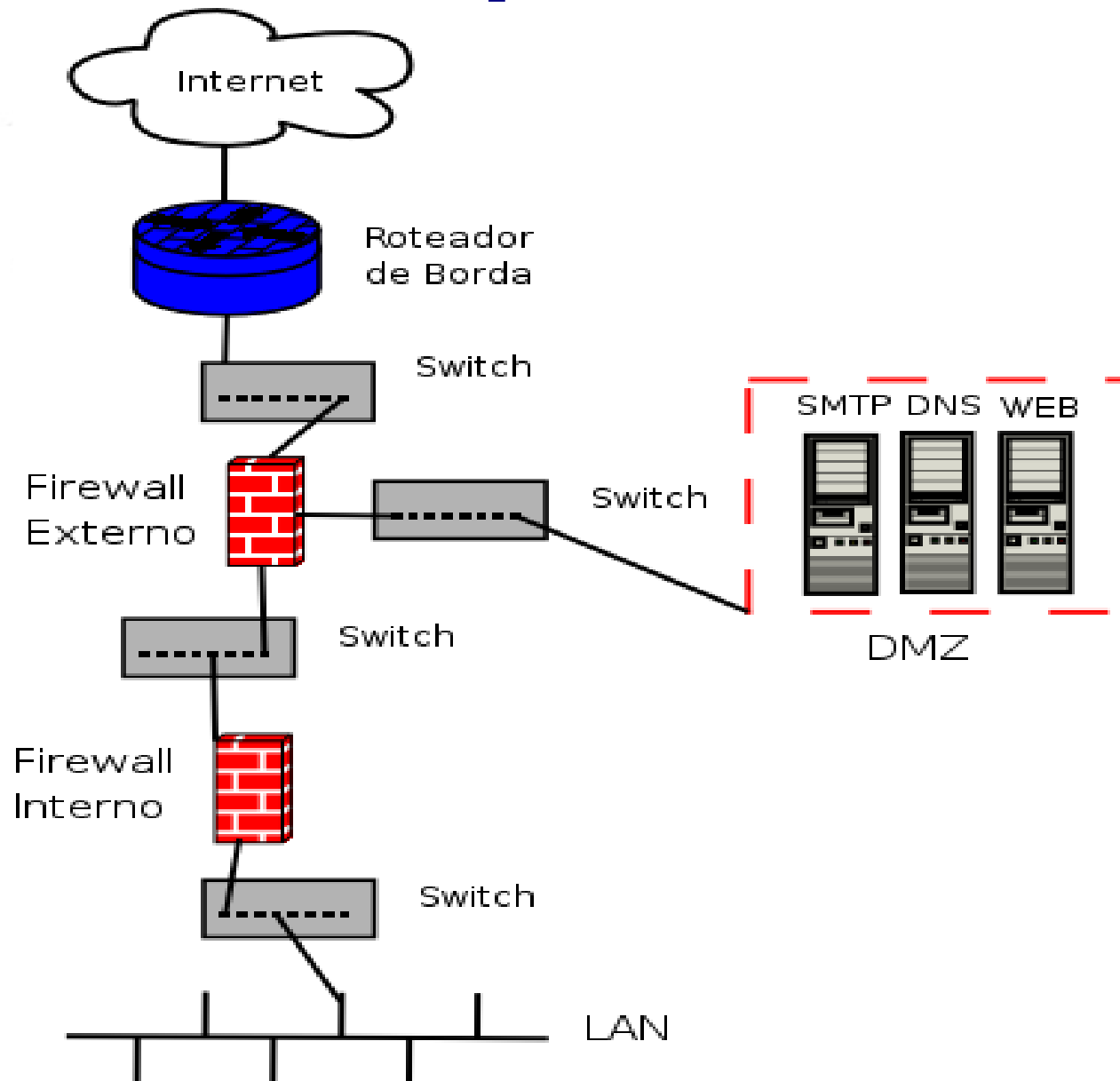
**SCREENED
SUBNET**



Club Linux

Linux sem segredos

Arquiteturas de Firewall



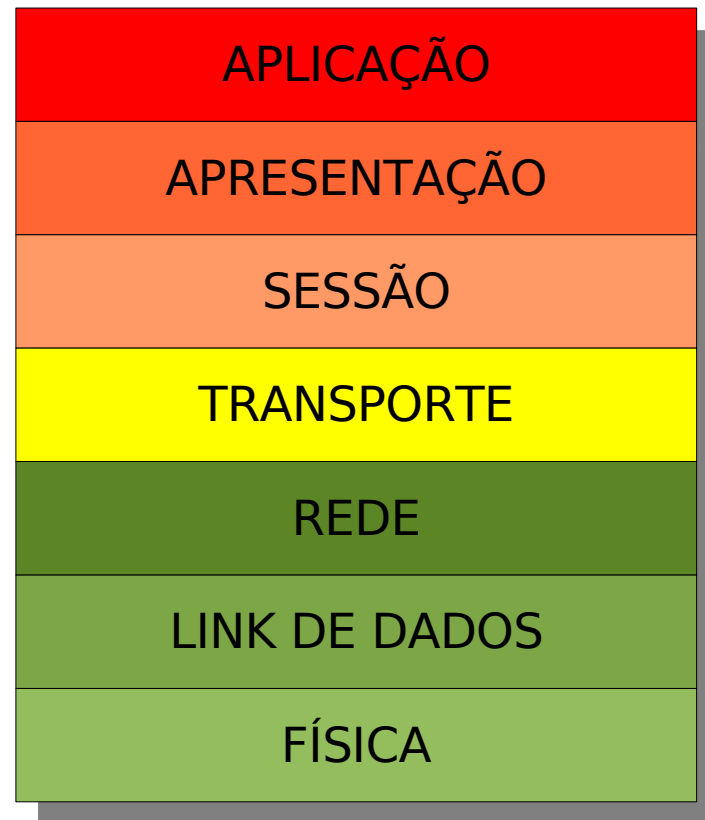
**SCREENED
SUBNET 2**



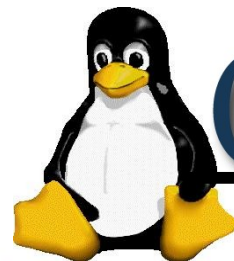
Club Linux

Linux sem segredos

O que eu preciso saber antes de começar...



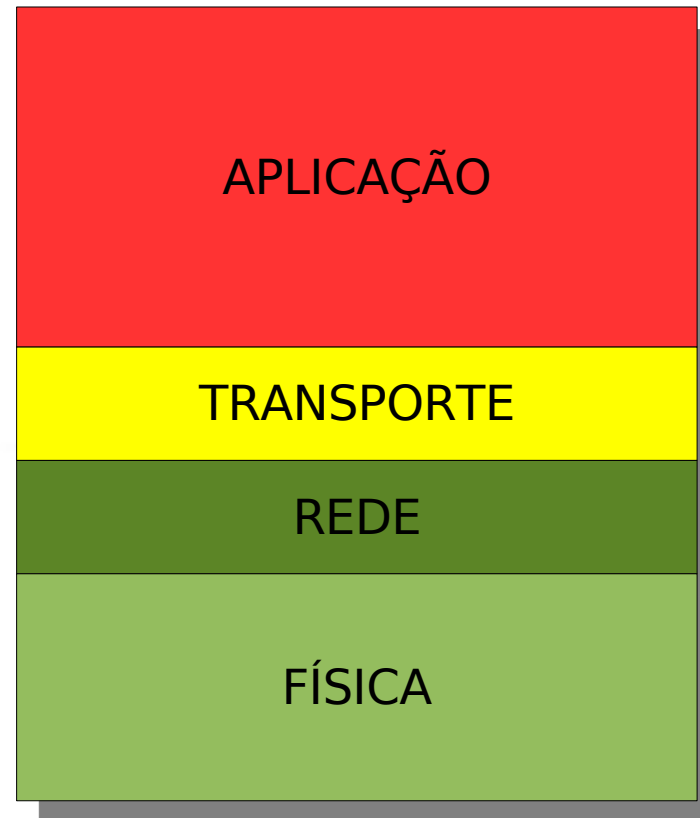
Modelo OSI de Referência



Club Linux

Linux sem segredos

O que eu preciso saber antes de começar...



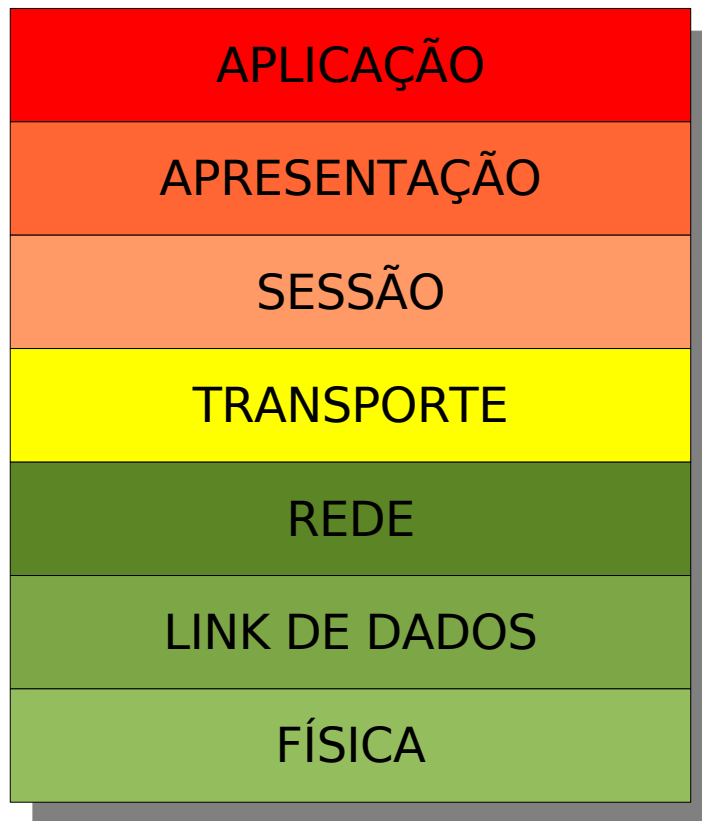
Pilha TCP-IP



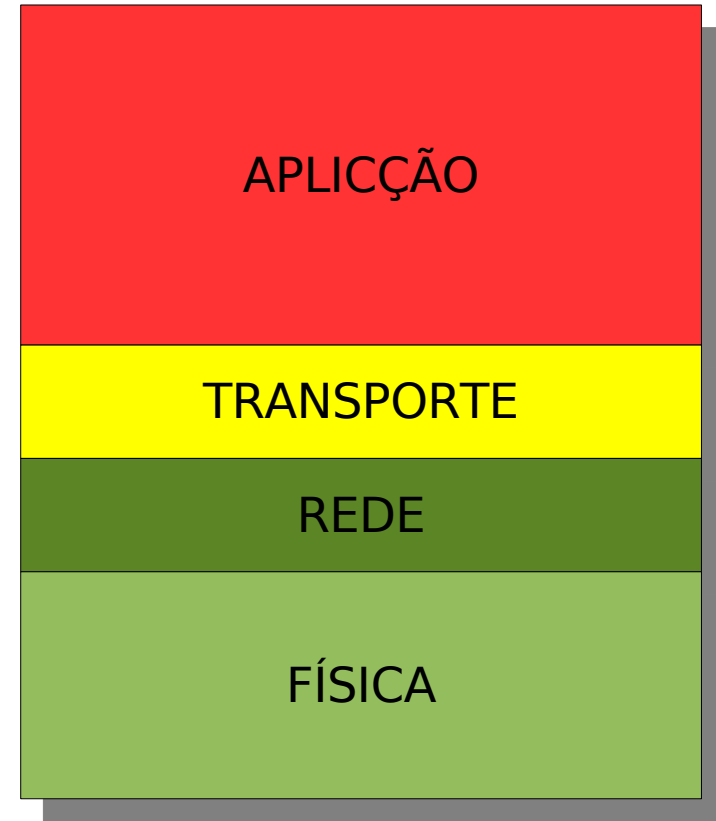
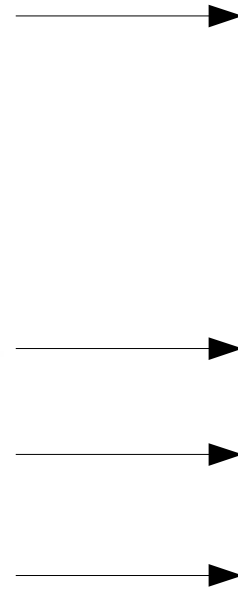
Club Linux

Linux sem segredos

O que eu preciso saber antes de começar...



Modelo OSI



Pilha TCP-IP



Club Linux

Linux sem segredos

Conhecendo o Elenco...

DNS	SMB	SSH
FTP	HTTP	HTTPS
SMTP	TELNET	ETC...

**Camada de
Aplicação**



Club Linux

Linux sem segredos

Regras em Nível de Aplicação

- O pacote **L7-Filter**, utilizando expressões regulares, faz a checagem dos dados no cabeçalho IP para determinar a qual protocolo da camada de aplicação o pacote pertence.

Por exemplo:

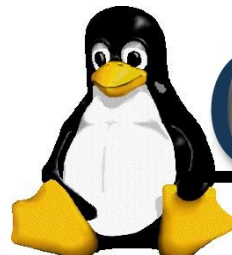
Utilizando esta ferramenta é possível criar uma regra para o protocolo HTTP, independente da porta.(O servidor web pode ser configurado para ouvir em qualquer porta)

Regra com L7-Filter

```
# iptables -A FORWARD -s 192.168.0.0/24 -m layer7 --l7proto http -j DROP
```

Regra sem L7-Filter

```
# iptables -A FORWARD -p tcp -s 192.168.0.0/24 --dport 80 -j DROP
```



Club Linux

Linux sem segredos

Conhecendo o Elenco...



**Camada de
Transporte**



Club Linux

Linux sem segredos

O que eu preciso saber antes de começar...

Porta origem	Porta destino
Comprimento	Soma de verificação
Dados da Aplicação	

Segmento UDP



Club Linux

Linux sem segredos

Segmento TCP

Porta Origem		Porta Destino						
Número de sequência								
Número de Reconhecimento								
Comprimento do Cabeçalho	Não usado	R	S	F	U	A	P	Tamanho da janela
		S	Y	I	R	C	S	
		T	N	N	G	K	H	
Soma de verificação				Ponteiro para dados urgente				
Opções								
Dados da Aplicação								



Club Linux

Linux sem segredos

O que eu preciso saber antes de começar...

- Os números de portas são números de 16 bits que vão de **0 a 65535**.
- Números de portas que vão de **0 até 1023**, estão reservados para uso por protocolos de aplicação bem conhecidos, como **HTTP** e **SMTP**, por exemplo.
- Números de portas que vão de **1024 até 65535** são portas registradas, não controladas pelo **IANA**.
- Leia a **RFC 1700**



Club Linux

Linux sem segredos

Flags do Segmento TCP

SYN

Flag de início de conexão

ACK

Confirma se o valor levado para o campo de reconhecimento é válido

RST

Flag usada para derrubar uma conexão

FIN

Flag usada para derrubar uma conexão

PSH

Quando o bit **PSH** esta ativado, o destinatário deve passar os dados para a camada de aplicação imediatamente.

URG

Quando o bit **URG** está ativado, significa que existem dados no pacote rotulado como urgente



Club Linux

Linux sem segredos

Three Way Handshake

Cliente

SYN

Servidor

SYN/ACK

ACK



Club Linux

Linux sem segredos

Regras em Nível de Transporte

- Veja abaixo, alguns exemplos de Regras em Nível de Transporte:

Bloqueando acesso do ip 192.168.0.30 ao servidor DNS 201.6.0.108

```
# iptables -A FORWARD -p udp -s 192.168.0.30 -d 201.6.0.108 -dport 53 -j DROP
```

Bloqueando acesso da Rede 192.168.0.0/24 ao servidor Web 200.221.2.45

```
# iptables -A FORWARD -p tcp -s 192.168.0.0/24 -d 200.221.2.45 -dport 80 -j DROP
```

Bloqueando a entrada de pacotes de inicio de conexão no Host

```
# iptables -A INPUT -p tcp ! --syn -j ACCEPT
```

ou

```
# iptables -A INPUT -p tcp --syn -j DROP
```



Conhecendo o Elenco...

IP

ICMP

IGMP

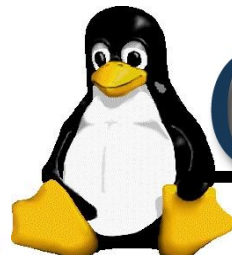
RIP

OSPF

BGP

ETC..

**Camada de
Rede**



Club Linux

Linux sem segredos

O que eu preciso saber antes de começar...

Versão	Comprimento do Cabeçalho	Tipo de serviço	Comprimento do datagrama (bytes)	
Identificador de 16 bits			Flags	Deslocamento de Fragmentação 13 bits
Tempo de vida (TTL)	Protocolo da camada superior		Soma verificadora do cabeçalho	
Endereço IP origem (32 bits)				
Endereço IP destino (32 bits)				
Opções				
Dados				

**Datagrama
IP**



Club Linux

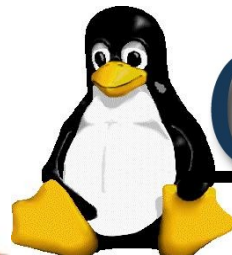
Linux sem segredos

O que eu preciso saber antes de começar...

Tipo de serviço -> Os bits de tipo de serviço (type of service – **TOS**), servem para distinguir os diferentes tipos de datagramas IPS, eles podem ser manipulados quando a rede está sobrecarregada.

Tempo de vida -> Time to live (**TTL**), é incluído para que os datagramas não fiquem circulando para sempre na rede, gerando tráfego. Esse campo é decrementado uma unidade, cada vez, que passa por um roteador. Se o TTL chegar a zero o datagrama deve ser descartado.

OBS: Utilizando a tabela Mangle do **Netfilter** podemos manipular estes dois campos.



Club Linux

Linux sem segredos

Regras em Nível de Rede

- Veja abaixo, alguns exemplos de Regras em Nível de Rede:

Bloqueando a Rede 192.168.0.0/24 de enviar pacotes ICMP Echo Request

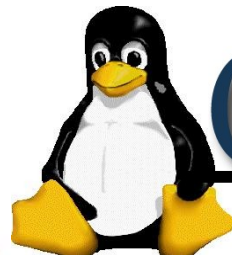
```
# iptables -A FORWARD -p icmp -icmp-type 8 -s 192.168.0.0/24 -j DROP
```

Bloqueando o endereço IP 192.168.0.35 de acessar o IP 200.221.2.45

```
# iptables -A FORWARD -s 192.168.0.35 -d 200.221.2.45 -j DROP
```

Priorizando o processamento do tráfego de saída FTP data

```
# iptables -t mangle -A POSTROUTING -p tcp -sport 20 -j TOS --set-tos 8
```



Club Linux

Linux sem segredos

Conhecendo o Elenco...

ETHERNET

FDDI

ATM TOKEN RING ETC..

Camada Física



Club Linux

Linux sem segredos

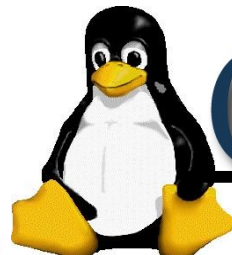
O que eu preciso saber antes de começar...

Preâmbulo	Endereço Mac Destino	Endereço Mac Origem	Tipo	Dados	CRC
-----------	----------------------	---------------------	------	-------	-----

Campo de dados (46 a 1500 bytes) -> este campo carrega o datagrama **IP**.

A unidade máxima de transferência (**MTU**), do quadro **Ethernet** é 1500 bytes.

Quadro Ethernet



Club Linux

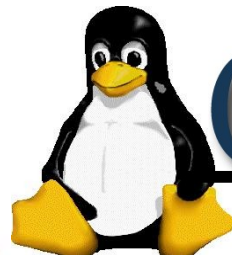
Linux sem segredos

Regra em Nível de Camada Física

- Exemplo de Regra em Nível de Camada Física:

Impedindo o Mac Address 00:40:F4:5D:AB:F8 de encaminhar pacotes pelo Firewall.

```
# iptables -A FORWARD -m mac --mac-source 00:40:F4:5D:AB:F8 -j DROP
```

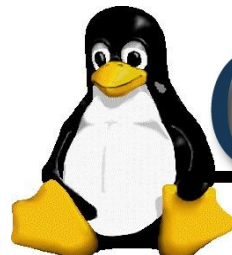


Club Linux

Linux sem segredos

Stateless X Statefull

- Com um filtro de pacotes **STATELESS**, todos os pacotes são tratados como pacotes individuais, ou seja, todo pacote recebido é considerado novo. Você terá que tratar no Firewall o sentido completo de uma comunicação.
- Com um filtro de pacotes **STATEFULL**, podemos trabalhar com o **estado de uma conexão**. No **Netfilter** o mapeamento lógico connection track (**conntrack**), é que permite a implementação de um firewall baseado no estado da conexão.

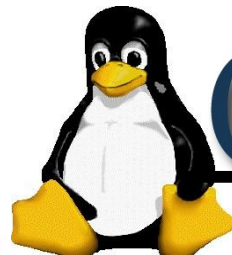


Club Linux

Linux sem segredos

Conexão TCP & Contrack

- 1** -> Cliente envia pacote **SYN**
- 2** -> Firewall com Netfilter classifica o pacote como NEW
- 3** -> servidor responde com um **SYN/ACK**
- 4** -> Firewall com Netfilter classifica o pacote como ESTABLISHED

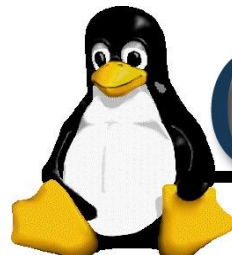


Club Linux

Linux sem segredos

UDP & Conntrak

- 1** -> Cliente envia pacote **UDP**
- 2** -> Firewall com Netfilter classifica o pacote como NEW
- 3** -> servidor responde a requisição do cliente
- 4** -> Firewall com Netfilter classifica o pacote como ESTABLISHED

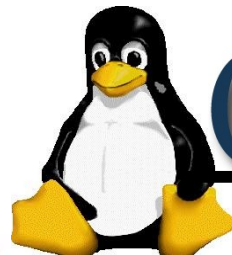


Club Linux

Linux sem segredos

ICMP & Conntrak

- 1 ->** Cliente envia pacote **ICMP echo request**
- 2 ->** Firewall com Netfilter classifica o pacote como NEW
- 3 ->** servidor responde a requisição do cliente com um **ICMP echo reply**
- 4 ->** Firewall com Netfilter classifica o pacote como ESTABLISHED



Club Linux

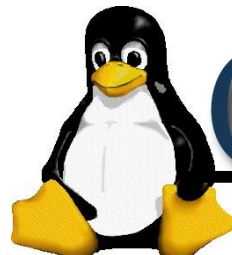
Linux sem segredos

Estado da Conexão

- Exemplo de Regra para trabalhar com o estado da conexão:

Garantindo resposta as requisições feitas a partir do Host

```
# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

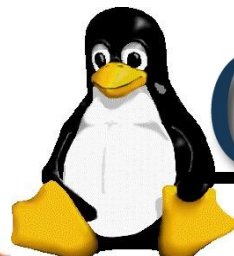


Club Linux

Linux sem segredos

Dicas importantes...

- Utilize ferramentas como o **HPING**, **NMAP** e **NESSUS** para validar o seu firewall
- Verifique se o seu firewall esta trabalhando com o estado da conexão (**STATEFULL**).
- Se você ainda usa o **Ipchains**, mude imediatamente para o **Netfilter/Iptables**
- Verifique se a versão do **Kernel** do Linux que você está utilizando não apresenta vulnerabilidades



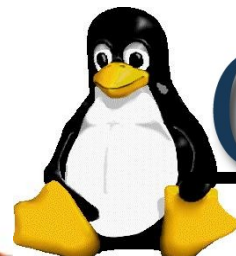
Club Linux

Linux sem segredos

Não existe segurança 100 %



Papillon, aqui interpretado no cinema por Steve McQueen, ao lado de Dustin Hoffman, conseguiu fazer o que muitos achavam impossível, fugir da ilha do diabo, uma prisão de segurança máxima.

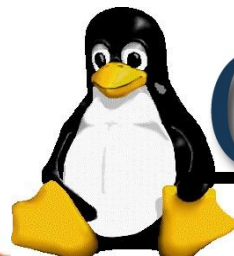


Club Linux

Linux sem segredos

Referências Utilizadas

- www.netfilter.org
- Redes de Computadores e a Internet, uma nova abordagem – James F Kurose – Keith W Ross
- www.frozentux.net
- www.ietf.org
- www.google.com.br
- www.wikipedia.org



Club Linux

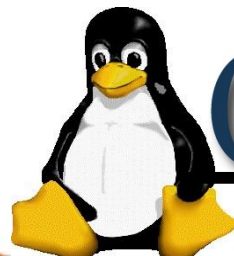
Linux sem segredos

Contato

**Palestrante: Flávio Cunha
(Perukka)**

www.clublinux.com.br

OBRIGADO !!!



Club Linux

Linux sem segredos