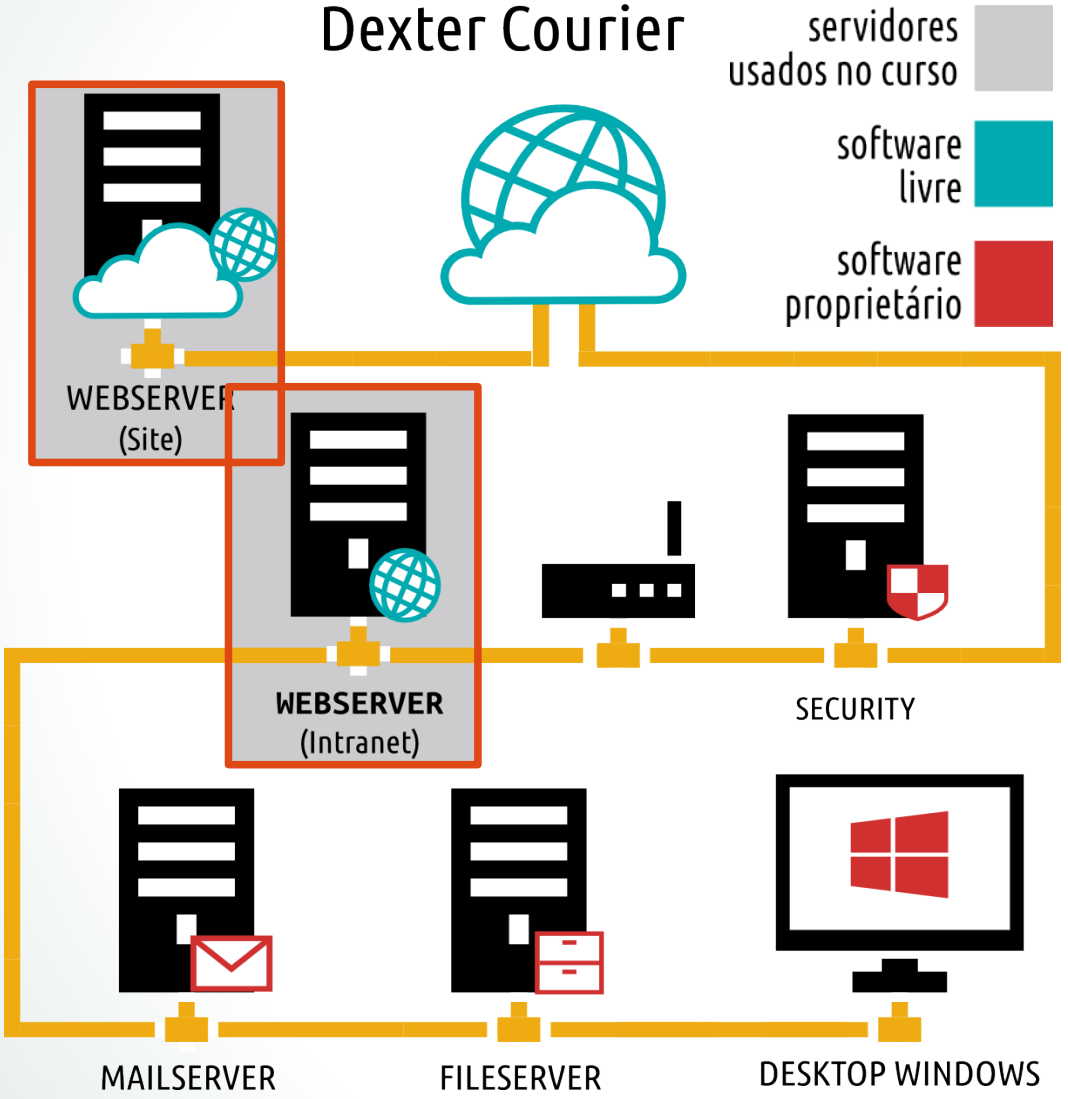

4LINUX
FREE SOFTWARE SOLUTIONS

Só na 4Linux você aprende MUITO MAIS!

TCPWrappers

IT Experience



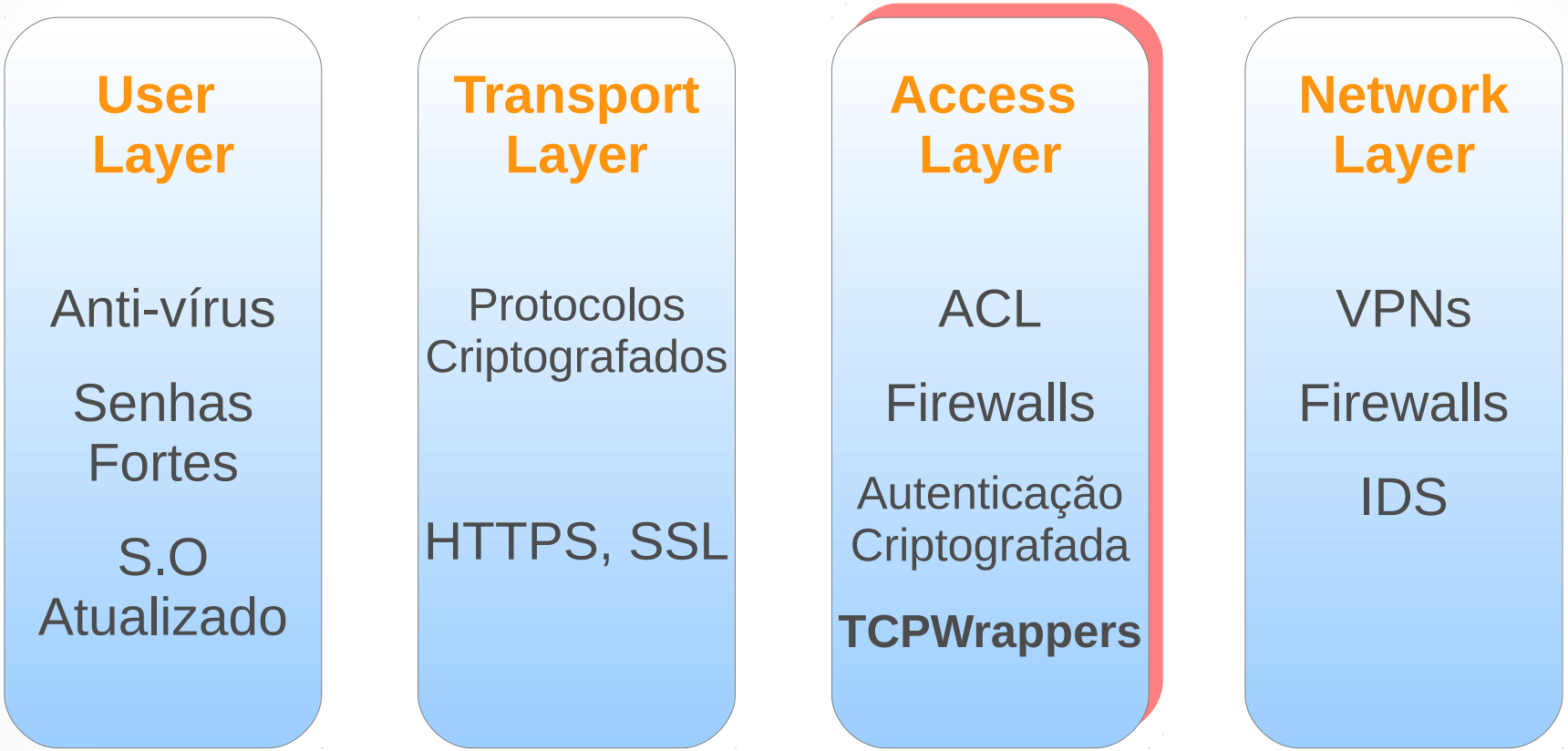
Nesta Aula:

- Usaremos os Servidores da Dexter:
- WebServerInterno

Objetivos da Aula

- Entender o Serviço TCPWrappers;
- Definir acessos ao Servidor WebServerInterno;
  - Configurar o arquivo /etc/hosts.allow
  - Configurar o arquivo /etc/hosts.deny

TCPWrappers

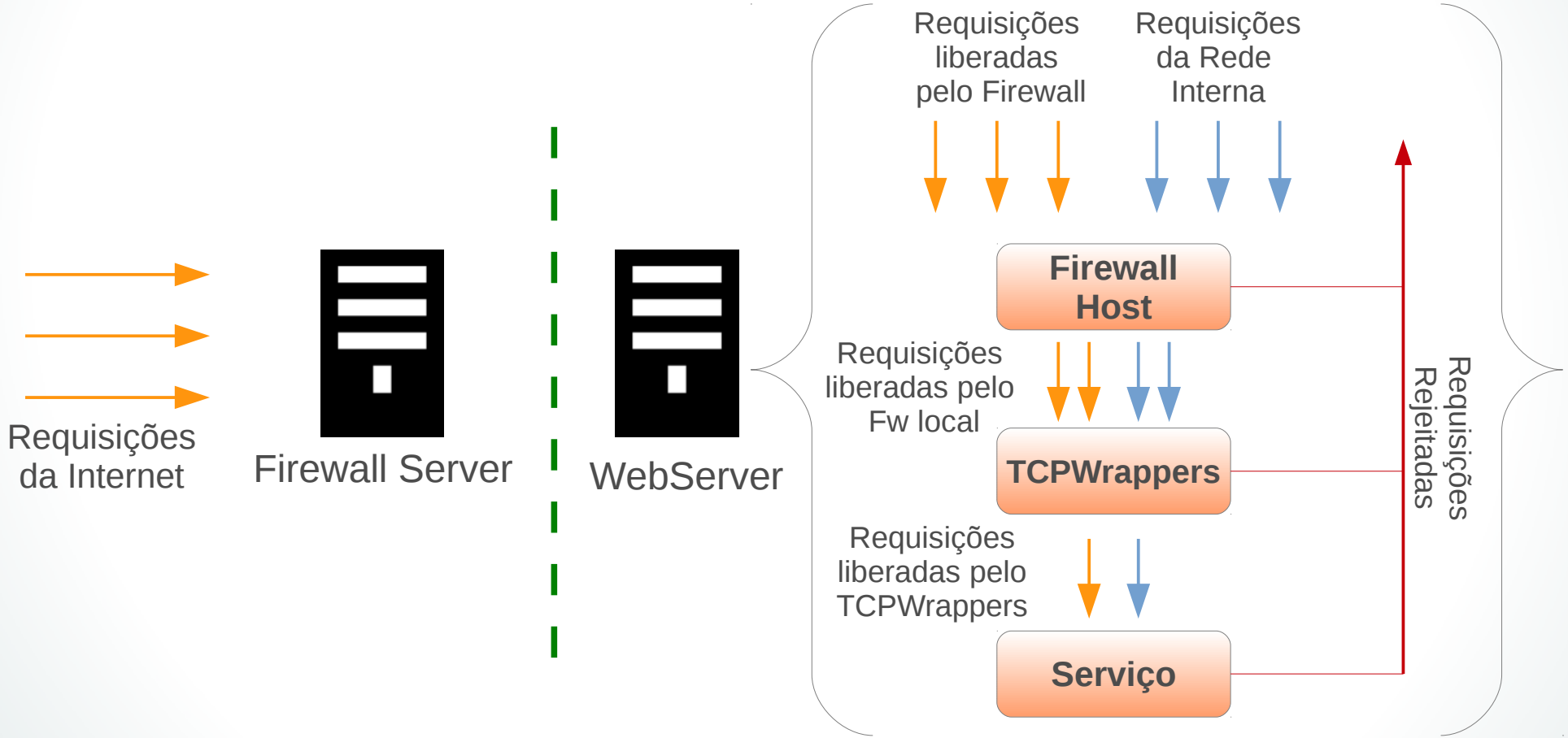


TCPWrappers

- Controlar o acesso aos serviços de rede é uma das tarefas de segurança mais importantes para um SysAdmin.
- Existe uma variedade de ferramentas que nos auxiliam nessa tarefa, como firewall com iptables, ferramentas de detecção de intruso (IDS), dentre outras.
- O TCPWrappers é uma ferramenta para adicionar uma camada a mais de proteção no acesso a serviços de redes.

Camadas de Proteção

- Diagrama Básico das Camadas de Proteção:



TCPWrappers

- O TCPWrappers se resume basicamente em 2 arquivos de controle de acesso:

  /etc/hosts.allow → Regras de liberação de Acesso;

  /etc/hosts.deny → Regras de bloqueio de Acesso;

- O arquivo hosts.allow tem prioridade pois é o primeiro a ser lido.

- Se um cliente é liberado para se conectar, o TCPWrappers libera o controle da conexão para o serviço solicitado e não participa mais na comunicação entre o cliente e o servidor.

TCPWrappers

- Suporte ao TCPWrappers:

```
1# which sshd
2# ldd /usr/sbin/sshd
3# ldd /usr/sbin/sshd | grep wrap
   libwrap.so.0 => /lib/libwrap.so.0...
4# ldd /usr/sbin/httpd | grep wrap
```

Humm... Nenhuma saída!

Fique atento aos serviços que possuem suporte o TCPWrappers. Repare que enquanto o SSH tem suporte, o Apache não tem.

Para que seja possível realizar controle de acesso pelo TCPWrapper primeiramente você precisa verificar se o serviço em específico tem **suporte a biblioteca libwrap**.

O comando **ldd** é usado para listar todas as bibliotecas de um determinado comando.

No Capítulo sobre Bibliotecas você verá mais detalhes sobre o ldd.

TCPWrappers

- Sintaxe dos Arquivos de Controle de Acesso:

<daemon list>: <client list> [: <option>: <option>: ...]

<daemon list> → Uma lista separada por vírgula de nomes de serviços (como é apresentado no processo) ou o carácter ALL.

<client list> → Uma lista separada por vírgula de host (IP ou FQDN).

<option> → Uma ação opcional ou lista separada por dois pontos de ações realizadas quando a regra é acionada.

TCPWrappers

- Bloqueando o acesso de toda rede ao servidor da Dexter Courier.

```
# vim /etc/hosts.deny
   sshd: 192.168.20*.      (Representa toda rede 192.168.20*.0)
```

Tente acessar o servidor WebServerInterno pela Máquina Física.

TCPWrappers

- Verificando o Acesso :

Abra um Terminal na Máquina Física.

Aplicativos > Acessórios > Terminal

```
1# ssh root@192.168.20*.X
ssh_exchange_identification: Connection closed by remote host
```

Tente acessar o Servidor WebserverInterno pela Máquina Física.

TCPWrappers

- O bloqueio está sendo realizado porém não temos log dos acessos negado. Para isso usamos a opção spawn do tcpwrappers:

```
1# vim /etc/hosts.deny
  sshd: 192.168.20*.   :spawn /bin/echo "$(date) - Conexao Recusada - SSH - %a" >> /var/log/tcpwrappers_deny.log

2# tail -f  /var/log/tcpwrappers_deny.log  (Monitorar o Log)
```

Tente acessar o servidor WebServerInterno pela Máquina Física.

TCPWrappers

- Toda rede está bloqueada, agora libere o acesso apenas para o IP da sua máquina física.

Dica:

O bloqueio da rede foi realizada no arquivo /etc/hosts.deny. Agora temos que liberar o acesso apenas para um determinado IP.

TCPWrappers

- Toda a rede está bloqueada, agora libere o acesso apenas para o IP da sua máquina física.

```
# vim /etc/hosts.allow
   sshd: 192.168.20*.X          (O X representa o IP
da sua máquina física)
```

Tente acessar o servidor WebServerInterno pela Máquina Física.

Pergunta LPI

Qual arquivo do sistema contém a lista de hosts que não podem acessar os serviços da máquina?

A. /etc/hosts/denial

B. /etc/hosts.deny

C. /etc/deny.hosts

D. /etc/host.deny

E. /etc/tcpwrappers.deny

Pergunta LPI

Qual arquivo do sistema contém a lista de hosts que não podem acessar os serviços da máquina?

A. /etc/hosts/denial

B. /etc/hosts.deny

C. /etc/deny.hosts

D. /etc/host.deny

E. /etc/tcpwrappers.deny

Resposta: B


4LINUX
FREE SOFTWARE SOLUTIONS