Estou fazendo a disciplina de Redes de Computadores. Tenho um trabalho que necessita que eu tenha um computador windows, que será o cliente, e um linux que será o servidor da empresa 316 que vai disponibilizar internet para o cliente. Preciso configurar um roteador com LAN 200.10.0.16 e WAN 192.168.0.8 para que ele não deixe acessar o site bet365.bet.br e mostrar em uma página html o nome do meu grupo (Eric e Frazzon) e uma informação que o acesso foi barrado e o site que foi barrado. Como posso começar a fazer esse trabalho?

**O ChatGPT disse:**

Ótimo, você está lidando com uma tarefa bem prática de redes que envolve:

1. Um cliente **Windows**.
2. Um servidor **Linux** (que será o **roteador/firewall** e provavelmente um **gateway**).
3. Um **roteador** com interfaces LAN e WAN.
4. **Bloqueio de um site específico** (bet365.bet.br).
5. Exibição de uma **página HTML personalizada** quando esse site for acessado.
6. Toda a configuração deve funcionar como se o servidor **disponibilizasse internet** para o cliente.

**📌 Etapas principais do trabalho**

**🔧 Etapa 1: Configuração de rede básica**

**Topologia (simples):**

[CLIENTE WINDOWS] <---> [SERVIDOR LINUX (roteador)] <---> [INTERNET SIMULADA OU REDE EXTERNA]

**IPs sugeridos:**

* **LAN** (cliente e lado interno do servidor):
  + Cliente Windows: 200.10.0.2/28
  + Servidor Linux (interface LAN): 200.10.0.16/28
* **WAN** (interface externa do servidor):
  + Servidor Linux (interface WAN): 192.168.0.8/24
  + Gateway da internet (simulada): 192.168.0.1/24 *(pode ser seu roteador doméstico ou uma rede simulada)*

**🔧 Etapa 2: Ativar roteamento no servidor Linux**

1. Habilite o encaminhamento de pacotes no Linux:

sudo sysctl -w net.ipv4.ip\_forward=1

Para tornar permanente, edite:

sudo nano /etc/sysctl.conf

E descomente (ou adicione):

net.ipv4.ip\_forward=1

1. Crie regras de NAT para compartilhar a internet com o cliente:

# Supondo que a interface WAN se chame enp0s3 e a LAN seja enp0s8 (use `ip a` para ver as interfaces reais)

sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

**🚫 Etapa 3: Bloquear acesso ao site bet365.bet.br**

**Opção A: Usar o Squid Proxy + DansGuardian (mais refinado)**

Você pode instalar o **Squid** (proxy transparente ou manual) e configurar o bloqueio de domínios.

**Opção B: Usar o iptables + DNS + página customizada (mais direto para seu caso)**

Vamos focar nesta por ser mais próxima da proposta do trabalho.

**✅ Abordagem com iptables + redirecionamento de HTTP**

**1. Bloquear acesso ao domínio via DNS**

Você pode resolver o IP do domínio:

dig bet365.bet.br

Ou

ping bet365.bet.br

Vamos supor que o IP seja 185.39.44.20.

**Bloqueie esse IP na porta 80 e 443:**

# Bloquear HTTP e HTTPS para esse IP

sudo iptables -A FORWARD -d 185.39.44.20 -p tcp --dport 80 -j REJECT

sudo iptables -A FORWARD -d 185.39.44.20 -p tcp --dport 443 -j REJECT

💡 Isso bloqueia o tráfego, mas o usuário verá erro de conexão. Para exibir uma **página personalizada**, você precisa interceptar a requisição e redirecioná-la para um servidor web local.

**2. Criar um servidor web para a página de bloqueio**

No servidor Linux, instale um servidor HTTP simples:

sudo apt install apache2

Crie a página HTML:

sudo nano /var/www/html/bloqueado.html

Com o conteúdo, por exemplo:

<!DOCTYPE html>

<html>

<head>

<title>Acesso Bloqueado</title>

</head>

<body>

<h1>Eric e Frazzon</h1>

<p>O acesso ao site <strong>bet365.bet.br</strong> foi barrado pela política da empresa 316.</p>

</body>

</html>

**3. Redirecionar requisições HTTP para a página de bloqueio**

Como o HTTPS é criptografado, não dá para redirecionar sem um proxy transparente com interceptação SSL (mais complexo). Mas com **HTTP**, você pode redirecionar assim:

# Redirecionar todo tráfego HTTP para a página de bloqueio (exemplo básico)

sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -d 185.39.44.20 -j DNAT --to-destination 200.10.0.16:80

**Explicação**:

* Quando o cliente tenta acessar o IP de bet365.bet.br na porta 80, é redirecionado para o servidor local Apache que mostra a página bloqueado.html.

Para garantir que ele veja a página correta, altere a página padrão do Apache para ser o bloqueado.html:

sudo cp /var/www/html/bloqueado.html /var/www/html/index.html

**📁 Resumo do que precisa configurar:**

| **Etapa** | **Descrição** |
| --- | --- |
| 1. Configuração de rede | Interfaces com IPs corretos, cliente acessando via gateway Linux |
| 2. Ativar roteamento/NAT | Encaminhamento de pacotes e internet compartilhada |
| 3. Bloqueio com iptables | Rejeição ou redirecionamento de IP específico do site |
| 4. Servidor web com página | Apache mostrando HTML personalizado com nomes e mensagem de bloqueio |

**🧪 Testes recomendados**

* Verifique se o cliente tem acesso à internet normalmente.
* Teste se consegue abrir bet365.bet.br (deve ver sua página de bloqueio).
* Tente acessar outros sites (ex: example.com) para garantir que o bloqueio é seletivo.
* Use iptables -L -n -v para verificar contadores de pacotes e confirmar que a regra foi ativada.

Se quiser, posso te ajudar com um **script Bash completo** que configura tudo automaticamente ou montar um **roteiro de apresentação** com base nesse trabalho.

Deseja isso também?

**Você disse:**

E apache será utilizado

**O ChatGPT disse:**

Perfeito — se o **Apache** será utilizado, isso confirma que a abordagem correta para o seu trabalho é:

**Interceptar as requisições HTTP destinadas ao site bet365.bet.br e redirecioná-las para o servidor Apache local**, que mostrará uma **página HTML personalizada** com o nome do grupo (Eric e Frazzon) e a mensagem de bloqueio.

**✅ Visão geral do que você vai fazer com o Apache:**

**🔧 1. Instalar e configurar o Apache no servidor Linux**

No seu servidor Linux (roteador), execute:

sudo apt update

sudo apt install apache2

Isso inicia o Apache com uma página padrão (index.html) localizada em:

/var/www/html/index.html

**📝 2. Criar a página de bloqueio personalizada**

Substitua o conteúdo do index.html pela sua página de bloqueio:

sudo nano /var/www/html/index.html

Conteúdo sugerido:

<!DOCTYPE html>

<html lang="pt-BR">

<head>

<meta charset="UTF-8">

<title>Acesso Bloqueado</title>

</head>

<body style="font-family: Arial, sans-serif; text-align: center; margin-top: 100px;">

<h1 style="color: red;">Acesso Bloqueado</h1>

<h2>Grupo: Eric e Frazzon</h2>

<p>O site <strong>bet365.bet.br</strong> foi bloqueado conforme as políticas da empresa 316.</p>

</body>

</html>

Salve e feche com CTRL+O, ENTER, depois CTRL+X.

Reinicie o Apache só por garantia:

sudo systemctl restart apache2

**🚧 3. Interceptar e redirecionar o acesso com iptables**

**Etapas:**

1. **Descobrir o IP do site bloqueado**:

dig +short bet365.bet.br

Vamos supor que o IP retornado seja:

185.39.44.20

*(Verifique isso no momento do teste, pois pode mudar.)*

1. **Criar regra iptables de redirecionamento (NAT)**

Redirecione o tráfego HTTP (porta 80) que iria para o site bloqueado para o seu Apache:

# Suponha que enp0s8 seja a interface LAN conectada ao cliente

# Altere para o nome correto da interface se for diferente

sudo iptables -t nat -A PREROUTING -i enp0s8 -p tcp -d 185.39.44.20 --dport 80 -j DNAT --to-destination 200.10.0.16:80

Isso faz com que quando o cliente tentar acessar http://bet365.bet.br, ele seja levado para o servidor Apache local (que mostra a página personalizada).

**⚠️ Importante: HTTPS não pode ser redirecionado dessa forma**

Se o site for acessado por https://, o navegador verá um erro de certificado (porque o Apache não tem um certificado válido para bet365.bet.br).

Então, **esta solução funciona apenas com HTTP**, o que é aceitável para muitos trabalhos acadêmicos, **desde que você documente isso**.

**✅ Testes finais**

1. No cliente Windows, configure o **gateway padrão como o IP do servidor Linux**, ex: 200.10.0.16.
2. Acesse http://bet365.bet.br no navegador.
3. Você deverá ver a **página de bloqueio personalizada** feita em HTML.

**🧪 Teste alternativo**

Se bet365.bet.br redirecionar automaticamente para HTTPS (o que é provável), você pode testar com um **site HTTP qualquer** para validar o redirecionamento, por exemplo:

* Bloqueie http://example.com ou um site HTTP simples qualquer, usando a mesma lógica.
* Isso ajuda a validar que o Apache + iptables estão funcionando corretamente, mesmo que o site final use HTTPS.

Se você quiser, posso:

* Criar um **script Bash** que configure tudo automaticamente no servidor.
* Gerar um PDF com as **etapas formatadas como relatório técnico**.
* Ajudar com um **roteiro para apresentação oral** do trabalho.

Me avise do que você preferir!

**Você disse:**

eu preciso saber como posso começar esse trabalho, ainda estou perdidio

**O ChatGPT disse:**

Sem problemas, Eric! Vamos começar **do zero**, passo a passo, como se você estivesse começando agora, com explicações bem claras.

**🎯 Objetivo do seu trabalho**

Você precisa simular o seguinte cenário:

* Um **cliente Windows** (por exemplo, um notebook).
* Um **servidor Linux** que:
  + Age como **roteador/firewall** (controla o acesso à internet do cliente).
  + Está com o **Apache instalado** para mostrar uma página de bloqueio.
  + **Bloqueia o acesso ao site bet365.bet.br**.
  + Mostra uma **página HTML personalizada** com nome do grupo e motivo do bloqueio.

**🧩 Estrutura da rede (topologia básica)**

Imagina sua rede assim:

[ Cliente Windows ]

|

(cabo de rede)

|

[ Servidor Linux (com 2 placas de rede) ]

| |

Interface LAN Interface WAN

200.10.0.16/28 192.168.0.8/24

| |

Roteia a rede Sai para a "Internet"

O servidor Linux vai funcionar como um **roteador**: o cliente vai passar por ele para acessar a internet.

**✅ Como começar seu trabalho (passo a passo)**

**🔹 Etapa 1 – Preparar o ambiente (o que você precisa)**

✔️ 1 computador com **Windows** (cliente).  
✔️ 1 computador ou máquina virtual com **Linux** (servidor/roteador).  
✔️ As duas máquinas conectadas por rede (cabo ou rede virtual).  
✔️ O servidor Linux com **duas interfaces de rede**:

* Uma conectada ao cliente (**LAN**).
* Outra conectada à internet real ou simulada (**WAN**).

Se for usar máquinas virtuais, pode configurar isso com **VirtualBox** ou **VMware**.

**🔹 Etapa 2 – Configurar IPs**

**No servidor Linux:**

Use o comando:

ip a

Identifique as duas interfaces (ex: enp0s3 e enp0s8). Configure IPs fixos:

sudo ip addr add 200.10.0.16/28 dev enp0s8 # Interface LAN

sudo ip addr add 192.168.0.8/24 dev enp0s3 # Interface WAN

Ative as interfaces:

sudo ip link set enp0s8 up

sudo ip link set enp0s3 up

**No cliente Windows:**

Configure IP fixo:

* IP: 200.10.0.2
* Máscara: 255.255.255.240
* Gateway: 200.10.0.16
* DNS: (pode usar 8.8.8.8 para teste)

**🔹 Etapa 3 – Ativar roteamento no Linux**

No servidor Linux, execute:

sudo sysctl -w net.ipv4.ip\_forward=1

Para tornar isso permanente:

sudo nano /etc/sysctl.conf

Descomente ou adicione:

net.ipv4.ip\_forward=1

**🔹 Etapa 4 – Compartilhar internet com o cliente**

Suponha que a interface de internet seja enp0s3, e a do cliente seja enp0s8.

Ative o NAT com iptables:

sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

Agora, o cliente deve conseguir acessar a internet!

Teste no navegador do Windows: acesse http://example.com

**🔹 Etapa 5 – Instalar o Apache no servidor**

No servidor Linux, instale o Apache:

sudo apt update

sudo apt install apache2

Crie a página HTML de bloqueio:

sudo nano /var/www/html/index.html

Cole o conteúdo abaixo:

<!DOCTYPE html>

<html>

<head>

<title>Acesso Bloqueado</title>

</head>

<body>

<h1>Acesso Bloqueado</h1>

<p>Grupo: Eric e Frazzon</p>

<p>O site <strong>bet365.bet.br</strong> foi bloqueado conforme as políticas da empresa 316.</p>

</body>

</html>

Salve (Ctrl+O, Enter, Ctrl+X) e reinicie o Apache:

sudo systemctl restart apache2

**🔹 Etapa 6 – Bloquear o site com iptables**

1. Descubra o IP do site:

dig +short bet365.bet.br

Suponha que seja: 185.39.44.20

1. Redirecione tentativas de acesso HTTP ao site para o Apache:

sudo iptables -t nat -A PREROUTING -i enp0s8 -p tcp -d 185.39.44.20 --dport 80 -j DNAT --to-destination 200.10.0.16:80

Isso faz com que o cliente veja sua página de bloqueio ao acessar http://bet365.bet.br.

**✅ Pronto! Você começou seu trabalho!**

Agora você tem:

* 💻 Cliente com Windows com IP fixo e internet via Linux.
* 🌐 Servidor Linux roteando e controlando a internet.
* 🚫 Bloqueio de site específico via iptables.
* 🌍 Página HTML personalizada com Apache.

**🧠 Dica para não se perder**

Pense em blocos:

| **Bloco** | **O que você precisa fazer** |
| --- | --- |
| **Rede** | IPs fixos no cliente e servidor |
| **Roteamento** | Ativar ip\_forward e NAT com iptables |
| **Bloqueio** | Descobrir IP do site e redirecionar com iptables |
| **HTML** | Criar a página e testar no Apache |

Se você quiser, posso te ajudar a **criar um roteiro de comandos para copiar e colar** ou até um **mapa visual da rede**.

Quer ajuda com isso agora?