

SERVIDOR PROXY

Instalação e Configuração

Prof. Fábio Henrique Ribeiro Machado
fabiohenriquerm@gmail.com

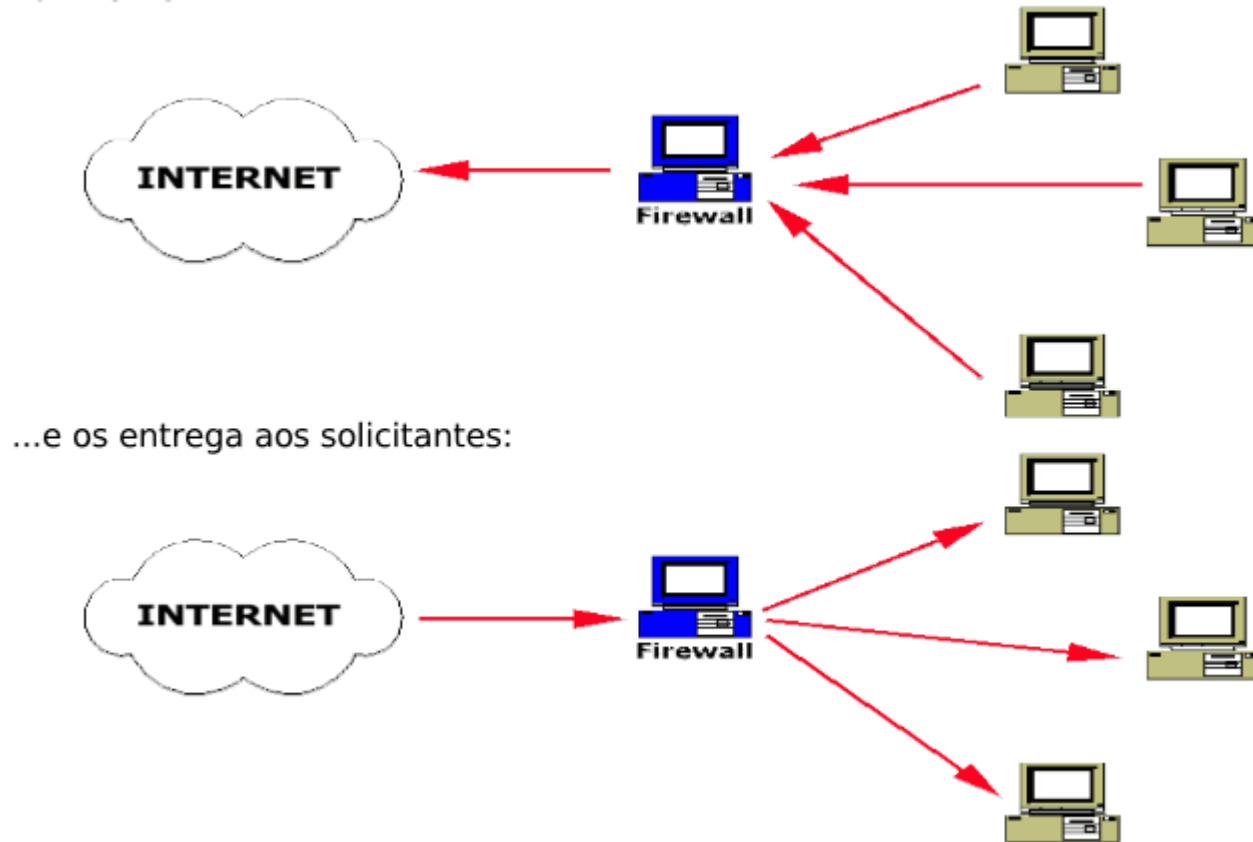


Conexão via NAT - Mascaramento

- Mascaramento é uma forma de fazer NAT (Network Address Translation);
- A rede inteira navega na Internet com segurança, solicitando os dados para a máquina fazer o mascaramento.



Conexão via NAT - Mascaramento



Conexão via NAT - Mascaramento

- Porém, um host não consegue por vontade própria ultrapassar o firewall que faz mascaramento em direção à rede.



Conexão via NAT - Mascaramento

- O único endereço IP que irá circular na Internet será o do firewall;
- O mascaramento também possui um esquema de funcionamento;
- Como haverá trocas de endereços, é necessário utilizar uma tabela NAT.



Conexão via NAT - Mascaramento

- O exemplo mais comum de roteador NAT são os modems ADSL e roteadores Wi-Fi, que muitas vezes oferecem recursos avançados, incluindo firewall e até mesmo QoS (que permite priorizar o tráfego, fazendo com que as chamadas do Skype tenham prioridade sobre os downloads via bittorrent por exemplo). Outro exemplo clássico é um servidor com duas placas de rede, uma para a rede local e outra para a Internet. Depois de configuradas ambas as conexões e ativado o compartilhamento, falta apenas configurar os demais micros da rede local para utilizarem endereços dentro da mesma faixa do servidor e usarem seu endereço de rede local como gateway padrão.



Configuração de Proxy Transparente

- Uma garantia de que os usuários realmente vão usar o proxy e, ao mesmo tempo, uma grande economia de trabalho e dor de cabeça para você é o recurso de proxy transparente.
- Permite configurar o Squid e o firewall de forma que o servidor proxy fique escutando todas as conexões na porta 80. Mesmo que alguém tente desabilitar o proxy manualmente nas configurações do navegador, ele continuará sendo usado.



Configuração de Proxy Transparente

- Outra vantagem é que este recurso permite usar o proxy sem precisar configurar manualmente o endereço em cada estação;
- Basta usar o endereço IP do servidor rodando o proxy como gateway da rede.

Configuração de Proxy Transparente

- Lembrando que, para usar o proxy transparente, você já deve estar compartilhando a conexão no servidor via NAT, como vimos anteriormente;
- O proxy transparente apenas fará com que o proxy intercepte os acessos na porta 80, obrigando tudo a passar pelas suas regras de controle de acesso, log, autenticação e cache, diferente de um proxy tradicional, onde você não ativa o compartilhamento via NAT, fazendo com que o proxy seja a única porta de saída da rede.



Configuração de Proxy Transparente

- Lembrando que, para usar o proxy transparente, você já deve estar compartilhando a conexão no servidor via NAT, como vimos anteriormente;
- O proxy transparente apenas fará com que o proxy intercepte os acessos na porta 80, obrigando tudo a passar pelas suas regras de controle de acesso, log, autenticação e cache, diferente de um proxy tradicional, onde você não ativa o compartilhamento via NAT, fazendo com que o proxy seja a única porta de saída da rede.



Configuração de Proxy Transparente

- Para ativar o proxy transparente, rode o comando abaixo. Ele direciona as requisições recebidas na porta 80 para o Squid:

```
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j \
    REDIRECT --to-port 3128
```

- O "eth0" no comando indica a placa da rede local, onde o proxy recebe as requisições dos outros micros da rede e o "3128" indica a porta usada pelo Squid.



Configuração de Proxy Transparente

- Adicione o comando junto com os 4 comandos que compartilham a conexão no final do arquivo `/etc/rc.local` ou ao seu script de firewall para que ele seja executado durante o boot.



Configuração de Proxy Transparente

- Finalmente, você precisa ativar o suporte ao modo transparente dentro do arquivo `/etc/squid/squid.conf` e reiniciar o serviço;
- Se você está usando uma versão recente, do **Squid 2.6** em diante, a configuração é mais simples. Basta substituir a linha `"http_port 3128"` no início do arquivo por:

`http_port 3128 transparent`



Configuração de Proxy Transparente

- Ou seja, na verdade você precisa apenas adicionar o "transparent" para que o Squid passe a entender as requisições redirecionadas pela regra do firewall.
- No caso das versões mais antigas, anteriores à 2.6 (como a usada no Debian Sarge e no Ubuntu 5.10), é necessário adicionar as quatro linhas abaixo, no final do arquivo "/etc/squid/squid.conf" (nesse caso, sem alterar a linha "http_port 3128"):

```
httpd_accel_host virtual  
httpd_accel_port 80  
httpd_accel_with_proxy on  
httpd_accel_uses_host_header on
```



Configuração de Proxy Transparente

- Em qualquer um dos dois casos, você precisa reiniciar o serviço para que a alteração entre em vigor:

/etc/init.d/squid restart

- Para saber a versão do squid digite o comando:

squid -v



Configuração de Proxy Transparente

- **Em resumo**, ao usar o proxy transparente você vai ter a conexão compartilhada via NAT no servidor e configurará os clientes para acessar através dela, colocando o servidor como gateway da rede. Ao ativar o proxy, a configuração dos clientes continua igual, a única diferença é que agora (graças à nova regra do Iptables) todo o tráfego da porta 80 passará, obrigatoriamente, pelo servidor Squid;
- Isso permite que você se beneficie do log dos acessos e do cache feito pelo proxy, sem ter que se sujeitar às desvantagens de usar um proxy, como ter que configurar manualmente cada estação.



Configuração de Proxy Transparente

- Uma observação importante é que esta configuração de proxy transparente **não** funciona em conjunto com o sistema de autenticação incluso no Squid;
- Ao usar o proxy transparente a autenticação deixa de funcionar, fazendo com que você precise escolher entre as duas coisas.

Configuração de Proxy Transparente

- Outra limitação importante do uso do proxy transparente é que ele atende apenas ao tráfego da porta 80. Como a conexão é compartilhada via NAT, todo o tráfego de outros protocolos (incluindo páginas em HTTPS, que são acessadas através da porta 443) é encaminhado diretamente, sem passar pelo proxy;
- Ou seja, embora seja uma forma simples de implementar um sistema de cache e algumas restrições de acesso, o uso do proxy transparente está longe de ser uma solução ideal.



Configuração de Proxy Transparente

- Em situações onde você realmente precisa ter controle sobre o tráfego da rede, a única opção acaba sendo utilizar um proxy "normal", sem NAT;
- Uma solução para reduzir seu trabalho de administração nesse caso é implantar um sistema de configuração automática de proxy nos clientes.

