LABORATÓRIO XVIII

Servidor Proxy não Transparente
instalado no Gateway

Redes de Computadores – Da Teoria à Prática com Netkit

Laboratório XVIII – Servidor Proxy instalado no Gateway

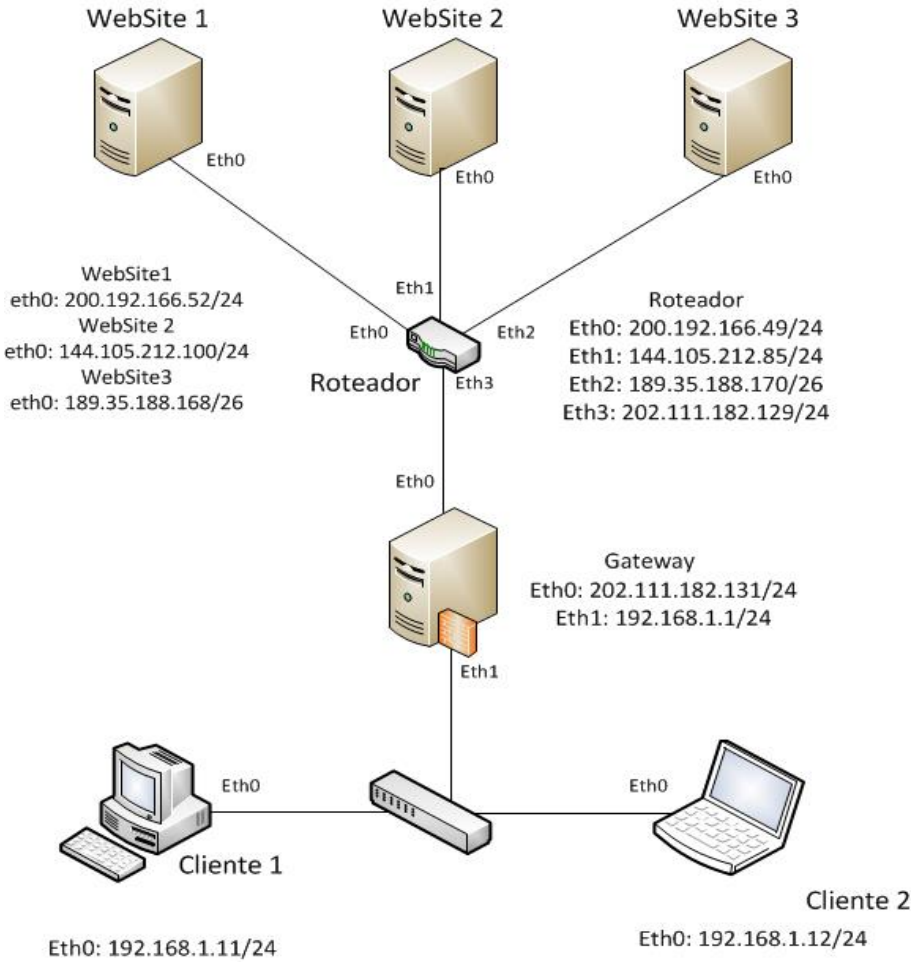
Objetivos do laboratório

- Aprender sobre servidores proxy e Squid
- Criar novas regras de controle
- Modificar autenticação dos usuários do proxy

Cenário sendo reproduzido

O diagrama abaixo representa a topologia de rede a ser estudada. Temos dois computadores, Cliente 01 e Cliente02, conectados por um hub no gateway da rede local. Neste gateway existe um servidor proxy instalado sendo utilizado para filtragem das requisições HTTP dos Clientes. Existem também três servidores web, cada um contém um arquivo HTML diferente, no intuito de identificar o servidor.

O roteador é neste cenário é uma simplificação da internet, criando a conexão entre os elementos da rede.



Conhecimentos de rede que você irá adquirir

Neste laboratório iremos explorar as configurações da ferramenta Squid para criação regras para o controle de acesso HTTP e fazer modificações nos arquivos de autenticação do servidor proxy.

Execução do laboratório

Importante: Antes de fazer a execução deste lab, você deve seguir os seguintes requisitos:
Se você estiver no laboratório da universidade logado com um usuário com quota de disco limitada, verifique se você possui espaço suficiente para as atividades. Considere também que ao invés de utilizar /export/home/seu_usuário, você deverá fazer os labs na pasta /tmp

1. [real] Salve o arquivo netkit_labX.tar.gz em sua pasta de labs (/home/seu_usuario/nklabs).

2. [real] Acesse a pasta nklabs a partir do terminal

3. [real] Utilize o comando para descompactar a pasta:
   [seu_nome@suamaquina_~]$ `tar –xf netkit_labX.tar.gz`

   A pasta labX sera descompactada dentro da sua pasta nklabs

4. [real] Use o comando:
   [seu_nome@suamaquina_~]$ `lstart –d /home/seu_nome/nklabs/labX`

Serão inicializadas 07 máquinas virtuais. As interfaces de rede já estão configuradas com os IP's mostrados no diagrama e nos três servidores web os sites ja estão rodando.

5. A partir da máquina SERVIDOR, utilize o comando:
   [seu_nome@suamaquina_~]$ `/etc/init.d/squid restart`

Esse commando iniciará o squid.

6. A partir de um dos clientes, abra o web browser links

[seu_nome@suamaquina_~]$ `links`

Quando o links for inicializado, uma mensagem de boas vindas aparecerá aperte ENTER. A tela ficará preta, para acessar a barra de ferramentas aperte ESC e usando as setas do teclado, vá até a aba `Setup -> Network options -> Proxies`.

7. No campo `HTTP proxy`, insira `192.168.1.1:3128`

O primeiro campo corresponde ao ip da máquina que o Squid está rodando e o segundo campo é a porta definida para o Squid. Neste lab, foi seguido o padrão da ferramenta e utilizado a porta 3128. Dê OK nas configurações e volte para a pagina inicial do links.

8. Aperte `ESC` e vá em `File -> Go to URL`, como nosso lab não possui um servidor DNS, será necessário a utilização dos IP dos sites.

9. Digite o IP do site 3, `189.35.188.168`.

Nosso Squid está configurado para pedir a autenticação no sistema. Existem três usuários cadastrados no nosso lab: o usuário foo, com nivel de acesso completo, logo podendo acessar qualquer um dos sites, o usuário bar, com nível de acesso 2, ou seja, é possível acessar os websites 1 e 2 e o usuário foobar, com nível de acesso 3, capaz apenas de acessar o site 1. A senha de cada usuário é seu próprio login.

10. Faça a autenticação como o usuário foobar

O sistema pediu a autenticação novamente, isso ocorre porque o usuário não tem acesso ao site 3.

11. Tente fazer o acesso com o usuário bar e depois com o foo

12. Tente acessar o site 2 (`144.105.212.100`)

13. Tente acessar o site 1(`200.192.166.52`)

14. Feche o links

15. No SERVIDOR, vá até a pasta do squid, `cd /etc/squid`

16. Digite o comando `vi squid.conf`

Caso o estudante não deseje utilizar o vi, basta criar uma cópia da pasta squid em sua home com o comando `cp –r /etc/squid/ /hosthome/` e usar o editor de sua preferência. Lembre-se de copiar a pasta modificada de volta, com o comando `cp –r /hosthome/squid /etc/squid/` antes de iniciar o squid.
O squid.conf, é composto essencialmente por configurações e ACL's, que são as regras impostas pelo servidor.
Agora, vamos inserir uma nova regra:

17. Crie a regra abaixo logo acima da acl "blockws2"
    Para criar a acl digite: `acl blockws1 dst 200.192.166.52`
    E na linha de baixo: `http_access deny all`

Na primeira linha, o primeiro argumento significa a declaração de uma nova regra, seguida pelo seu nome, o comando dst significa que será passado um ip no próximo argumento, por fim o IP do site bloqueado. A segunda linha faz o bloqueio do acesso a todos.

18. Reinicie o squid com o comando `/etc /init.d/squid restart`

19. Utilizando o links em qualquer cliente, configure o browser para acessar o proxy e tente abrir o site 1 (`200.192.166.52`)

20. Feche o links

21. Vamos agora criar novo usuário para autenticação no servidor. Use o comando: `htpasswd squid_passwd acme`. Defina uma senha para este usuário.

22. Vá para a pasta acesso e crie um novo arquivo chamado acesso_site1 e insira o nome do novo usuário criado.

    Iremos criar uma nova lista de acesso, para que somente o usuário acme possa acessar o website1.

23. Abra o `squid.conf`

24. Nas regras de acesso, insira: `acl acessows1 proxy_auth "etc/squid/acessos/acesso_site1"`

25. Na linha de baixo da regra blockws1, modifique o acesso para `http_access deny !acessows1`

    Essa regra faz o bloqueio do site 1 para todos os usuários que não estiverem na lista da regra "acessows1". Note o sinal de negação "!" na frente da lista.

26. Reinicie o squid com o comando `/etc/init.d/squid restart`

27. Abra o links na máquina CLIENTE01 e na máquina CLIENTE02

28. Configure o proxy nas duas máquinas

29. Agora na máquina CLIENTE01, tente acessar o site 01(`200.192.166.52`), e faça a autenticação com o usuário acme

30. Na máquina CLIENTE02, acesse o site 01(`200.192.166.52`), e tente faze a autenticação com os demais usuários.

31. [real] Use o comando a seguir para encerrar o experimento:
    [seu_nome@suamaquina_~]$ `lhalt -d /home/seu_nome/nklabs/labX`

32. [real] Use o comando a seguir para limpar os arquivos temporários:
    [seu_nome@suamaquina_~]$ `lclean -d /home/seu_nome/nklabs/labX`

Formule as teorias

1. Se o usuário foo pode ter acesso a todos os sites, porque quando criamos a regra `blockws1` no passo 16, esse usuário perdeu o acesso ao site 1?
2. O que acontece se algum usuário desconfigurar a configuração do proxy no web browser? Como detectar isso?
3. É possivel fazer um filtro de palavras no Squid, assim se qualquer palavra contida nessa lista aparecer em algum site, esse site é automaticamente bloqueado. Que tipo de problemas isso pode trazer?

Aprendendo um pouco sobre linux

Este laboratório mostrou como utilizar a ferramenta Squid no ambiente linux para fazer o controle de requisições HTTP de uma rede. Mesmo sendo uma ferramenta proxy, o Squid ainda tem diversas funcionalidades adicionais, como por exemplo, controle da banda.

É possível no Squid, fazer uma lista de palavras que são proibidas, logo sempre que algum site possuir qualquer uma dessas palavras, esse site será bloqueado automaticamente. Entretanto esse filtro deve ser utilizado com muito cuidado.