

ADMINISTRAÇÃO CENTRALIZADA E SINCRONIZADA DE SERVIDORES PROXY USANDO SQUID

Gabriel R. OLIVEIRA¹; Chrystian da S. MARQUES²; Vinícius F. de SOUZA³

RESUMO

Este trabalho apresenta uma solução para centralizar e sincronizar a administração de servidores proxy usando o software livre squid. Tal solução foi implementada em uma empresa composta por quarenta filiais, na qual todas as filiais utilizam um servidor proxy para monitorar o acesso web. Por meio da configuração do squid na matriz, foi possível centralizar todas as alterações de proxy e replicá-las aos servidores de cada filial, de modo sistematizado e automatizado. Essa implementação proporcionou a redução do tempo gasto na atualização dos servidores e evitou que algum servidor ficasse desatualizado em função da configuração realizada manualmente.

Palavras-chave: Proxy; Squid; Sincronização; Web.

1. INTRODUÇÃO

Atualmente, as organizações utilizam diversas ferramentas para realizar a filtragem de conteúdo web. O objetivo dessa filtragem é permitir ou negar acesso às informações em redes com base nas regras explícitas em uma política de segurança (GURGEL et al., 2015).

A ferramenta *Squid* é um dos proxies para Linux mais utilizados na Internet. Trata-se de um software robusto, simples e confiável, que melhora o desempenho da conexão e permite criar regras de acesso para servidores web. O squid é software livre, nativo da plataforma Linux, mas que pode ser executado em outras plataformas. Atua como um servidor proxy para alguns serviços específicos da camada de aplicação, tais como HTTP (*Hypertext Transfer Protocol*) e FTP (*File Transfer Protocol*) (MARCELO, 2006).

Um servidor *Proxy* é um agente, localizado entre o cliente e o servidor destino, no qual existe uma lista de regras que valida qualquer requisição ou resposta, permitindo ou negando

¹ Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – Campus Inconfidentes. Inconfidentes/MG - E-mail: g.rezende.oliveira@gmail.com

² Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – Campus Inconfidentes. Inconfidentes/MG - E-mail: chrystianmarques2007@gmail.com

³ Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – Campus Inconfidentes. Inconfidentes/MG - E-mail: vinicius.souza@ifsuldeminas.edu.br

o acesso. Esse filtro funciona por meio de regras impostas pela política da rede, podendo assim bloquear determinados sites, protocolos ou conteúdo de mensagens, o que representa uma grande vantagem no ambiente corporativo, pois, com esse bloqueio, os funcionários têm menos chance de se distraírem, reduzindo a sua produtividade (GURGEL et al., 2015).

Outra vantagem, é a capacidade de armazenamento temporário de documentos. Uma cópia da página acessada é colocada no *cache* do proxy, que é uma área com um tamanho especificado pelo administrador e que contém as requisições ao sistema. Desse modo, caso um usuário acesse a mesma página a partir de outra estação, o proxy fornece para esse usuário a página contida em seu cache, o que otimiza o acesso à Internet. Além disso, o proxy pode ser utilizado como ferramenta para auditoria de acessos, já que possui a capacidade de armazenar em seus arquivos de log todas as conexões realizadas (MARCELO, 2006).

Este trabalho apresenta uma solução que foi implementada em uma empresa, localizada na cidade de Estiva/MG, que possui quarenta filiais e cada uma utiliza um servidor proxy para controlar o acesso web. Com a administração descentralizada dos servidores proxy de cada filial, a atividade de liberação ou bloqueio de páginas web ou usuários exigia, por parte do administrador da rede, um tempo considerável para a execução dessa tarefa. Além disso, a execução de uma tarefa repetitiva é altamente propensa à falha humana.

A configuração proposta utilizou o squid com o objetivo de centralizar e sincronizar as atualizações e alterações que são realizadas em cada filial, reduzindo assim o tempo consumido para efetuar a configuração manual e evitando que algum servidor ficasse desatualizado.

2. MATERIAL E MÉTODOS

Para a realização deste trabalho, foram utilizadas as seguintes versões de softwares: Linux Debian 7.0, Squid 3.1.20, OpenSSH 6.0p1 e Rsync 3.0.9. O squid foi instalado em todas as filiais para funcionar como servidor proxy. A solução proposta é independente da versão do squid, pois manipula apenas arquivos de configuração do mesmo.

A Figura 1 representa, de forma esquemática e simplificada, a topologia de rede empregada nesta implementação. A estação cliente não tem acesso direto ao servidor web na Internet. Como o servidor proxy está ciente de toda a comunicação web da rede interna, é possível armazenar as requisições e as respostas de cada cliente na rede interna, mantendo um histórico arquivado, e usar essas informações para um maior controle da rede.

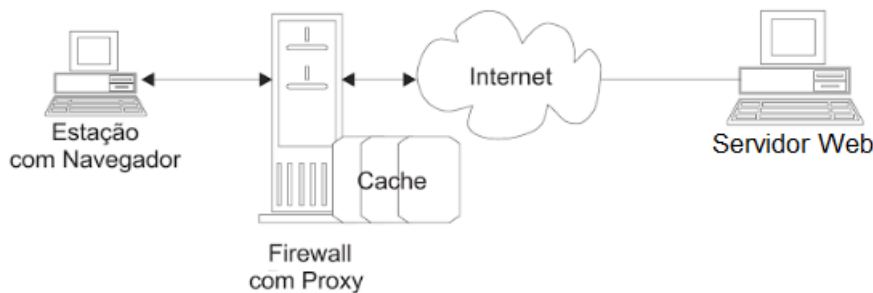


Figura 1 - Representação da topologia de rede com firewall proxy (MARCELO, 2006).

A linguagem utilizada para o script na edição dos arquivos foi a Shell Script. O rsync foi usado para sincronizar o conteúdo das pastas, de forma a transferir somente as modificações realizadas. O rsync verifica o conteúdo de cada arquivo e, caso somente uma parte do arquivo seja alterada, apenas essa modificação é transferida, sem a necessidade de copiar todo o arquivo novamente (MORIMOTO, 2009).

O crontab foi aplicado para agendar a periodicidade (na configuração utilizada, a cada dois minutos) na qual cada filial conecta-se à matriz para verificar se há alguma alteração nas regras do squid. Após a leitura da pasta do squid, havendo alguma alteração, ela é copiada para o squid da filial. O registro da operação é armazenado em log, identificando o horário da conexão e qual filial fez a atualização, o que permite o monitoramento das atualizações realizadas em cada filial (RICCI; MENDONÇA, 2006).

Para a conexão entre matriz e filiais foi utilizado o protocolo SSH, que oferece um serviço de acesso remoto, permite transferir arquivos em diferentes formatos e, também, encapsular outros protocolos. O túnel SSH proporciona maior segurança na transferência de dados, visto que o protocolo requer autenticação, utiliza criptografia para proteger as mensagens trocadas e mantém a integridade da conexão estabelecida (MORIMOTO, 2009).

4. RESULTADOS E DISCUSSÕES

A centralização da administração dos servidores proxy das filiais, com o uso do squid, trouxe unidade à configuração das regras de liberação/bloqueio de páginas. Assim, o servidor da matriz concentra todas as informações e, quando necessário, realiza as alterações nos servidores de cada filial.

O processo passou a ocorrer de forma automatizada e sistematizada, o que reduziu o tempo total de configuração das alterações em todos os servidores e eliminou a possibilidade de algum servidor ficar desatualizado ou apresentar um erro de configuração local.

Estimou-se, por observação, que o tempo médio gasto pelo administrador da rede para liberar ou bloquear determinada página web era de três minutos e meio. Portanto, para executar essa mesma tarefa em quarenta servidores, o tempo gasto seria de, aproximadamente, duas horas e meia. Após a automatização do processo, o tempo total médio para atualizar todas as filiais foi inferior a cinco minutos.

A abordagem inversa, ou seja, com a matriz conectando-se às filiais também foi testada e mostrou-se ineficaz. Com a matriz responsável por aplicar as modificações em todos os servidores, foi gerado um alto tráfego com o envio dessas atualizações e um elevado processamento na máquina da matriz. Com cada filial sendo responsável por buscar as alterações na matriz, esses problemas foram minimizados.

Qualquer alteração que seja realizada localmente em uma filial, será removida após a próxima sincronização entre os servidores, o que confere à matriz o poder de controlar as alterações realizadas, garantindo a padronização da política de acesso em todas as filiais.

Caso alguma filial fique sem acesso ao servidor da matriz, o acesso à Internet não será comprometido na filial. Quando o acesso à matriz for restabelecido, todas as informações do squid serão atualizadas na próxima sincronização.

4. CONCLUSÕES

A solução proposta para a centralização e sincronização de servidores proxy através do squid garantiu a padronização da política de acesso em todas as filiais, reduziu o tempo total gasto para alterar ou atualizar localmente todos os servidores e eliminou a possibilidade de erro ou desatualização em algum servidor, de forma individual. Todos os arquivos de log ficam disponíveis na matriz, permitindo o controle e o monitoramento das atualizações realizadas. Além disso, a solução apresentada é aberta e independente da versão utilizada do squid, podendo ser implementada em qualquer plataforma que tenha suporte para squid, rsync, crontab e SSH.

REFERÊNCIAS

- GURGEL, P. H. M. et al. **Redes de Computadores:** da teoria à prática com Netkit. Rio de Janeiro: Elsevier, 2015.
- MARCELO, A. **Squid:** configurando o proxy para linux. 5. ed. Rio de Janeiro: Brasport, 2006.
- MORIMOTO, C. E. **Servidores Linux:** guia prático. Porto Alegre: Sul Editores, 2009.
- RICCI, B.; MENDONÇA, N. **Squid:** solução definitiva. Rio de Janeiro: Ciência Moderna, 2006.