

Protótipo de um Sistema para o Gerenciamento de Redes Baseado em Políticas – Estudo de Caso dos Laboratórios de Informática da UNOCHAPECÓ

LIMA, Erich R. Cunha¹; PAZETO, Tatiana A¹.

¹ Centro Tecnológico – Universidade Comunitária Regional de Chapecó
(UNOCHAPECÓ)

Caixa Postal 747 – 89809-000 – Chapecó – SC – Brasil

{erich,tatiana} @unochapeco.edu.br

Resumo. *Permitindo uma visão holística da rede, abstraindo detalhes da configuração dos dispositivos e centralizando a criação e armazenamento de políticas de rede, o Gerenciamento de Redes Baseado em Políticas (PBNM) oferece uma solução para muitos dos problemas relacionados ao gerenciamento. Analisando a arquitetura proposta para o PBNM e seus conceitos, desenvolveu-se um protótipo visando melhor compreender essa tendência e ao mesmo tempo procurando aprimorar a forma de gerenciamento de redes adotada até então nos laboratórios de informática da UNOCHAPECÓ. Ele atende, inicialmente, a área de segurança através do gerenciamento de políticas de firewall em plataformas Linux.*

1 Introdução

Tradicionalmente, o gerenciamento de redes exige que o gerente de rede tenha conhecimento avançado sobre a enorme diversidade de equipamentos e suas formas de gerenciamento específicas. O problema é que a evolução das redes de computadores, através do desenvolvimento de novas tecnologias, juntamente com a velocidade de sua expansão, têm tornado a tarefa de administrar os recursos cada vez mais complexa.

Esse processo de evolução é visível na estrutura da rede dos laboratórios de informática da Universidade Comunitária Regional de Chapecó (UNOCHAPECÓ), onde a expansão do parque computacional tem sido constante ao longo dos anos. Neste aspecto, hoje os equipamentos são gerenciados com o auxílio de diversas ferramentas, sendo que cada dispositivo tem de ser configurado manualmente.

Dentre as diversas arquiteturas para o gerenciamento de redes, aquela que se demonstra promissora é o Gerenciamento de Redes Baseado em Políticas (PBNM). Seu objetivo é afastar o gerente de rede da interação direta com a configuração dos dispositivos, cabendo a este definir as regras de gerenciamento, ou políticas, de uma forma abstrata. Assim, os ajustes nos dispositivos para seguir as políticas definidas são efetuados automaticamente pelo sistema PBNM.

Analisando a estrutura dos laboratórios de informática e a forma como os dispositivos são gerenciados, verificou-se que no momento políticas de segurança seriam de maior importância, visto que o gerenciamento se dá principalmente no controle de acesso aos recursos da rede. Atualmente este controle é realizado basicamente através de *firewall* e *proxy*.

Dessa forma, este trabalho tem o intuito de desenvolver um protótipo que implemente o gerenciamento de redes baseado em políticas nos laboratórios de informática da UNOCHAPECÓ, possibilitando a definição de políticas de *firewall* a serem aplicadas no servidor dos laboratórios.

2 Gerenciamento de Redes Baseado em Políticas (PBNM)

O Gerenciamento de Redes Baseado em Políticas, ou PBNM, é uma proposta que visa diminuir a complexidade atual existente na gerência de redes de computadores. Permite o controle coordenado de uma rede, mediante a automação da maioria, ou mesmo de todos, os dispositivos gerenciados e as tarefas de configuração, tradicionalmente manuais.

Segundo Kosiur (2001), existem inúmeras razões pelas quais o PBNM está se tornando importante para as redes atuais. Por exemplo, não somente os dispositivos têm aumentado em quantidade nas redes, como também se tornaram mais complicados de configurar em função do acréscimo de serviços. Além disso, é cada vez mais difícil encontrar pessoas qualificadas para configurar esses dispositivos, com experiência nos novos algoritmos e técnicas incorporadas aos mesmos.

Para entender o funcionamento de um sistema PBNM, é necessário revisar a arquitetura geral proposta pela Internet Engineering Task Force (IETF) e seus componentes, o que será abordado a seguir.

2.1 Arquitetura Geral

A IETF constituiu um grupo de trabalho, o Policy Framework Working Group, que desenvolveu um framework para a arquitetura de sistemas PBNM. Tal framework inclui os seguintes componentes:

- console de gerenciamento de políticas: corresponde à interface de usuário para criar políticas, aplicá-las e monitorar o estado do ambiente gerenciado;
- Ponto de Decisão de Políticas (PDP – *Policy Decision Point*): é um software que realiza decisões baseado nas regras das políticas e no estado dos serviços que tais políticas gerenciam;
- Ponto de Aplicação de Políticas (PEP – *Policy Enforcement Point*): trata-se de um agente em execução sobre ou dentro de um recurso (por exemplo, um servidor) que aplica uma decisão de política e/ou realiza a alteração de configuração do recurso;
- repositório de políticas: é um diretório e/ou outro serviço de armazenamento (por exemplo, um banco de dados relacional) onde políticas e informações relacionadas são armazenadas (MOREIRA, 200?);
- protocolos de comunicação: provêm a comunicação entre os vários módulos da arquitetura PBNM, como o *Lightweight Directory Access Protocol* (LDAP), o SNMP e o *Common Open Policy Server* (COPS).

Além disso, “é necessária a utilização de uma Linguagem de Definição de Políticas (PDL - *Policy Definition Language*), a qual deve definir regras de sintaxe e

semântica, de forma que possam ser interpretadas pelo PDP” (GONÇALVES, 2003, p.17).

Para entender o funcionamento dessa forma de gerenciamento, é necessário compreender o conceito de políticas, o qual será descrito a seguir.

2.2 Definição de Políticas

Políticas na sociedade e nas organizações são geralmente tratadas em leis, contratos, acordos, memorandos e procedimentos. Em sistemas de computadores, política é uma maneira de declarar e formalizar o comportamento dos sistemas. O PBNM, dessa forma, é a aplicação dos conceitos das políticas organizacionais no gerenciamento de sistemas de computadores. Políticas são formadas por condições e ações. As condições definem as situações nas quais as ações devem ser executadas. (SHERIDAN, 2003).

3 Protótipo para Gerenciamento de Redes Baseado em Políticas

O protótipo é composto por dois softwares. O primeiro, console gerenciador de políticas, foi intitulado Gerenciamento Integrado de Redes Baseado em Políticas (GIRPOL), sendo responsável pelo cadastramento das políticas. O outro, denominado PDP/PEP, age sobre o servidor dos laboratórios de informática, decidindo a aplicação das políticas cadastradas e as transformando em comandos de configuração. Além destes dois programas, existem as políticas propriamente ditas, que são arquivos XML. A estrutura do protótipo pode ser observada na Figura 1.

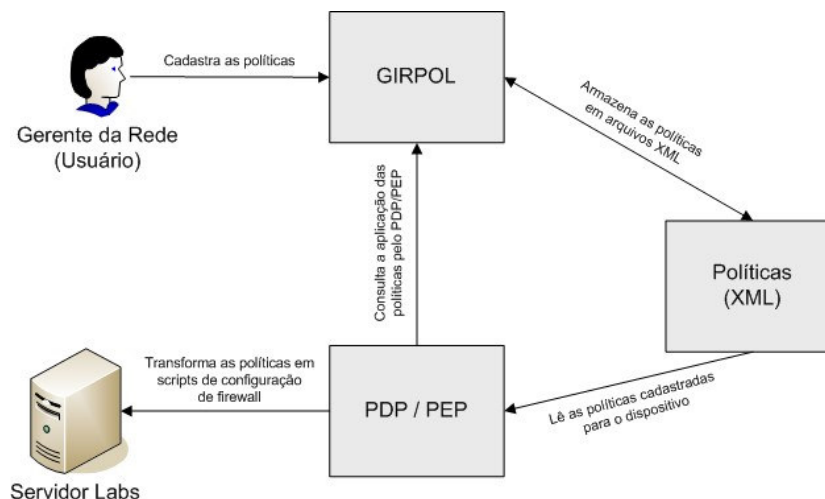


Figura 1. Esquema geral do protótipo

Na Figura, observa-se o gerente da rede que acessa o console GIRPOL via web e efetua o cadastramento das políticas. As políticas e outras informações relacionadas são armazenadas em arquivos XML. O PDP/PEP, por sua vez, lê esses arquivos e verifica a necessidade de aplicar as políticas, com base nos parâmetros das mesmas. Caso seja preciso, ele as traduz em scripts de configuração de *firewall* (as quais são

regras do iptables) para que posteriormente sejam carregadas no servidor com o intuito de aplicar as políticas. Este último processo é realizado com o auxílio da ferramenta de sistema Crontab.

O GIRPOL é um aplicativo desenvolvido em PHP com o propósito de permitir o cadastramento e aplicação das políticas de segurança na rede. Atualmente, este software provê, apenas parcialmente, o gerenciamento de *firewall* de servidores rodando o sistema operacional Linux em suas diversas distribuições. Contudo, os testes foram realizados apenas no CentOS 4.3.

Ao acessar o endereço onde ele está rodando, será exibida uma janela de login de usuário. O usuário deve inserir seu nome de usuário e senha e clicar em “Entrar >>”. Uma vez que o usuário acessou o aplicativo, estão disponíveis três opções que dão acesso às principais funções do protótipo, sendo elas:

- endereços: permite cadastrar endereços IP;
- agendamentos: possibilita definir os períodos em que as políticas irão executar;
- políticas: opção que dá acesso ao cadastramento das políticas bem como possibilita verificar se as mesmas foram executadas.

A seguir será apresentada uma breve explicação de cada uma destas opções.

3.1 Cadastramento de Endereços

Esta opção permite centralizar a definição dos endereços, através da criação de nomes que os representem. Por exemplo, pode-se definir que o endereço 192.168.0.203 seja o de uma impressora de rede. Dessa forma, quando se deseja referenciar tal endereço, utiliza-se o seu nome, facilitando o trabalho de atualização deste endereço em mais de um lugar caso ele seja alterado posteriormente.

3.2 Cadastramento de Agendamentos

A partir de qualquer janela do aplicativo é possível acessar a opção de Agendamentos, utilizando o menu. Estes permitem definir períodos em que as políticas devem ser executadas. Pode-se, por exemplo, condicionar a execução de determinadas regras apenas a finais de semana, ou ainda determinar que políticas entrem em vigor apenas nos cinco primeiros dias de dezembro e janeiro, sempre após as onze horas da noite. As políticas ativas que não utilizam agendamentos serão executadas sempre, enquanto que as políticas que utilizam agendamentos só funcionam se as condições dos agendamentos relacionados forem satisfeitas.

3.3 Cadastramento de Políticas

Ao selecionar a opção de Cadastramento de Políticas, uma janela com a listagem dos dispositivos cadastrados no GIRPol é exibida. O usuário deve selecionar um dispositivo e então a tela seguinte mostra as políticas cadastradas para o mesmo. Essa tela traz três opções: “Incluir”, “Depurar” e “Atualizar”. A primeira permite a inclusão de uma nova política para o dispositivo. A segunda roda o PDP/PEP em modo de depuração (debug) para fazê-lo gerar um script (que é mostrado no GIRPOL) com o intuito de auxiliar o

gerente a verificar como será o script final de configuração do dispositivo. Já a opção “Atualizar” recarrega a página para atualizar a situação das políticas.

A listagem das políticas exibe a identificação da política, sua descrição, a existência de agendamentos ou não, se está habilitada, desabilitada ou marcada para depuração e se ela está em execução ou não no dispositivo. A existência de agendamentos é representada pelo símbolo de um relógio, enquanto a ausência é exibida através do símbolo de infinito, já que nesse caso a política estaria sempre ativa. A Figura 2 apresenta a referida listagem.










	ID	Descrição da Política		Situação da política	Em execução no dispositivo
	P4	Aceitar todo tráfego que se destina ao servidor		Desabilitada	Não
	P5	Bloquear ping no servidor proveniente da Internet		Desabilitada	Não
	P7	Bloquear conexão FTP no servidor		Desabilitada	Não
	GIRPol_Testel	Impedir o PC RT14 de navegar na internet das 23:45 às 23:50		Habilitada	Sim

Figura 2. Políticas cadastradas para o dispositivo

Na Figura constam quatro políticas cadastradas. A última, identificada por “GIRPol_Testel”, foi definida para impedir o acesso do “PC RT14” a páginas da Internet. Está agendada para funcionar das 23:45 às 23:50, encontra-se habilitada e em execução no dispositivo. Esta listagem foi obtida exatamente às 23:45 e por isso a política encontrava-se em execução no dispositivo. Caso o horário fosse outro, mesmo estando habilitada ela não seria executada em função do agendamento cadastrado.

A inclusão de uma política define diversas características que um pacote deve possuir para que a política seja executada. Essas características são as condições da política de *firewall*. Entre as diversas condições que podem ser definidas para a política, estão o protocolo (ftp, http, icmp, entre outros), o endereço de origem, de destino e as portas de origem e destino. Na definição da política, além das condições, também devem ser informadas as ações que serão executadas caso as condições sejam atendidas. As ações para políticas de *firewall* podem ser a aceitação do pacote, o cancelamento, a recusa ou ainda um simples log do mesmo.

3.4 Tradução das Políticas em Scripts de Configuração

As políticas cadastradas são armazenadas em arquivos XML que são lidos a cada minuto pelo segundo módulo do protótipo, o PDP/PEP. Ele foi desenvolvido em C e é carregado de minuto em minuto com o auxílio do *Crontab* existente na plataforma Cent OS assim como nas diversas distribuições do Linux.

O PDP/PEP verifica todas as políticas cadastradas para o dispositivo para o qual está configurado, analisando se existem agendamentos cadastrados para cada política. As políticas não habilitadas são descartadas. Já as habilitadas são verificadas quanto à existência de agendamentos. Caso não exista agendamento, ela é automaticamente traduzida em scripts de configuração de *firewall*. Caso contrário, os agendamentos cadastrados para a política são testados para verificar se seus requisitos são atendidos, como o horário, o dia ou o mês. Caso todos os parâmetros dos agendamentos forem atendidos, então a política será traduzida.

A tradução ocorre através da leitura das políticas a serem aplicadas no dispositivo e posterior gravação dos comandos de *firewall* necessários para realizar as configurações definidas nas políticas. Esses comandos são escritos em scripts *bash*, contendo chamadas ao aplicativo *iptables*, responsável por definir as regras de *firewall*, seguidas de parâmetros de configuração de filtragem de pacotes. Quando o script contendo os comandos de configuração do *firewall* é gerado, verifica-se se ele difere do último script executado no dispositivo. Caso o conteúdo do script for diferente, ele é então executado (aplicado) no dispositivo.

4 Considerações Finais

Através do presente trabalho foi possível observar que o gerenciamento de redes baseado em políticas irá se tornar cada vez mais importante para o gerenciamento eficiente das redes modernas, que crescem tanto em quantidade quanto em complexidade de dispositivos e serviços. Isso se deve principalmente ao fato de que exige do administrador da rede apenas a definição de políticas abstratas enquanto fica a cargo do sistema a implantação dessas políticas nos dispositivos através da tradução em comandos de configuração.

Com o estudo dos conceitos e da arquitetura geral do gerenciamento de redes baseado em políticas, embora ainda não definida por completo, foi possível desenvolver um protótipo para atender as necessidades do gerenciamento dos laboratórios de informática na área de segurança, mais especificamente através da definição de regras de *firewall*. Para isso utilizou-se políticas baseadas nos parâmetros do *iptables*, de forma que o protótipo foi direcionado a sistemas operacionais baseados no Linux.

Os testes efetuados demonstraram que o protótipo desenvolvido, embora passível de diversas melhorias e exigindo conhecimentos de filtragem de pacotes em Linux, facilita a definição e aplicação de políticas de *firewall*, centralizando o gerenciamento. Assim, verificou-se que a evolução da arquitetura de gerenciamento baseado em políticas possibilitará aplicações de tecnologia cada vez mais complexas.

5 Referências

- Gonçalves, Carlos Rairon Ribeiro. (2003) “Utilizando Redes Neurais Artificiais para Predição de Falhas em *Links* de Redes Ópticas”. Dissertação (Mestrado em Ciência da Computação) – Programa de Pós-Graduação da Universidade Federal do Ceará, Fortaleza.
- Kosiur, Dave R. (2001) “Understanding Policy-based Networking”, John Wiley & Sons, Inc, Indianápolis, IN.
- Moreira, Priscilla. (200?) “Policy Based Network Management”, http://services.eng.uts.edu.au/~kumbes/ra/Network_Management/PBNM/48740%20-%20Policy-Based.pdf. Acesso em: 18/08/2004.
- Sheridan, Smith Nigel. (2003) “A Distributed Policy-based Network Management (PBNM) system for Enriched Experience Networks™ (EENs)”. Tese de Doutorado submetida à *University of Technology*, Sydney.