Gestão por políticas: arquitectura e aplicações

Filipe Caldeira[1,2], Edmundo Monteiro[2]
caldeira@di.estv.ipv.pt, edmundo@dei.uc.pt

[1] **Departamento de Informática**
Escola Superior de Tecnologia de Viseu / IPV
Campus Politécnico de Repeses, 3504-510 Viseu
http://www.estv.ipv.pt

[2] **Laboratório de Comunicações e Telemática**
CISUC / DEI – Universidade de Coimbra
Pólo II, Pinhal de Marrocos, 3030-290 Coimbra
http://lct.dei.uc.pt

Palavras chave: PBN, Segurança de redes, Gestão de redes por políticas, COPS, COPS-PR, SPSL.

Resumo

Neste artigo é feita uma abordagem à gestão de redes baseadas em políticas focando a arquitectura PBN (Policy-Based Networking) proposta no âmbito do grupo de trabalho Policy Framework do IETF (Internet Engineering Task Force). São evidenciados os principais aspectos desta arquitectura, desde os protocolos de comunicação até às linguagens de especificação de políticas, passando pelos modelos necessários à representação de informação.

Relativamente às linguagens de especificação de políticas, apresenta-se uma visão geral sobre a sua aplicabilidade na arquitectura PBN. No âmbito dos protocolos de difusão de política, destaca-se o protocolo COPS (Common Open Policy Service) e COPS-PR (COPS for Policy provisioning).

O artigo termina com a descrição de uma aplicação de gestão de firewalls através do uso de políticas. Esta aplicação baseia-se na arquitectura de gestão por políticas (PBN) proposta e aplica a linguagem SPSL e o protocolo COPS-PR.

1. Introdução

Têm sido efectuadas, ao longo dos últimos anos, diversas tentativas para o desenvolvimento de novos métodos de gestão de redes. Actualmente está a ser feito um grande esforço para diminuir a complexidade crescente da administração de redes, recorrendo a novos paradigmas. O modelo de gestão baseado em políticas (PBN – *Policy Based Networking*) [Stevens 1999] pretende ser o resultado da mudança dos actuais mecanismos de configuração para um sistema integrado de gestão.

O modelo PBN pretende criar uma infra-estrutura que permita ao administrador um elevado grau de abstracção acerca das capacidades dos equipamentos que pretende gerir. Esta abstracção permite elevar o nível de controlo do equipamento para o nível da rede, representando também uma transição da gestão de equipamentos e serviços realizada de modo individual em cada equipamento, para a gestão de serviços e equipamentos efectuada no interior do próprio conceito de funcionamento da rede.

A gestão baseada em políticas pretende combinar todos os procedimentos e protocolos que permitem o controlo dos recurso disponíveis, de modo a que estes possam servir de suporte ao modelo de negócio da organização. A gestão baseada neste modelo, deve começar por identificar e conhecer a política global da organização e efectuar a sua aplicação nos sistemas e tecnologias de informação. Após a definição da política global, normalmente estabelecida a um nível hierárquico superior, a política pode então ser traduzida e aplicada nos sistemas e equipamentos.

O objectivo a atingir com a gestão por políticas é a especificação de um conjunto de regras genéricas que podem ser aplicadas num ou em vários equipamentos de rede. Com as ferramentas apropriadas, estas regras genéricas, ou políticas, podem ser criadas, instaladas, monitorizadas, modificadas ou ainda eliminadas dos diversos equipamentos da rede com um pequeno custo operacional independentemente do tipo de equipamento ou fabricante dos equipamentos que

constituem a rede. Para além da criação de políticas, este modelo de gestão pretende construir um sistema de informação uniforme que representa o modo como a rede deve funcionar.

Pretende-se neste artigo apresentar uma arquitectura de gestão por políticas PBN (*Policy Based Networking*) e a sua aplicação à gestão de redes de computadores, com especial detalhe na área de segurança. Assim, pretende-se analisar os mais recentes desenvolvimentos que têm sido levados a cabo sobre esta arquitectura, efectuando, para esse efeito, um estudo acerca dos seus principais componentes. Apresenta-se também uma proposta de aplicação da arquitectura PBN à gestão de *firewalls*.

2. Gestão por políticas

A arquitectura de gestão por políticas (PBN) teve origem no trabalho desenvolvido pelo grupo *Policy Framework* do IETF (*Internet Engineering Task Force*) [Stevens 1999]. Este trabalho teve como principais objectivos, a administração centralizada da rede, suporte a uma definição abstracta das regras e políticas usadas, utilização das mesmas regras por vários equipamentos e automatização de tarefas de gestão de rede. A concretização destes objectivos permite uma maior consistência entre todos os elementos da rede. Neste conceito, o administrador de um sistema deve descrever o que a rede deve fazer, em lugar de se preocupar com o modo como isso deverá ser feito [Shepard 2000] [Mahon 1999].

2.1. Arquitectura PBN

A arquitectura de gestão baseada em políticas, definida pelo IETF [Stevens 1999], descreve, de um modo geral, as principais entidades existentes (Figura 2.1), sem contudo descrever nenhuma norma para a sua implementação. Esta arquitectura é composta por quatro entidades principais: consola de gestão de políticas, repositório de políticas, *Policy Decision Point* (PDP) e *Policy Enforcement Point* (PEP). A comunicação entre estas entidades é efectuada usando dois protocolos distintos: protocolo para acesso ao repositório e protocolo para difusão de políticas.

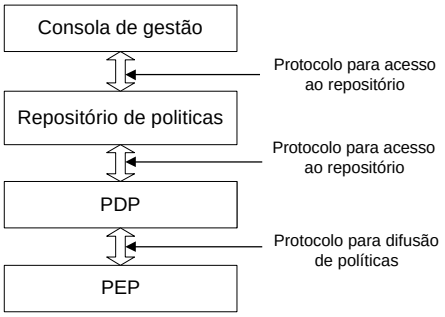

Figura 2.1 – Componentes da arquitectura PBN [INTAP 2001]

O PEP funciona normalmente nos equipamentos activos de uma rede, gerindo-os de acordo com instruções que recebe de um PDP. Um PDP efectua o processamento de políticas definidas para a rede, juntamente com outros dados relevantes para a administração da rede e toma decisões posteriormente transformadas em novas configurações para os PEPs. O repositório de políticas armazena o conjunto de políticas definidas dentro da organização. Nesta arquitectura o PDP acede ao repositório para obter todas as políticas que devem constar da sua configuração. A consola de gestão permite a edição, tradução e validação das políticas definidas de modo a poderem ser armazenadas no repositório de políticas e posteriormente postas em prática.

Usando a arquitectura PBN, o conjunto de políticas definidas pelo administrador é posto em prática pelos dispositivos de rede, após a configuração de cada PEP (Figura 2.2). A arquitectura PBN pode ser vista sobre duas perspectivas: o modelo de três camadas e o modelo de duas camadas [Raju 1999].

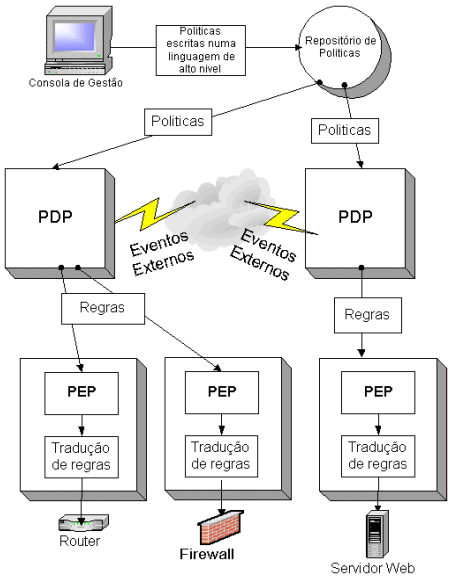

Figura 2.2 – A arquitectura PBN

A Figura 2.3 representa uma visão genérica do modelo de três camadas, sendo constituído por PEPs, PDPs e repositório de políticas. Neste modelo, o PEP é uma entidade que põe em prática as regras que recebe do PDP, não tendo contudo mais nenhuma capacidade de processamento.

O modelo de duas camadas apresentado na Figura 2.4 pode ser visto como uma simplificação do modelo de três camadas. Este modelo existe pelo facto de que alguns componentes da rede podem ser capazes de efectuar algum tipo de processamento, isto é, capazes de guardar regras e efectuar as suas próprias decisões.

Numa rede complexa é possível existir uma combinação destes dois modelos, existindo PDPs para os equipamentos com menos poder de processamento e a funcionalidade de PEP e PDP instalada nos servidores de rede.

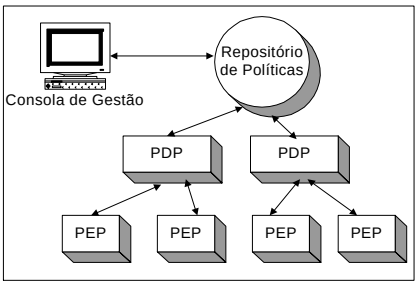

Figura 2.3 – Modelo de três camadas

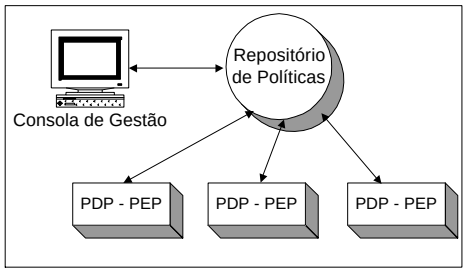

Figura 2.4 – Modelo de duas camadas

2.2. Os modelos Outsourcing e Provisioning

A arquitectura PBN efectua a interacção entre PDPs e PEPs usando o modelo cliente-servidor. Nesta arquitectura podem ser distinguidos dois modelos distintos de operação: *outsourcing* e *provisioning* [IPHighway 2001].

No modelo *outsourcing*, no caso de existir um evento que o PEP não saiba tratar de acordo com os critérios que tem instalados, é enviado um pedido ao PDP correspondente, notificando-o da ocorrência desse mesmo evento. O PDP responde ao PEP enviando informação que necessita de ser instalada de acordo com o evento. Este modelo também é conhecido por *pull* ou *reactive* [IPHighway 2001], visto que o PDP reage a eventos originados nos PEPs por ele controlados.

No modelo *provisioning*, quando o PEP efectua uma ligação inicial ao PDP este envia toda a informação existente, aplicável a esse mesmo PEP. Estas políticas são guardadas no PEP e todos os eventos que venham a ocorrer serão tratados usando esta informação. Podemos também chamar a

este modelo *push* ou *proactive* [IPHighway 2001] pelo facto de o PDP enviar antecipadamente todas as políticas para os PEPs que controla.

Em ambos os casos os PDPs têm conhecimento das políticas postas em acção pelos PEPs pelo que pode decidir em qualquer altura efectuar uma actualização, instalando, apagando ou alterando a informação contida nos PEPs.

3. Repositório de políticas

O repositório de políticas pode ser visto como sendo o local onde as políticas associadas a um determinado domínio estão armazenadas, ou, de uma forma geral, como uma base de dados contendo essa mesma informação.

Neste contexto, existem várias possibilidades para efectuar o armazenamento físico dos dados (ficheiros de texto, SGBD, etc.), contudo este armazenamento deve, necessariamente, obedecer a modelos de dados utilizados para modelar a informação. Nesta secção são apresentados o modelo CIM (*Common Information Model*) e o modelo baseado na estrutura de dados PIB (*Policy Information Base*).

3.1. Common Information Model

O IETF e o grupo *Directory Enabled Networking* (DEN) da organização DMTF (*Distributed Management Task Force*) estão a concentrar esforços na criação de um modelo de dados orientado a objectos, o *Common Information Model* (CIM) [Moore 2000]. Este modelo de dados pretende vir a ser a base para a representação de políticas referentes a diferentes áreas.

O principal objectivo do modelo CIM é a descrição dos dados necessários para efectuar a gestão de sistemas de informação assim como os relacionamentos existentes entre estes dados, estando definido usando a linguagem UML (*Universal Modeling Language*) [Booch 1996]. Esta abordagem define um modelo de dados e não uma linguagem, ou implementação, para a definição desses mesmos dados.

O modelo CIM utiliza os conceitos do paradigma orientado a objectos para a descrição das entidades existentes no sistema, como por exemplo os computadores, *software*, utilizadores e redes [CIM 1999].

Sendo baseado no paradigma orientado a objectos, existem no modelo CIM noções de classes, instâncias dessas classes, tipos de dados, herança, regras de associação entre objectos e métodos.

O modelo CIM baseia-se numa arquitectura conceptual de três camadas ou esquemas de dados, sendo constituída por *core model*, *common model* e *extension model* (Figura 3.1).

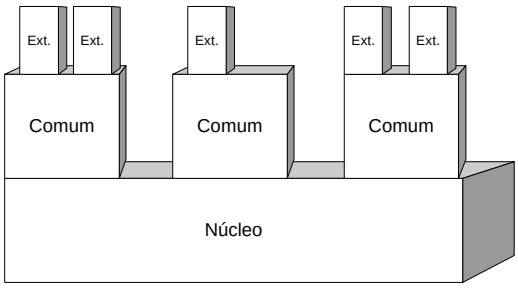

Figura 3.1 – Arquitectura conceptual do modelo CIM [Oliveira 2000]

A camada *Core Model* (núcleo), permite armazenar informação geral para todos os domínios de gestão. É constituída por um pequeno conjunto de classes, associações e propriedades que fornecem um vocabulário inicial para descrever os sistemas a gerir.

Os esquemas *Common Models* (esquemas comuns), consistem num conjunto de classes destinadas a definir um modelo de dados para áreas mais específicas, sendo ainda independentes das várias tecnologias ou implementações. As áreas existentes vão desde os equipamentos, aplicações, redes utilizadores, até à gestão do suporte a utilizadores.

Os *Extension Models* (Esquemas extendidos), fornecem extensões aos esquemas *Common* existentes, de forma a poder ser representada informação sobre ambientes específicos como por exemplo os sistemas operativos (*Unix*, *Microsoft Windows*, etc.).

Das diversas definições de esquemas *Common* e *Extension*, pode ser salientado o esquema relacionado com a definição de políticas. Este esquema permite a definição de objectos do tipo *Política*, representando políticas relacionadas com diversas áreas: segurança, QoS, etc.

O CIM é um modelo conceptual permitindo, assim, que a implementação de um modelo baseado neste conceito possa ser efectuada, por exemplo, usando XML (*eXtensible Markup Language*) ou mesmo uma base de dados relacional, podendo assim ser uma opção a considerar para a criação de um repositório de políticas numa arquitectura de gestão baseada em políticas.

3.2. Policy Information Base

O modelo de dados PIB (*Policy Information Base*) é apresentado no âmbito da sua utilização com os protocolos de difusão de políticas COPS (*Common Open Policy Service*) e COPS-PR (*COPS for Policy Provisioning*).

No protocolo COPS-PR, cada cliente tem que conter uma base de dados chamada *Policy Information Base* (PIB) [Fine 2000] onde armazena a informação recebida. Esta base de dados pode ter origem num modelo de dados mais abrangente como o CIM.

A estrutura de uma PIB é semelhante ao de uma MIB (*Management Information Base*) usada no protocolo SNMP (*Simple Network Management Protocol*), existindo inclusive mecanismos que permitem efectuar a conversão de uma PIB para uma MIB [Fine 1999]. A PIB contêm toda a informação estruturada de acordo com o tipo ou classe das políticas definidas. Uma PIB pode ser representada por uma estrutura em árvore (Figura 3.2), onde cada ramo da árvore corresponde a um diferente tipo de políticas ou classe de políticas (PRCs – *Policy Rules* ou *Policy Rule Classes*) e as folhas representam o conteúdo dessa mesma política – instâncias desse tipo de política (PRIs – *Policy Rules* ou *Policy Rule Instances*). Cada PRC pode conter múltiplas PRIs. Cada PRI é identificada por um identificador (PRID – *Provisioning Instance Identifier*), sendo que um PRID pode ser considerado como um nome único nos objectos COPS. Um exemplo de um PRID pode ser o nome "1.2.3.4.5" em que os primeiros quatro números representam a classe PRC ("1.2.3.4") e o ultimo número representa a PRI ("5").

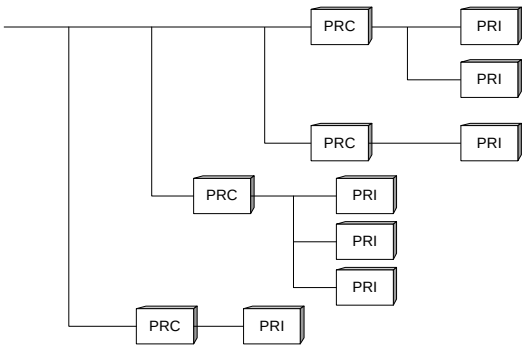

Figura 3.2 – Estrutura da PIB

De modo similar às MIBs usadas com SNMP, as PIBs usam a linguagem de definição de dados ASN.1 (*Abstract Syntax Notation One*) [MS 2000] e a informação deve respeitar as regras BER (*Basic Encoding Rules*) [MS 2000] de modo a que algum código SNMP possa ser reutilizado [Sanchez 1999].

As PIBs estão definidas no âmbito do protocolo COPS-PR apenas como estruturas abstractas, sendo que os detalhes referentes a cada PIB (PRCs e semântica) estão especificados em documentos separados (ex. *internet drafts*).

A definição de uma PIB é efectuada com um elevado nível de abstracção, permitindo que os detalhes de implementação do *hardware* sejam escondidos. Desta forma, pode-se controlar o

comportamento dos vários equipamentos existentes na rede, usando a mesma estrutura de dados para todos.

O PDP pode instalar novas PRIs ou alterar as PRIs existentes num PEP, enviando as respectivas mensagens COPS. Pode ainda eliminar determinada PRI através de uma decisão que contenha o PRID do PRI que se pretende eliminar. As políticas são construídas através de um conjunto de PRIs existentes na PIB. Deste modo pelo facto de o PDP poder acrescentar, alterar ou remover PRIs de cada PEP ele pode implementar as políticas que pretende em cada equipamento.

As políticas que cada PIB pode implementar estão pré-definidas no documento que define a PIB. De forma ao PDP poder controlar um determinado equipamento, este terá que conseguir mapear as políticas que lhe foram dadas através da consola de gestão, nas políticas que podem ser suportadas pela PIB em determinado PEP. As classes que são comuns a todas as PIBs estão definidas no documento "*Framework Policy Information Base*" [Fine 2000]. Esta PIB deve ser implementada em todos os clientes de COPS-PR.

O uso de PIBs permite uma grande abstracção dos dados, que passam assim a ser reconhecidos por todos os equipamentos existentes no domínio da rede em questão, deixando de existir a necessidade de criar novas políticas exclusivamente para determinado PEP, de um ou outro fabricante especifico.

4. Protocolos de difusão de políticas

Na arquitectura PBN existe a necessidade de utilizar protocolos normalizados para os dispositivos efectuarem a troca de informação entre os vários componentes da arquitectura. Estes protocolos são necessários de modo a permitir uma comunicação sem restrições entre produtos de diversos fabricantes e assegurar que a solução para a gestão por políticas tenha uma âmbito de aplicação bastante alargado.

Neste contexto apresenta-se o protocolo COPS (*Common Open Policy Service*) e o protocolo COPS-PR (*COPS for Policy Provisioning*), focando o seu modo de funcionamento conforme é apresentado em [Durham 2000] e [Chan 2001].

4.1. Common Open Policy Service

O protocolo COPS [Durham 2000] teve origem no trabalho realizado pelo IETF com o objectivo de criar uma nova norma para efectuar a comunicação entre os PDPs e os PEPs. Este protocolo e as suas extensões está a ser desenvolvido pelo grupo de trabalho do RAP (*Resource Allocation Protocol*) [RAP 2001] com especial incidência para a área do RSVP (*Resource Reservation Protocol*) [Braden 1997], contudo, devido à sua arquitectura genérica, este protocolo está a captar o interesse de outros grupos a trabalhar nas mais diversas áreas.

O protocolo COPS pode ser dividido em três camadas distintas: o protocolo base, os comandos específicos do tipo de cliente e a representação dos dados.

O protocolo base define os mecanismos de comunicação que permitem a troca de informação entre um PDP e os PEPs que lhe estão associados. O PEP fica com o papel de cliente e o PDP é o servidor. Diferenciando-se do protocolo SNMP, o protocolo COPS está baseado em ligações TCP e é um protocolo baseado em estados, significando isto que o servidor guarda o estado dos clientes, reagindo sempre que necessário de modo apropriado, mesmo que não exista uma solicitação para o efeito.

O conceito de tipo de cliente existente no protocolo COPS, permite a adição de um segundo nível constituído por comandos específicos de cada cliente, permitindo assim a sua utilização em diversas áreas com a criação de novas camadas deste tipo.

O protocolo COPS é bastante flexível ao suportar objectos definidos para vários contextos. Neste protocolo cada cliente suporta uma estrutura de dados própria (PIB) contendo também esta estrutura, objectos comuns a todos os clientes e contextos.

4.1.1. Funcionamento

O protocolo COPS é usado para difundir as políticas a implementar na rede. No COPS, cada PDP pode ter um ou mais clientes de tipos diferentes (diferentes áreas de aplicação); e cada tipo de cliente pode representar uma área diferente de especificação de políticas (segurança, QoS, controlo de admissão, entre outras.). Ao suportar o tipo de cliente apropriado, o PDP fornece um modo de controlar os vários aspectos de configuração de um determinado equipamento.

O protocolo COPS dispõe de procedimentos de sincronização entre os PDPs e os PEPs, utilizando para tal troca de mensagens definidas para o efeito, assim como tem instruções de como reagir se a ligação se perder. Para além destes aspectos, este protocolo define mecanismos que asseguram a segurança e integridade das mensagens que são trocadas.

A semântica ou o formato dos dados transportados pelo protocolo COPS não estão definidos no âmbito do protocolo. O COPS fornece apenas um meio para trocar informação sendo que a definição do formato dos dados a serem enviados e recebidos é definida individualmente para cada tipo de cliente existente.

Na Figura 4.1 encontra-se representado um modelo COPS genérico. Neste exemplo é usado o protocolo COPS para efectuar a comunicação de políticas entre um PEP e um PDP remoto no âmbito do contexto de um determinado tipo de cliente. O PDP Local (LPDP) é um componente opcional usado com o objectivo de manter um conjunto de regras activas no PEP, funcionando mesmo na ausência do PDP. O PEP pode comunicar com um servidor de políticas de forma a obter decisões ou directivas, sendo responsável por iniciar uma ligação TCP persistente para o PDP. O PEP usa então essa ligação TCP para enviar pedidos e receber decisões provenientes do PDP.

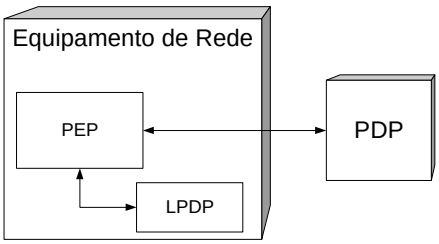

Figura 4.1 – COPS - Modelo genérico

4.2. COPS for Policy Provisioning

O protocolo *COPS for Policy Provisioning* (COPS-PR) [Chan 2001] é uma extensão do protocolo COPS que funciona apenas no modelo *provisioning*, no qual o PDP transfere todas as políticas relevantes para o PEP. Com este protocolo, os clientes ligam-se a um PDP informando-o das suas capacidades e limitações, requerendo que seja enviado um conjunto inicial de políticas que estes irão armazenar localmente.

No modelo *outsourcing*, os pedidos efectuados por um PEP devem ser respondidos por uma única decisão, existindo assim uma relação 1:1 entre pedidos e decisões. No modelo *provisioning* a relação não é sempre 1:1 pois o PDP pode enviar uma decisão baseada num evento externo, por exemplo uma nova introdução de uma política na consola de gestão de rede pode desencadear uma alteração numa regra do PEP ou mesmo que o PDP envie toda uma nova informação de configuração para o PEP.

Funcionamento

O funcionamento do protocolo COPS-PR inicia-se com a abertura de uma ligação COPS, do PEP para o PDP primário. Após a ligação ter sido efectuada com sucesso, o PEP envia uma mensagem do tipo REQ contendo informação específica desse cliente (ex. tipo de *hardware*, versão de *software*, informação de configuração) para o PDP. Nesta fase, o PEP pode também especificar o valor máximo do tamanho de cada mensagem COPS-PR. Após ter recebido esta informação, o PDP guarda esta informação e caso contenha políticas para serem aplicadas por esse PEP estas serão enviadas. Caso o PDP não suporte o tipo de cliente que está a tentar ligar, pode transmitir uma

mensagem de erro onde pode estar contido o endereço de um PDP adicional que contenha suporte para esse mesmo cliente [Chan 2001].

O protocolo COPS-PR utiliza, para o seu funcionamento, a estrutura de dados PIB.

Na Figura 4.2 é ilustrado o funcionamento genérico do protocolo COPS-PR.

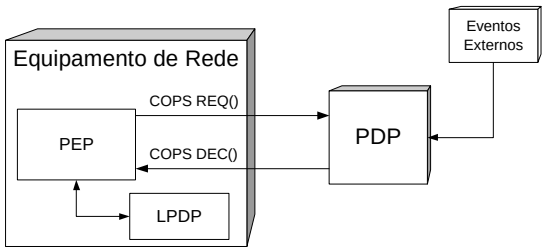

Figura 4.2 – Funcionamento COPS-PR

O funcionamento do protocolo COPS-PR introduz vantagens nas situações em que se pretenda usar gestão por políticas para efectuar a configuração de equipamentos e não apenas controlar o seu funcionamento.

5. Linguagens de especificação de políticas

De forma a representar as políticas usadas na arquitectura de gestão baseada em políticas, existe a necessidade da utilização de algum modelo de dados. Este modelo, pode, neste ponto, ser considerada como uma linguagem através da qual o gestor de rede descreve o comportamento que pretende que a sua rede tenha. Actualmente ainda não existe um norma para uma linguagem deste tipo, existindo sim, vários documentos orientadores, cada um vocacionado para a área de gestão que se pretende efectuar.

A linguagem a criar, como norma, deve fornecer uma plataforma única que suporte os novos conceitos das arquitecturas baseadas em políticas que estão a ser desenvolvidos actualmente. Neste cenário, devem-se identificar os requisitos que uma linguagem para especificação de políticas deve suportar.

Uma linguagem de especificação de políticas deve ser simples e facilmente compreensível pelos utilizadores. Deve permitir suporte para múltiplas actividades de gestão, nomeadamente políticas de segurança e controlo de acessos. As políticas devem ser agrupadas e não serem apenas tratadas de forma individual de modo a facilitar a especificação de políticas relacionadas com grandes redes de dados. Para que as acções referentes a segurança e gestão da rede possam estar relacionadas entre si, sempre que necessário, a linguagem deve permitir efectuar algum tipo de composição de políticas, com a possibilidade de as analisar em termos de conflitos com outras políticas, bem como verificar a sua consistência dentro da especificação global. Por ultimo, a linguagem deve ser expansível, de modo a permitir novos tipos de políticas que previsivelmente irão surgir no futuro. Este objectivo pode ser atingido, utilizando algo semelhante à herança das linguagens orientadas a objectos [Stone 2001].

A especificação de políticas pode ser efectuada através do uso de uma linguagem e um conjunto de acessórios que permitam manipular essa mesma linguagem. Um acessório importante para a especificação de políticas será a criação de um interface gráfico que permita ao gestor uma maior abstracção da linguagem.

Existindo várias especificações, cada uma com a sua própria sintaxe e semântica, deve ser escolhida uma linguagem que seja bastante extensível e com um grande grau de escalabilidade, pois estão constantemente a surgir novas necessidades de gestão o que implica que novas funcionalidades devem ser adicionadas à linguagem sem grande esforço adicional.

Apesar de ainda não existir uma norma sobre qual a linguagem de especificação de políticas que deve ser utilizada pelos fabricantes de equipamentos, existem já algumas propostas como por exemplo, XML [Bray 1998], PFDL [Strassner 1998], PONDER [Damianou 2001], SRL [Brownleee 1999], RPSL [Meyer 1999]e SPSL [Condell 2000].

6. Aplicação à gestão de *firewalls*

Tendo em consideração a arquitectura de gestão por políticas (PBN), assim como o funcionamento do protocolo COPS e COPS-PR, propõe-se a arquitectura representada na Figura 6.1. Esta arquitectura é composta por três componentes principais: consola de gestão, PDP e PEP.

A consola de gestão é uma ferramenta que permite a introdução e o tratamento de políticas escritas na linguagem adoptada. A consola de gestão deve conter um conjunto de módulos de grande relevância para o processamento da linguagem de descrição de políticas, nomeadamente, integrar um *parser* e mecanismos de verificação e normalização de regras. Deste modo, um ficheiro contendo uma descrição de políticas numa determinada linguagem, é tratado na consola de gestão, gerando informação passível de ser armazenada no repositório de políticas ou, como na arquitectura actual, passível de ser integrada na estrutura de dados existente no PDP.

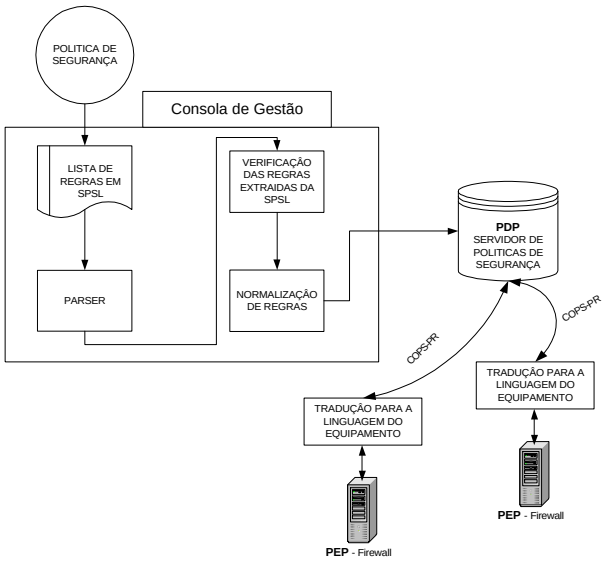

Figura 6.1 – Arquitectura do sistema proposto

O servidor de políticas (PDP) está pensado de modo a ser o módulo responsável pela distribuição das políticas pelos elementos da rede. Na arquitectura proposta, o PDP integra também o repositório de políticas proposto na arquitectura PBN.

O destinatário das políticas enviadas pelo PDP, o PEP, é responsável pela tradução e instalação dessas mesmas políticas nos equipamentos que as devem implementar. No sistema proposto o PEP está em funcionamento no próprio equipamento.

Os protocolos COPS e COPS-PR estão implementados de forma independente da arquitectura, existindo neste âmbito a necessidade de desenvolver uma PIB (*Policy Information Base*), utilizada pelo protocolo COPS-PR para o transporte de políticas referentes às diversas áreas de gestão.

6.1. Implementação

O sistema implementado é um protótipo que permite efectuar a aplicação da arquitectura PBN à gestão de *firewalls,* utilizando como protocolo de difusão de políticas e linguagem de descrição, respectivamente, o protocolo COPS-PR e a linguagem SPSL (*Security Policy Specification Language*). É utilizada a linguagem SPSL, devido ao facto de ser uma linguagem vocacionada para a especificação de políticas relacionadas com aspectos de segurança, principalmente no que concerne a especificação de políticas para filtragem de pacotes. Para a implementação do protocolo COPS-PR foi usada e melhorada uma API desenvolvida na *Luleå University of Technology* [Bergsten 2000].

Pelo facto de cada tipo de *firewall* ter um conjunto de instruções próprias para efectuar a sua configuração, pretende-se com a aplicação desenvolvida, partir da política de segurança global da organização e gerar um conjunto de regras que serão entendidas por cada um dos tipos de *firewall* que se pretenda gerir.

A implementação dos módulos apresentados na Figura 6.1 foi efectuada no sistema operativo *Linux RedHat* e pode ser utilizada para a configuração de sistemas de *firewall* que utilizem o *software IPChains* [Russel 2000] (*IPTables* nas versões mais recentes do *kernel*)e/ou listas de acesso da *Cisco* (ACL) [Cisco 2001].

Na Figura 6.2 apresenta-se um cenário de utilização do protótipo desenvolvido. Neste cenário, o servidor de políticas de segurança (PDP) é usado para efectuar a configuração de duas *firewalls* (PEP). No cenário apresentado, podemos verificar a existência de dois domínios diferentes para a aplicação de políticas de segurança: a ligação à Internet e a ligação a uma *extranet*. Nesta situação, as políticas a por em prática em cada um dos domínios serão necessariamente diferentes. A aplicação desenvolvida pode ser facilmente integrada com outras que operem em áreas distintas, por exemplo, no caso apresentado, pode também ser usado o mesmo servidor de políticas para efectuar alguma configuração de qualidade de serviço nos *routers*, desde que o PDP e os PEPs suportem esse tipo de cliente/serviço.

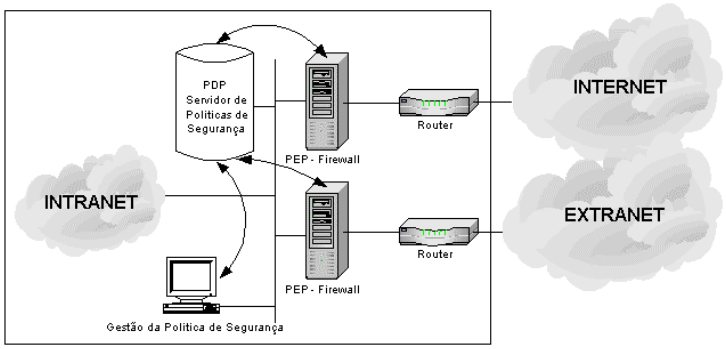

Figura 6.2 – Cenário de utilização da aplicação desenvolvida

Após a definição da política de segurança global criada para a organização, esta deve ser escrita num formato bastante simples e com um elevado grau de abstracção – a linguagem SPSL. Esta linguagem é processada ao nível da consola de gestão onde são verificadas regras como a sintaxe da linguagem ou num nível superior a verificação de sobreposição de objectivos de segurança [Caldeira 2000].

Depois da colocação da política na consola de gestão, esta informa o PDP de alterações efectuadas à política de segurança que deve ser posta em prática no seu campo de acção. O PDP inicia assim a sua tarefa de informar todos os PEPs em funcionamento, das regras que estes devem instalar. Cada PEP ao obter informação sobre as políticas que deve utilizar, é responsável pela sua tradução para o equipamento que lhe está subjacente assim como pela sua instalação do equipamento.

A informação é armazenada numa PIB definida para o efeito, sendo que todos os intervenientes no processo devem ser capazes de interpretar essa mesma PIB.

6.2. Avaliação da proposta

Existindo a definição de uma política de segurança global para a organização, o uso da aplicação apresentada pode melhorar a forma de implementar essa mesma política nos vários equipamentos existentes na rede, principalmente pelo facto de automatizar os procedimentos de configuração de um conjunto de sistemas independentes. Paralelamente, permite ao administrador da rede não necessitar de ter um conhecimento aprofundado das linguagens ou técnicas usadas para configurar cada um dos dois tipos de equipamentos suportados pela aplicação.

O facto de a aplicação proposta estar, nesta fase, vocacionada para lidar apenas com políticas referentes à filtragem de pacotes, introduz limitações relacionadas com a falta de mecanismos para configurar outros aspectos dos equipamentos.

A linguagem utilizada para especificação de políticas (SPSL) mostrou-se adequada para o cenário de aplicação previsto, permitindo com facilidade exprimir as políticas a aplicar na rede. Contudo, mesmo sendo expansível, verifica-se que esta linguagem não é suficientemente abrangente, no que

concerne à especificação de políticas em várias áreas da gestão de redes, para ser usada num cenário mais alargado no âmbito de gestão por políticas.

O módulo de tradução de regras para comandos *IPChains* e ACL da cisco introduz a possibilidade de a configuração gerada para os equipamentos não ser a mais indicada, pois por vezes não se trata apenas uma questão de traduzir a sintaxe mas de manter a semântica pretendida.

No que concerne ao protocolo de difusão de políticas usado (COPS-PR), verifica-se que este protocolo permite que a comunicação entre os PDPs e os PEPs se processe de uma forma bastante simples e eficaz.

7. Conclusão e trabalho futuro

A gestão por políticas em áreas específicas da gestão de redes de computadores representa uma visão do futuro a curto ou médio prazo, pois a expansão e o ritmo da evolução desta arquitectura leva-nos a ser optimistas. No entanto, do presente estudo, pode-se verificar que, no que concerne à gestão de todos os equipamentos da rede, a gestão por políticas ainda é, actualmente, uma arquitectura cuja implementação generalizada está bastante distante. De um modo geral, é possível dizer que estamos perante uma arquitectura com elevado potencial no sentido de possibilitar a redução de custos e melhorar a qualidade do serviço prestado em redes de computadores.

A construção do protótipo permite concluir que a aplicação desta metodologia, de uma forma generalizada, à configuração de um grande numero de *firewalls* de diferentes fabricantes é uma tarefa árdua se não existir o apoio desses mesmos fabricantes.

Conclui-se também, através deste estudo, que os protocolos COPS e COPS-PR apresentam potencialidades interessantes para serem escolhidos em soluções de gestão por políticas.

No que concerne à linguagem de especificação utilizada, esta, sendo indicada para o trabalho desenvolvido, não é suficientemente abrangente para ser uma solução adoptada de uma forma generalizada para a gestão por políticas.

Como trabalho futuro deve ser prevista a extensão da linguagem proposta, ou mesmo a adopção de uma outra linguagem. Deve também ser analisada a possibilidade de usar uma nova metodologia para representação de políticas.

8. Referências

[Bergsten 2000] Bergsten Anders, Borg Niklas, Implementation and Evaluation of the Common Open Policy Service (COPS) Protocol and its use for Policy Provisioning, (extwww.lulea.trab.se/cops), 2000.

[Booch 1996] Booch Grady, Rumbaugh James, *Unified Method for Object-Oriented Development Document Set*, Rational Software Corporation, 1996, (http://www.rational.com/uml).

[Braden 1997] Braden R., Zhang L., Berson S., Herzog S., Jamin S., *Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification*, RFC 2205, Network Working Group, IETF, Setembro 1997.

[Bray 1998] Bray, T. et al., *eXtensible Markup Language (XML) 1.0*, W3C, Fevereiro 1998, (http://www.w3c.org/TR/REC-xml).

[Brownleee 1999] Brownleee N., *SRL: A Language for Describing Traffic Flows and Specifying Actions for Flow Groups*, Internet draft, draft-ietf-rtfm-ruleset-language-07.txt, IETF, Agosto 1999.

[Caldeira 2000] Caldeira Filipe, Monteiro Edmundo, Descrição, Geração e Difusão de Políticas de Segurança, *in Actas da 3ª Conferência sobre Redes de Computadores, Tecnologias e Aplicações (CRC'2000)*, Novembro 2000.

[Chan 2001] Chan, K., Seligson, J., Durham, D., Gai, S., McCloghrie, K., Herzog, S., Reichmeyer, F., Yavatkar, R. and A.Smith, *COPS Usage for Policy Provisioning (COPS-PR)*, RFC 3084, Network Working Group, IETF, Março 2001.

[CIM 1999] *Common Information Model (CIM) Specification – Version 2.2*, DMTF, Junho 1999 (http://www.dmtf.org/spec/cim_spec_v22/).

[Cisco 2001] Manuais Online: (http://www.cisco.com)

[Condell 2000] Condell M., Lynn C., Zao J., *Security Policy Specification Language*, Internet draft, draft-ietf-ipsp-spsl-00.txt, IETF , Março 2000.

[Damianou 2000] Damianou Nicodemos, Policy Specification and Implementation for Distributed Systems Management, *Imperial College of Science, Technology and Medicine*, Janeiro 2000.

[Durham 2000] Durham D., Boyle J., Cohen R., Herzog S., Rajan R., Sastry A., *The COPS (Common Open Policy Service) Protocol*, RFC 2748, Network Working Group, IETF, Janeiro 2000.

[Fine 1999] Fine, M., McCloghrie, K., Seligson, J., Chan, K., Hahn, S., A. Smith, *Quality of Service Policy Information Base*, Internet draft, draft-mfine-cops-pib-01.txt, IETF, Junho 1999.

[Fine 2000] Fine M., McCloghrie K., Seligson J., Chan K.; Hahn S., Sahita R., Smith A., Reichmeyer F.; *Framework Policy Information Base*, Internet draft, draft-ietf-rap-frameworkpib-04.txt, IETF, Novembro 2000.

[INTAP 2001] *Survey on Policy-Based Networking - Addressing Issues, Technological Trends, Future Prospects of Policy Exchange Methods in Multi-Domain Scenarios*, INTAP, 2001, (http://www.net.intap.or.jp/INTAP/).

[IPHighway 2001] *Policy Standards and IETF Terminology*, White paper, Volume #2, IPHighway, Janeiro 2001.

[Mahon 1999] Mahon H., Bernet Y., Herzog S., *Requirements for a Policy Management System*, Internet draft, draft-ietf-policy-req-02.txt, IETF, Novembro, 1999.

[Meyer 1999] Meyer D., Schmitz J., Orange C., Prior M., and Alaettinoglu C., *Using RPSL in Practice*, RFC 2650, Network Working Group, IETF, Agosto 1999.

[Moore 2000] Moore B., Ellesson E., Strassner J., *Policy Core Information Model – Version 1 Specification*, Internet draft, draft-ietf-policy-core-info-model-04.txt, IETF Março 2000.

[MS 2000] Microsoft Support Online, A Brief Introduction to ASN.1 and BER, *Doc. n.º Q252648*, Outubro 2000.

[Oliveira 2000] Oliveira, J., Aguiar R., Network and Desktop Management Convergence, *in Proceedings of the 33rd Hawaii International Conference on System Sciences*, Hawaii, Janeiro 2000.

[Raju 1999] Raju Rajan, Dinesh Verma, Sanjay Kamat, Eyal Felstaine, Shai Herzog, A policy framework for integrated and differentiated services in the internet, *in IEEE Network*, Setembro/Outubro 1999.

[RAP 2001] *Resource Allocation Protocol (rap)*; (http://www.ietf.org/html.charters/rap-charter.html), 2001.

[Russel 2000] Russell Rusty, *Linux IPChains HowTo*, Online, Julho 2000.

[Sanchez 1999] Sanchez Luis, McCloghrie Keith, Jon Saperia, *Evaluation of COPS/PIB and SNMP/MIB approaches for configuration management of IP-based networks*, Internet draft, draft-ops-mumble-conf-management-00.txt, IETF, Outubro 1999.

[Shepard 2000] Shepard, Susan; Policy-based networks: hype and hope; *in IT Professional, Vol. 2, No. 1*, Janeiro-Fevereiro 2000.

[Stevens 1999] Stevens M., Weiss W., Mahon H., Moore B., Strassner J., Waters G., Westerinen A., Wheeler J., Policy Framework, Internet draft, draft-ietf-policy-framework-00.txt, IETF, Setembro 1999.

[Stone 2001] Stone G., Lundy B., Xie G., Network Policy Languages: A Survey and a New Approach, in IEEE Network, pag. 10-21, Janeiro/Fevereiro 2001.

[Strassner 1998] Strassner J. and Schleimer S., *Policy Framework Definition Language*, Internet draft, draft-ietf-policy-framework-pfdl-00.txt, IETF, Novembro 1998.