# LARCES_Seg - Uma Arquitetura para Gerenciamento de VPNs Baseada em Políticas utilizando XACML

**Silvia Helena Jucá Fontenelle Ferreira, Rodrigo Almeida dos Santos, Joaquim Celestino Junior**

Laboratório de Redes de Comunicação e Segurança da Informação – LARCES
Universidade Estadual do Ceará (UECE) ,
Av. Paranjana, 1700 – Fortaleza – CE - CEP: 60.740-020
{silvia, rodrigo, celestino}@larces.uece.br

***Abstract.*** *This paper presents an architecture for management of VPNs where will be analyzed the coexistence between the policies based on IPSec parameters, used to configure VPN and others policies based on an application parameters. This architecture is based on policy based management model, defined by IETF, where will be focus principally on security access, with policies defined in XACML. A case study will be analyzed for VPN intradomain configuration to sample this architecture, using policies defined in XACML. Previous papers presents XML policies however without aggregate the restrictions of an application.*

***Resumo*** *Neste artigo apresentaremos uma arquitetura para o gerenciamento de VPNs onde serão analisadas as coexistências entre as políticas baseadas em parâmetros do IPSec, pertinentes à configuração da VPN e outras políticas baseadas em parâmetros da aplicação. Esta arquitetura é baseada no modelo de gerenciamento baseado por políticas, definido pelo IETF, com ênfase à segurança de acesso, com políticas definidas em XACML. Analisaremos um estudo de caso para a configuração de uma VPN intradomínio, para exemplificar esta arquitetura. Estudos anteriores mostram a utilização de políticas em XML, todavia sem agregar as restrições da aplicação.*

## 1. Introdução

A necessidade de comunicação segura tem se tornado um requisito indispensável para os usuários de redes de computadores que precisam ter seus dados protegidos. A alternativa que combina custo baixo e nível de segurança alto, consiste em prover uma rede virtual privada (VPN), que permite a comunicação segura, mesmo quando as informações trafegam através de uma rede pública.

O aumento na utilização de VPNs obrigou os gerentes de redes a fazerem configurações de restrições de acessos em diversos equipamentos de diferentes fabricantes, a fim de adequá-los às restrições impostas pelos Acordos de Nível de Serviços (SLAs) das empresas, em relação à QoS e segurança. A configuração manual é difícil e passível de erros. A utilização de políticas permite facilitar estas configurações, melhor gerenciá-las e diminuir os erros.

O objeto do trabalho é propor uma arquitetura para gerenciamento de VPNs utilizando XACML, permitindo mostrar que é possível a coexistência entre as políticas de configuração de uma VPN e as políticas particulares de uma aplicação.

Este trabalho está dividido em 8 seções. Na seção 2 serão relacionados os trabalhos nos quais baseamos nossa pesquisa. Na seção 3 serão abordados alguns conceitos de Redes Privadas Virtuais, Ipsec e Freeswan, na seção 4 serão abordados os conceitos da Arquitetura de Gerência de Políticas, PBNM, e o framework LARCES PBM. Na seção 5 será abordado o XACML, na seção 6, a Arquitetura LARCES-Seg. Na seção 7 abordaremos o cenário do estudo de caso, os testes e resultados obtidos. As conclusões e perspectivas estão na seção 8 e as referências podem ser encontradas ao final do artigo.

## 2. Trabalhos Relacionados

Existem vários artigos recentes onde são tratadas as soluções de gerência utilizando políticas, bem como soluções relativas à segurança e interoperabilidade entre redes.

Um sistema para gerenciar redes IP-VPN baseado em políticas, visando atender os requisitos de crescentes redes VPNs foi proposto por Xin Guo et al [23], e apresentado no congresso Policy 2003, onde fora proposto um framework que validasse somente os requisitos de segurança e, baseados neste trabalho definimos o nosso framework de forma a validar através de políticas as restrições de uma aplicação comercial e obtivemos resultados satisfatórios.

Em OASIS [16], vemos que a utilização de gerência utilizando políticas envolve a linguagem XACML *(eXtensible Acess Control Markup Language)*, que é uma linguagem baseada em XML, proposta por OASIS consortium [16], e é utilizada para expressar as políticas de controle de acesso definidas pelo administrador, sendo utilizada também para realizar a comunicação entre o *Policy Enforcement Point* (PEP) e o *Policy Decision Point* (PDP). Utilizamos estas definições para o nosso trabalho, pois a linguagem XACML define as requisições de políticas efetuadas pelo PEP e consulta o PDP para enviar a resposta.

Madeline Baltatu [1] propõe um *framework* experimental para políticas IPSec e discorre sobre várias delas. Zhi Fu e outros autores [7] enfocam o problema de configuração quando houver erros nas definições de políticas. No trabalho a geração automática de políticas IPSec. Utilizamos estas referências, pois para validação do nosso *framework*, utilizamos também VPN/IPSec.

Como referencias de trabalhos envolvendo os conceitos de PBNM, temos: Dinesh Verma [22] que apresenta as tecnologias de gerenciamento baseado em políticas; Pedatella [18] que propõe um *framework* que visa garantir Qos fim-a-fim para a Internet através de um software gerencial baseado em políticas de configuração e do

uso conjunto do modelo MPLS e DiffServ e outro trabalho relacionando políticas para qualidade de serviços é citado por Lymberopoulos [12].

Além destes trabalhos citamos as RFCs 3060 – PCIM [14] e RFC 3460 – PCIM Extensions [15] como referências para as classes a serem verificadas no monitoramento das VPNs.

## 3. Redes Privadas Virtuais (VPN)

Uma VPN é uma rede de comunicações, construída para uso privado da empresa, sobre a infraestrutura pública compartilhada[19]. A utilização de VPNs simula uma rede privada a um menor custo, pois utiliza a rede de comunicação já existente.

Uma das maneiras de prover segurança em uma VPN pode ser obtida utilizando o protocolo IPSec, que será um dos elementos utilizado na arquitetura e melhor descrito na seção seguinte.

### 3.1. IP Security (IPSec)

O IP Security (IPSec ou IPSEC) é o protocolo (conjunto de protocolos) que utilizaremos na VPN para torná-la segura. Pode ser dividido em:

- Protocolos de segurança: autenticação - AH (*Autentication header)* definido pela RFC 2402 [10] e cifragem – ESP (*Encapsulation Security Payload),* definido pela RFC 2403 [13];
- Algoritmos de segurança: Implementam diversos algoritmos, sendo que atualmente é orientada a utilização de algoritmos mais fortes, como o 3DES, o *Blowfish* e, mais recentemente, o AES (*Advanced Encryption Standard)*, atual padrão adotado pelo NIST*(National Institute of Standards and Tecnology ).*
- Mecanismos de gerência e distribuição de chaves (IKE).
- Associações Seguras – (*Security Association* – SA) são utilizadas para a negociação das chaves e verificação dos protocolos de segurança.

O IPSec é um dos serviços de rede que aceita políticas. Se as definições das políticas forem corretas, o serviço irá realizar suas funções corretamente. Atualmente ainda existe a prática de configuração manual de políticas, o que ocasionalmente gera problemas, mas já existem algumas soluções de forma a permitir uma configuração mais automática [7]. Para a configuração da VPN, utilizaremos o software livre *Freeswan*, uma implementação do Ipsec, melhor descrito a seguir.

### 3.2. FreeSwan

O *FreeSwan* é uma implementação dos protocolos IPSec para LINUX. Serve para a configuração e montagem de VPNs. Utiliza os seguintes protocolos: AH – (*Autentification Header)*, para a autentificação; ESP – (*Encapsulating Security Payload*) para a cifragem; IKE (*Internet Key Exchange*) para a negociação dos parâmetros da conexão, a menos que seja usado somente "*manual keying*", que não é recomendado. O KLIPS (Kernel Ipsec) é utilizado para a implementação de

autenticação e cifragem no *kernel* IPSec [6], [11]. O arquivo ipsec.conf especifica a maioria das informações para controle e configuração da VPN.

## 4. Gerenciamento Baseado em Políticas

O modelo de gestão de redes com a utilização de políticas traduz as diretrizes das empresas (políticas de alto nível) para o mundo dos elementos de rede (políticas de baixo nível), permitindo que estas políticas sejam difundidas mais fáceis e rapidamente, sem a necessidade de gerência direta em cada um dos equipamentos e, possibilitando desta forma, a reutilização de conhecimentos e processos. A utilização de políticas também reduz a incidência de erros e a facilita a detecção e correção de eventuais erros. Após o entendimento da política global, o administrador da rede deverá utilizar a ferramenta de gerência para a definição e validação das políticas, que serão armazenadas em um repositório e aplicadas automaticamente aos equipamentos.

Resumidamente, temos que os objetivos da empresa são traduzidos em regras que são aplicadas sobre os elementos gerenciados da seguinte forma [14], [20]:

**Objetivos** traduzidos em → **Regras** aplicadas sobre → **elementos gerenciados.**

### 4.1. Arquitetura de PBNM ( Policy Based Network Management )

Foi definido pelo IETF *Policy Work Group* [8], que a arquitetura básica de políticas consistiria em quatro elementos básicos: ferramenta para gerenciamento de políticas; repositório de políticas, *Policy Decision Point* (PDP) e o *Policy Enforcement Point* (PEP) , conforme pode ser observado na figura 1:

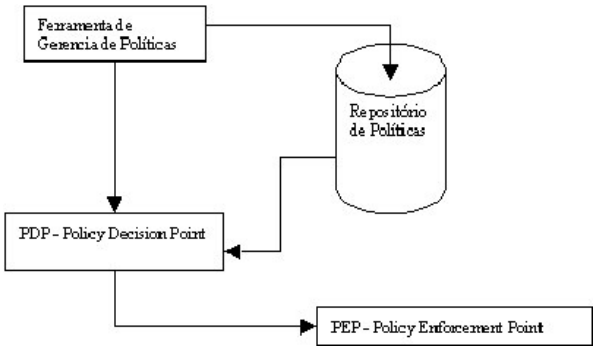


**Fig 1. Exemplo da Arquitetura PBNM - [14],[22]**

#### 4.1.1. PEP – Policy Enforcement Point

O PEP é responsável por executar as políticas como definidas pelo PDP, que está mais bem detalhado no item a seguir. Também é responsável pelo monitoramento de quaisquer estatísticas ou outras informações relevantes para sua operação. Essas informações estatísticas também servem a outras partes interessadas.

O PEP é o componente freqüentemente invocado pelo *path* dos pacotes que chegam através do tráfego da rede. Exemplos comuns de PEPs são os roteadores de rede, *firewalls* e *proxies* [22].

### 4.1.2. PDP – Policy Decision Point

Trata-se de uma entidade que toma decisões de políticas para si mesma ou para outros elementos de rede que requisitam tais decisões. O PDP é responsável por interpretar as políticas armazenadas no repositório de políticas e retorná-las ao PEP. Atua como centro de comandos para políticas de uma rede, localizando e transformando as políticas para um formato compreensível pelo PEP, verificando o estado corrente da rede e que todas as condições requeridas para a aplicação de qualquer política estejam satisfeitas e mantém controle das alterações nas políticas que podem ocorrer, através do monitoramento do repositório [22] .

Quanto ao posicionamento do PDP, ele pode estar tanto no mesmo dispositivo que o PEP, funcionando como um Local PDP (LPDP), como em dispositivos separados. Um PDP pode ser um software em um servidor que trata das políticas vindas do repositório e configura a pilha local de rede para obedecer às políticas especificadas.

### 4.1.3. Repositório de Políticas:

Por repositório de políticas entende-se a entidade que representa o banco de dados de políticas. Um tipo de repositório que pode ser utilizado com o propósito de armazenar políticas é um servidor de diretórios acessado pelo protocolo LDAP (*Lightweight Directory Access Protocol*).

O uso de um diretório LDAP traz como vantagens o suporte para múltiplas plataformas e a possibilidade do administrador de redes facilmente consultar os diretórios e determinar a atual configuração da rede. Como desvantagem, temos o fato de que os diretórios LDAP são implementados para otimizar acessos e consultas e não para realizar atualizações rápidas. Portanto, políticas que podem ser alteradas freqüentemente são inapropriadas a ser armazenadas em uma distribuição LDAP.

## 5. XACML

Existem várias linguagens utilizadas para definição de políticas: XML [2], Ponder [4], SPSL [3], entre outras. Optamos por adotar XACML (*eXtensible Access Control Markup Language*) para controle de acesso. Esta linguagem é baseada em XML e foi padronizada pelo OASIS (*Organization for the Advancement of Structured Information Standards*)[16]. Uma das razões de sua escolha foi sua grande flexibilidade, extensibilidade, que permite a definição de requisitos da aplicação, sintaxe e semânticas simples, além de ser largamente suportada por diversos equipamentos, já que é derivada de uma linguagem já padronizada.

O XACML descreve uma linguagem de controle de políticas e uma linguagem de requisição/resposta. A linguagem de políticas é utilizada para expressar políticas de controle de acesso. A linguagem de requisição/resposta expressa consultas (requisições) sobre onde um acesso particular pode ser permitido, além de descrever respostas para essas consultas.

O XACML foi proposto para ser aplicável a uma grande variedade de ambientes de aplicação. O núcleo da linguagem é retirado do ambiente de aplicação pelo contexto XACML. Esse contexto é definido em um esquema XML, que descreve uma representação canônica para as entradas e saídas do PDP. Os atributos referenciados por uma instância da política XACML podem ser da forma de expressões dentro do contexto, ou através de designadores de atributo que identificam o atributo pelo assunto, ação, recurso ou ambiente e seus identificadores. As implementações devem se preocupar tanto com a representação do atributo no ambiente de aplicação (como J2SE, CORBA, etc.) quanto com a representação do atributo no contexto XACML. Como isso é obtido está fora do escopo da especificação XACML.

**Modelo da linguagem de políticas:**

Os principais componentes do modelo da linguagem de políticas são as regras, as políticas e o conjunto de políticas.

A regra é a porção mais elementar da política. Ela pode existir isoladamente somente como um dos principais atores de um domínio XACML. Entre seus componentes se incluem um alvo, um efeito e uma condição.

- O alvo é definido como um conjunto de recursos, assuntos e ações para o qual a regra será aplicada.
- O efeito de uma regra indica a escrita que será conseqüência de um processamento verdadeiro (*true*) de uma política. Dois valores são permitidos: "*Permit"* e *"Deny"*.
- A condição representa uma expressão booleana que refina a aplicabilidade da regra através de predicados implicados pelo alvo.

Por política entende-se a estrutura que reúne um conjunto de regras. A política engloba os seguintes elementos:

- um alvo;
- um algoritmo identificador de regras combinadas;
- um conjunto de regras e;
- obrigações a cumprir.

Uma política em XACML contém um elemento, chamado de alvo, que especifica um conjunto de assuntos, recursos e ações. O algoritmo identificador especifica o procedimento pelo qual os resultados da análise das regras são combinados com os resultados da análise das políticas, isto é, o valor de decisão retornado ao PDP é o valor da política, como retornado pelo algoritmo.

Caso seja necessário que ocorra em uma política, as **obrigações** podem ser adicionadas ao contexto XACML. Tais obrigações incorporam funcionalidades que devem ocorrer para que o contexto de análise da política retorne um valor de aceitação ao PDP.

## 6. A Arquitetura LARCES_Seg

A arquitetura proposta em nosso trabalho, LARCES_Seg, garante a segurança por meio de restrições de acesso. Foi baseada no *framework* LARCES_PBM [21], que especifica um *framework* para políticas. Neste trabalho enfatizamos a abordagem para segurança, onde os usuários que não preencham os requisitos definidos pelo administrador da rede não terão acesso para o estabelecimento da VPN.

Esta arquitetura é apresentada na figura 2, e é composta de uma Console Gerente onde o administrador da rede irá definir as políticas de restrições de acesso em uma interface gráfica, que serão mapeadas em XACML no PDP. Estas políticas referem-se a políticas de configuração da VPN e da aplicação. Utilizamos como estratégia para a agregação das políticas a definição conjunta [9], em XACML, forçando assim o modelo a validar os dois tipos de políticas de forma composta. As políticas compostas exemplificadas no estudo de caso referem-se às políticas de configuração da VPN e as de restrição de horários impostas pelo administrador da rede. Este exemplo irá mostrar que outras restrições estabelecidas pelo administrador podem ser verificadas através de políticas. A política composta é formada com a combinação de políticas simples. Estas políticas conjuntas serão gravadas em um repositório LDAP. O PDP será um servidor que será acessado pela Console Gerente, pelos PEPs (em XACML) e também irá acessar o repositório de políticas. Os PEPs representam roteadores, servidores ou *firewalls*, onde serão aplicadas as políticas. Estas políticas são baseadas nas classes *IPSecDiscardedAction*, *IPSecPreconfigurateAction* [9], com requisição e resposta em XACML, restringindo desta forma o acesso e garantindo a segurança.

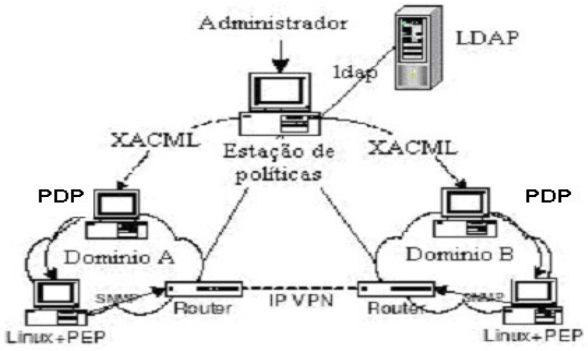


**Fig 2. Arquitetura LARCES_Seg**

Em nosso estudo de caso, serão cadastradas as seguintes informações pelo administrador: servidor de origem e destino, utilização ou não de criptografia, horário permitido para acesso, se o usuário é do tipo "cliente" ou do tipo "funcionário".

Nos PDPs de cada domínio, serão validadas estas informações ao ser solicitada a VPN. Caso o acesso seja negado, será gerado um relatório de ocorrências que será disponibilizado para eventuais consultas do administrador, possibilitando assim a detecção da configuração errônea de políticas e/ou detecção de intrusão, ou tentativas de usuários burlarem as permissões.

As definições mais freqüentemente propostas para segurança de computadores identificam três objetivos primários: *confidencialidade*, *integridade*, *disponibilidade*.

Para atingir esses objetivos, três técnicas são utilizadas: *autenticação*, *auditoria e controle de acesso*. Existem três componentes básicos para sistemas de controle de acesso: Os *sujeitos*, os *alvos* e as *regras*, as quais especificam as maneiras que os sujeitos podem acessar os alvos [5].

A seguir, na figura 3, vemos um exemplo de código referente à implementação em XACML, onde é definida uma política onde somente será permitido o acesso a um determinado servidor. Caso o servidor para acesso seja diferente de VPNServer não será permitido ao usuário efetuar o "*logon*".

```
...
       <ResourceMatch    MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">VPNServer</AttributeValue>
        <ResourceAttributeDesignator
DataType="http://www.w3.org/2001/XMLSchema#string"

AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
...
```

**Fig 3. Exemplo de Implementação em XACML**

O código acima trata do aspecto de reconhecimento de *host* comunicante na comunicação VPN. No caso o *host* foi denominado VPNServer. Qualquer requisição enviada pelo PEP para montagem de uma VPN terá que ser para o *host* VPNServer. Torna-se importante para efeito de controle de acesso.

O trecho de código a seguir, apresentado na figura 4, mostra que se as condições forem atendidas, teremos a aplicação da regra: somente será permitido o *login* se o resultado for "*permit*"

```
....

<Rule RuleId="LoginRule" Effect="Permit">
....
```

**Fig 4 – Aplicação da regra de política**

O trecho de código abaixo, apresentado na figura 5, mostra o caso da condição não ser atendida, então o resultado será "deny" e não será permitido o acesso.

```
....
     <Rule RuleId="FinalRule" Effect="Deny"/>
....
```

**Fig 5 – Resultado da aplicação da regra de política**

## 7. Estudo de Caso – Cenário e Testes

Para a definição do cenário proposto no estudo de caso imaginamos uma empresa com várias filiais geograficamente distribuídas e que tem relacionamentos com clientes e empregados através de VPNs. A configuração e o acompanhamento das restrições de acessos serão feitos com a utilização das políticas em XACML. Para tanto, é necessário a definição de quais políticas serão adotadas; da parametrização dos valores iniciais de referencia; e entre quais máquinas será feita a conexão.

Adotaremos a comunicação entre os domínios A e B para o estabelecimento da VPN (figura 2). Após a validação das políticas, caso haja a combinação de critérios, a VPN será estabelecida e o roteador será configurado via SNMP. Caso contrário, haverá a negação do acesso e a geração do relatório de ocorrências.

Algumas definições adotadas para o estudo de caso foram citadas anteriormente na seção 6, quando abordamos o aspecto da arquitetura.

As políticas definidas pelo administrador da rede são compostas por políticas de configuração do IPSec e da aplicação. Na conexão, o acesso será validado de acordo com o modelo definido em XACML, no seguinte formato simplificado:

**requisição de acesso → verificação de políticas → resposta (*Negada-IPSec Discard, ou Permissão - IPSecPreconfigure* ).**

Para a base de políticas foi gerado o arquivo *policyVPN.xml*. Este arquivo tem por objetivo armazenar todas as regras de comunicação e estabelecimento de uma VPN. Ele estará armazenado em um repositório e servirá como base na tomada de decisões por parte do PDP. Durante a construção da base de políticas, foi decidido qual tipo de informações serão tratadas para o estabelecimento da VPN IPSec. Os pontos relacionados a seguir serão abordados na implementação:

1. Verificação de acesso;
2. Quantidade de VPN's estabelecidas por determinado usuário;
3. Horário de estabelecimento das VPNs. (Aqui se analisa o caso de uma empresa com funcionamento em horário comercial. É interessante que a política analise o caso da tentativa de montagem de uma VPN no horário não autorizado)

As requisições de políticas ficam no arquivo *requestVPN.xml* e as respostas das políticas no arquivo *responseVPN.xml* . A partir do resultado gerado é que o acesso será permitido ou negado para o estabelecimento da VPN.

Neste cenário, identificamos como tentativas de ataques ou quebra de acordo, a tentativa de acesso fora do horário pré-estabelecido, a tentativa de acesso a um servidor não autorizado ou não utilização de criptografia, se estiver sido recomendada e o estabelecimento de mais do que um valor determinado de conexões. Analisaremos também a quantidade de conexões estabelecidas por padrão de usuário.

Para nosso estudo de caso, estabelecemos também que a quantidade máxima de Sas estabelecidas a um só tempo será inicialmente de 5 conexões/dia, se solicitado pelo usuário denominado de "cliente" e no máximo 8 conexões/dia, caso proveniente do usuário denominado "funcionário".

Para tanto definiremos algumas variáveis, que representarão em nível de sistema os parâmetros para o controle de acesso da aplicação VPN, e que serão gerenciadas por políticas:

- **LimCon** – é a quantidade máxima de conexões, isto é, SAs estabelecidas;
- **QtdConUsr** – quantidade de conexões de um mesmo usuário.
- **TipUsuario** – tipo do usuário, se "cliente" ou "funcionário"

Os valores iniciais de referencia, utilizados para demonstração são: LimCon = 100; QtdConUsr = 5 se do tipo cliente, e 8, se do tipo funcionário.

Para esta política adicional de segurança o objetivo é estabelecer critérios próprios à empresa para gerências da segurança entre as SAs. Serão avaliados os critérios entre os Domínios A e B. (figura 2). As regras adotadas são: se os critérios definidos não forem cumpridos, a conexão (SA) não será feita, e a VPN não será estabelecida (*IPSecDiscard*).

No modelo que estamos desenvolvendo, definimos as políticas de acesso e as requisições e respostas em XACML para verificação destes requisitos. Desenvolvemos uma interface gráfica em Java, que permite o teste destes requisitos e a geração de um relatório de auditoria, relatando as situações encontradas e permitindo uma melhor gerência da segurança.

## 7.1 Testes e Resultados

Após aplicarmos o modelo de gerência utilizando políticas definidas em XACML, verificamos que podemos definir as restrições de acesso de configuração e da aplicação utilizando XACML, bem como consultá-las, o que agrega muitos benefícios uma vez que a linguagem é baseada em XML, que já é um padrão. As definições de políticas facilitam os trabalhos dos administradores de rede, pois permitem a definição única das representações das políticas, que poderá ser aplicado em diversos elementos de rede, independendo do fabricante. O resultado da consulta que é gerado em XACML após a decisão é apresentado na figura 6.

```
<Response>
<Result>
<Decision>True</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

**Fig. 6 – Resultado da Consulta em XACML**

A partir do resultado das políticas verificadas será gerado um relatório para acompanhamento das conexões VPNs por parte do administrador de rede, contendo informações relevantes para o controle, tais como: origem e destino da conexão; tipo de usuário; quantidade de tentativas de acessos; status final da solicitação ( permitida ou negada ), entre outras.

## 8. Conclusões e Perspectivas

Concluímos que a utilização da arquitetura proposta para gerenciamento de VPNs é viável e que as definições de políticas em XACML podem ser utilizadas para gerenciar VPNs de forma bastante amigável e simples para o administrador de rede, bem como podem gerenciar outros tipos de conexões, pois o XACML é uma linguagem extensível e de fácil manuseio, permitindo assim a definição de novas políticas.

Sugestões para futuros trabalhos: ampliar as definições adaptando políticas para MPLS em XACML; desenvolver restrições de segurança que possam ser adaptadas ao protocolo 802.11.

## Referências


[1] BALTATU, M., LIOY, A., LOMBARDO, D., MAZZOCCHI, D."Towards a Policy System for Ipsec: Issues and an Experimental Implementation", IEEE International Conference on Networks (ICONN-2001) Bangkok, Thailand, outubro de 2001.

[2] BRAY, T. et al, "eXtensible Markup Language (XML) 1.0, second edition", W3C, Outubro de 2000, Disponível em: < http://www.w3.org/XML >.

[3] CONDELL, M. et al. "Security Policy Specification Language", Internet Draft, março de 2000, draft-ietf-ipsp-spsl-00.txt

[4] DAMIANOU, N. et al " The Ponder Specification Language", Workshop on Policies for Distributed Systems ans Networks (POLICY 2001), Bristol, UK, junho de 2001.

[5] DAMIANOU, N., "A Policy Framework for Management of Distributed Systems", Tese de doutorado, University of London, UK, fevereiro de 2002.

[6] FreeS/WAN, 2003, Disponível em: < http://www.freeswan.org >

[7] FU, Z. e WU, S. F - "Automatic Generation of IPSec/VPN Policies in an Intra-Domain Environment", 12th International Workshop on Distributed Systems: Operations & Management ( DSOM 2001) , Nancy , France, outubro de 2001.

[8] IETF Policy WorkGroup, 2002, Disponível em: <http://www.ietf.org/html.charters/policy-charter.html>

[9] JASON J., RAFALOW L. VYNCKE E. , MOORE B., RFC 3585,“ IPSec Configuration Policy Information Model”, agosto de 2003 .

[10] KENT, S., Atkinson, R., RFC 2402," IP Authentication Header", novembro de 1998.

[11] LIN, J., CHANG, C. e CHUNG, W., “Design, Implementation and Performance of IP-VPN”, Proceedings of the 17th International Conference on Advanced Information Networkings and Applications (AINA 03), China, março de 2003.

[12] LYMBEROPOULUS, L., LUPU, E., SLOMAN, M. “An Adaptative Policy Based Framework for Network Services Management”, Appear in Journal of Networks ans Systems Management, Special Issue on Policy Based Management of Networks Services, Vol 11, n°. 3, setembro de 2003.

[13] MADSON, C., Glenn,R., NIST, RFC 2403, ”The Use of HMAC-MD5-96 within ESP and AH", novembro de 1998.

[14] MOORE B. et al, RFC 3060, “Policy Core Information Model - Version 1 Specification”, fevereiro de 2001.

[15] MOORE B., RFC 3460, “Policy Core Information Model (PCIM) Extensions”, janeiro de 2003.

[16] OASIS, "A Brief Introduction to XACML”, Disponível em:< http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html , março de 2003.

[17] OASIS-XACML-1.0.pdf, Disponível em <http://www.oasisopen.org/committees/xacml/repository/ >, fevereiro de 2003.

[18] PEDATELLA, R., MADEIRA, E., MAGALHAES, M., "Um Framework para obtenção de QoS Fim-a-Fim na Internet", XXI Simpósio Brasileiro de Redes de Computadores,(SBRC2003), Natal, Brasil, maio de 2003.

[19] PERLMUTTER, B., ZARKOWER, J. “Virtual Private Networking : a view from the trenches”, cap. 1, pp 10, Prentice-Hall PTR, ISBN 0-13-020335-1, 2000.

[20] POLYRAKIS, A., BOUTABA, R., "The Meta Policy Information Base", IEEE Network, Março/Abril 2002.

[21] Relatório Interno LARCES – “LARCES_PBM – Um Framework para Gerência da Qualidade de Serviços e Segurança em Redes”, agosto de 2002.

[22] VERMA, D., " Policy-Based Networking - Architecture and Algorithms", cap. 7, New Riders Publishing, ISBN 1-57870-226-7, 2001.

[23] XIN GUO et al, “A Policy-Based Network Management Systems for IP VPN “ Proceedings of the 4th International Workshop on Policies for Distributed Policies and Networks. (POLICY 2003), Itália, junho de 2003.