Gestão de Identidade em Testbeds Brasileiros para a Internet do Futuro

Natalia C. Fernandes[1], **Edelberto F. Silva**[1],
Débora Muchaluat-Saade[1] **e Luiz Schara Magalhães**[1]

[1]Universidade Federal Fluminense (UFF) – Laboratório MídiaCom
Niterói, RJ – Brasil

Abstract. *Testbed federation allows researchers from different institutions to use network resources managed by different organizations, with different policies and procedures. This federated environment requires the coordination and mutual cooperation for identity management. This work proposes an architecture to the identity management and access control for the FIBRE project in Brazil, which is one of the main initiatives for experimental facilities for the Future Internet in Brazil. We compare our proposal to the architecture of other international projects, showing the required adjustments for the Brazilian scenario.*

Resumo. *A federação de testbeds permite que pesquisadores de diferentes instituições possam utilizar recursos de rede que são administrados por organizações distintas, e que por sua vez seguem diferentes políticas e procedimentos de uso. Nesse ambiente federado, é necessária a coordenação e cooperação mútua pela gestão de identidade. Esse artigo propõe uma arquitetura para a gestão de identidades e controle de acesso no Brasil para o projeto FIBRE, o qual é uma das principais iniciativas de redes para experimentação de Internet do Futuro no Brasil. A proposta é comparada com as arquiteturas utilizadas em outros projetos internacionais, com fim de mostrar as adaptações necessárias ao cenário de pesquisa brasileiro.*

1. Introdução

Uma vez conhecidas as limitações da arquitetura atual da Internet, um grande movimento com relação à pesquisa e proposta de novas arquiteturas surgiu em todo o mundo. Essa nova área de pesquisa visa a criação de uma nova Internet, a Internet do Futuro (IF), e deverá ser avaliada em ambientes experimentais antes de efetivamente poder ser utilizada em produção. Para tanto, várias testbeds têm sido criadas nos últimos anos[1]. A necessidade de interconexão dos ambientes de experimentação para avaliação dessas novas arquiteturas permite que pesquisadores de diferentes instituições possam utilizar, em seus experimentos, recursos de rede que são administrados por organizações distintas, e que por sua vez seguem diferentes políticas e procedimentos de uso. Esse ambiente integrado traz desafios tanto em termos de autenticação e autorização de usuários para uso e alocação de recursos, como em funções relacionadas ao conceito de gestão de identidade. A cooperação e interconexão lógica nesse ambiente é possível por meio de federações, que auxiliam na gestão dos recursos compartilhados.

Uma recente iniciativa para a criação de testbeds no Brasil é o Projeto FIBRE(*Future Internet testbeds experimentation between BRazil and Europe*)[2] O FIBRE tem como proposta a construção de uma rede para experimentação de larga escala, a qual inclui ambientes cabeados e sem fio, através da interligação de ilhas em diversos pontos do Brasil e da Europa. Assim, além de construir novos testbeds, ou ilhas, o FIBRE também é fortemente embasado na construção de um ambiente federado.

[1]http://cordis.europa.eu/fp7/ict/fire/ , http://www.geni.net
[2]http://www.fibre-ict.eu/

Esse artigo propõe uma arquitetura para gestão de identidade e controle de acesso para o FIBRE-BR, o que corresponde a federação das ilhas brasileiras do FIBRE. A ideia chave é prover meios para que o acesso ao FIBRE para pesquisadores brasileiros ligados a instituições de pesquisa seja feito de forma simples, através do uso da federação CAFe (Comunidade Acadêmica Federada). Além disso, é projetada uma arquitetura que permite autonomia nas ilhas sem comprometer as premissas de segurança e gerência do *Network Operating Center* (NOC) da rede.

O restante do artigo encontra-se da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. Na Seção 3 é apresentada a proposta para gestão de identidade no Projeto FIBRE e a Seção 4 apresenta as considerações finais.

2. Trabalhos relacionados

O objetivo da interconexão de testbeds para a Internet do Futuro é permitir que diversas redes sejam unidas de forma a criar um ambiente de teste de maior escala e de maior diversidade de equipamentos. Com isso, um pesquisador pode alocar seu experimento utilizando recursos de diferentes testbeds. Nesse caso, é preciso garantir que a autenticação de um usuário de uma testbed sirva como identificação para o uso dos recursos de qualquer outra testbed federada, desde que o usuário atenda às políticas locais de cada uma das redes.

Uma das principais propostas para federação de redes é o SFA 2.0 (*Slice-based Federation Architecture*) [Peterson et al. 2010]. Inicialmente desenvolvido para ser empregado no PlanetLab, Emulab, VINI [Bavier et al. 2006] e GENI, o SFA também pode ser expandido a outros *testbeds*. No SFA, cada entidade do sistema possui um identificador global (*Global Identifier* - GID), o qual é usado para autenticação e autorização. Especificamente, o GID é um certificado que contém três campos: uma chave pública, um UUID (*Universally Unique Identifier*) e uma validade. O GID é assinado por uma autoridade, de forma a validar as informações, gerando um certificado X.509. Após a autenticação, o usuário pode requisitar suas credenciais junto ao sistema de autorização. As credenciais descrevem os direitos e privilégios de um determinado usuário e são utilizadas para a obtenção de Tickets, que dão acesso ao uso de recursos específicos dentro da testbed. De forma geral, pode-se descrever as credenciais e os tickets como arquivos XML assinados.

A popularização do SFA se deu devido ao uso no ProtoGENI e no PlanetLab, cobrindo boa parte das redes que compõem o GENI. A autenticação no ProtoGENI é feita através de uma rede de confiança (*web of trust*). Cada ilha tem os certificados raiz de todos os membros da federação. A ideia chave é que os membros da federação confiam uns nos outros, de forma que o certificado gerado por um membro da federação deve ser aceito por qualquer outro membro. As permissões de acesso são definidas pelas credenciais, de acordo com o modelo do SFA.

Novas iniciativas no contexto de SFA e GENI estão desenvolvendo ferramentas para a realização da autenticação e do controle de acesso através do uso do Shibboleth [Mitchell 2011, Klingenstein 2010]. Entre as vantagens desse tipo de abordagem, está a utilização de todas as ferramentas já desenvolvidas para as organizações virtuais. Além disso, muitas instituições de pesquisa já uma mantém base de dados sobre os seus usuários, que pode ser utilizada para a autenticação nas testbeds. Outra vantagem é que esse tipo de gerência de identidades já traz os atributos de cada usuário, o que permite o uso de esquemas de autorização baseados em atributos, como o ABAC (*Attribute-Based Access Control*). Com isso, não é necessário que a testbed federada mantenha grandes bases de dados com usuários e listas de controle de acesso, já que todos os dados para a autorização podem ser providos pela instituição de origem do usuário. As implementações dessa proposta atualmente utilizam a rede InCommon de federação

de identidades, a qual inclui mais de 500 instituições de ensino e/ou pesquisa, instituições governamentais e empresas parceiras.[3]

Outras testbeds apresentam, atualmente, suporte a federação sem o uso do SFA, como a OFELIA [Köpsel and Woesner 2011, Channegowda et al. 2012]. No OFELIA, cada ilha tem um portal de acesso à rede federada chamado de Expedient, o qual é capaz de acessar os gerenciadores de agregados de todas as outras ilhas. Os usuários são registrados utilizando a *OFELIA registration tool* (OFREG), a qual atualiza um diretório LDAP (*Lightweight Directory Access Protocol*) global com as credenciais do usuário. Assim, o LDAP global é responsável pela autenticação e autorização na testbed federada. Para aumentar a disponibilidade e a confiabilidade, cada ilha mantém uma instância sincronizada do LDAP global. O acesso de usuários externos à testbed é feito através de túneis VPN (*Virtual Private Network*), após a fase de autenticação.

3. Proposta de Gestão de Identidade no FIBRE

Esse artigo propõe uma arquitetura para gestão de identidades e controle de acesso na rede do FIBRE-BR. A seguir, são apresentados alguns dos principais requisitos para a construção dessa arquitetura e a estrutura proposta. A ideia central é prover diferentes formas de acesso, sendo a principal por meio da CAFe[4].

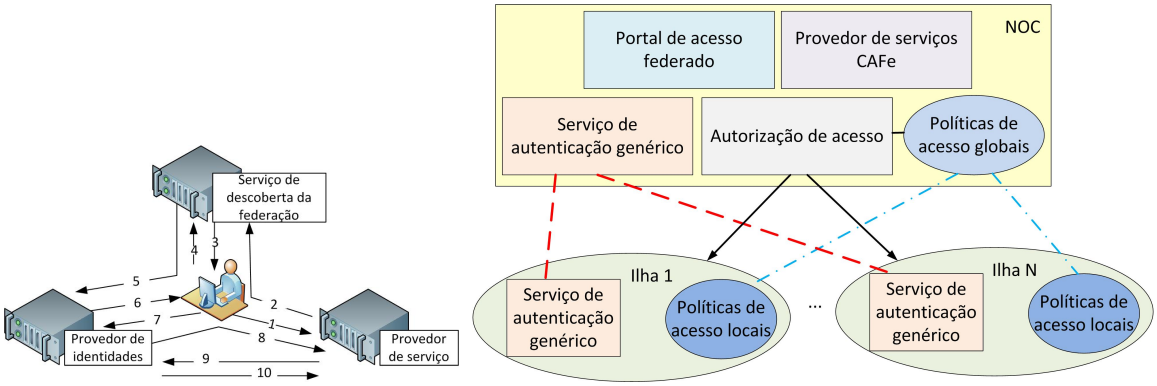
3.1. O Projeto FIBRE

O FIBRE (*Future Internet experimentation between BRazil and Europe*) [Sallent et al. 2012] é uma parceria entre instituições brasileiras e europeias com o fim de criar uma testbed de larga escala. Topologicamente, o FIBRE pode ser visto como a união de uma grande ilha europeia e uma grande ilha brasileira. A ilha brasileira, chamada de FIBRE-BR, consiste da federação de diversas pequenas ilhas, situadas em diferentes universidades e centros de pesquisa. A interligação dessas ilhas é feita através do uso do *backbone* da RNP e de outras redes de pesquisa, como a GIGA e a Kyatera.

No FIBRE, existem diversos arcabouços de controle de experimentação. Para controlar os equipamentos OpenFlow, o experimentador usa o arcabouço *OFELIA Control Framework* (OCF) [Köpsel and Woesner 2011], o qual foi desenvolvido pelo projeto OFELIA para lidar com comutadores OpenFlow e máquinas virtuais. Para controlar equipamentos sem fio, o FIBRE disponibiliza o *cOntrol and Management Framework* (OMF) [Rakotoarivelo et al. 2010]. O OMF foi desenvolvido para o projeto ORBIT, mas atualmente é utilizado em diversas testbeds, devido a sua interface flexível. Além disso, o FIBRE conta ainda com ilhas baseadas no ProtoGENI, que é um arcabouço de controle desenvolvido para o projeto GENI[5]. A ideia é que o FIBRE possa disponibilizar diferentes interfaces de controle e que possa agregar um número cada vez maior de ilhas, através da federação.

Embora a existência de diferentes arcabouços traga a flexibilidade para o experimentador, a heterogeneidade do controle traz dificuldades na federação dos recursos e na gestão de identidade, pois cada arcabouço de controle utiliza diferentes mecanismos e API's de controle. Uma proposta para fazer essa interligação seria o uso de um portal único para a autenticação, reserva de recursos e monitoramento, o qual seria responsável pela comunicação com os gerenciadores de *slice* e de agregado de cada ilha. Um proposta inicial para esse portal seria o uso do MySlice[6]. Além disso, seria necessária uma interface para o compartilhamento de recursos, o que poderia ser feito através do SFA [Peterson et al. 2010]. Uma dificuldade para esse tipo de implementação

[3]http://www.incommonfederation.org/participants/
[4]http://portal.rnp.br/web/servicos/cafe
[5]http://www.protogeni.net/wiki/ClearingHouseDesc
[6]http://myslice.info/



(a) Fluxo de dados na federação CAFe. (b) Visão geral da arquitetura proposta para a gerência de identidades e controle de acesso do FIBRE.

Figura 1. Visões gerais da federação CAFe e do esquema proposto para o FIBRE.

é que o arcabouço de controle deve ter suporte ao SFA para poder ser integrado, ou seja, é necessário um *wrapper* para cada arcabouço de controle, como proposto no NOVI [Lymberopoulos et al. 2012]. Atualmente, tanto o OCF quanto o OMF ainda estão em fase de desenvolvimento desse *wrapper*, o qual está disponível apenas no ProtoGENI, que tem suporte nativo ao SFA. Portanto, o FIBRE precisa utilizar uma solução para federação mais genérica, que permita a integração de outros testbeds com diferentes arcabouços. Assim, seria possível dar suporte ao SFA e também a novos padrões.

Para a gerência dos recursos da rede, o FIBRE conta com um *Network Operations Center* (NOC). O NOC do FIBRE é responsável pelo gerenciamento e controle da rede em alto nível, podendo prover serviços básicos, como o servidor de portal para acesso de recursos centralizado, ou ainda, uma terceira parte confiável, caso certificados estejam sendo utilizados na rede.

3.2. Comunidade Acadêmica Federada – CAFe

A CAFe (Comunidade Acadêmica Federada) é uma federação que reúne instituições de ensino e pesquisa brasileiras. Através da CAFe, um usuário mantém todas as suas informações na instituição de origem e pode acessar serviços oferecidos pelas instituições que participam da federação.

Como se pode observar na Figura 1(a), a autenticação e autorização federadas da CAFe são baseadas nos provedores de identidade, responsáveis por manter os dados dos usuários e autenticá-los, e nos provedores de serviço, que oferecem um recurso ou serviço específico. Esse tipo de federação só funciona quando existe uma relação de confiança entre os provedores de identidade e de serviço. Para utilizar um serviço com a CAFe, o usuário deve tentar acessar o provedor de serviço (1). Ao perceber que o usuário não foi autenticado, o provedor de serviço redireciona o usuário para uma página (2) na qual ele seleciona o seu provedor de identidades (3 e 4). O navegador é, então, redirecionado para o provedor de identidade (5), o qual deve autenticar o usuário (6 e 7), passar o resultado para o provedor de serviços (8) e criar uma sessão de uso associada ao usuário, de tal forma que novos serviços ou pedidos de atributos dentro de uma janela de tempo não gerem novos pedidos de autenticação (9 e 10).

A CAFe está integrada à eduGAIN[7], que reúne, em uma rede de confiança, as federações acadêmicas da GÉANT. Por ser uma federação de instituições de ensino e pesquisa, está sendo proposta a utilização da CAFe/eduGAIN como principal meio de

[7]http://www.geant.net/service/edugain/

autenticação no FIBRE. Nesse caso, o portal de acesso à testbed atuaria como um provedor de serviço no esquema da CAFe.

3.3. Proposta de gestão de identidade e de controle de acesso

Uma proposta para gestão de identidade no Projeto FIBRE se baseia, portanto, na utilização da CAFe como provedora de identidade no lado brasileiro, uma vez que essa federação já se encontra associada à eduGAIN, que poderia ser usada para autenticação no FIBRE pelo lado europeu. Contudo, os usuários do FIBRE podem ser de empresas parceiras, além das instituições da comunidade acadêmica ainda não associadas à CAFe. Então, apenas a CAFe não basta como provedor de identidade. Por essa razão, essa proposta prevê, somando-se ao uso da CAFe, outras formas de autenticação. Uma delas é baseada no uso do LDAP com um esquema que estende brEduPerson, esquema usado na CAFe, com outros atributos necessários para os arcabouços de controle dos testbeds. Uma vez que o FIBRE é uma rede colaborativa, propõe-se o uso de um LDAP hierarquizado, onde a raiz encontra-se no NOC e cada instituição mantém sua própria base de acesso. Além disso, o acesso poderia ser provido por meio de outros esquemas para gestão de identidade, como o OpenID, desde que se criasse os mecanismos para a geração das credenciais aceitas nos gerenciadores de agregados das diversas ilhas.

A Figura 1(b) mostra uma visão geral da arquitetura de gestão de identidade e controle de acesso proposta. Na parte superior da figura, encontram-se os serviços do NOC para gestão de identidade e controle de acesso. Primeiramente, tem-se o portal de acesso federado, o qual é acessado pelo experimentador para realização de um experimento. É nesse portal que o usuário irá indicar suas credenciais de acesso e os recursos que deseja alocar. Com base nos recursos selecionados, o sistema terá como saber como será provido o acesso aos recursos, seja por meio de certificados, como no SFA, ou com algum outro tipo de token. Com base nas credenciais, o sistema selecionará se a autenticação deve ser feita por meio do provedor de serviços da CAFe ou por um sistema de autenticação genérico. No caso do sistema genérico, é importante observar a estrutura hierárquica, ou seja, cada ilha irá apresentar a sua base de usuários local e o NOC será a raiz da estrutura de confiança entre as ilhas.

Após autenticar os usuários, é necessário checar se o usuário terá acesso ou não aos recursos solicitados. Assim, após receber a resposta do módulo de autenticação, o módulo de autorização de acesso deve consultar a base de políticas de acesso da rede federada. Para isso, propõe-se o uso de uma base global, que define as regras globais da testbed, ou seja, as regras que devem ser seguidas por todas as ilhas. Em seguida, deve-se consultar as políticas locais das ilhas cujos recursos estão sendo alocados, de forma que cada ilha tenha autonomia sobre os seus recursos. Após essas consultas, esse módulo deve liberar o acesso, seja pelo redirecionamento do usuário para os gerenciadores de agregados ou pela geração de certificados ou tokens. De fato, a forma de liberar o acesso depende do arcabouço de controle que será utilizado.

3.4. Comparação com outras abordagens

A Tabela 1 mostra algumas das principais características da autenticação e controle de acesso a alguns dos principais testbeds. Com base nessa tabela, é possível observar algumas das escolhas para o FIBRE, baseadas na diversidade dos ambientes de experimentação.

4. Considerações Finais

Este trabalho é motivado pela necessidade de interconexão de ambientes de experimentação para a Internet do Futuro. Neste contexto, as chamadas federações de autenticação e autorização podem ser utilizadas para facilitar o uso compartilhado dos recursos por pesquisadores de diferentes instituições.

Tabela 1. Comparação de esquemas de diferentes testbeds .

Rede	Política de acesso	Gestão de ID	Acesso	Portal
GENI	Registro + Projeto de pesquisa	SFA	Credenciais GENI + tickets	Flack, OMNI
PlanetLab	Disponibilizar recursos + Registro + Projeto de pesquisa	SFA	Credenciais GENI + tickets + SSH	EMULAB, interfaces do GENI
OFELIA	Registro + Projeto de pesquisa	LDAP/MySQL	Chave pública + VPN	Expedient
NITOS	Registro + Requisição por e-mail	Base local ou LDAP	Chave pública + SSH	NITOS Scheduler
FIBRE (proposta)	Registro + Projeto de pesquisa	CAFE/LDAP/ bases locais/ SFA	Misto (depende de arcabouço)	MySlice, Expedient, NITOS Scheduler

O levantamento de soluções e a proposta de arquitetura realizados por esse trabalho visam apresentar soluções que possam ser empregadas no âmbito do projeto FIBRE e auxiliem na integração dos ambientes tanto no sentido de alocação de recursos quanto da gerência da identidade do usuário para fins de autenticação e autorização. Como trabalho futuro, pretende-se detalhar os módulos da arquitetura proposta e implementá-los no âmbito do projeto FIBRE.

Referências

Bavier, A., Feamster, N., Huang, M., Peterson, L., and Rexford, J. (2006). In VINI veritas: realistic and controlled network experimentation. *SIGCOMM Comput. Commun. Rev.*, 36(4):3–14.

Gavras, A., Brüggemann, H., Witaszek, D., Sunell, K., and Jimenez, J. (2006). Pan european laboratory for next generation networks and services. In *TRIDENTCOM*. IEEE.

Köpsel, A. and Woesner, H. (2011). Ofelia: pan-european test facility for openflow experimentation. Em *Proc. 4th European conference on Towards aservice-based internet*, ServiceWave'11, p.p. 311–312, Berlin, Heidelberg.

Lymberopoulos, L., Grammatikou, M., Potts, M., Grosso, P., Fekete, A., Belter, B., Campanella, M., and Maglaris, V. (2012). NOVI tools and algorithms for federating virtualized infrastructures, pages 213–224. Berlin, Heidelberg.

Peterson, L., Ricci, R., Falk, A., and Chase, J. (2010). Slice-based federation architecture. Technical report.

Rakotoarivelo, T., Ott, M., Jourjon, G., and Seskar, I. (2010). OMF: a control and management framework for networking testbeds. *SIGOPS Oper. Syst. Rev.*, 43(4):54–59.

Sallent, S., Abelém, A., Machado, I., Bergesio, L., Fdida, S., Rezende, J., Simeonidou, D., Salvador, M., Ciuffo, L., Tassiulas, L., and Bermudo, C. (2012). FIBRE project: Brazil and Europe unite forces and testbeds for the Internet of the future. In *Proceedings of TridentCom 2012*.

Szegedi, P., Figuerola, S., Campanella, M., Maglaris, V., and Cervelló-Pastor, C. (2009). With evolution for revolution: managing federica for future internet research. *Comm. Mag.*, 47(7):34–39.

Yuan, E.; Tong, J. (2005) Attributed based access control (ABAC) for Web services. Proceedings of the 2005 IEEE International Conference on Web Services (ICWS 2005), 561–569.

Channegowda, M.; Kotronis, V.; Bergesio, L.; Puype, B.; Efstathiou, N. (2012) OFELIA First report on implementation testing and operation of Federated Islands Technical report. Version 1.0 - ICT-258365, 1–48.

Tom Mitchell (2011) Identity Management and Attributes in GENI. In 11th GENI Engineering Conference - GEC11

K. Klingenstein (2010) External Identity and Authorization in GENI. In 8th GENI Engineering Conference - GEC8