Autenticação Centralizada em Sistemas Heterogêneos

Wanderson Nunes da Rosa[1] **, Carlos Vinícius Rasch Alves**[2]

[1]Redes de Computadores
Faculdade de Tecnologia SENAC Pelotas (FATEC)
Rua Gonçalves Chaves 602 – 96015560 – Pelotas – RS – Brazil

wandnrosa@gmail.com, cvalves@senacrs.edu.br

Abstract. *This work aims to implement an interoperable heterogeneous network environment, where client stations will be able to verify credentials through servers on different platforms, thus promoting centralized authentication. To achieve this goal, a Linux platform server (openSUSE) and another Microsoft (Windows Server 2008 Enterprise) server were implemented, thus providing an open source and a proprietary strand for the analysis of the feasibility and advantages of the proposed integration*

Resumo. *Este trabalho tem por objetivo a implementação de um ambiente de rede heterogêneo interoperável, onde estações clientes estarão habilitadas a realizarem a verificação de credenciais através de servidores em plataformas distintas, promovendo assim a autenticação centralizada. Para alcançar tal objetivo foi implementado um servidor em plataforma Linux (openSUSE) e outro em plataforma Microsoft (Windows Server 2008 Enterprise), proporcionando assim uma vertente open source e outra proprietária, para a análise da viabilidade e vantagens da integração proposta.*

1. Introdução

Nessa seção iremos abordar o contexto do tema, o que motivou a escolha, juntamente com o objetivo do que será abordado no presente trabalho.

1.1. Contextualização

O alto custo na adoção de uma plataforma que seja totalmente proprietária para a estruturação de um ambiente de TI (Tecnologia da Informação) é um problema permanente e que tem se tornado um grande desafio para muitas organizações. Destas, em particular podemos destacar as pequenas, onde em sua maioria possuem orçamentos e recursos limitados. Muitas dessas organizações acabam por adotar medidas de contenção de gastos levando serviços e departamentos de TI a sofrerem deficit em resposta a este problema. Como conseqüência, elas são muitas vezes limitadas a tecnologias mais antigas e até mesmo a versões obsoletas do *software*, devido ao alto custo de atualizações constantes e aquisições de novas licenças.

A confiabilidade dos sistemas atuais também se tornou uma questão importante e preocupante devido ao grande crescimento das redes de computadores locais e da Internet. Em decorrência de tal fato temos como consequência uma disseminação de vírus cada vez mais acelerada e dinâmica em um âmbito global, colocando em risco diariamente todos os processos organizacionais que rodam sobre a infraestrutura de TI.

Assim temos um ambiente onde empresas estão cada vez mais preocupadas com a segurança de seus sistemas e proteção de seus dados. Todo este cenário, aliado à crescente popularização dos sistemas operacionais *open source*, tem elevado o número de empresas interessadas na adoção dos serviços baseados nesta plataforma.

A adoção desta plataforma se deve principalmente a fatores como: segurança, disponibilidade e também ao baixo custo de implementação e licenciamento. Com isso nos deparamos cada vez mais com uma mudança na estruturação dos *Data Centers* atuais. Atualmente não encontramos mais um ambiente homogêneo e com predominância de uma única tecnologia, mas sim uma diversificação de plataformas onde *software* proprietário e livre se juntam em um mesmo cenário [Souza 2015].

Na perspectiva de [Figueiredo et al. 2016], grande parte das organizações acabam por adotar múltiplas plataformas em seus ambientes de TI devido a razões históricas e pragmáticas, tendo como intuito, atender as suas diversas necessidades as quais não podem ser sanadas com apenas uma única tecnologia.

Entretanto, novos desafios são gerados ao se unir tecnologias distintas em um mesmo ambiente, um desses desafios é continuar provendo de forma eficiente e segura a autenticação e acesso a rede através dos serviços de diretório para os diferentes tipos de sistemas operacionais clientes. As grandes empresas possuem uma gama de plataformas, onde cada uma possui seu próprio gerenciamento de usuários. Essa descentralização gera uma demanda enorme aos responsáveis pela administração dos objetos de diretório como contas de usuários, contas de computador, diretivas de segurança, dentre outros.

Nesse modelo de arquitetura de controle baseada em banco de dados distribuídos, acabam-se por criar desafios como, replicação e consistência nas múltiplas bases de diretórios, aumentando também assim a exposição a ataques e falhas de segurança [Barreto et al. 2013].

Com o aumento das redes de computadores e as constantes mudanças e evoluções, o gerenciamento de identidade torna-se cada vez mais complexo. Uma organização não pode esperar um longo período para que um determinado empregado consiga se autenticar na rede e obter acesso a uma determinada aplicação. As exigências de produtividade dos ambientes corporativos exigem que o acesso do usuário aos recursos da rede seja imediata e satisfatória, não prejudicando assim seu desempenho.

Porém, mais do que implementar diferentes plataformas nas redes de computadores contemporâneas, existe hoje uma alta necessidade de integração desses novos sistemas *open source* com as tecnologias proprietárias já utilizadas, permitindo assim que os serviços oferecidos pelos mesmos continuem operando de forma ininterrupta e consistente. Em especial destacamos o serviço de diretório, pois é através deste poderoso recurso que provemos de forma centralizada e segura todo o gerenciamento e autenticação dos usuários corporativos. Existem alguns mecanismos que permitem tal gerenciamento e autenticação em ambientes mistos, em particular o LDAP (*Lightweight Directory Access Protocol*) merece destaque. O foco principal deste trabalho é apresentar este protocolo, procurando analisar e descrever duas de suas implementações, *Active Directory* e OpenLDAP, tendo como foco a centralização através da autenticação.

1.2. Motivação

De acordo com pesquisa realizada pela Fundação Getúlio Vargas [FGV 2016], Figura 1, foi constatado que nos *Data Centers* atuais 12% dos servidores contam com o sistema operacional Unix, 20% com o sistema Linux, 66% Windows e 2% outros sistemas. Estas estatísticas mostram a grande heterogeneidade das redes de computadores contemporâneas [Coulouris et al. 2013] e que há um grande desafio a ser vencido no gerenciamento de identidade entre essas plataformas distintas.

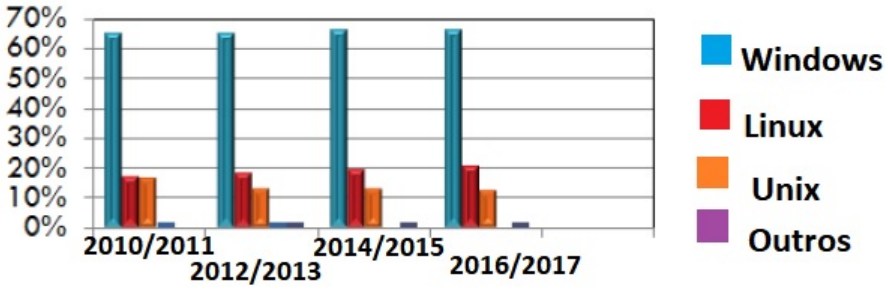

Figura 1. Gráfico Evolução 2010/2017

A autenticação entre sistemas proprietários e de código aberto já é uma realidade no meio empresarial. Devido a esse cenário, e as inúmeras mudanças no mundo dinâmico da TI com foco cada vez maior em interoperabilidade, se faz necessário uma maior explanação e pesquisa sobre a capacidade de tecnologias distintas coexistirem no mesmo ambiente, provendo a autenticação cruzada de forma harmoniosa e mais do que isso, produtiva.

1.3. Objetivo

Este trabalho tem por objetivo a implementação de um ambiente de rede heterogêneo e interoperável através da autenticação cruzada, utilizando para isso ferramentas que estejam disponíveis nas plataformas adotadas e que permitam a comunicação entre os sistemas.

O ambiente proposto tem como propósito que usuários de estações clientes Linux ou Windows possam ser autenticados usando o protocolo LDAP, tanto no serviço de diretório da Microsoft, o *Active Directory*, quanto em sua versão livre, o OpenLDAP, de forma que estes possam usufruir das potencialidades de ambas as tecnologias, garantido assim maior segurança e versatilidade no acesso às informações.

2. Referencial Teórico

Para uma melhor compreensão do trabalho apresenta-se nesta seção os conceitos e ferramentas necessárias para a implementação e desenvolvimento do ambiente de autenticação cruzada proposto.

2.1. Domínio

Podemos definir um domínio como um limite administrativo e de segurança. Em um limite administrativo, as contas que possuem tais privilégios têm permissões de acesso

em todos os recursos do domínio ao qual estão inseridas, mas não em recursos de outros domínios, ou seja, o domínio é quem define as fronteiras de permissões.

Já a caracterização como um limite de segurança se dá pelo fato de que cada domínio em particular tem suas definições de políticas de segurança que se aplicam às contas de usuários e demais recursos dentro do domínio e não a outros domínios. Assim, diferentes domínios podem ter diferentes políticas e configurações de segurança [Barreto et al. 2013].

O conjunto de contas de computadores e de usuários cadastrados de forma centralizada em um banco de dados compartilhado por toda a rede também é uma das formas de definirmos um domínio. Por contas de usuários e computadores entende-se ser o nome e a senha dos mesmos, credenciais necessárias para que possam acessar os recursos da rede, ou seja, o domínio ao qual pertençam. Em se tratando de domínios podemos enumerar várias vantagens, dentre as mais pertinentes destacam-se: escalabilidade, portabilidade e a facilidade de administração.

Escalabilidade: A utilização da estrutura de domínio promove um crescimento da rede computacional de forma organizada e simples, nesse ambiente os usuários possuem apenas um nome e uma senha e conseguem acessar todos os recursos da rede aos quais tenham permissão [MINASI 2008].

Portabilidade: Habilita os usuários que pertencem ao domínio se autenticarem e usarem qualquer computador que esteja nesse domínio, permitindo que os mesmos tenham suas configurações disponíveis em qualquer máquina da rede, alcançando assim uma maior portabilidade [MINASI 2008].

Facilidade de administração: Ambientes que possuem um domínio de rede, ao contratar um funcionário, basta apenas cadastrá-lo no banco de dados do domínio, com as permissões aos recursos de rede necessários. Não é necessária nenhuma alteração nas estações de trabalho para que esse usuário possa ser um membro de toda a rede do domínio. Para excluir um usuário, basta excluí-lo do banco de dados do domínio [MINASI 2008].

2.2. Diretório

Uma das formas de sintetizar e entender o conceito de diretório é imaginar um banco de dados centralizado com informações sobre usuários, senhas, computadores e outros elementos necessários ao funcionamento de um sistema. Esse sistema pode ser representado por um conjunto de aplicações em um servidor, serviços de email ou autenticação. Pode-se também fazer uma analogia à uma lista telefônica com os cadastros dos nomes dos usuários, telefones e endereços, que também refletem uma analogia com um típico diretório [Barreto et al. 2013].

Em termos gerais, grande parte dos profissionais de informática associa o termo diretório ao contexto de sistemas de arquivos, o que só em parte é verdadeiro. Ao pesquisar o conceito da palavra diretório percebe-se que a mesma tem vários significados, se diferenciando de acordo com o contexto. No contexto de sistemas de arquivos possui um significado, no contexto de redes e ambientes distribuídos outro e no contexto de banco de dados um terceiro significado [Zeilenga 2012].

Diretório em sistemas de arquivos nada mais é do que um arquivo especial que

contém as lista dos arquivos pertencentes a esse diretório. No contexto de redes e ambientes distribuídos, diretório é uma lista que contém informações de serviços de rede que, por exemplo, exigem algum tipo de autenticação, obrigando que os serviços mantenham um diretório de usuários, ou seja, uma lista de usuários. Já no contexto de banco de dados é mais intuitivo, uma vez que lista é na verdade um depósito de informação [Zeilenga 2012].

Nas redes de computadores com modelo baseado em diretório, há uma base única de informações, que podem ser contas de usuários, contas de computador ou qualquer outro recurso da rede. Porém, na prática não é que exista uma única base armazenada em um determinado servidor e todos os demais acessam esta base. O que realmente acontece é que todos contêm uma cópia do diretório e alterações efetuadas em um dos servidores são repassadas para os demais, para que todos fiquem com uma cópia idêntica da base de dados do diretório. Esta sincronização entre os servidores é conhecida como replicação [Barreto et al. 2013].

De acordo com [Quirino 2013], a utilização de um diretório varia de acordo com a necessidade. Em resumo, pode-se citar os seguintes:

Sistemas de Arquivos: Nesse contexto, um diretório é simplesmente definido como um arquivo especial que contém as informações pertencentes a esse diretório.

Redes em Ambientes Distribuídos: Com esse contexto o diretório corresponde a uma lista que contém informações dos serviços da rede para o efeito de autenticação da mesma.

Base de Dados: No que diz respeito à base de dados, um diretório é uma estrutura (*schema*), que armazena diversas tabelas, sendo estas tabelas com características comuns.

Em resumo, pode-se definir um diretório como uma base de dados especialista com o propósito de prover o acesso rápido aos dados de forma padronizada, contendo diferentes tipos de informações e oferecendo uma versatilidade muito grande na hora de buscar o dado desejado.

2.3. Serviço de Diretório

Os serviços de diretório despontam atualmente nos domínios de softwares para gestão de redes de computadores, principalmente no campo de servidores. Esses tipos de serviços, implementam uma base de dados distribuída, onde a informação é armazenada de forma hierárquica, seguindo a estrutura de uma árvore [Praia 2006].

Se o diretório é uma base de dados organizada, ou seja, uma lista de dados, um serviço de diretório nada mais é do que uma aplicação que controla os objetos e seus atributos em um diretório. Com o serviço de diretório, os objetos e os atributos podem estar disponíveis aos usuários e a outras aplicações de forma ininterrupta e centralizada. Existem hoje, muitas implementações de software que desempenham a função de diretório, por exemplo, o *Active Directory* e o Openldap. Serviço de diretório é a implementação cliente/servidor para o conceito de diretório [Zeilenga 2012].

Dada a necessidade crescente de informações, em particular através da Internet, a popularidade do diretório tem crescido na última década e hoje é uma escolha comum para aplicações distribuídas [Whitmore et al. 2015].

Para o cumprimento dos objetivos de integração das plataformas heterogêneas através da autenticação cruzada, será necessária a implementação de servidores Microsoft e Linux, com os serviços de diretório do *Active Directory* e OpenLDAP respectivamente, atuando no mesmo domínio.

2.4. O protocolo LDAP (*Lightweight Directory Access Protocol*)

O LDAP (*Lightweight Directory Access Protocol*) é um protocolo padrão inicialmente projetado para o acesso a serviços de diretório com o padrão X.500. O LDAP é a versão reduzida de um protocolo chamado DAP (*Directory Access Protocol*). A principal função do DAP era a de estabelecer, de forma padrão, regras de comunicação de acesso com um diretório baseado no padrão X.500, mas por ser complexo permitiu o surgimento do LDAP que implementa apenas as operações básicas do DAP como: *Bind*, *Read*, *List*, *Search*, *Compare*, *Modify*, *Add*, *Delete* e *ModifyRDN* [Santos 2013]. De acordo com [SENA 2014], o LDAP trabalha diretamente sobre o protocolo TCP/IP e oferece mais funcionalidades do que o DAP e a um custo menor. Como se trata também de um diretório, ele baseia-se fundamentalmente no modelo cliente/servidor e fornece autenticação e o serviço de diretório para os utilizadores.

O protocolo LDAP é utilizado pela arquitetura do *Active Directory* e ainda é possível de ser implementado usando o OpenLDAP em plataforma livre, que será tratado posteriormente neste artigo. Serviços de diretórios implementando LDAP podem conter informações particulares de funcionários e informações sobre a organização [SENA 2014].

O OpenLDAP se tornou o primeiro serviço de diretório de código aberto em decorrência da Universidade de Michigan que trabalhava em um projeto com o objetivo de desenvolver o seu próprio servidor LDAP e decidiu abrir o código fonte do seu *software*, surgindo assim a versão de código aberto, o OpenLDAP, colocando esses recursos disponíveis para usuários da plataforma Linux [SENA 2014].

2.5. Implementações do Protocolo LDAP

Nesta seção serão abordadas duas implementações do protocolo LDAP que serão utilizadas para a criação do ambiente misto proposto neste trabalho, *Active Directory* da Microsoft e a vertente livre o, OpenLDAP.

2.5.1. OpenLDAP

O OpenLDAP pode ser descrito como uma composição de um conjunto de aplicativos LDAP *open source*, no qual estão dispostas todas as ferramentas necessárias para fornecer um serviço de diretório padrão LDAP v.3 em um ambiente de rede, disponível em várias plataformas (Linux, Solaris, MacOS). É uma solução considerada estável e possui amplo suporte, sendo largamente utilizada como alternativa às implementações comerciais existentes como, *Active Directory*, *Novell eDirectory* e *Sun Java System Directory Server* [JUNIOR 2009].

Para [SENA 2014], o OpenLDAP é definido como uma implementação livre do protocolo LDAP, que foi criado inicialmente com o objetivo de permitir acesso a serviços de diretório, através da Internet, embora seja possível utilizar qualquer tipo de dados.

A autenticação usando o OpenLDAP, conforme [Quirino 2013] e [JUNIOR 2009], baseia-se fundamentalmente em dois métodos básicos que são os seguintes:

LDAP *Bind*: Método que consiste em fazer login enviando sua senha, em seguida o serviço fornece a permissão de autenticação ou então nega o acesso aos recursos solicitados. Neste caso, o utilizador apenas faz a requisição do serviço sem se preocupar com a forma como a validação do seu pedido será executado.

LDAP *Compare*: Outro método de autenticação onde é utilizada a comparação. O utilizador envia sua senha e pede ao servidor para compará-la com a que se encontra armazenada no diretório e a resposta é retornada com a permissão ou negação de acesso.

2.5.2. *Active Directory*

O *Active Directory* armazena informações sobre usuários, computadores e recursos de rede, tornando os recursos acessíveis aos aplicativos. Ele fornece uma forma consistente de nomear, descrever, localizar, acessar, gerenciar e garantir a segurança de informações sobre os recursos. De acordo com [Radeck 2012], o *Active Directory* possui as seguintes funções:

Centralizar o controle de recursos de rede: Com a centralização do controle de recursos como servidores, arquivos compartilhados e impressoras, apenas usuários autorizados podem acessar os recursos oferecidos no *Active Directory*.

Centralizar e descentralizar o gerenciamento de recursos: Os administradores podem gerenciar os computadores de clientes distribuídos, serviços de rede e aplicativos a partir de um local central usando uma interface de gerenciamento consistente. Também podem distribuir tarefas administrativas, delegando o controle de recursos a outros administradores.

Armazenar objetos de modo seguro em uma estrutura lógica: O *Active Directory* armazena todos os recursos como objetos em uma estrutura lógica, hierárquica e segura.

Otimizar o tráfego de rede: A estrutura física do *Active Directory* permite usar a largura de banda da rede de modo mais eficiente. Por exemplo, ela garante que os usuários, ao efetuarem logon, sejam autenticados pela autoridade mais próxima, o que reduz o tráfego de rede.

3. Ferramentas para a Autenticação Centralizada

Para o ingresso de máquinas Linux em um domínio do *Active Directory* e sua posterior autenticação, foi utilizada a ferramenta *Likewise Open*, uma aplicação *open source* a qual permite que máquinas Linux, Unix e Mac possam ingressar em um domínio do *Active Directory* e serem autenticadas de maneira segura com suas credenciais de domínio. Para autenticação de clientes Windows no OpenLDAP foi adotada a ferramenta pGina. O pGina é um *software* livre de autenticação cujo propósito é substituir de forma parcial a biblioteca GINA (*Graphical Identification and Authentication*) a qual é carregada pelo sistema winlogon do Windows e é responsável pelos processos de login e de logout dos usuários [Rosa 2008].

3.1. Topologia

Para a instalação dos sistemas operacionais clientes, servidores e ferramentas mencionadas anteriormente, foi projetado um cenário utilizando uma única máquina física com a seguinte configuração de hardware, conforme Tabela 1:

Tabela 1. Recursos de hardware disponíveis

Recursos	Características
Disco	2 TB
Memória RAM	16 GB
Rede	100 MB/s
Processador	3.70 GHz

Todos os sistemas foram virtualizados utilizando o *software VMware Workstation Pro*. Sua adoção deu-se por motivos como o acesso gratuito, testes de utilização prévios e pesquisas sobre o produto, facilitando assim sua instalação e configuração. *VMware Server* é um produto gratuito de virtualização para servidores em ambas as plataformas, Windows e Linux. Ele permite particionar um servidor físico em várias máquinas virtuais para assim poder usufruir das vantagens da virtualização. Com isso tem-se um cenário virtualizado conforme apresentado na Figura 2, onde temos um centralizador Linux (Samba 4) representando a ligação feita entre os sistemas virtualizados.

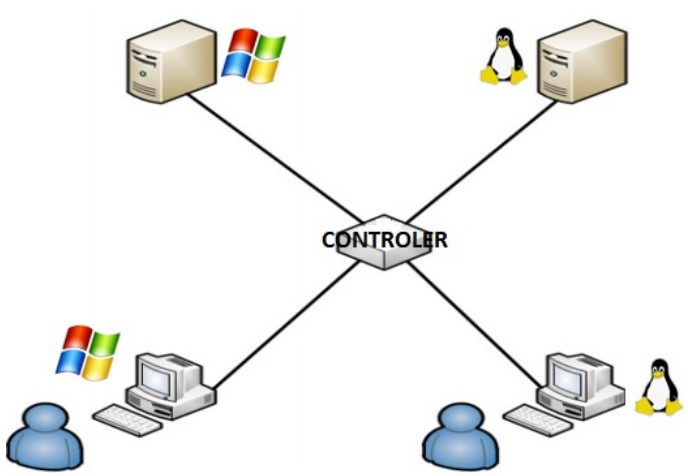

Figura 2. Autenticação entre Sistemas Heterogêneos

4. Principais Metodologias de Autenticação Externa

A seguir, serão descritas as principais metodologias de autenticação externa, ou seja, visando trabalhos futuros, onde será possível a expansão da autenticação a dispositivos móveis. Sabendo que a tecnologia tem seu crescimento contínuo, será mostrada a autenticação de uma forma completa, com intuíto de implementação em cenários reais.

4.1. Dispositivos Móveis

Um dispositivo móvel é um dispositivo de computação portátil, pequeno, geralmente equipado com um método de entrada e uma tela de exibição, tanto *smartphones* quanto

notebooks. Muitos dispositivos móveis portáteis têm sistemas operacionais que podem executar aplicativos, tais como Windows, Android, Linux, iOS. Os Sistemas Operacionais permitem que os dispositivos móveis e celulares sejam usados como dispositivos de trabalho ou de acesso pessoal, tanto em lugares privados como públicos.

4.1.1. Autenticação da Rede sem Fio através do Protocolo LDAP

O LDAP, segundo [Castro 2017] , nada mais é do que um banco de dados que armazena as credenciais dos usuários de uma determinada rede. Cada cliente (suplicante) necessita de um usuário e senha validos para adentrar a rede. Quando um suplicante solicita entrada na rede, o ponto de acesso manda uma requisição ao servidor de autenticação centralizada (neste caso, PfSense), este por sua vez consulta no servidor LDAP (Samba4 - *Active Directory*) e verifica se o usuário é valido, se a senha é a correspondente e quais são as permissões daquele usuário dentro da rede.

4.1.2. Autenticação

Autenticação é um processo para identificar se a identidade alegada é autenticada, por meio de comparação das credenciais apresentadas pelo cliente com outras já pré-definidas.

4.1.3. Autorização

A autorização ocorre logo após a autenticação e possui a função de distinguir e separar os privilégios atribuídos ao cliente que está tentando realizar a autenticação. Isto significa que ele apenas entregará os privilégios ao usuário do grupo em que o mesmo pertencer.

4.2. Pfsense

O pfSense também possui vários pacotes de software livre de terceiros para estender suas funcionalidades, tais como Snort e Suricata para detecção e prevenção de intrusão, OpenBGPD, Squid com cache e proxy reverso com SquidGuard, antivírus com ClamWin, além de vários outros pacotes de monitoramento e estatísticas.

Ele é um *software* com a licença BSD, ou seja não precisa-se pagar licenças de uso. Além de ser um sistema gratuito, seus pacotes adicionais permite que ele seja considerado um UTM (*Unified Threat Management* ou Central Unificada de Gerenciamento de Ameaças), já que pode-se realizar com o pfSense muitas das atividades que esperamos de sistemas com esta funcionalidade. Ele também possui relatórios em gráficos RRD, que mostra o estado atual do *firewall* e o consumo de CPU, onde também a modelagem de tráfego e filtragem e usa informações em tempo real. Todos os recursos disponíveis são gerenciados exclusivamente por uma interface *Web* de fácil interpretação. [MAFIOLETTI 2012]

4.2.1. Portal Captive

O *Portal Captive* ou Portal de Captura é uma aplicação responsável por controlar e gerenciar o ingresso de usuários em redes públicas e privadas de forma automatizada. Portais

de captura são comumente utilizados em redes com acesso aberto, disponibilizadas em lojas, shoppings, clínicas, aeroportos, supermercados, e também em redes corporativas, para o gerenciamento do acesso de visitantes. Basicamente, o portal de captura permite que os administradores forneçam acesso à Internet mediante repasse de informações, que possibilitem identificação do usuário, tais como nome, e-mail, CPF, ou então através de autenticação por *vouchers* [Aryeh et al. 2016].

5. Cenário de Testes

Nesta seção será abordada a metodologia dos testes realizados, onde será apresentado o cenário de teste escolhido e aplicado para este trabalho e os resultados obtidos com a proposta.

5.1. Topologia Adotada

Conforme apresentado na Figura 3, a topologia escolhida concentra tudo no *Active Directory* do Samba, na plataforma Linux, e foi vinculado a ele o *Pfsense* para controle de uso dos dispositivos móveis que não fazem parte da rede, direcionando a um portal de captura específico. Com isto, obtendo uma rede heterogênea.

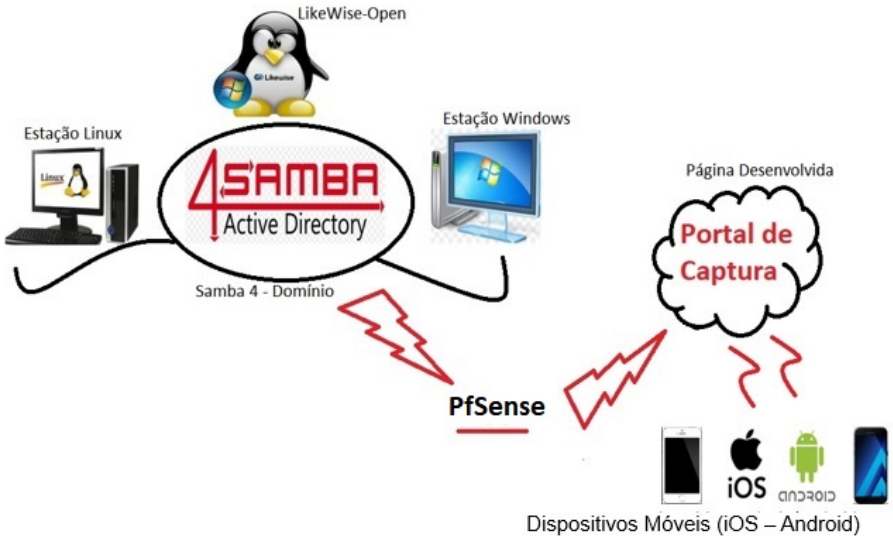

Figura 3. Topologia da Rede

5.2. Implementação do Cenário

Os resultados apresentados durante a realização deste estudo garantem que é possível implantar este tipo de autenticação baseada em Linux, utilizando um *Active Directory* com o protocolo LDAPT de autenticação como local de registros.

O *Active Directory* foi configurado com um usuário padrão, podendo expandir para quantos necessários. Os clientes heterogêneos realizam a autenticação no centralizador, juntamente com os dispositivos móveis.

Conforme Figura 4, o portal de captura foi desenvolvido para quando quaisquer clientes (LAN ou WLAN) quiserem logar na rede, este redirecionará os mesmos para a página do portal de captura, onde farão o login e assim, terão acesso a navegação.

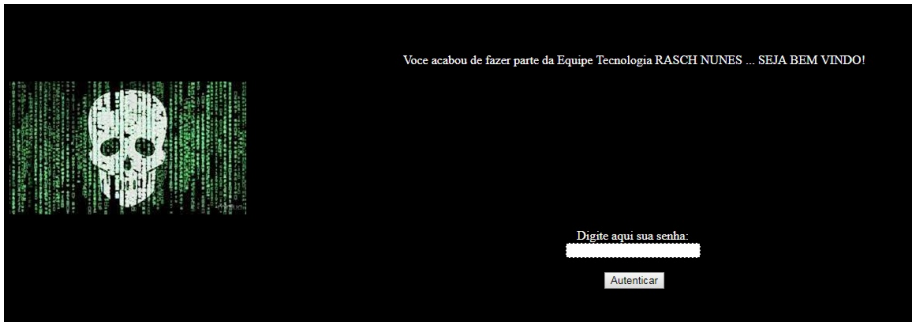

Figura 4. Portal de Captura

Outras vantagens podem ser observadas através do estudo destes protocolos, entre elas pode-se citar: a possibilidade de criação de redes wireless com maior facilidade podendo implementar uma VLAN (*Virtual Local Área Network*) dinâmica. Permite também com que cada usuário tenha acessos e restrições distintas na rede, aumentando a segurança. Além de realizar uma melhor utilização das faixas de IP disponíveis na rede.

A Figura 5 exibi a tela da estação cliente Windows 7 após ter sido autenticado com uma conta Linux criada no OpenLDAP e as diversas opções de configurações do software pGina.

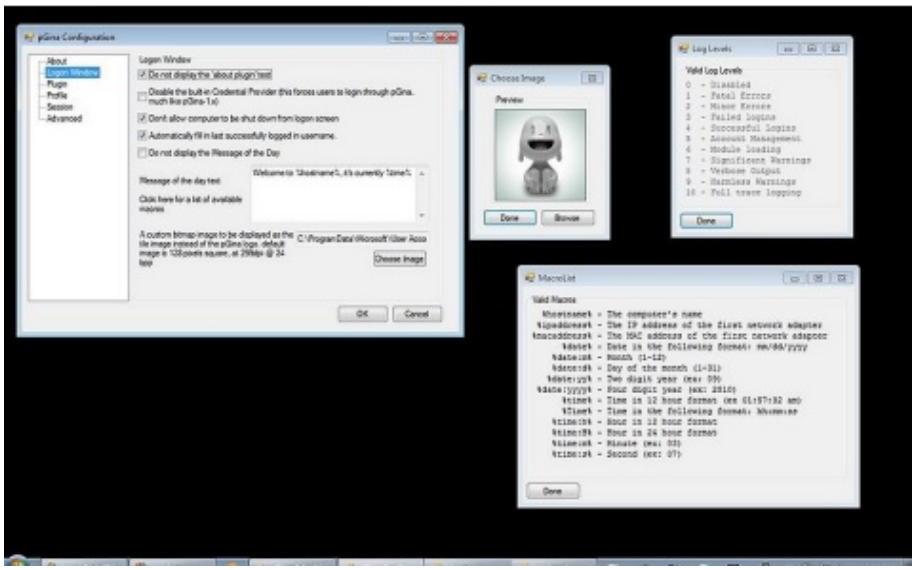

Figura 5. Estação cliente Windows autenticada no OpenLDAP

6. Conclusões

A implementação de um ambiente de rede heterogêneo com as plataformas Windows e Linux para a autenticação centralizada demonstrou-se extremamente viável e benéfica. Como primeiro resultado, a geração de uma documentação onde diretrizes e ressalvas estão documentadas como forma de orientar futuros administradores de rede que necessitem implementar um ambiente misto e precisem de informações para alcançar tais objetivos.

A autenticação centralizada entre as estações clientes (Windows e Linux) foi realizada com sucesso, e com isso obtiveram-se novas potencialidades que podem ser exploradas como a centralização da autenticação das estações de trabalho independente do sistema operacional cliente adotado, Linux ou Windows. Isso gera uma série de benefícios como:

• Segundo [de Menezes et al. 2013] a redução no número de senhas para gerenciar e administrar. Pesquisas indicam que 35% das chamadas ao *helpdesk* são para resetar senhas, aumentando os custos da organização de TI na medida em que o número de repositórios de usuários cresce. Uma grande organização tem mais de vinte repositórios de usuários, resultando numa média de mais de cinco pares de logins e senhas por usuário final caso as integrações não estejam configuradas;

• Possibilidade de um ponto único de manipulação dos objetos que servem a diversos sistemas, plataformas ou ambientes. Esse ponto central pode ser tanto um servidor Windows com o serviço de diretório do *Active Directory*, ou um servidor Linux com o OpenLDAP.

• Ambientes integrados requerem um número menor de servidores, diminuindo por consequência a necessidade de aquisição de novas licenças, realização de configurações e manutenção;

• A integração proposta mantém na rede da empresa a solução do serviço de diretório do *Active Directory*, que já foi um investimento absorvido pela empresa, visto que o serviço de diretório da Microsoft é o líder de instalações no mercado. A solução configurada mantém esse legado da empresa;

• A integração permite ao administrador a flexibilidade do uso de qualquer plataforma tanto para servidores quanto para estações de trabalho, aumentando assim as soluções possíveis de serem instaladas na empresa, dando maior flexibilidade ao ambiente.

O desenvolvimento deste trabalho e as pesquisas na área de interoperabilidade demonstram que a opção por soluções em plataforma livre gera um custo menor devido a não aquisições de licenças, que pode chegar a zero, todavia, temos um custo de mão de obra na instalação e configuração desse sistema, uma vez que há uma escassez maior de profissionais especialistas. Já para a plataforma proprietária pode-se considerar o inverso.

Com isso, concluído o objetivo deste trabalho gera-se uma gama maior de opções, onde possíveis soluções de problemas na área de gerenciamento de identidades podem agora ser analisadas com uma visão maior levando em conta ambas as plataformas, Windows e Linux.

Referências

Aryeh, F. L., Asante, M., and Danso, A. (2016). Securing wireless network using pfsense captive portal with radius authentication–a case study at umat. *Ghana Journal of Technology*, 1(1):40–45.

Barreto, L., Siqueira, F., da Silva Fraga, J., and Feitosa, E. (2013). Gerenciamento de identidades tolerante a intrusões. *Anais do XXXI SBRC*.

Castro, J. P. L. d. (2017). Integração do samba 4 na plataforma ipbrick para criar um active directory open source.

Coulouris, G., Dollimore, J., Kindberg, T., and Blair, G. (2013). *Sistemas Distribuídos-: Conceitos e Projeto*. Bookman Editora.

de Menezes, J. V., da Rocha Fernandes, A. M., de Miranda, E. M., and Moreira, B. G. (2013). Sistema de help desk utilizando raciocínio baseado em casos. *Anais SULCOMP*, 2.

FGV (2016). Fundação getúlio vargas–fgv. *Mestre em Sociologia, Universidade*.

Figueiredo, C. U. d. C., Grande, P., and Verde, S. C. (2016). Integração dos sistemas operativos windows e linux.

JUNIOR, C. H. F. G. (2009). Gerenciamento de identidade.

MAFIOLETTI, R. (2012). Uso do pfsense para o controle de acesso em uma rede local. *REPOSITÓRIO DE RELATÓRIOS-Sistemas de Informação*, 1(2).

MINASI, M. (2008). Dominando o windows server 2008: A bíblia. 1ª edição. *São Paulo-SP*.

Praia (2006). Integração dos sistemas operativos windows e linux.

Quirino (2013). Autenticação distribuída de sistemas híbridos e serviços de rede baseada em serviço de diretórios. *Projeto Final de Graduação em Engenharia de Redes de Comunicação-publicação unb. labredes. pfg*, 20.

Radeck, F. (2012). Configuração de políticas de segurança no windows server 2008: Active directory.

Rosa, A. (2008). Windows server 2008, curso completo.

Santos, M. d. (2013). Uso de ldap implementado em software livre para integrar a autenticação dos controladores de domínio ms-active directory e samba/linux. B.S. thesis, Universidade Tecnológica Federal do Paraná.

SENA (2014). Ldap (lightweight directory access protocol) um guia prático. *Editora Ciência Moderna*.

Souza, J. R. d. (2015). Autenticação cruzada em ambientes heterogêneos (windows x linux).

Whitmore, A., Agarwal, A., and Da Xu, L. (2015). The internet of things—a survey of topics and trends. *Information Systems Frontiers*, 17(2):261–274.

Zeilenga, K. (2012). Lightweight directory access protocol (ldap): Technical specification road map.