Uso do Packetfence como solução de *captive portal* para a "UFRGS Sem Fio"

Liliane Lewis Xerxenevsky, Rui de Quadros Ribeiro

Universidade Federal do Rio Grande do Sul
Centro de Processamento de Dados
Rua Ramiro Barcelos, 2574 – Portão K – Porto Alegre – RS

{liliane,rui}@cpd.ufrgs.br

Resumo. *Ao longo dos últimos anos temos presenciando o crescimento vertiginoso do número de dispositivos capazes de acessar redes sem fio. Uma lista não extensiva pode ser formada por smartphones, tabletes, notebooks e leitores de livros digitais. O avanço da Internet das Coisas (IoT) deverá contribuir ainda mais para o aumento desta lista. Se por um lado esta variedade de dispositivos coopera para a mobilidade e interatividade dos usuários, por outro, representa um grande desafio aos administradores de infraestrutura de rede. Neste artigo é abordado um resumo histórico sobre o uso de redes sem fio e as dificuldades encontradas pela UFRGS; uma análise sobre as soluções existentes de captive portal e a opção da Universidade pelo uso da ferramenta Packetfence; detalhes sobre a modelagem e metodologia de instalação que foram utilizadas; e por fim uma análise crítica sobre este primeiro ano de experiência com o Packetfence seguida de alguns desafios que nortearão os próximos passos da equipe.*

1. Introdução

O Centro de Processamento de Dados da Universidade Federal do Rio Grande do Sul (CPD UFRGS) possui em seu Catálogo de Serviços de Tecnologia da Informação três alternativas para conectividade sem fio, são elas: "UFRGS Sem Fio", "Eduroam" e "Unidade Sem Fio".

A rede "UFRGS Sem Fio" foi o primeiro serviço oficial de rede sem fio da Universidade. Possui finalidade acadêmica e tem seu funcionamento baseado em *captive portal*. Em uma solução do tipo *captive portal* as requisições *web* são inicialmente interceptadas e redirecionadas para uma página onde o usuário deve se autenticar. Em razão da sua simplicidade de uso - basta se conectar à rede e posteriormente se identificar através de uma página *web* - costuma ser a opção mais utilizada pela comunidade.

A rede "Eduroam"[1] também possui finalidade similar à "UFRGS Sem Fio" e é uma iniciativa internacional para disponibilizar Internet segura à comunidade acadêmica. Tal rede utiliza 802.1X e uma vez que tenha sido configurada em um dispositivo, é possível obter acesso através de qualquer um das centenas de pontos presentes em mais de 70 países.

Por fim, a "Unidade Sem Fio" possui finalidade administrativa e proporciona acesso seguro e com permissões equivalentes a um dispositivo que está conectado a rede cabeada, ou seja, acesso aos sistemas da Universidade, impressoras, servidor de arquivos, etc.

O aumento do número de dispositivos móveis - em especial *smartphones* e *tablets* - tem esgotado a capacidade da infraestrutura de rede sem fio em diversos locais da

[1] https://www.eduroam.org/

Universidade. O maior impacto é observado na rede "UFRGS Sem Fio". Tal situação pode ser justificada pelo fato da "UFRGS Sem Fio" possuir a maior capilaridade dentre as redes presentes nos *campi* da Universidade. Outro aspecto a ser considerado é a sua configuração simplificada.

O presente trabalho apresenta um relato sobre o uso do software Packetfence como alternativa viável de *captive portal* na rede "UFRGS Sem fio". A Seção 2 apresenta um histórico sobre o uso de redes sem fio e dificuldades encontradas. A Seção 3 trata sobre a análise das soluções existentes de *captive portal* e a opção da UFRGS pelo Packetfence. Na Seção 4 são abordadas características pertinentes à modelagem da solução bem como metodologia de instalação. Por fim, na Seção 5 são discorridos alguns desafios que devem ser tratados pela equipe que administra o serviço.

2. O uso da rede sem fio na UFRGS

Desde o ano de 2007 a CPD da UFRGS possui oficialmente um serviço de conectividade sem fio [Tonin et al 2008]. O serviço foi concebido como uma resposta ao crescente número de pontos de acesso que eram instalados de forma indiscriminada na rede da Universidade. Tais pontos de acesso promoviam a exposição da rede administrativa da Universidade à inúmeras vulnerabilidades. Outro aspecto relevante era a falta de um mecanismo de identificação dos usuário que utilizavam a rede sem fio.

A modelagem inicial do serviço era composta por: CoovaChilli como ferramenta de *captive portal;* o SNORT para detecção de intrusão; LDAP e PostgreSQL como bases de autenticação e RADIUS para contabilização de acesso. Este arranjo de softwares foi utilizado até meados de 2014 sendo que a carga era dividida em dois servidores.

Com o passar do tempo foram encontradas dificuldades em relação a atualização do CoovaChilli e alguns *bugs* inviabilizaram continuidade da utilização de tal ferramenta. Tais *bugs* comprometiam a estabilidade dos servidores de forma que muitos usuários apresentavam problemas de conectividade. O problema tornava-se mais evidente quando era alcançado o número de 1000 dispositivos por servidor. Outro fator crítico foi a constatação da grande tendência de crescimento do número de dispositivos conforme pode ser observado na Figura 1. Como a solução era seguimentada em apenas dois servidores, o volume de *broadcast* afetava a desempenho da rede.

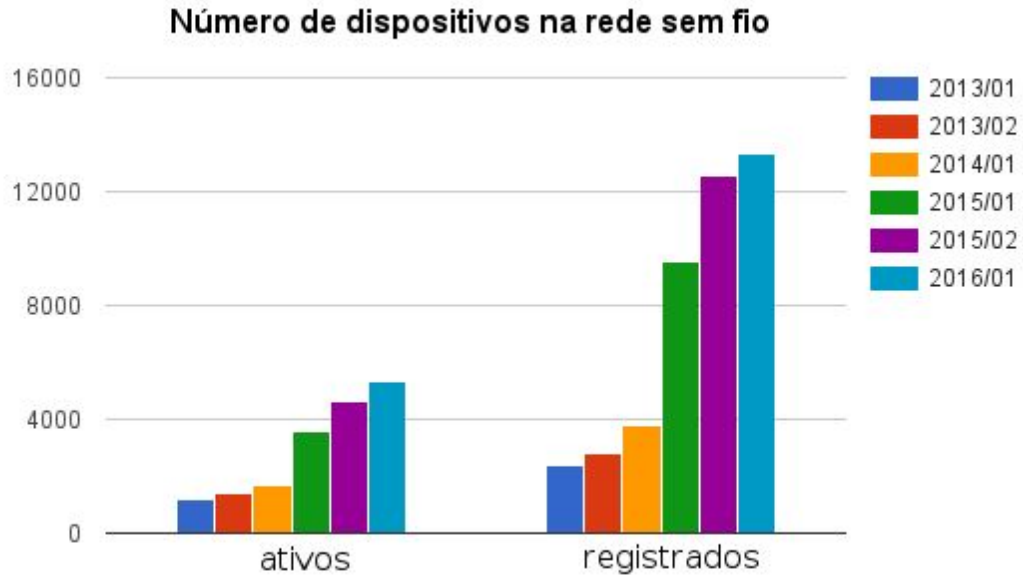

Figura 1. Evolução do número de dispositivos na "UFRGS Sem Fio"[2]

3. Escolha da ferramenta de *captive portal*

Diante das dificuldades encontradas com o antigo sistema de *captive portal* era notória a necessidade de se buscar uma nova alternativa para continuidade do serviço. Assumiu-se os seguintes requisitos como fundamentais a nova ferramenta:

- Possibilidade de integração com os sistemas já existentes;
- Suporte a escalabilidade garantido o crescimento da rede;
- Estabilidade;

3.1. Possíveis soluções

Como alternativas de *captive portal* foram consideradas três possibilidades: controladora Motorola; pfSense e Packefence.

Desde 2011 a UFRGS adota a Motorola (atualmente Zebra[3]) como solução oficial de *hardware* para rede sem fio. Desta forma, a utilização do sistema de *captive portal* nativo da controladora é uma alternativa natural. Porém, durante o processo de análise, foi identificado que é utilizado o *software* Wing 5. Tal *software* é fechado e impõe restrições que inviabilizariam a integração com o sistema de segurança da UFRGS.

A segunda alternativa foi o pfSense[4] que é um *software* livre, baseado no sistema operacional FreeBSD, e que apresenta diversas funcionalidades como por exemplo *firewall*,

[2]O gráfico não apresenta os dados do segundo semestre de 2014 em razão de que em tal período ocorreu a substituição da controladora de rede sem fio e a precisão dos dados ficou comprometida. Este também foi o período de migração entre as soluções de *captive portal*.

[3] https://portal.motorolasolutions.com/Support/US-EN/Wireless+Networks/Wireless+LAN/Unified+Access+Platforms/RFS7000_US-EN

[4] https://www.pfsense.org/

roteador, VPN, *captive portal*, entre outros. Na ocasião, a forma recomendada de instalação era através de um *virtual appliance* o que contribui para facilitar o processo de instalação. Porém, devido a limitações quanto a integração do FreeBSD com o XenServer, que é a plataforma de virtualização utilizada pelo CPD da UFRGS, não foi possível utilizar o pfSense.

A terceira alternativa foi o Packetfence[5] que é um *software* livre de controle de acesso ao meio (NAC). O Packetfence foi a escolha do CPD da UFRGS e será detalhado na sub-seção a seguir.

3.2. PacketFence

O Packetfence é uma solução completa para gerenciamento de acesso que possui um série de funcionalidades integradas como *captive portal*, gerenciamento centralizado de rede cabeada e sem fio, análise e tratamento de incidentes de segurança, suporte a 802.1X , entre outros.

Tais funcionalidades são disponibilizadas como módulos podem ser habilitados de acordo com os requisitos de implantação. Por exemplo, para o cenário da "UFRGS Sem Fio" era desejado utilizar o *captive portal* já as funcionalidades de segurança como *sniffer* de rede (Snort); IDS (suricata) e autenticação RADIUS não eram necessárias, pois a UFRGS já possui estas funcionalidades implementadas.

A instalação do Packetfence pode ser feita pelo gerenciador de pacotes do sistema operacional (*e.g.:* apt, yum, etc.) Após o procedimento de instalação, a configuração do sistema é realizada através de uma interface *web*. Embora a interface *web* apresente uma grande variedade de parâmetros para configuração, é possível realizar configurações mais avançadas diretamente nos arquivos de configuração. Além de tratar o aspecto de configuração, a interface *web* apresenta uma série de relatórios que contribuem para o gerenciamento do serviço. A Figura 2 apresenta um relatório com os sistemas operacionais presentes no dispositivos que se conectaram a rede sem fio.

[5] http://packetfence.org/

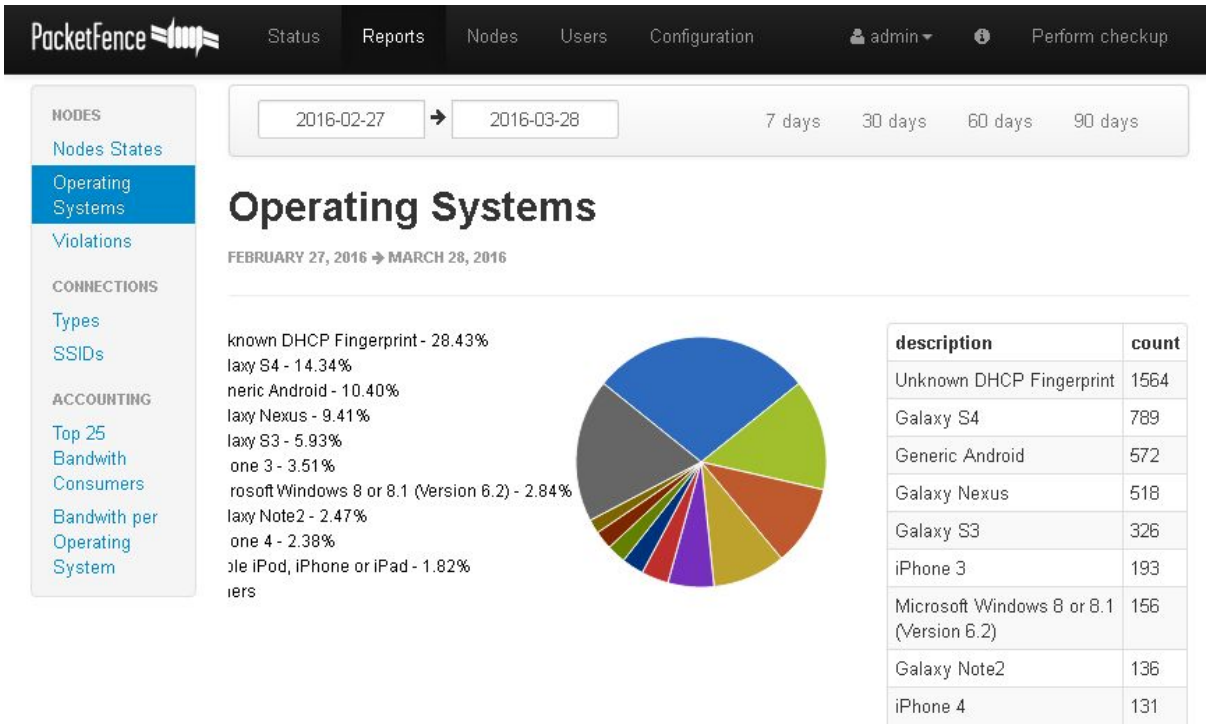

Figura 2. Interface de relatórios

4. O novo serviço “UFRGS Sem Fio”

Em complementação a escolha da nova ferramenta de *captive portal* percebeu-se que era necessário a elaboração de uma nova topologia de rede bem como uma nova metodologia de instalação de servidores. A nova topologia de rede tem por objetivo atender demandas de ordem técnica uma vez que busca resolver problemas presentes na solução anterior (e.g.: *broadcast*, escalabilidade, etc.). Já a nova metodologia de instalação de servidores visa facilitar a transferência de conhecimento entre os membros da equipe. Tal aspecto é muito relevante uma vez que o conhecimento relativo aos serviços da Universidade não deve depender da permanência dos funcionários.

4.1. Modelagem do serviço

Para garantir a escalabilidade e qualidade do serviço aos usuários, optou-se por seguimentar a rede em seis VLANs. Esta seguimentação permite limitar o volume de *broadcast* na rede que, conforme já mencionado na Seção 3, tem influência no desempenho. Cada VLAN é atendida por um servidor com Packetfence e representa um conjunto de unidades acadêmicas, em geral, um campi. A topologia corrente pode ser vista na Figura 3. A figura apresenta ainda a integração com os sistemas de monitoramento e segurança da UFRGS.

Um elemento fundamental nesta arquitetura é o “supergateway” que é o servidor responsável por concentrar o tráfego das redes sem fio e fazer a tradução de endereços (NAT). Antes desta versão do serviço, a rede sem fio utilizava IPs válidos. Com o aumento do número de dispositivos e concomitante esgotamento de endereços válidos IPv4, esta estratégia de mostrou inviável sendo necessário a utilização de NAT para suprir a quantidades de IPs requeridos.

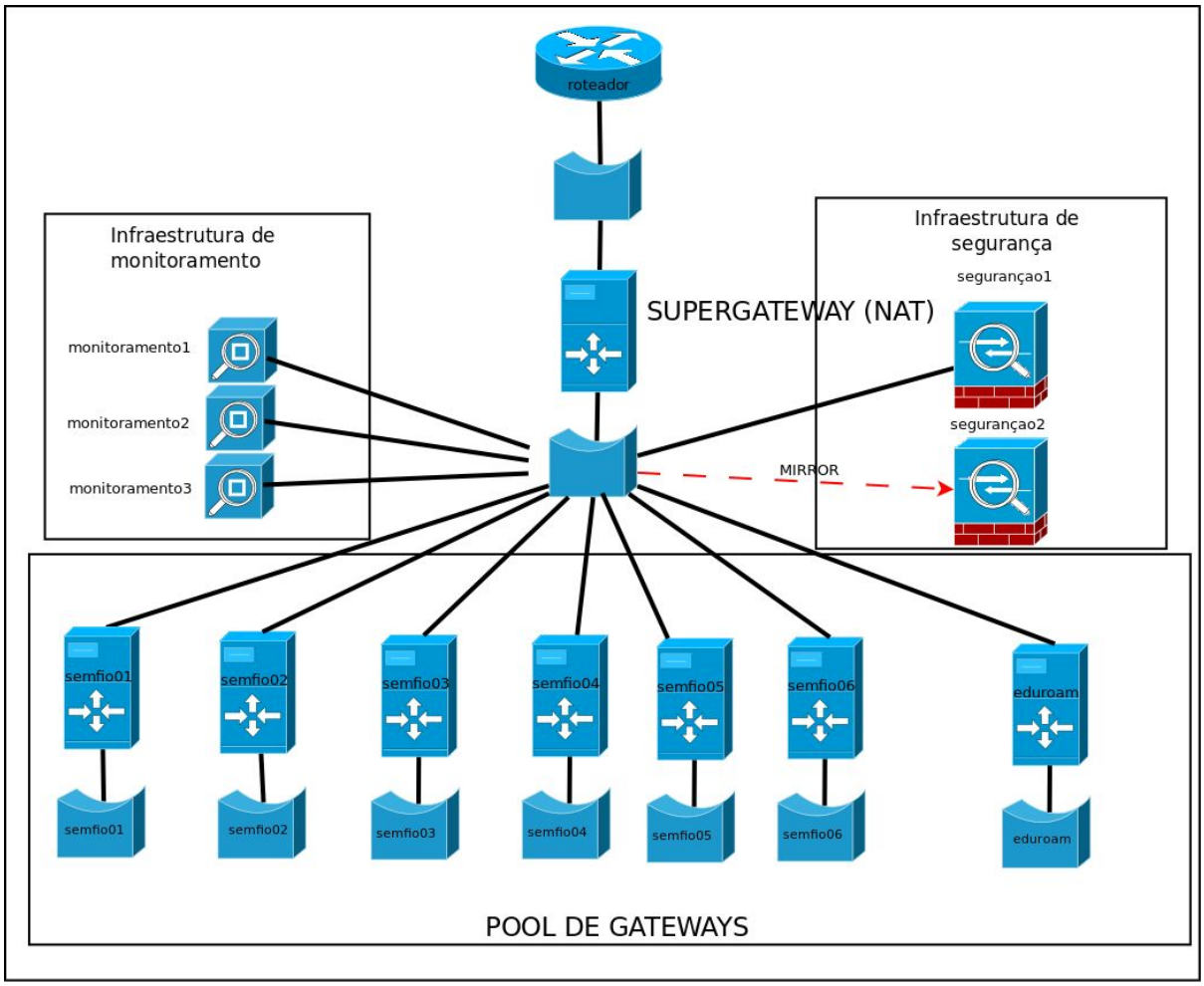

Figura 3. Topologia da rede sem fio

4.2. Metodologia de instalação

Seguindo um direcionamento adotado para outros serviços da Universidade, optou-se por utilizar o *software* de gerenciamento de configuração Ansible[6]. Através de tal software define-se um *playbook* que contêm uma sequência de passos (*e.g.:* instalar pacotes, copiar arquivos, alterar permissões, etc.) que devem ser executados para se completar uma determinada tarefa (*e.g.:* instalar um servidor de *captive portal*). O uso do Ansible foi combinado com a ferramenta de versionamento SVN. Tal combinação possibilitou um melhor fluxo de trabalho entre os membros da equipe.

Ao analisarmos a metodologia de instalação adotada é possível constatar que ocorreram melhorias no que diz respeito a documentação e agilidade do processo de instalação. Uma vez que a instalação esteja descrita na forma de um *playbook*, indiretamente ela estará documentada sendo possível repeti-la infinitas vezes com baixo custo operacional e minimizando a possibilidade de erros humanos.

Um desafio inerente ao planejamento de uma instalação automatizada é identificar quais passos realmente devem ser automatizados. Por exemplo: após a instalação do Packetfence é necessário executar um configurador via interface *web*. As alterações feitas por este configurador poderiam ser mapeadas e replicadas no *playbook*. Porém, observou-se que,

[6] https://www.ansible.com/

a cada *release* do Packetfence, este configurador sofre alterações de forma que caso optássemos por mapeá-las, este trabalho deveria ser refeito a cada nova *release*. Dessa forma foi escolhido automatizar: a instalação básica do servidor; a manipulação dos arquivos relativos ao sistema de segurança da UFRGS; e a interface *web* do *captive portal* que foi desenvolvida pela equipe do Departamento de Soluções de Software do CPD UFRGS.

5. Conclusão e desafios para evolução do serviço

Ao longo deste primeiro ano de utilização do Packetfence como ferramenta de *captive portal* na Universidade foi possível observar que as requisitos inicialmente assumidos foram atingidos. Desta forma o Packetfence mostra-se uma alternativa viável ao cenário imposto pela comunidade da UFRGS.

Como desdobramento natural desta experiência foram identificados alguns desafios que devem ser superados pela equipe de administração do serviço.

O primeiro desafio é a implementação do IPv6. Tal objetivo não foi alcançado ainda por duas rações: um *bug* apresentado na controladora da rede sem fio onde o tráfego de IPv6 causava o travamento do sistema; já o segundo motivo é a falta de suporte à IPv6 pelo Packetfence.

O segundo desafio é a possibilidade de *login* de usuários sem vínculo com a Universiadade. Já existe o *login* através de *tickets* temporários, mas cogita-se aprimorar tal técnica através do uso de algum meio de indentificação do usuário, como associação com conta de redes sociais. O Packetfence já possui tal funcionalidade e a ativação deste recurso é importante principalmente para eventos aberto ao público, como formaturas.

Por fim, o último desafio diz respeito a um melhor aproveitamento das funcionalidades de segurança do Packetfence de forma integrada a infraestrutura de segurança já existente na Universidade.

Referências

Tonin, R., Machado, C., Postal, E., Rey, L., & Ziulkoski, L. (2008). Sistema de Gerenciamento de Redes Wireless da UFRGS. In II Workshop de Tecnologia da Informaçao das IFES.