Sistema de Gerenciamento de Redes *Wireless* na UFRGS

Rafael Tonin, Caciano Machado, Eduardo Postal, Leandro Rey, Luís Ziulkoski

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

{rtonin, caciano, leandro, luis}@cpd.ufrgs.br
edupostal@inf.ufrgs.br

Resumo. *As redes wireless são uma realidade na vida dos usuários de recursos de tecnologia da informação. Com a queda nos custos dos equipamentos os próprios usuários vêm implantando suas redes, desconsiderando as melhores práticas recomendadas para o uso desta tecnologia. O sistema de gerenciamento implementado pela UFRGS visa disponibilizar uma estrutura capaz de prover os mecanismos necessários para utilização segura de redes wireless. Através do sistema é possível habilitar o uso de criptografia dos canais de comunicação, bem como autorizar o uso da rede baseado em credenciais. Uma vez constituído, o sistema minimizará a possibilidade de exposição de dados confidenciais, permitindo o controle de utilização e o gerenciamento centralizado de toda a estrutura.*

1. Introdução

Impulsionados pela necessidade de mobilidade e facilidade de uso, os usuários da rede da UFRGS tem instalado pontos de acesso *wireless* de forma disseminada, não controlada e principalmente insegura. Estas instalações, na maioria das vezes, não são comunicadas à equipe de suporte a redes e expõe perigosamente a rede a toda a sorte de ataques e usos indevidos.

Baseado nesta necessidade, o Centro de Processamento de Dados da UFRGS realizou o estudo e a implantação de uma infra-estrutura de controle e supervisão de redes *wireless* que disponibiliza à comunidade acadêmica os benefícios de autenticação centralizada e uso de criptografia, sem abdicar da facilidade de utilização.

Neste trabalho, apresentaremos o projeto Gerenciamento de Redes *Wireless* na UFRGS que especifica os estudos necessários, ferramentas utilizadas, bem como a forma com que foram instalados os serviços que compõem a solução. Este projeto utiliza de forma extensiva, ferramentas de software livre para a implantação de todos os serviços necessários.

A seguir, apresentaremos os problemas que motivaram o estudo e a execução do projeto Gerenciamento de Redes *Wireless* na UFRGS. Em seguida serão apresentadas as soluções comerciais que possibilitam o controle centralizado de redes *wireless*. Seguiremos apresentando a solução adotada pela UFRGS. Por fim, apresentaremos a solução completa, com detalhes sobre a implementação, problemas enfrentados e considerações finais a respeito do sistema.

2. Motivação

A rede da UFRGS vem recebendo a cada dia a instalação de novos *Access Points* e roteadores *wireless*. O uso indiscriminado de tais equipamentos ocasiona a perda total de controle e de supervisão da rede bem como expõe de forma desnecessária a infra-estrutura de rede aos mais diversos vetores de ataque possíveis. Dentre estes, podemos destacar a proliferação de vírus e o uso de softwares P2P por conta de usuários desconhecidos e conseqüente perda de capacidade, por parte da equipe de segurança, de identificar tais usuários. Muitas vezes os próprios usuários de redes *wireless* desconhecem os riscos aos quais estão expostos ao usar as redes sem criptografia, utilizando tais redes para trafegar dados confidenciais de forma insegura.

O uso de roteadores *wireless* com NAT piora ainda mais o problema, pois mascara o uso da rede, apresentando aos serviços de supervisão da rede apenas o IP do roteador quando na realidade diversas estações se utilizam deste IP para acessar a rede. Quando uma destas estações encontra-se infectada ou apresenta tráfego suspeito ou indevido, torna-se impossível descobrir, de forma imediata, o causador do problema.

Outro fator determinante para a criação deste projeto é a necessidade de configuração individual dos mecanismos de proteção dos *Access Points*, em todas as situações em que se deseja configurar ao menos uma forma básica de segurança. O gerenciamento de chaves compartilhadas para o uso de WPA-PSK torna-se inviável e não escalável para soluções com grande densidade de pontos de acesso.

As seguintes demandas foram definidas para este projeto: necessidade de criação de uma infra-estrutura de autenticação que possuísse a capacidade de se integrar com o serviço de diretórios da Universidade, prover um mecanismo que possibilitasse o acesso de usuários visitantes de forma facilitada, porém, com certo nível de controle e por fim, que o sistema possuísse a capacidade de habilitar, de forma eventual, o uso da rede *wireless* para eventos, utilizando para isto tickets com validade pré-determinada.

3. Soluções Comerciais

O uso de soluções comerciais de gerenciamento de redes *wireless* facilmente resolveria todos os problemas descritos acima, facilitando inclusive a distribuição de *Access Points* para todos os Campi. Soluções ofertadas por fabricantes como Extreme, Enterasys, Cisco e 3Com utilizam o conceito de ‘Controlador *Wireless*’ onde um equipamento central controla os *Access Points*. Estes *Access Points* não possuem quase nenhuma inteligência, contendo apenas o transmissor/receptor de RF e um software que faz VPN para o controlador central. O controlador por sua vez faz todo o papel de supervisão de intensidades de sinal, atribuição de SSIDs, Autenticação, Autorização e Contabilização de usuários.

Todavia, o uso de soluções proprietárias, não permite a integração de nenhum outro tipo de *Access Point*. Os chamados ‘Controladores *Wireless*’ somente funcionam com *Access Points* do mesmo fabricante, levando a um aprisionamento tecnológico indesejável para uma instituição pública. Mas provavelmente o mais relevante de todos os problemas seja realmente o custo de tal solução, uma vez que a distribuição de algumas centenas de *Access Points* faz com que os custos cheguem a casa das dezenas de milhares de dólares.

4. Solução UFRGS

Uma vez concluído que a adoção de soluções comerciais seria completamente inviável para a Universidade, partimos para o estudo de soluções baseadas em software livre.

Existem duas formas de acesso possíveis no sistema. A primeira forma permite o acesso de usuários *wireless* à rede de dados da UFRGS de forma transparente e integrada, permitindo o acesso e o compartilhamento de arquivos, impressoras, etc. A segunda forma provê o acesso através de uma rede paralela, destinada aos usuários visitantes e que não tem necessidade de uma maior integração com a rede da UFRGS.

O sistema mostrado na figura 1 utiliza ferramentas dos projetos FreeRADIUS, OpenLDAP, PostgreSQL, Apache, SNORT e CoovaChilli[1]. Também está sendo utilizada a linguagem Perl para efetuar alguns testes customizados necessários para o enquadramento adequado de usuários em seus perfis.

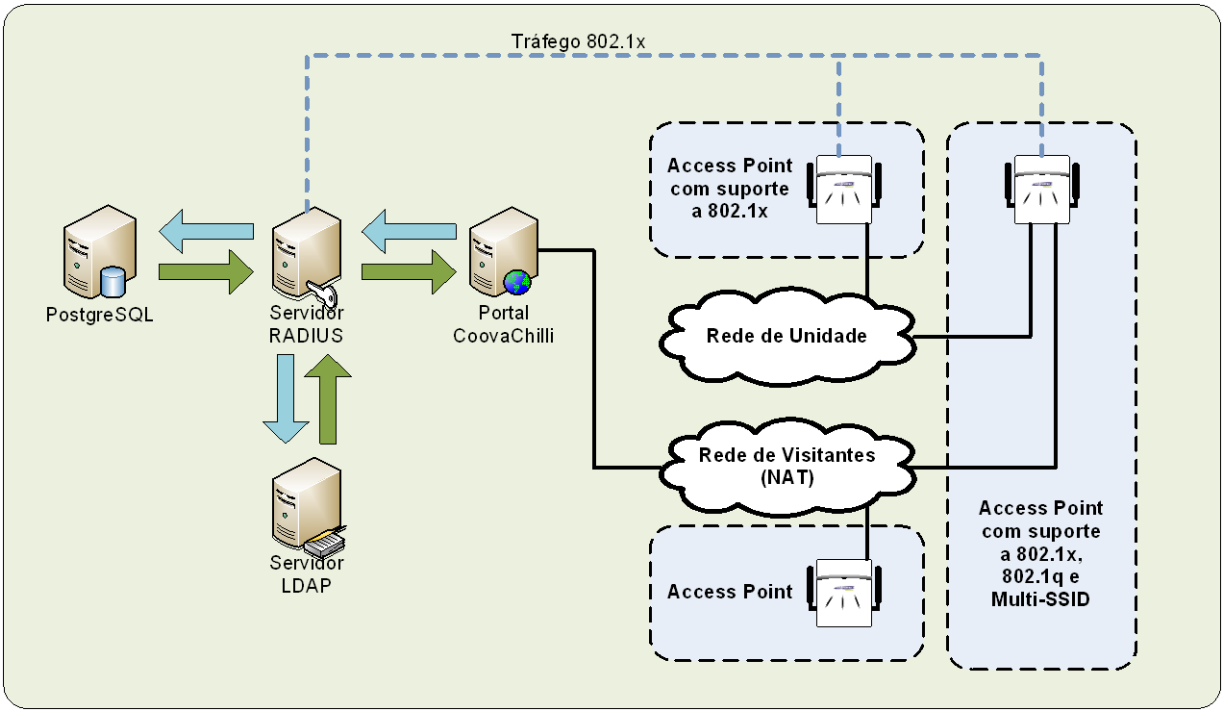

Fig1 – Estrutura de Gerenciamento *Wireless* da UFRGS

4.1. Rede de Unidade

Esta modalidade de rede *wireless* integra as estações na rede local de cada Unidade da UFRGS, tornando-a equivalente a um computador, com número IP válido, conectado na rede cabeada. O controle é efetuado por um servidor RADIUS que é utilizado na autenticação, autorização e contabilização de usuários. Optou-se por usar neste caso a autenticação através de PEAP[2] por permitir uma maior compatibilidade com os diversos clientes existentes e sem a necessidade de utilização de certificados digitais no lado do cliente. O servidor está integrado com o serviço de diretórios da Universidade, permitindo, portanto, a utilização dos números de identificação de alunos, professores e funcionários. Visando permitir um controle granular de quem pode ou não acessar a rede, foi criado um script integrado ao RADIUS que efetua a verificação de que um determinado número de identificação possui permissão de acesso para um determinado SSID. Estas informações são guardadas em um banco de dados que se encontra integrado ao portal de serviços da UFRGS. A configuração dos *Access Points* nesta estrutura é feita utilizando-se autenticação WPA/WPA2 Enterprise com IEEE802.1x, possibilitando o maior nível de segurança possível até o momento.

4.2. Rede de Visitantes

Nesta rede cada computador recebe um número IP de uma rede privada, ficando isolado da rede da Unidade onde está instalado o *Access Point*. Esta rede, cuja estrutura de controle é mostrada na figura 2, será a de maior impacto na comunidade universitária, quando de sua disseminação, visto que todas as bases instaladas são compartilhadas, levando o acesso Internet a todos os usuários, em todos os locais, dentro da área de cobertura. A autenticação é feita de forma indireta, através de um mecanismo de portal que intercepta, inicialmente, as requisições web e solicita a identificação de usuário para a utilização da rede. Esta identificação pode ter origem em duas fontes diferentes. O serviço de diretórios da Universidade permite o acesso a usuários com identificação. A segunda fonte é um sistema de tickets baseado em PostgreSQL e PHP, desenvolvido de forma a viabilizar o uso temporário da rede utilizando tickets com validade pré-determinada. O mecanismo de tickets permite viabilizar o acesso a usuários sem vínculo com a Universidade e que não necessitam ou não possuem acesso permanente.

Para criação do portal foi utilizado o CoovaChilli, projeto baseado no mecanismo que inicialmente foi criado pelo projeto Chillispot[3] e que através de um único *daemon* provê os serviços de túnel, DHCP, NAT e as páginas web que compõem o portal. Este modelo de controle foi inicialmente descrito pela equipe do NAS – NASA[4] e descreve em linhas gerais o funcionamento do sistema. A comunicação do CoovaChilli com o serviço de diretórios e com o banco de dados também é realizada através de um servidor RADIUS configurado exclusivamente para este propósito.

Como esta rede utiliza NAT, precisamos instalar um servidor SNORT junto ao serviço CoovaChilli para a detecção e bloqueio de computadores infectados ou com tráfego suspeito. Uma vez que qualquer anomalia seja detectada pelo SNORT, um script efetua o bloqueio, via endereço MAC, do computador em questão.

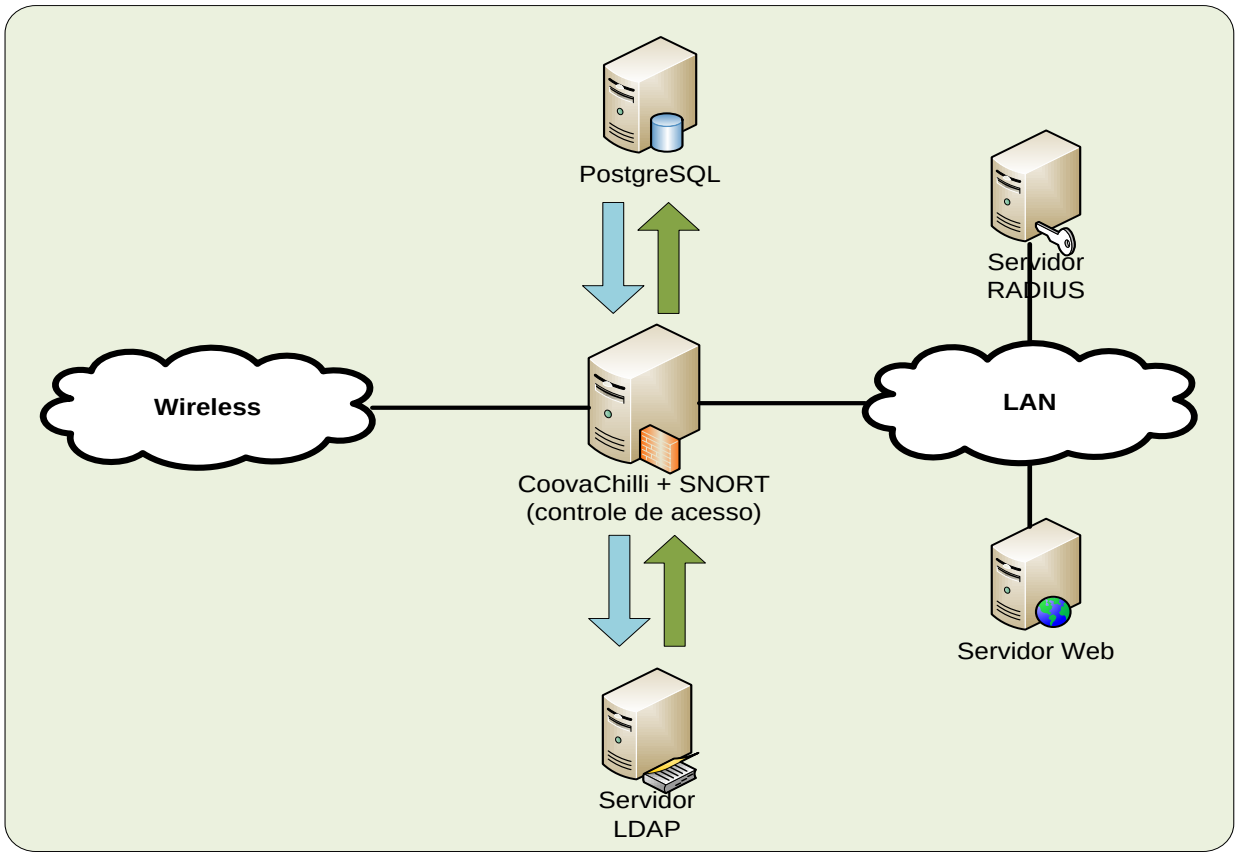

Fig2 – Estrutura de controle CoovaChilli

4.3. *Access Points* recomendados

Para utilização em apenas uma das redes mostradas indica-se aos usuários a aquisição de *Access Points* que tenham suporte a IEEE802.1x. Para otimizar o uso dos recursos e facilitar a integração ao projeto, recomendamos a aquisição de *Access Points* com suporte a IEEE802.1q e Multi-SSID onde apenas um equipamento possui a capacidade de atender as duas categorias de acesso, evitando portanto a duplicidade de equipamentos para atender uma mesma região de cobertura.

5. Problemas Enfrentados

Durante a instalação inicial da estrutura enfrentamos alguns problemas que foram corrigidos através de pequenas alterações no código do CoovaChilli. Dentre eles destacamos a necessidade de alteração da interface de submissão de usuário e senha para que fosse possível o uso de senhas criptografadas utilizadas no serviço de diretórios da UFRGS, implementação de uma interface para obtenção do status do usuário e a capacidade de efetuar a saída do sistema.

6. Conclusão e Considerações Finais

A disseminação de bases *wireless* mal configuradas e que expõem a rede da UFRGS a uma série de riscos de segurança impulsionou de forma decisiva a elaboração deste projeto.

Após a fase inicial de testes, a rede *wireless* para visitantes encontra-se instalada e operacional. Algumas das unidades da UFRGS já demonstraram interesse na sua utilização. Os serviços que dão suporte a infra-estrutura de IEEE802.1x encontram-se em fase final de testes e serão colocados em produção em breve.

Com a implementação deste projeto a administração da rede da UFRGS oferece uma alternativa flexível e segura para o uso de redes *wireless* na Universidade, direcionando as unidades a adotar uma solução aberta, escalável e de custo acessível.

7. Referencias

[1] CoovaChilli - http://coova.org/wiki/index.php/CoovaChilli
[2] Microsoft - http://go.microsoft.com/fwlink/?linkid=23459
[3] Chillispot - http://www.chillispot.info/
[4] NASA - http://www.nas.nasa.gov/Resources/Networks/wireless_paper.html