POLÍTICAS DE SEGURANÇA PARA AS REDES SEM FIO DAS UNIDADES DO CEFETES

Juliana Cristina dos Santos
CEFETES, Unidade Serra e Coordenadoria de Informática – Rod ES 101, Km 6.5, Manguinhos – 29.164-731 – Serra – ES – julianacristina.ti@gmail.com

Resumo: *As unidades do CEFETES necessitam de políticas de segurança que garantam a integridade e confiabilidade das informações transmitidas, a disponibilidade e usabilidade da rede sem fio, e a segurança do legado já existente nas unidades. Além disso, as políticas implementadas nas unidades devem seguir o mesmo padrão, apesar de sofrerem alterações devido às diferenças de infra-estrutura das unidades. Neste documento é descrita a importância da definição de políticas de segurança, e são mostradas as políticas de segurança que foram definidas para serem implementadas nas unidades do CEFETES.*

Palavras-chave: *Segurança em redes sem fio, integridade e confiabilidade da informação, usabilidade e disponibilidade da rede.*

INTRODUÇÃO

Os aspectos de segurança em redes sem fio são de grande importância devido às vulnerabilidades intrínsecas ao processo de comunicação e ao fato de os métodos de segurança desenvolvidos para redes cabeadas não serem adequados para utilização em redes sem fio [KUROSE]. Assim, são necessários métodos específicos de segurança que garantam a integridade e a privacidade da comunicação, bem como a autenticação das entidades envolvidas.

A pesquisa a cerca da segurança de redes sem fio leva em consideração quatro aspectos fundamentais [DUARTE, NETO]: confidencialidade, integridade, disponibilidade e usabilidade.

Estas características devem ser balanceadas para que o sistema não fique tão seguro a ponto de impedir usuários legítimos de utilizá-lo eficientemente, mas também para que não seja inseguro a ponto de permitir a ação de usuários não autorizados [RUFINO].

Devido à complexidade da definição de políticas de segurança para redes sem fio, foi realizado um trabalho de pesquisa para definir políticas de segurança que possam ser aplicadas a todas as unidades do CEFETES.

RESULTADOS E DISCUSSÃO

Com base nas necessidades dos usuários, e com o objetivo de prover segurança tanto para a rede sem fio quanto para o legado existente na unidade, definiu-se a implementação de duas redes sem fio em cada unidade, denominadas neste trabalho de *Guest* e *Corp*.

Os usuários da rede Guest somente terão acesso à Internet, enquanto que os usuários da rede Corp terão acesso tanto à Internet quando aos recursos providos pela rede interna da unidade.

A implementação de duas redes sem fio na unidade é necessária devido aos diferentes tipos de usuários das redes do CEFETES e que, conseqüentemente, devem ter diferentes tipos de acesso aos recursos da rede.

Os usuários da rede sem fio Guest necessitam apenas de uma chave pré-compartilhada WPA para se autenticarem e se associarem na rede. E os usuários da rede Corp fazem uma autenticação IEEE 802.1x com método de autenticação PEAP, em que será necessário ter um usuário cadastrado na base de dados LDAP, e ter permissões para acessar esta rede sem fio.

O elemento da rede que autentica os usuários da Guest é o ponto de acesso sem fio (AP), enquanto os usuários na rede sem fio Corp são autenticados por um servidor Radius.

Tecnicamente falando, cada rede sem fio (Guest e Corp) é na realidade um VAPs (Virtual Acess Point), com SSID (Service Set Identifier) configurado como Guest ou Corp. Dessa forma os pontos de acesso instalados nas unidades proverão acesso tanto para a rede sem fio Guest quanto para a rede Corp. Para prover ainda mais segurança, será configurada uma VLAN (Virtual Local Area Network) para separar o tráfego das redes sem fio Guest e Corp.

Todos os pontos de acesso estarão conectados ao firewall da unidade que fará o controle de acesso da seguinte forma:

- A rede Guest somente acessará a Internet;

- A rede Corp acessará tanto à Internet quanto a rede interna da unidade;
- Não haverá roteamento entre a rede Guest e a rede Corp.

A Figura 1 mostra como é recomendável que seja configurada a topologia da rede da unidade. É necessário que a rede sem fio tenha seu tráfego separado dos demais tráfegos da rede, por isso, ela deve estar conectada a uma interface do firewall para que este faça o controle de acesso das conexões da rede sem fio.

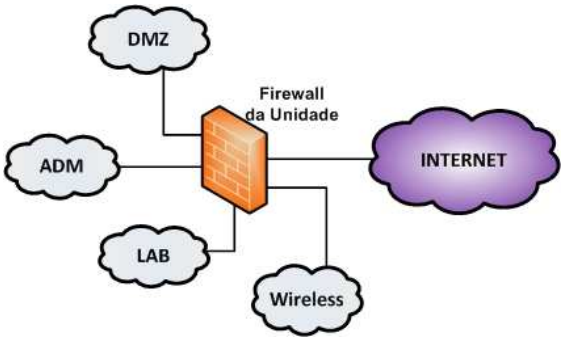

Figura 1 – Topologia recomenda para a unidade.

A Figura 2 detalha o segmento "Wireless" e "DMZ" mostrado na Figura 1. As linhas em cores vermelhas representam link *trunking* entre os dipositivos. Nesses links *trunking* passam o tráfego da rede Corp e da Guest utilizando tags de VLAN.

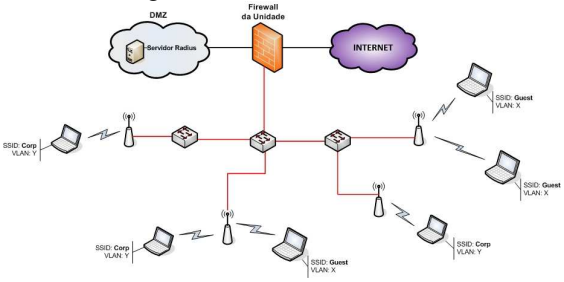

Figura 2 - Detalhamento do segmento "Wireless" e "DMZ".

Estas políticas foram implementadas em um ambiente de testes no CEFETES Vitória e foi comprovada sua segurança desde que as regras de firewall sejam corretamente configuradas e desde que seja escolhida uma chave WPA considerada segura.

Testes demonstraram que a usabilidade e disponibilidade da rede podem ficar comprometidas se estas políticas forem implementadas em APs com baixo desempenho. As políticas definidas não impedem ataques do tipo "*Man in the Middle*" e neste caso, propõe-se a aquisição de um IDS (Sistema Detector de Intrusos).

Mas de forma geral, as políticas definidas neste trabalho atendem satisfatoriamente as necessidades atuais das unidades do CEFETES garantindo um bom nível de segurança.

CONCLUSÃO

As redes sem fio necessitam, para implantação e gerenciamento, de cuidados e políticas de seguranças que devem ser cuidadosamente testadas, a fim de evitar a perda de confiabilidade e integridade das informações [RUFINO].

Após estudos e testes realizados, concluiu-se que as políticas de segurança definidas neste trabalho provêem um nível robusto de segurança que atendem às necessidades das unidades CEFETES. Para garantir a usabilidade, as políticas propostas requerem a aquisição de equipamentos de bom desempenho o que pode representar um alto investimento.

Agradecimentos

Agradeço ao Prof. Msc. Sérgio Nery Simões por ter me orientado neste projeto de pesquisa, por ter me ajudado em minhas dúvidas, avaliado meu desempenho e me cobrado quando necessário. Agradeço também ao Prof. Msc. José Eduado Medonça Xavier, por ter colaborado informalmente como co-orientador, fornecido informações relativas ao CEFETES e provido meios para a implementação dos protótipos e execução dos testes.

REFERÊNCIAS

KUROSE, J. F, Keith W. R. **Rede de Computadores e a Internet**. Editora Pearson, 2004.

DUARTE, L.O. **Análise de Vulnerabilidades e Ataques Inerentes a Rede sem Fio 802.1x**. 2003. Monografia - Universidade Estadual Paulista Júlio de Mesquita Filho, São Paulo.

RUFINO, N. M. O. **Segurança em Redes Sem Fio: Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**. 2 ed. São Paulo: Novatec, 2005.

NETO, R.M. **A Evolução dos Mecanismos de Segurança para Redes sem Fio 802.11.** 2004. Monografia – Faculdade de Engenharia da Computação, Pontifícia Universidade Católica do Rio de Janeiro.