

CONTROLE DE ACESSO A REDES WLAN: PFSense INTEGRADO AO RADIUS E AD PARA AMBIENTES MULTIPLATAFORMA

LUIZ FERNANDO ELIAS MARTINEZ¹, MARCELO HENRIQUE STOPPA¹.

1. LaMOt, Regional Catalão, Universidade Federal de Goiás
Av. Dr. Lamartine Pinto de Avelar, 1120 Catalão/GO
luiz_martinez@ufg.br, mhstoppa@pq.cnpq.br

Recebido em: 28/10/2014 – Aprovado em: 05/11/2014 – Publicado em: 06/11/2014

RESUMO

A crescente utilização de rede sem fio em instituições públicas, bem como em redes empresariais e domésticas imprime uma necessidade de se analisar questões como segurança e controle de acesso, ou seja, determinar quais tecnologias estão disponíveis como apoio a rede sem fio que permitam a integração de equipamentos com diferentes fabricantes e modelos, com garantia de controle de que os usuários só terão acesso aos recursos que lhes couber. O padrão IEEE 802.11 é utilizado nestes cenários. Desenvolvido pelo *Institute of Electrical and Electronics Engineers* especifica redes do tipo WLAN (*Wireless Local Area Network*). Os protocolos de autenticação aliados ao uso das técnicas de criptografia permitem aos servidores de autenticação gerenciarem o acesso dos usuários à rede sem fio uma vez que se não implementados, qualquer dispositivo que estiver dentro da área de cobertura da rede poderá conectar-se a ela. Como servidores de autenticação foram utilizados o RADIUS (*Remote Authentication Dial In User Service*) integrado ao *Active Directory* (AD) da *Microsoft*[®]. O servidor PsSense atua integrado ao RADIUS recebendo e encaminhando as credenciais dos usuários. Foram avaliados diferentes cenários de autenticação em ambientes multiplataforma. Os resultados obtidos foram bastante satisfatórios tanto em relação ao tempo do processo de autenticação quanto à validação deste processo.

PALAVRAS-CHAVE: Autenticação, Controle de Acesso, Segurança, WLAN.

ABSTRACT

The increasing use of wireless networking in public institutions as well as business and home networks prints a need to consider issues such as security and access control, ie determine which technologies are available to support the wireless network that allow the integration equipment with different manufacturers and models, with a guarantee of control that users only have access to resources due to them. The IEEE 802.11 standard is used in these scenarios. Developed by the Institute of Electrical and Electronics Engineers specifies Networks WLAN (*Wireless Local Area Network*). Authentication protocols combined with the use of encryption techniques allow authentication servers to manage users' access to the wireless network since it is not implemented, any device that is within the coverage area of the network can connect

to it. As authentication server was used RADIUS (Remote Authentication Dial In User Service) integrated with Active Directory (AD) of Microsoft ®. The PsSense integrated RADIUS server acts receiving and forwarding user credentials. Different authentication scenarios were evaluated in multiplatform environments. The results were satisfactory both in terms of time of the authentication process and the validation of the process.

KEYWORDS: Autentication, Access Control, Security, WLAN

INTRODUÇÃO

Uma rede de computadores é um conjunto de computadores autônomos interconectados por uma única tecnologia. Desta forma, dois computadores estão interconectados quando podem trocar informações. A conexão pode ser estabelecida utilizando-se diversos meios, como por exemplo, fios de cobre, fibras ópticas ou mesmo, micro-ondas e ondas de infravermelho TANEMBAUM (2011).

Desde a descoberta das ondas de rádio, pesquisas são realizadas nesta área para entender as possibilidades de suas propriedades para a transmissão de dados sem fio, permitindo mobilidade e conexões entre localidades remotas. Segundo GAST e LOUKIDES (2002) a mobilidade é a grande justificativa ao uso das redes sem fio. Porém, como as transmissões ultrapassam barreiras físicas como paredes e móveis, mesmo com o sinal degradado, este pode se propagar além da área desejada ocasionando problemas com a segurança.

Uma rede sem fio (*Wireless*) é tipicamente uma extensão de uma rede local (*Local Area Network* - LAN) convencional com fio, criando-se o conceito de rede local sem fio (*Wireless Local Area Network* - WLAN). Uma WLAN converte pacotes de dados em ondas de rádio ou infravermelho e os envia para outros dispositivos sem fio ou para um ponto de acesso que serve como uma conexão para uma LAN com fio.

O IEEE 802.11, também conhecido como *Wi-Fi* representa um conjunto de padrões de redes locais sem fio que foram desenvolvidos pelo grupo de trabalho 11 do IEEE (*Institute of Electrical and Electronics Engineers*) para redes locais sem fio (WLANs). O propósito destes padrões é desenvolver um controle de acesso à rede pela camada física através do protocolo TCP/IP. São específicos para conexões sem fio com estações de trabalho fixas ou móveis dentro de uma rede local. Estes padrões definem os tipos de protocolos necessários proporcionando uma interoperabilidade entre equipamentos de rede sem fio de diferentes fabricantes. O termo IEEE 802.11x é também usado para representar este conjunto de padrões onde a variação do "x" pode representar, por exemplo, os padrões: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac. (*Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2012). Outros padrões de comunicação sem fio também são estabelecidos pelo IEEE, são eles:

- *Wireless Personal Area Network* (WPAN) - IEEE 802.15: Possui alcance limitado, porém capaz de efetuar a comunicação entre dispositivos pessoais. Tem como principal representante o *Bluetooth* especificado pelo padrão IEEE 802.15.1 (*Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)* , 2012);

- *Wireless Metropolitan Area Network (WMAN) IEEE 802.16*: A rede metropolitana sem fios (WMAN ou *Wireless Metropolitan Area Network*) é estabelecida pelo padrão IEEE 802.16. A especificação mais conhecida para este padrão é o WiMAX (*IEEE Standard for Air Interface for Broadband Wireless Access Systems*, 2012).

Equipamentos que disponibilizam redes sem fio segundo o padrão IEEE 802.11, fornecem algumas técnicas de criptografia de forma a impedir a interceptação de dados e o uso da rede por usuários não autorizados. A primeira técnica padronizada foi o *Wired Equivalent Privacy (WEP)* com a premissa de conceder confidencialidade de dados equivalente à de uma rede cabeada. Porém, com o surgimento de técnicas de criptoanálise capazes de descobrirem chaves de acesso em um curto prazo de tempo, o WEP se tornou rapidamente obsoleto (BORISOV *et al*, 2001). A *Wi-Fi Protected Access (WPA)* e seu aprimoramento, WPA2, são as atuais soluções padronizadas existentes para redes sem fio baseadas em algoritmos com segurança matematicamente comprovada (Jonsson, 2002). Tanto o WEP como o WPA e WPA2 são baseados na existência de uma chave comum e compartilhada entre os usuários e o AP.

AMBIENTE DE IMPLEMENTAÇÃO

O ambiente definido para validação do projeto foi a biblioteca da Universidade Federal de Goiás - Regional Catalão. Justifica-se em virtude da edificação possuir grande número de dispositivos com interfaces sem fio além de vários perfis de usuários conectados em um mesmo ambiente. Os perfis de usuários para uso da rede sem fio desta edificação são estudantes de graduação e pós-graduação, técnicos administrativos e docentes.

O ambiente de rede estruturado para o projeto consistiu em:

- 1 Servidor *Windows Server 2008 R2*® com AD (*Active Directory*) e RADIUS (*Remote Authentication Dial In User Service*);
- 1 Servidor PfSense;
- 1 Access Point;
- Dispositivos com interface de rede (notebooks, celulares e tablets).

A Fig. 1 representa o processo de autenticação dos usuários mediante os servidores PfSense e AD com RADIUS. O processo se inicia quando o usuário com seu dispositivo móvel verifica a disponibilidade da rede sem fio. Ao solicitar conexão, o AP encaminha o pedido ao servidor PfSense e o *browser* padrão do dispositivo é aberto sendo lhe solicitada suas credenciais (usuário e senha). O servidor PfSense encaminha ao servidor RADIUS as credenciais do usuário. Por sua vez, o servidor RADIUS verifica na base de dados do servidor AD a existência do usuário e valida sua senha. Em caso de validação o RADIUS informa a liberação ao PfSense que passará a controlar seus acessos de acordo com suas permissões.

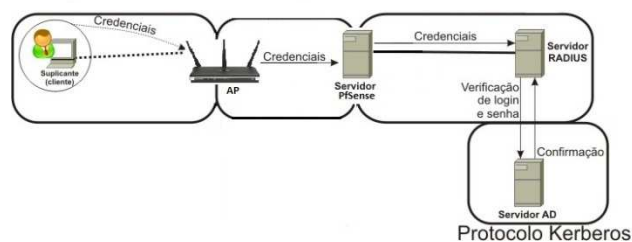


FIGURA 1: Processo de autenticação de usuários na rede sem fio da Biblioteca

Servidor Windows Server 2008 R2®

O *hardware* definido para o servidor comportar o sistema operacional Windows Server 2008 R2® com as aplicações necessárias consistiu da seguinte configuração:

- Processador Intel® i5-3330;
- 8GB de memória RAM DDR3 1333MHz;
- 320GB de Hard Disk.

Segundo as informações disponíveis pela *Microsoft®* através de seu site institucional a configuração mínima para instalação deste sistema operacional consiste em:

- Processador – Recomendado 2GHz;
- 2GB de memória RAM;
- 40GB de Hard Disk.

O sistema operacional Windows Server 2008 R2® foi escolhido em detrimento da licença de uso que o Centro de Recursos Computacionais (CERCOMP) da Universidade Federal de Goiás (UFG) possui. O cenário deste projeto não permite uso de versões anteriores ao Windows Server 2008® em função de aplicações necessárias ainda não terem sido disponibilizadas.

Configuração do Servidor PfSense

O Servidor PfSense foi instalado em um *hardware* exatamente igual ao utilizado para instalação do Servidor *Windows Server 2008®*. Por se tratar de uma customização do sistema operacional *FreeBSD*, os recursos de *hardware* necessários são ainda menores quando comparados ao servidor com *Windows Server®*. Assim sendo, o *hardware* atende a demanda para o servidor com PfSense. O processo de implantação do servidor PfSense envolveu as configurações:

- Interfaces de Rede Físicas;
- DHCP Server;
- Serviço de Proxy do PfSense;
- *Captive Portal*.

Ressalta-se que o protocolo de autenticação escolhido para o RADIUS deve obrigatoriamente ser o mesmo definido para o PfSense, caso contrário o processo de autenticação apresentará falha.

A Fig. 2 apresenta o ambiente de *login* disponibilizado pelo *Captive Portal* do PfSense ao usuário para o processo de autenticação na rede sem fio. Uma vez validadas as credenciais, o usuário terá acesso à rede segundo suas permissões.



FIGURA 2: Página de autenticação do usuário através do uso do PfSense

RESULTADOS OBTIDOS

De modo a validar o cenário proposto, foram inseridos quinhentos usuários no controlador de domínio *Active Directory* (AD). Os usuários receberam os *usernames* “usuario1, usuário2, ... , usuário500” e a senha padrão para todos “12345”. Os testes avaliados foram:

- Tempo de carregamento da tela de autenticação;
- Validação da autenticação por usuário e senha para autenticações com credenciais corretas e incorretas;
- Tempo de autenticação dos usuários.

Configuração das Estações Clientes

Os testes desenvolveram-se em duas estações clientes. A primeira com sistema operacional *Windows 7 ultimate*[®] e a segunda com distribuição Ubuntu (14.04) do sistema operacional Linux, ambos versão de 64 *bits*.

As estações clientes possuem exatamente a mesma configuração de *hardware* de modo a não ocorrer variação nas respostas dos testes em virtude deste item.

- Processador Intel[®] i5 3330, clock de 3.0GHz, Cache 6MB;
- 500 GB de HD (*Hard Disk*);
- 8 GB de memória RAM DDR3 1333MHz.

As estações clientes foram devidamente formatadas para a realização dos testes, instalando-se apenas os referidos sistemas operacionais e os *browsers* C-

- *DevTools: Chrome Developer Tools.*

O teste realizado avaliou sequencialmente o carregamento da página de autenticação de usuários. A amostra foi de 50 carregamentos em cada *browser* e em cada estação cliente. A Fig. 4 mostra comparativamente os resultados obtidos.

Os resultados mostram a variação dos tempos de acesso entres os diferentes *browsers* nas duas estações clientes. Destaca-se que o menor e o maior tempo foram obtidos pelo Firefox na estação com Windows[®] com os tempos de 39ms e 84ms. Os tempos médios de acesso foram próximos com 55,3ms para o Firefox com Windows[®]; 53,46ms para o Firefox com Linux; 57,88ms para o Chrome com Windows[®] e 56,48ms para o Chrome com Linux. Apesar de pequena a diferença, o *browser* Firefox obteve um desempenho superior ao Chrome. Em relação às estações clientes, o computador com sistema operacional Linux obteve melhor desempenho em relação ao computador com Windows[®]. Quando comparado com o resultado de 120ms ressaltado em Aiftimiei *et al* (2008), a média geral de 55,78ms mostrou-se bem abaixo e, portanto, satisfatória para atender aos usuários da rede.

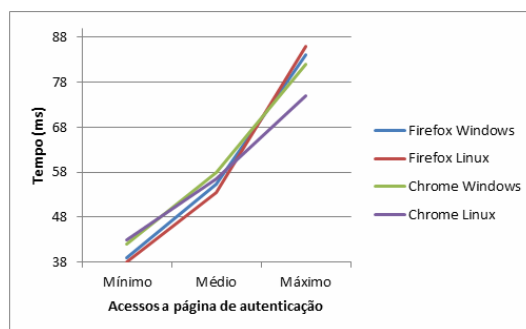


FIGURA 4: Tempo de acesso a página de autenticação de usuários

Segundo Teste: Validação da Autenticação por Usuário e Senha

O segundo teste de validação do cenário de controle de acesso representa ser o mais importante, uma vez que uma falha durante o processo de autenticação poderia permitir que usuários pudessem ter acessos indevidos ou mesmo ter acessos negados quando não deveria.

Foram realizadas três séries de acesso (por usuário e senha para este teste):

- Todos os usuários com senhas corretas;
- Todos os usuários com senhas incorretas;
- Vinte usuários aleatórios com senha “123456”;

Em cada uma das três séries realizadas o índice de sucesso na validação do processo de autenticação foi de 100%, ou seja, em nenhum caso um usuário que não deveria ter acesso foi autenticado, ou então, um que deveria ter acesso não o tenha sido. Os resultados do processo de autenticação foram retirados dos *logs* do servidor *Windows Server*[®] onde estava o AD.

Terceiro Teste: Tempo de autenticação dos usuários

Para a realização deste teste, utilizou-se a mesma estrutura de estações clientes e *softwares* da seção 3.3. O tempo de autenticação foi analisado para as três séries da seção 3.4, porém, com a amostragem de cem usuários por série. A terceira série com tentativas de acesso com senha “123456” foi realizada para 30 usuários.

Os resultados obtidos por série foram:

Validação com todas as Senhas Corretas

A Fig. 5 apresenta as variações de tempo para as cem tentativas de acesso onde todas as senhas do *script* estavam corretas.

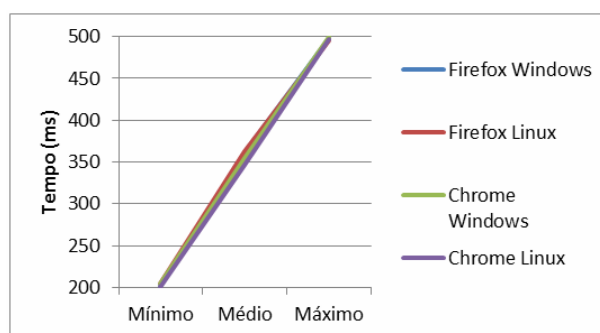


FIGURA 5: Tempo de autenticação com todas as senhas corretas

Os resultados apresentados na Fig. 5 mostram que em nenhuma tentativa de autenticação os tempos ficaram fora do intervalo entre 200 e 500ms. As médias de tempo obtidas por *browser* foram: 360,99ms no Firefox do Windows[®]; 365,09 no Firefox do Linux; 354,08ms no Chrome do Windows[®] e 346,26ms no Chrome do Linux.

Validação com todas as Senhas Incorretas

A Fig. 6 apresenta as variações de tempo para as cem tentativas de acesso onde todas as senhas do *script* estavam incorretas.

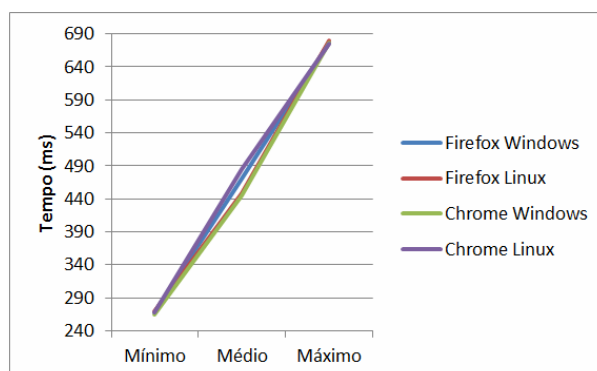


FIGURA 6: Tempo de autenticação com todas as senhas incorretas

Os resultados apresentados na Fig. 6 mostram que em nenhuma tentativa de autenticação os tempos ficaram fora do intervalo entre 240 e 640ms. As médias de tempo obtidas por *browser* foram: 470,41ms no Firefox do Windows®; 448,81 no Firefox do Linux; 444,4ms no Chrome do Windows® e 484,54ms no Chrome do Linux. Quando comparado com a Fig. 5, nota-se que o processo de autenticação com avaliação de senhas incorretas é maior do que quando comparado com autenticação de senhas corretas. Os tempos mínimo, máximo e também as médias são maiores.

Usuários aleatórios com senha "123456"

A Fig. 7 apresenta as variações de tempo para as cem tentativas de autenticação onde vinte usuários tentaram acesso com a senha "123456".

Os resultados apresentados mostram que em nenhuma tentativa de autenticação os tempos ficaram fora do intervalo entre 220 e 530ms. As médias de tempo obtidas por *browser* foram: 376,33ms no Firefox do Windows®; 374,73 no Firefox do Linux; 372,97ms no Chrome do Windows® e 360,75ms no Chrome do Linux. Quando comparado com as Fig. 5 e 6, nota-se que os valores de tempo médio estão entre os dois gráficos. Desta maneira, pode-se sugerir que em função de alguns usuários da amostra terem tentado acesso com senhas incorretas, aumentou o tempo de validação do processo de autenticação.

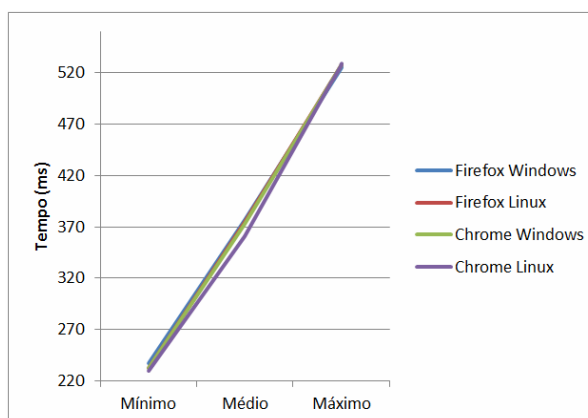


FIGURA 7: Tempo de autenticação com vinte senhas incorretas

CONCLUSÃO

O ambiente de controle de acesso utilizando a integração entre AD, RADIUS e PfSense obteve êxito em todos os testes realizados, mostrando-se um processo eficaz e rápido de autenticação de usuários. O *hardware* utilizado para o cenário do projeto pode-se facilmente ser encontrado no mercado, não havendo nenhum circuito integrado específico.

Em uma análise sobre as três séries realizadas em relação ao tempo de autenticação dos usuários, percebe-se que as variações dos tempos foram muito pequenas considerando-se todo o processo de autenticação. Mesmo em casos cujos tempos superaram 600ms o tempo ainda é consideravelmente baixo para o usuário que aguarda a autenticação para poder usufruir dos recursos da rede sem fio.

AGRADECIMENTOS

Agradeço a FAPEG (Fundação de Apoio a Pesquisa do Estado de Goiás) pelo apoio e financiamento através de bolsa na modalidade mestrado dedicada ao projeto. Ao meu orientador Marcelo Henrique Stoppa que além de ser um grande mestre de ensinamentos também se mostrou um verdadeiro amigo. Aos meus companheiros do LabMOt pelo incentivo à conclusão deste projeto.

REFERÊNCIAS

AIFTIMIEI, C.; ANDREOZZI, S.; CUSCELA, G.; DAL PRA, S.; DONVITO, G.; DUDHALKAR, V.; FANTINEL, S.; FATTIBENE, E.; MAGGI, G.; MISURELLI, G.; PIERRO, A. **Design Principles of a Web Interface for Monitoring Tools**. In. International Conference on Computing in High Energy and Nuclear Physics, Journal of physics, 2008.

BORISOV, N.; GOLDBERG, I.; WAGNER, D. **Intercepting mobile communications: The insecurity of 802.11**. 2001.

GAST, M. S.; LOUKIDES, M. **802.11 wireless networks: the definitive guide**. O'Reilly&Associates, Inc. Sebastopol, CA, USA, 2002.

IEEE 802.11. **Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**, 2012.

IEEE 802.15. **Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)**, 2012

IEEE 802.16. **IEEE Standard for Air Interface for Broadband Wireless Access Systems**, 2012.

JONSSON, J. **On the Security of CTR + CBC-MAC: NIST Modes of Operation - Additional CCM Documentation**. Proceedings from Selected Areas of Cryptography. 2002.

TANEMBAUM, A. S. **Redes de Computadores**. Campus, 4ª edição, 2011.