doi.org/ 10.51891/rease.v8i4.5098

UMA BREVE EXPLANAÇÃO SOBRE A UTILIZAÇÃO DO SOFTWARE TGM 2010

A BRIEF EXPLANATION OF THE USE OF THE SOFTWARE TGM 2010

Brazelino Bertolete Neto[1]
Fábio José Colombo[2]
Luciano de Jesus Rodrigues de Barros[3]

RESUMO: O objeto de estudo é a demonstração de aspectos de segurança na utilização do sistema operacional Windows em servidores de internet para redes corporativas. Para isso, coube ao estudo contar com explanações e com todo um referencial teórico, além de exemplos práticos envolvendo estudos de casos com um servidor de internet de alta confiabilidade que uniu a segurança do sistema operacional Windows Server 2008 com a facilidade de gerenciamento e configuração do software de firewall TMG 2010 o que deixou a rede mais segura e fácil de administrar.

Palavras-Chaves: Servidor. Sistema Operacional Windows Server 2008. Confiabilidade.

ABSTRACT: The object of study is the demonstration of security aspects in the use of the Windows operating system on Internet servers for enterprise networks. To this end, it fell to the study rely on explanations and with a whole theoretical, and practical example involving case studies with a web server for high reliability that united the security of Windows Server 2008 operating system with ease of management and configuration software firewall TMG 2010 that has left the network more secure and easier to administer.

Keywords: Server. Windows Server 2008 operating system. Reliability.

INTRODUÇÃO

Com o crescimento da população, houve a necessidade de novas tecnologias de informação, mais rápidas e eficazes, surgindo assim a rede mundial de computadores

[1] Professor do Centro de Educação Tecnológica Paula Souza. Pós-graduado em Análise de Segurança Digital. E-mail: brazelino.neto@fatectq.edu.br.
[2] Professor do Centro de Educação Tecnológica Paula Souza. Pós-graduado em Análise de Segurança Digital. E-mail: fabio.colombo@fatectq.edu.br.
[3] Professor do Centro de Educação Tecnológica Paula Souza. Pós-graduado em Gestão em Sistemas de Informação. E-mail: lennontaqua@hotmail.com.

(internet). Empresas, escolas, faculdades, órgãos públicos, começaram a implantá-la sendo que hoje, boa parte da população já a utiliza.

Enfim ao analisar todas as evoluções da internet e o seu uso crescente nos ambientes corporativos com um número cada vez maior de computadores e uma diversificação cada vez maior de conteúdos de sites, vê-se a necessidade de implantação de um bom projeto de rede nesses locais onde todos os acessos à web ficam centrados em um servidor que implemente boas políticas de segurança e que gerencie de forma eficiente todo o conteúdo acessado pela rede.

Devido a necessidade e até mesmo a falta de informações sobre servidores de internet Microsoft, este trabalho procurará apresentar através de exemplos práticos e explanações, alguns aspectos de segurança na utilização do Windows Server dentro das empresas como servidor de internet.

O objetivo deste projeto será estudar todos estes aspectos de segurança na utilização do Windows 2008 Server em servidores de internet e buscará uma melhor compreensão das ferramentas deste sistema operacional para zelar pelas políticas de segurança adotadas pelas empresas e de suas praticidades, em especial o TMG 2010.

A metodologia de estudos envolverá a observação das documentações cedidas pela Microsoft, além de analisar a implementação das rotinas de segurança aplicadas nas empresas e o desempenho do Windows Server para aplicá-las, através de um estudo de caso.

TMG 2010 - CONCEITOS INICIAIS

O Microsoft Forefront Threat Management Gateway 2010(TMG) é a versão nova e melhorada do Microsoft Internet Security and Aceleretion ISA, incluindo novos mecanismos de proteção como inspeção de rede, filtragem de url, proteção de e-mail dentre outros. (MSEVENTS.MICROSOFT, 2012).

Para que possamos entender a função do TMG 2010 devemos compreender os conceitos de firewall e de camadas de redes. Um firewall é uma espécie de "barreira" existente entre a rede externa(internet) e a rede interna (rede local), um elemento que filtrará os tráfegos advindos tanto no sentido internet para a rede interna como rede interna para a internet.

O firewall geralmente é instalado num ponto de encontro entre a rede local e a internet, ponto este chamado de servidor proxy que faz justamente a união entre as duas redes, servindo assim como uma espécie de ponte entre as duas.

Um proxy funciona como intermediário entre clientes, que desejam fazer alguma conexão a internet, e os servidores, aos quais os pedidos são feitos. O cliente faz o pedido ao proxy e este é que na realidade contacta ao servidor pretendido e transfere o documento, enviando-o depois ao cliente. Se o proxy funcionar também como servidor de cache, armazena o documento durante um período de tempo pré-determinado e em subsequentes pedidos desse mesmo documento devolve a cópia que tem armazenada, o que acelera consideravelmente o tempo de resposta. O proxy trabalha na camada de aplicação do Modelo OSI.

No firewall pode-se definir as regras de tomadas de ações baseadas em algum evento. Através destas regras o firewall consegue liberar, bloquear ou negar basicamente todo o tráfego.

Esquematização do uso do firewall representada pela **figura 1:**

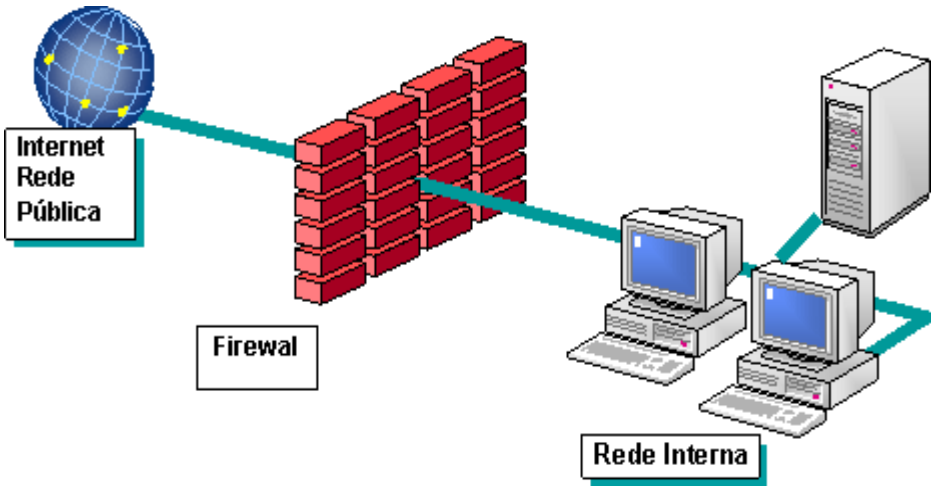

Figura 1-Firewall entre a rede interna e externa

Fonte: Júlio Battisti. http://www.juliobattisti.com.br/tutoriais/breinerqueiroz/isaserver2k001.asp. Acesso em 12/04/2013

FUNCIONALIDADES E RECURSOS DO TMG 2010

Conforme dito anteriormente, o TMG possui algumas melhorias e novas funcionalidades. Segundo o site da Microsoft, este software possui os seguintes recursos:

- Múltiplas fontes de dados para filtragem de URL para um melhor bloqueio de websites mal intencionados.
- Mecanismo antimalware de alta precisão.
- Prevenção de intrusão contra a exploração de vulnerabilidades.
- Tecnologias comprovadas de proteção de rede nativas do ISA SERVER 2006.
- Múltiplas tecnologias de segurança de web integradas numa única solução.
- Autenticação, atualização, distribuição de diretivas e relatórios da infraestrutura.
- Interface única para o gerenciamento de políticas de segurança da web.
- Logs e relatórios abrangentes.

Todas as funcionalidades e melhorias do software demonstram bom desempenho particularmente quando é instalado num sistema que execute o Windows Server 2008.

Por agir como filtro, para permitir ou negar um acesso desejado deve-se criar uma **Acess Rule (Regra de acesso).** Pode-se também criar regras de acesso de publicação web, regras de publicação no servidor de e-mail e regras de publicação de outros servidores para controlar o acesso para a rede e de sua rede.

Através do firewall policy podemos definir as Acess Rules que são baseadas em vários tipos de elementos a saber:

- *Protocols:* Este elemento de regra contém os protocolos os quais você poderá usar para definir os protocolos que serão usados dentro de uma Acess Rule. Você pode permitir ou negar o acesso sobre um ou mais protocolos
- *Users:* Dentro deste elemento de regra você poderá criar um grupo de usuários para o qual a regra será explicitamente aplicada ou não. Por exemplo: Talvez você queira criar uma regra que permita o acesso a internet para todos os usuários de uma organização com exceção de todos os empregados temporários.
- *Content type:* Este tipo de elemento de regra fornece os tipos de conteúdo comuns para o qual você poderá aplicar uma regra para bloquear todos os conteúdos de downloads para as extensões .exe, .bat, .cmd, etc

- *Schedules:* Este tipo de elemento, por sua vez, permite que você estipule e determine horários durante a semana em que as regras serão aplicadas. Se você precisa definir um ***Acess Rule*** que permita o acesso à internet somente durante algumas horas específicas, você poderá fazer uso deste elemento onde essas horas serão definidas.

- *Network Object:* Este elemento de regra permite que você crie um grupo de computadores para o qual a regra será imposta ou não.

Através da firewall policy podemos definir as Acess Rules que são baseadas em vários tipos de protocolos. Uma característica notável do TMG 2010 é que ele também atua diretamente na camada de aplicação, correspondente à camada mais alta do modelo OSI de rede e a principal vantagem de se ter um firewall atuando na camada de aplicação é que se pode bloquear a execução de arquivos e programas com possíveis extensões maliciosas como .bat, .exe, .cmd, dentre outros, todos, indesejáveis para a boa segurança da rede. Com todas essas vantagens, o usuário também tem acesso a uma vasta gama de soluções e conhecimento disponíveis a nível mundial.

DEFESA ATRAVÉS DE ESTUDOS DE CASOS PRÁTICOS

Os estudos realizados constataram alguns problemas que afetam o desempenho da rede e da prestação de serviço como um todo. Nos itens subseqüentes citar-se-ão os problemas encontrados em algumas empresas:

- **Sistema operacional:** o servidor atual da rede conta com sistemas operacionais que não são considerados sistemas ideais para um servidor de rede, pois não contém um alto nível de segurança e recursos primordiais para o gerenciamento da rede, afetando assim o bom desempenho dessa rede.

- **Software para criação de regras:** Não há software instalado que permita criar regras de acesso a sites e páginas da web, dessa maneira há um livre acesso por todos os usuários a sites de qualquer conteúdo. Os precários controles de acesso e restrição de sites são feitos nas estações locais.

Diante de todos os problemas expostos, algumas soluções poderiam ser apresentadas como a implantação de um novo servidor com o sistema operacional

Windows 2008 Server em substituição de antigos sistemas, tornando o gerenciamento mais fácil para quem administra e também oferecendo recursos próprios de rede e segurança, tornando a rede mais rápida e segura além da instalação aliada ao software TMG 2010 que permite implementar a idéia de firewall centralizado, gerenciando e otimizando os acessos a páginas da web, sem mencionar o fato que a partir dele poderíamos definir uma política de melhor controle de banda, criação de grupos de usuários e de regras de acesso que se aplicariam a esses grupos, permitindo ou restringindo acessos a determinados grupos.

É possível se deparar com uma série de situações que as empresas querem lidar, exemplificando, uma, onde usuários específicos possuem acessos restritos a determinados sites durante um certo intervalo de tempo, como o horário em que o expediente da empresa se encontra aberto. Nesse caso, estes sites ficariam restritos apenas no horário de expediente ficando os acessos aos mesmos liberados fora deste horário, além de restrição total a qualquer site de conteúdos impróprios, todos fatores fáceis e simples de implementar no TMG 2010.

Esquematização de regras criadas no TMG 2010

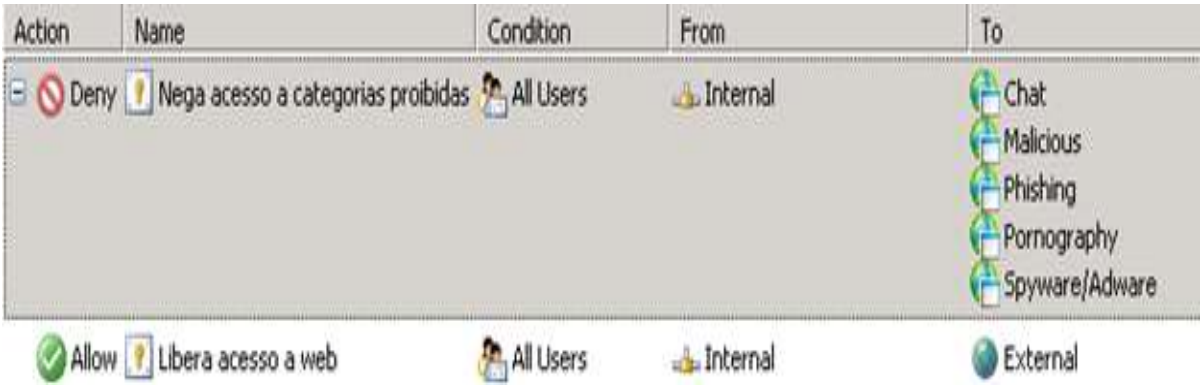

Figura 2-Tela das regras criadas no Servidor
Fonte: Autores

CONCLUSÃO

A apresentação decorrida defende uma série de aspectos positivos de segurança no uso do sistema operacional Windows Server 2008 aliado ao software TMG 2010, aspectos como sua facilidade de configuração, bom desempenho, melhorias que foram surgindo ao longo dos lançamentos das novas versões, boas documentações e ainda a possibilidade de acessar a uma vasta gama de soluções e conhecimentos disponíveis a nível mundial.

Todo e qualquer projeto, requer dos seus autores grande conhecimento e habilidade para o seu pleno desenvolvimento. Com base nas documentações da Microsoft e na implantação prática de um servidor com o software TMG 2010 instalado, pode-se chegar à conclusão de que um servidor de internet Windows, quando bem configurado, cumpre seus objetivos nos quesitos de segurança.

O projeto de rede com a implantação de um servidor de internet com Windows Server 2008 e o software de firewall TMG 2010 nos estudos de casos nas empresas estudadas se destaca por suas vantagens oferecidas às mesmas e aos clientes, como maior segurança na manipulação de seus dados, maior conforto e rapidez no acesso para os clientes, criação de regras de permissão de acesso para alguns usuários e restrição a outros, dentre uma série de outras vantagens.

Desta forma, afirma-se que este projeto atende a todas as necessidades das empresas, com agilidade, facilidade e praticidade em sua operação, sendo um grande apoio para a administração, implantação e manutenção do órgão estudado.

REFERÊNCIAS

Batista, J. **Tutoriais Diversos.** Disponível em: < http://www.juliobattisti.com.br/tutoriais/> (Acesso feito em 12/04/2013).

Felipe, D. **Instalando e Configurando o Forefront TMG 2010.** Disponível em:

<http://blog.douglasfilipe.com.br/2010/05/02/instalando-e-configurando-o-forefront-tmg-2010/> (Acesso feito em 16/04/2013).

Honda,D. **Administração do Windows Server 2008 R2.** Rio de Janeiro: Brasport, 2011.

MINASI, M. **Dominando o Windows Server 2008 Usando em Rede**. São Paulo:Alta Books, 2009.

Site Microsoft. **Microsoft Forefront-Visão Geral.** Disponível em:<www.microsoft.com/brasil/servidores/forefront/tmg/default.mspx >Acesso em 15/01/2012.

Site MsEvents. **What's New in Forefront Threat Management Gateway 2010?.** Disponível em:<https://msevents.microsoft.com/CUI/EventDetail.aspx?culture=ptBR&EventId=1032433940&CountryCode=br >Acesso em 15/01/2013.

Site da Technet Brasil.**Baixe o Microsoft Forefront Threat Management Gateway 2010.** Disponível em:<http://technet.microsoft.com/pt-br/evalcenter/ee423778.>
Acesso em 20/01/2013.

Site Technet Microsoft. **Biblioteca de Produtos e Aprendizagem.** Disponível em: < http://technet.microsoft.com/pt-br/library/ >Acesso em 08/02/2013.