UNIVERSIDADE FEDERAL DE MATO GROSSO
COORDENAÇÃO DE ENSINO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

RELATÓRIO DE ESTÁGIO SUPERVISIONADO

HIGIENIZAÇÃO E IMPLANTAÇÃO DE FIREWALL FORTIGATE EM AMBIENTE CORPORATIVO

ARTHUR MESSI FREITAS

CUIABÁ – MT
2014

UNIVERSIDADE FEDERAL DE MATO GROSSO
COORDENAÇÃO DE ENSINO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

RELÁTORIO DE ESTÁGIO SUPERVISIONADO

HIGIENIZAÇÃO E IMPLANTAÇÃO DE FIREWALL FORTIGATE EM AMBIENTE CORPORATIVO

ARTHUR MESSI FREITAS

Relatório apresentado Instituto de Computação da Universidade Federal de Mato Grosso, para obtenção do título de Bacharel em Sistemas de Informação.

CUIABÁ – MT
2014

UNIVERSIDADE FEDERAL DE MATO GROSSO
COORDENAÇÃO DE ENSINO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

ARTHUR MESSI FREITAS

Relatório de Estágio Supervisionado apresentado à Coordenação do Curso de Sistemas de Informação como uma das exigências para obtenção do título de Bacharel em Sistemas de Informação da Universidade Federal de Mato Grosso

Aprovado por:

Prof. MSc Nilton Hideki Takagi
Instituto de Computação
(Orientador e Coordenador de Estágios)

Ricardo Saddi Becker
(Supervisor)

José de Paula Neves
Instituto de Computação - UFMT
(Avaliador Externo)

DEDICATÓRIA

Este trabalho não poderia ter sido realizado sem o incentivo de meus pais, dedicados observadores do meu esforço. Também merecem honrosa menção, meus amigos, que me cobram, incentivam e estão presentes, seja com palavras diretas ou ações, me ajudando a escolher o caminho que devo seguir.

Também se faz presente o nome deles, Jéssica Bastos e Thiago Almeida, que me servem de exemplo para que eu não descanse enquanto posso melhorar, motivando-me a dedicar cada vez mais de mim aos meus objetivos, pois esta visão sempre me lembra o quanto meu esforço vale a pena.

AGRADECIMENTOS

Sou grato a todos os amigos, principalmente aqueles que também são companheiros de trabalho e que sempre estão dispostos a tirar minhas dúvidas, me ensinando novos meios de alcançar o que sozinho eu não posso. Mas acima de tudo, a grande oportunidade que encontrei na empresa Becker Consultoria, de ampliar meus conhecimentos e buscar sempre o máximo de minha capacidade, através de um ambiente em que todos são incentivados a evoluir de acordo com seus esforços.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ADSL	Asymmetric Digital Subscriber Line – Sem definição em Português
DHCP	Dynamic Host Configuration Protocol – Protocolo Dinâmico de Configuração de Endereços
PPPoE	Point-to-Point Protocol over Ethernet – Protocolo Ponto-a-Ponto sobre Ethernet
WAN	Wide Area Network – Rede de Longa Distância
DVR	Digital Video Recorder – Gravação de Vídeo Digital
HTTP	HyperText Transfer Protocol – Protocolo de Transferência de Hipertexto
HTTPS	HyperText Transfer Protocol Secure – Protocolo de Transferência de Hipertexto Seguro
MCP	Microsoft Certified Professional – Profissional Certificado Microsoft
TI	Tecnologia da Informação
SO	Sistema operacional
DoS	Denial of Service – Negação de Serviço

RESUMO

Este trabalho ressalva a importância de se investir em opções que tragam segurança a rede de pequenas e médias empresas, que nem sempre possui uma medida preventiva para controlar o tráfego de dados entre sua rede a internet. Apresentando o conceito e funcionalidade de Firewalls de rede, tenta justificar a necessidade de se tratar a falta de segurança a qual toda a informação valiosa de uma empresa está sujeita. Para tanto, apresenta a experiência obtida na participação de um projeto de implantação de Firewall FortiGate realizado pela empresa Becker Consultoria, no qual tive a oportunidade de participar, além de objetivar ser uma referência a qualquer pessoa que possua conhecimento relevante na área de Tecnologia e queira instalar e configurar um Firewall FortiGate. Utiliza-se de linguagem objetiva e ilustração para tornar o caminho da instalação mais fácil, além de possuir também informações a respeito das alternativas das várias opções de configurações possíveis do equipamento.

INTRODUÇÃO

O uso comum de internet é fundamental para se levar adiante qualquer tipo de trabalho hoje em dia, seja em empresas ou residências, porém não existe uma maneira completamente segura de se estar conectado à rede mundial de computadores. No entanto, podemos adotar uma série de medidas para minimizar os riscos aos quais somos expostos. Em 2013, foram registrados 91 mil incidentes de segurança aos clientes da Dimensiona Data, segundo pesquisa divulgada pela empresa e realizada a nível mundial (DIMENSION DATA, 2014). Num ambiente corporativo, os riscos são exponencialmente maiores, devido ao maior volume de dados, de forma que uma pequena brecha pode ser o suficiente para que uma empresa tenha informações roubadas ou dados perdidos. Por mais que todas as opções representem perdas significativas, nada irá pesar mais do que perder dados ou informações em decorrência da falta de investimento e atenção a segurança.

A necessidade de se investir em segurança da informação é imprescindível, e o cenário atual das empresas indica que não se investe o suficiente. Apenas 38% dos funcionários de TI acreditam que suas empresas investem o suficiente em pessoal e tecnologias qualificadas quando se trata da segurança virtual em suas empresas (WEBSENSE, 2014).

Há muito que se pode fazer para tentar evitar situações prejudiciais, dentre elas, manter um bom Firewall entre sua rede e o ambiente digital externo pode representar a diferença entre ser mais um a sofrer perdas ou ter uma um ambiente em bom funcionamento e seguro.

Segundo pesquisa, de 685 empresas brasileiras, 98% afirma utilizar Firewall em suas redes, enquanto que 50% afirmam a pretensão de investir acima de R$ 110.000 em soluções de segurança da informação (DELL, 2013). Esses dados nos permitem inferir a importância significativa dada a esta área dentro do setor de tecnologia do ramo corporativo, onde o investimento em segurança de sua informação ocupa um dos níveis mais altos em importância.

Avaliando os riscos aos quais os computadores correm na internet, no *top* 10 de *malwares* detectados na América Latina, uma das principais ameaças é o programa AdWare.Win32, baseado num esquema de exibição de publicidade em

meio as páginas de internet acessadas. Elas monetizam o proprietário baseada no número de cliques (KASPERSKY LAB, 2013). Este fato nos alerta dos perigos de uma rede desprotegida e sem restrição de acessos, agravado pela necessidade de um conhecimento técnico para se livrar desse tipo de software.

Por definição, firewalls são ferramentas que aumentam a segurança de computadores conectados a uma rede. Um *firewall* separa computadores da internet, inspeciona pacotes de informações que chegam ou saem da rede, para determinar aquilo que é ou não permitido (HAZARI, 2000). Podemos ainda dizer que eles fazem o papel de guardas entre os dispositivos que temos dentro de um ambiente, daqueles que estão fora.

Este trabalho descreve a execução de um projeto de *firewall*, realizado pela Becker Consultoria em prestação de serviço a um cliente. Tal projeto foi implantado no ambiente de rede da empresa cliente, tendo por objetivo tornar a rede mais segura, beneficiando a empresa com as características apresentadas pela ferramenta.

1. REVISÃO DE LITERATURA

No relatório intitulado “*Security in the internet architecture*”, emitido pelo *Internet Architecture Board* (IAB), é estabelecido um consenso no qual a internet necessita de um maior nível de segurança, onde também são indicadas as áreas mais afetadas. O monitoramento e controle não autorizado do tráfego de rede são destaques como principais pontos a serem protegidos, garantindo autenticação ponto a ponto para usuários, utilizando ferramentas com criptografia. (STALLINGS, 2006, p. 4).

Este relatório, ainda que publicado em 1994, relaciona o princípio da preocupação com as informações trafegadas na internet, com cada vez mais importância em nossos períodos atuais. Em tempos onde a informação é uma arma poderosa, sua segurança tem sido motivo de atenção dos profissionais a frente de redes corporativas, buscando sempre novas práticas a fim de impedir que dados sigilosos possam ser obtidos por alguém não autorizado.

Em sistemas de comunicação via internet, o controle das informações trafegadas entre origem e fonte é exercido por computadores, que nem sempre são os únicos participantes dessa transmissão. Podem existir vários outros computadores separando essas pontas, em especial quando há um grande caminho separando essas máquinas (TERADA, 2008, p. 16). Nossa informação tem de passar por um longo caminho até chegar ao objetivo final, e em geral, o ponto onde ela está mais vulnerável é nas extremidades. Utilizando de pesquisa e análise de portais, podemos criar confiança em empresas ou sistemas que investem muito em segurança para que nossos dados sejam bem cuidados quando realizamos uma transição de informações. Apesar de sempre haver o risco de falhas, é durante o momento em que está em nossa rede que a informação normalmente é interceptada, sendo capturadas através de programas maliciosos que sondam nossas máquinas ou apanhadas no meio do caminho por máquinas infectadas e que acabam tendo que trabalhar para invasores.

Com o passar dos anos, é cada vez menor a necessidade por conhecimentos especializados para se realizar ataques a dispositivos e sistemas disponíveis *online*. A criatividade e empenho por parte de criminosos digitais aumentaram de forma

inversamente proporcional a esta exigência (STALLINGS, 2006 p. 5). É cada vez maior o número de pessoas dispostas a tentar trespassar a segurança imposta entre a internet e redes privadas. Novas ferramentas a serem usadas para tal meio surgem a cada dia. Apesar de um ataque bem elaborado e proveniente de alguém realmente preparado possa ser muito assustador, iniciantes sempre podem se aproveitar de vulnerabilidades conhecidas que nem sempre recebem a devida atenção, softwares que não são atualizados e a falta de ferramentas adequadas para defender aquilo que é mais precioso.

A necessidade de se implantar camadas adicionais de segurança é sem dúvida enorme, e designar uma parte dos recursos de uma empresa para diminuir os riscos de uma invasão é pequeno se comparado às perdas que podem acontecer em virtude da falta dessas opções. Um *firewall* sozinho certamente não pode oferecer toda a segurança necessária que uma rede precisa, mas é um passo fundamental para controlar o que entra e sai dela.

Podemos em um ponto dizer que um Firewall não se trata de um produto, mas de um conceito a ser posto em prática, onde se leva em conta todas as regras que devem ser aplicadas dentro da rede. A elaboração dessas regras, apesar de possuir fatores comuns com as mais variadas empresas, deve ser personalizada para se adequar à realidade desejada. Serviços e ferramentas que são utilizados dentro de uma rede e que possuem saída com a internet podem precisar de liberações específicas para seu correto funcionamento.

2. MATERIAS, TÉCNICAS E MÉTODOS.

Meu estágio prático foi realizado na empresa Becker Consultoria, situada em Cuiabá-MT, tendo como supervisor direto, Ricardo Saddi Becker, Diretor Geral da empresa. Tive a oportunidade de acompanhar tarefas não apenas relacionadas com o objetivo prático deste trabalho, mas também tarefas de Help Desk de nível um, estudos complementares das áreas trabalhadas e material para certificação. Durante o vínculo com a empresa, obtive aprovação na certificação *70-680 – Windows 7, Configuring*, me tornando um MCP (*Microsoft Certified Professional*), sendo esta certificação fruto não apenas do incentivo da empresa como também financiamento dos custos de realização da prova.

O aprendizado adquirido nas áreas práticas foi de muita valia para a bagagem profissional, trazendo experiências de relacionamentos interpessoais e boas práticas profissionais. A área de maior destaque no estágio foi sem dúvidas a de segurança, onde tive a oportunidade de participar da implantação de um projeto de segurança em um dos clientes da empresa. Este, portanto será um trabalho onde tento reproduzir o conhecimento obtido.

Para fins de segurança, nenhuma informação dos clientes e/ou da empresa Becker Consultoria poderá ser revelada, tendo esse ponto em vista, as imagens e textos citados conterão restrições e serão utilizados recursos de edição de imagem para garantir que tais informação não sejam exibidas.

O projeto de implantação é definido em partes, sendo elas:

- Proposta comercial;
- Preparação do ambiente;
- Implantação;
- Pós-implantação;
- Análise posterior.

O início é dado pelo setor comercial da empresa. Em visita acompanhada de um consultor técnico, nela são levantadas informações a respeito da empresa, tais como número de ativos, serviços utilizados, necessidades e projeções administrativas da área tecnológica. É então apresentada uma proposta comercial ao cliente, nela são descritos os procedimentos a serem realizados, escopo do projeto, requisitos técnicos

e valores. Ao realizar o aceite do projeto, cabe ao cliente realizar a aquisição do equipamento, dispondo de consultoria e indicação do modelo adequado.

A empresa em questão possui entre 35 a 50 estações de trabalho, com número semelhante de usuários. Levando em conta que além do projeto de Firewall, foi contratado também um serviço de suporte técnico aos ativos de rede, inicia-se a fase onde o ambiente é preparado para a implantação. As estações são analisadas uma a uma, onde são usados procedimentos necessários para correção de não conformidades, dentre elas, softwares antivírus desatualizados e programas nocivos instalados.

Ao final dessa fase, cerca de metade das máquinas apresentavam problemas graves na estrutura do sistema operacional, onde foram utilizados pontos de restauração de sistema quando disponíveis, pacotes de correções disponibilizados pela fabricante do sistema operacional e atualizações de software. Em outros 25% das estações, houve a necessidade de se realizar uma formatação, isto é, nova instalação do sistema operacional.

O próximo passo é a implantação do *firewall*. Dentre as opções disponíveis e das quais tive contato, a ferramenta a ser utilizada neste trabalho é o FortiGate, um produto da empresa FortiNet, uma das mais bem conceituadas na área de segurança em nível mundial, a qual dispõe de complexas e bem estruturadas ferramentas para segurança de redes. O modelo a ser utilizado foi escolhido baseado nas necessidades da empresa.

O *firewall* será instalado de tal forma que permita que a empresa utilize duas conexões diferentes com a internet. Isso permite maior disponibilidade e aumenta a capacidade teórica de conexão com a internet. O aparelho é fisicamente instalado entre o Switch e os Modems de conexão com a internet.

Para o equipamento em questão, o primeiro passo após a instalação física é configurar uma conta de acesso no portal da fabricante, pois é através dela que as informações de licença e suporte são obtidas e gerenciadas. Em seguida, é efetuado acesso ao sistema do *firewall*. Sua interface gráfica é baseada em navegador web, podendo ser acessada de qualquer máquina com devido acesso, sendo realizado através dela o gerenciamento das configurações. Neste momento é definida a senha

de administração, o que permite o acesso ao gerenciamento do equipamento, como indicado na Figura 01.

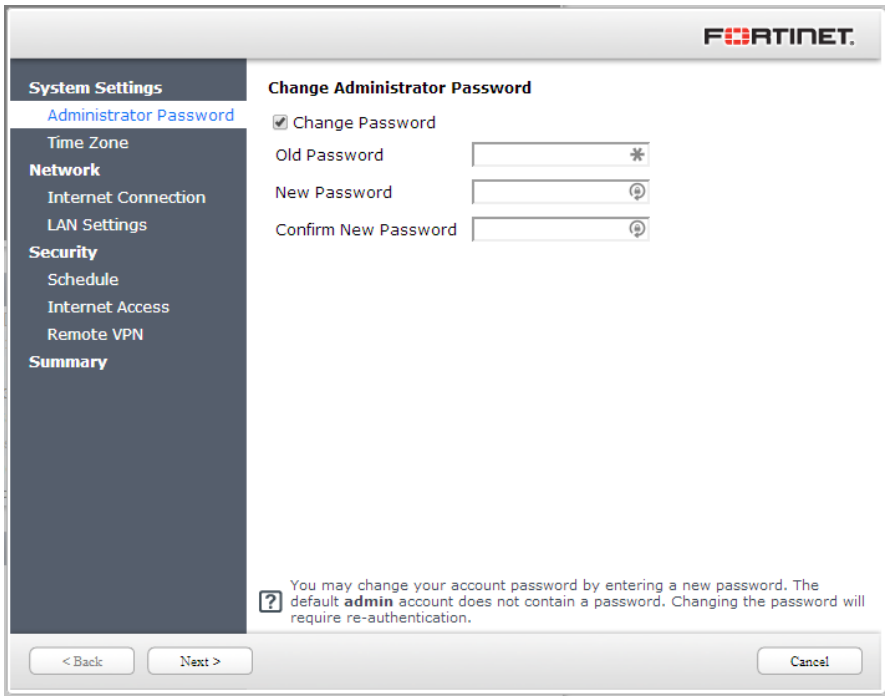

Figura 01 – Página de Configuração
Fonte: o autor (2014).

Em uma rede de pequena ou média empresa, o FortiGate é normalmente utilizado em *Transparent Mode*, onde ele é invisível para a rede, sendo todas as suas interfaces de rede pertencentes à mesma *subnet* e utilizando o mesmo intervalo de IP. Uma alternativa ao *Transparent Mode* é o NAT Mode, onde o Firewall é visível a toda a rede e normalmente gerencia várias *subnets*, sendo responsável pelo roteamento dos pacotes e comunicação entre as interfaces de rede. Este modo é quase sempre utilizado quando se possui um desenho de rede com várias áreas separadas e que podem ou não comunicar-se entre si. Apesar de importante a ser ressaltado, o modelo em questão possui apenas o *Transparent Mode*.

Existe uma série de informações a serem acrescidas ao sistema, sendo elas: data/hora, formato de data/hora, servidor de sincronização de data/hora e informações pertinentes à operação de ajuste de horário. Feito isso, a Figura 02 ilustra a próxima tela, onde são mostradas as informações de licença e suporte, obtidas através do usuário da conta cadastrada no sistema web da FortiNet, esta área lista os serviços disponíveis para sua assinatura, bem como limite de usuários e informações sobre as ferramentas obtidas.

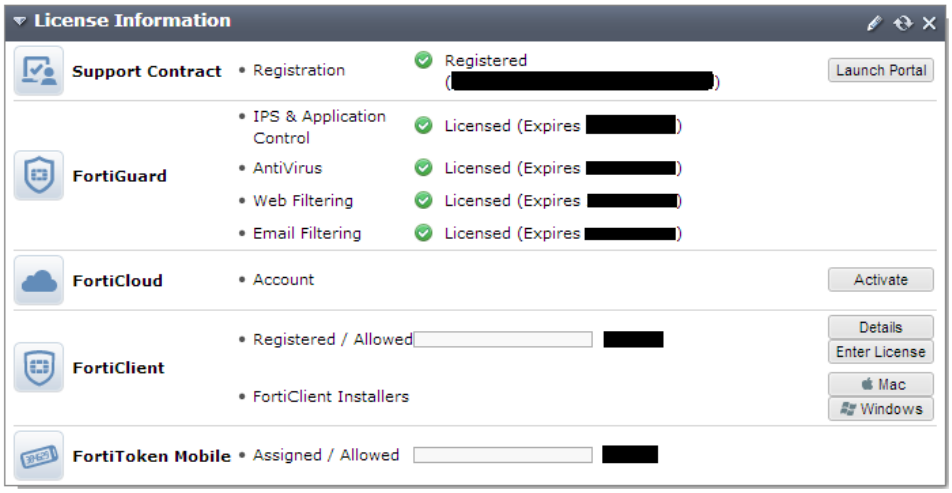

Figura 02 – Informações de licença
Fonte: o autor (2014).

A partir de agora se devem realizar as configurações de segurança, o básico dessa parte se resume a três passos, sendo eles: incluir um endereço de IP, adicionar o roteamento e configurar as políticas de segurança. Tais configurações podem ser realizadas por duas maneiras distintas, a CLI (*Command Line Interface*) mostrada na Figura 03 e a interface baseada em *web* (*web-based manager*) (Figura 04). A interface *web* será utilizada daqui em diante, pois oferece maior praticidade e rapidez nas configurações, embora ambas ofereçam os mesmos recursos.

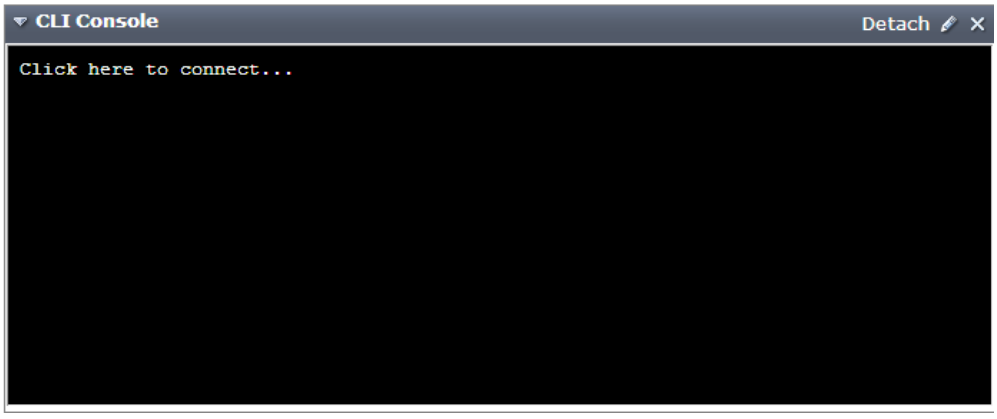

Figura 03 – Command Line Interface (CLI)
Fonte: o autor (2014).

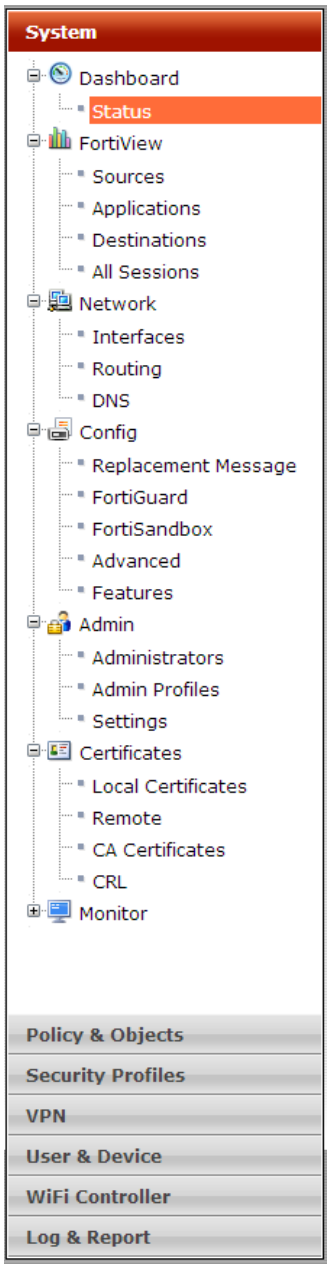

Figura 04 – Web-Based Manager – Menu de Configuração
Fonte: o autor (2014).

Configurando a Interface de Rede: Ao acessar o menu System > Network > Interface, nós podemos configurar interfaces físicas ou virtuais para o FortiGate, uma vez que depende do modo de utilização e do desenho da rede. Aqui vai ser realizada a configuração de uma interface física, de início definindo um nome e um endereço de IP para ela, sendo este pertencente ao mesmo intervalo de endereços da rede interna, e em seguida configuramos a máscara da rede (Figura 05). Dentre as configurações adicionais disponíveis para a interface de rede, devemos indicar o modo de operação, manual, DHCP ou PPPoE. Para o nosso caso, esta será a interface

utilizada para comunicação com a rede interna, então será atribuído um endereço de IP fixo, que também será utilizado como Gateway para a rede.

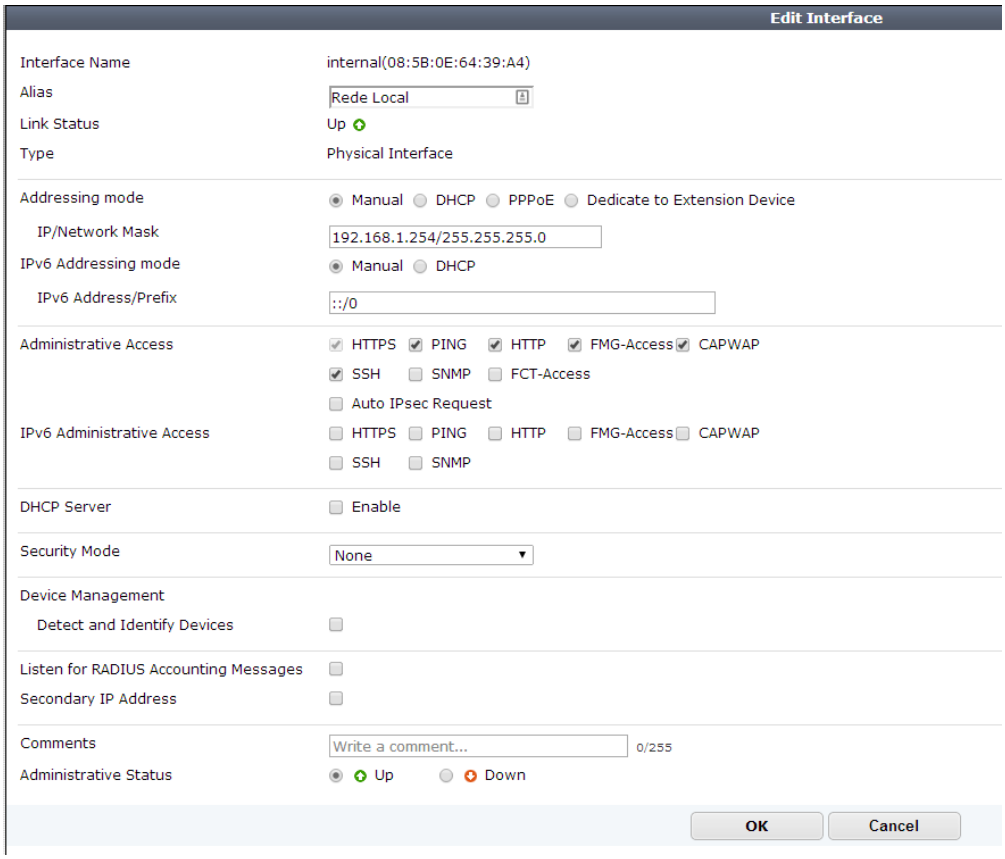

Figura 05 – Criação de Interface Local
Fonte: o autor (2014).

O próximo passo são as interfaces externas, onde nesse caso haverá duas, uma para cada *link* de internet disponível, mas temos que definir o conceito a ser utilizado. Podemos nos valer de três opções de configuração, sendo elas: interfaces redundantes, onde temos uma interface principal que distribui a conexão e quando esta sofre uma queda, uma secundária ocupa seu lugar na distribuição; balanceamento de carga, sendo ambas configuradas para trabalharem juntas e oferecerem uma taxa de saída mais elevada; e uma combinação da redundância com o balanceamento de carga.

A opção a ser utilizada varia conforme a disponibilidade dos *links*, por exemplo, se ao possuir dois links, um deles possui uma velocidade de acesso mais elevada e o outro uma velocidade inferior, podemos configurar a interface referente ao *link* maior como principal e usar a segunda interface como link redundante, garantindo uma conexão em caso de queda da interface principal. Quando ambos os

links oferecem velocidades elevadas, ou um deles possuir um serviço dedicado e normalmente mais caro, o mais indicado é utilizar a opção combinada, onde temos uma redundância e o balanceamento de carga, podendo direcionar serviços que demandam maior banda para determinados links e o restante das conexões para o link de menor capacidade.

Usaremos essa opção de combinação, e nesse caso temos que configurar ambas as interfaces com as informações de acesso do modem que proverá acesso à internet. No cenário atual, ambos os modem realizam a discagem da conexão, sendo responsáveis pela autenticação, assim sendo, deve-se configurar cada interface com um endereço de IP do intervalo ao qual o respectivo modem está configurado. Estas interfaces são as portas WAN, serão elas a se comunicarem com cada modem. A Figura 06 mostra a tela de criação da interface WAN.

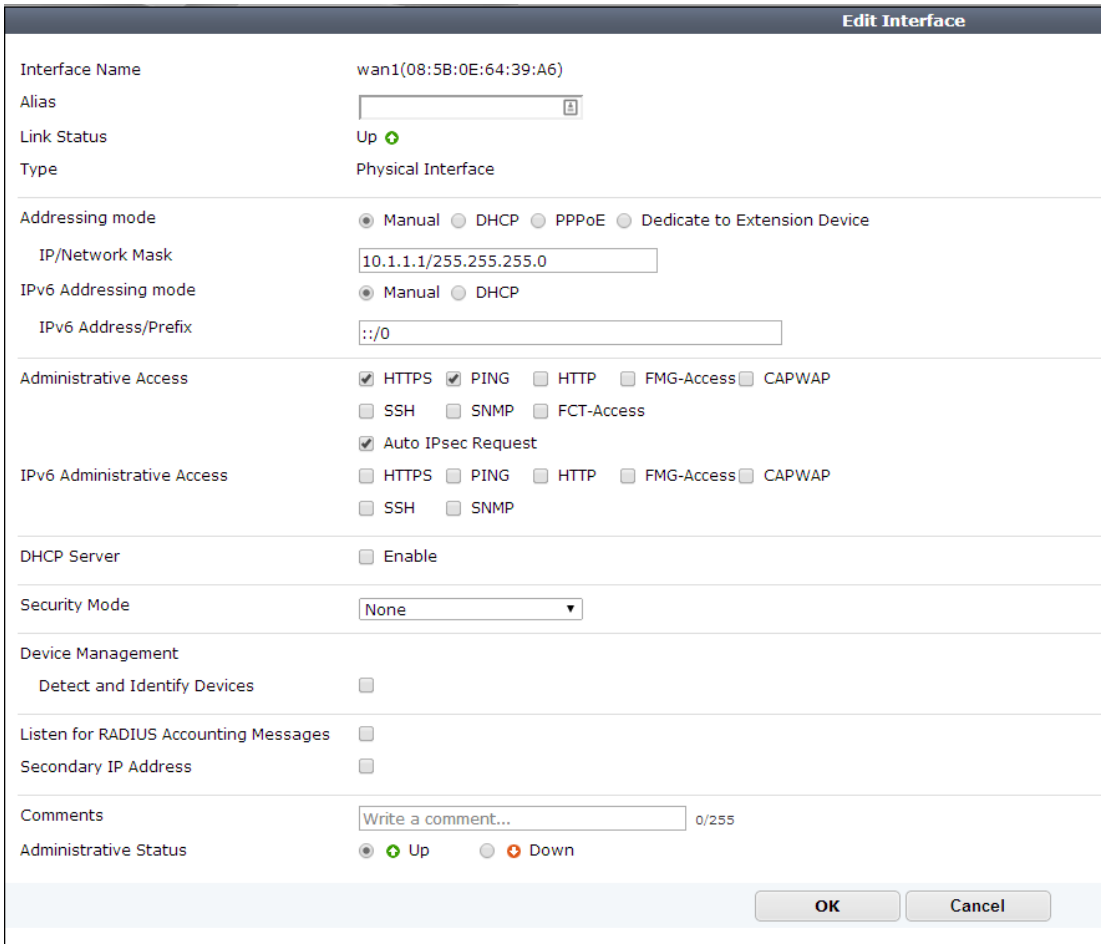

Figura 06 – Criação de Interface WAN
Fonte: o autor (2014).

Deve-se agora configurar o roteamento entre essas interfaces, e é neste momento que definiremos qual interface tem prioridade, definindo a distância de

cada uma. Partindo do princípio que usaremos o modo combinado entre a redundância de link e o balanceamento de carga, definiremos ambas as interfaces com a mesma distância.

No menu de acesso *Router* > *Static* > *Static Routes*, temos acesso à configuração do roteamento das interfaces, devemos criar uma nova (Figura 07), definindo a faixa de rede e a máscara, e em seguida o Gateway de conexão. Nomeie a interface como WAN1 e defina o gateway de conexão, que é o endereço do modem. Em seguida devemos definir a distância. Nas configurações avançadas, usaremos uma distância de valor 10.

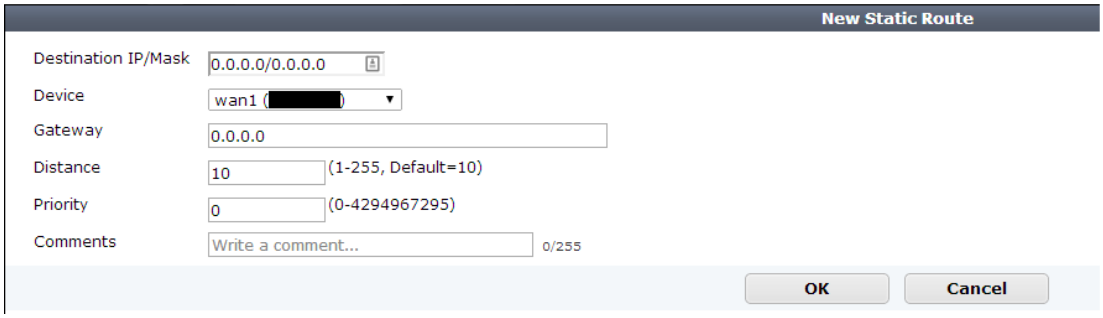

Figura 07 - Roteamento
Fonte: o autor (2014).

Para configurar a segunda interface, o procedimento deverá ser repetido, nomeando a nova interface como WAN2. Desse modo temos nossa configuração básica.

O passo final para esta configuração é definir o conjunto de regras a serem aplicadas, sendo necessário tomar algumas decisões. Antes de tudo temos que definir o modo como iremos começar a implantar as políticas, podemos começar com toda a passagem de informação liberada e bloquear aquilo que desejamos, ou então iniciar com tudo bloqueado e seguir liberando somente aquilo que é necessário. A segunda opção oferece uma menor quantidade de riscos, pois deixa menos possibilidades abertas, e neste ambiente pequeno, é a opção a ser utilizada.

Neste ponto, devemos ter em mãos um planejamento executado, com as características de uso dos usuários da rede e suas necessidades, tais como, softwares e serviços que utilizam conexão com a internet. Para navegação básica, liberar as portas 80 (HTTP) e 443 (HTTPS) garante o acesso a qualquer site que um usuário comum possa acessar, e indo mais além, deve-se efetuar a liberação das portas utilizadas por clientes de e-mail, caso sejam utilizados, e demais serviços presentes.

Feito isso, os próximos passos variam de acordo com a particularidade da rede. Existem serviços que utilizam portas específicas e devem ser acessados de fora da rede, programas de mensagens utilizados para comunicação com fornecedores e clientes, ou seja, tudo que se utilize de uma porta específica.

Não existe meio de se compartilhar uma imagem ilustrativa sobre as portas a serem liberadas sem que informações vitais sejam exibidas, mas essas configurações se dão de forma relativamente simples, seguindo um padrão de vários firewalls presentes no mercado. É utilizado uma fonte de origem do tráfego, seu destino, a porta e o protocolo a ser utilizado e a ação a ser tomada quando um pacote que se encaixe nesse molde seja identificado.

É necessário citar ainda alguns serviços apresentados pelo produto em questão que acrescentam uma grande funcionalidade de controle, o proxy, que define um conjunto de perfis de acesso, onde cada grupo pode ter privilégios diferentes de acesso a sites de internet. O equipamento possui uma lista interna atualizada frequentemente pela fabricante e que contem conjuntos com temas a serem bloqueados, assim como exibido na Figura 08. Este tipo de opção depende de um sistema de autenticação de usuários, o qual pode ser uma integração com AD (*Active Directory*), comumente utilizado e disponível na rede desta empresa. Ele fornece a identificação dos usuários, e utilizado em conjunto com os grupos de segurança, fornecem o necessário para que se possa administrar o acesso dos usuários na navegação de internet.

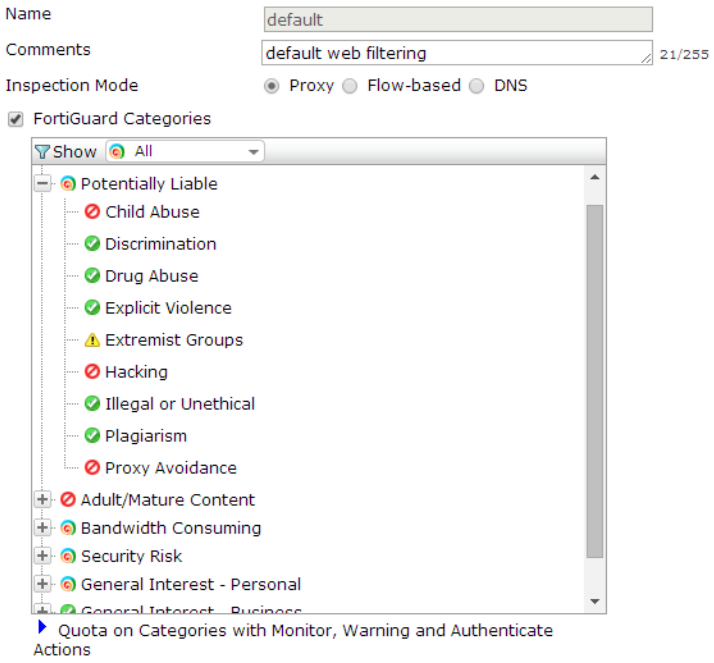

Figura 08 – Filtro de Conteúdo
Fonte: o autor (2014).

Na lista de conteúdos, podem-se definir por liberar ou não diversas categorias de acesso, podendo-se ainda efetuar liberações ou bloqueios a URLs específicas. Embora essa seja uma ferramenta muito prática, sites que utilizem protocolo HTTPS para navegação segura, é uma questão diferente, pois os dados incluídos nos pacotes de dados são encriptados, não sendo possível então a verificação do destinatário. Vários sites podem acabar escapando de bloqueios dessa forma, como por exemplo, redes sociais, que tomam muito tempo de utilização em empresas e que é comumente alvo de bloqueios. Para uma medida eficiente, nesse caso deve-se aplicar uma restrição de endereço de IP, observando cada um dos endereços de IP do site a ser restringido, pois grandes portais possuem vários intervalos de endereços.

O processo de implantação é realizado fora de horário de expediente, sendo no próximo dia útil da empresa feito a validação do processo. O consultor responsável pela execução do projeto acompanha esse primeiro dia localmente, sendo este o início da fase de pós-implantação, além disso, nos próximos 4 dias haverá acompanhamento remoto direto, estando este pronto para realizar intervenções caso haja necessidade.

A última etapa ocorre posteriormente, cerca de 50 dias após o término da implantação, neste momento a equipe técnica realiza uma análise das estações ativas

da rede, semelhante a inicial. Nessa avaliação, foi constatado que nenhuma das estações possuía falhas semelhantes às detectadas no início, pois o acesso a arquivos de instalação e sites prejudiciais as máquinas já não era mais possível.

3. RESULTADOS

As estações ao final dos procedimentos encontram-se todas com sistema operacional atualizado, sendo que 20% delas usavam Microsoft Windows XP, o qual não possui mais atualizações de segurança fornecidas pela fabricante. Elas foram atualizadas para o Microsoft Windows 7 durante o processo de formatação e juntamente com os 10% de estações que rodam Microsoft Windows 8, tiveram as últimas atualizações de segurança instaladas.

Em comparação ao ambiente encontrado, é esperado haver uma redução de mais ou menos 70% no volume de atendimentos de suporte às estações. Hoje existe um contrato de suporte com valor fixado por estação, mas a realidade anterior previa gastos superiores ao contrato atual, pois o atendimento era realizado por demanda e gerava gastos constantes, visto que o ambiente não possuía qualquer forma de controle ou restrição de ameaças.

Outro importante fator a mencionar, o plano de internet usado anteriormente não suportava a demanda das requisições, sendo uma constante reclamação por parte dos funcionários. A empresa estudava realizar um *upgrade* do plano para um com maior velocidade, gerando uma despesa maior e que não traria resultados satisfatórios. Com a implantação do equipamento de *firewall*, restrições de acesso a sites e serviços não essenciais ao escopo da empresa, o plano de internet existente atende a demanda com folga, tendo sido contrato um segundo *link* com velocidade inferior para fins de redundância e disponibilidade para eventuais falhas, as quais todo serviço está sujeito.

Segundo a empresa, os supervisores notaram aumento na produtividade, levando em conta que períodos de trabalho antes usados para fins pessoais e ociosidade devido à liberdade de navegação, hoje não acontecem. Existe uma lacuna de intervalos fixos em cada período de trabalho destinado à livre navegação, embora ainda sujeita às regras, onde o funcionário pode utilizar de breve período para distração ou entretenimento.

Levando em consideração a segurança acrescentada ao ambiente, não é possível citar uma situação específica onde o *firewall* tenha impedido um ataque orquestrado a rede da empresa, mas é essencial dispor dessa segurança para que tais atos não possam se tornar realidade.

Os passos apresentados até aqui garantem uma configuração segura, na qual apenas o necessário é permitido e todo o resto é bloqueado. Como citado anteriormente, ao final do projeto, o ambiente encontra-se livre de ameaças detectáveis. Tudo isso através de uma forte estruturação de políticas de segurança, complementadas com funcionalidades de gerenciamento que permitem a emissão de relatórios detalhados de acesso, permissões e restrições aplicadas. A Figura 09 ilustra a topologia aproximada da rede após a conclusão do projeto.

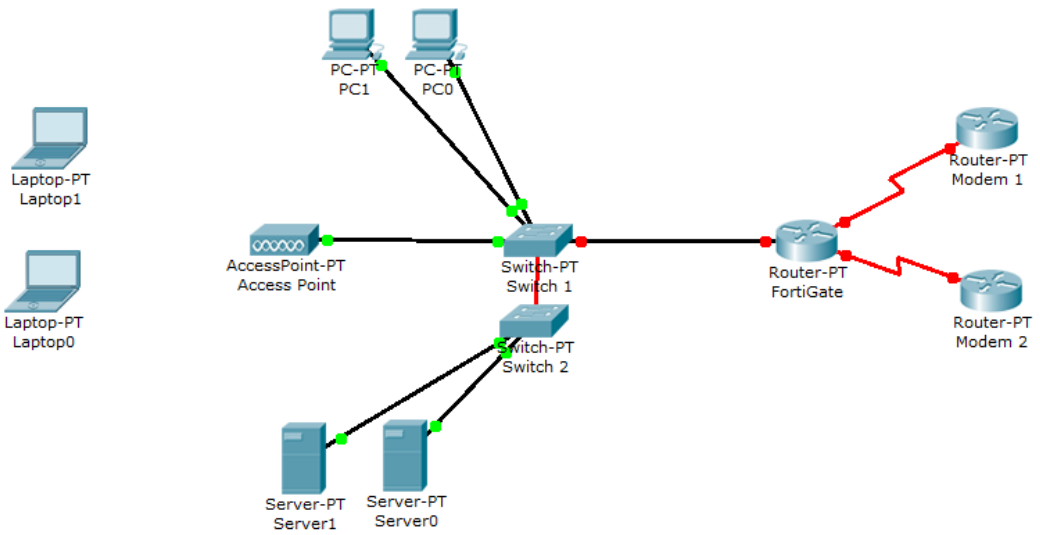

Figura 09 – Topologia aproximada da rede.
Fonte: o autor (2014).

A topologia da empresa durante o período que antecedeu a implantação não possuía o segundo modem, sendo que o primeiro era também usado como distribuidor DHCP e gateway direto da rede.

O equipamento utilizado possui uma série de vantagens que o qualificam como uma forte ferramenta de segurança, podendo dizer que neste momento a rede da empresa possui um nível completamente diferente de segurança em relação ao

período anterior à implantação do projeto. Podemos citar uma das várias características do equipamento, como o *FortiGate DoS Protection*, que utiliza técnicas avançadas para reduzir os efeitos sofridos por um ataque de negação de serviço.

Esse tipo de ataque é muito difícil de prevenir completamente, uma vez que tenta sobrecarregar o alvo com inúmeras requisições, ao ponto em que não seja possível identificar requisições verdadeiras das falsas, impedindo o acesso ao serviço alvo. O *DoS Sensor*, ferramenta interna do FortiGate, procura por anomalias específicas no tráfego e identifica o que em meio a todo o tráfego tem o potencial para causar um ataque de negação de serviço, podendo detectar 12 tipos de anomalias de rede.

Outro ponto que merece destaque é o serviço de pesquisa e testes da FortiNet, que mantêm uma equipe dedicada à descoberta de novas vulnerabilidades (*Zero-day*) e formas de prevenção, disponibilizando atualizações rápidas aos produtos da empresa. Existe um canal de relacionamento com a empresa responsável pela análise de vulnerabilidades reportadas pela comunidade, garantindo que seus produtos possam ser atualizados da maneira mais rápida.

Sempre que novas ameaças são descobertas em aplicações *web*, as informações referentes são repassadas aos equipamentos FortiGate, através de um canal de atualização automática.

4. DIFICULDADES ENCONTRADAS

Durante o período de duração do estágio, uma das maiores dificuldades ocorreu durante a fase de recolhimento de informações da empresa para estruturar o projeto da implantação do *firewall*, pois o ambiente encontrava-se em estado debilitado devido à má gestão de TI realizado antes da equipe da Becker Consultoria assumir esta responsabilidade. A análise minuciosa realizada na preparação do ambiente se mostrou custosa devido ao número de estações que tiveram que passar por reparos para que não ocorresse nenhum problema posterior à implantação do firewall.

O processo de formatação sofrido pelas estações tomam um grande tempo, pois este procedimento exige cuidados como *backup* prévio de dados do usuário e dedicação póstumo para configuração de acordo com o padrão utilizado pela empresa. No final das contas, são utilizadas quase 12 horas para cada estação.

Durante a fase de suporte pós-implantação, surgiu a necessidade de adequação das políticas de segurança para realizar a liberação de um serviço que não havia sido reportado anteriormente. Tal serviço era utilizado por um pequeno setor da empresa e ficou suspenso até que fosse realizada a análise e determinada qual porta de acesso era usada.

Ao final, foi necessário um trabalho em conjunto com a administração da empresa para conscientizar os funcionários da necessidade de se realizar as mudanças aplicadas, pois o ambiente se encontrava em um nível sem gerenciamento, onde os funcionários possuíam acesso livre a quaisquer sites ou sistemas que desejassem. Para tanto, foi realizada uma reunião entre as equipes, onde pudemos apresentar detalhes que instruíssem os funcionários sobre o funcionamento das ferramentas implantadas, explicando o motivo exato da necessidade delas e como isso traria benefícios não somente a empresa como também a eles, pois suas ações afetam diretamente o funcionamento da empresa.

5. CONCLUSÕES

O projeto implantado na empresa em questão serviu para adicionar não apenas uma camada extra de segurança à rede, como também para garantir que houvesse um melhor gerenciamento dos recursos disponíveis. Através dos relatórios gerados pela ferramenta, tais como sites e serviços acessados, administradores são capazes de analisar melhor a distribuição de tarefas, tais como áreas que demandam mais atenção ou outras que possuem maior ociosidade. São também capazes de gerenciar a utilização da infraestrutura da empresa, garantindo que não haja desperdício de recursos que existem para o bom andamento da empresa e que antes eram utilizados para fins pessoais de funcionários.

A segurança dos dados da empresa é agora relevante, pois partiu de um nível inexistente. O trabalho realizado está no início, pois com o ambiente melhor estruturado e com a atenção que conseguimos dar a esta questão, devemos introduzir a empresa assuntos novos, capazes de preencher lacunas que antes não eram vistas, como por exemplo, soluções de gerenciamento de e-mails corporativos, capazes de oferecer maior nível de gestão e segurança, além de sistemas de backup, fundamentais para garantir uma recuperação em caso de acidentes ou imprevistos.

Não existe um ponto final onde se deixa de evoluir. Novas tecnologias surgem a cada dia e é parte do trabalho de um profissional de TI estar sempre informado sobre novas ameaças ou áreas de risco e também formas de se prevenir. Realizar um bom trabalho para seus clientes é garantir que todas as áreas possíveis sejam abordadas, pois quando se trata de segurança, deve-se sempre estar atento.

O próximo passo a ser sugerido ao cliente será um serviço de AD, onde há a possibilidade de se manter um controle rígido das estações, restringindo acesso a configurações do sistema e permissões em arquivos e compartilhamentos por usuário.

6. REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL, Dell. **Empresas brasileiras projetam investir até R$ 110 mil em Segurança da Informação em 2013**.: 2013. Disponível em: <http://www.dell.com/learn/br/pt/brcorp1/press-releases/2013-10-04-pesquisa-dell-sonicwall-1>. Acesso em: 08 ago. 2014.

DATA, Dimension. **Network Barometer Report 2014**.: 2014. Disponível em: < http://www.dimensiondata.com/Global/Global-Microsites/NetworkBarometer/Documents/assets/PDF/Network_Barometer_Report_2014.pdf>. Acesso em: 11 ago. 2014.

FORTINET. **FortiOS™ Handbook:** Install and System Administration for FortiOS 5.0.: 2014. Disponível em: <http://docs.fortinet.com/uploaded/files/1087/fortigate-install-system-admin-50.pdf>. Acesso em: 02 jul. 2014.

HAZARI, Sunil. **Firewall For Beginners**.: 2000. Disponível em: <http://www.symantec.com/connect/articles/firewalls-beginners>. Acesso em: 20 jul. 2014.

LAB, Kaspersky. **El panorama viral em América Latina durante la primera mitad del 2013**.: 2013. Disponível em <http://latam.kaspersky.com/2013h1malware>. Acesso em: 09 jul. 2014.

MEDEIROS, C. D. R. **Segurança da Informação:** Implantação de Medidas e Ferramentas de Segurança da Informação.: 2001. Disponível em: < http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf>. Acesso em: 07 ago. 2014.

STALLINGS, William. **Criptografia e Segurança de Redes**. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

TERADA, Routo. **Segurança de dados:** Criptografia em redes de computadores. 2. ed. São Paulo: Blucher, 2008.

WEBSENSE. **Exposing the cybersecurity cracks:** A global perspective.: 2014. Disponível em: <http://www.websense.com/content/2014-ponemon-report-part-2.aspx?cmpid=prnr7.17.14>. Acesso em: 08 ago. 2014.