Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

TIAGO AQUINO FERNANDES LOPES

PROPOSTA DE *HARDENING* PARA *FIREWALLS* DE UMA INSTITUIÇÃO BANCÁRIA

BRASÍLIA

2016

TIAGO AQUINO FERNANDES LOPES

PROPOSTA DE *HARDENING* PARA *FIREWALLS* DE UMA INSTITUIÇÃO BANCÁRIA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança

Orientador: Prof. Dr. José Eduardo M. S. Brandão

BRASÍLIA

2016

TIAGO AQUINO FERNANDES LOPES

PROPOSTA DE *HARDENING* PARA *FIREWALLS* DE UMA INSTITUIÇÃO BANCÁRIA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança

Orientador: Prof. Dr. José Eduardo M. S. Brandão

Brasília, ___ de dezembro de 2016.

Banca Examinadora

_____

Prof. Dr. José Eduardo M. S. Brandão

_____

Prof. MSc. Marco Antonio Araújo

_____

Prof. Dr. Gilson Ciarallo

A todos que me deram
a força que me faltou.

RESUMO

O processo de *hardening* nos *firewalls* envolve muito mais do que manter senhas fortes e políticas de segurança complexas. São o conjunto de pequenas ações de segurança que visem incrementar gradativamente, e em camadas, o nível geral de segurança no uso diário dos equipamentos. Este trabalho aborda diversos aspectos de configuração nos firewalls de um ambiente específico na Instituição Banco X, trazendo exemplos de vulnerabilidades identificadas e apresentando caminhos para que o ambiente seja fortalecido como um todo, a partir da correta configuração de seus firewalls, demonstrando que o processo de *hardening* de equipamentos de *firewall* é realizado em diversas atividades.

Palavras-chave: firewall. hardening. estudo de caso.

ABSTRACT

The hardening process in firewalls involves much more than maintaining strong passwords and complex security policies. They are a set of small security actions that aim to gradually increment, and in layers, the general level of security in daily use of equipment. This work addresses several aspects of configuration in the firewalls of a specific environment in the Bank X Institution, bringing examples of identified vulnerabilities and presenting ways for the environment to be strengthened as a whole, from the correct configuration of its firewalls, demonstrating that the process of Hardening of firewall equipment is carried out in various activities..

Keywords: firewall. hardening. case study.

Lista de Ilusrações

Lista de Quadros

SUMÁRIO

INTRODUÇÃO

A indústria bancária está caminhando cada vez mais para o modelo digital, em prejuízo ao antigo modelo de agências físicas e transações realizadas com o atendente no caixa. Das antigas planilhas preenchidas a mão para controle de saldo nos anos 70, aos bancos completamente digitais que dispomos hoje por meio de aplicativos móveis, a sociedade, e a Federação Brasileira de Bancos (FEBRABAN) já perceberam que o meio digital, mais que uma tendência, é um caminho sem volta.

Na sua última Pesquisa FEBRABAN de Tecnologia Bancária 2015 (FEBRABAN, 2015), a entidade destaca o crescimento de mais de 138% das transações eletrônicas em comparação com 2014, e a incrível cifra de 19 bilhões de reais investidos em tecnologia pela indústria bancária apenas em 2015.

Nakamura e Geus (2003) alertam que os avanços tecnológicos vêm resultando em grandes oportunidades de negócios, porém, quanto maior essa evolução, maiores as vulnerabilidades que aparecem e devem ser tratadas com a sua devida atenção.

Não é difícil imaginar os motivos que fazem da indústria bancária um alvo estratégico para criminosos digitais. Ainda segundo a FEBRABAN, no ano passado os bancos registraram perdas de 1,8 bilhão de reais em fraudes eletrônicas.

A ameaça pode estar em qualquer parte do mundo, fazendo uso de um computador, ou dentro da própria empresa, com ou sem dolo nas práticas lesivas ao sistema de informação do banco.

Uma saída comum e muito eficiente é o *hardening*, que é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas (DIOGENES; MAUSER, 2011).

Optou-se por restringir, nessa atividade, o processo de *hardening* apenas para os equipamentos de *firewall*, para desmistificar o conceito que os mesmos são meros controladores de acesso entre usuários e serviços.

Visando agregar mais elementos seguros nos equipamentos, trouxemos de recomendações de fabricantes e de levantamentos feitos em campo, uma série de medidas corretivas para serem aplicadas nos *firewalls*.

Com o objetivo de tornar mais fácil o entendimento, este trabalho está dividido em cinco partes.

Inicialmente, o trabalho apresentará, em seu segundo capítulo, a revisão conceitual abordada no documento, com as definições de segurança, *hardening*, *firewalls* e alguns protocolos implementados.

Adiante, no capítulo terceiro, será apresentado o ambiente da Instituição Banco X alvo da proposta de *hardening*, com levantamento de fabricantes, modelos de equipamentos e situação de momento a respeito de configurações de segurança. Ao final, esses dados serão compilados em um quadro de riscos.

Avançando pelo capítulo quarto, a proposta de *hardening* será apresentada, visando mitigar cada um dos riscos apontados no capítulo anterior. Ao final, esses dados serão compilados em um quadro de ações.

Após, no quinto capítulo, os dois quadros, de riscos e ações, serão cruzadas para dar origem qo quadro Matriz de Riscos x Ações.

Por fim, uma conclusão será apresentada no sexto capítulo revisitando todo o conteúdo abordado no trabalho.

1 REVISÃO CONCEITUAL

1.1 Segurança

Para Stallings (2008), a segurança é um serviço de processamento ou comunicação que é fornecido por um sistema para prover um tipo específico de proteção aos recursos do sistema. Os serviços de segurança implementam políticas de segurança e são implementados por mecanismos de segurança, divididos em cinco categorias: Autenticidade, Controle de Acesso, Confidencialidade, Integridade e Irretratabilidade.

Inicialmente, o serviço de autenticidade provê a garantia de que uma comunicação é autêntica. Ou seja, garantir ao destinatário, que a mensagem recebida é proveniente de onde ela afirma ser (STALLINGS, 2008).

Stallings (2008) prossegue apontando que o controle de acesso trata da capacidade de limitar o acesso aos sistemas e aplicações hospedeiras, identificando cada entidade antes que o acesso seja concedido e analisado.

Continua Stallings (2008), destacando que o serviço de confidencialidade é responsável por proteger os dados transmitidos contra ataques durante a transmissão. Um exemplo fácil de imaginar é uma transmissão de e-mail entre servidores através da internet. A confidencialidade, por meio de uso de métodos de criptografia, consegue garantir que a mensagem chegue ao destino sem que seu conteúdo seja lido durante a transmissão.

Tão importante quanto manter a confidencialidade, é manter a integridade da informação. Garantir que a mensagem que saiu do emissor, é a mesma, integralmente, que chegou ao receptor. Esse serviço garante que se a integridade da mensagem for violada, o sistema de segurança o detectará e informará aos envolvidos (STALLINGS, 2008).

A irretratabilidade previne que os envolvidos na comunicação neguem o seu envio ou recebimento. Dessa forma, o emissor sempre pode comprovar que o emissário indicado, de fato enviou a mensagem, e por outro lado, o emissário pode provar que o receptor a recebeu, a despeito de outras argumentações contrárias (STALLINGS, 2008).

1.2 *Hardening*

Hardening é o processo de reforço de segurança de sistema, no qual todos os componentes interconectados em uma rede e que fazem uso dele, como dispositivos, sistemas e aplicativos, terão diretrizes especificas de reforço de segurança (DIOGENES; MAUSER, 2014).

O conceito do *hardening* pode ser aplicado a quaisquer áreas que envolvam segurança da empresa, sejam ambientes ou estações de trabalho.

Se pensássemos no terminal de trabalho, poderíamos descrever o *hardening* desse equipamento como um conjunto de ações de segurança, atuando em diferentes camadas, que diminuam o risco desse equipamento ser vítima de ataques maliciosos. Essas ações, pensando num computador, iriam desde manter o sistema operacional e aplicativos atualizados, à instalação de *softwares* antivírus e anti-spyware, passando por desabilitação de serviços não utilizados de servidores de arquivo e outras funções do sistema operacional.

Quando trazemos o processo de *hardening* para o parque de *firewalls* da instituição Banco X, devemos encará-lo da mesma maneira, embora adaptando as ações ao ambiente.

Infelizmente, não existe uma norma padrão ou recomendação formal para para a promoção do *hardening* nos equipamentos *firewalls*. Contudo, alguns fabricantes publicam documentos com atividades a serem tomadas visando o incremento na segurança de seus equipamentos contra eventos maliciosos.

A Fortinet, fabricante dos *firewalls* Fortigate, elenca uma série de ações (FORTINET, 2015) que o usuário deve tomar para incrementar a segurança ao acesso administrativo de seus produtos, as quais, destacamos:

- Instalar o *firewall* em um local fisicamente seguro;
- Manter o *firmware* atualizado;
- Adicionar novas contas de administrador;
- Alterar o nome da conta *admin* padrão;
- Permitir acesso administrativo por interface externa apenas quando necessário;
- Quando permitir acesso remoto, configurar redes de origem confiáveis e autenticação em dois níveis;
- Alterar a porta padrão de acesso administrativo para uma porta não padrão;
- Alterar o nome do dispositivo;
- Fazer o registro do suporte de serviços;
- Estabelecer tempos de expiração curtos para os acessos;
- Habilitar sincronização automática do relógio;
- Definir uma política de senhas;
- Desabilitar auto instalação via *USB*; e
- Configurar a auditoria e coleta de *logs*.

Apesar de serem recomendações de um fabricante específico, consideramos que essas recomendações podem ser estendidas aos demais, visto que se tratam de recomendações que independem de arquitetura, sistema operacional ou protocolo proprietário.

Percebe-se que o processo de *hardening* não é um processo imutável, mas um método de incremento de segurança em camadas, com alta capacidade de adaptação a diferentes cenários, ficando a cargo do responsável pelo ambiente, investigar e levantar junto aos fabricantes progressivas ações que levem ao resultado pretendido.

O processo é contínuo e progressivo. Constantemente deve-se identificar novas ações que melhorem o nível geral de segurança dos ambientes.

1.3 *Firewall*

Firewall é um ponto entre duas ou mais redes, no qual circula todo o tráfego. A partir desse único ponto, é possível controlar e autenticar o tráfego, além de registrar, por meio de logs, todo o tráfego da rede, facilitando sua auditoria (NAKAMURA; GEUS, 2003).

Inicialmente, os *firewalls* eram filtros de pacotes. As primeiras tentativas de tornar o TCP/IP seguro se basearam na ideia de que é bastante fácil para um roteador inspecionar o cabeçalho dos pacotes (STREBE; PERKINS, 2002).

Há dois tipos básicos de filtragem de pacote:

- Padrão ou filtragem de pacotes sem estados (*stateless*); e
- Filtros de pacotes com inspeção de estados (*stateful*).

Filtros de pacotes sem estado podem ser configurados para operar com base em qualquer parte do cabeçalho de pacote individual, mas a maioria é configurada para filtrar os campos de dados mais úteis, como o tipo de protocolo, endereços IP, e portas TCP/UDP.

Os protocolos mais comuns são os tipos UDP, TCP, ICMP e IGMP. Num filtro por tipo de protocolo hipotético, o administrador precisa liberar, para fins de gerenciamento, os pacotes ICMP (CHESWICK; BELLOVIN; RUBIN, 2005) para que servidores respondam à solicitações *PING* (CHESWICK; BELLOVIN; RUBIN, 2005) em redes distintas. Esse tipo de filtro é tão genérico que pouco é usado no dia-a-dia.

A filtragem de pacotes por endereços IP permite limitar as conexões para e de *hosts* e rede específicos com base em seus endereços IP (STREBE; PERKINS, 2002). Basicamente, o *firewall* recusa todas as conexões, exceto as permitidas; ou aceita todas as conexões, exceto as proibidas. Preferencialmente, se configura o firewall com filtragem de redes permitidas, negando todas as demais conexões.

Os pacotes ainda podem ser filtrados por portas de serviço TCP/UDP. Essa também são habituais na filtragem de pacotes, pois concentram a esmagadora maioria do tráfego analisado pelos *firewalls*. São protocolos comuns filtrados nessa categoria, o HTTP, HTTPS, FTP, Telnet, DNS, SMTP, e assim por diante.

A filtragem de pacotes sem estado sofre de dois problemas. Em primeiro lugar, analisam apenas o cabeçalho do pacote, sem verificar o conteúdo em busca de dados perigosos ou malformados. Em segundo lugar, não guardam o estado da conexão. Sendo assim, não estabelecem uma tabela de sessões ativas no *firewall*, analisando cada pacote individualmente, incluindo as respostas das conexões. Por esse motivo, os *firewalls* precisam ser configurados para deixar passar todas as portas TCP no intervalo de retorno normal, acima de 1024.

Os *firewalls* modernos usam a informação de estado para acompanhar o status da conexão e, dessa maneira, conseguir controlar de forma mais posistiva o roteamento de pacotes pela rede (STREBE; PERKINS, 2002).

Os filtros de pacotes de inspeção com estado (*stateful*), retém na memoria os estados de todas as comunicações que passam pelo *firewall* e usam essa informação para determinar se os pacotes devem ou não ser abandonados. A inspeção filtra fluxos de comunicação inteiros, e não apenas os pacotes (STREBE; PERKINS, 2002).

Para entender melhor essa definição, tomemos o seguinte exemplo. Quando um host e conecta a um soquete TCP em um host externo, ele transmite no pacote de sincronização da conexão o soquete (endereço IP e porta) no qual ele espera receber uma resposta. Ou seja, hipoteticamente, eu faço uma requisição na porta TCP 80, já indicando que receberei a resposta na porta 3000. Esse pacote, denominado SYN, é direcionado pelo filtro de pacotes com estado, e é adicionado a uma tabela de estados. No retorno do pacote, o *firewall* analisa a tabela de estados para confirmar se aquela resposta em direção à porta 3000 havia sido registrada na tabela de estados. Caso não existisse, o *firewall* descartaria o pacote. Esse era um tipo comum de ataque na filtragem de pacote sem estado. Usuários maliciosos simulavam uma resposta à uma requisição, se aproveitando da liberação das portas acima de 1024, para injetar pacotes numa rede.

Os registros da tabela de estado são removidos (i.e., as sessões são encerradas) quando pacotes específicos de encerramento de sessões são enviados por um dos agentes da conexão, ou depois de um tempo pré-determinado de inatividade.

Neste trabalho trataremos apenas dos *firewalls* com filtragem de pacote *stateful*, já que é o caso da totalidade dos equipamentos presentes no ambiente estudado.

Os *firewalls* ainda podem ser classificados de acordo com a sua arquitetura. Destacam-se três entre as mais comuns: *bastion host*, *screened subnet*, e *mult-hommed*.

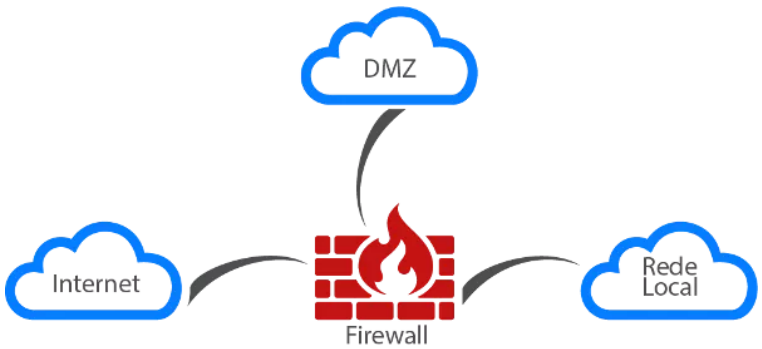
A arquitetura *bastion host* é a mais comum para a maioria dos pequenos ambientes. O *firewall* é posicionado entre a duas redes onde seja necessário controlar o acesso entre ambas, por exemplo, entre a *internet* e a rede local de uma empresa, conforme a figura 1:

Figura 1 - Arquitetura Bastion Host

Essa arquitetura oferece apenas uma camada de proteção e não deve ser utilizada para proteger servidores dentro da rede local; apenas para controlar o acesso da rede local à internet. Não se aplicaria, portanto, a um cenário onde a empresa proveja algum serviço a ser acessado a partir da internet.

Incrementando o grau de segurança e usabilidade, temos a arquitetura *screened subnet*, também conhecida como subnet com triagem, que permitem que as empresas ofereçam serviços pela internet, sem o comprometimento da rede local. Conforme a figura 2 a seguir, observamos que o *firewall* necessita de, ao menos, três interfaces físicas, para que se possa isolar o acesso externo (internet), do interno (rede local), e da Zona Desmilitarizada (DMZ).

Figura 2 - Arquitetura Screened Subnet



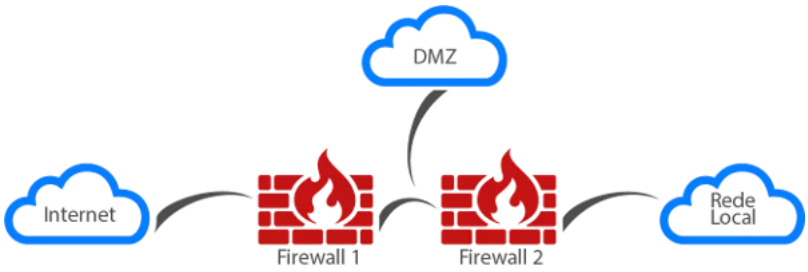
A DMZ é uma sub-rede que contém e expõe serviços externos de uma organização para acesso a partir de uma rede maior não-confiável, como a internet. Ao segregar seus servidores de web, e-mail, arquivos, e etc, a organização blinda sua rede local contra acessos externos, principais fontes de risco às redes protegidas.

Na arquitetura apresentada deve-se ter o cuidado de permitir que acessos externos possam ser realizados apenas nos servidores dentro da estrutura DMZ, de forma a garantir os benefícios dessa arquitetura.

Por último, a arquitura *multi-homed* vem complementar a sub-rede com triagem. Ainda com a previsão de uma estrutura DMZ, essa arquitetura prevê a instalação de dois ou mais *firewalls* para controlar o acesso entre as redes.

No ponto mais externo da rede, o *firewall* de acesso, que controla as requisições externas aos servidores hospedados na DMZ. No ponto mais interno, o *firewall* interno que controla o acesso da rede local ao ambiente externo da rede, como observado na figura 3 a seguir:

Figura 3 - Arquitetura Multi-Homed



Nessa arquitetura, ainda que o *Firewall* 1, o externo, fosse comprometido, o invasor ainda não teria acesso ou conhecimento à rede local, tornando ainda mais difíceis ações mal intencionadas contra a rede local.

É essa a arquitetura empregada na maior parte do Ambiente Central da Instituição Banco X.

Um *firewall* pode ser implementado via equipamento dedicado ou software, ainda, apesar de fundamental, não garante por si só a segurança de uma organização, (NAKAMURA; GEUS, 2003).

A função básica de um *firewall*, é a análise de pacotes para seu bloqueio ou permissão, através de *policies*.

As *policies* são regras de *firewall*. A estrutura básica de uma regra de *firewall* consiste em objeto de origem, objeto de destino, serviço, e ação a ser tomada.

Objetos são elementos cadastrados com informações de endereços IP de determinadas máquinas, sequência de endereços, ou redes inteiras. Os objetos cadastrados podem ser usados tanto como objetos de origem como de destino, em uma ou várias *policies*. Os *firewalls* ainda permitem criar grupos de objetos para facilitar a visualização na exibição das *policies*.

O serviço é o protocolo e porta utilizada naquela regra. Podem ser cadastrados como elementos únicos, por exemplo TCP 80, ou sequência de portas, como as conhecidas "portas altas", que são portas TCP de 1024 a 65535. Um conjunto de serviços individuais também podem ser agrupados em um um elemento de grupo para uso na *policy*.

A ação a ser tomada é simplesmente a escolha entre negar e permitir aquele tráfego descrito.

Como exemplo de *policy*, se um usuário da REDE_INTERNA necessita de um acesso à porta TCP 80 na REDE_DMZ, o responsável pelo *firewall*, então, cria uma nova regra, configurando-a com REDE_INTERNA como objeto de origem, REDE_DMZ como objeto de destino, TCP 80 como serviço, e PERMITIR como ação (quadro 1):

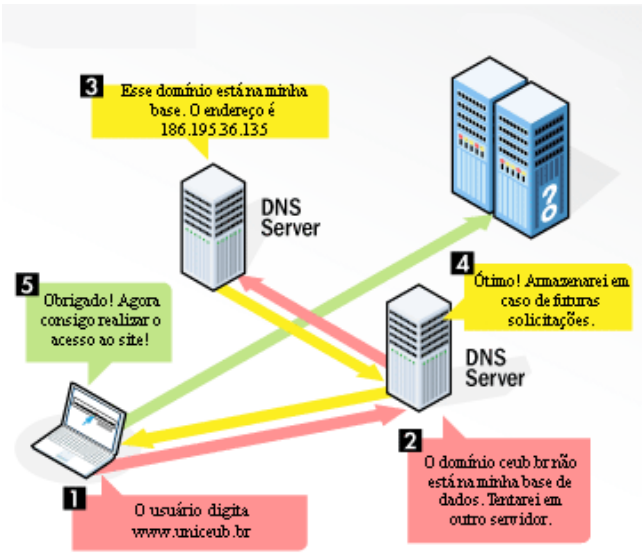
Quadro 1 - Exemplo de policy

Objeto de Origem	Objeto de Destino	Serviço	Ação
REDE_INTERNA	REDE_DMZ	TCP 80	permitir

1.4 *Domain Name System* (DNS)

O Domain Name System (DNS) é um sistema globalmente distribuído que depende da interação cooperativa de muitos servidores de DNS para armazenar registros sobre domínios e para se comunicar uns com os outros (NORTHCUTT; NOVAK; MCLACHLANM, 2001). Em outras palavras, servidores de DNS traduzem endereços amigáveis, como *www.exemplo.com*, em endereços IP que podem ser roteados através da rede. A figura a seguir demonstra didaticamente como funciona uma requisição DNS:

Figura 4 - Funcionamento do DNS



Inicia-se o processo com o usuário digitando o endereço a ser visitado (1). A consulta DNS é encaminhada ao servidor indicado nas configurações de rede do terminal do usuário, mas esse não tem o registro da resolução daquele nome (2). A consulta é, então, encaminhada a outros servidores DNS até que um outro responda com a resolução solicitada (3). O resultado retorna ao servidor DNS inicial, que inclui aquele endereço em seus registros para uso em futuras consultas semelhantes (4). Por último, o usuário recebe a resolução do nome e consegue navegar no site pretendido (5).

1.5 *Network Time Protocol* (NTP)

O Network Time Protocol (NTP) é um protocolo usado para sincronizar o relógio de uma máquina com o mundo externo. O NTP suporta a sincronização com relógios atômicos ou relógios de rádio sintonizados com serviços nacionais de data/hora (CHESWICK; BELLOVIN; RUBIN, 2005).

Atualmente a correta configuração e padronização desse protocolo mostra-se crítica por que todos os aspectos do gerenciamento de segurança envolvem o momento em que determinados eventos ocorreram. A medida do tempo é a única janela de referência de um evento através de todos os elementos da rede.

Investigar falhas de segurança, consumo de banda excessivo ou determinado problema afetando um grande número de componentes numa rede pode se tornar praticamente inviável se os logs dos equipamentos estiverem com o serviço de tempo desconfigurado.

2 ESTUDO DE CASO - A INSTITUIÇÃO BANCO X

2.1 Descrição da Empresa

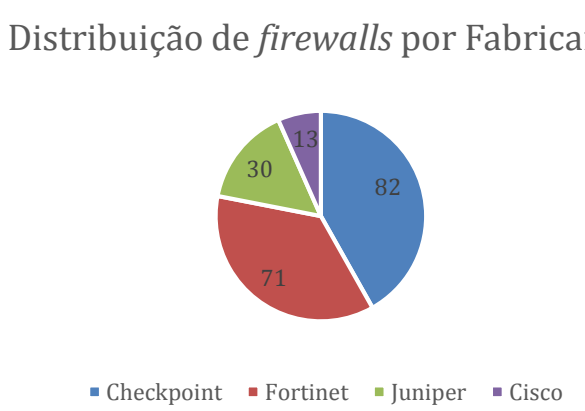
A instituição Banco X é uma das maiores empresas do ramo no país e na América Latina. Possui negócios com clientes pessoas físicas, jurídicas e governo por todo o território nacional, além de contar com agências e escritórios em todos os continentes, para atender às empresas brasileiras que operam no exterior, e expatriados que necessitam usar serviços bancários brasileiros.

Não obstante sua obrigação com a regulação bancária brasileira, e conformidade com os Acordos de Basileia, a instituição ainda se vê obrigada a atender a regulamentação dos países onde opera; tanto localmente no exterior, quanto nos seus *datacenters* localizados no Brasil.

A sua rede é atendida por dois *datacenters* espelhados, onde estão localizados os servidores que provém aplicações e informações para todo o conglomerado. Há mais de quinhentas *"virtual local area network" (VLAN)* distintas cadastradas nas ferramentas de configuração. Há ambientes segredados, como o Ambiente Central, que é onde estão localizadas as principais aplicações e serviços, utilizados por toda a empresa; o Ambiente Exterior, composto pela estrutura de suas dependências no exterior; o Ambiente Intranet, e assim por diante.

Este estudo de caso será focado no Ambiente Central. Nele estão instalados 196 equipamentos de *firewall*, de quatro fabricantes diferentes, com a seguinte distribuição (figura 5):

Figura 5 - Distribuição de firewalls por fabricante



Essa distribuição entre diferentes fabricantes, fruto da natureza da modalidade aplicada em sua aquisição, por si só já dificulta o gerenciamento dos equipamentos por meio

de ferramentas de gestão centralizadas, já que cada fabricante disponibiliza uma ferramenta específica. Ademais, dentro de cada conjunto de fabricantes, ainda há diversos modelos de equipamentos, o que pode, em alguns casos, capilarizar ainda mais o controle.

2.2 Vulnerabilidades Identificadas no Ambiente

O levantamento das vulnerabilidades foi realizado no ambiente entre os meses de agosto e setembro. Foi levado em consideração as vulnerabilidades apresentadas no documento *FortiOS™ Handbook - Hardening your FortiGate (2015)*, da fabricante dos *firewalls* Fortigate, além de vulnerabilidades identificadas pelos administradores da área de segurança da Instituição.

Algumas recomendações não serão abordadas como vulnerabilidades, por já estarem atendidas. As demais serão descritas abaixo além da atribuição de um código V*x* a cada uma, onde V representa a palavra vulnerabilidade, e *x* um índice numérico.

2.2.1 Firmware desatualizado (V1)

Firmware é o conjunto de instruções operacionais programadas diretamente no hardware de um equipamento eletrônico (OLIVEIRA; ANDRADE, 2006). Manter esses programas atualizados é uma faca de dois gumes. Se por um lado o ambiente ganha com correções de vulnerabilidades e novas funcionalidades na ferramenta (FORTINET, 2015), por outro o administrador de segurança tem que assumir o risco de promover alterações em um ambiente complexo e estabilizado. Há que se mensurar e avaliar os eventuais benefícios contra os riscos trazidos ao ambiente.

2.2.2 Acesso a partir de redes não-confiáveis (V2)

Definir redes de acesso seguras limita de quais origens um *firewall* pode ser acessado (FORTINET, 2015). O acesso aos equipamentos deve ser feito apenas por redes confiáveis. Os administradores dos *firewalls* estão alocados numa faixa de endereço IP restrita e conhecida. Ainda assim, foi verificado que diversos equipamentos não estão configurados para permitir o acesso a partir dessa rede, somente.

2.2.3 Auto instalação via USB habilitada (V3)

Um usuário mal intencionado, com acesso físico ao equipamento pode carregar uma configuração a um equipamento Fortigate se essa opção estiver habilitada (FORTINET, 2015). Todos os equipamentos Fortigate do nosso parque estão com essa opção habilitada. Trata-se de uma função facilitadora em um momento de recuperação de ambiente. Caso o

administrador perca acesso administrativo ao *firewall*, basta que carregue o *firmware* desejado, e um arquivo de configuração num *drive* externo *USB*, conectando-o ao equipamento, e reinicie o *firewall* fisicamente, para que esse inicialize com os arquivos contidos no *pen drive*.

Apesar de bastante útil nesse cenário, essa funcionalidade é desaconselhada pela fabricante por expor o ambiente a um usuário mal intencionado que tenha acesso ao ambiente físico.

2.2.4 Auditoria e coleta de logs não configuradas (V4)

A coleta de *logs* no ambiente central é feita através de ferramentas próprias para tal. Para os *firewalls* Checkpoint, o mesmo *Secure Domain Server* que gerencia os equipamentos, faz a coleta. Para os *firewalls* Fortinet, está disponível o equipamento Fortianalyzer. Praticamente todos os *firewalls* do ambiente estão configurados corretamente, à exceção de alguns *Fortigates*, por incompatibilidade de hardware (FORTINET, 2016).

2.2.5 Gerenciamento centralizado não configurado (V5)

Os fabricantes disponibilizam ferramentas de gerenciamento centralizado para seus equipamentos. Essas ferramentas padronizam as configurações, especialmente no cadastramento de objetos a serem utilizados nas regras de *firewall*, configurações gerais dos equipamentos, como servidores de autenticação, de resolução de nome (DNS), e sincronização de relógio.

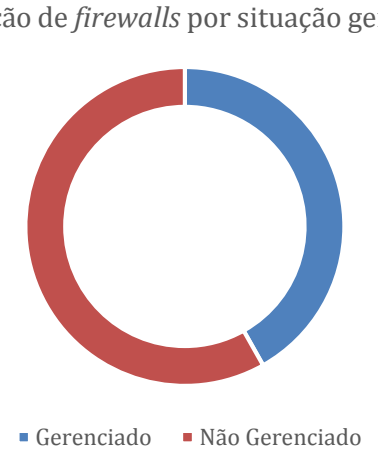
A Fortinet apresenta o FortiManager, como hardware gerenciador dos dispositivos de segurança, com capacidade para gerenciar até mil equipamentos, dependendo do modelo. A fabricante destaca dentre as vantagens, a criação de Domínios Administrativos (ADOM) personalizados por serviços, área geográfica, e outros pontos de afinidade; a capacidade de gerenciar em um único local todos os objetos entre todos os ADOMs, e a capacidade de inserção de *policies* globais (FORTINET, 2016). Com essa última facilidade, os *firewalls* podem ser mapeados para que, se necessário, o usuário crie uma *policy* e a aplique em todos os dispositivos. O próprio FortiManager se encarrega de indicar individualmente em cada *firewall* quais são as interfaces envolvidas. Esse sistema opera sob o protocolo FGFM (FortiGate to FortiManager) na porta TCP 541, e não permite inclusão de *firewalls* de outros fabricantes.

Para os *Firewalls* Checkpoint, a fabricante fornece o *Secure Management Server*, que por meio de Domínios Administrativos provê serviços semelhantes aos indicados

anteriormente pela Fortinet, operando na porta TCP 443 e também sendo exclusivo aos equipamentos de mesmo fabricante.

Num ambiente onde o operador gerencia poucos equipamentos, o Gerenciamento Centralizado pode ser dispensado. Porém, no nosso cenário, onde a contagem por fabricante ultrapassa a barreira das dezenas, a falta de gerenciamento centralizado torna-se uma vulnerabilidade.

Figura 6 - Distribuição de firewalls por situação gerenciável



Como demonstrado na figura 6, mais da metade dos *firewalls* do nosso ambiente não estão sendo gerenciados por ferramentas centrais dos fabricantes.

Com isso, perdemos um poderoso aliado na mitigação de riscos apenas por não dispor do controle de configurações básicas e objetos de maneira centralizada.

Como exemplo um mesmo nome de objeto a ser utilizado em uma regra em dois *firewalls* diferentes, podem ser cadastrados com endereços diferentes e induzir o administrador a um erro. Nesse cenário, se em um equipamento o objeto de nome "REDE_GERENCIA" está cadastrado como 192.168.0.0/24, e em outro equipamento, um objeto de mesmo nome está cadastrado como 192.168.0.0/23, um administrador inadvertido cadastrará uma regra com uma rede abrangendo um número maior de máquinas para um serviço que pode ser de natureza restrita.

Essa situação pode ocorrer por um erro de digitação no momento do cadastramento, sem que tenha havido má fé, mas também pode ter sido provocada propositadamente por criminosos infiltrados nas empresas.

Em janeiro de 2005, a gigante financeira Morgan Stanley demitiu um de seus funcionários por anunciar online a venda de informações financeiras de mais de 350.000 clientes, segundo o Wall Street Journal (BAER, 2015)

Essa situação demonstra que o acesso a informação deve ser concedido corretamente, o mínimo acesso necessário, para evitar que pessoas não autorizadas visualizem conteúdo restrito. Esse controle deve ser implementado em todos os níveis possíveis, onde atua o *firewall*.

Num cenário de gerenciamento central, o objeto dado no exemplo, "REDE_GERENCIA", teria sido criado uma única vez, e uma eventual auditoria no sistema de gerenciamento dos *firewalls*, validaria o objeto para todos os equipamentos associados por aquela ferramenta.

Os sistemas de gerenciamento central por si só não afastam o risco de edição por parte de um usuário mal-intencionado, porém facilita a detecção da vulnerabilidade e agiliza a correção do problema.

2.2.6 Sincronização automática de relógio, e padronização de servidores de NTP (V6)

Manter o relógio dos *firewalls* ajustados com os dos demais equipamentos de rede facilita a auditoria (FORTINET, 2015), e *troubleshooting*.

Durante as crises, muitas vezes os analistas envolvidos não sabem bem por onde começar o *troubleshooting*. Muitas variáveis estão envolvidas em redes de grandes corporações. Há muitos elementos de redes, roteadores, *switches*, IPS, IDS, balanceadores, e a falha causadora da crise pode estar em qualquer um desses atores.

O que auxilia enormemente o trabalho de investigação é a análise de *logs*. Equipamentos cujos servidores de NTP não foram configurados atrapalham e atrasam essa atividade.

Considere-se uma situação de crise em que é necessário comparar *logs* de diversos equipamentos e cada um está com uma data e hora aleatórias. Quanto tempo será gasto apenas convertendo um relógio para o outro diversas vezes para analisar a ordem correta das informações? Adicione-se a esse cenário conturbado a informação de que a empresa é do ramo financeiro, e que a crise acontece nos sistemas de compra e venda de ações. É o cenário da tempestade perfeita. É preciso deixar as ferramentas prontas para tornar a análise dos problemas mais fáceis, e não o contrário.

Como já demonstrado, os *firewalls* são pontos que conectam duas ou mais redes, portanto, são equipamentos-chave em *troubleshooting*. Manter configurações de NTP atualizadas é uma das boas práticas a serem postas em prática para aumentar a segurança de um ambiente.

No Ambiente Central, no levantamento realizado, foram identificados 8 equipamentos sem servidor NTP ou com servidor inexistente cadastrado. Suas datas e horas, todas aleatórias e bem diferentes da correta, certamente atrapalhariam os trabalhos de quem quer que necessitasse de seus *logs* para analisar uma eventual crise. Em pelo menos um dos casos, o *firewall* atendia a uma das redes mais críticas do *datacenter* da instituição.

Estariam as configurações incompletas dos *firewalls* contribuindo para o surgimento de brechas de segurança em redes corporativas?

2.2.7 Controle de acesso prejudicado (V7)

A autenticação de administradores nos *firewalls* é outra preocupação que os gestores da segurança devem ter. O uso de um servidor central de autenticação ajuda a diminuir os riscos de acesso, mas ainda assim, medidas adicionais devem ser observadas.

No Ambiente Central, foi identificado um único *firewall*, em uma rede de homologação, que não tinha configurado um servidor remoto de autenticação, ficando assim com uma conta local para acesso.

Afora a óbvia brecha de segurança, não identificando o administrador que acessa e modifica o equipamento, corre-se o risco de as credenciais de acesso dessa conta serem perdidas, atrasando uma intervenção em um momento de crise.

Ademais, para os equipamentos em que o servidor de autenticação estava devidamente configurado, percebeu-se que o grupo em que os funcionários da equipe responsável pela manutenção dos *firewalls* estavam cadastrados no servidor, também continha funcionários de outras equipes, não afetas ao serviço. Esse descuido expõe novamente a instituição ao risco de um agente interno mal intencionado agir sorrateiramente contra a própria empresa.

Ainda assim, no documento produzido pela Fortinet com recomendações para *hardening* de seus equipamentos, a fabricante orienta a definir *trusted hosts* permitidos para acesso remoto. Esse procedimento define redes bem específicas de onde pode ser originado o acesso aos equipamentos.

Atualmente, a instituição Banco X usa o *Terminal Access Controller Access-Control System* (TACACS) para controlar o acesso aos equipamentos de segurança. Esse sistema possibilita personalizar todo o ambiente de acesso, atribuindo a grupos de equipamentos, por exemplo os equipamentos de segurança, grupos específicos de funcionários, apesar dessa funcionalidade não estar sendo empregada na instituição.

2.2.8 Regras de *firewall* sobrepostas e desorganizadas (V8)

Por definição de boas práticas, em um *firewall* todo o tráfego é negado, a menos que seja permitido (CONTRERAS, 2016). Dessa forma, haverá uma regra negando todo o tráfego na última linha. Assim, a requisição que não se encaixar em nenhuma regra de permissão, será automaticamente negada.

Quando uma requisição chega a um *firewall* ele será testado em todas as regras existente naquele equipamento, em um sentido *top-down*, do topo até a última regra ordenada.

O dia-a-dia dos administradores de segurança no Ambiente Central é, em sua maior parte, o atendimento a pedidos de permissão de tráfego pelos *firewalls* desse ambiente. Não há um processo bem definido de como essas solicitações são atendidas, ficando a cargo de cada analista o roteiro de atendimento dos pedidos.

Ao longo dos anos, os analistas foram mudando, e os que permaneceram foram evoluindo sua forma de trabalhar, o que tornou a lista de regras dos *firewalls* mais heterogênea possível. Detectou-se inúmeras regras sombreadas e *firewalls* rigorosamente abertos, apesar de carregado de regras.

O sombreamento de regras ocorre quando uma determinada regra engloba a outra de alguma forma, como no seguinte exemplo:

- Em 2010, um determinado usuário solicitou uma regra de *firewall* com origem na máquina dele, IP 192.168.0.1, para o servidor de IP 10.10.0.1, na porta TCP 80. O acesso foi concedido e essa ficou sendo a regra 1;
- Em 2015, um gerente de setor solicitou uma regra de *firewall* permitindo o acesso de todos os usuários na rede 192.168.0.0/24 para todos os servidores na rede 10.10.0.0/24 nas portas TCP 80 e TCP 443. O acesso foi concedido e essa ficou sendo a regra 20.

É perceptível que a regra 20 do exemplo é mais abrangente que a regra 1, e, mais que isso, que há um sombreamento total: de origem, destino e serviço. O IP de origem do usuário na regra 1 está contido na rede de origem da regra 20, assim como o IP de destino está contido na rede de destino, e o serviço da regra 1 está contido no serviço da regra 20. Mais do que possível, a exclusão da regra 1 é recomendada, salvo sob argumento de manter histórico para auditoria. Nesse caso, não haveria a necessidade de alterar a regra 20 para acomodar a regra 1, já que essa estaria integralmente atendida. Quanto mais regras estão na tabela do *firewall*, mais tempo ele levará para processar cada requisição.

O sombreamento de regras também pode acontecer de maneira parcial. Considere essas três regras hipotéticas (quadro 2):

Quadro 2 - Exemplo de policy sombreada

ID REGRA	ORIGEM	DESTINO	SERVIÇO
1	192.168.0.0/24	10.10.0.0/24	TCP 80
2	172.20.1.10/32	10.10.0.0/24	TCP 80 TCP 8080 TCP 443
3	192.168.0.13/32	10.10.0.0/24	TCP 80 TCP 443

Nesse exemplo observamos que as três regras permitem o acesso à rede 10.10.0.0/24 na porta TCP 80; duas dessas regras também permitem o acesso à essa mesma rede na porta TCP 443; e apenas uma regra permite também o acesso ao serviço TCP 8080.

Seguindo essa metodologia, a cada novo pedido de permissão de acesso à essa rede na porta TCP 80, o analista incluiria uma nova regra, medida que, com o passar do tempo, inviabilizaria a gestão desse *firewall*.

O extremo das vulnerabilidades de regra de *firewall* foi encontrado em 16 dos equipamentos do ambiente central, que apesar de estarem com um bom número de regras, ainda possuem uma regra que libera a comunicação de qualquer origem com qualquer destino em qualquer serviço, isto é, tudo. Apesar de não serem *firewalls* de borda – *firewalls* que se comunicam com o mundo exterior – essa vulnerabilidade expõe os servidores a usuários mal-intencionados, *malwares* trazidos pelos usuários inadvertidamente, vírus, etc.

A explicação para essas regras ainda figurarem nos equipamentos, é a de que os serviços naquelas redes ainda não estarem totalmente mapeados, ou seja, os gestores dos serviços ainda não conhecem quem os acessa, o que acessam, nem em quais portas o fazem. Todo o tráfego dessas regras está sendo analisado para que novas regras mais específicas possam surgir dessa análise.

2.3 Quadro de vulnerabilidades

Fica assim desenhado o Quadro de vulnerabilidades identificadas no Ambiente Central da Instituição Banco X (quadro 3):

Quadro 3 - Quadro de vulnerabilidades

Índice	**Descrição**	**Referência**
V1	*Firmware* desatualizado	(FORTINET, 2015)
V2	Acesso a partir de redes não-confiáveis	(FORTINET, 2015)
V3	Auto instalação via *USB* habilitada	(FORTINET, 2015)
V4	Auditoria e coleta de *logs* não configuradas	(FORTINET, 2016)
V5	Gerenciamento centralizado não configurado	(FORTINET, 2016)
V6	Sincronização automática de relógio, e padronização de servidores de NTP	(FORTINET, 2015)
V7	Controle de acesso prejudicado	(FORTINET, 2015)
V8	Regras de *firewall* sobrepostas e desorganizadas	(CONTRERAS, 2016)

3 APRESENTAÇÃO DE PROPOSTAS

3.1 Análise do Problema

Tendo em vista os problemas apresentados, não é incorreto resumir tudo em falta de gerenciamento. Não estamos falando em ameaças novas e ofensas inovadoras. O *hardening* no Ambiente Central pode ser realizado apenas em se cumprindo o papel de gestor de segurança corretamente. Não é aceitável que uma equipe de menos de uma dezena de funcionários tenha que gerenciar mais de uma centena de *firewalls* sem o uso de uma ferramenta gerenciadora, sem que se admitam falhas nas configurações do equipamento e fragilidades na criação de regras de *firewall*.

E, uma vez gerenciados os *firewalls* através de ferramenta, como é um caso de pouco menos da metade dos *firewalls*, o esforço para a padronização do procedimento de criação das regras de *firewall* deve ser constante e incansável.

Apesar de não haver formalmente um roteiro para análise de problemas nesse no campo que se propõe este trabalho, fizemos uma interseção entre recomendações de fabricantes e propostas oriundas da observação no dia-a-dia do trabalho dentro do ambiente.

Esse conjunto de propostas é o que se segue.

3.2 Propostas

As propostas a seguir seguem recomendações de fabricantes (FORTINET, 2015) e implementações de melhores práticas (CONTRERAS, 2016). Serão contempladas ações visando melhoria no gerenciamento centralizado dos equipamentos, a padronização dos servidores NTP, o controle de acesso aos *firewalls*, e a manutenção das regras de firewall.

Da mesma forma que as vulnerabilidades, as propostas também serão descritas a seguir, acompanhadas de um identificador P*x*, onde P representa a palavra “proposta”, e *x* um índice.

3.2.1 Política de atualização de *firmware* (P1)

O versionamento de *firmwares* segue um padrão “X.Y.Z”, onde “X” representa a versão do *firmware*, que o torna incompatível com versões diferentes, “Y” representa um versionamento menor, que o torna compatível com outros versionamentos dentro da versão “X”, e “Z” representa pequenas mudanças, correções, etc.

Isso posto, identificamos que as mudanças mais sensíveis e que trazem riscos aos ambientes ocorrem quando o *firmware* muda de versão (X). Nessa ocasião, o modo como o

equipamento funciona pode ser alterado, sintaxes de arquivo de configuração podem mudar e causar alguma indisponibilidade no ambiente, o que já ocorreu.

Fica definido que, nessas ocasiões, as atualizações de *firmware* devem ser realizadas em *firewalls* em laboratório, com as configurações iguais às de produção, para que possa ser analisado o seu funcionamento pós-procedimento de atualização (FORTINET, 2015).

Para versionamentos (Y), a recomendação é que seja analisado as notas de lançamento de cada versão para definir a necessidade da atualização.

Em caso de pequenas mudanças e correções de *bugs* (Z), a recomendação é que a atualização seja realizada sem maiores precauções.

3.2.2 Definição de redes de acesso seguras (P2)

Como visto no capítulo anterior, a ausência de definição nas redes de origem para acesso aos equipamentos de firewall, configura-se em uma vulnerabilidade. Faz-se necessário configurar em todos os equipamentos as redes permitidas de acesso administrativo aos equipamentos. O acesso deve estar restrito à rede de usuários da gerência responsável pela administração dos *firewalls*, cuja faixa de endereçamento IP é conhecida (FORTINET, 2015).

3.2.3 Desabilitar auto instalação via *USB* (P3)

Seguindo a recomendação do fabricante, definiu-se por desabilitar em todos os equipamentos a possibilidade de auto instalação de firmware e configuração via *USB* (FORTINET, 2015).

3.2.4 Substituir equipamentos obsoletos (P4)

Há no Ambiente Central equipamentos antigos que não são mais compatíveis com as ferramentas de gerenciamento centralizado ou de coleta de logs (FORTINET, 2016). Para esses casos, não há outra saída senão acelerar o processo de substituição desses equipamentos.

3.2.5 Configurar o gerenciamento centralizado (P5)

Antes de qualquer outra proposta, há que se implementar o gerenciamento centralizado nos *firewalls* (FORTINET, 2016).

Os equipamentos fornecidos pela *Checkpoint* já se encontram todos nessa situação. Para os fabricados pela *Fortinet*, já há ferramenta disponível, adquirida junto do processo de aquisição dos próprios equipamentos, incluindo mão de obra para auxiliar na tarefa. Serão incluídos na ferramenta centralizada por etapas, agrupando os *firewalls* de

acordo com a afinidade da rede em que esse está inserido, já que esse processo acaba por fundir os objetos cadastrados em cada equipamento.

Os equipamentos fornecidos pela *Cisco*, embora poucos, já estão em processo de adequação à ferramenta fornecida. Há uma previsão que sejam adquiridos para outro ambiente mais de dois mil novos *firewalls* desse mesmo fabricante, e que serão gerenciados conjuntamente com os do Ambiente Central.

O problema persistirá ainda nos equipamentos fabricados pela *Juniper*, que não dispõem, na instituição, de uma ferramenta dessa natureza. É bem verdade que esses *firewalls* remanescentes, atualmente em trinta, fazem parte de um planejamento de modernização do parque, e que haverá mudança no fornecedor. Mas até que isso aconteça, esses equipamentos seguirão sendo gerenciados um a um, o que demandará maior esforço por parte da equipe e a a necessidade de maior cuidado no atendimento diário de pedidos de regra de *firewall*.

3.2.6 Fusão e padronização de objetos (P6)

Uma vez gerenciados, os *firewalls* trarão para o sistema centralizado todos os objetos que carregavam em suas configurações. Muitas vezes, esses objetos estarão em duplicidade, com nomes diferentes. Por exemplo, um *firewall* A tem um objeto com o nome "REDE_GERENCIA" cadastrado com o endereço 192.168.1.0/24; o *firewall* B tem um outro objeto de nome "NET_GERENCIAL", mas com o mesmo endereço.

Agora imagine a situação em que a rede a qual esses objetos fazem referência, seja alterada pela instituição. Num cenário onde os objetos não tenham sido unificados, o gestor do ambiente terá que se certificar que alterou todos os objetos que façam menção àquela rede, e isso por si só, já anula todo o esforço empregado para se implantar o gerenciamento em primeiro lugar.

O objeto para uma determinada rede precisa ser único dentro de um gerenciador centralizado. Para que todas as vezes que necessite ser alterado, que a alteração só se faça em um único ponto e incida em todos as regras que referenciam aquele objeto. Objetos duplicados e não utilizados ainda comprometem o desempenho do firewall (CHECKPOINT, 2016).

3.2.7 Padronização das configurações de protocolos e controle e acesso (P7)

Junto com o gerenciamento centralizado, o Ambiente se beneficiará também com a padronização das configurações gerais do *firewall*.

Protocolos de sincronia de data e hora, de resolução de nomes e de credenciamento remoto de usuários serão atribuídos pela ferramenta central.

O acesso, se antes permitido apenas com credenciais locais, agora seguirá o padrão configurado para a ferramenta, e passará a seguir as diretrizes contidas na política de segurança da instituição.

Serão incluídos *trust hosts* nas configurações dos equipamentos apenas para as redes onde trabalham funcionários que prestam suporte aos equipamentos.

Embora isso por si só ainda não resolverá a vulnerabilidade relacionada a esse tópico. Já vimos anteriormente que há usuários indevidos com acesso de escrita aos *firewalls* do Ambiente Central por estarem cadastrados no mesmo grupo de permissão do protocolo de autenticação remoto.

A instituição precisa criar um grupo próprio para a equipe responsável pela administração dos *firewalls* e associar os equipamentos a esse perfil, diminuindo assim a exposição do Ambiente a falhas acidentais e usuários mal-intencionados (FORTINET, 2015).

3.2.8 Revisão das regras de *firewall* (P8)

O sombreamento de regras e a falta de padronização na inclusão das mesmas, é o grande desafio das equipes cuja responsabilidade é gerenciar os *firewalls* da instituição.

No exemplo citado no item 3.6 deste trabalho, foi apresentado uma situação de sombreamento cruzado e parcial de regra de *firewall*. Essa situação é a mais comum no Ambiente analisado.

A solução para esse tipo de situação passa, primeiramente, na definição de um padrão para a inclusão de novas regras.

O que se propõe aqui é que as regras devem ser agrupadas por destino e serviço, concomitantemente.

Considerando, inicialmente, que um *firewall* se destina a blindar os serviços hospedados abaixo dele, a regra com essa origem, seus próprios serviços, deve ser ampla e abrangendo todas as redes da instituição, visto que quem deve negar eventualmente algum acesso, é o *firewall* da outra ponta, que está antes daquele determinado serviço. Por esse motivo, discutiremos apenas regras de destino. Essa primeira diretriz já reduz o trabalho de inclusão de regra pela metade, já que as interações serão realizadas apenas nos *firewalls* de destino.

Levando em conta também que uma regra de *firewall* é composta, basicamente, por origem, destino e serviço, se esses dois últimos coincidirem, então devem ser agrupadas as origens. Dessa forma, teremos que "determinada regra permitirá que *tais* usuários acessem o seguinte destino no serviço especificado".

Nessa linha, quando um pedido de inclusão de regra de *firewall* solicitar, dentre os demais, algum serviço para o qual já possua uma regra específica, esse pedido de regra será quebrado para que parte dele seja apenas incluído na regra existente, e as demais solicitações que não se encaixarem nas regras existentes, deem origem a novas regras.

É importante reafirmar que essa proposta diz respeito apenas a quando o destino e o serviço forem coincidentes.

Retornando o exemplo dado no item 3.6, temos as seguintes regras (quadro 4):

Quadro 4 - Exemplo de policy sombreada

ID REGRA	ORIGEM	DESTINO	SERVIÇO
1	192.168.0.0/24	10.10.0.0/24	TCP 80
2	172.20.1.10/32	10.10.0.0/24	TCP 80 TCP 8080 TCP 443
3	192.168.0.13/32	10.10.0.0/24	TCP 80 TCP 443

Aplicando o conceito apresentado, tendo em vista que o destino das três regras é o mesmo, teríamos os seguintes procedimentos a realizar:

- agrupar destino e serviço TCP 80 em uma única regra;
- agrupar destino e serviço TCP 443 em uma única regra;

Assim, teremos (quadro 5):

Quadro 5 - Exemplo de policy ajustada

ID REGRA	ORIGEM	DESTINO	SERVIÇO
1	192.168.0.0/24 172.20.1.10/32	10.10.0.0/24	TCP 80
2	172.20.1.10/32	10.10.0.0/24	TCP 8080
3	192.168.0.13/32 172.20.1.10/32	10.10.0.0/24	TCP 443

Apesar de continuar com o mesmo número de regras, fica fácil perceber que desse ponto em diante, ficará mais simples gerenciar permissões para a rede destino em um daqueles serviços.

As aplicações práticas podem vir em diversos exemplos:

- extinção de um servidor em um determinado serviço;
- alteração de determinada porta na qual responde um serviço;
- ter a informação precisa de quais origens acessam aquele determinado serviço; etc.

Para inclusão de novas regras, esse processo não chega a ser traumático. O desafio será implantar essa filosofia nas regras existentes, já que se trata de um ambiente de produção, onde residem as redes mais críticas da instituição.

A proposta é que não se alterem as regras existentes, mas que se incluam novas regras baseadas nas que já existem, e que, num primeiro momento, elas coexistam no *firewall*. Essas novas regras devem ser posicionadas acima das existentes, já que o equipamento faz uma verificação baseado na sequência em que as regras aparecem. Ao mesmo tempo, habilitar a função de contador nas regras antigas até que o contador deixe de incrementar durante trinta dias, para que se tenha a segurança de remover aquela regra.

Durante esse processo, as novas inclusões já devem obedecer às instruções aqui contidas.

Os *firewalls* que foram identificados como "abertos", ou seja, com regra permitindo todas as origens para todos os destinos em todos os serviços, posicionar essa regra no final da lista de regras, e habilitar a função de *log* na mesma, para que se possa analisar o tráfego que está sendo permitido, dando origem a regras específicas, até o ponto em que se possa excluir essa regra demasiada abrangente.

Ademais, serão padronizados os nomes de objetos de *firewall*. Estabelece-se que para facilitar o *troubleshooting* e a visualização no modo gráfico, os objetos serão criados com o nome repetindo o endereço IP.

3.2.9 Ajuste automático de relógio e padronização de servidor NTP (P9)

Será usado o servidor NTP padrão da Instituição Banco X para o ajuste automático dos relógios de todos os equipamentos do Ambiente Central, conforme orientação de fabricante (FORTINET, 2015)

3.3 Quadro de propostas

Fica assim desenhado o Quadro de propostas de *hardening* levantadas para o Ambiente Central da Instituição Banco X (quadro 6):

Quadro 6 - Quadro de propostas

Índice	**Descrição**	**Referência**
P1	Política de atualização de *firmware*	(FORTINET, 2015)
P2	Definição de redes de acesso seguras	(FORTINET, 2015)
P3	Desabilitar auto instalação via *USB*	(FORTINET, 2015)
P4	Substituir equipamentos obsoletos	(FORTINET, 2016)
P5	Configurar o gerenciamento centralizado	(FORTINET, 2016)
P6	Fusão e padronização de objetos	(CHECKPOINT, 2016)
P7	Padronização das configurações de protocolos e controle e acesso	(FORTINET, 2015)
P8	Revisão das regras de *firewall*	(CONTRERAS, 2016)
P9	Ajuste automático de relógio e padronização de servidor NTP	(FORTINET, 2015)

3.4 Matriz de Vulnerabilidades x Propostas

Quadro 7 - Matriz de Vulnerabilidades x Propostas

	P1	P2	P3	P4	P5	P6	P7	P8	P9
V1	X								
V2		X							
V3			X						
V4				X					
V5				X	X				
V6									X
V7		X					X		
V8						X		X	

Lendo o quadro 7, teremos:

Para a vulnerabilidade V1 - *Firmware* desatualizado, propomos a P1 - Política de atualização de *firmware* baseada na especificidade de cada caso.

Para a vulnerabilidade V2 - Acesso a partir de redes não-confiáveis, propomos a P2 - Definição de redes de acesso seguras.

Para a vulnerabilidade V3 - Auto instalação via *USB* habilitada, propomos a P3 - Desabilitar auto instalação via *USB*.

Para a vulnerabilidade V4 - Auditoria e coleta de *logs* não configuradas, propomos a P4 - Substituir equipamentos obsoletos.

Para a vulnerabilidade V5 - Gerenciamento centralizado não configurado, propomos a P4 - Substituir equipamentos obsoletos, e P5 - Configurar o gerenciamento centralizado.

Para a vulnerabilidade V6 - Sincronização automática de relógio, e padronização de servidores de NTP, propomos a P9 - Ajuste automático de relógio e padronização de servidor NTP.

Para a vulnerabilidade V7 - Controle de acesso prejudicado, propomos a P2 - Definição de redes de acesso seguras, e P7 - Padronização das configurações de protocolos e controle e acesso.

E, finalmente, para a vulnerabilidade V8 - Regras de *firewall* sobrepostas e desorganizadas, propomos a P6 - Fusão e padronização de objetos, e P8 - Revisão das regras de *firewall.*

3.5 Resultados obtidos

O processo de *hardening* do ambiente agrega segurança em diversas frentes. A maior beneficiada, ao final do processo, será a própria instituição, que sairá fortalecida com processos mais sólidos e amadurecidos no trato com uma área crítica como é a área de segurança de redes.

Ainda há benefícios para os próprios funcionários que trabalham diariamente com esse processo, pois haverá clareza na execução de suas tarefas; padrão na forma de execução; maior facilidade para auxiliar em um *troubleshooting* durante uma crise.

O custo total desse processo é medido apenas em horas de trabalho dos funcionários, uma vez que não está prevista a aquisição de nenhum bem ou serviço.

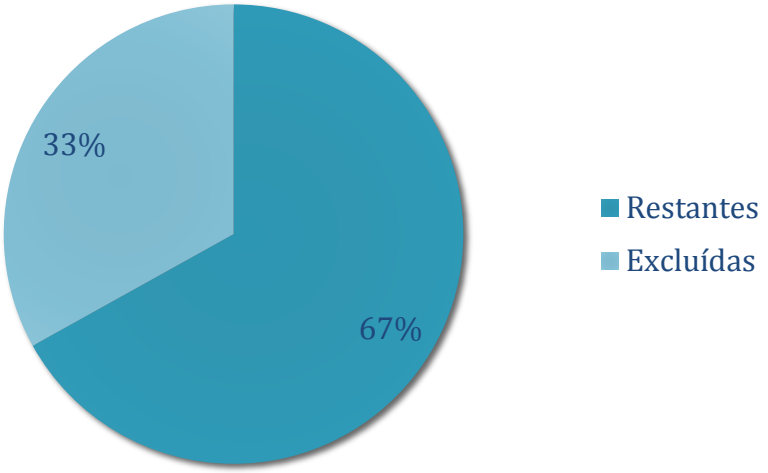
O atendimento de pedidos de inclusão, alteração ou exclusão de regras de *firewall* na Instituição Banco X, se dá através de solicitação no sistema de Gestão de Solicitações de Segurança, denominado GSS.

Para fins de validação de proposta, as orientações definidas neste trabalho estão implementadas em um *firewall* do Ambiente Central.

Foram executadas as P2, P3, P5 e agendado a substituição do equipamento (P4), além de estar em andamento as atividades P6 e P8.

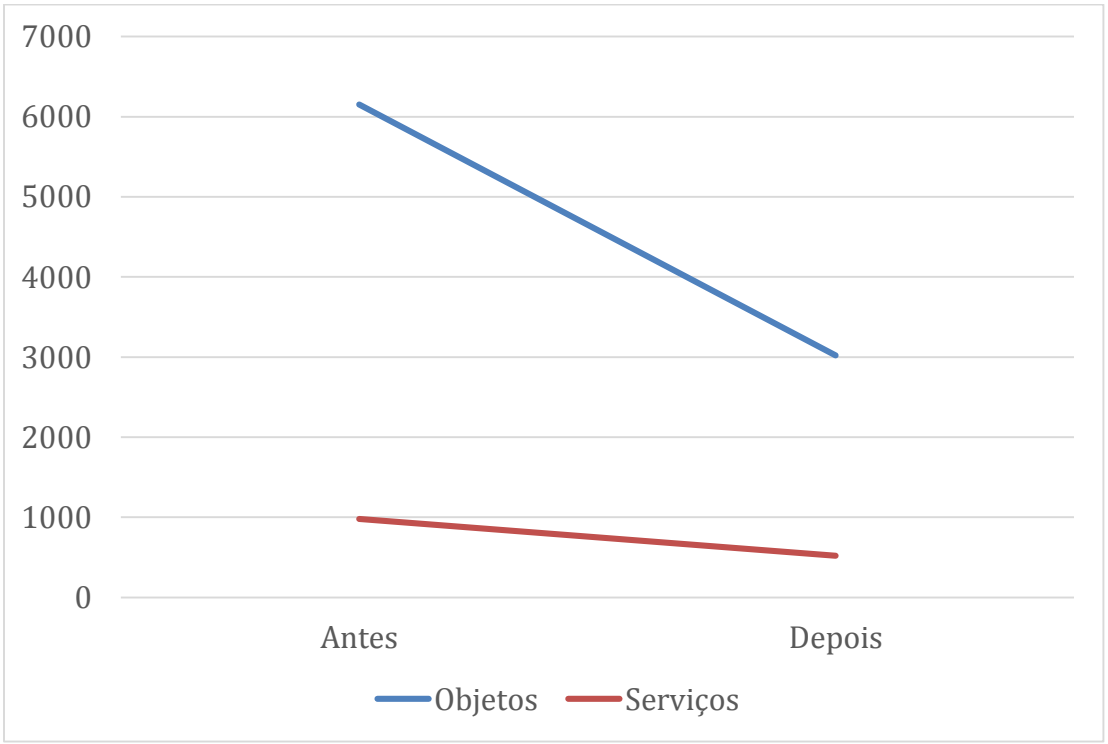
Já foram reduzidas mais de trinta por cento das regras de firewall apenas lidando com o sombreamento de regras e aglutinação de regras por serviço. Das 650 regras iniciais, o *firewall* já se encontra com 435, número ainda bem elevado, conforme a figura 7:

Figura 7 - Número de policies restante após P8



A fusão de objetos reduziu a tabela de objetos de mais de seis mil elementos para pouco mais de três mil. Foram excluídos objetos de regras suprimidas e objetos em duplicidade (figura 8):

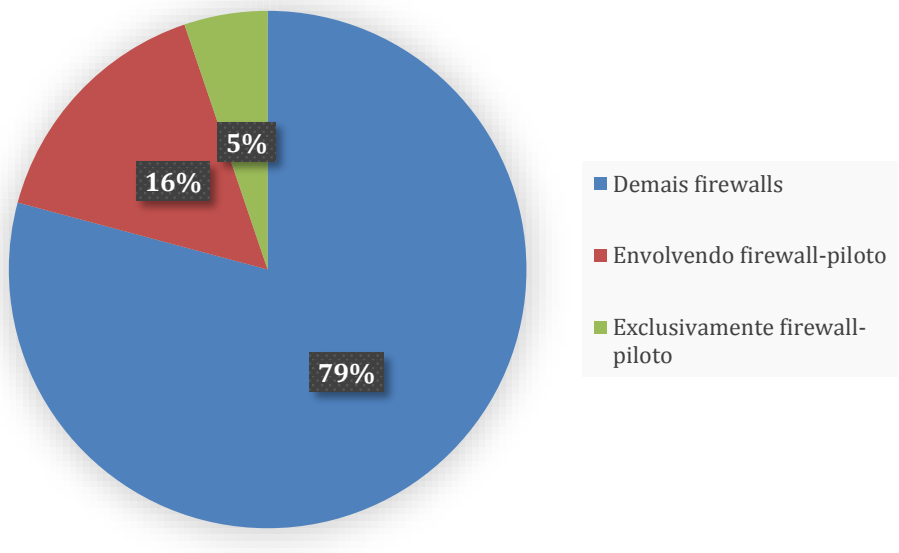
Figura 8 - Número de elementos de firewall após P7



Setenta e seis GSSs atendidas na semana entre 26 e 30 de outubro de 2016 foram acompanhadas para medição de tempo de atendimento. Dessas, quinze solicitações envolviam

o *firewall* escolhido no Ambiente Central para aplicação das regras, e outras cinco tratavam exclusivamente desse equipamento-piloto, conforme a figura 9:

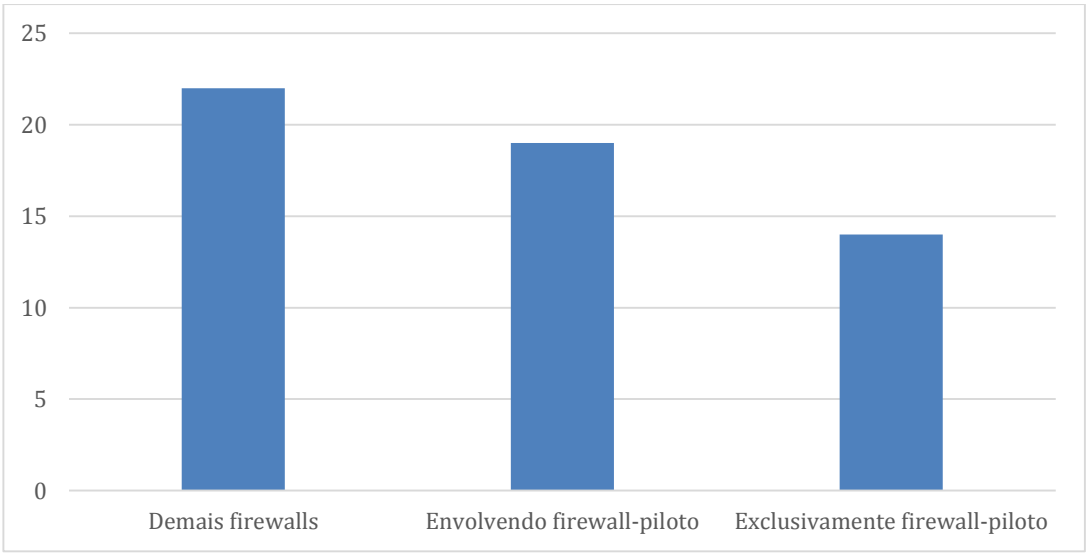
Figura 9 - Distribuição de GSSs de acordo com firewall



O tempo de atendimento compreende desde o recebimento da solicitação, a análise de aceitabilidade, de acordo com os normativos internos, a verificação de compatibilidade com outras regras no firewall, até a confecção do roteiro para que a atividade seja programada.

Houve redução de cerca de 13% no tempo médio de atendimento quando as solicitações envolviam o *firewall*-piloto objeto da aplicação das instruções deste trabalho. Houve uma redução ainda maior, de 36% quando esse *firewall* era o único elemento a ser alterado na solicitação GSS, conforme apresentado na figura 10, quantidades expressas em minutos:

Figura 10 - Tempo médio em minutos de atendimento de GSS



Apesar de, num primeiro momento, aceitar que o atendimento de GSS que trata apenas de um *firewall*, seja naturalmente mais ágil, como na terceira coluna da figura 10, na primeira coluna, designada “Demais firewalls” também há GSSs atendidas que tratam de apenas um *firewall*, sendo que esses não passaram pelas propostas deste trabalho.

Há a expectativa que, concluídas as atividades propostas, o *firewall* permaneça com algo em torno de cem regras

Além de dar sobrevida ao equipamento, já que o número de elementos aproximava-se de sua capacidade máxima, sua operacionalização ficou facilitada. Ao abrir a visualização de *policies* e observar endereços, o usuário consegue fazer análises mais rápidas e precisas.

CONCLUSÃO

Numa indústria que trilha um caminho sem volta em rumo ao digital, fortalecer a infraestrutura de segurança passou a ser imperativo.

Muito além de manter senhas fortes e políticas de segurança complexas em armários, o processo de *hardening* de um ambiente envolve uma série de atividades em diferentes camadas, conectadas entre si para o fortalecimento do sistema como um todo.

Um ambiente corporativo com vulnerabilidades no seu ambiente de segurança representa riscos financeiros e de imagem à organização, agravados ainda se essa se trata de uma instituição financeira.

Nos eventos que ocorrerem, o processo de análise deve ser rápido e preciso, dessa forma, as equipes envolvidas nesse trabalho devem dispor de elementos que auxiliem no labor intelectual, ao invés de prejudicarem. Nesse ínterim, protocolos básicos como o NTP, se mal configurados, podem fazer o papel de vilão, ou uma poderosa ferramenta de auxílio, se bem configurados.

Levantar as vulnerabilidades para um processo de *hardening* em equipamentos *firewalls* torna-se um desafio quando não há roteiros formais para fazê-lo, mas com o apoio de documentos emitidos pelos fabricantes e a análise diária no ambiente corporativo, podem fornecer subsídios valiosos na elaboração desse processo.

Manter *firewalls* atualizados, com controle rígido de acesso e manutenção, regras organizadas e sem duplicidades estão entre as atividades que ajudam a proteger o parque de ferramentas de segurança de uma organização menos exposto a vulnerabilidades.

O processo envolve uma relação contínua de atividades que devem se reiniciar ciclicamente, retroalimentando o próprio processo com novos passos e atividades a serem tomadas.

Depois que essa atividade se incorpora ao dia-a-dia da organização, incrementá-la é o caminho orgânico e mais fácil do que sua implantação.

Futuramente, já se planeja avançar no gerenciamento das regras de *firewall*, agregando-as ainda mais para formar pacotes fechados por serviços, possibilitando assim montar verdadeiros enxovais de regras de *firewall* para novos equipamentos em instalação. Saberemos que determinado equipamento, instalado no ambiente *Alfa*, que tem interesse de tráfego com os ambientes *Beta* e *Ômega*, necessita dos pacotes *X, X, e Z*, como exemplo. Esses pacotes já estarão montados nas ferramentas gerenciadoras dos equipamentos, e serão apenas selecionados para instalação.

E assim avançar-se-á o gerenciamento de um número crescente de *firewalls* no nosso ambiente.

REFERÊNCIAS

BAER, Justin. ***Morgan Stanley Fires Employee Over Client-Data Leak***, 2015. Disponível em: <http://www.wsj.com/articles/morgan-stanley-terminates-employee-for-stealing-client-data-1420474557>. Acesso em: 7 out. 2016.

BRODBECK, Cassio. **Entendendo as principais topologias de *firewall***, 2015. Disponível em: <http://blog.ostec.com.br/seguranca-perimetro/entendendo-as-principais-topologias-de-firewall>. Acesso em: 7 out. 2016.

CHECKPOINT. **Best Practices - Rulebase Construction and Optimization**, 2016. Disponível em: < https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk106597> Acesso em: 7 out. 2016.

CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D. ***Firewalls* e segurança na *Internet*: repelindo o *hacker* ardiloso**. 2. ed. Tradução Edson Furmankiewicz. Porto Alegre: Bookman, 2005.

CONTRERAS, Rose. ***Best practices for firewall rules configuration***, 2016. Disponível em: <https://support.rackspace.com/how-to/best-practices-for-firewall-rules-configuration/>. Acesso em: 7 out. 2016.

DIÓGENES, Yuri; MAUSER, Daniel. **Certificação *Security*+: Da prática para o exame SYO-301**. Rio de Janeiro: Editora Novaterra LTDA, 2011.

FORTINET. ***FortiOS™ Handbook - Hardening your FortiGate***, 2015. Disponível em: <http://docs.fortinet.com/uploaded/files/2340/hardening-52.pdf>. Acesso em: 7 out. 2016.

FORTINET. ***FortiManager Datasheet***, 2016. Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiManager.pdf>. Acesso em: 7 out. 2016.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de Redes em Ambientes Cooperativos**. 2. ed. São Paulo: Futura, 2003.

NORTHCUTT, Stephen; NOVAK, Judy; MCLACHLANM, Donald. **Segurança e Prevenção em Redes**. São Paulo: Berkeley, 2001.

OLIVEIRA, André Schneider; ANDRADE, Fernando Souza de. **Sistemas Embarcados: hardware e firmware na prática**. 2. ed. Rio de Janeiro: Editora Érica Ltda, 2010.

Pesquisa FEBRABAN de Tecnologia Bancária 2015, 2015. Disponível em: <https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Relatorio%20-%20Pesquisa%20FEBRABAN%20de%20Tecnologia%20Banc%C3%A1ria%202015.pdf>. Acesso em: 7 out. 2016.

RUSSO, Rafael. **Redes – Conheça o que é uma rede DMZ**, 2012. Disponível em: <http://escreveassim.com.br/2012/08/03/rede-dmz/>. Acesso em: 7 out. 2016.

STALLINGS, William. **Criptografia e segurança de redes**. 4. ed. Tradução Daniel Viera. São Paulo: Pearson Prentice Hall, 2008.

STREBE, Matthew; PERKINS, Charles. ***Firewalls 24 seven***. Tradução Lavio Pareschi. São Paulo: Makron Books, 2002.

TOZETTO, Claudia. **Cibercrime faz bancos perderem R$ 1,8 bilhão**, 2015. Disponível em: <http://link.estadao.com.br/noticias/cultura-digital,cibercrime-faz-bancos-perderem-r-18-bilhao,10000028721>. Acesso em: 7 out. 2016.