X_CONGRESSO_
INTEGRADO_DA_
TECNOLOGIA_DA
_INFORMAÇÃO.
TECNOLOGIAS EMERGENTES: NOVOS DESAFIOS NA EDUCAÇÃO E NA FORMAÇÃO DO PROFISSIONAL DE TI

Implantação da distribuição Endian Firewall Community em uma rede empresarial: Um Estudo de Caso

José Danilo Alves de Azevedo
Graduado em Sistemas de Informação pelo Instituto Federal Fluminense (IFF)
Analista de Sistemas - Cia do Crédito. E-mail: josedanilo161@gmail.com

Marcos Vinicius Aguiar Ribeiro
Graduando em Sistemas de Informação pelo Instituto Federal Fluminense (IFF)
Segundo Sargento - Exército Brasileiro. E-mail: marcosribeirosf@gmail.com

Vinicius Barcelos da Silva
Mestre em Engenharia de Produção pela Universidade Estadual do Norte Fluminense (UENF)
Professor do Instituto Federal Fluminense - Campus Campos Centro/RJ – Brasil. E-mail: viniciusbs@iff.edu.br

Abstract. It is impossible to imagine at present a business environment that does not have digital assets heavily dependent on the local computer network and the internet. Managing this business network by observing criteria such as security, availability and scalability is not a trivial task, requiring the use of several tools, such as firewall, antivirus, intrusion detection systems, proxy, among others. This study reports the deployment of the UTM Endian Firewall Community in an enterprise network, resulting in increased security, greater control over network traffic, allied with low deployment cost.

Keywords: LAN, firewall, security, endian, UTM.

Resumo. É impossível imaginar na atualidade um ambiente empresarial que não possua ativos digitais fortemente dependentes da rede local de computadores e da internet. Administrar essa rede empresarial observando critérios como segurança, disponibilidade e escalabilidade não é uma tarefa trivial, sendo necessária a utilização de diversas ferramentas, tais como firewall, antivírus, sistemas de detecção de intrusão, proxy, entre outros. Este estudo relata a implantação do UTM Endian Firewall Community em uma rede empresarial, resultando no aumento da segurança, maior controle sobre o tráfego da rede, aliado com baixo custo de implantação.

Palavras-chaves: LAN, firewall, segurança, endian, UTM.

1. Introdução

A utilização da internet em ambientes corporativos cresce de forma exponencial. Segundo CGI.BR (2018), o uso de internet por microempresas chegou a 88% em 2017, enquanto em empresas de médio e grande porte esse número tende a ser ainda maior. Junto ao avanço do uso da internet nas empresas, cresce de igual forma os números de incidentes relacionados à segurança. Tais incidentes, em 2017, subiram 28% quando comparados ao ano anterior, considerando apenas o Brasil (CERT.BR, 2018).

Incidentes de segurança podem expor dados sigilosos da empresa e de seus clientes. Em 2018, é aprovada no Brasil a Lei nº 13.709/2018, no qual define que é de responsabilidade da empresa a armazenagem segura dos seus dados e informações, bem como de seus clientes (BRASIL, 2018). De acordo com Gonçalves (2001), os prejuízos a uma corporação oriundos de vazamentos de informações sigilosas podem não ser apenas financeiros, como também

produzir danos à imagem da empresa perante o mercado. Além disso, a necessidade de prover um ambiente digital seguro torna-se cada vez maior à medida que uma empresa apresenta um crescimento gradativo.

Uma rede está constantemente exposta a ataques externos e internos, que ocorrem por motivações diversas, tais como financeira, obtenção de vantagens comerciais, fraude fiscal, entre outras (TANEMBAUM, 2011). Esse cenário denota a importância de as corporações protegerem suas informações contra invasores, uma vez que todas as informações de uma empresa estão armazenadas em ambientes digitais que são suscetíveis à ataques.

Infelizmente, muitas empresas só fornecem a relevância necessária à segurança de sua rede de dados após sofrerem algum tipo de ataque/invasão. Segundo KMPG (2018), a maioria das companhias ao redor do mundo não fornecem dados claros relativos às suas estratégias de segurança da informação. Ademais, muitas que optam por algum tipo de segurança digital, o fazem por meio de soluções insatisfatórias as quais não protegem seus ativos dentro de sua rede. Os softwares de antivírus, por exemplo, não são capazes de detectar sozinhos um tráfego malicioso ou evitar uma tentativa de invasão à rede. Desta forma, é necessária uma solução integrada que ofereça um conjunto de ferramentas capazes de gerir toda a necessidade de segurança de uma rede de dados e de todos os seus ativos (TANENBAUM, 2011).

Para esse fim, se torna necessário a utilização de uma solução mais elaborada, como um firewall que efetue o controle dos pacotes que trafegam na rede. Outras ferramentas devem ser usadas, tais como proxy, sistemas de detecção de intrusão, antivírus, entre outros, nas quais, em conjunto ao firewall, aumentam significativamente a segurança na rede de dados das organizações.

Além do fator de segurança, o uso exacerbado da internet em ambientes de trabalho também diminui a produtividade dos funcionários. De acordo com Coker (2011), funcionários que gastam até 20% de sua carga horária total navegando na internet tem um ganho significativo em sua produtividade, porém quando o tempo gasto ultrapassa esse percentual, ocorre uma queda gradativa no desempenho. Entretanto, Bucciol, Houser e Piovesan (2013) afirmam que a proibição do acesso à internet durante o expediente não é a solução para maximizar a produtividade. De mesmo modo que o uso irrestrito ocasiona problemas, o bloqueio total não é recomendado, mas sim uma flexibilização na utilização.

Atualmente o mercado dispõe de diversas ferramentas capazes de gerir, de forma mais ampla, o tráfego dos dispositivos conectados à rede de dados, conhecidos como UTM (*Unified Threat Management*), capazes de atuar não apenas no tangente a segurança, mas também ao controle de acesso por parte dos usuários. Dentre algumas das soluções em software mais populares temos o PfSense e o Endian Firewall. Ambas as ferramentas destacam-se por possuírem versões gratuitas e uma implementação fácil e intuitiva, o que permite que não somente grandes corporações possam usufruir de uma solução robusta, mas também pequenas e médias empresas possam garantir a segurança de sua rede e de seus ativos e uma melhor utilização de sua rede.

Em face do exposto, visando a segurança dos dados de uma rede empresarial, o objetivo deste trabalho é implantar a distribuição Endian Firewall Community em uma concessionária de veículos, bem como verificar as vantagens obtidas na segurança dos dados com a utilização deste UTM de software e avaliar a viabilidade da replicação da solução supracitada em outras empresas do mesmo seguimento.

2. Unified Threat Management – UTM

Um dispositivo de gerenciamento unificado de ameaças, conhecido como UTM (*Unified Threat Management*), tornou-se o melhor modo de tratar questões de segurança em ambientes corporativos (TAM, 2013). Consiste em uma unificação de firewall, proxy,

sistemas de detecção de intrusão, antivírus e outras ferramentas dentro de um mesmo equipamento, que juntos elevam consideravelmente o nível de segurança de uma rede de dados. Um UTM é uma solução abrangente capaz de gerir diversos setores de segurança, facilitando a vida dos administradores de redes, pois ao invés de possuir diversos aparelhos onde cada um exerceria uma função, um único dispositivo UTM seria capaz de administrar todos esses recursos, conforme figura 1. Um UTM centraliza diversos dispositivos de rede, facilitando seu gerenciamento (FORTINET, 2018).

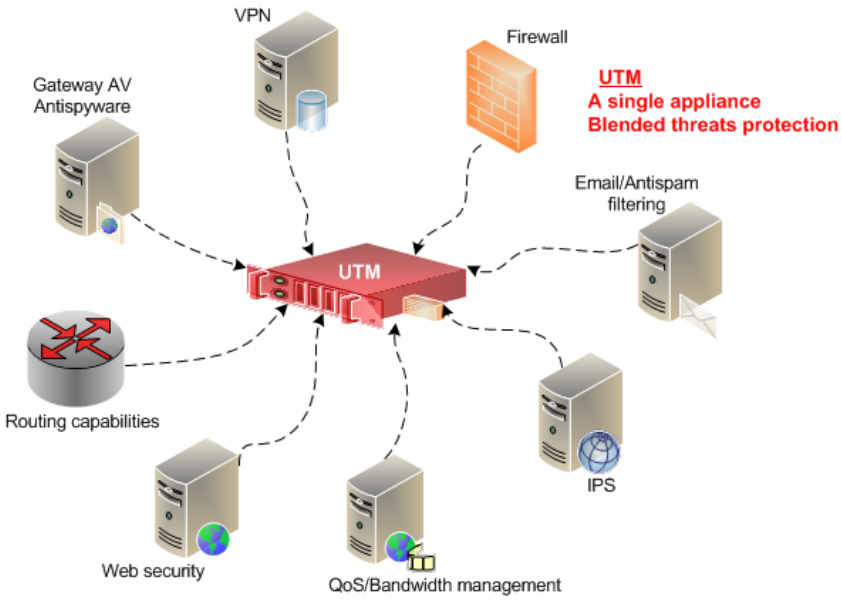


***Figura 1**. Solução de UTM. Fonte: (FORTINET, 2018)*

Segundo Tam (2013), nas últimas décadas os dispositivos de UTM se tornaram cada vez mais comuns em ambientes empresariais, sendo a primeira opção de defesa contra ameaças digitais cada vez mais desenvolvidas. A utilização de um único dispositivo minimizou os problemas de incompatibilidade entre as plataformas, uma vez que não existe a necessidade haver vários hardwares de diversos fabricantes, pois as organizações passaram a utilizar apenas uma solução completa e com uma complexidade de gerenciamento muito menor (TAM, 2013).

Segundo Kurose e Ross (2013), existe uma infinidade de soluções de UTM sendo disponibilizadas no mercado, desde hardwares robustos dedicados para este fim, com custo de aquisição mais elevado, até soluções mais viáveis que podem ser implantadas em computadores/servidores convencionais.

No seguimento de hardware, o mercado é dominado pelos UTM fornecidos pelas empresas Fortinet, Check Point e Sophos, sendo esses considerados os três maiores empresas no ramo de UTM (GARTNER, 2017). A NSSLabs realiza constantemente pesquisas e testes de performance, comparando diversos UTM de hardware, exibindo os pontos fracos e fortes de cada fabricante. Os relatórios disponibilizados pela NSSLabs evidenciam que grande parte dos fabricantes mantêm seu desempenho em níveis de segurança muito elevados, o que é esperado por clientes os quais adquirem essas soluções de UTM. Entretanto, é visível que nenhuma solução é 100% a prova de falhas (NSSLABS, 2018).

Fora do segmento de hardwares UTM, existem algumas distribuições que, instaladas em servidores, desempenham o papel de UTM. Dentre as várias soluções disponíveis no mercado, destacam-se o Endian e o PfSense, no qual ambos dispõem de versões gratuitas.

O PfSense é a solução de UTM muito difundida no mercado atual, sendo uma distribuição baseada no sistema operacional FreeBSD. O PfSense possui sua versão gratuita

com disponibilidade de todos os recursos de um UTM robusto comercial, sendo alguns recursos disponível nativamente e outros distribuídos na forma pacotes os quais podem ser instalados a medida em que forem necessários. Também existem versões virtualizadas e em hardware (PFSENSE, 2018).

O Endian Firewall Community é software de segurança gratuito baseado em Linux, especificadamente na distribuição RedHat, desenvolvido para que qualquer computador possa ser transformado em uma solução para o gerenciamento unificado de ameaças. Seu desenvolvimento foi desde o princípio pensando em prover um software robusto e de fácil gerenciamento (ENDIAN, 2019).

Por tratar-se de uma distribuição baseada em Linux, o Endian atrai usuários que já possuam alguma familiaridade com segurança de sistemas Linux. Além disso, a solução conta com tecnologias integradas pertencentes a outras empresas de segurança, tais como a Panda (responsável pelo motor do Antivírus nativo do Endian), a Cyren (líder em soluções de segurança para internet e e-mail), a Cloud4Wi (desenvolvedor de soluções para redes sem fio comerciais), além de utilizar ferramentas livres e consolidadas como Squid, uma solução de proxy bem difundida no mercado (ENDIAN, 2019).

O Endian é disponibilizado de quatro formas: Hardware Appliance, Virtual Appliance, Software Appliance e Community Appliance. As versões Software e Community são solução de UTM em software capaz de ser instalada em um hardware simples, transformando-o em um UTM completo. A versão Community é similar à versão Software, porém sem o suporte comercial e sem custos de aquisição, sendo a plataforma ideal para ser a porta de entrada para as soluções Endian. Caso for de interesse da organização, é possível a migração da versão Community para a versão Software. Segundo Endian (2019), nenhuma das versões disponibilizada é, necessariamente, superior a outra, sendo apenas uma mais adequada a certa finalidade do que outra.

Assim como o Pfsense, o Endian também dispõe de uma interface de gerenciamento Web bastante intuitiva, na qual todas as suas funcionalidades são categorizadas de acordo com sua finalidade. A quantidade de funcionalidades presentes na versão inicial (Community) até a versão mais robusta (Hardware) é imensa, tais como: firewall através do Iptables; proxy através do Squid; serviço de DHCP; antivírus através do Clamav; sistema de prevenção de intrusão (IPS) através do SNORT; monitoramento de tráfico; DNS dinâmico; qualidade de serviço (QoS) para definição de largura de banda especifica para cada serviço ou cliente da rede; monitoramento via SNMP; VPN; autenticação de usuários; relatórios de acessos; entre outros. Todas essas funcionalidades podem ser ativadas e utilizadas de acordo com cada cenário o qual o Endian seja implantado (ENDIAN, 2019).

Soluções que desempenham papel de UTM possuem tantas funções quanto um hardware de UTM dedicado, tendo como principal vantagem o baixo custo de aquisição e implantação. Além dos custos da própria aquisição, também se deve levar em consideração os valores gastos para manter o UTM de hardware em pleno funcionamento. Operar um hardware UTM como um CISCO ASA, por exemplo, não é algo trivial e demanda profissionais qualificados. Nesse cenário, as empresas acabam sendo obrigada a arcar com custos de treinamento para seus colaboradores o que, além do valor do próprio treinamento e provas, inclui viagens, material, alimentação, passagens, entre outros.

Desta forma, para empresas de pequeno e médio porte que não dispõe de condições financeiras para implantar um hardware de UTM, as distribuições que desempenham papel de UTM se tornam uma escolha bem atrativa.

Ao comparar o Pfsense e o Endian, é possível observar que ambos possuem praticamente as mesmas funcionalidades, além de recursos adicionais como suporte dedicado e linha de comunicação direta, que são cobrados como um serviço prestado. Desta forma, Assim como ocorre com os hardwares dedicados para UTM descritos pela NSSLabs (2018),

não há como afirmar qual solução é de fato superior a outra. A decisão da escolha fica a cargo de questões particulares de cada rede onde será realizada a implantação.

Para este trabalho o diferencial considerado para a escolha do Endian Community foi principalmente o fato de a solução ser baseada em Linux RedHat e fazer uso do Iptables, uma combinação de sistema operacional e ferramenta de regras de firewall que já existia na empresa, familiarizada pelos seus administradores de redes e muito difundida no mercado.

O segundo fator deve-se ao custo. A versão Community pode ser implantada sem nenhum custo, mas permite a migração para a versão Software, que possui suporte comercial, e para a versão Hardware. Neste último caso, foi levado em consideração que o appliance em hardware do Endian possui um preço muito mais acessível do que os seus concorrentes.

3. Estudo de Caso

Este estudo foi realizado em uma empresa de médio porte do ramo de venda de veículos, localizada na cidade de Campos dos Goytacazes, interior do estado do Rio de Janeiro. Foi implantada a distribuição Endian Firewall Community na versão 3.2.5 disponibilizada em 20 de setembro de 2017 pelo fabricante. A iniciativa da utilização do Endian Firewall Community deu-se ao fato da necessidade de uma solução de segurança unificada que fosse de fácil gerenciamento, baixo custo e que pudesse ser replicada a outras filiais e empresas pertencentes ao mesmo grupo econômico.

Antes da implantação, a segurança de redes era efetuada apenas por servidor Linux com o sistema operacional OpenSuse, no qual estava parametrizado o proxy no Squid e regras de firewall no Iptables. Esse conjunto provia uma boa segurança, bloqueando acesso a sites indevidos, entretanto sua manutenção era lenta e complexa, além de exigir profissionais com conhecimento elevado em servidores Linux. Devido ao fato da empresa integrar um grupo econômico de 53 empresas, a quantidade de solicitações para novos bloqueios a portais, liberação de rotas de acesso, desbloqueios temporários a sites, entre outros, tornou-se extremamente trabalhoso atender toda a demanda usando a solução existente na época.

Em face ao exposto, surgiu a necessidade de que fosse implantada uma solução de segurança que pudesse ser gerenciada local e individualmente por cada empresa, mas também com possibilidade de uma eventual gestão remota e que permitisse que um conjunto de regras iniciais pudesse ser replicado a todas as outras concessionárias do grupo de modo fácil e rápido. O Endian Firewall Community atenderia desta forma, a necessidade não apenas de uma concessionária, mas de todo o grupo.

Como já havia profissionais com conhecimento em servidores Linux com RedHat, seria possível, caso necessário, expandir ainda mais as funcionalidades já disponibilizadas nesse UTM. Além disso, sua interface Web permite que as alterações possam ser realizadas localmente por um responsável de cada empresa, de forma rápida e simples. O Endian ainda permite que as todas as configurações, ou apenas uma parte delas, possam ser facilmente exportadas e importadas em outro ambiente, permitindo desta forma que uma empresa matriz possa sempre replicar novas configurações para suas filiais.

A Figura 2 exibe a topologia simplificada de rede da empresa alvo da implantação. É importante destacar que nenhuma alteração em sua estrutura foi necessária para a implantação do Endian Firewall Community, apenas a substituição do antigo equipamento pelo Endian. Conforme observado na Figura 2, o servidor com a solução de UTM Endian foi instalado no início da rede, entre os modems de comunicação externa e o switch principal da empresa, de forma que todo o tráfego com destino a Internet ou oriundo de uma rede externa seja obrigado a passar pelo Endian.

Uma das particularidades encontrada nesta empresa é a presença de um modem de comunicação via satélite, o qual é utilizado exclusivamente para envio de dados destinados

aos servidores da montadora, sendo independente da internet. Dessa forma, também foi preciso garantir que os dados trafegados por essa via fossem seguros, efetuando a ligação do cabeamento do modem via satélite ao Endian, tal como realizado com o modem de fibra ótica.

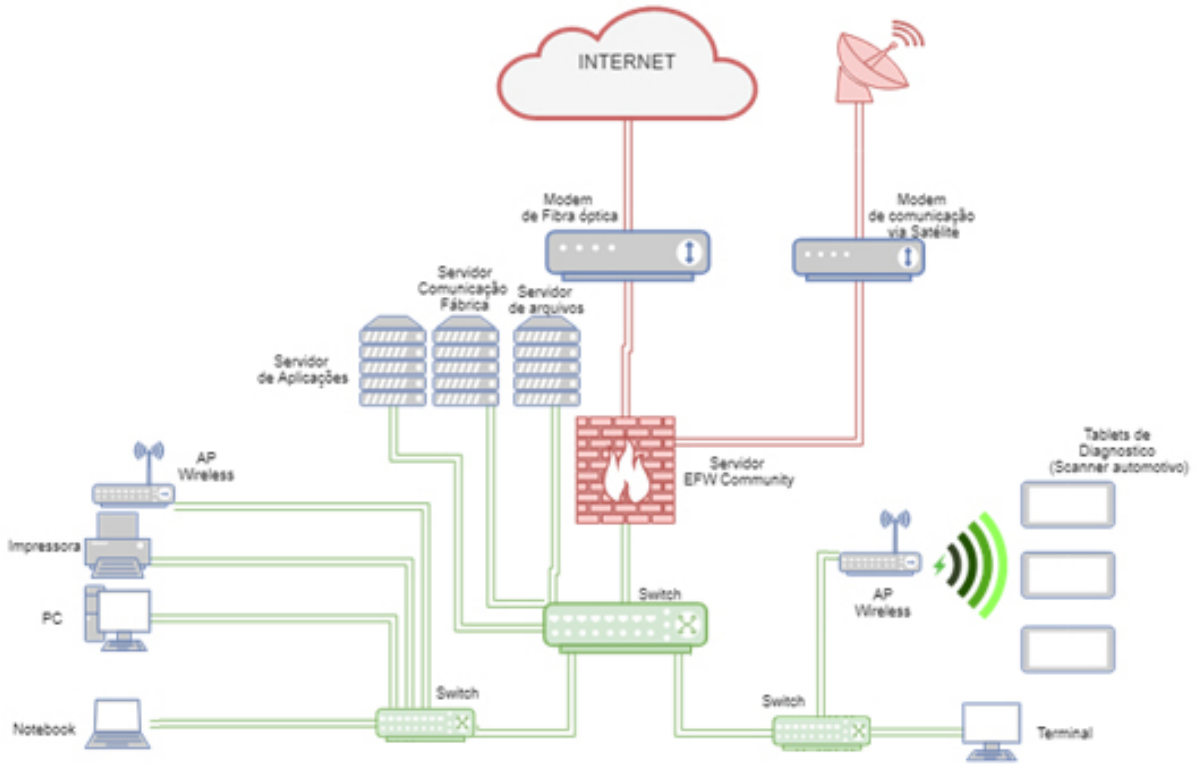


***Figura 2**. Topologia simplificada da rede da concessionária. Fonte: (Autoria Própria).*

Conforme dito anteriormente, o Endian permite que qualquer computador ocioso presente na empresa possa ser transformado em um UTM. Optou-se pela utilização de um hardware menos robusto realizando o reaproveitamento de outro computador ocioso presente na própria empresa, sendo esse composto pela seguinte configuração de hardware: Um processador Intel Celeron de 1.80 GHz, memória principal de 1GB DDR2 e um disco rígido de 160 GB, além de três placas de rede Ethernet.

4. Resultados e Discussões

Durante a realização deste estudo foi observado diversas necessidades dos usuários e da gestão da empresa no que tange a administração da rede. As mesmas puderam ser atendidas graças à utilização dos recursos presentes no Endian. Dentre as principais demandas, podemos destacar: a necessidade de uma gestão eficiente da largura de banda da internet; liberação especial por endereço MAC; detecção de sistemas infectados; bloqueio e liberação de redes sociais em horários específicos; liberação de portas de comunicações específicas para algumas aplicações.

A instalação e utilização do módulo Squid Proxy no Endian permitiu não somente identificar, mas também solucionar, um exagerado consumo da banda de internet. Antes de sua implantação o link de dados dedicado com 10 Mbps de velocidade não conseguia suprir a demanda dos usuários. O problema supracitado tornava-se critico sempre que os aparelhos de scanner veicular, utilizado para diagnóstico e correção de falhas nos veículos, eram utilizados. Devido ao fato de que seu sistema se comunicar com os servidores da Montadora durante todo o processo, sua utilização era um fator crucial para o correto funcionamento dos

processos internos da empresa, tendo em vista que um diagnóstico lento impacta diretamente no tempo que o cliente permanecia aguardando dentro da empresa, o que afeta de forma negativa a imagem da empresa quanto a sua eficiência na resolução de problemas.

Através do log em tempo real do proxy e da ferramenta de monitoramento de tráfego NTOP, pode-se constatar que poucos ativos da rede consumiam mais de 95% de toda banda disponível, tráfego que, em geral, era destinado a rede sociais, principalmente ao instagram. Este fato evidenciava que, apesar dos dispositivos de diagnósticos veiculares consumirem bastante recurso, não era esses ativos que estavam impactando no desempenho da rede.

Seguindo a orientação da gestão da empresa, optou-se pela implementação de regras no proxy com o propósito de bloquear todo o tráfego destinado a domínios pertencentes a redes sociais. Entretanto, conforme relatado por Cocker (2011), quando os funcionários dedicam uma parcela de até 20% de sua carga horária total a navegação na internet, ocorre ganho de produtividade no restante de seu tempo. Tendo em vista essa informação, foi necessária a criação de um meio no qual os colaboradores pudessem navegar livremente por redes sociais, mesmo que por um curto período de tempo. O Squid presente no Endian foi capaz de solucionar plenamente esse cenário, através de uma política de acesso que permitisse determinados usuários acessar domínios definidos previamente somente no horário adequado, como ilustrado na figura 3.

Política	Origem	Destino	Grupo/usuário de autenticação	Quando	Agente	Actions
filter using 'default'	GREEN	.fbcdn.net .facebook.com.br .facebook.com .instagram.com .instagram.com.br .snapchat.com .americanas.com.br .pontofrio.com.br .shoptime.com.br .mercadolivre.com.br	grupo1 grupo23 gerentes	MTWHF 11:30-13:00	QUALQUER	

Figura 3. *Regra de proxy por horário. Fonte: (Autoria Própria).*

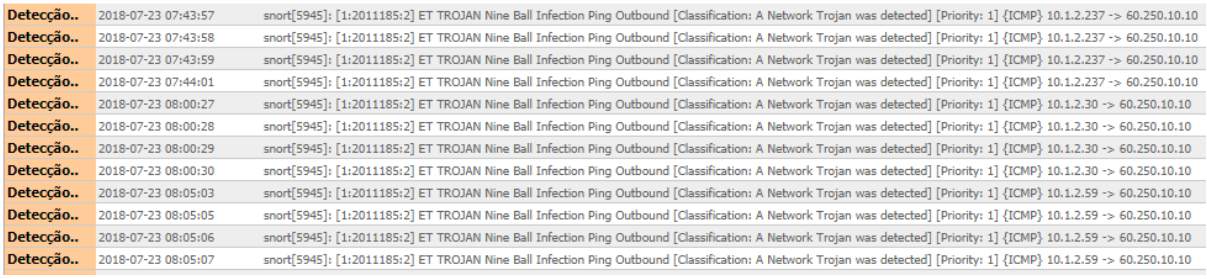
Outra solução implementada foi referente à necessidade de permissão especial para os diretores da empresa, que precisavam de acesso irrestrito a internet. Após identificar os endereços MAC dos equipamentos dos diretores, foram criadas regras de firewall, no qual permita que o tráfego oriundo dos equipamentos dos diretores não passassem pelo proxy, ou seja, seus pacotes irão trafegar diretamente pelo firewall.

Assim como qualquer firewall, o Endian também possibilita a liberação de portas de comunicações específicas para tráfego para redes externas. Um caso específico consistiu em um computador que utilizava a versão corporativa do aplicativo bancário, para acesso a conta corrente da empresa. Após uma atualização automática do mesmo, o usuário relatou que não conseguia mais utilizar seu token para efetuar a autenticação que dá acesso à conta da empresa. Mesmo após todos os domínios pertencentes ao banco terem sido liberados no firewall e no proxy, a autenticação não era realizada. Após contato com o banco em questão, pode-se constatar a necessidade de apenas liberar o tráfego pela porta TCP 1723. Desta forma, bastou a liberação dessa porta dentro do firewall e do proxy para que a autenticação via token, dentro do internet banking, fosse realizada normalmente.

Outro exemplo consistiu um sistema utilizado pelo setor de contabilidade da empresa, responsável pelo envio de informações fiscais referente a escrituração digital de rendimentos pagos e de retenções de imposto de renda e contribuição social. Para essa aplicação havia a orientação da necessidade de liberar o acesso a porta TCP 240 no firewall e no proxy. Após a criação das regras em questão, a aplicação funcionou perfeitamente.

A implantação do Endian Firewall Community também permitiu que os administradores de rede da empresa encontrassem uma vulnerabilidade de segurança desconhecida até então pela equipe de TI da concessionária. Por meio do registro de logs

realizada pela ferramenta Snort, foi observado um comportamento incomum em três dos ativos da rede, conforme figura 4.



Detecção..	2018-07-23 07:43:57	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.237 -> 60.250.10.10
Detecção..	2018-07-23 07:43:58	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.237 -> 60.250.10.10
Detecção..	2018-07-23 07:43:59	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.237 -> 60.250.10.10
Detecção..	2018-07-23 07:44:01	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.237 -> 60.250.10.10
Detecção..	2018-07-23 08:00:27	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.30 -> 60.250.10.10
Detecção..	2018-07-23 08:00:28	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.30 -> 60.250.10.10
Detecção..	2018-07-23 08:00:29	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.30 -> 60.250.10.10
Detecção..	2018-07-23 08:00:30	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.30 -> 60.250.10.10
Detecção..	2018-07-23 08:05:03	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.59 -> 60.250.10.10
Detecção..	2018-07-23 08:05:05	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.59 -> 60.250.10.10
Detecção..	2018-07-23 08:05:06	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.59 -> 60.250.10.10
Detecção..	2018-07-23 08:05:07	snort[5945]: [1:2011185:2] ET TROJAN Nine Ball Infection Ping Outbound [Classification: A Network Trojan was detected] [Priority: 1] {ICMP} 10.1.2.59 -> 60.250.10.10

***Figura 4**. Log ao vivo do Snort. Fonte: (Autoria Própria).*

Três dispositivos da concessionária tentavam se comunicar constantemente com um endereço IP específico, desconhecido pela empresa, indicando que esses computadores poderiam estar potencialmente infectados com um Trojan de rede reconhecido pelo Snort como “Nine Ball”. De acordo com FireEye (2009), uma infecção do tipo Nine Ball tenta estabelecer uma conexão via Socket com um endereço remoto de forma a permitir a esse malware uma funcionalidade de root kit capaz de interceptar o tráfego de rede do usuário.

Mesmo havendo um antivírus em todos os três dispositivos, eles não detectaram nenhum Trojan ou qualquer outro aplicativo malicioso presente nas maquinas. Por se tratar de um endereço de IP o qual a sua faixa pertence a países asiáticos, os quais não condizem com qualquer tipo de comunicação padrão efetuada pelos sistemas utilizados na empresa e pelo alerta gerado no registro do Snort, optou-se por realizar uma manutenção nos dispositivos, além de uma varredura mais completa com outro antivírus atualizado o qual identificou e removeu uma infecção nos computadores. Após a manutenção supracitada nenhum outro registro similar foi apresentado pelo Snort. Cabe ressaltar que graças a utilização do UTM nenhuma informação chegou a ser enviada ao endereço de IP de destino, visto que não havia uma regra prévia que permitisse que qualquer pacote, para esse destino, saísse da rede.

Muitos dos sistemas utilizados em um ambiente empresarial acabam necessitando que algumas portas sejam abertas, não somente para comunicação e envio de dados como também para conexões de entrada. Essa necessidade também pode surgir em virtude de processos departamentais ou mesmo do ramo de atuação da empresa. Uma das situações vivenciadas foi a de prover um meio que permitisse a equipe de suporte da montadora de veículos revendidos pela empresa acessar seus dispositivos de diagnostico veicular para realização de atualizações ou mesmo auxilio na execução dos processos.

Esses dispositivos já dispunham de uma ferramenta de manutenção a qual abria uma porta de comunicação via VNC nos mesmos, entretanto essa comunicação não funcionaria sem que haja uma liberação de acesso para essa porta dentro do Firewall e uma forma de encaminhar os pacotes recebidos por ela para o endereço de IP de um dos Scanners.

O Redirecionamento de Porta presente dentro da guia *Firewall* do Endian permitiu atender precisamente essa necessidade, bastou informar qual a porta que o serviço utilizava dentro do ativo (5900) e qual seria a porta aberta pelo Firewall. Além disso também se optou por somente fazer a permissão de acesso caso o endereço de IP de origem seja os da montadora, evitando que pessoas não autorizadas consigam acesso.

Devido a implantação do UTM ter sido realizado em um ambiente o qual já era realizado a utilização de um servidor Linux com Squid e Iptables, todos os endereços web, rotas e usuários de autenticação já existiam previamente. Desse modo, uma vez que essas configurações prévias foram copiadas para o Endian, ele já estava pronto para ser utilizado de forma definitiva, não gerando impactos sobre as rotinas da empresa.

Estando o funcionamento do Endian adequado as políticas de rede da empresa, foi possível iniciar as observações de desempenho do servidor referente ao consumo de seus recursos de hardware. Como o próprio UTM já disponibiliza suas ferramentas de testes capazes de gerar gráficos, alertas e logs de desempenho, não foi necessário a utilização de qualquer outra ferramenta.

Mesmo utilizando o hardware de baixo desempenho, o consumo de recursos do Endian ainda ficou em níveis satisfatórios. Ao monitorar o consumo de CPU e RAM do Endian já em produção, em horário de pico de utilização da rede, pode-se observar que o máximo de processamento (CPU) utilizado pelo UTM foi de 54% e o consumo de memória RAM atingiu o máximo de 47%, demonstrando que o desempenho do Endian em hardwares de baixo custo mostra-se bastante satisfatório.

Nos testes realizados durante a monitoração das placas de redes não foi identificado nenhuma situação atípica a qual pudesse indicar qualquer ineficiência de hardware em nenhum dos dois links. O resultado obtido referente ao tráfego de rede da zona vermelha (conexão com a internet) está disposto na figura 6. É possível perceber que o uso da banda da internet se mantém quase sempre em quantidades bem baixas. O pico de uso ao meio dia corresponde ao horário reservado a navegação das redes sociais dos colaboradores. Esse alto consumo na hora do almoço demonstra o impacto sobre a rede da empresa em situações onde não houvesse uma gestão ativa sobre o uso da internet.

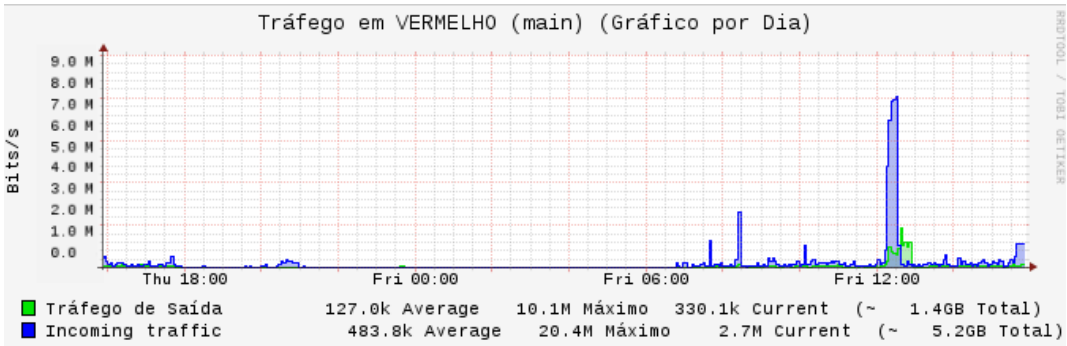


Figura 6. *Gráfico da placa da zona vermelha. Fonte: (Autoria Própria).*

5. Conclusão

Administrar uma rede empresarial não consiste apenas na necessidade de mantê-la protegida, mas também de fazer com que a rede seja otimizada de forma que possibilite aos seus usuários obterem um ambiente que possibilite uma elevação de produtividade à empresa e uma maior agregação de valor ao negócio.

Com a observação dos gráficos de utilização da rede é possível notar que os resultados supracitados puderam ser atingidos por meio da realização deste trabalho. O Endian Firewall Community proporcionou um maior controle sobre todo o tráfego da rede e uma maior confiabilidade sobre como as informações são tradadas dentro dela, ao passo que o custo dessa implantação, que a princípio era o maior desafio, foi o menor possível, visto que essa solução OpenSource dispensou na necessidade de aquisição de um hardware de UTM.

Ademais, os módulos de firewall e proxy presentes no UTM elevaram significativamente a segurança da rede por meio do controle de portas, de modo no qual somente as que realmente eram utilizadas pela empresa ficassem abertas, evitando o uso nocivo da rede.

Como sugestão para trabalhos futuros, planeja-se a replicação dessa implantação para todas as outras empresas do grupo empresarial e a ativação do controle de banda por meio do QoS. Dessa forma, será possível delimitar o quanto cada ativo da rede poderá consumir.

Referencial Bibliográfico

BRASIL. Lei nº 13709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera o Marco Civil da Internet. Brasília, 14 ago. 2018.

BUCCIOL, A.; HOUSER, D.; PIOVESAN, M. Temptation at Work. *PLoS One*, v. 8, n. 1, 2013.

CERT.BR. Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil: Estatísticas dos Incidentes Reportados ao CERT.br. Disponível em < http://www.cert.br/stats/incidentes/>. Acessado em: 12 de junho de 2019.

CGI.BR. Comitê Gestor da Internet no Brasil. TIC empresas 2017: Pesquisa sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras. São Paulo, 2018.

COKER, B. L. S. Freedom to surf: The positive effects of workplace internet leisure browsing. New Technology, Work and Employment, vol. 26, n. 3, 238-247, 2011.

ENDIAN. Página oficial. Disponível em: <http://www.endian.com/community/overview/>. Acessado em: 12 de junho de 2019.

FIREEYE. What's behind the "Nine Ball" attacks?. Disponível em: <https://www.fireeye.com/blog/threat-research/2009/06/whats-behind-nine-ball.html>. Acessado em: 12 de junho de 2019.

FORTINET. Connected UTM for Complete Small Business Security Protection Disponível em: <https://www.fortinet.com/solutions/small-business/connected-utm.html>. Acessado em: 28 de julho de 2018.

GARTNER. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls). 2017. Disponível em: <https://www.gartner.com/doc/3746429?ref=mrktg-srch>. Acessado em: 12 de junho de 2019.

GONÇALVES, S. R. M. Web no serviço. Empregado não deve usar e-mail para assunto particular. Revista Consultor Jurídico, 13 de Novembro. 2001. Disponível em: https://www.conjur.com.br/2001-nov-13/empregado_nao_usar_e-mail_assunto_particular>. Acessado em 19 de junho de 2018.

KUROSE, J. F.; ROSS, K. W. Redes de Computadores e a Internet: uma abordagem top-down. 6. ed. São Paulo: Editora Pearson, 2013.

NSSLABS. NEXT GENERATION FIREWALL COMPARATIVE REPORT: Security Value Map. Disponível em: <https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/nss-labs-2018-ngfw-comparative-report-svm.pdf>. Acessado em: 28 de julho de 2018

PFSENSE. Página Oficial. Disponível em: <https://www.pfsense.org/>. Acessado em: 21 de junho de 2018.

TAM, K. UTM Security with Fortinet: Mastering FortiOS. Waltham: Syngress, 2013.

TANENBAUM, A. S. Redes de Computadores. 5. ed. São Paulo: Pearson Prentice Hall, 2011.