Aumentando a produtividade e a segurança da sua empresa com o Sophos XG

Autores: Marcelo Puntel, Felipe Becker Nunes, José Luiz Rodrigues Filho

Antonio Meneghetti Faculdade

Tema de pesquisa

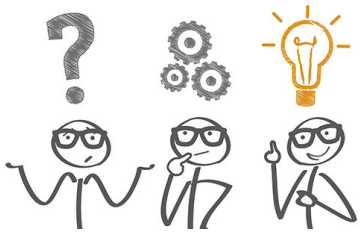
Este trabalho tem como finalidade apresentar o uso do software de segurança Sophos XG para averiguar o impacto do uso deste tipo de solução em um ambiente corporativo e indicar indícios de como isto pode afetar na produtividade da empresa, definindo a partir de políticas de acesso, quais conteúdos contidos na internet serão liberados aos colaboradores durante o período de trabalho.

Problema de pesquisa

- Necessidade de um controle de acessos;
- Diminuir tempo ocioso dos colaboradores;
- Implementar um firewall;
- Importância de ter um firewall bem configurado em sua empresa.

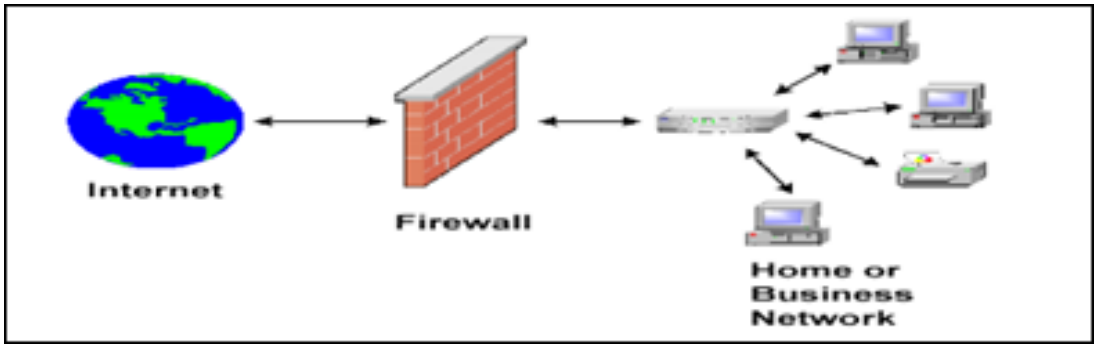
Justificativa

- Facilitar o entendimento de como essa ferramenta de segurança unificada funciona, quais os benefícios trazidos;
- Como são aplicados filtros, bloqueios, regras para acesso a aplicações web;
- Bem como mostrar o resultado final por meio de gráficos que possam comprovar seus benefícios.



Abordagem teórica

- O que é e como funciona um Firewall?
- Firewall é basicamente o que há entre o nosso computador e a internet. É um software capaz de gerenciar regras de entrada ou saída. As regras nele configuradas são as regras que podem permitir ou negar a entrada ou saída de protocolos, categorias de conteúdo ou endereços IP (*Internet Protocol*) válidos ou inválidos (TECMUNDO, 2017).
- O firewall segue as regras e configurações determinadas e realizadas pelo administrador de redes, determinando assim as políticas de segurança que o firewall irá tomar, onde será instalado após o link da internet, ele podendo ser montado de acordo com a figura abaixo.



Fonte: IMGBUDDY, 2015

Abordagem teórica

- **Sophos**

- Fundada em 1985 pelo Dr. Peter Lammer e o Dr. Jan Hruska, Sophos é uma empresa privada e sediada em Abingdon, Oxfordshire, Inglaterra e Burlington, Massachusetts, Estados Unidos.

- Focada somente em mercado empresarial.

Metodologia

- A pesquisa foi realizada através de relatórios gerados no Firewall XG, implementado em uma empresa x.

- No primeiro momento apenas para coleta das informações o Firewall foi deixado em modo Bridge por 15 dias, onde ele só coleta as informações que trafegam na rede, gerando assim um relatório com os acessos de seus colaboradores antes de aplicar as políticas de acesso.

- Após 15 dias em modo Bridge, foi definido juntamente com o responsável de TI, uma política de acesso, baseado no relatório anterior, onde foi executado bloqueios de acesso em determinados horários e para determinados grupos de colaboradores.

Resultados da Pesquisa

- Foi constatada uma considerável queda no tráfego de internet que antes era desperdiçado com o acesso a aplicações e páginas não produtivas tais como: Redes sociais, jogos on-line, músicas e vídeos

- Além da diminuição do tráfego internet obtido através dos filtros web e de aplicação, o XG Firewall ainda contribui para monitoramento em tempo real da quantidade de usuários autenticados, horário, tentativas de ataque externa, vírus na rede e transferência de download/upload.

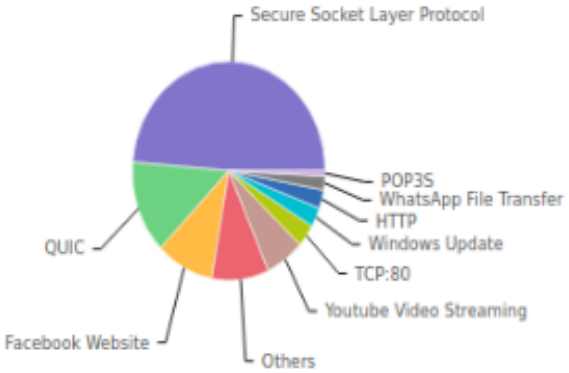
Resultados da Pesquisa

- Os gráficos foram retirados de uma empresa X ao qual ficou em modo de coleta por 15 dias e após os 15 dias foram realizados bloqueios de acesso, baseado no relatório obtido. Nisso obtivemos os seguintes relatórios:

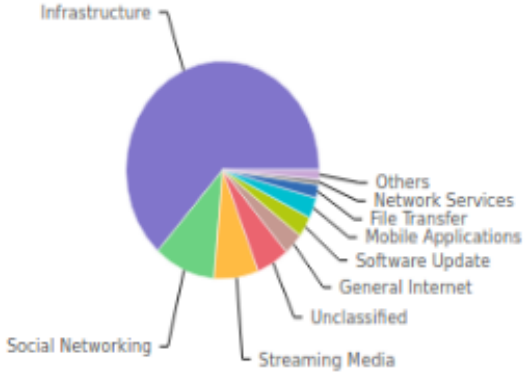
- Aplicações mais bloqueadas;
- Aplicações mais acessadas;
- Aplicações bloqueadas.

Resultados da Pesquisa

- Aplicações mais acessadas antes de implementar a politica de acesso.
- Categorias mais acessadas antes de implementar a politica de acesso.



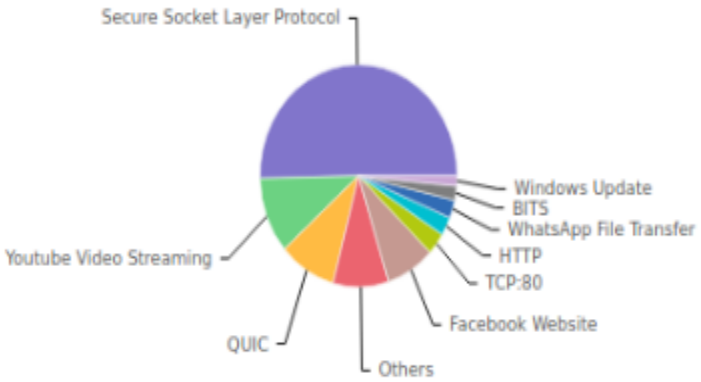
Application...	Category	Risk	Bytes	Percent
Secure Socke...	Infrastructure	1	375.64 GB	48.76 %
QUIC	Infrastructure	1	105.71 GB	13.72 %
Facebook We...	Social Networ...	3	74.65 GB	9.69 %
Others	Unclassified	?	73.62 GB	9.21 %
Youtube Video...	Streaming Me...	3	50.13 GB	6.51 %
TCP:80	Unclassified	?	25.86 GB	3.36 %
Windows Upd...	Software Upd...	3	22.08 GB	2.87 %
HTTP	General Intern...	1	21.12 GB	2.74 %
WhatsApp Fil...	Mobile Applica...	3	15.78 GB	2.05 %
POP3S	Network Servi...	1	5.87 GB	0.76 %



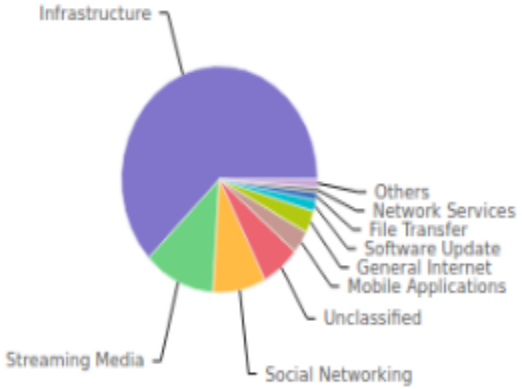
Category	Bytes	Percent
Infrastructure	487.58 GB	63.28 %
Social Networking	79.51 GB	10.32 %
Streaming Media	57.17 GB	7.42 %
Unclassified	41.92 GB	5.44 %
General Internet	25.45 GB	3.3 %
Software Update	23.6 GB	3.06 %
Mobile Applications	23.57 GB	3.06 %
File Transfer	15.2 GB	1.97 %
Network Services	6.08 GB	0.79 %
Others	10.4 GB	1.35 %

Resultados da Pesquisa

- Aplicações mais acessadas após implementar as políticas de acesso;
- Categorias de aplicação mais acessadas após a implementação das políticas de acesso;



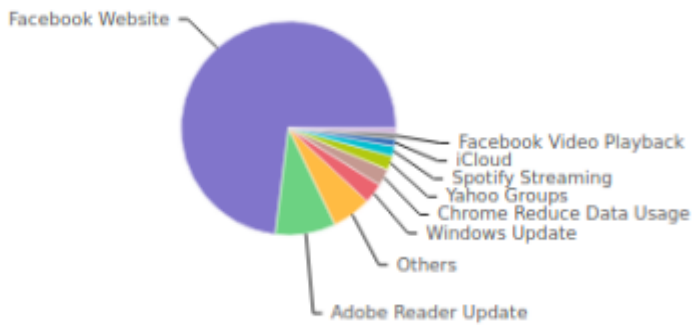
Application...	Category	Risk	Bytes	Percent
Secure Socke...	Infrastructure	1	158.61 GB	50.39 %
Youtube Video...	Streaming Me...	3	34.85 GB	11.07 %
QUIC	Infrastructure	1	29.49 GB	9.37 %
Others	Unclassified	?	28.7 GB	8.9 %
Facebook We...	Social Networ...	3	25.21 GB	8.01 %
TCP:80	Unclassified	?	10.05 GB	3.19 %
HTTP	General Intern...	1	8.52 GB	2.71 %
WhatsApp Fil...	Mobile Applica...	3	8.32 GB	2.64 %
BITS	Infrastructure	2	6.45 GB	2.05 %
Windows Upd...	Software Upd...	3	4.56 GB	1.45 %



Category	Bytes	Percent
Infrastructure	195.7 GB	62.17 %
Streaming Media	37.16 GB	11.8 %
Social Networking	27.53 GB	8.74 %
Unclassified	19.82 GB	6.3 %
Mobile Applications	10.38 GB	3.3 %
General Internet	9.9 GB	3.15 %
Software Update	5.13 GB	1.63 %
File Transfer	3.49 GB	1.11 %
Network Services	2.28 GB	0.72 %
Others	3.43 GB	1.09 %

Resultados da Pesquisa

- Aplicações mais bloqueados durante os 15 dias com as políticas de acesso aplicada



Application...	Category	Risk	Hits	Percent
Facebook We...	Social Networ...	3	597272	73.04 %
Adobe Reader...	Software Upd...	2	74297	9.09 %
Others	Unclassified	?	48407	5.87 %
Windows Upd...	Software Upd...	3	24895	3.04 %
Chrome Redu...	Proxy and Tun...	5	21128	2.58 %
Yahoo Groups	Social Networ...	2	17484	2.14 %
Spotify Strea...	Streaming Me...	2	12346	1.51 %
iCloud	File Transfer	3	8745	1.07 %
Facebook Vid...	Streaming Me...	2	7640	0.93 %
Twitter Website	Social Networ...	3	5470	0.67 %

Resultados da Pesquisa

- Como visto nos relatórios de acesso, o uso de internet para conteúdos não produtivos era muito alto, onde os colaboradores deixavam de produzir para acessar redes sociais, vídeos, jogos entre outros.

- Após implementar o Firewall, tivemos uma redução de mais de 50% de acesso nas redes sociais, identificando que os usuários ficavam muito tempo acessando o facebook, deixando de produzir para a empresa.

Considerações finais

A utilização do XG SOPHOS auxilia o gerenciamento da segurança da informação, como criar e gerenciar políticas de acesso, redirecionamentos, consultar relatórios de consumo, páginas mais acessadas, além de evitar que pessoas não autorizadas usem a conexão do ambiente para acesso à internet.

Referências

Bär, H. (2017). 4 vulnerabilidades que mais afetam a segurança da informação. Disponivel em: https:// triplait.com/4-vulnerabilidades-que-mais-afetam-a-seguranca- da-informacao. Acesso em: 25/05/2019.

Carvalho, G. M. (2018). Diagnóstico de gestão da segurança da informação em empresas nacionais do setor financeiro. Trabalho de conclusão de curso,

Departamento de Ciências Administrativas, UFRGS, 76 p. Ferreira, M. R.; Dolci, D. B.; Tondolo, V. A. G. (2016). Uma Proposta de Diagnóstico e Autoavaliação da Gestão da Segurança da Informação. XL Encontro da ANPAD,.

Kurose, J. F. (2013). Redes de Computadores e a Internet: uma abordagem topdown. 6. ed. São Paulo: Editora Pearson.

NIC.BR. Disponível em: <http://www.nic.br/noticia/releases/cresce-uso-de-internet-e-redes-sociais-pormicroempresas-no-brasil-aponta-pesquisa-do-cetic-br/ >. Acessoem: 06 de junho de 2019.

Panes, G. G. (2011). Firewall Dinâmico: Uma implementação Cliente/Servidor.
Dissertação de Mestrado, Pós-Graduação em Ciência da Computação, 72p.

Sophos XG. (2017). Disponível em: https://www.m3corp.com.br/sophos/sophos-utm-2.Acesso em: 26/06/2019

Sophos. (2017). Disponível em: <https://www.sophos.com/en-us.aspx. Acesso em:26/06/2019

Turban, E.; Volonino, L. (2013). Tecnologia da Informação para Gestão: Em busca do melhor desempenho Estratégico e Operacional. 8ed. Porto Alegre: Bookman. 721 p.

Muito Obrigado!

Marcelo Puntel
marcelopuntelc9@gmail.com

Felipe Becker Nunes
nunesfb@gmail.com

José Luiz Rodrigues Filho
joseluiz.rodriguesf@gmail.com