UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

Firewalls, A Próxima Geração

Mestrado em Segurança Informática

Miguel António Moreira Boavida Maneca

Dissertação orientada por:
Prof. Pedro Lopes da Silva Mariano e co-orientada por Sérgio Miguel Dos Santos Martins

2015

Agradecimentos

Após tantos anos passados na Faculdade de Ciências da Universidade de Lisboa, sou obrigado a começar esta secção com: “Eu quero agradecer” aos meus colegas e amigos que entraram na faculdade comigo e com quem passei momentos marcantes. Gonçalo Rodrigues, Jorge Flório, Bruno Fernandes, Tiago Filipe, João Cruz, Artur Lozynskyy, Luís Marquito e Mauro Carreira. Foram muitas as batalhas que passámos juntos.

A duas pessoas que sempre me acompanharam e ensinaram muito, obrigado Frederico Sequeira e Ana Leal pelas lições de vida.

Ao meu orientador e co-orientador (Pedro Mariano e Sérgio Martins), obrigado pela paciência e dedicação para a conclusão desta dissertação.

Ao Radu, Rodrigo, Pedro, Miguel e Bernardo (Bernas) que me ensinaram a ir para lá dos meus limites na busca da excelência. No tópico de excelência quero adicionar os nomes Prof. Paulo Verissímo e Prof. Doutor Eduardo Vera Cruz, um obrigado especial.

A toda a equipa Unisys pela ajuda em que sou obrigado a destacar Ricardo Meireles, Filipe Firmo e Rodrigo Vinagre por me terem ajudado a dar os primeiros passos nesta nova etapa da minha vida.

Um grande obrigado aos meus amigos que não só na minha vida académica, mas em toda ela, sempre fizeram parte nos bons e maus momentos. Obrigado Pedro Cabeleira, Bruno Santos, Rui Araújo, Tiago Surrador, Gil Tavares, Nuno Cantinho, James Paulo, Carla Peixe e Sara Cunha por todos os momentos que passaram comigo e pelos momentos que estão para vir.

Obrigado Andreia por todo o apoio e força que me deste até agora por toda a alegria e sorrisos que têm feito toda a diferença na minha vida.

À minha “Famiglia” em que vou apenas destacar João Fernandes, Sasha Fonseca e Pedro Ramos pois somos muitos e, apesar desta página não suportar o nome de todos, jamais serão esquecidos.

Por fim às duas mulheres mais importantes da minha vida, Teresa Boavida e Maria Encarnação (São), um grande obrigado por fazerem de mim o homem que sou hoje e ao meu pai António Maneca que, apesar de longe, vejo no espelho todos os dias da minha vida, obrigado.

Aos meus pais, António e Teresa,

A todos que ajudaram no meu percurso académico.

Resumo

Nos dias que correm, a realidade dos sistemas de informação das organizações é cada vez mais complexa e os requisitos de segurança inerentes mais exigentes. Nas últimas décadas, a utilização da *firewall* tem sido uma ferramenta fulcral para conseguir alcançar o nível de isolamento desejável nas diversas redes existentes nas organizações.

De forma a satisfazer esses requisitos, a *firewall* tradicional (primeira geração) oferece a capacidade de filtrar os pacotes com base em endereços de rede e portas de rede (ex: TCP/UDP), permitindo bloquear trafego não autorizado. *Firewalls* de segunda geração oferecem a possibilidade de armazenar o estado das ligações e fazer uma filtragem com base nas sessões estabelecidas (*Stateful Firewall*) e as *firewall*s de terceira geração introduziram o conceito de *proxy* e de controlo de acesso aplicacional que é capaz de receber uma ligação, descodificar o protocolo, intercetar a comunicação entre cliente/servidor e aplicar as regras de controlo de acesso. Mais recentemente, com a evolução das tecnologias e com o aumento da complexidade de ciberataques, a segurança tornou-se uma área crítica para as organizações. Ao contrário das *firewalls* de gerações anteriores, as de quarta geração conseguem bloquear especificamente uma aplicação, sendo denominadas de *Next Generation Firewalls*. Esta caraterística permite que haja uma verificação mais aprofundada do conteúdo de cada pacote que é trocado ao mesmo tempo que mantém o estado das sessões.

Esta última geração possui, ainda, caraterísticas que oferecem benefícios significativos como: funcionalidades *all-in-one* em que integram vários componentes como antivírus, *firewall,* sistemas de prevenção de intrusos e filtragem por reputação de endereços IP, permitindo uma análise holística; uma visão mais detalhada, com um controlo superior pois é possível observar não só as ligações mas também cada aplicação, utilizador e/ou grupo de utilizadores associados; uma gestão mais simplificada pois enquanto em *firewalls* de gerações anteriores era necessário configurar um conjunto díspar de nós, é possível configurar de forma centralizada várias *firewalls* numa só aplicação; custo de licenciamento reduzido e, por fim, o fato de estas *firewalls* terem várias funcionalidades numa só plataforma reduz, consequentemente a necessidade de outros produtos.

Palavras-chave: controlo aplicacional, funcionalidades *all-in-one*, gestão simplificada, segurança informática.

Abstract

Nowadays the reality of the information systems of most organizations is increasingly complex and the inherent security requirements more demanding. In recent decades the use of the firewall has been a key tool so that organizations can achieve the desired level of isolation in their multiple networks.

To meet these requirements, the traditional firewall (first generation) provides the ability to filter packets based on network addresses and network ports (e.g.: TCP / UDP), giving the possibility to block unauthorized traffic. Second generation Firewalls offer the possibility of storing the state of its links and make a filtering based on the established sessions (stateful firewall), and third generation firewalls introduced the concept of proxy servers and application access control that is capable of receiving a connection , decode the protocol, intercept the communication between server/client and apply access control rules. More recently, with the evolution of technology and the increasing complexity of cyber-attacks, security has become a critical area for organizations. Unlike the previous generation firewalls, the fourth generation can specifically block an application, being named “Next Generation Firewalls”. This feature allows for a more thorough check of the contents of each packet that is exchanged while maintaining the state of the sessions.

This latest generation firewall also has features that provide significant benefits such as: all-in-one functionality that integrate various components such as antivirus, firewall, intrusion prevention and filtering systems based on IP addresses reputation, enabling a holistic analysis; a more detailed view, and with an upper control that makes it possible to observe not only the connections but, more specifically, each application, user and/or group of associated users; a more simplified management hence in previous generations of firewalls had to configure a disparate set of nodes, you can set centrally multiple firewalls in one application; reduced licensing cost and, finally, the fact that these firewalls have several features in a single platform consequently reduces the need for other products.

Keywords: application control, all-in-one functionality, simplified management, computer security

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1 Introdução

Neste capítulo é descrita, resumidamente, a capacidade de uma *Next Generation Firewall* (NGFW) sobre a qual foi desenvolvido este trabalho tal como os objetivos que se pretendem alcançar. É também apresentada a estrutura deste documento por capítulo.

1.1 Motivação

Nos dias que correm a realidade dos sistemas de informação das organizações é cada vez mais complexa e os requisitos de segurança inerentes mais exigentes. Nas últimas décadas, a utilização da *firewall* tem sido uma ferramenta fulcral para conseguir alcançar o nível de isolamento desejável nas diversas redes existentes nas organizações. Mas, infelizmente, as *firewalls* tradicionais já não são suficientes para preencher este requisito. A *firewall* tradicional tem a capacidade de descartar pacotes especificando os campos de origem (*source*), destino (*destination*), protocolo (*protocol*), mas este critério é, hoje em dia, muito limitado. É necessária uma visão mais focada e detalhada do tráfego de rede, o que levou ao surgimento das NGFW. Em gerações anteriores, as *firewalls* eram utilizadas para prevenir ameaças externas (ex: *internet*), atualmente as organizações têm a necessidade de controlar não só o trafego externo como também o interno, ao restringir e controlar as ações dos utilizadores internos das organizações. Esta visão surge por motivos de segurança interna em que técnicas de obter credenciais de utilizadores como, por exemplo, engenharia social (*social engineering*) e a falta da sensibilização dos utilizadores (*user awareness*) são um perigo cada vez maior. Alarabeyat [1] defende que, para proteger contra ataques de engenharia social, é necessário garantir que certos requisitos de segurança sejam assegurados: a política de segurança da organização; a sua estrutura na organização; a gestão de controlos de acessos; a mitigação do risco de fuga de informação; a resposta a incidentes de segurança. Ao analisar estes requisitos, verificamos que uma NGFW é uma componente fundamental para os cumprimentos dos requisitos listados. Quanto à sensibilização do utilizador, Roesner [2] acredita que a maioria dos Sistemas Operativos (SO) não possuem um mecanismo eficaz para conceder permissões e criou um *access control gadget* (ACG) para resolver essa deficiência. Este ACG foi adicionado a um SO protótipo onde o acesso de aplicações foi testado e monitorizado.

Foi concluído que com um ACG é possível reduzir cerca de 82% das vulnerabilidades do *google chrome* e 96% do *firefox*. Através de uma NGFW é possível criar políticas de segurança diferenciadas por utilizador, aplicação e *website* de destino, limitando o acesso a recursos estritamente necessários, e bloquear trafego malicioso que possa explorar as vulnerabilidades existentes nas aplicações.

1.2 Objectivos

Nesta tese é utilizada uma plataforma de NGFW que teve como objetivo passar por todas as fases de um projeto de raiz, do seu início até à sua conclusão e otimização. Estas fases consistiram em:

- Análise de requisitos do cliente, em que são ouvidas as suas necessidades e expectativas;
- Desenho detalhado da solução a integrar com a infraestrutura existente;
- Documentação de todo o processo referido previamente (relatórios, gráficos e/ou apresentação)

1.3 Estrutura do documento

Para lá deste capítulo introdutório, é possível resumir os próximos capítulos da seguinte forma:

- Capítulo 2: Next Generation Firewall – Definição e caraterísticas globais deste tipo de tecnologia.
- Capítulo 3: Next Generation Firewall da Stonesoft – Descrição detalhada da plataforma tal como as suas caraterísticas, especificações e arquitetura. É sobre esta plataforma que vai decorrer todo o trabalho e serão, portanto, descritas todas as suas capacidades.
- Capítulo 4: O trabalho – É descrito todo o trabalho feito até à data da elaboração deste documento e o trabalho previsto até à conclusão do estágio.

Capítulo 2

Next Generation Firewall

Neste capítulo é focado o tema central do trabalho e oferece-se uma visão geral dos componentes e objetivos comuns às diversas tecnologias de NGFW existentes. A filtragem das ligações pode ser dividida em três fases distintas nas quais se decidem se os pacotes são aceites ou não. São elas: **identificar**, **categorizar** e **controlar**.

São também apresentadas situações que mostram a utilidade da inclusão de uma NGFW e uma visão sucinta do seu futuro.

2.1 Introdução

No início das redes informáticas, a "segurança" era razoavelmente simples pois existiam apenas dois estados para o tráfego: bom e mau [12]. A abordagem tradicional seria permitir o "bom" e bloquear o "mau" e, na altura, era o suficiente para as *firewalls* distinguirem corretamente entre tráfego benigno e maligno. Com o passar do tempo, a complexidade dos ciberataques aumentou e essa mentalidade mostrou-se perigosa devido às técnicas evasivas usadas pelas aplicações de *hacking* que tentam ganhar acesso à rede (pessoal ou empresarial). Para combater este aumento de complexidade, a Palo Alto lançou, em 2007, a primeira NGFW com a "PA-4000 series". Até à data, não foi possível alcançar um consenso para a definição duma NGFW [3][4][9], ou seja, quais as funcionalidades que têm de ser incluídas e/ou excluídas para ser considerada uma NGFW.

Para a ESG Labs [9] uma NGFW deve ter uma mistura das capacidades de uma *firewall* de primeira geração e de um *Intrusion Prevention System* (IPS) e, ao mesmo tempo, fornecer uma inspeção mais extensiva de forma a dar uma maior visibilidade do tráfego. Essas capacidades são:

- Identificação e filtragem de tráfego aplicacional – em vez de simplesmente abrir ou fechar portas, uma NGFW tem de ser capaz de identificar e filtrar tráfego baseado em certas caraterísticas específicas da aplicação de forma a prevenir *malware* independentemente das portas utilizadas (para tentar não ser detetado).

- Deteção e prevenção de intrusão – uma NGFW deve ser capaz de usar uma inspeção extensiva do tráfego de forma a identificar e prevenir intrusões à rede privada/interna.
- Inspeção SSL – NGFW devem ser capazes de decifrar e inspecionar tráfego SSL cifrado de forma a validar que a ligação provém duma aplicação fidedigna e de acordo com a política de segurança. Esta inspeção só pode ser feita com a interceção do túnel SSL e implica a utilização de chaves privadas.
- Inteligência baseada em identidade – Para gerir aplicações autorizadas e tráfego baseado em utilizador, grupos de utilizador, NGFWs integram com *directory services* comuns como *Active Directory* (AD), RADIUS e LDAP.
- Deteção de *Malware* e filtragem – NGFW deve ser capaz de detetar e filtrar *malware* baseado na sua assinatura ou lista de reputação de endereços IP e categorias de forma a bloquear aplicações e *sites* maliciosos.

2.2 Pilares de uma NGFW

Posto em traços gerais, uma NGFW deve ter o seguinte comportamento:

- **Identificar –** O contato inicial que uma NGFW faz é receber tráfego a querer entrar/sair de/para uma rede. Ao invés das abordagens tradicionais de identificação por porto/protocolo, IP ou nome do ficheiro, é feita a identificação por aplicação, utilizador/grupo ou inspeção de conteúdo.

- **Categorizar –** Após o pacote ser identificado, é necessário atribuir uma categoria em que se enquadra. Esta categorização é feita por categoria aplicacional, categoria do destino, categoria do conteúdo e utilizador/grupo.

- **Controlar –** Após o tráfego ter sido identificado e categorizado, é feito o controlo sobre o mesmo. As principais funções nesta fase passam por aplicar a política instalada de forma a: prioritizar, permitir ou bloquear aplicações, detetar e bloquear *malware*, detetar e prevenir tentativas de intrusão.

2.3 NGFW vs UTM

Como foi discutido no ponto anterior, é difícil definir uma NGFW. Isto acontece pois esta nova geração de *firewalls* possui várias funcionalidades, à semelhança de uma **UTM** (*Unified Threat Management*) que pode, ou não, oferecer diversas funcionalidades como: IPS/IDS (*Intrusion Prevention System/Intrusion Detection System*), *Web Filtering*, *Application Detection*, *Virtual Private Network* (VPN) entre outras. Apesar de algumas empresas criarem uma distinção entre a NGFW e uma UTM, a realidade é que, de um ponto de vista funcional, são semelhantes, visto que possuem as mesmas caraterísticas e funcionalidades.

	FW/VPN	IPS	AV	Web Filtering	Application Detection	Email Security	DLP
Next Generation Firewalls							
Checkpoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim
McAfee	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Palo Alto Networks	Sim	Sim	Sim	Sim	Sim	?	Sim
Sourcefire	Sim	Sim	Sim	Sim	Sim	?	Sim
Unified Threat Management							
Astaro	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Fortinet	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Sonicwall	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Watchguard	Sim	Sim	Sim	Sim	Sim	Sim	Sim
UTM/NGFW?							
Cisco	Sim	Sim	Sim	Sim	Não	Sim	Não
Juniper	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tabela 1 - Comparação de funcionalidades de NGFW [13]

Através desta tabela é possível observar que em 2012 não existia grande diferença entre a maioria das UTM e NGFW, sendo que, nos dias de hoje, ainda é possível

argumentar que as NGFW são UTMs. É de referir que tanto a PAN (Palo Alto Networks) como a Sourcefire não possuíam segurança de *email* nos seus produtos mas que, no entanto, é possível argumentar que o Antivírus (AV) e as restantes funcionalidades oferecem esse serviço.

2.4 Benefícios da inclusão de uma NGFW

O fato de esta nova geração de *firewalls* possuir diversas aplicações integradas num só produto cria uma facilidade na gestão da segurança das organizações. Uma organização recém-criada terá um menor custo no licenciamento de produtos, tal como é reduzido o número de pessoas que têm de ser responsáveis por cuidar da segurança da empresa (ex: não é necessário um empregado A para a *firewall*, um empregado B para o IPS, o empregado C para a *Virtual Private Network* (**VPN**), etc.). Não só as pequenas empresas beneficiam com as NGFW, como também as grandes empresas cuja complexidade de redes internas pode ser abismal. Agora é possível ter apenas um ponto central de segurança que englobará todas as redes, *firewalls*, VPNs, entre outras.

2.5 O Futuro da NGFW

De um ponto de vista teórico, as NGFW são a solução perfeita para criar um controlo de segurança centralizado. No entanto, os fabricantes necessitam de rever e melhorar os seus produtos. Não só afirmam que os seus produtos têm um melhor desempenho do que efetivamente possuem, como também não existe um que possua "todas" as capacidades no mercado (ex: Na tabela 1 é possível ver que a Fortinet tem IPS, mas não tem *Web Filtering*, a Cisco tem *firewall* mas não tem IPS). A seguinte tabela da NSS Labs mostra um ponto de vista global e atual de cada produto e as suas capacidades a nível de segurança.

Nome do Produto (NGFW)	Eficiência (Segurança)		Valor (Medição feita por Mbps protegido)		Classificação Final
Barracuda F800b	89.70%	Abaixo da Média	$20.03	Acima da Média	Neutro
Check Point 13500	96.40%	Acima da Média	$21.45	Acima da Média	Recomendada
Cisco ASA 5525 - X	99.20%	Acima da Média	$21.60	Acima da Média	Recomendada

Cisco ASA 5585 – X SSP60	99.20%	Acima da Média	$48.00	Abaixo da Média	Neutro
Cisco FirePOWER 8350	99.20%	Acima da Média	$20.03	Acima da Média	Recomendada
Cyberoam CR2500iNG – XP	88.20%	Abaixo da Média	$13.48	Acima da Média	Neutro
Dell SonicWALL SuperMassive E10800	97.90%	Acima da Média	$15.46	Acima da Média	Recomendada
Fortinet FortiGate - 1500D	94.10%	Acima da Média	$6.35	Acima da Média	Recomendada
Fortinet FortiGate - 3600C	96.30%	Acima da Média	$8.30	Acima da Média	Recomendada
McAfee NGF – 1402	95.50%	Acima da Média	$11.38	Acima da Média	Recomendada
Palo Alto Networks PA - 3020	60.10%	Abaixo da Média	$63.66	Abaixo da Média	Cuidado
WatchGuard XTM1525	97.80%	Acima da Média	$11.87	Acima da Média	Recomendada

Tabela 2 – Testes de segurança feitos a NGFW [5]

Como é possível verificar, existem diversos produtos e soluções que podem ser adquiridos. No entanto, a qualidade e serviços que proporcionam não são homogéneos.

Capítulo 3

Next Generation Firewall da McAfee (Stonesoft)

Neste capítulo é apresentada a solução de NGFW da McAfee sobre onde incidiu todo o trabalho ao longo do estágio. Após introdução, no capítulo anterior, do funcionamento geral duma NGFW, é possível aprofundar a arquitetura e caraterísticas desta solução.

3.1 Introdução

A Stonesoft era uma empresa nórdica sediada em Helsínquia, Finlândia. Começou por fabricar *firewalls* de alta disponibilidade e, ao longo dos anos, expandiu-se de forma a abordar tecnologia de *clustering*, ambiente *Firewall*, VPN e balanceamento de carga. Hoje conta com diversas funcionalidades e em anos recentes chegou mesmo a rivalizar com líderes de mercado como a Check Point até ser adquirida pela subsidiária da Intel, a McAfee, em 2013 [6].

3.2 Arquitectura

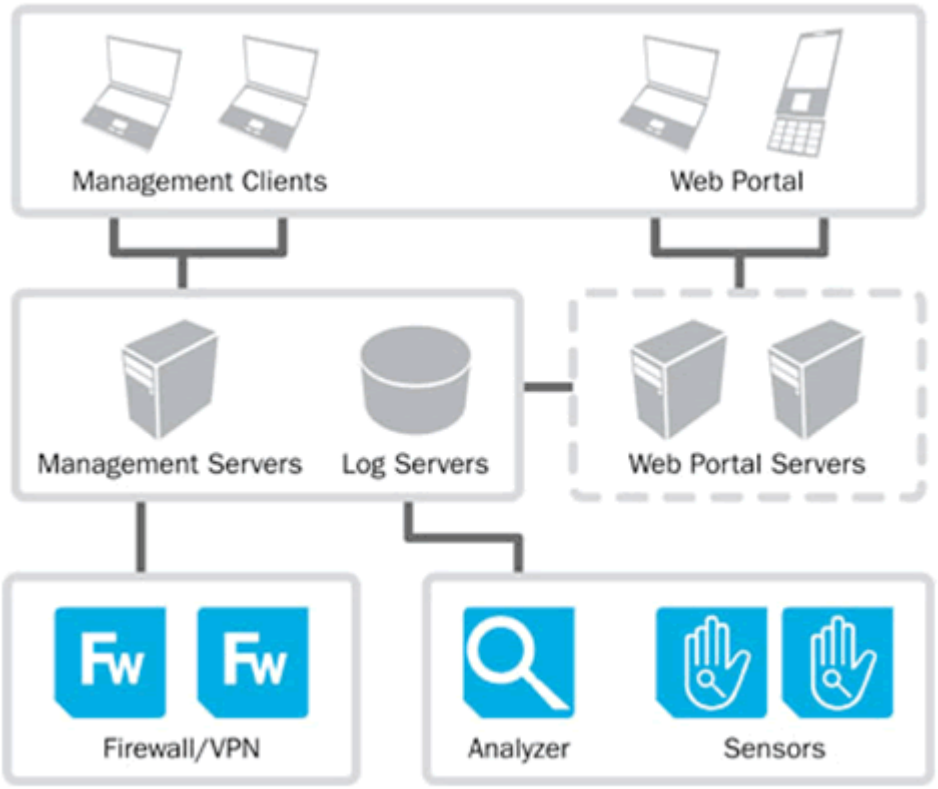


Figura 1 - Arquitetura da Stonesoft

Como descrito no ponto anterior, a Stonesoft é uma solução que rivaliza com os líderes de mercado e possui uma arquitetura semelhante à Figura 1. Nesta arquitetura, os componentes principais são o *Management Server* (SMC), *Log Server* e um, ou mais, *Management Clients* (é assumido que as *firewalls*/VPNs já estão previamente instaladas no sistema). Opcionalmente é possível adicionar *Management Servers* e *Log Servers* adicionais para oferecer redundância tal como um, ou mais, *Web Portal Servers*. [7]

3.3 Funcionalidades

Na Figura 2 podemos observar o que a NGFW da McAfee tem para oferecer. É possível ativar todas ou apenas algumas destas funcionalidades. Seja num ambiente virtual ou físico, é necessário ter em conta que quantas mais funcionalidades estiverem ativas, mais recursos (memória, processador, etc.) são necessários.

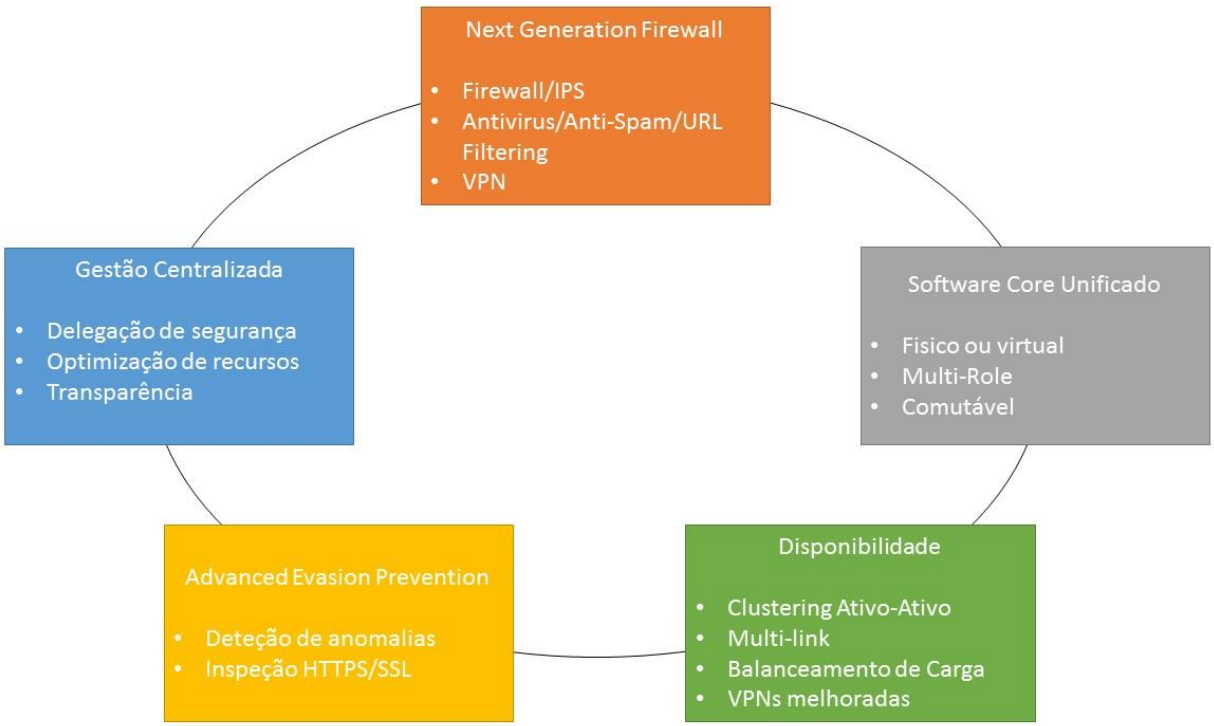


Figura 2 – Serviços oferecidos pela NGFW da McAfee

De seguida aprofundamos ainda mais as capacidades desta solução no que toca a serviços, protocolos, algoritmos e mecanismos de segurança [8].

3.3.1 Firewall/VPN

3.3.1.1 Geral

Neste papel de *Firewall*/VPN a NGFW da McAfee oferece diversos protocolos como: *File Transfer Protocol* (**FTP**) que é dos protocolos de transferência de ficheiros mais usados no mundo; **H.323** que utiliza pacotes com dados de áudio e vídeo; *Hypertext Transfer Protocol* (**HTTP**) e *Hyper Text Transfer Protocol Secure* (**HTTPS**) que é, provavelmente, o protocolo aplicacional (layer 5) mais conhecido; *Internet Message Access Protocol* (**IMAP4**) que é usado por clientes de e-mail para recolher mensagens electrónicas dum servidor de *e-mail* via TCP/IP; *Media Gateway Control Protocol* (**MGCP**) que é um protocolo de controlo de chamadas que é normalmente usado em sistemas de Voice over IP (VoIP); *Microsoft Remote Procedure Call* (**MSRPC**) que é utilizado em modelos cliente/servidor; *NetBios over TCP/IP* (**NBT**) que permite que computadores/aplicações mais antigos que dependem da *NetBIOS API* tenham um protocolo compatível com redes TCP/IP mais recentes; *Post Office Protocol* (**POP3**) que é um protocolo utilizado no acesso remoto a uma caixa de correio eletrónico; *Remote Shell* (**RSH**) que permite correr um script remotamente por uma linha de comandos; *Real Time Streaming Protocol* (**RTSP**) que é um protocolo utilizado para o controlo de transferências de dados com propriedades de tempo real; *Signalling Connection Control Part* (**SCCP**) é um protocolo que fornece uma extensão de roteamento, controlo de fluxo e segmentação às ligações; *Session Initiation Protocol* (**SIP**) que é um protocolo usado para controlar sessões de ligações multimédia; *Simple Mail Transfer Protocol* (**SMTP**) que é usado como norma na internet para transmissão de correio eletrónico; *Secure Shell* (**SSH**) é um protocolo cifrado utilizado para sessões remotas em *shell*; *Trivial File Transfer Protocol* (**TFTP**) cuja principal utilidade, semelhante ao FTP, é a transferência de ficheiros oferecendo, no entanto, muito menos segurança que o seu sucessor.

Para a autenticação, esta NGFW oferece mecanismos de autenticação como: uma base de dados local (interna); *Lightweight Directory Access Protocol* (**LDAP**) que oferece, duma forma centralizada, uma solução aberta para aceder e manter a informação de todos os utilizadores dum domínio num directório distribuído; *Microsoft Active Directory* (**MS AD**) que é semelhante ao LDAP, mas é uma solução proprietária da Microsoft; *Remote Authentication Dial-In User Service* (**RADIUS**) que é um protocolo que fornece uma gestão centralizada de autenticação, autorização e contabilização (**AAA**) para utilizadores que se ligam a uma rede; *Terminal Access Controller Access-Control*

System (**TACACS**) refere-se a um conjunto de protocolos que lidam com autenticação remota e serviços relacionados a acessos numa rede através dum servidor centralizado.

No que toca à alta disponibilidade, é suportado: *clustering* até 16 nós ativo/ativo (todos os nós estão ativos) ou ativo/standby (existem *n* nós ativos e os restantes estão em standby). No caso do nó ativo/ativo significa que existem *n* nós ativos e existe um balanceamento de carga em que ambos os nós recebem e processam o pacote. No caso do ativo/standby temos *n* nós que recebem e distribuem o pacote e os restantes estarão em standby caso haja uma falha com algum nó ativo. *Virtual Router Redundancy Protocol* (**VRRP**) que é um protocolo de rede que atribui de forma dinâmica um router ao anfitrião (*host*) dando, portanto, redundância. Balanceamento de carga que, como o nome indica, balanceia pelos nós o tráfego; ***Link aggregation*** (802.3ad) que consiste em combinar várias ligações de rede numa só, desta forma aumenta-se a taxa de transferência duma ligação, que sozinha seria incapaz de atingir, e oferecendo também redundância. Detecção de falha na ligação (*link*), através de mecanismos de segurança como o *heartbeat* em que um nó envia um sinal de X em X tempo para um sistema central. Caso o limite de tempo para a recepção desse sinal expire, o nó primário é considerado perdido e é feito o *failover* para outro nó secundário, ou seja, este nó secundário assume o papel do primário.

A atribuição de endereços IP pode ser feita manualmente (IPv4 ou IPv6) ou por *Dynamic Host Configuration Protocol* (**DHCP**), independentemente do número de nós existentes. Esta atribuição é feita de acordo com os endereços disponíveis num intervalo de IPs definido (*Scope/IP Pool*) ou de forma estática. Quanto aos utilizadores da VPN, a NGFW pode tomar um papel de DHCP e fornecer esse serviço ou fazer reencaminhamento (*relay*) de um outro servidor DHCP.

A NGFW oferece uma tradução de endereços IPv4 e IPv6 através de: *Network Adress Translation* (**NAT**) estático em que é feita uma tradução um para um; NAT de origem com *Port Address Translation* (**PAT**) e NAT de destino com PAT, ou seja, a tradução de IPs é feita atribuíndo uma porta a cada tradução (apesar de existirem 65536 portas, por norma costumam ser utilizadas apenas as dinâmicas (49152 a 65535).

As capacidades de roteamento baseiam-se em dois tipos diferentes, rotas estáticas e rotas dinâmicas. Nas rotas dinâmicas é suportado: *Internet Group Management Protocol* (**IGMP**) que é usado por anfitriões (*hosts*) e router adjacentes para estabelecer conjuntos de membros multicast; *Routing Information Protocol v2* (**RIPv2**) que é o

sucessor dum dos protocolos de roteamento mais antigo do mundo que se baseia no número de saltos (*hops*) como métrica de roteamento limitando até 15 saltos para prevenir ciclos infinitos; *Open Shortest Path First v2* (**OSPFv2**) que é o *interior gateway protocol* (**IGP**) mais utilizado em grandes empresas e se baseia num algoritmo de roteamento que calcula o caminho mais curto para estabelecer uma rota dum ponto A a um ponto B; Por fim temos o *Border Gateway Protocol* (**BGP**) que, ao contrário dos IGP, é usado entre sistemas autónomos (SA) e não dentro do próprio sistema e é usado por toda a internet para definir e partilhar rotas entre SA.

Relativamente ao IPv6, a NGFW suporta: ***dual stack IPv4/IPv6*** que é um mecanismo de transição de IPv4 para IPv6 e permite que IPv4 e IPv6 possam ambos ser utilizados simultaneamente; *Internet Control Message Protocol* v6 (**ICMPv6**) que é um protocolo que fornece relatórios de erro à máquina de origem (ferramentas usadas no Windows baseadas neste protocolo são, por exemplo, o *ping* e o *tracert*); *Domain Name System* v6 (**DNSv6**) que é um sistema de gestão de nomes em que cada máquina tem um nome associado.

Para ambientes em que existe uma taxa de transferência muito alta, pode ser necessário inspecionar o conteúdo de protocolos como HTTP, FTP e SMTP. Para isso, a NGFW está preparada para efetuar um redireccionamento para um servidor dedicado, ao invés de se sobrecarregar.

Existe também uma ferramenta antivírus em que são examinados protocolos como HTTP, HTTPS, POP3, IMAP e SMTP. Este tipo de exame funciona baseado em ficheiros e assinaturas da base de dados local.

Nos dias que correm é preciso ter cautela quanto ao conteúdo de mensagens eletrónicas. Por essa razão existe uma categoria *anti-spam* em que o protocolo SMTP é examinado. Este motor de exame é baseado em pontuações em que, quanto maior for o número de deteções desse *spam*, maior é a sua pontuação. A filtragem do *spam* é completamente personalizável: é possível fazer uma correspondência entre as assinaturas da base de dados local e o assunto, cabeçalho ou conteúdo. Existem também listas negras (*blacklists*), filtragem *honeypot* (que se baseia em aliciar um atacante para roubar dados monitorizados) e *antispoofing* local de forma a facilitar a deteção de agentes maliciosos.

3.3.1.2 VPN

Na VPN os protocolos suportados são: *Internet Key Exchange v1* (**IKEv1**) e IKEv2 que são protocolos usados para estabelecer uma *security association* (**SA**) no *Internet Protocol Security* (**IPsec**). A VPN consiste em estabelecer um canal seguro entre um ponto A e um ponto B em que o conteúdo é cifrado após uma troca de chaves criptográfica. Este canal pode ser anfitrião-para-anfitrião, rede-para-rede ou rede-para-anfitrião.

Para ser feita cifra de conteúdo na VPN, estão disponíveis os seguintes algoritmos: *Data Encryption Standard* (**DES**) que usa um algoritmo de chave simétrica para cifrar dados (foi à muito considerado inseguro a ataques de força bruta por possuir uma chave de apenas 56 bits); *Triple DES* (**3DES**) que, apesar de tornar o seu precessor (DES) mais robusto, possui um tempo de computação maior o que torna este algoritmo uma má escolha para plataformas com recursos limitados e devido à chave de apenas 64 bits; o *Advanced Encryption Standard* (**AES**) de 128 e 256 bits que sucedeu ao DES e 3DES; e o algoritmo *Blowfish* que é apresentado como uma alternativa aos algoritmos anteriores possuindo, também, uma estrutura *Feistel*.

A NGFW oferece diversos algoritmos de *hash*. Um dos algoritmos de *hash* é o MD5 que oferece uma proteção de 128 bits mas apresenta um problema de resistência a colisões, isto é:

É possível encontrar dois inputs a e b de forma a que $H(a) = H(b)$ e $a \neq b$

Secure Hash Algorithm (**SHA**) 1, 2-256 e 2-512 que é o algoritmo padrão da *National Security Agency* (NSA) e oferece uma segurança de 160bits, 256bits e 512bits respetivamente. Apesar de SHA-1 ser o algoritmo de *hash* mais usado no mundo, a partir de 2017 muitas organizações como a *Microsoft*, *Mozilla*, etc vão parar de aceitar certificados cifrados com SHA-1 para dar lugar a certificados com algoritmos mais seguros [11].

Para autenticação são usadas assinaturas **RSA**, cujo nome provém da junção do apelido dos seus criadores (Ronald Rivest, Adi Shamir, e Len Adleman), *Digital*

Signature Standard (**DSS**), que usa o *Digital Signature Algorithm* (**DSA**) como padrão e, por fim, o *Elliptic Curve Digital Signature Algorithm* (**ECDSA**) que é uma alternativa ao DSA.

3.3.2 IPS e FW Layer 2

Durante a instalação dos nós é necessário escolher entre duas funções distintas: IPS ou *Firewall Layer* 2. Neste subcapítulo juntam-se os dois papéis pois as funcionalidades nele descrito são comuns a ambos.

Nestas funções a NGFW oferece, no caso do *IPS*, filtragem de pacotes (com estado) para protocolos IP (*layer 3*) e, no caso de *FW Layer 2*, filtragem de pacotes (sem estado) para protocolos *ethernet* (*layer2*) – a arquitetura *ethernet* faz a ligação entre duas redes locais e é baseada no envio de pacotes. Correspondência automática de interfaces lógicos com interfaces físicos e *Virtual Local Area Network* (**VLAN**) - que é uma segmentação de rede virtualizada que costuma ser utilizada para configurar *switchs* e *routers* de forma a oferecer isolação das restantes redes/VLANs. Filtragem por endereço do *Media Access Control* (**MAC**) que corresponde a um identificador único associado a um interface de rede.

É também garantida alta disponibilidade através de: um *cluster* de *firewall* (*layer 2*) ativo-passivo; um *cluster* de IDS ativo-ativo ou ativo-passivo;

3.3.3 Funcionalidades Gerais

3.3.3.1 Geral

Independentemente da função, escolhida existem várias funcionalidades que estão sempre inerentes.

O encapsulamento disponível pode ser: *ethernet*; 802.1Q (VLAN) que atua a nível das VLANs, e tem como ideia geral identificar a rede/VLAN acrescentando 32 bits (denominados de 802.1Q *tag*) para que esses pacotes com o mesmo *tag* sejam partilhados apenas por máquinas dessa rede/VLAN; *Point-to-Point Protocol over ATM* (**PPPoA**) que

é um protocolo para encapsular *frames* em AAL5 (*ATM Adaptation Layer 5*); *Point-to-Point Protocol over Ethernet* (**PPPoE**) que é um protocolo para encapsular *frames* PPP dentro de *frames ethernet*.

São oferecidos diversos tipos de encapsulamento como: IPv4 e IPv6; tuneis IP (*Tunneled IP*) que é um canal de comunicação usado entre duas redes distintas e é usado para transportar um protocolo de outra rede. *IP-in-IP* que é um protocolo de tuneis IP que encapsula um pacote IP dentro de outro pacote IP; *Generic Routing Encapsulation* (**GRE**) que é outro protocolo de tuneis IP proprietário da Cisco que permite um encapsulamento de vários protocolos.

É possível fazer um controlo de acesso a nível de interfaces, domínio, informações de utilizador, aplicações, de tempo ou até informação transportada por *Secure Socket Layer* (**SSL**) ou *Transport Layer Security* (**TLS**) – protocolos que cifram conteúdo através dum canal seguro.

Quanto à gestão de tráfego e qualidade de serviço (*Quality of Service* – **QoS**) é possível: fazer uma gestão baseada em políticas (ex: limitar a taxa de transferência para um certo destino/origem); priorizar a largura de banda garantida/máxima; limitar o número de sessões concorrentes; utilizar o *Differentiated Services Code Point* (**DSCP**) que são 6 bits que são inseridos num *Differentiated Services Field* (**DS Field**) de 8 bits que são postos no cabeçalho de um pacote IP; redefinição do TCP *Maximum Segment Size* (**MSS**) que redefine o tamanho máximo que um segmento pode conter e, assim, reduzir a quantidade de tráfego na rede de forma a garantir uma menor saturação.

3.3.3.2 Inspeção

A NGFW efetua uma inspeção protocolar específica a: DNS; FTP; HTTP; IMAP; IMAP usando SSL (**IMAPS**); SMTP; SSH; NBT; *Server Message Block* (**SMB**) que atua como um protocolo a nível aplicacional e é usado para fornecer acesso partilhado a ficheiros, impressoras, e outras ligações pela rede; SMB2 que se diferencia da versão anterior porque ao invés de ter mais de cem comandos tem apenas dezanove e permite vários pedidos concorrentes (que na versão inicial estava limitado a um de cada vez); MSRPC; POP3; POP3 usando SSL (**POP3S**); SIP; TFTP; HTTPS.

A inspeção é feita também ao comparar impressões digitais (*fingerprinting*) de qualquer protocolo TCP/UDP. Isto consiste em tentar encontrar a origem dos dados através duma impressão digital contida neles e que é única para cada máquina.

É possível detetar anomalias/evasões utilizando: comparação de impressões digitais (*fingerprinting*) de vulnerabilidades; um motor de inspeção baseado em *software* que é atualizável e faz uma comparação do tráfego com assinaturas duma base de dados local; através de *logs* de anomalias/evasões.

Ao nível dos túneis SSL/TLS a NGFW consegue decifrar o conteúdo das *streams* cliente-servidor, analisá-lo e voltar a cifrá-lo. Faz a validação de certificados e possui uma lista de isenção de certificados de domínio, ou seja, caso seja isento será sempre aceite.

Numa nota adicional, o fato de a NGFW estar preparada para reencaminhar *logs* para um servidor de *logs* (ex: HP ArcSight) permite que haja uma correlação local em que o *log* é analisado e, consoante o seu comportamento, é detetada, ou não, uma ameaça em tempo real para ameaças pontuais ou persistentes.

Quanto a proteção de ataques como *Denial of Service* (**DoS**) / *Distributed Denial of Service* (**DDoS**), a NGFW deteta inundações de mensagens SYN (**SYN Flood**). Quando é estabelecida uma ligação entre um cliente e um servidor, é usado o protocolo *TCP three-way handshake* que pode ser observado na Figura 3.

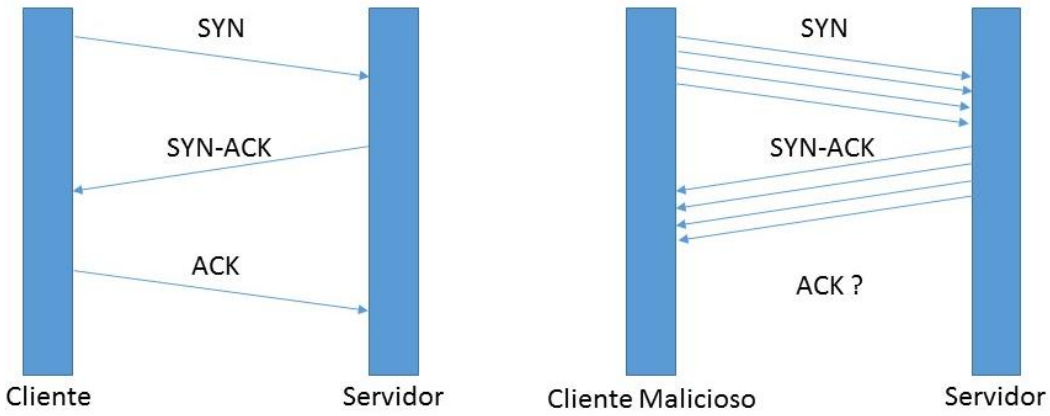


Figura 3 – TCP three-way handshake protocol

Caso o Servidor nunca receba a mensagem ACK (*Aknowledgment*), ficará à espera durante um X tempo para o receber. Se forem enviados pedidos suficientes, o servidor pode ficar sem capacidade para aceitar novos pedidos por estar à espera de receber o ACK dos pedidos anteriores.

Para prevenir este tipo de ataques (DoS/DDoS), é também feita uma limitação do número de ligações concorrentes e é feita uma compressão de *logs* baseado em interfaces para evitar a quantidade excessiva do tamanho de *logs* quando estes ataques sucedem.

Quando é detetado um ataque, existem diferentes maneiras de lidar com a situação. A NGFW oferece as seguintes: bloqueio direto em que é fechada a ligação do possível atacante; reinicio da ligação; através duma lista negra (*Blacklist*) local ou distribuída em que são bloqueadas as ligações especificadas na lista; resposta *HyperText Markup Language* (**HTML**) e/ou redireccionamento, ao invés de bloquear é redirecionado para uma página HTML onde pode ser notificado que foi detetado um possível ataque.

3.3.3.3 Web Filtering

Em algumas empresas existem políticas de uso de internet que proíbem o acesso a certas páginas que são consideradas impróprias para o local de trabalho (ex: *facebook, abola, etc*). Para ser feito esse controlo existe a possibilidade de fazer uma filtragem às páginas que podem ser acedidas.

Protocolos suportados para esta filtragem são HTTP e HTTPS. O bloqueio é possível baseado em categorias (ex: desporto, música, etc.) e por listas negras. Em alternativa é possível criar as chamadas listas brancas (*whitelist*) que permitem o acesso à lista de *Uniform Resource Locator* **(URL**), ou seja, páginas listadas (URLs presentes na lista).

A base de dados deste filtro contém cerca de 280 milhões de domínios de alto nível e subpáginas (milhares de milhões de URLs), suportando mais de 43 línguas e 82 categorias.

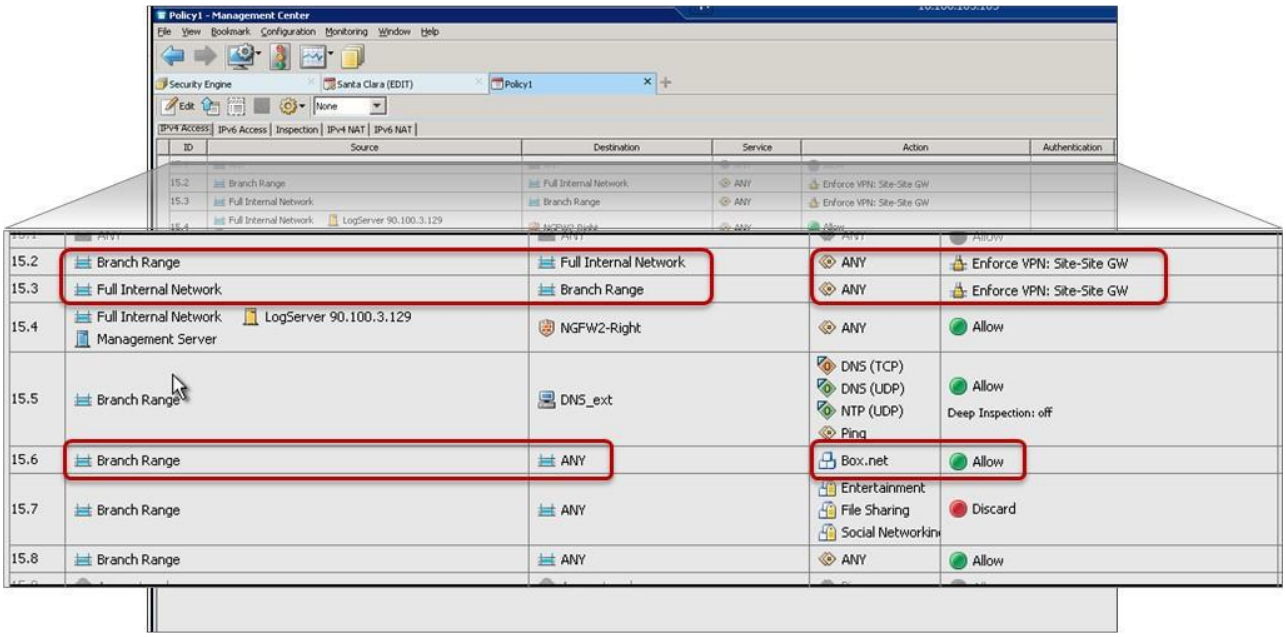
3.3.3.4 Gestão e Monitorização

A componente SMC é responsável pela gestão e monitorização. Neste componente é possível gerir e monitorizar o tráfego que passa pela NGFW através dum sistema de *logs* e relatórios (*report*). Inclusive é possível fazer um *tcpdump* que mostra informação dos pacotes que passam pela NGFW e uma captura de tráfego. Tudo isto é feito única e exclusivamente a partir do SMC.

3.4 Serviços

3.4.1 Policies

Policies são o conjunto de regras relativas ao tráfego da rede, o que é permitido ou descartado (Figura 4). Ao contrário de gerações anteriores, temos a possibilidade de bloquear aplicações. Podemos também juntar objetos de utilizadores, grupos ou até



servidores ao invés do tradicional IP nos campos de origem/destino.

Figura 4 – Regras de uma Policy

3.4.2 Logs

Um *log* é o registo individual, que contem informação variada, de cada pacote do tráfego de rede que passa pelo SMC e que, posteriormente, pode ser utilizado para elaborar *reports*.

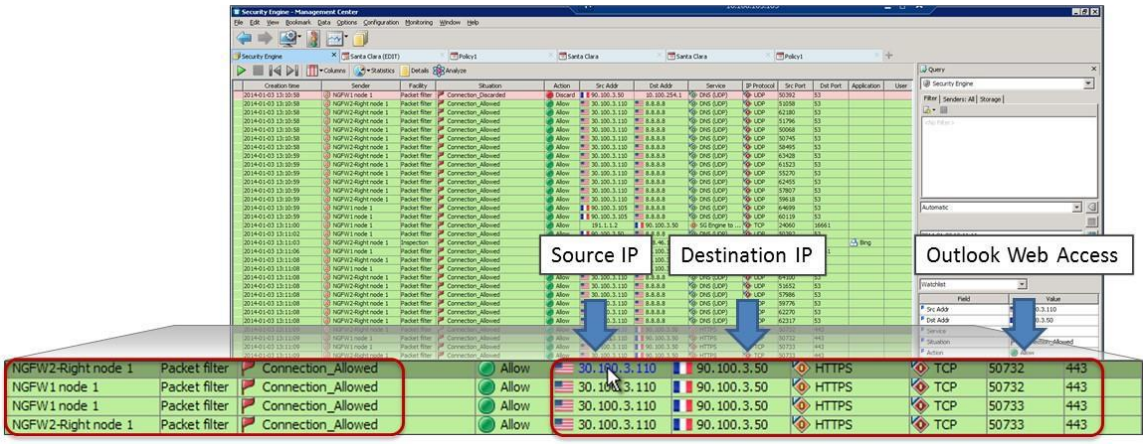


Figura 5 – Logs

Na Figura 5 podemos ver como é apresentada a informação de um pacote na NGFW na secção dos *logs*. Estes *logs* podem também ser reencaminhados para servidores que podem fazer correlações destes *logs* como, por exemplo, *Security information and event management* (SIEM).

3.4.3 Reports

Reports – a informação consolidada após a junção de vários *logs*. Esses *logs* contêm a informação individual de cada pacote que, posteriormente, possibilita a construção de gráficos e estatísticas (Figura 6).

Figura 6 – Estatísticas utilizáveis em Reports

3.4.4 Third-Party Management

O SMC da Stonesoft fornece um centro de gestão centralizado onde podem ser adicionados componentes de terceiros (Figura 7). Isto é uma mais-valia de um ponto de vista de *logs* pois permite que seja feita uma monitorização de equipamentos cujo intuito inicial seria de um funcionamento *standalone* (e não integrado num SMC).

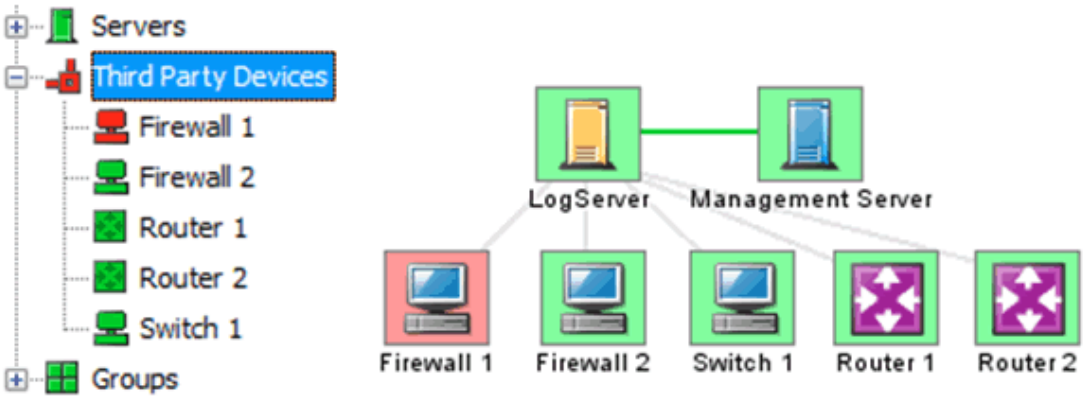


Figura 7 – Third Party Management [10]

Capítulo 4

O Trabalho

Este capítulo descreve o trabalho efetuado para implementar de raiz a solução NGFW da McAfee na organização em questão. Detalham-se as fases pelas quais passou esta concretização, iniciando-se na sua análise inicial de requisitos até à implementação na infraestrutura do cliente.

4.1 Levantamento de requisitos do cliente

Ao fazer a sua própria análise de necessidades a serem satisfeitas com esta solução NGFW, o cliente delineou os seguintes objetivos de segurança:

Identificação de aplicações – A solução deverá permitir a identificação de aplicações atuando com base nos padrões de tráfego e não apenas nos portos e protocolos utilizados;

Método de identificação – A solução deverá explicar de forma clara os métodos de identificação de aplicações, assinaturas suportadas e políticas de atualização de assinaturas;

Deteção e bloqueio de comandos maliciosos - Capacidade de deteção e bloqueio de comandos maliciosos através da análise de anomalias relativamente a padrões conhecidos. Esta funcionalidade, atuando como análise de comportamentos, deverá permitir identificar ataques 0-day;

Identificação de tráfego não autorizado - Identificação de tráfego que não esteja a circular pelos canais autorizados recorrendo p.ex. a *proxies* alternativos ou outras formas de dissimulação de tráfego para ultrapassar os mecanismos de proteção existentes;

Identificação de tráfego aplicacional - Identificação de tráfego aplicacional com detalhe das ações realizadas, permitindo um controlo pormenorizado, distinguindo ações simples de leitura, comandos destrutivos, partilha/envio de ficheiros ou ambiente de trabalho,

chamadas e videoconferência VoIP, etc. Como exemplo de aplicações cujo tráfego deve ser analisado temos*: Facebook, Dropbox, Skype*;

Inspeção de tráfego cifrado - Inspeção de tráfego cifrado utilizando os protocolos SSL/TLS, independentemente do porto utilizado;

Definição de políticas baseadas no tipo de tráfego - Capacidade de definir políticas de uso aceitável com base no tipo de tráfego, utilizadores e rede ou endereços de origem e/ou destino desse tráfego;

Identificação e bloqueio de tráfego de redes perigosas - Capacidade de identificar e bloquear tráfego com origem/destino em redes identificadas como perigosas, por exemplo reportadas como redes de *botnets*.

De seguida, é detalhada a forma como estes requisitos são atingidos.

4.1.1 Identificação de aplicações

A solução deverá permitir a identificação de aplicações atuando com base nos padrões de tráfego e não apenas nos portos e protocolos utilizados.

A NGFW é capaz de identificar aplicações, independentemente da porta por onde o tráfego passe. Por exemplo, se uma aplicação, como o *telnet*, utilizar a porta 2323/tcp, a NGFW da McAfee é capaz de detetá-la e, caso haja uma regra que bloqueie essa aplicação, esse padrão de tráfego será rejeitado.

A NGFW da McAfee é capaz de detetar um grande número de aplicações, aproximadamente 1000, contabilizando aplicações primárias e aplicações baseadas na identificação de tráfego.

Além disso, esta funcionalidade pode ser anexada à autenticação de utilizadores com a AD, de forma a podermos definir que utilizadores têm acesso às aplicações, dependendo do grupo e/ou de onde se ligam (Figura 8).

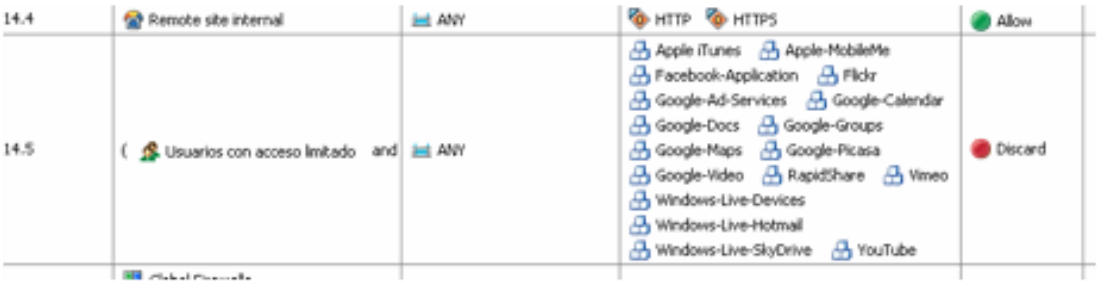


Figura 8 – Política que limita acesso de um grupo de utilizadores

4.1.2 Método de identificação

A Solução deverá explicar de forma clara os métodos de identificação de aplicações, assinaturas suportadas e políticas de atualização de assinaturas.

A NGFW da McAfee utiliza um método chamado DFA (*Deterministic Finite Automation*). Este método é bastante eficaz na busca de padrões de tráfego sobre grandes quantidades de dados, por vários motivos:

- Consegue obter maior rendimento que outros métodos existentes, uma vez que compara os padrões apenas naqueles protocolos e partes do protocolo onde tem efetivamente que comparar.

- Por conseguinte, o número de falsos positivos é reduzido porque, por exemplo, identifica um *cross site scripting* numa estrutura de dados SMTP, fazendo-o apenas em HTTP.

Além disso, para a correspondência de padrões, utilizamos uma linguagem proprietária baseada em expressões regulares, que é bastante simples de aprender através de uma formação de apenas 10 horas.

Através deste tipo de análise, não só comparamos os padrões de assinaturas como também as malformações nos protocolos e a estandardização do mesmo, o que nos permite ter uma maior granularidade que outros NGFW na deteção de "*0-day exploits*" (ataques que exploram vulnerabilidades que ainda não tinham sido identificadas e, portanto, dificilmente podem ser detetados).

As bases de dados de assinaturas e formas de análise são normalmente atualizadas na segunda terça-feira de cada mês, de forma automática, embora isto possa ser configurado no sistema. No entanto, caso haja uma vulnerabilidade grave, pode haver

uma atualização antes da data prevista. Para tal, o sistema é capaz de verificar a cada 20 minutos, se existe uma nova versão, fazer o *download* e atualizá-la.

4.1.3 Deteção e bloqueio de comando maliciosos

Capacidade de deteção e bloqueio de comandos maliciosos através da análise de anomalias relativamente a padrões conhecidos. Esta funcionalidade, atuando como análise de comportamentos, deverá permitir identificar ataques 0-day.

Os ataques baseados em *0-day exploits* são muito difíceis de detetar. Com a NGFW da McAfee, a taxa de deteção deste tipo de ataques é muito elevada, pois esta é capaz de analisar, não só as assinaturas, mas também o protocolo propriamente dito e procurar malformações do mesmo.

O IPS da NGFW utiliza um método de inspeção de pacotes baseado em diferentes tipos de deteções. Podem ser baseados em assinaturas, estatísticas de tráfego e / ou anomalias de protocolo.

O IPS da McAfee é baseado em dois módulos principais, que se complementam entre eles. São o *Sensor* e *Analyzer* (Figura 9).

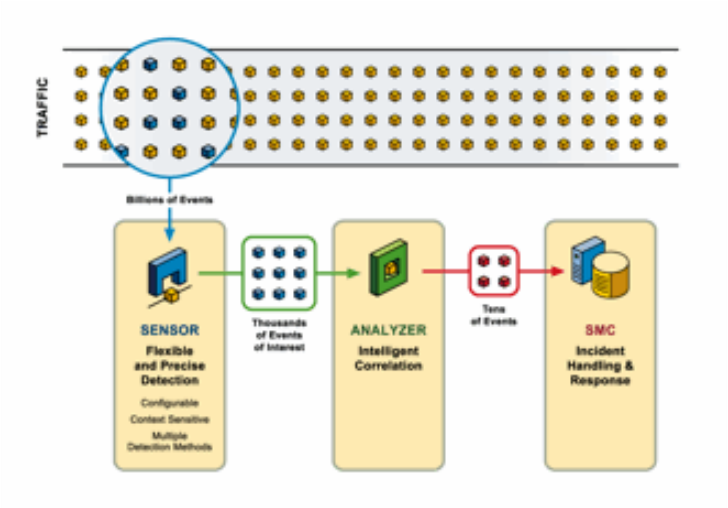


Figura 9 – Sensor e analisador da NGFW McAfee

O sensor é responsável por detetar padrões, que, uma vez detetados, geram eventos que são passados ao analisador para processamento. Quando o analisador recebe eventos, dependendo das suas políticas, processa e escala os eventos que lhe vão chegando de cada um dos sensores distribuídos pela rede. Com base nesta correlação, a qual é explicada

neste documento, são gerados os *logs* necessários ou, inclusivamente, alertas, cortes de ligações, etc.

Deteção de Eventos no Sensor

Para tal, em cada um dos métodos de deteção utilizados se encarrega de procurar qualquer anomalia da seguinte forma:

Deteção baseada em assinaturas

Neste método são utilizadas expressões regulares baseadas no contexto do protocolo em que um ataque ou tentativa de ataque pode ser realizado. Assim, apenas procura por *exploits* que são prejudiciais para protocolos como HTTP dentro desse mesmo protocolo e não de qualquer outro. Dentro desse protocolo, se uma assinatura está definida apenas para *http client stream*, fará a pesquisa apenas dentro desse *stream*.

Com este método de analise, comparando e detetando assinaturas, dada a dimensão da arquitetura de *hardware*, é aumentado o desempenho tanto da rede como dos serviços e alertas gerados.

Deteção baseada em estatísticas de tráfego

Nem todos os ataques são considerados ataques por todas as empresas: o que é o tráfego normal para uma empresa pode ser uma negação de serviço para outra, e vice-versa, o que é normal para uma empresa pode ser uma perda de serviço para outra. Por isso é importante conhecer a utilização das redes e dimensionar a arquitetura das mesmas para que, caso haja desvio aos padrões, seja possível emitir um aviso ou alerta com as informações dos eventos. A Figura 10, Figura 11 e Figura 12 mostram-nos exemplos de estatísticas que podem ser recolhidas através da NGFW da McAfee. Desta forma, é possível perceber se o nosso sistema funciona corretamente e reage atempadamente evitando danos maiores e que posteriormente seriam de mais difícil resolução.

Figura 10 – Relatório sobre o número de ligações por Origem

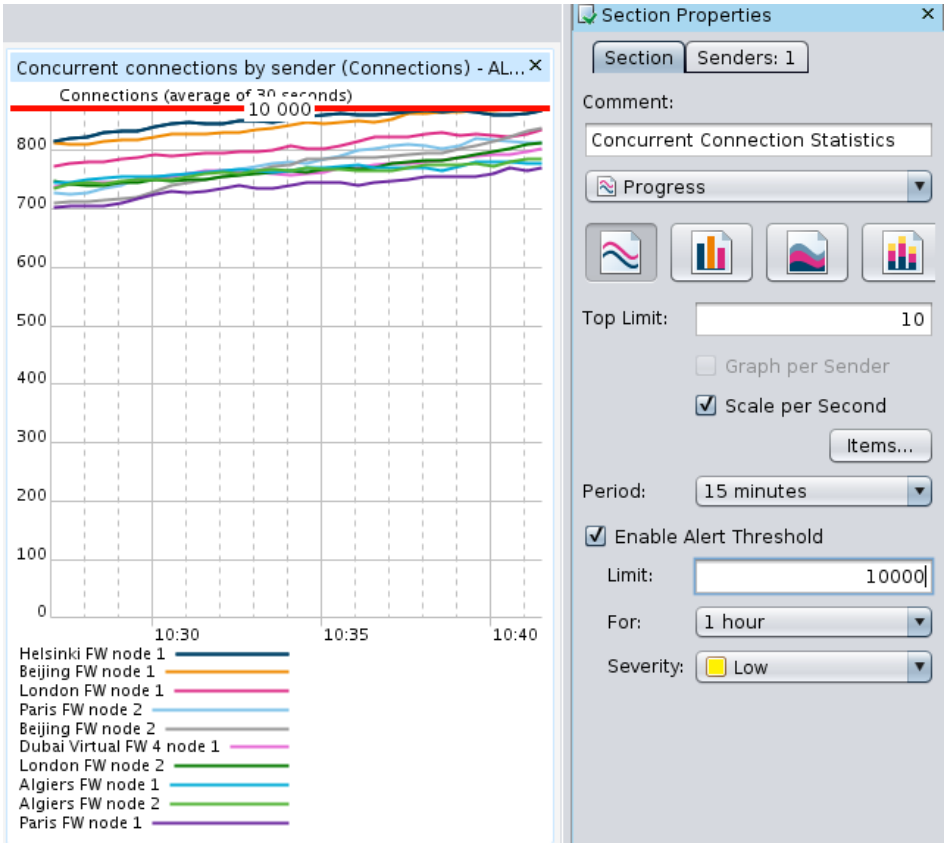


Figura 11 – Relatório sobre a utilização das aplicações

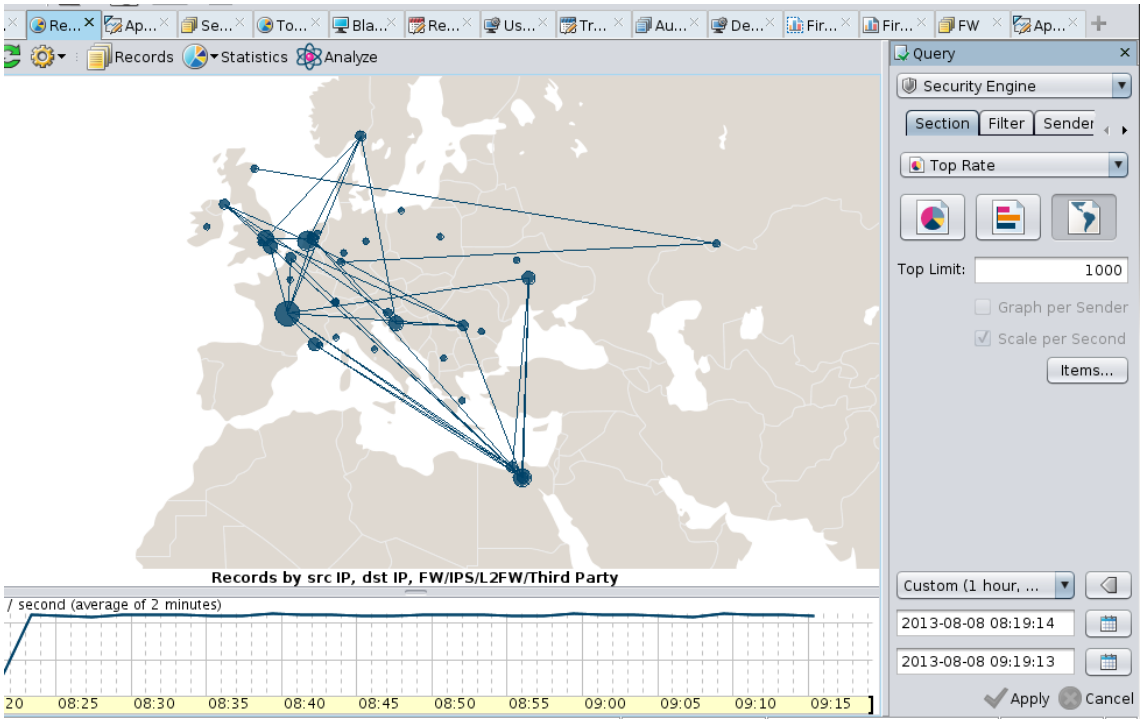


Figura 12 – Relatório geográfico sobre as origens/destinos

Deteção baseada em anomalias de protocolo

Muitos ataques são baseados em vulnerabilidades dos próprios protocolos. O IPS da NGFW faz uma análise detalhada de todo o tráfego que passa pelo IPS procurando anomalias de protocolo que não sejam consistentes com o RFC para cada um dos protocolos.

Assim, é possível que, no caso de um ataque *Zero Day Exploit* baseado numa anomalia detetada no protocolo, o IPS da NGFW o detete a tempo sem que este possa causar dano nos sistemas por ser um ataque para o qual ainda não existe assinatura de deteção criada.

Correlação de eventos no analisador

Assim que o analisador receba os eventos, estes são processados e correlacionados com base em vários tipos de correlação:

Correlação com base em sequências

São correlações complexas que requerem um pedido do cliente e uma resposta do servidor. Em caso afirmativo, se tudo for cumprido no tempo indicado no estado de correlação, os alertas correspondentes e as ações a tomar são enviadas.

Esta abordagem permite reduzir os falsos positivos. Outros sistemas de deteção de intrusão, ao detetar o início de um ataque, lançam um alerta sem ter em consideração que não é um ataque e que esse resultado positivo é insignificante caso não seja seguido de outro tipo de eventos.

Correlação baseada em grupos

Neste tipo de correlação, sendo do mesmo tipo que a anterior, enquanto na anterior era importante a ordem, neste o importante são os grupos. Se, por um lado, um evento isolado, por si só, não causa qualquer efeito nocivo na rede, se este for acompanhado de outros dentro de um intervalo de tempo fechado, pode causar graves perturbações na infraestrutura de rede.

Não é necessário gerar um alerta sempre que detetamos um evento. Apenas será necessário no momento em que o dito ataque está a acontecer, mantendo obviamente um log com o registo de todos os eventos.

Correlação baseada na compressão de eventos

Uma técnica de evasão ao IPS é enviar muitos eventos de modo a que o servidor não seja capaz de processá-los e deixe de responder, ou execute as ações tardiamente, quando o sistema já nada pode fazer contra o ataque. Uma técnica para evitar estas situações é comprimir os eventos de modo a que, se um evento ocorre "n" vezes, o analisador apresente apenas uma entrada nos *logs* durante uma janela de tempo, evitando o ruído no sistema. Assim poderemos concentrar-nos nos *logs* e nos ataques que efetivamente estão a ocorrer.

Correlação baseada em contagem de eventos

Muitos dos eventos que se produzem podem, por si só, não ser um ataque. No entanto, se tal evento ou tentativa de ataque tem ocorrido mais de um determinado número de vezes, num intervalo de tempo definido, pode tornar-se num ataque.

Correlação baseada em ocorrências de outros eventos

Este tipo de correlação é baseado em outros tipos de eventos: por exemplo, se for feito um *scan*, depois forem detetadas tentativas de ataques e ainda um *log flooding* a partir dos mesmos endereços IP de origem, podemos determinar que o IP em questão está a tentar efetuar um ataque e este será mantido sob vigilância de modo a evitar futuros ataques.

4.1.4 Identificação de tráfego não autorizado

Identificação de tráfego que não esteja a circular pelos canais autorizados, recorrendo p.ex. a proxies alternativos ou outras formas de dissimulação de tráfego para ultrapassar os mecanismos de proteção existentes.

A NGFW da McAfee incorpora um potente sistema de filtro de URLs baseado em categorias. Para tal utiliza a base de dados e o serviço da BrightCloud sendo as suas principais caraterísticas e benefícios:

- Mais de 200 milhões de URLs em mais de 90 categorias;
- Disponibiliza informação acerca da atividade de cada URL;
- Proteção ativa contra *Malware* e *Phishing*;
- Permite notificação de utilizadores;
- Permite *whitelisting* e *blackllisting* de URLs

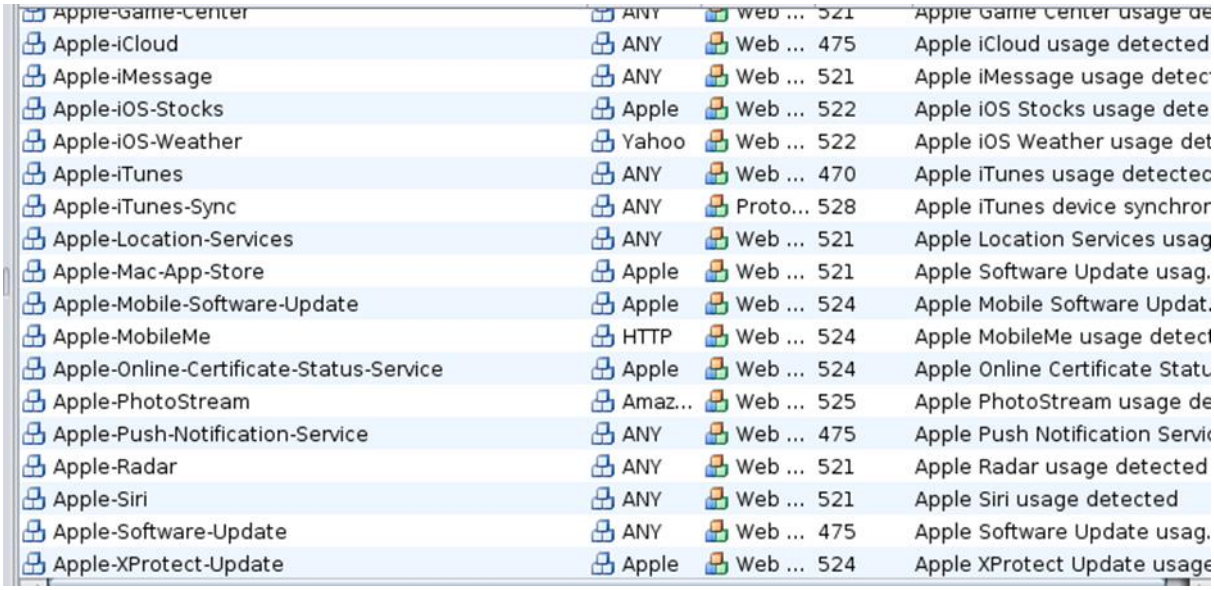
Adicionalmente podem ser realizadas filtragens baseadas no *upload* e *download* de tipos de ficheiros e/ou extensões, independentemente da extensão que tenha o ficheiro. Também é possível filtrar por conteúdo do ficheiro.

4.1.5 Identificação de tráfego aplicacional

Identificação de tráfego aplicacional com detalhe das ações realizadas, permitindo um controlo pormenorizado, distinguindo ações simples de leitura, comandos destrutivos, partilha/envio de ficheiros ou ambiente de trabalho, chamadas e videoconferência VoIP, etc. Por exemplo: Facebook, Dropbox, Skype.

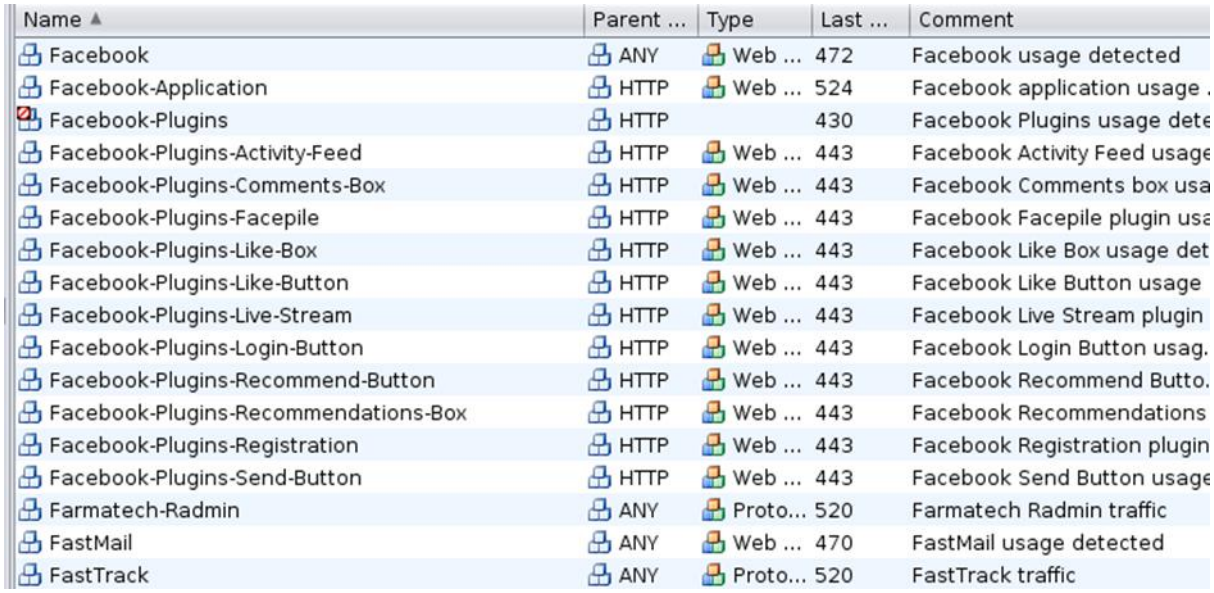
A NGFW da McAfee é capaz de identificar as aplicações e entrar mais em detalhes em cada uma delas. É possível identificar atividades de *upload* e *download* de ficheiros nas aplicações, por exemplo. Essa capacidade de análise também pode ser aplicada a informação contida dentro do protocolo HTTPS.

As figuras a seguir apresentam exemplos de aplicações, e respetivas atividades, que podem ser detetadas (Figura 13, Figura 14, Figura 15, Figura 16).



Apple-Game-Center	ANY	Web ...	521	Apple Game Center usage de
Apple-iCloud	ANY	Web ...	475	Apple iCloud usage detected
Apple-iMessage	ANY	Web ...	521	Apple iMessage usage detec
Apple-iOS-Stocks	Apple	Web ...	522	Apple iOS Stocks usage dete
Apple-iOS-Weather	Yahoo	Web ...	522	Apple iOS Weather usage det
Apple-iTunes	ANY	Web ...	470	Apple iTunes usage detected
Apple-iTunes-Sync	ANY	Proto...	528	Apple iTunes device synchror
Apple-Location-Services	ANY	Web ...	521	Apple Location Services usag
Apple-Mac-App-Store	Apple	Web ...	521	Apple Software Update usag.
Apple-Mobile-Software-Update	Apple	Web ...	524	Apple Mobile Software Updat.
Apple-MobileMe	HTTP	Web ...	524	Apple MobileMe usage detect
Apple-Online-Certificate-Status-Service	Apple	Web ...	524	Apple Online Certificate Statu
Apple-PhotoStream	Amaz...	Web ...	525	Apple PhotoStream usage de
Apple-Push-Notification-Service	ANY	Web ...	475	Apple Push Notification Servi
Apple-Radar	ANY	Web ...	521	Apple Radar usage detected
Apple-Siri	ANY	Web ...	521	Apple Siri usage detected
Apple-Software-Update	ANY	Web ...	475	Apple Software Update usag.
Apple-XProtect-Update	Apple	Web ...	524	Apple XProtect Update usage

Figura 13 – Aplicações Apple



Name ▲	Parent ...	Type	Last ...	Comment
Facebook	ANY	Web ...	472	Facebook usage detected
Facebook-Application	HTTP	Web ...	524	Facebook application usage .
Facebook-Plugins	HTTP		430	Facebook Plugins usage dete
Facebook-Plugins-Activity-Feed	HTTP	Web ...	443	Facebook Activity Feed usage
Facebook-Plugins-Comments-Box	HTTP	Web ...	443	Facebook Comments box usa
Facebook-Plugins-Facepile	HTTP	Web ...	443	Facebook Facepile plugin usa
Facebook-Plugins-Like-Box	HTTP	Web ...	443	Facebook Like Box usage det
Facebook-Plugins-Like-Button	HTTP	Web ...	443	Facebook Like Button usage
Facebook-Plugins-Live-Stream	HTTP	Web ...	443	Facebook Live Stream plugin
Facebook-Plugins-Login-Button	HTTP	Web ...	443	Facebook Login Button usag.
Facebook-Plugins-Recommend-Button	HTTP	Web ...	443	Facebook Recommend Butto.
Facebook-Plugins-Recommendations-Box	HTTP	Web ...	443	Facebook Recommendations
Facebook-Plugins-Registration	HTTP	Web ...	443	Facebook Registration plugin
Facebook-Plugins-Send-Button	HTTP	Web ...	443	Facebook Send Button usage
Farmatech-Radmin	ANY	Proto...	520	Farmatech Radmin traffic
FastMail	ANY	Web ...	470	FastMail usage detected
FastTrack	ANY	Proto...	520	FastTrack traffic

Figura 14 – Aplicações Facebook

Google-Admeld	HTTP	Web ...	488	Google Admeld usage detect
Google-Analytics	ANY	Web ...	521	Google Analytics usage dete
Google-App-Engine	HTTP	Web ...	488	Google App Engine usage de
Google-Cache	HTTP	Web ...	408	Google Cache usage detecte
Google-Calendar	Google	Web ...	517	Google Calendar usage dete.
Google-Code	Google	Web ...	437	Google Code usage detected
Google-Docs	Google	Web ...	517	Google Docs usage detected
Google-DoubleClick	ANY	Web ...	521	Google DoubleClick usage de
Google-Earth	HTTP	Web ...	514	Google Earth usage detected
Google-Groups	Google	Web ...	517	Google Groups usage detect
Google-Mail	ANY	Web ...	475	Google Mail usage detected
Google-Maps	Google	Web ...	517	Google Maps usage detected
Google-Orkut	HTTP	Web ...	524	Google Orkut usage detected
Google-Picasa	Google	Web ...	517	Google Picasa usage detecte
Google-Plus	Google	Web ...	426	Google+ usage detected
Google-Reader	Google		532	Google Reader usage detect
Google-Safebrowsing	HTTP	Web ...	419	Google Safebrowsing service

Figura 15 – Aplicações Google

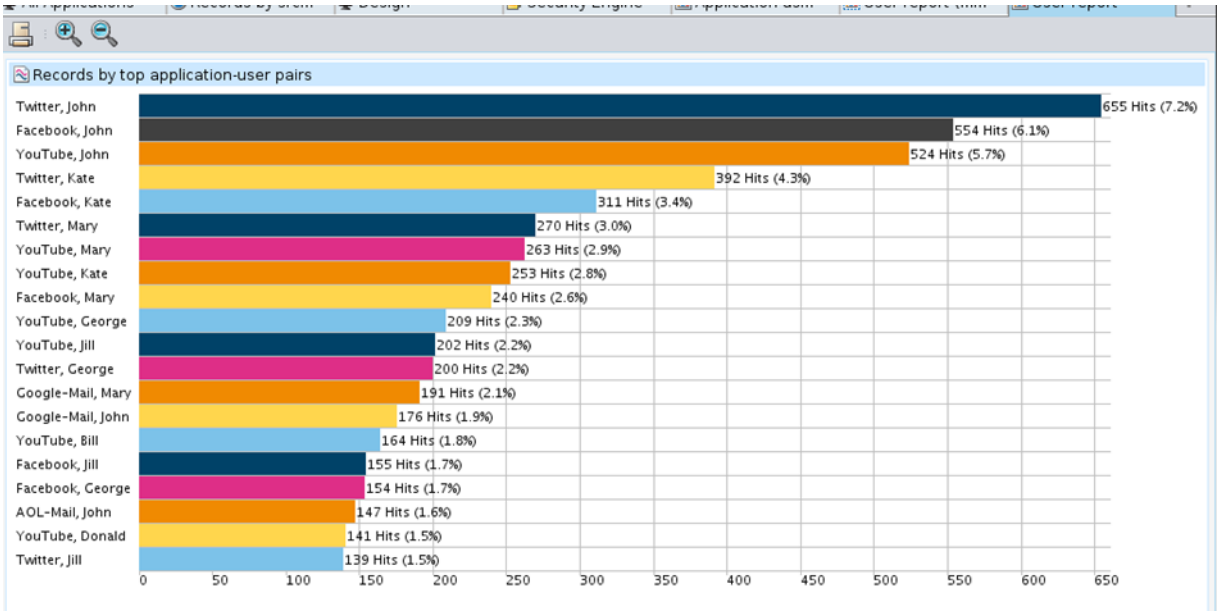


Figura 16 – Relatório sobre pares Aplicação-Utilizador

4.1.6 Inspeção de tráfego cifrado

Inspeção de tráfego cifrado utilizando os protocolos SSL/TLS, independentemente do porto utilizado.

A NGFW da McAfee é capaz de inspecionar o tráfego HTTPS, ou seja, tráfego cifrado SSL. Assim, com o IPS seremos capazes de distinguir se o tráfego SSL que passa pela nossa rede é tráfego HTTP, ou não, e inspecioná-lo com o objetivo de proteger tanto os servidores como os utilizadores. Não é necessário equipamento externo. A Figura 17 mostra os elementos da configuração de inspeção TLS.

O protocolo TLS permite às aplicações comunicar pela rede de um modo que garante a confidencialidade e integridade das comunicações. No entanto, as ligações cifradas podem ser utilizadas para encapsular tráfego malicioso. A funcionalidade de Inspeção TLS decifra o tráfego TLS de modo a que este possa ser inspecionado como se fosse tráfego em claro, cifrando-o, em seguida, antes de enviá-lo ao destino.

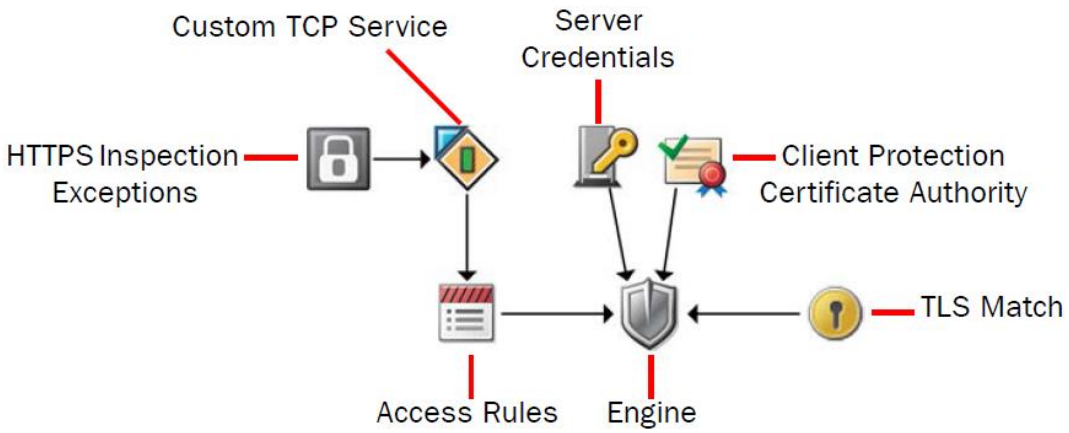


Figura 17 – Elementos da configuração de Inspeção TLS

A Inspeção TLS pode ser aplicada a diferentes componentes:

- Proteção dos servidores ao inspecionar as ligações TLS com destino em servidores da rede protegida do cliente;
- Proteção dos clientes ao inspecionar as ligações TLS iniciadas por utilizadores da rede protegida do cliente.

Requisitos para Proteção de Servidores

Quando é efetuado uma ligação TLS a um servidor protegido, o *Security Engine* irá utilizar o certificado e chave privada configuradas para o servidor de modo a decifrar

e analisar o tráfego. A chave privada e certificado do servidor interno que se pretende proteger têm de ser compatíveis com *OpenSSL* e estar no formato PEM.

Requisitos para Proteção dos Clientes

Quando um cliente interno efetua uma ligação TLS a um servidor externo, o Security Engine irá gerar um certificado substituto que será utilizado para estabelecer a ligação segura com o cliente. O *Security Engine* utiliza uma "*Client Protection Certificate Authority*" para assinar os certificados gerados. Caso esta entidade certificadora não seja confiada pelos utilizadores, será emitido um alerta pelo *browser*. Caso o cliente não disponha de uma entidade certificadora interna, poderá ser gerada uma nova no *Security Engine*, devendo o seu certificado ser publicado como confiável nos *browsers* dos utilizadores. Esta funcionalidade está disponível para o protocolo HTTPS, independentemente do porto utilizado.

4.1.1 Definição de políticas baseadas no tipo de tráfego

Capacidade de definir políticas de uso aceitável com base no tipo de tráfego, utilizadores e rede ou endereços de origem e/ou destino desse tráfego.

A NGFW da McAfee é capaz de implementar segurança com base em nomes de utilizadores, de modo a que um utilizador, depois de estar com sessão iniciada na AD, possa ser identificado pelo endereço IP obtido através de DHCP e atribuídas as permissões adequadas, consoante o grupo a que pertença, a permissão do utilizador, ou mesmo a rede à qual está ligado (Figura 18, Figura 19).

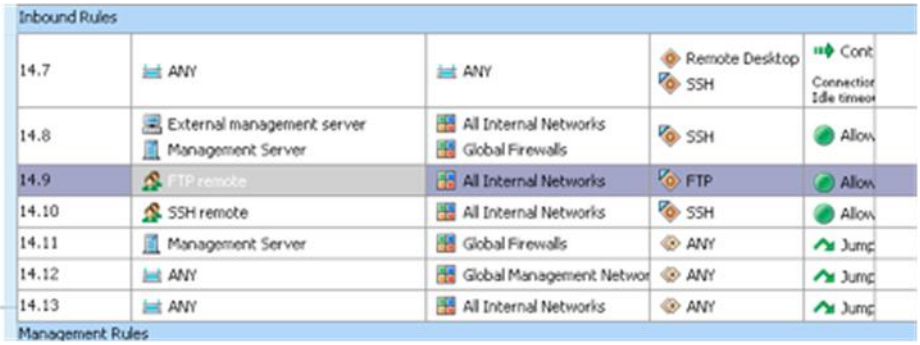


Figura 18 – Exemplo de regra de acesso aplicada a um grupo de utilizadores

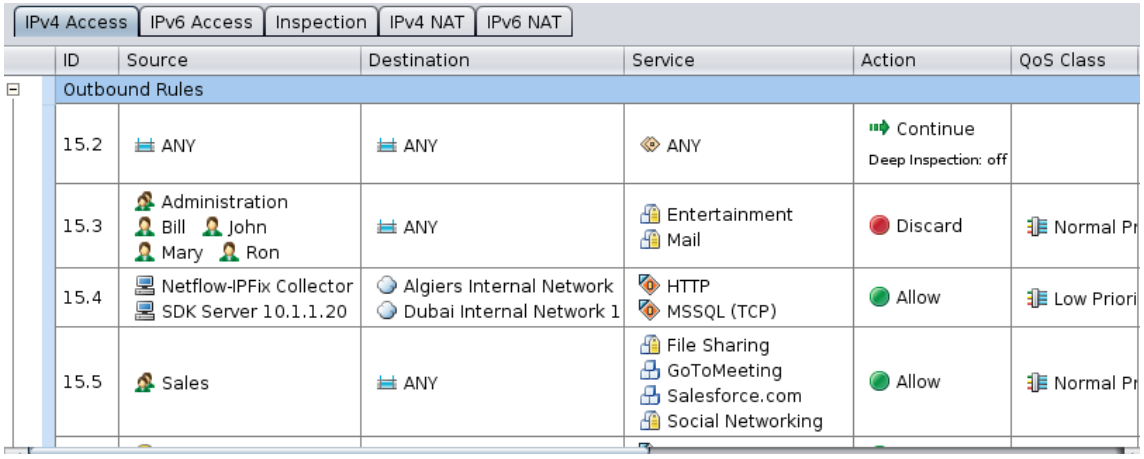


Figura 19 – Exemplo de regra de acesso aplicada a utilizadores ou grupos.

Da mesma forma, após ser feito o log na *firewall* dos acessos desses utilizadores, a partir do *Report System*, podemos definir relatórios que indicam a utilização e acessos que são feitos na rede, identificado diretamente por utilizador (Figura 20).

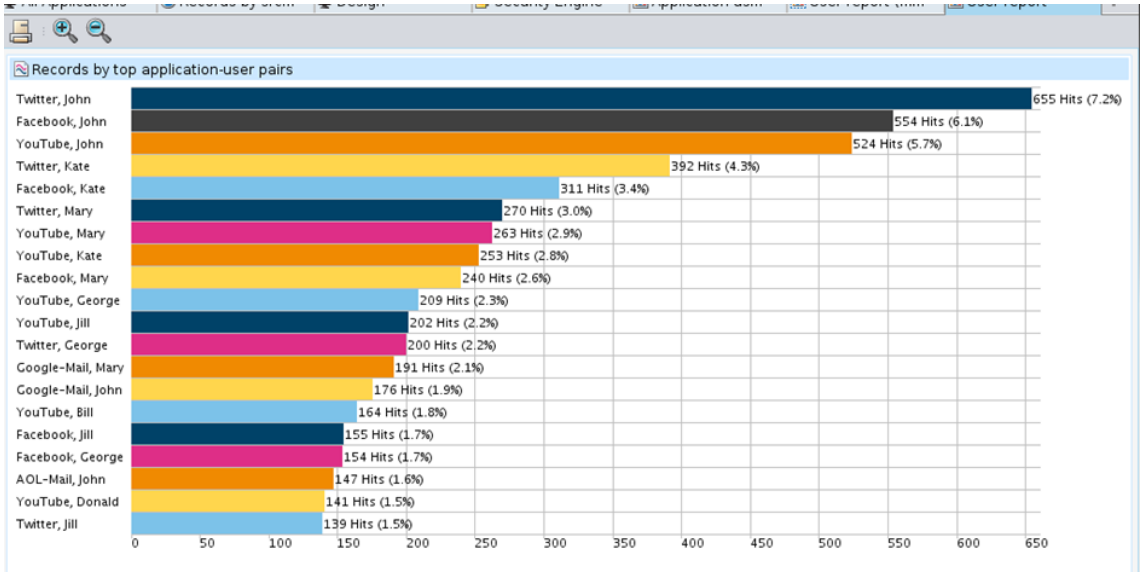


Figura 20 – Relatório sobre pares Aplicação-Utilizador

Podem ainda ser identificados grupos ou zonas, redes e outros elementos, tais como aplicações e subaplicações, ou seja, aplicações que estão dentro de outra aplicação principal, por exemplo, no caso do Facebook consideraríamos uma subaplicação o *chat*, um jogo, etc.

4.2 Desenho

A Figura 21 mostra o desenho arquitetural da solução da NGFW da McAfee que foi implementada na rede do cliente em 4 locais distintos, fruto da análise de requisitos efetuada.

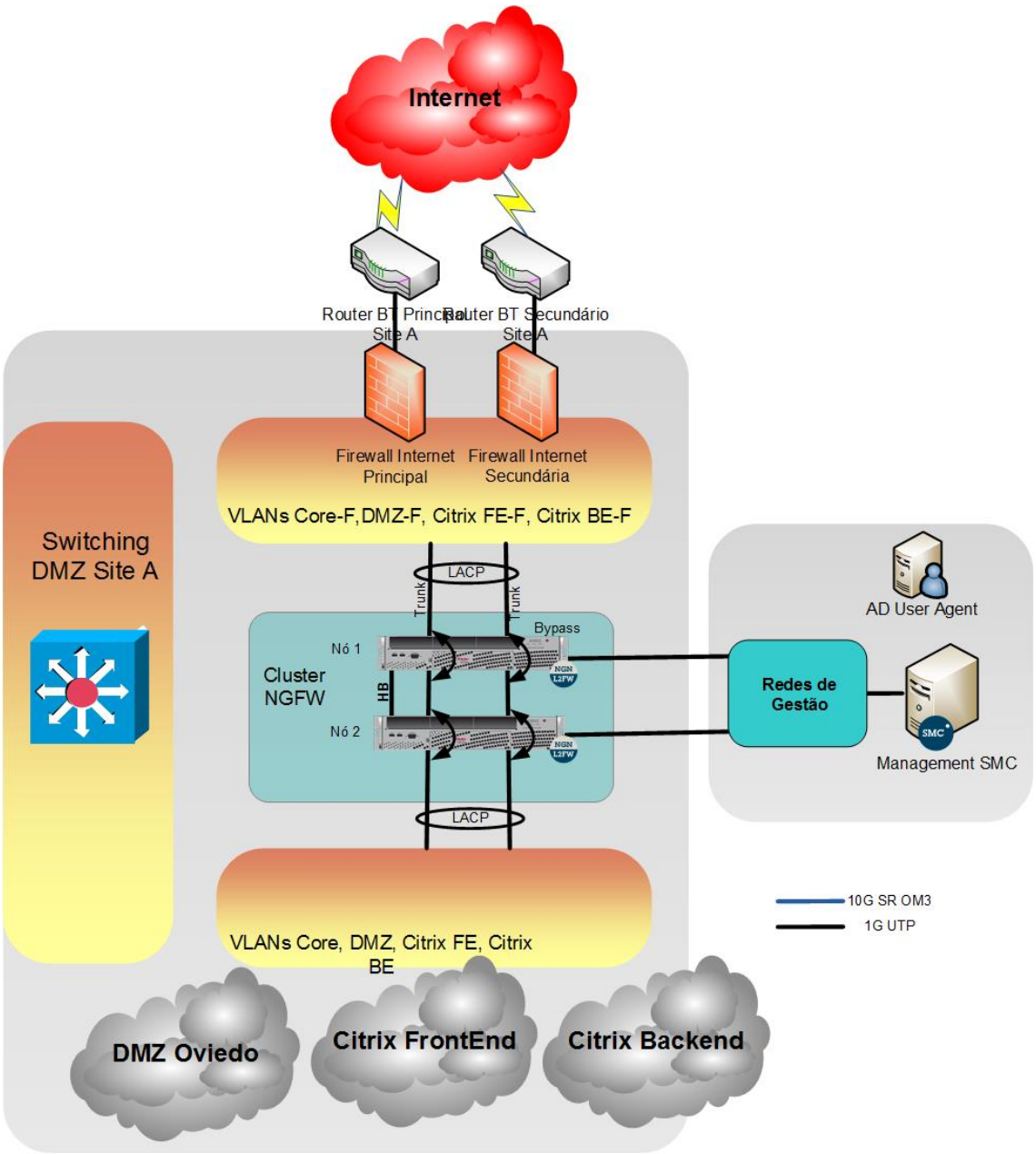


Figura 21- Arquitetura implementada no cliente

Nesta implementação o *cluster* de NGFW foi colocado em série *inline*, o tráfego passa sempre pelos 2 nós que têm um algoritmo que define quem é que processa as regras

de segurança. Na falha de um dos nós é efetuado um *bypass* aos seus interfaces, isto é, enquanto o nó da NGFW estiver ativo, o tráfego é filtrado e inspecionado por este, caso exista algum tipo de indisponibilidade em que o nó fique inativo (*offline)*, é feito o *bypass* automaticamente ao interface e o outro nó da NGFW passa a filtrar todo o tráfego. Para garantir a redundância das ligações, o trafego é intercetado num par de links a 10 Gbps em fibra. Estes links estão agregados a 20 Gbps com de *Link Aggregation Control Protocol* (LACP), que permite combinar/agregar múltiplas ligações em paralelo de forma a garantir redundância e oferecer maior largura de banda.

4.3 Pré-Configuração

Antes de serem enviadas ao cliente, é necessário efetuar algumas pré-parametrizações em todas as *appliances*. Esta fase preparatória, denominada de *staging*, tem como objetivo efetuar eventuais atualizações necessárias às máquinas NGFW da McAfee, caso tenham sido disponibilizadas novas versões enquanto era feito o transporte das *appliances*.

Na Figura 22 podemos ver a configuração descrita no fim do ponto anterior em que é descrita a configuração de cada par de interfaces em modo *inline*.

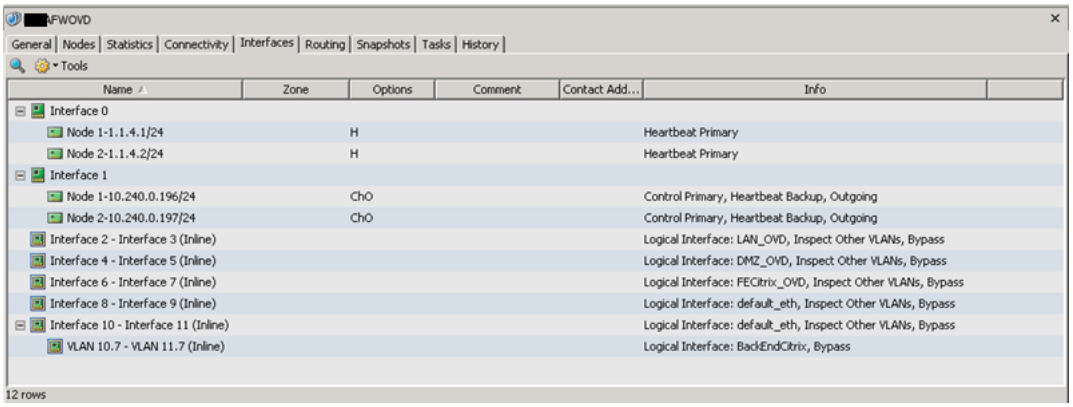


Figura 22 – Configuração de Interfaces

Para além dessas configurações, outras se podem fazer para que quando as *appliances* chegarem ao cliente sejam praticamente *plug-and-play*. Nomeadamente, dado que o cliente providenciou antecipadamente as devidas informações, conseguiu-se pré-configurar os endereços IP de cada interface das máquinas, *hostnames*, servidores de DNS, SMTP, *Network Time Protocol* (NTP), etc.

Após estas definições preliminares, as máquinas são enviadas ao cliente onde serão instaladas no seu *datacenter* já com endereços e ligações a outros serviços definidos.

4.4 Instalação no cliente

4.4.1 Instalação dos Nós

Seguem-se imagens feitas num ambiente virtual que representam a instalação real feita no cliente. Após a fase do *staging*, os nós foram pré-configurados escolhendo o papel que ia tomar Figura 23.

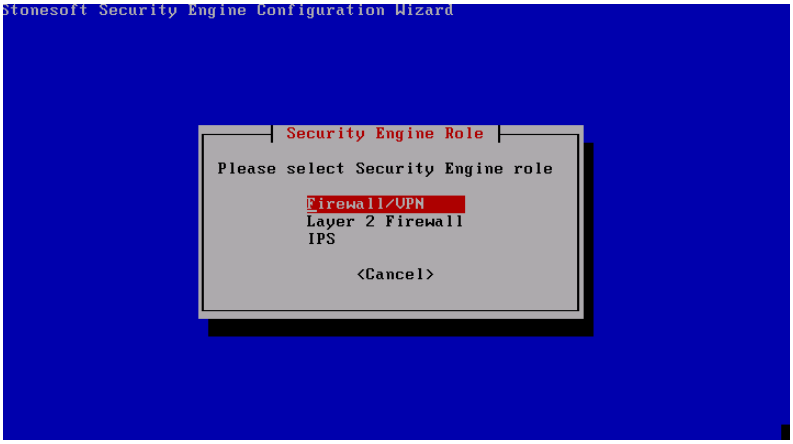


Figura 23 – Escolha do Papel do nó (role)

Posteriormente foi definido o nome do nó (*hostname*) e *password* para aceder ao nó (Figura 24)

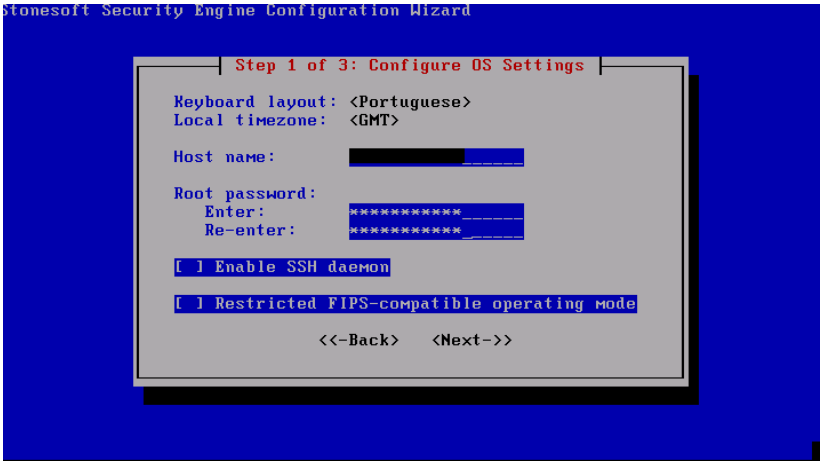


Figura 24 – Definição de hostname e password

Depois foi feito um teste para detetar todos os interfaces existentes no nó (Figura 25), e escolher o interface que ia ser utilizado para gestão (onde ia comunicar com o SMC).

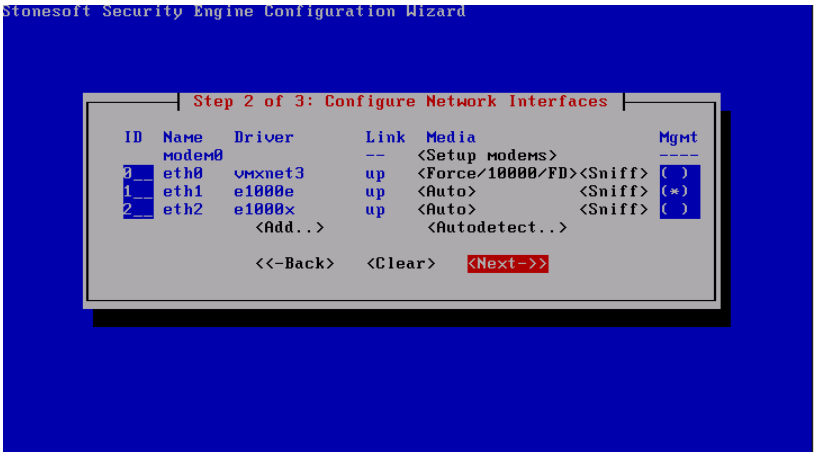


Figura 25 – Deteção dos interfaces do nó

Por fim, na Figura 26 é possível definir como é feito a atribuição de IP (DHCP ou manual) e se é, ou não, feita uma ligação ao servidor de gestão (SMC) por parte do nó. Por motivos de segurança pode ser adicionado uma *one-time password* (OTP).

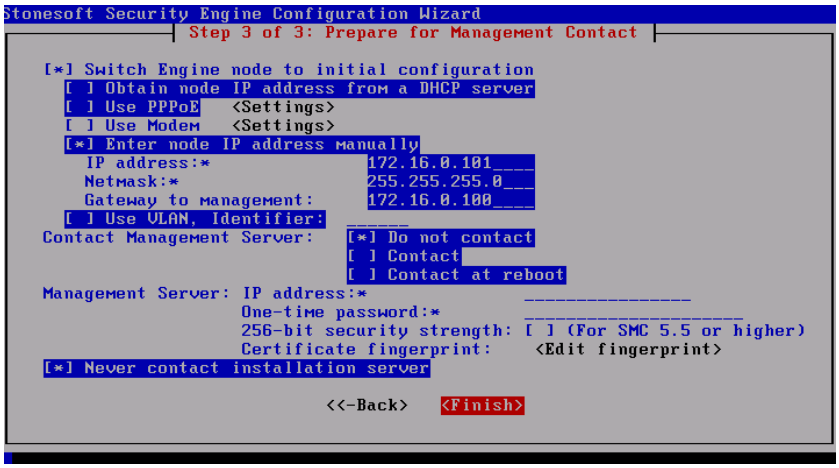


Figura 26 – Definição do IP e Servidor SMC

No caso do cliente foi adicionado um IP manualmente (não o representado na figura) e foi definido que o nó deveria contatar o servidor de gestão (SMC), utilizando uma OTP, para ser feita a instalação de políticas no nó. Este processo foi replicado para o outro nó. Após o fim da implementação desta solução, foi necessário fazer a atualização de ambos os nós. Isto porque a versão inicialmente instalada durante o *staging* (5.4.1) e a versão disponível no fim da implementação (5.5.6) era substancial. Ao ser feita a atualização é oferecido um sistema de *dual boot* em que, no fim da atualização do nó, é sempre guardada a versão anterior à atualização. Desta forma, caso exista algum problema de

compatibilidade ou instalação que provoque um estado erróneo do nó, é sempre possível voltar a um estado válido de bom funcionamento.

4.4.2 Instalação da Consola de gestão (SMC)

A instalação da consola de gestão foi um processo extremamente simples em que foram apenas necessário os seguintes passos:

Definir o IP do servidor de gestão onde é instalado o SMC (Figura 27)

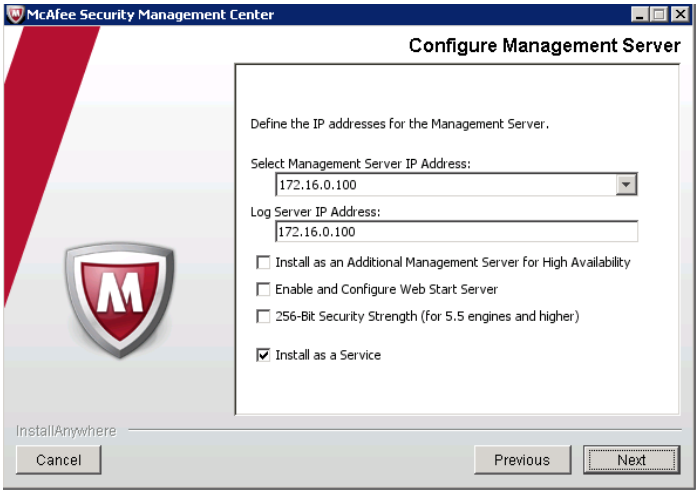


Figura 27 – Configuração Servidor SMC

Criação duma conta de administração (Figura 28)

Figura 28 – Criação de conta de Administração

Por fim, opcionalmente, definir um servidor de *logs* onde serão recolhidos os *logs* provenientes dos nós (Figura 29).

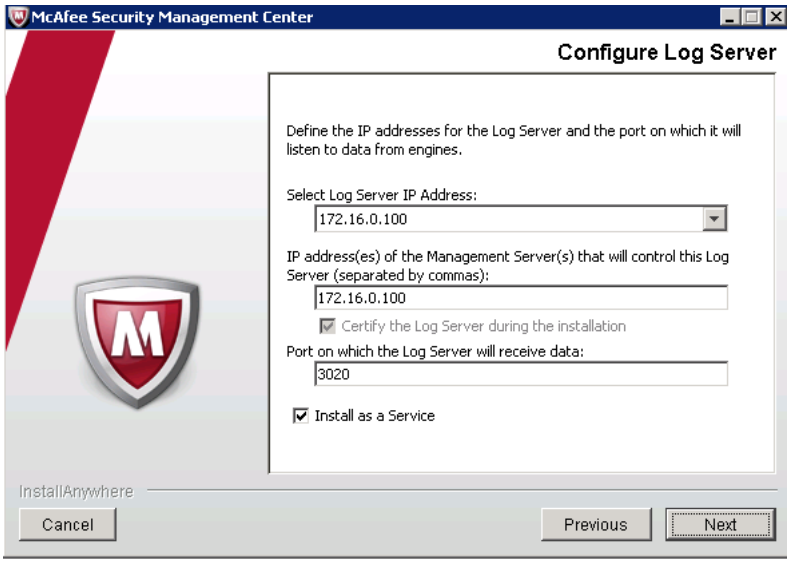


Figura 29 – Configuração do servidor de logs

Depois da instalação, é necessário proceder à configuração dos nós individualmente (*single node*) e, posteriormente, o *cluster* (Figura 30). É necessário criar os nós como objetos representativos no SMC.

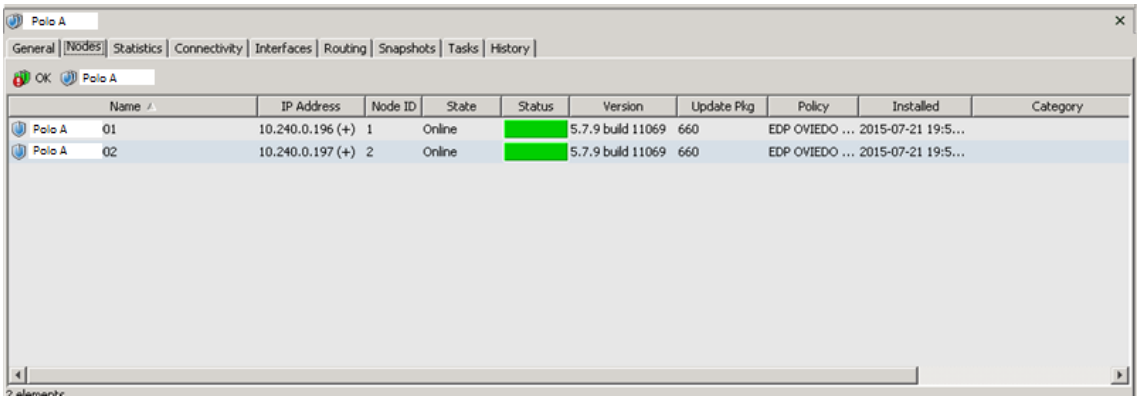


Figura 30 – Criação dos nós (objetos)

Depois da criação dos objetos dos nós e do *cluster* no SMC, é necessário a criação duma política inicial para, posteriormente, fazer o *upload* da *Access List Control* (ACL) para começar a filtrar o conteúdo desejado e indesejado. Ao selecionar a opção "*save initial configuration*" no objeto que representa cada nó, o SMC gera uma chave 256 bits para ser inserida durante a instalação do nó para o nó poder contatar o SMC (Figura 26).

Após a instalação de cada nó, é finalmente possível instalar a política de segurança no *cluster*. Os nós pertencentes ao *cluster* fazem apenas o que é definido no SMC.

4.5 Conclusão do capítulo

Este capítulo apresentou o trabalho efetuado no cliente para a implementação da solução NGFW da McAfee de forma a monitorizar a sua infraestrutura e bloquear ações maliciosas. Após esta fase de concretização, a solução encontra-se em produção e a proteger a infraestrutura do cliente sem haver, até ao momento, complicações. O próximo capítulo apresenta a avaliação a esta solução, não só em termos de níveis de bloqueio de aplicações/pacotes como a nível de desempenho.

Capítulo 5

Avaliação

Neste capítulo são apresentados os resultados da avaliação da solução implementada. Esta apreciação tem em conta dois fatores:

- Bloqueio de aplicações e tráfego: utilizando a capacidade da NGFW de gerar relatórios, nomeadamente ao nível de bloqueio de aplicações e protocolos;
- Desempenho: mostrando os habituais elementos de análise: consumos de memória RAM e CPU de cada componente da solução.

5.1 Bloqueio de aplicações e tráfego

Após a instalação e configuração da NGFW, foi possível avaliarmos diversas situações recorrendo à análise de *logs* e capacidade de gerar relatórios. Seguem-se alguns exemplos que mostram que esta implementação foi uma melhoria para a organização.

A quantidade de tráfego que por ela passa é apresentada na Figura 31. Estes dados são de apenas 15 minutos, o que nos mostra a elevada quantidade de dados que são analisados.

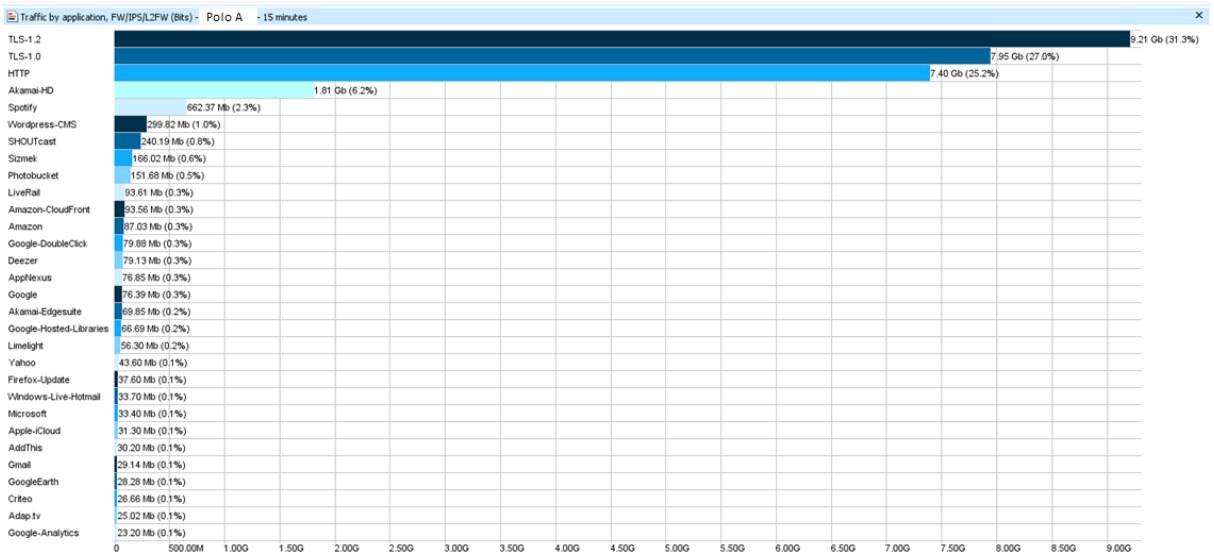


Figura 31 – Tráfego por Aplicação

Pela tabela seguinte (Tabela 3) podemos verificar que existiu uma quantidade de tráfego que foi descartado pela NGFW.

Resultado	Quantidade de Tráfego	Quantidade de pacotes
Tráfego Permitido	59.85 TBits	11.48 GPackets
Tráfego Descartado	3.04 GBits	3.56 MPackets

Tabela 3 – Tráfego Permitido/Descartado

A NGFW dá-nos outra visão do tráfego que por ela passa. Na figura 32 podemos ver o número de incidentes, por segundo, em que foram detetados comportamentos anómalos.

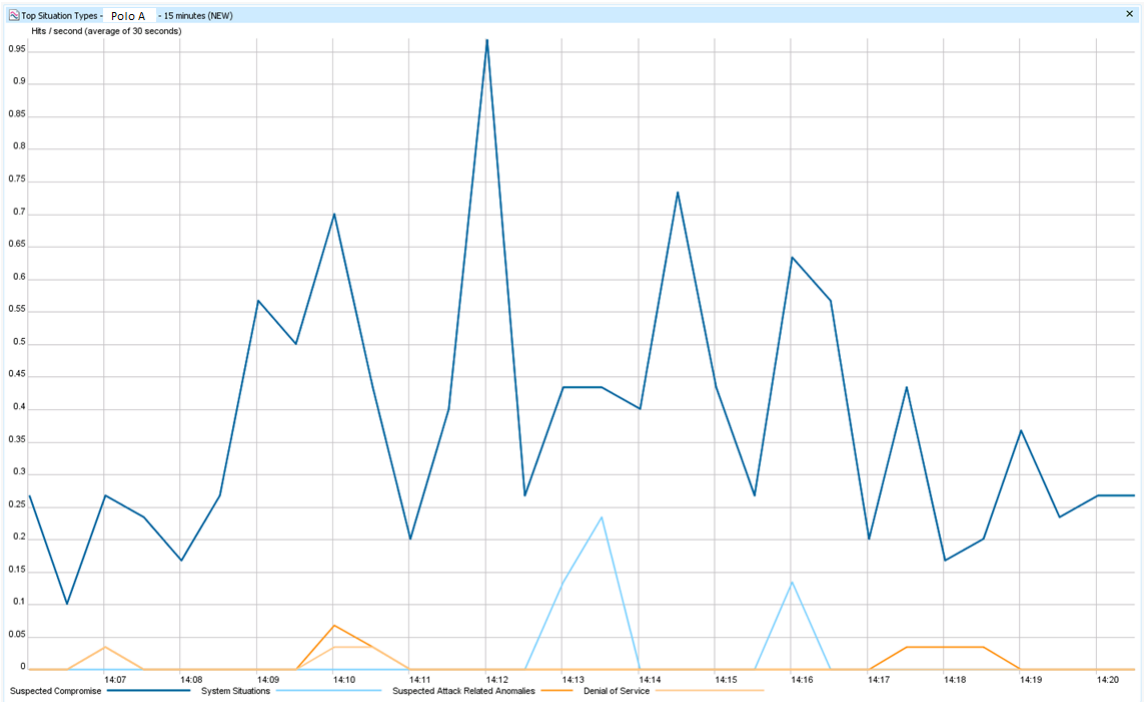


Figura 32 – Incidentes de Segurança

5.2 Desempenho

Podemos avaliar o estado do sistema através do SMC, onde é mostrado o estado das componentes do sistema (Figura 33). Nesta secção é possível verificar a voltagem, temperatura e espaço que está a ser ocupado pela *appliance*.

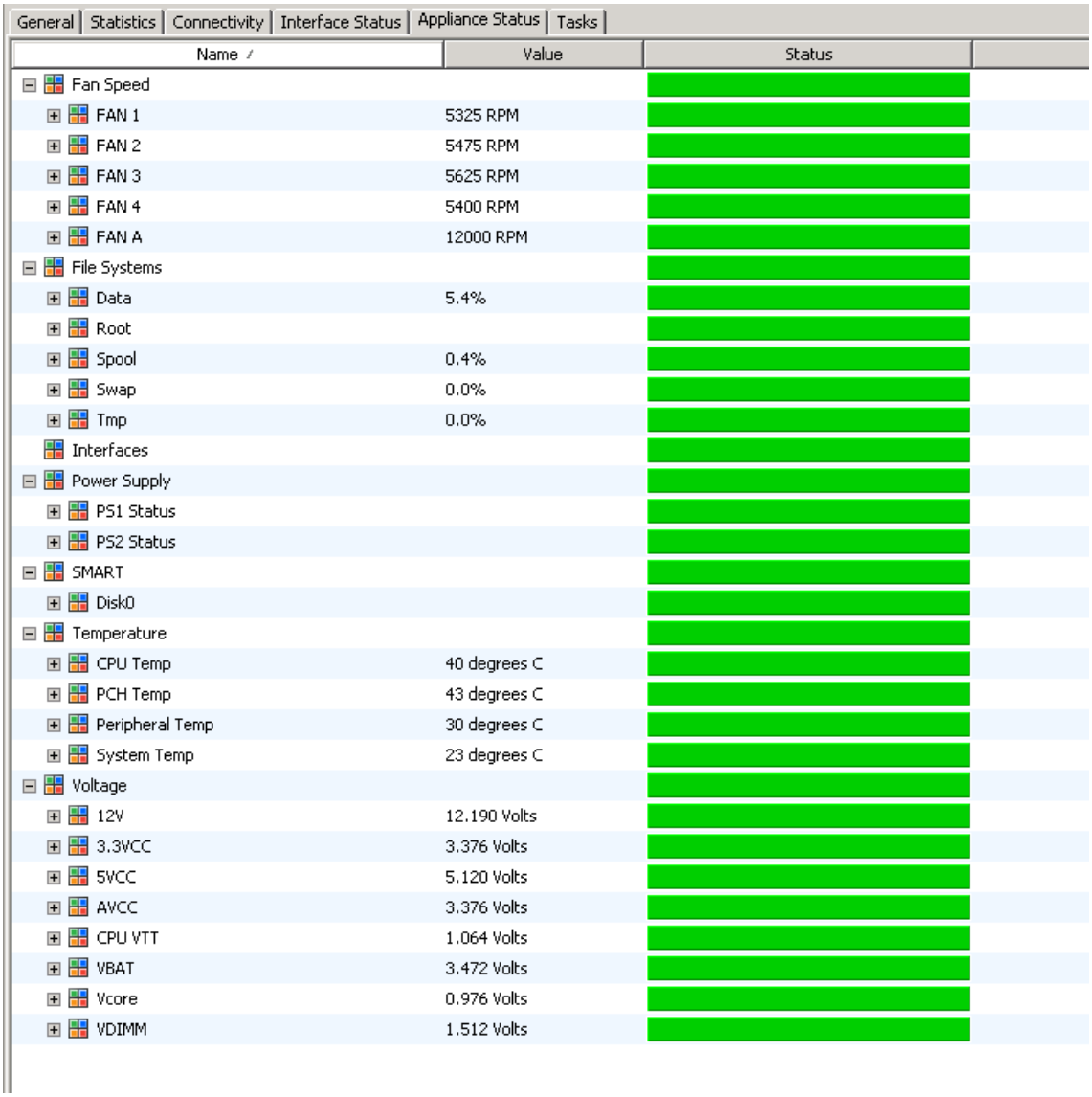


Figura 33 - Estado do Sistema

Quanto ao processamento de tráfego pelo motor de segurança da NGFW, podemos verificar, na figura 34, que o processamento neste Polo A é quase ínfima o que, para já, torna esta solução inadequada tendo em conta o pouco tráfego que tem. Em contraste, temos, no Polo B, um processamento mais significativo que justifica o uso desta NGFW (figura 35).

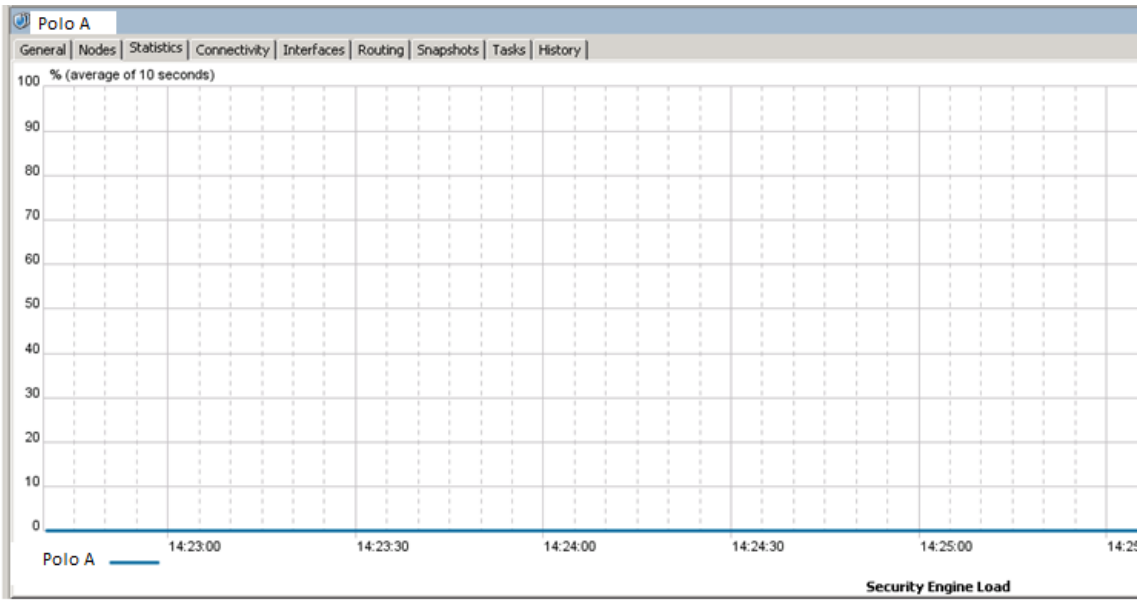


Figura 34 – Processamento do motor de segurança Polo A

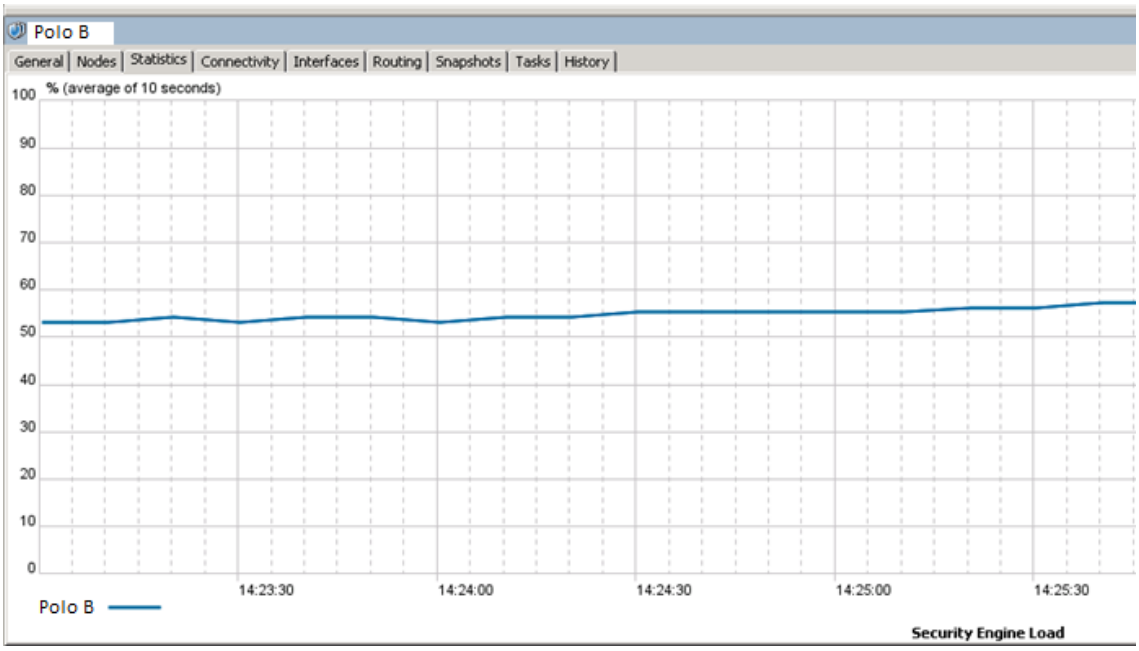


Figura 35 – Processamento do motor de segurança Polo B

Numa suma, vemos que esta solução é uma componente de segurança que se tem mostrado valiosa à organização e continua a oferecer maior segurança à rede interna apesar de, nesta altura, não ter a mesma preponderância em todos os polos.

Capítulo 6

Conclusão

Este relatório documenta o trabalho efetuado para implementar uma solução de NGFW da McAfee na infraestrutura de uma organização. Não obstante este projeto ter sido baseado na solução da McAfee, a implementação de qualquer NGFW numa organização não deverá ser muito diferente do observado aqui: análise de requisitos, instalação das *appliances*, instalação de nós e consola de gestão, configuração de políticas de segurança e otimização final do sistema.

Apesar da quantidade considerável de pacotes que dão entrada na solução, esta mostra ser capaz de dar resposta às necessidades do cliente em tempo útil, demonstrando que foi arquitetada uma solução fiável que, caso seja necessário no futuro, ainda pode crescer, não só a nível dos número de nós para oferecer redundância, como a também a nível de funções (ex: VPN).

Hoje em dia, as soluções de NGFW surgem cada vez mais como uma necessidade para salvaguardar a segurança da infraestrutura de qualquer organização porque oferecem uma visibilidade bastante superior às *firewalls* tradicionais. Em particular para estas organizações que lidam diariamente com um número elevado de utilizadores, limitar e controlar os acessos torna-se fundamental para a segurança da organização.

No caso específico do cliente em questão, esta plataforma NGFW veio para consolidar e centralizar a segurança na rede e, ao mesmo tempo, recolher informação valiosa que é depois reencaminhada para coletores de *logs* que, por sua vez, vão conseguir suprir a falta de monitorização que existia na sua rede oferecendo uma enorme visibilidade da mesma.

Bibliografia

[1] Abdulsalam Alarabeyat et al; Increasing Information Security Inside Organizations Through Awareness Learning For Employees, Journal of Theoretical and Applied Information Technology.

[2] Franziska Roesner et al; User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems, 2012 IEEE Symposium on Security and Privacy.

[3] http://blog.anitian.com/utm-v-ngfw-a-single-shade-of-gray/

[4] Lawrence C. Miller; Next-Generation Firewalls For Dummies, Wiley Publishing, 2011.

[5] http://www.fortinet.com/sites/default/files/whitepapers/Next-Generation-Firewall-Comparative-Analysis-SVM.pdf

[6] http://en.wikipedia.org/wiki/Stonesoft_Corporation

[7] http://www.networks365.net/stonegate-smc-overview.html

[8] Stonesoft Next Generation Firewall Datasheet, Stonesoft

[9] Tony Palmer, Examining Next Generation Network Security, April, 2014.

[10] http://www.networks365.net/stonegate-smc-overview.html#top6

[11] http://www.symantec.com/connect/blogs/how-manage-sha-1-deprecation-ssl-encryption

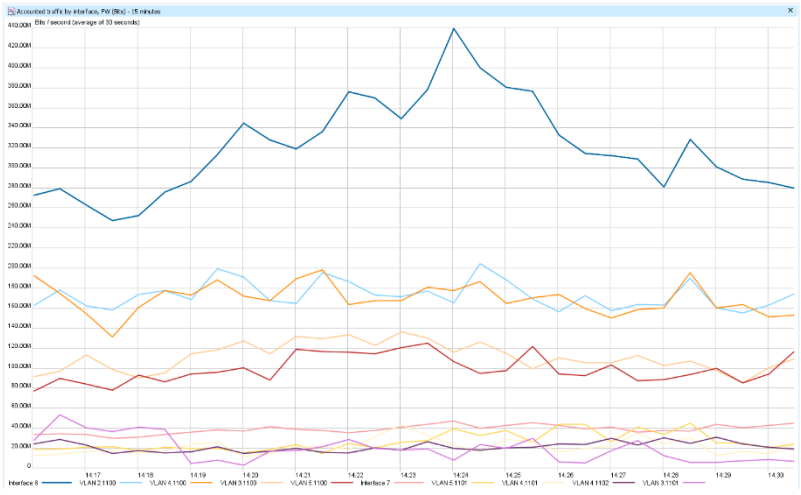
[12] Allan Liska, Building an Intelligence-Led Security Program

[13] https://blog.anitian.com/utm-v-ngfw-a-single-shade-of-gray/

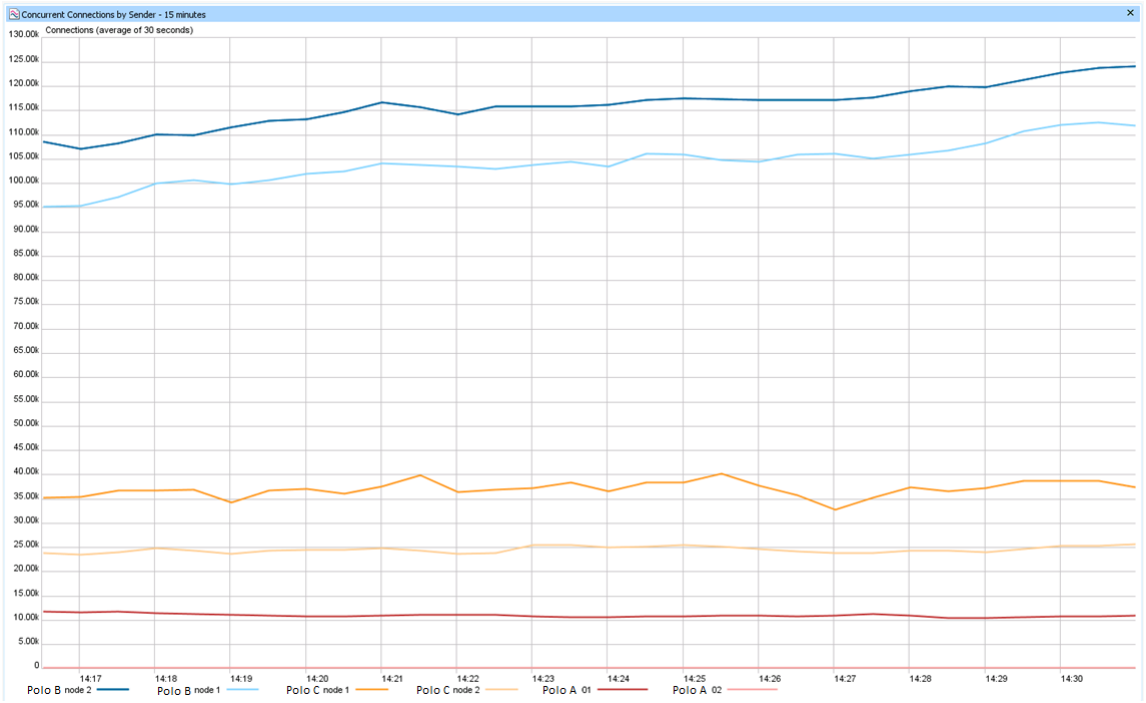
Anexos

Os seguintes anexos contém informação de todos os polos.

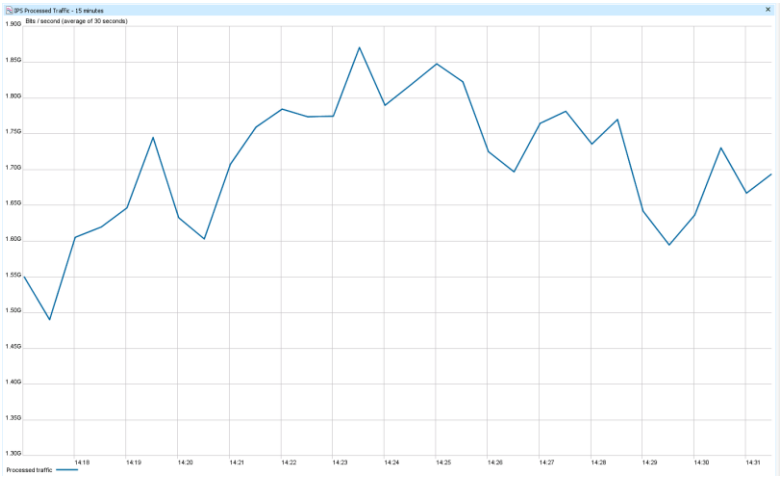
Tráfego por interface



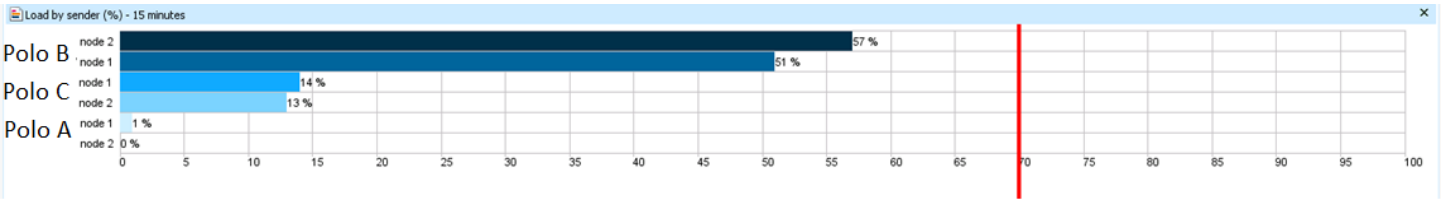
Ligações concorrentes por emissor



Tráfego processado pelo IPS



Carga por emissor



- Caso a carga atinja a linha vermelha, é enviado um e-mail alertando o excesso de carga

Destinos (Top)

Situações (Top)