

CENTRO UNIVERSITÁRIO UNIVATES  
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS  
CURSO DE ENGENHARIA DA COMPUTAÇÃO

**ANÁLISE DA IMPLANTAÇÃO E UTILIZAÇÃO DE  
SISTEMAS DE GERENCIAMENTO UNIFICADO DE  
AMEAÇAS (*UNIFIED THREAT MANAGEMENT* – UTM) EM  
EMPRESAS DE DIFERENTES PORTES**

Tiago Piazza

Lajeado, novembro de 2015

Tiago Piazza

**ANÁLISE DA IMPLANTAÇÃO E UTILIZAÇÃO DE  
SISTEMAS DE GERENCIAMENTO UNIFICADO DE  
AMEAÇAS (*UNIFIED THREAT MANAGEMENT* – UTM) EM  
EMPRESAS DE DIFERENTES PORTES**

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Tecnológicas do Centro Universitário UNIVATES, como parte dos requisitos para a obtenção do título de bacharel em Engenharia da Computação.

**ORIENTADOR:** Marcus Vinicius Lazzari

Lajeado, novembro de 2015

Tiago Piazza

**ANÁLISE DA IMPLANTAÇÃO E UTILIZAÇÃO DE  
SISTEMAS DE GERENCIAMENTO UNIFICADO DE  
AMEAÇAS (*UNIFIED THREAT MANAGEMENT* – UTM) EM  
EMPRESAS DE DIFERENTES PORTES**

Este trabalho foi julgado adequado para a obtenção do título de bacharel em Engenharia da Computação e aprovado em sua forma final pelo Orientador e pela Banca Examinadora.

Orientador: \_\_\_\_\_

Prof. Marcus Vinicius Lazzari, UNIVATES

Mestre pela PUC - Rio de Janeiro, Brasil

Banca Examinadora:

Prof. Luis Antônio Schneiders, UNIVATES

Mestre pela UFRGS - Porto Alegre, Brasil

Prof. Edson Moacir Ahlert, UNIVATES

Graduado pela UNIVATES - Lajeado, Brasil

Coordenador do Curso de Engenharia da Computação: \_\_\_\_\_

Prof. Marcelo de Gomensoro Malheiros

Lajeado, novembro de 2015.

## **AGRADECIMENTOS**

A todos que colaboraram direta ou indiretamente para a realização deste trabalho.

## RESUMO

Segurança da informação em redes de computadores é um tema cada vez mais em voga no cenário atual de Tecnologia da Informação e Comunicação (TIC). Grandes empresas deste segmento dedicam seus esforços na construção de complexas e eficientes soluções que visam a garantia das três metas básicas da segurança: confidencialidade, integridade e disponibilidade. Um modelo que ganha cada vez mais destaque neste mercado são as ferramentas baseadas no conceito do gerenciamento unificado de ameaças (*Unified Threat Management - UTM*), que consiste numa plataforma onde concentram-se os principais recursos de proteção, tais como: *firewall*, sistema de prevenção/detecção de intrusões (*Intrusion Prevention/Detection System - IPS/IDS*), rede privada virtual (*Virtual Private Network - VPN*), filtro de conteúdo (*sites* e aplicações), antivírus de *gateway*, entre outros. Este documento tem como objetivo realizar uma análise da implantação e utilização de dispositivos UTM em companhias de diferentes portes, bem como o levantamento comparativo dos principais benefícios gerados em cada contexto. Também objetiva detectar os fatores decisivos para a escolha de ferramentas UTM como solução de segurança para cada porte de empresa.

**Palavras-chave:** Redes de Computadores, Segurança da Informação, Gerenciamento Unificado de Ameaças.

## **ABSTRACT**

Computer networks security information is a topic increasingly in vogue in the current scenario of ITC (Information Technology and Communication). Big companies in this segment dedicate their efforts in building complex and efficient solutions aimed at ensuring the safety of the three basic objectives: confidentiality, integrity and availability. A model that has gained increasing prominence in this market are the tools based on the concept of Unified Threat Management (UTM), which is a platform where are concentrated the main protection features, such as: firewall, intrusion prevention/detection system (IPS/IDS), virtual private network (VPN), content filtering (sites and applications), gateway anti-virus and others. This document aims to conduct an analysis of the deployment and use of UTM devices in companies of different sizes, as well as the comparative survey of the main benefits generated in each context. Also aims to detect the decisive factors for choosing UTM tools as a security solution for each size company.

**Keywords: Computer Networks, Information Security, Unified Threat Management.**

## LISTA DE FIGURAS

Figura 1 – Camadas do modelo OSI.....	18
Figura 2 – <i>Firewall</i> de filtragem de pacotes.....	23
Figura 3 – <i>Firewall proxy</i> .....	23
Figura 4 – Estrutura organizacional de um Sistema de Detecção de Intrusões.....	25
Figura 5 – Estrutura organizacional de um Sistema de Prevenção de Intrusões.....	26
Figura 6 – Comparativo entre redes interconectadas por MPLS e VPN.....	28
Figura 7 – VPN <i>Site to Site</i> convencional.....	32
Figura 8 – VPN <i>Site to Site Hub and Spoke</i> .....	33
Figura 9 – VPN <i>Site to Site Mesh</i> .....	33
Figura 10 – Arquitetura organizacional de um sistema de defesa em camadas.....	41
Figura 11 – Arquitetura organizacional de um sistema UTM.....	41
Figura 12 – Funcionalidades presentes em soluções UTM e NGFW.....	43
Figura 13 – Classificação do porte empresarial de acordo com o número de funcionários.....	44
Figura 14 – Estrutura organizacional de rede da Empresa 1.....	51
Figura 15 – Nível de acesso básico à <i>Internet</i> na Empresa 1.....	53
Figura 16 – Nível de acesso privilegiado à <i>Internet</i> na Empresa 1.....	53
Figura 17 – Estrutura organizacional de rede da Empresa 2.....	54
Figura 18 – Rotas criadas na Empresa 2.....	56
Figura 19 – Grupos de acesso da Empresa 2.....	57
Figura 20 – Estrutura organizacional de rede da Empresa 3.....	59
Figura 21 – Interfaces de rede da Empresa 3.....	60
Figura 22 – ACLs da rede alunos para rede administrativa na Empresa 3.....	61
Figura 23 – ACLs da rede administrativa para <i>Internet</i> na Empresa 3.....	61
Figura 24 – Políticas de acesso da Empresa 3.....	63
Figura 25 – Portas mapeadas antes da ferramenta UTM na Empresa 1.....	64
Figura 26 – Portas mapeadas antes da ferramenta UTM na Empresa 2.....	65
Figura 27 – Portas mapeadas antes da ferramenta UTM na Empresa 3.....	65
Figura 28 – Registros de <i>logs</i> de <i>scan</i> na Empresa 1.....	65
Figura 29 – Registros de <i>logs</i> de <i>scan</i> na Empresa 2.....	66
Figura 30 – Registros de <i>logs</i> de <i>scan</i> na Empresa 3.....	66
Figura 31 – Detalhamento das portas mapeadas na Empresa 1.....	66
Figura 32 – Registro de vírus bloqueados na Empresa 1.....	67
Figura 33 – Registro de vírus bloqueados na Empresa 2.....	67
Figura 34 – Registro de vírus bloqueados na Empresa 3.....	68
Figura 35 – Fatores determinantes para empresas de pequeno porte.....	70
Figura 36 – Fatores determinantes para empresas de médio porte.....	71
Figura 37 – Fatores determinantes para empresas de grande porte.....	71
Figura 38 – Tempo gasto com conteúdos indevidos na Empresa 1.....	73
Figura 39 – Tempo gasto com conteúdos indevidos na Empresa 2.....	75
Figura 40 – Tempo gasto com conteúdos indevidos na Empresa 3.....	77

## LISTA DE TABELAS

Tabela 1 – Comparativo entre as características do IDS e IPS .....	27
Tabela 2 – Protocolos de VPN e o modelo OSI .....	30
Tabela 3 – Características dos ambientes de estudo.....	45
Tabela 4 – Descrições técnicas dos dispositivos UTM .....	45
Tabela 5 – NATs criadas na Empresa 1 .....	51
Tabela 6 – NATs criadas na Empresa 2 .....	55
Tabela 7 – NATs criadas na Empresa 3 .....	60
Tabela 8 – Custos da ferramenta UTM .....	72
Tabela 9 – Comparativo do consumo energético na Empresa 1.....	74
Tabela 10 – Comparativo do consumo energético na Empresa 2.....	75
Tabela 11 – Comparativo dos <i>links</i> MPLS e ADSL na Empresa 2.....	76
Tabela 12 – Comparativo do consumo energético na Empresa 3.....	77



## LISTA DE ABREVIATURAS

3DES:	Triple Data Encryption Standard
ACL:	Access Control List
AD:	Active Directory
ADSL:	Asymmetric Digital Subscriber Line
CGSS:	Comprehensive Gateway Security Suite
DES:	Data Encryption Standard
DH:	Diffie-Hellman
DHCP:	Dynamic Host Configuration Protocol
DLP:	Data Loss Prevention
DNS:	Domain Name System
DNSBL:	Domain Name System Black List
DOS:	Denial Of Service
ERP:	Enterprise Resource Planning
FEC:	Forwarding Equivalency Class
Gbps:	Giga bits por segundo
HA:	High Availability
HIDS:	Host based Intrusion Detection System
HIPS:	Host based Intrusion Prevention System
HTTP:	HyperText Transfer Protocol
HTTPS:	HyperText Transfer Protocol Secure
IBGE:	Instituto Brasileiro de Geografia e Estatística
IDS:	Intrusion Detection System
IETF:	Internet Engineering Task Force
IP:	Internet Protocol
IPS:	Intrusion Prevention System
IPSec:	Internet Protocol Security
ISO:	International Standards Organization
L2F:	Layer 2 Forwarding Protocol
L2TP:	Layer 2 Tunneling Protocol
LAN:	Local Area Network
LDP:	Label Distribution Protocol
LER:	Label Edge Router

LSP:	Label Switch Path
LSR:	Label Switch Router
MAN:	Metropolitan Area Network
Mbps:	Mega bits por segundo
MD5:	Message Digest Algorithm 5
MITM:	Man In The Middle
MPLS:	Multiprotocol Label Switching
MSSP:	Managed Security Services Provider
NASL:	Nessus Attack Scripting Language
NAT:	Network Address Translation
NGFW:	Next Generation Firewall
NIDS:	Network based Intrusion Detection System
NIPS:	Network based Intrusion Prevention System
OSI:	Open System Interconnection
PC:	Personal Computer
PPPoE:	Point-to-Point Protocol over Ethernet
PPTP:	Point-to-Point Tunneling Protocol
P2P:	Peer-to-Peer
RBL:	Real-time Blackhole List
RFC:	Request For Comments
RSVP:	Resource Reservation Protocol
SA:	Security Association
SEBRAE:	Serviço Brasileiro de Apoio às Micro e Pequenas Empresas
SHA1:	Secure Hash Algorithm 1
SO:	Sistema Operacional
TCP:	Transmission Control Protocol
TIC:	Tecnologia da Informação e Comunicação
UDP:	User Datagram Protocol
URL:	Uniform Resource Locator
UTM:	Unified Threat Management
VPN:	Virtual Private Network
WAN:	Wide Area Network
WSUS:	Windows Server Update Services
WWW:	World Wide Web

## SUMÁRIO

1	INTRODUÇÃO.....	13
2	REVISÃO BIBLIOGRÁFICA.....	15
2.1	Redes de computadores.....	15
2.1.1	Modelo OSI.....	16
2.1.2	Modelo TCP/IP.....	18
2.2	Segurança da informação.....	19
2.2.1	Conceitos fundamentais de segurança.....	20
2.2.2	Tipos de ataque.....	20
2.3	Mecanismos de segurança.....	21
2.3.1	<i>Firewalls</i> .....	21
2.3.2	<i>Intrusion Detection System - IDS</i> .....	24
2.3.3	<i>Intrusion Prevention System - IPS</i> .....	25
2.3.4	Antivírus.....	27
2.4	Interconexão de redes.....	28
2.4.1	<i>Multi Protocol Label Switching - MPLS</i> .....	28
2.4.2	<i>Virtual Private Network - VPN</i> .....	29
2.4.3	<i>Internet Protocol Security - IPSec</i> .....	31
2.4.4	Topologias de VPN.....	31
2.5	Navegação segura.....	34
2.5.1	Filtragem de URL ( <i>Uniform Resource Locator</i> ).....	34
2.5.2	Filtragem de aplicação.....	35
2.5.3	Antivírus de <i>gateway</i> .....	35
2.6	Controle de mensagens.....	36
2.6.1	<i>AntiSpam</i> .....	37
2.6.2	Antivírus de <i>e-mail</i> .....	38
2.7	Soluções de Gerenciamento Unificado de Ameaças.....	39
2.8	Comparativo entre UTM e NGFW.....	42
3	MATERIAIS E MÉTODOS.....	44
3.1	Definição dos cenários de estudo.....	44
3.2	Justificativa da solução escolhida.....	45
3.3	Análise da implementação da ferramenta UTM.....	46
3.3.1	Pré-instalação.....	46
3.3.2	Instalação.....	47
3.3.3	Pós-instalação.....	47
3.4	Métodos de avaliação.....	47
3.4.1	Análise comparativa.....	47
3.4.2	Análise estatística.....	48
3.5	Análise financeira - Retorno sobre Investimento.....	48
4	RESULTADOS.....	50
4.1	Implementação da ferramenta UTM.....	50
4.1.1	Empresa 1 - Ambiente de pequeno porte.....	50
4.1.2	Empresa 2 - Ambiente de médio porte.....	54
4.1.3	Empresa 3 - Ambiente de grande porte.....	58
4.2	Comparativo entre os ambientes antes e após a implantação da ferramenta UTM.....	64
4.3	Resultados estatísticos - fatores determinantes.....	68

4.3.1	Empresa 1 - Ambiente de pequeno porte.....	69
4.3.2	Empresa 2 - Ambiente de médio porte .....	69
4.3.3	Empresa 3 - Ambiente de grande porte .....	69
4.3.4	Fatores determinantes para empresas de pequeno porte.....	70
4.3.5	Fatores determinantes para empresas de médio porte .....	70
4.3.6	Fatores determinantes para empresas de grande porte .....	71
4.4	Resultados financeiros - retorno sobre o investimento.....	72
4.4.1	ROI - Empresa 1 .....	72
4.4.2	ROI - Empresa 2 .....	74
4.4.3	ROI - Empresa 3 .....	76
5	CONCLUSÃO.....	79
	REFERÊNCIAS .....	80
	ANEXO A: FORMULÁRIO UTILIZADO PARA COLETA DOS FATORES DETERMINANTES.....	84

## 1 INTRODUÇÃO

Durante as primeiras décadas de sua existência, as redes de computadores foram usadas principalmente por pesquisadores universitários, com a finalidade de enviar mensagens de correio eletrônico, e também por funcionários de empresas, para compartilhar impressoras. Sob essas condições, a segurança nunca precisou de maiores cuidados. Porém, como milhões de cidadãos comuns atualmente estão usando as redes para executar operações bancárias, fazer compras e arquivar sua devolução de impostos, a segurança das redes está despontando no horizonte como um problema em potencial (TANENBAUM, 2003).

A interconexão dessas redes (*Internet*) abre as portas para o mundo externo. Então, se métodos de segurança não forem implementados, todo sistema de informação corre o risco de ser explorado indevidamente. As ameaças de segurança apresentam-se de diferentes fontes e de diferentes formas, podendo causar perda de conectividade ou divulgação de dados importantes (BHARDWAJ, 2007).

Atualmente vive-se na era da informação. Precisa-se manter informações sobre cada aspecto da vida das pessoas. Em outras palavras, a informação é um ativo que tem valor, assim como qualquer outro. Como um ativo, e para ser considerada segura, a informação precisa ser protegida contra ataques, acessos não autorizados (confidencialidade) e alterações não autorizadas (integridade); também deve estar disponível para uma entidade autorizada quando necessário (disponibilidade) (FOROUZAN & MOSHARRAF, 2013). O conceito de segurança da informação está especificamente embasado em garantir o cumprimento desta tríade: confidencialidade, integridade e disponibilidade.

Com o constante crescimento das ameaças cibernéticas, aliado à sofisticação nas ferramentas de ataque que visam explorar brechas de segurança, organizações de diferentes portes lutam para permitir o acesso necessário para que seus funcionários realizem suas atividades sem comprometer a segurança organizacional. Uma opção comum tem sido a de adicionar novas tecnologias de segurança de forma isolada, cada uma para um determinado propósito, como por exemplo: soluções de *firewall*, sistemas de detecção e prevenção de intrusões, antivírus, filtros de conteúdo, entre outras. Trata-se de uma boa alternativa, porém que pode elevar muito os custos de implantação, além de não haver uma total garantia na compatibilidade das ferramentas.

Em contrapartida, uma solução que tem se destacado no mercado atual e angariado cada vez mais adeptos, são os dispositivos que baseiam-se no conceito do gerenciamento unificado de ameaças, que o grupo Gartner (2015) - uma das maiores empresas mundiais do setor de

pesquisa e fomento à tecnologia - define como: “uma plataforma de convergência de distintos produtos de segurança divididos em conjuntos de recursos típicos: *firewall*, sistema de prevenção e detecção de intrusão, rede privada virtual, navegação segura (filtragem de URL, filtragem de aplicações, antivírus de *gateway*) e segurança de mensagens (*AntiSpam*, antivírus de *e-mail*)”. Com foco na simplificação da gestão da segurança, na grande maioria dos casos, as ferramentas UTM apresentam-se na forma de *appliance (hardware + software)*.

Tendo em vista os temas citados, este trabalho tem como objetivo principal a implementação de um sistema de gerenciamento unificado de ameaças em três companhias de diferentes segmentos e portes (pequeno, médio e grande). Ainda como parte deste objetivo, deseja-se documentar e analisar todo o processo, desde o projeto inicial (mapeamento do ambiente), até o acompanhamento pós instalação. Como objetivos secundários visa-se gerar um estudo estatístico -baseado na entrevista e *feedbacks* dos gestores de TIC- das melhorias promovidas pela ferramenta, a mensuração (a partir de análises comparativas) do aumento geral no nível de segurança das corporações, além de compreender os fatores que motivaram a escolha de um dispositivo UTM como solução de segurança de redes. Outro objetivo deste trabalho é a determinação do Retorno Sobre o Investimento (*Return On Investment - ROI*) para implementar a ferramenta UTM nos três cenários de estudo.

Inicialmente é apresentado um referencial teórico contendo os conceitos fundamentais para a compreensão do trabalho, tais como: Redes de computadores (estrutura e organização), segurança da informação (definição e sistemas relacionados), Interconexão de redes, Controle de navegação, Segurança de mensagens (*AntiSpam*), Dispositivos de *firewall* UTM e *Next Generation Firewall* (NGFW).

O Capítulo 3 descreve a metodologia utilizada, os materiais e métodos de análise necessários para a execução do estudo. Neste capítulo também são detalhados os diferentes ambientes de TIC considerados na implementação das soluções UTM. Já o Capítulo 4 é destinado à apresentação dos resultados obtidos a partir do estudo realizado. No capítulo final encontram-se as conclusões oriundas do trabalho e as sugestões à continuidade do mesmo.

## 2 REVISÃO BIBLIOGRÁFICA

Este capítulo tem como objetivo descrever os conhecimentos teóricos básicos para a realização do estudo. Os tópicos de redes de computadores e seus modelos são apresentados de forma resumida, visto que sua compreensão é tida como pré-requisito para o entendimento dos temas primordiais: segurança da informação e gerenciamento unificado de ameaças.

### 2.1 Redes de computadores

Redes de computadores estabelecem a forma padrão de interligar computadores para o compartilhamento de recursos físicos ou lógicos. Esses recursos podem ser definidos como unidades de CD-ROM, diretórios do disco rígido, arquivos e documentos, impressoras, *scanners*, placa de *fax modem* entre outros (MENDES, 2007).

De acordo com Forouzan e Mosharraf (2013), uma rede de computadores é a interligação de um conjunto de dispositivos capazes de se comunicar. Nesta definição, um dispositivo pode ser um *host* (sistema final), tal como um servidor, estação de trabalho, *notebook*, telefones celulares ou sistemas de segurança. Também podem ser dispositivos de conexão, como roteadores que interligam duas ou mais redes, *switches* (comutadores) que conectam dispositivos entre si, *modems* (que alteram a forma dos dados) e assim por diante. Tais nodos em uma rede são conectados usando meios de transmissão com ou sem fio, como cabos ou o ar.

Simplificadamente, redes de computadores são uma infraestrutura que fornece a interconexão de múltiplos sistemas de computação autônomos, com o objetivo de comunicar e compartilhar recurso entre si.

Inúmeras são as subdivisões para as redes (de acordo com sua extensão geográfica), porém destacam-se as seguintes:

- Pequeno alcance - *Local Area Network* (LAN), interligam computadores comportados dentro de um mesmo espaço físico, tais como: empresas, escolas, residências e afins.
- Médio alcance - *Metropolitan Area Network* (MAN), interconecta diversas redes locais dentro de um raio de dezenas de quilômetros. As fronteiras de uma cidade representam a atuação de uma MAN.
- Grande alcance - *Wide Area Network* (WAN), uma rede de longa distância capaz de abranger grandes áreas, como por exemplo um país ou até mesmo um continente.

### 2.1.1 Modelo OSI

Para satisfazer as necessidades e solicitações das novas redes de comunicação, os fabricantes de equipamentos e sistemas desenvolveram soluções proprietárias para as várias arquiteturas de sistemas. Conseqüentemente, várias redes foram criadas a partir de diferentes implementações de *hardware* e de *software*. Essas soluções passaram, então, a definir o inter-relacionamento dos sistemas com os usuários. Entretanto, muitas redes eram incompatíveis entre si, com diferentes especificações, impossibilitando a interoperabilidade e a comunicação entre elas. Tal situação levou a elaboração de um modelo que servisse como referência para que todos os fabricantes desenvolvessem soluções capazes de interagir entre si. A arquitetura de Interconexão de Sistemas Abertos (*Open Systems Interconnection - OSI*) foi criada pela Organização Internacional de Normalização (*International Standards Organization - ISO*) com a finalidade de padronizar o desenvolvimento dos produtos destinados às redes de computadores. Seu objetivo é permitir a interligação de equipamentos e sistemas distintos sem problemas de compatibilidade. É uma referência que mostra sempre o que fazer, mas não como fazer (PINHEIRO, 2008).

A estrutura do modelo OSI apresenta-se subdivida em sete camadas verticais (Física, Enlace de Dados, Rede, Transporte, Sessão, Apresentação e Aplicação), cada qual com sua função específica e funcionamento isolado umas das outras.

Tanenbaum (2003) explana sobre cada camada da seguinte forma:

- Camada 1 (Física) - trata da transmissão de *bits* brutos por um canal de comunicação. O projeto da rede deve garantir que, quando um lado enviar um *bit* 1, o outro lado o receberá como um *bit* 1, não como um *bit* 0. Nessa situação, as questões de projeto lidam em grande parte com interfaces mecânicas, elétricas e de sincronização, e com o meio físico de transmissão que se situa abaixo da camada física.
- Camada 2 (Enlace) - a principal tarefa da camada de enlace de dados é transformar um canal de transmissão bruta em uma linha que pareça livre de erros de transmissão não detectados pela camada de rede. Para executar tal ação, a camada de enlace de dados faz com que o transmissor divida os dados de entrada em quadros de dados (que, em geral, têm algumas centenas ou alguns milhares de *bytes*), e transmita os quadros sequencialmente.
- Camada 3 (Rede) - controla a operação da sub-rede. Uma questão fundamental de projeto é determinar a maneira como os pacotes são roteados da origem até o destino. As rotas podem se basear em tabelas estáticas, "amarradas" à rede e raramente



alteradas. Se houver muitos pacotes na sub-rede ao mesmo tempo, eles dividirão o mesmo caminho, provocando gargalos. O controle desse congestionamento também pertence à camada de rede.

- Camada 4 (Transporte) - a função básica da camada de transporte é aceitar dados da camada acima dela, dividi-los em unidades menores caso necessário, repassar essas unidades à camada de rede e assegurar que todos os fragmentos chegarão corretamente à outra extremidade. A camada de transporte também determina que tipo de serviço deve ser fornecido à camada de sessão e, em última análise, aos usuários da rede.
- Camada 5 (Sessão) - permite que os usuários de diferentes máquinas estabeleçam sessões entre si. Uma sessão oferece diversos serviços, inclusive o controle de diálogo (mantendo o controle de quem deve transmitir em cada momento), o gerenciamento de símbolos (impedindo que duas partes tentem executar a mesma operação crítica ao mesmo tempo) e a sincronização (realizando a verificação periódica de transmissões longas para permitir que elas continuem a partir do ponto em que estavam ao ocorrer uma falha).
- Camada 6 (Apresentação) - está relacionada à sintaxe e à semântica das informações transmitidas. Para tornar possível a comunicação entre computadores com diferentes representações de dados, as estruturas a serem intercambiadas podem ser definidas de maneira abstrata, juntamente com uma codificação padrão que será usada durante a conexão. A camada de apresentação gerencia essas estruturas de dados abstratas e permite sua definição e intercâmbio a níveis mais altos.
- Camada 7 (Aplicação) - a camada de aplicação contém uma série de protocolos comumente necessários para os usuários. Um protocolo de aplicação amplamente utilizado é o *HyperText Transfer Protocol* (HTTP), que constitui a base para a Rede de Alcance Mundial (*World Wide Web* - WWW). Quando um navegador deseja carregar uma página da *web*, ele envia o nome da página ao servidor, utilizando o HTTP. Então, o servidor transmite a página de volta. Outros protocolos de aplicação são usados para transferências de arquivos, correio eletrônico e transmissão de notícias pela rede.

A Figura 1 representa a hierarquia na estrutura em camadas do modelo OSI.

**Figura 1 – Camadas do modelo OSI**

Fonte: Elaborado pelo autor.

### 2.1.2 Modelo TCP/IP

Devido ao longo tempo demandado para a publicação do modelo de referência OSI, alguns outros modelos surgiram de forma paralela. Foi o caso do modelo de referência TCP/IP, criado pelo Departamento de Defesa do Governo dos Estados Unidos da América (DoD - *Department of Defense*).

Também possui seu conceito baseado em pilha de pacotes, porém possui uma estrutura mais simples quando comparado ao modelo OSI. Há uma divergência de autores quanto ao número de camadas deste modelo, alguns citam existir quatro camadas e outros apontam a definição de cinco camadas.

Forouzan e Mosharraf (2013) definem cada uma das cinco camadas da seguinte forma:

- Camada 1 (Física) - é responsável por transportar os *bits* individuais de um quadro através do enlace. Mesmo a camada física sendo o nível mais baixo no modelo TCP/IP, a comunicação entre dois dispositivos na camada física é ainda uma comunicação lógica.
- Camada 2 (Enlace) - sua atuação caracteriza-se pelo encapsulamento de um datagrama na forma de um quadro (*frame*) e posteriormente move-o através do

enlace. Não há um protocolo definido para esta camada, a referência TCP/IP suporta qualquer protocolo capaz de satisfazer esta necessidade.

- Camada 3 (Rede) - a comunicação na camada de rede é *host a host*, onde é criada uma conexão entre o computador de origem e o computador de destino. Também realiza o roteamento de pacotes através das múltiplas rotas existentes com base no melhor caminho. O principal protocolo utilizado na camada de rede é o *Internet Protocol (IP)*.
- Camada 4 (Transporte) - a conexão lógica (imaginária) na camada de transporte é fim a fim. Seu grande objetivo é prover serviço à camada de aplicação. Os principais protocolos desta camada são o TCP, seguido do UDP.
- Camada 5 (Aplicação) - também possui uma conexão lógica fim a fim. A conexão na camada de aplicação se dá entre dois processos (dois programas em execução nesta camada), que enviam mensagens entre si através de pedidos e respostas.

## 2.2 Segurança da informação

A norma NBR ISO/IEC 17799 de 2005 da Associação Brasileira de Normas Técnicas (ABNT) define que a informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente. A normativa também descreve que a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Forouzan e Mosharraf (2013) afirmam que a segurança da informação está amparada em garantir três metas básicas:

- Confidencialidade - propriedade responsável pela garantia do acesso à informação somente por entidades autorizadas.
- Integridade - garantia de que toda a informação, manipulada pelas entidades autorizadas, mantenha suas características originais.
- Disponibilidade - a informação somente é útil se estiver acessível quando necessária for. Tal característica assegura que a informação sempre esteja disponível às entidades autorizadas.

A segurança do computador e segurança de rede são partes de um conceito maior, que protege tudo a eles associados, seu *hardware*, seus terminais e impressoras, o sistema de cabos, seus discos e fitas. Mais importante ainda, a segurança do computador protege as informações nele armazenadas. É por isso que a segurança do computador é frequentemente chamada de segurança da informação (LEHTINEN, RUSSELL & GANGEMI, 2006).

### 2.2.1 Conceitos fundamentais de segurança

Existem quatro palavras-chave relacionadas à segurança da informação: vulnerabilidades, ameaças, riscos e ataques. Suas respectivas definições são:

- Vulnerabilidade: é um ponto onde um sistema de segurança é suscetível a ataques. Pode ser uma fraqueza (ou falha) de processo, implementação ou desenvolvimento de programas, serviços ou equipamentos que expõem a rede a invasões acidentais ou propositais.
- Ameaça: é um possível perigo para o sistema. O perigo pode ser uma pessoa, um objeto (peça com defeito), ou um evento (incêndio, inundação, desastres naturais) que venham a explorar uma vulnerabilidade do sistema.
- Risco: caracteriza-se pela probabilidade de uma fonte de ameaça explorar uma vulnerabilidade existente no sistema.
- Ataque: define-se pela exploração de uma vulnerabilidade de um determinado sistema. Tal ação geralmente resulta em impactos negativos à organização e está motivada pela obtenção de informações importantes, pelo acesso indevido à rede de destino ou pela perturbação do funcionamento de um determinado serviço.

### 2.2.2 Tipos de ataque

Segundo Convery (2004) é possível classificar os diferentes tipos de ataque em cinco grandes grupos, de acordo com a sua natureza específica:

- Divulgação de informações - é a divulgação de informações a qualquer pessoa não autorizada a recebê-las. Engloba ataques de *sniffing* de senhas, leituras não autorizadas a partes de uma unidade de disco rígido, entre outros.
- Corrupção de informação - é qualquer alteração não autorizada de arquivos armazenados em um computador (*host*) ou nos dados em trânsito de uma rede

qualquer. Exemplos incluem *defacement* (modificações de páginas *web*), ataques *man-in-the-middle* (MITM), vírus que destroem dados, e assim por diante.

- Negação de serviço - *Denial of Service* (DoS) é a degradação intencional ou bloqueio de computadores ou recursos de rede. A maioria dos ataques DoS baseiam-se no conceito de inundação. Uma grande quantidade de tentativas de acessos é direcionada a um determinado serviço ou servidor com o objetivo de sobrecarregá-lo e deixá-lo indisponível.
- Roubo de serviço - é o uso não autorizado de serviços de informática ou de redes, sem degradar o serviço a outros usuários. Roubo de senhas e registro não autorizados na rede são alguns exemplos deste tipo de ataque.
- Aumento do acesso - é o aumento não autorizado em privilégios de usuário que ocorre no acesso aos serviços de um computador ou de uma rede. Ataques de estouro de *buffer* caracterizam este tipo de ataque.

## 2.3 Mecanismos de segurança

Garantir a segurança de uma rede contra diferentes formas de ataque requer a utilização de mecanismos complexos de detecção e retenção de ameaças. Os principais métodos utilizados são a implementação de ferramentas de *firewall*, sistemas de detecção e prevenção de intrusões e *softwares* antivírus.

### 2.3.1 Firewalls

É possível afirmar que seja um dos mais básicos recursos de segurança de redes. Um *firewall* (ao contrário de um roteador, que simplesmente direciona o tráfego entre redes) é um sistema ou grupo de sistemas que reforçam uma política de controle de acesso do tráfego em diferentes pontos. O trabalho do *firewall* é garantir que nenhum acesso adicional, além dos que estão pré-definidos em suas diretrizes, entre ou saia da rede em que atua. Cabe ao *firewall* garantir que a política de controle de acesso seja seguida por todos os usuários (BRENTON & HUNT, 2001).

Um *firewall* é um dispositivo de *hardware* ou um aplicativo de *software* que fica entre a rede interna da organização e a rede externa (*Internet*) com o objetivo de proteger a comunicação entre ambas. Ele é responsável por bloquear todo o acesso não autorizado à rede interna (BHARDWAJ, 2007).

Para simplificar a definição, Tanenbaum (2003) metaforicamente associa o *firewall* a uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Esse recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas. No contexto de redes de computadores, é possível usar o mesmo artifício: uma empresa pode ter muitas LANs conectadas de forma arbitrária, mas todo o tráfego de saída ou de entrada da empresa é feito através de uma ponte levadiça eletrônica (*firewall*).

Por ser a primeira barreira de contenção de pacotes, o *firewall* geralmente é posicionado na borda externa da rede, entre a *Internet* e os dispositivos locais. Também é comumente utilizado para separar e controlar duas ou mais LANs.

As ferramentas de *firewall* são divididas em três principais grupos:

- *Firewall* de filtragem de pacotes - controla o tráfego usando informações armazenadas nos cabeçalhos dos pacotes. Como os pacotes são recebidos pelo dispositivo de filtragem, os atributos dos dados armazenados dentro dos cabeçalhos do pacote são comparados com a política de controle de acesso, referida como uma lista de controle de acesso (*Access Control List - ACL*). O resultado desta comparação determinará se o tráfego será permitido ou descartado (BRENTON & HUNT, 2001).

O objetivo deste tipo de *firewall* é simplesmente controlar o acesso a segmentos específicos da rede, definindo qual tráfego pode ou não passar por eles. Ele geralmente inspeciona o tráfego apenas nas camadas 3 e 4 do modelo OSI. Alguns exemplos de elementos dentro de um pacote que o *firewall* de filtragem de pacote inspeciona são: endereço de origem, endereço de destino, porta de origem, porta de destino e protocolo utilizado (FRAHIM & SANTOS, 2005).

- *Firewall* de aplicação / *Firewall Proxy* - são dispositivos que operam como agentes intermediários em nome dos clientes que estão no seu perímetro de atuação. Quando o processo-cliente do usuário enviar uma requisição, o *firewall proxy* executa um processo-servidor para receber o pedido. O pacote é aberto no nível da aplicação (camada 7 do modelo OSI) e verifica-se se o pedido é legítimo. Se for, o *firewall proxy* atua como processo-cliente e envia a resposta para o usuário. Caso contrário, o pedido é descartado e uma mensagem de erro é enviada ao solicitante (FOROUZAN & MOSHARRAF, 2013).

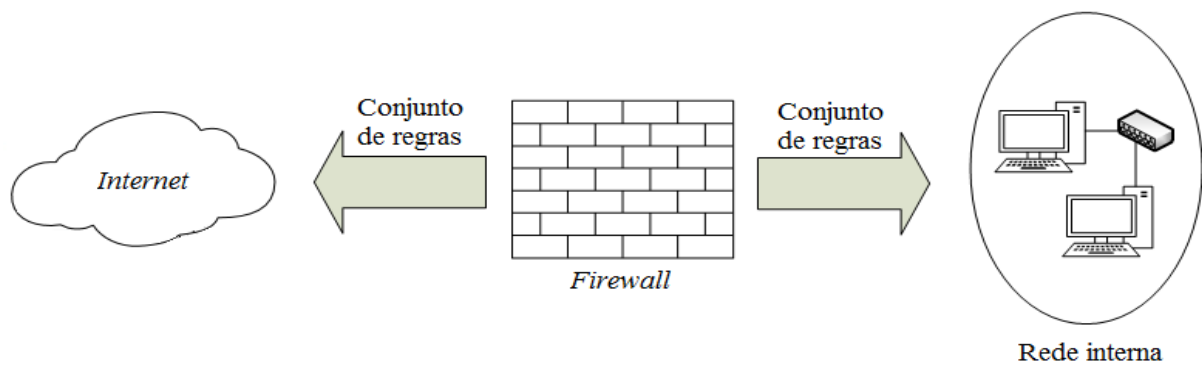
A tecnologia dos *firewalls* de aplicação é mais avançada do que a dos de filtragem de pacotes, pois examina o cabeçalho inteiro para permitir ou negar o

tráfego. A inspeção dos pacotes de dados na camada de aplicação, permite a análise de todo o pacote IP e, com base em regras pré-configuradas, liberar ou não o acesso. Possui uma velocidade de processamento levemente inferior aos *firewalls* convencionais devido ao complexo conjunto de regras e inspeções aos quais o pacote é submetido (BHARDWAJ, 2007).

- *Firewall* UTM - será descrito na seção sete deste capítulo.

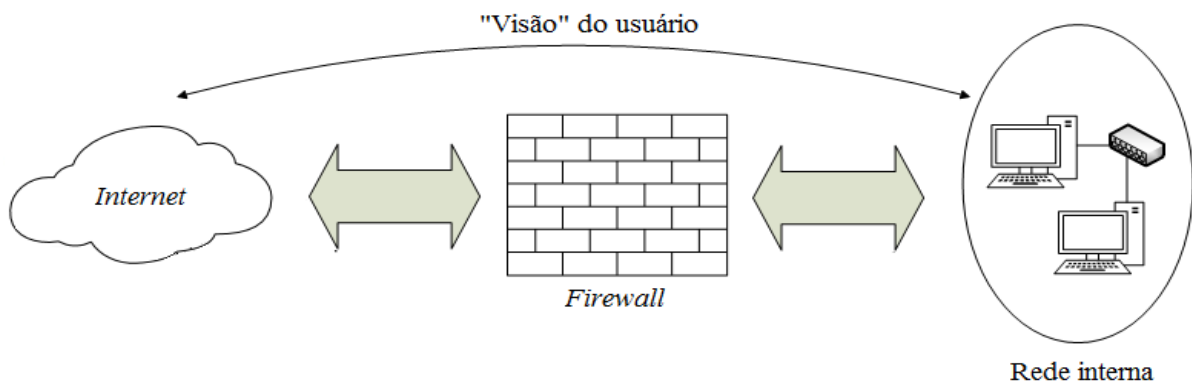
A Figura 2 e a Figura 3 ilustram, respectivamente, o funcionamento de um *firewall* de filtragem de pacotes e de um *firewall proxy*.

**Figura 2 – Firewall de filtragem de pacotes**



Fonte: Elaborado pelo autor.

**Figura 3 – Firewall proxy**



Fonte: Elaborado pelo autor.

### 2.3.2 *Intrusion Detection System - IDS*

Um Sistema de Detecção de Intrusões (*Intrusion Detection System - IDS*) é uma ferramenta capaz de detectar ataques e atividades maliciosas (não autorizadas) em uma rede de computadores ou dispositivos isolados (*host*).

Pode ser definido como as ferramentas, métodos e recursos para ajudar a identificar, avaliar e relatar a atividade de rede não autorizada ou não aprovada. A detecção de intrusão é tipicamente uma parte de um sistema de proteção global que está instalado em torno de uma rede ou dispositivo. Com isso, não se trata de uma medida de proteção independente (ENDORF, SCHULTZ & MELLANDER, 2004).

O IDS é usado para detectar intrusões e atividades maliciosas em redes corporativas que geralmente não podem ser detectadas por *firewalls* convencionais. O IDS normalmente trabalha através do monitoramento contínuo das atividades da rede e compara-as às assinaturas conhecidas de ataque. Eles podem ser hospedados em um único sistema para monitorar as atividades de um *host* específico ou em dispositivos de rede para monitorar todo o tráfego da rede (BHARDWAJ, 2007).

Há uma leve divergência entre autores quando tenta-se definir os tipos de Sistemas de Detecção de Intrusões existentes. Porém, três tipos são comumente citados, e de acordo com Endorf, Schultz e Mellander (2004) definem-se como:

*Host based Intrusion Detection System (HIDS)* - caracterizado por um *software* que reside no sistema operacional e pode verificar todos os recursos do *host* durante sua atividade. Ele registra (em um banco de dados seguro) todas as atividades que evidenciam e determinam se os eventos correspondem à alguma ação maliciosa listada na base de conhecimento.

*Network based Intrusion Detection System (NIDS)* - um sistema de NIDS é geralmente embutido na rede, e analisa os pacotes à procura de ataques. O NIDS recebe todos os pacotes em um segmento de rede particular, incluindo redes comutadas (onde este não é o comportamento padrão) através de um dos vários métodos existentes (torneiras, espelhamento de porta, entre outros). Ele reconstrói cuidadosamente os fluxos de tráfego para compará-los com padrões de comportamentos maliciosos. A maioria dos NIDSs estão equipados com ferramentas para registrar suas atividades, eventos ou alarmes em relatórios.

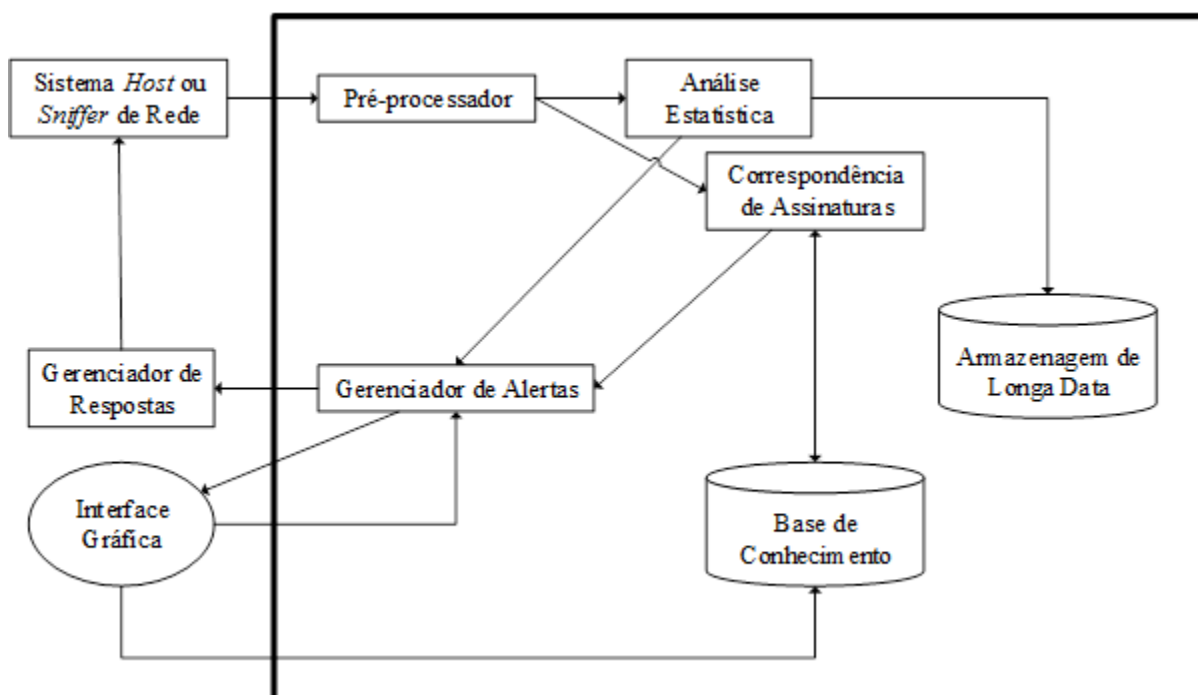
Híbridos - basicamente uma junção entre os dois métodos, pois combina um HIDS, que monitora os eventos que ocorrem no sistema *host*, com um NIDS, que monitora o tráfego de rede.



O funcionamento básico de um IDS (independentemente do seu tipo) consiste em recolher passivamente dados de diferentes processos e classificá-los. A partir disso, é possível realizar uma análise estatística a fim de determinar se a informação está fora de sua atividade normal e, se assim for, é então comparada com uma base de conhecimento. Se for encontrada uma correspondência, um alerta é enviado.

A Figura 4 descreve os principais componentes de um Sistema de Detecção de Intrusões.

**Figura 4 – Estrutura organizacional de um Sistema de Detecção de Intrusões**



Fonte: Elaborado pelo autor com base em Endorf, Schultz e Mellander (2004).

### 2.3.3 *Intrusion Prevention System - IPS*

De forma análoga ao IDS, os Sistemas de Prevenção de Intrusões (*Intrusion Prevention System - IPS*) são dispositivos de proteção de segurança ou aplicações que podem prevenir ataques contra os dispositivos de uma determinada rede.

Carter e Hogue (2006) afirmam que estes sistemas começaram como um recurso adjunto de produtos contemporâneos, tais como *firewalls* e antivírus, e evoluíram para um conjunto independente e completo de produtos em seu próprio direito.

Assim como o IDS, o IPS também se encontra dividido em três tipos (baseado em *host*, baseado em rede e híbrido). Além desta, existem muitas outras semelhanças nas configurações do IDS e do IPS, porém cabem algumas ressalvas: as ações de um usuário devem corresponder

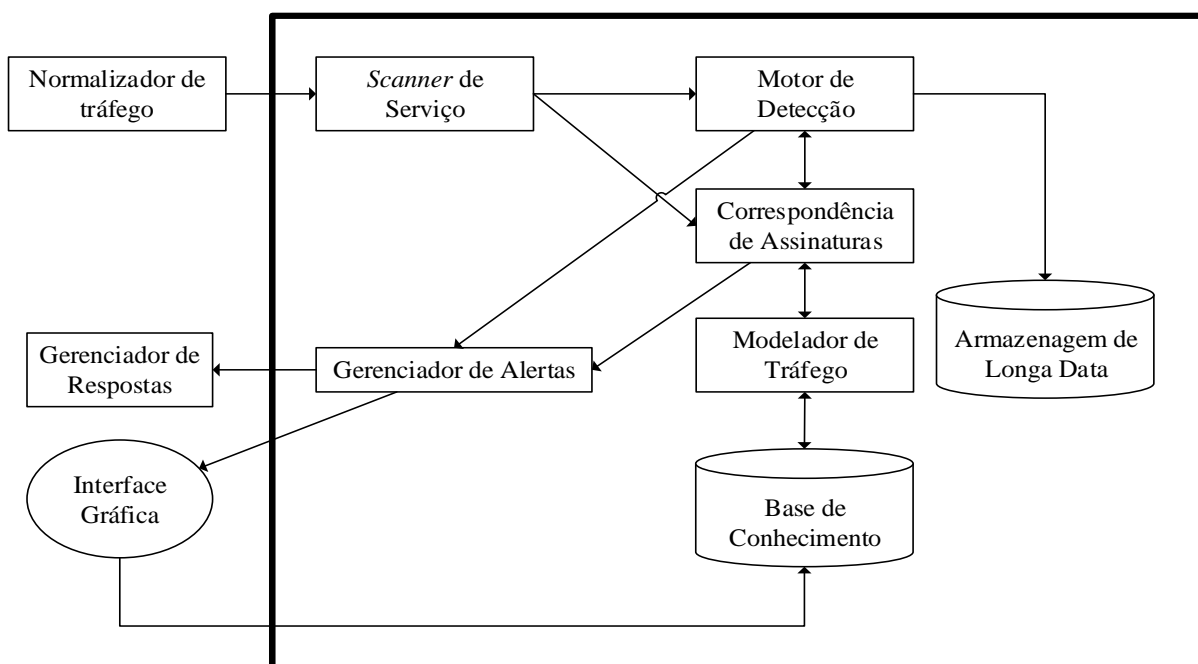
às de uma base de conhecimento pré-definida, se a ação não está na lista de permitidas, o IPS a impedirá. Ao contrário de um IDS, a lógica em um IPS é normalmente aplicada antes que a ação seja executada na memória. Alguns métodos conhecidos do IPS são os de interceptar chamadas do sistema; além comparar as somas de verificação (*checksum*) de um arquivo com uma lista de “boas somas de verificação”, antes de permitir que ele seja executado.

Segundo Endorf, Schultz e Mellander (2004), existem quatro mecanismos básicos que compõem o núcleo de um IPS:

- Normalizador de tráfego - responsável por interpretar o tráfego da rede, fazer a análise e remontagem dos pacotes, bem como executar funções básicas de bloqueio. Além destas tarefas, também fornece alimentação para o motor de detecção e para o *scanner* de serviço;
- *Scanner* de serviço - constrói uma tabela de referência, que classifica a informação e ajuda o modelador de tráfego a gerir o fluxo de informações;
- Motor de detecção - faz a correlação do padrão com a tabela de referência, além de determinar a resposta apropriada;
- Modelador de tráfego - gerencia o fluxo de informações.

Os componentes de um IPS estão esquematicamente representados pela Figura 5.

**Figura 5 – Estrutura organizacional de um Sistema de Prevenção de Intrusões**



Fonte: Elaborado pelo autor com base em Endorf, Schultz e Mellander (2004).

A Tabela 1 apresenta de forma resumida um comparativo entre as duas ferramentas.

**Tabela 1 – Comparativo entre as características do IDS e IPS**

IDS	IPS
Instalado em segmentos de rede (NIDS) e/ou em <i>hosts</i> (HIDS)	Instalado em segmentos de rede (NIPS) e/ou em <i>hosts</i> (HIPS)
Implementado na rede de forma passiva	Implementado em linha (não passiva)
Não inspeciona o tráfego criptografado	Melhor utilizado em aplicações de proteção
Controle de gerenciamento central	Controle de gerenciamento central
Melhor na detecção de ataques de <i>hackers</i>	Ideal para bloquear anomalias da WWW
Produto de alerta (reativo)	Produto de bloqueio (proativo)

Fonte: Elaborado pelo autor com base em Endorf, Schultz e Mellander (2004).

Embora cada uma das tecnologias de IDS e IPS têm seu próprio lugar em um programa de segurança, pois executam funções distintas, é possível concatená-las em uma grande solução devido à sua complementariedade.

### 2.3.4 Antivírus

Mantém o controle de vírus e outros *softwares* maliciosos. O antivírus usa assinaturas de vírus para detectar a presença de um *malware* (mecanismo semelhante ao do IDS/IPS). As assinaturas devem ser atualizadas regularmente para que o aplicativo possa efetivamente detectar e limpar o sistema de quaisquer novos vírus (BHARDWAJ, 2007).

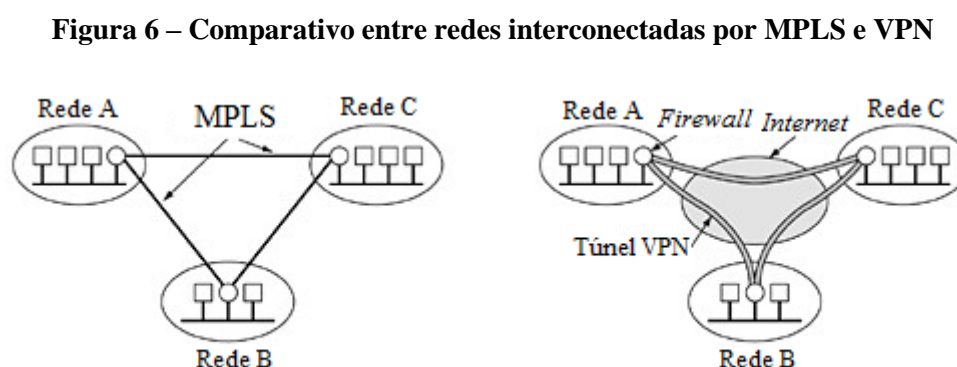
Outra técnica comumente utilizada por ferramentas de antivírus é a heurística. Basicamente, a heurística é uma regra ou comportamento. Se um vírus possui uma determinada ação, o *software* antivírus tenta pará-lo no ato. Se um trecho de código de repente acessa uma área crítica do Sistema Operacional (como o sector de definição da tabela de arquivos em um disco rígido), o antivírus reconhece esta malícia e a impede de causar danos ao dispositivo. Outros indicadores de risco incluem mudanças estranhas no tamanho do arquivo (particularmente em arquivos do SO), diminuições bruscas de espaço disponível no disco rígido, ou alterações no tempo de arquivo ou carimbos de data (LEHTINEN, RUSSELL & GANGEMI, 2006).

## 2.4 Interconexão de redes

As redes de computadores definem-se, resumidamente, pela conexão de dispositivos e periféricos em um mesmo ambiente compartilhado. Porém é comum que empresas de médio e grande porte possuam uma segunda necessidade de comunicação: interconectar duas ou mais redes (locais e remotas) em uma única malha corporativa. Este cenário, na grande maioria dos casos, exemplifica uma relação de dependência entre filial e matriz, onde é disponibilizado para todas as unidades o acesso aos servidores de *Enterprise Resource Planning* (ERP), banco de dados e demais serviços e ativos inerentes ao trabalho. Outro exemplo que geralmente demanda a interconexão de redes são as corporações que mantêm um vínculo estrutural direto com parceiros ou prestadores de serviço.

Quando há uma pequena distância entre as duas ou mais unidades as melhores opções de interconexão são baseadas diretamente no meio-físico, tais como: fibra óptica e rádios ponto a ponto. Porém quando se rompem as barreiras geográficas para cidades, estados, países ou até mesmo continentes, os principais meios de interconexão são as soluções de *Multi Protocol Label Switching* (MPLS) e *Virtual Private Network* (VPN). A seguir são apresentadas maiores informações sobre estas duas tecnologias.

A Figura 6 apresenta duas estruturas de redes interconectadas a partir de MPLS e VPN, exemplificando a diferença entre ambas.



Fonte: Adaptado pelo autor de Tanenbaum (2003).

### 2.4.1 *Multi Protocol Label Switching* - MPLS

O MPLS consiste em uma tecnologia baseada em pacotes etiquetados (rotulados), no qual cada rótulo representa um índice na tabela de roteamento que informa quem é o próximo

roteador no caminho da comunicação (*next-hop*). O objetivo de uma rede MPLS é servir como mecanismo de trânsito, transportando pacotes entre pontos de entrada e saída.

Os rótulos MPLS são anunciados entre os roteadores para que eles possam construir um mapeamento rótulo-a-rótulo. Estas etiquetas são anexadas aos pacotes IP, permitindo que os roteadores encaminhem o tráfego sem conhecer o endereço IP de destino, uma vez que apenas as *tags* são utilizadas para direcionar o pacote (DE GHEIN, 2006).

As estruturas de MPLS são compostas por quatro principais itens:

- *Label Switch Router (LSR)* - são roteadores que encaminham os pacotes baseados apenas no seu rótulo. Os LSRs se comunicam através de protocolos de sinalização, tais como: *Label Distribution Protocol (LDP)* ou *Resource Reservation Protocol (RSVP)*.
- *Label Edge Router (LER)* - análogo ao LSR, porém responsável também pela inserção e remoção do rótulo, além de atribuir os pacotes a uma classe de envio equivalente. O processo de inserção de um rótulo e posterior vínculo a uma FEC é efetuado somente na admissão (entrada) do pacote no circuito MPLS.
- *Forwarding Equivalency Class (FEC)* - trata-se de um conjunto de parâmetros (endereço IP de origem e destino, número da porta da origem e destino, ID do protocolo IP, entre outros) que irão determinar o caminho por onde pacotes percorrerão.
- *Label Switch Path (LSP)* - define-se pelo caminho determinado pela FEC.

No tráfego MPLS, a cada pacote que entra na rede é atribuído uma classe de envio equivalente (FEC). Esta atribuição utiliza um rótulo, que identificará a FEC. O rótulo é então inserido no cabeçalho e, em cada roteador por onde este pacote passar dentro da rede MPLS, ele será o único elemento a ser analisado para determinar o próximo roteador para onde deve ser encaminhado. O processo de análise do rótulo recebe o nome de permuta de rótulos (*label swapping*) (DE OLIVEIRA, 2006).

Devido a sua forma de atuação, entre as camadas 2 e 3 do modelo OSI, é comum encontrar referências do protocolo MPLS como pertencente a uma fictícia *layer 2,5*.

#### **2.4.2 Virtual Private Network - VPN**

Desde o advento da *Internet*, os administradores de rede têm procurado maneiras de aproveitar o seu baixo custo para transportar dados, sem comprometer a integridade e a

confidencialidade das informações, além de manter a transparência para o usuário final. Esta foi a origem do conceito de redes privadas virtuais (FRAHIM & SANTOS, 2005).

Uma VPN é um meio seguro e privativo de transmitir dados através de uma infraestrutura de rede não segura e compartilhada (*Internet*). A VPN protege as informações que são transmitidas com a utilização de recursos de encapsulamento e criptografia de dados. Na prática uma VPN é associada a um túnel, pois é um método eficaz de transmitir os dados de uma rede para outra (CARMOUCHE, 2006).

Embasada nas premissas de segurança, a VPN deve prover a confidencialidade dos dados (garantia de que o conteúdo da mensagem seja interpretado apenas por fontes autorizadas); a integridade (garantia da não adulteração/alteração em trânsito); o não-repúdio do remetente (evita que um remetente falsamente negue que tenha enviado uma mensagem para o receptor) e a autenticação (garantia de que a mensagem seja enviada e recebida apenas pelas entidades autênticas).

Com o passar do tempo, a Força Tarefa de Engenharia da *Internet - Internet Engineering Task Force* (IETF) definiu em suas respectivas RFCs (*Request for Comments*) inúmeros protocolos diferentes para o serviço de VPN, tais como: *Point-to-Point Tunneling Protocol* (PPTP), *Layer 2 Forwarding Protocol* (L2F), *Layer 2 Tunneling Protocol* (L2TP), *Multiprotocol Label Switching VPN* (MPLS VPN), até chegar ao então atual *Internet Protocol Security* (IPSec).

A Tabela 2 associa os protocolos de VPN de acordo com a sua respectiva atuação nas camadas de referência do modelo OSI.

**Tabela 2 – Protocolos de VPN e o modelo OSI**

IDS	IPS
Camada 7 - Aplicação	<i>Secure</i> HTTP (HTTPS)
Camada 6 - Apresentação	N/A
Camada 5 - Sessão	N/A
Camada 4 - Transporte	SSL e TLS, SSH
Camada 3 - Rede	IPSec, MPLS VPN
Camada 2 - Enlace	PPTP, L2TP, LF2
Camada 1 - Física	L1 VPN

Fonte: Elaborado pelo autor com base em Carmouche (2006).

### 2.4.3 Internet Protocol Security - IPsec

O IPsec tornou-se uma escolha óbvia para a maioria dos fornecedores devido às suas características robustas. Conforme definido na RFC 2401, garante as premissas de segurança na camada 3 (rede) da pilha do modelo OSI.

O IPsec é um conjunto de protocolos que definem padrões para quatro principais elementos necessários para uma solução robusta de VPN: protocolos de segurança; mecanismos de troca de chaves; algoritmos necessários para criptografia e troca de chave segura; definições e manutenção de *Security Associations* (SAs) (CARMOUCHÉ, 2006).

A versatilidade do IPsec resume-se em uma miscelânea de protocolos já existentes e amplamente utilizados, tais como: *Diffie-Hellman* (DH), *Data Encryption Standard* (DES), *Triple Data Encryption Standard* (3DES), *Secure Hash Algorithm One* (SHA-1), *Message Digest Algorithm 5* (MD5), entre outros. Esta flexibilidade de opções foi decisiva para sua ampla utilização e natural desuso dos demais protocolos de VPN.

De acordo com Souza (2010), o IPsec possui dois modos distintos de operação:

- Transporte - nesse modo, somente a informação é criptografada, enquanto o cabeçalho IP original não é alterado. Assim, apenas adiciona-se alguns octetos a cada pacote, deixando que dispositivos da rede pública vejam a origem e o destino do pacote.
- Túnel - nesse modo, todo o pacote IP original é criptografado e passa a ser a informação de um novo pacote IP. Este modo permite que um dispositivo de rede aja como um *Proxy* IPsec (o dispositivo realiza a encriptação em nome dos terminais). O roteador de origem criptografa os pacotes e os envia ao longo do túnel IPsec enquanto o roteador de destino descriptografa o pacote IP original e o envia ao sistema de destino.

### 2.4.4 Topologias de VPN

Frahim e Santos (2005) classificam as VPN em dois grandes grupos no que se refere à topologia de conexão:

- *Remote Access* - permite que usuários móveis possam trabalhar a partir de locais remotos (sua própria residência, hotéis, cafés e afins) como se estivessem conectados diretamente à rede corporativa. Tudo isso sem comprometer a segurança da corporação. Neste cenário, o usuário faz uso de um cliente (*software*) que se conecta diretamente ao concentrador de VPN.

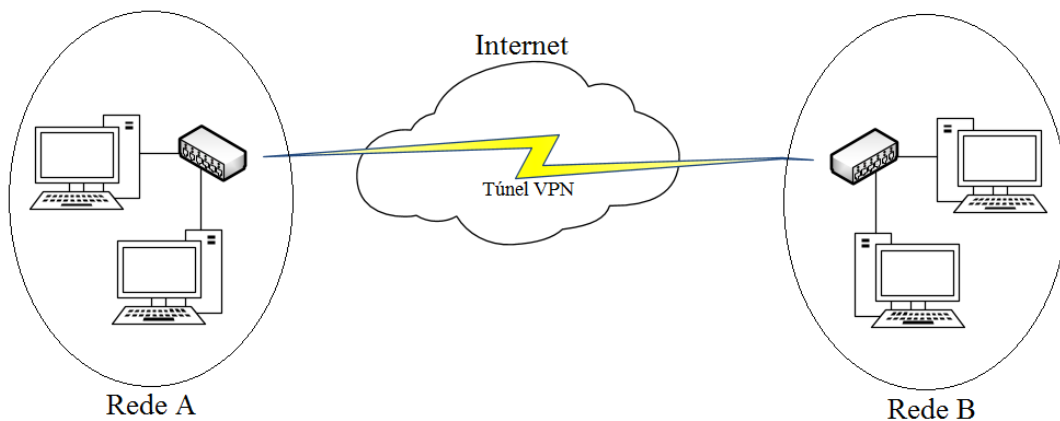
- *Site to Site* - permite que empresas estabeleçam conexões VPN entre dois ou mais escritórios para que possam trocar tráfego entre si. Neste ambiente, a conexão é estabelecida diretamente entre os dispositivos concentradores de VPN de cada unidade.

A modalidade *Site to Site* possui três subdivisões definidas de acordo com o fluxo dos pacotes de uma rede para outra:

- *Site to Site* convencional - conexão VPN entre dois pontos para que possam trocar tráfego entre si.

A Figura 7 contextualiza este cenário.

**Figura 7 – VPN *Site to Site* convencional**



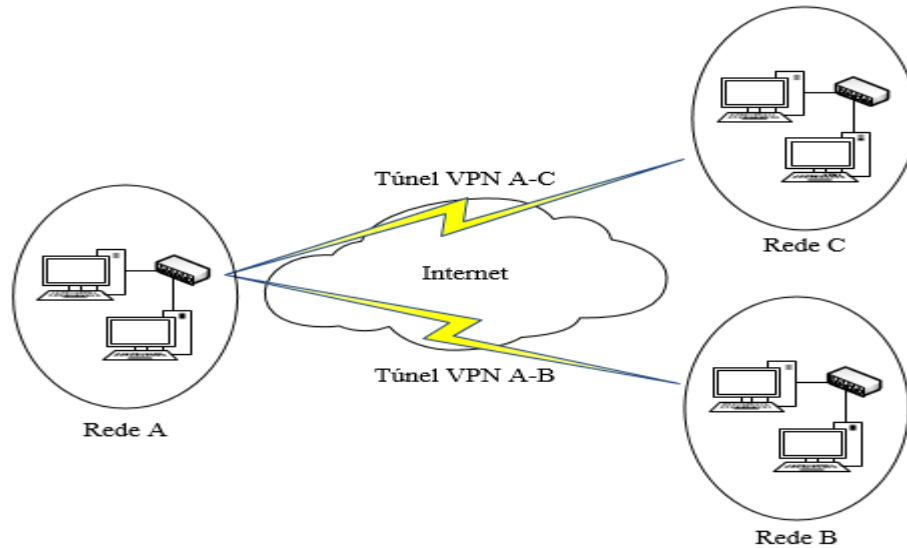
Fonte: Elaborado pelo autor.

- *Site to Site Hub and Spoke* - nesta modalidade há necessariamente mais de duas unidades envolvidas. Faz a utilização de um ponto central de concentração entre os túneis VPN (geralmente atribuído à unidade matriz). Para que os pacotes de uma rede cheguem à outra devem obrigatoriamente passar pelo ponto central de comunicação.

A subdivisão de VPN *Site to Site Hub and Spoke* é ilustrada na Figura 8.



**Figura 8 – VPN Site to Site Hub and Spoke**

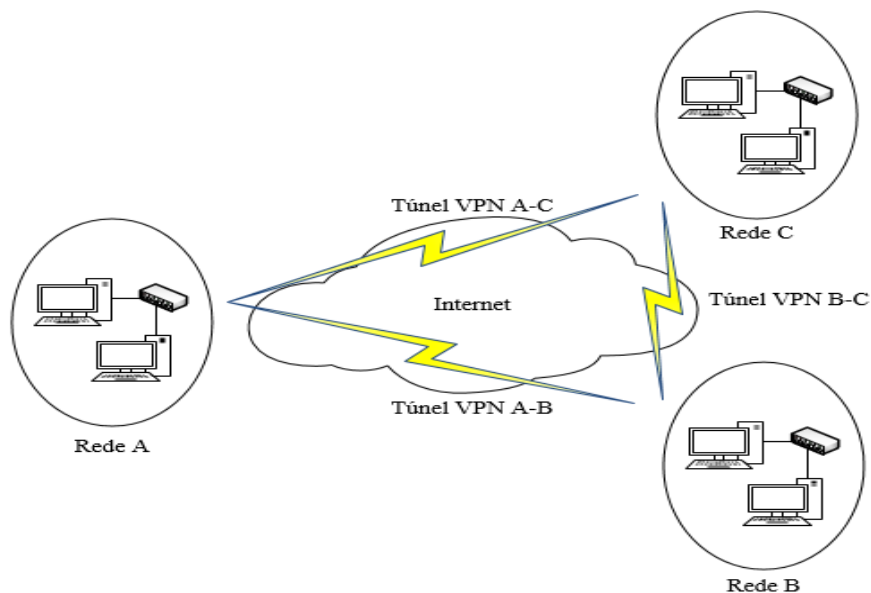


Fonte: Elaborado pelo autor.

- *Site to Site Mesh* – também requer mais de duas unidades em sua estrutura. Porém nesta forma de VPN há uma independência de comunicação entre todos os pontos envolvidos, pois há um túnel estabelecido entre cada ponta. Ou seja, duas redes distintas estabelecem um vínculo diretamente entre si, sem depender de um ponto central para a troca de tráfego.

A topologia de VPN *Site to Site Mesh* é representada pela Figura 9.

**Figura 9 – VPN Site to Site Mesh**



Fonte: Elaborado pelo autor.

## 2.5 Navegação segura

Para garantir a segurança das informações corporativas, muitas vezes o administrador de redes precisa ter controle de quais *sites* e aplicativos os usuários podem ou não utilizar. Esta estratégia minimiza significativamente as chances de uma ameaça penetrar na rede, através destas origens, e recebe o nome de “navegação segura”. Filtragem de Localizador Padrão de Recursos (*Uniform Resource Locator* – URL: endereço de qualquer tipo de recurso disponível em uma rede), filtragem de aplicação e antivírus de *gateway* são alguns dos seus principais recursos, e são explicados abaixo com maior detalhamento.

### 2.5.1 Filtragem de URL (*Uniform Resource Locator*)

A filtragem de URL permite controlar quais tipos de conteúdo *web* um usuário pode visualizar, reduzindo significativamente sua exposição a *spyware*, *phishing*, *pharming*, *sites* impróprios, *site* de redirecionamento e outras ameaças que rondam a *Internet*. Este recurso verifica o conteúdo de cada página da *web* que seja aceita por uma política de acesso. Os filtros de conteúdo permitem criar listas negras (conteúdos bloqueados) de palavras e frases, ou liberar acesso somente a uma lista branca (conteúdos permitidos) de *sites*. O controle por categoria é um terceiro método de filtragem, que se baseia em avaliações de URL para permitir o acesso aos "bons" *sites* e bloquear o acesso a *sites* classificados como "ruins", de acordo com uma listagem pré-definida (TITTEL, 2014).

Caracteriza-se por possibilitar aos administradores monitorar e controlar as atividades de navegação dos funcionários e usuários convidados. Com a capacidade de se integrar com ferramentas de autenticação, as políticas de filtragem de conteúdo podem ser personalizadas para restringir *sites* específicos ou procurar padrões em endereços da *web*, de acordo com cada nível de usuário, protegendo ainda mais a empresa a partir de uma matriz de riscos relacionados legal, regulatório ou de produtividade.

Apresenta-se na forma de *software*, geralmente associado a um servidor *proxy*, que é responsável por todo o tráfego *web* das máquinas da rede, onde é facilmente implementada uma base de regras com permissões ou bloqueios de *sites*. Também pode ser instalado diretamente nos dispositivos de borda, como *firewalls* UTM ou outros *gateways* com suporte à filtragem *web*.

### 2.5.2 Filtragem de aplicação

Os aplicativos que fornecem serviços para os usuários finais podem ser vulneráveis a diversas ameaças, mesmo que muitas delas sejam controladas pelos próprios fabricantes da ferramenta. O controle de aplicações fornece uma camada de proteção entre os usuários finais e os *softwares*, pois inspeciona tanto o tráfego destinado ao aplicativo como a sua respectiva resposta.

Conforme salienta Miller (2011), a *Internet* criou uma nova geração de aplicações que são acessadas por diversos usuários, tanto para fins pessoais como para fins empresariais. Muitas aplicações ajudam a melhorar a produtividade de quem a utiliza, porém outras consomem grandes quantidades de largura de banda, representam riscos de segurança e aumentam a probabilidade de vazamento de dados críticos.

O filtro de aplicativos pode identificar e controlar aplicações, *softwares*, serviços de rede e protocolos, com o intuito de proteger as redes contra as mais recentes ameaças baseadas na *web*. É capaz de detectar e controlar aplicativos como *YouTube*, *Facebook*, *Twitter* e afins, diretamente na camada 7 do modelo OSI. Sistemas avançados de retenção de aplicações possibilitam um controle granular de políticas, com suporte a regras baseadas na identificação dos usuários corporativos. Ou seja, um determinado *software* pode ser permitido para um determinado perfil de usuário e, ao mesmo tempo, negado para outro. Sua atuação estende-se aos diferentes terminais de rede (estações de trabalho, *notebooks*, *smartphones*, *tablets*). Além da negação do acesso, também é possível apenas monitorar a utilização do aplicativo ou realizar regras de controle de banda sobre ele (TITTEL, 2014).

Algumas vantagens oriundas da filtragem de aplicativos:

- Ter visibilidade e controle dos aplicativos utilizados por diferentes usuários.
- Minimizar a exposição da rede às ameaças externas.
- Possibilidade de priorização de tráfego das aplicações fundamentais.
- Melhoria da produtividade corporativa ao restringir a distração dos usuários.

### 2.5.3 Antivírus de gateway

*Softwares* de antivírus tradicionais são instalados diretamente nos dispositivos finais (estações de trabalho e servidores) com o objetivo de impedir que os mesmos sofram danos oriundos de códigos maliciosos.

Para Bhardwaj (2007) o antivírus mantém o controle de vírus e outros *softwares* maliciosos. Ajuda a proteger o sistema contra vírus, cavalos de Tróia, *worms* e *spywares*. O

*software* antivírus usa assinaturas de vírus para detectar a presença de um código malicioso, desta maneira possui um funcionamento análogo à ferramenta de IDS/IPS.

As soluções de antivírus de *gateway* possuem uma leve diferença em relação ao modelo tradicional: por atuarem diretamente na fronteira (borda) entre a rede local e a *Internet*, a inspeção em busca de ameaças é feita no fluxo entrante. Ou seja, conforme os múltiplos pacotes de um arquivo são baixados, a análise é realizada e, se for detectada a presença de um vírus, o seu descarte é imediato. Desta maneira o vírus é negado antes mesmo de chegar à máquina de destino.

## 2.6 Controle de mensagens

Robichaux (2004) salienta que ao longo dos anos, a necessidade de segurança aumentou, assim como a necessidade de apoiar modelos administrativos mais complexos e padrões constantemente atualizados. O aumento da utilização da *Internet* como um mecanismo de transporte para mensagens críticas de negócios (*e-mails*) têm levado a um aumento da demanda para a capacidade de proteger tais informações.

No entanto, as ferramentas de envio de *e-mail* não são utilizadas apenas por empresas e pessoas bem-intencionadas. Muitas vezes o envio de mensagens eletrônicas é feito de forma indevida e maliciosa, gerando danos a quem as recebe. O bloqueio do envio de *spam* (*e-mails* não solicitados, que geralmente são encaminhados a uma grande quantidade de destinatários e possuem conteúdos pornográficos, ofertas de produtos e afins) ou da propagação de mensagens que contenham vírus (que objetivam a infecção do computador receptor a fim de obter dados sigilosos ou prejudicar o sistema de forma deliberada) é a principal função dos dispositivos de controle de mensagem.

Abaixo são listados alguns exemplos de problemas enfrentados quando o controle de mensagens não é implementado:

- Utilização desnecessária de recursos de banda e tempo - para cada novo *spam* na caixa de entrada, é necessário que os usuários corporativos despendam seu tempo para lê-lo, analisá-lo e removê-lo, o que resulta em uma grande perda de produtividade. Além de comprometer as atividades corporativas, as mensagens não desejadas também representam um gasto desnecessário do *link* de *internet*, uma vez que todo o tráfego gerado no *download* deste conteúdo não traz nenhum benefício à empresa.

- Perda de mensagens importantes - em virtude do elevado número de *spams* recebidos, as corporações correm o risco de mensagens importantes não serem lidas, serem lidas com atraso, ou, em uma possibilidade ainda pior, serem apagadas equivocadamente.
- Má utilização dos recursos computacionais - boa parte do poder computacional dos servidores de *e-mail* (processamento, memória e espaço em disco) é empregado no tratamento de mensagens indesejadas.

### 2.6.1 *AntiSpam*

Schwartz (2004) descreve *AntiSpam* como uma ferramenta para análise de mensagens de *e-mail*, que determina qual a probabilidade de ser um *spam* e reporta/documenta suas conclusões. É um sistema que compara diferentes partes das mensagens de *e-mail* com um grande conjunto de regras, onde cada regra adiciona ou remove pontos em uma classificação. Uma mensagem com uma pontuação que ultrapasse o limite permitido é classificada como *spam*.

As principais técnicas utilizadas por sistemas de filtragem de *spam* são elencadas por Granier (2006):

- Análise de *Checksums* - a filtragem com base em algoritmos de *checksum* realiza uma série de cálculos matemáticos contra um *e-mail*, ou parte dele, para identificar e quantificá-lo com base em uma tabela de referência de *spams* conhecidos. Em vez de armazenar toda a informação em questão, os motores de *checksum* irão simplesmente executar cálculos sob esse conteúdo para apresentá-lo de uma forma mais simples, com a finalidade de facilitar a comparação. Se os resultados coincidirem com algum valor da tabela de referência, acrescentam-se pontos a sua classificação.
- Análise em Listas Negras de Tempo Real (*Real-time Blackhole List* - RBL) - também conhecidas como listas de bloqueio baseadas em DNS (*DNS Black List* - DNSBL), caracterizam-se por serem listas de endereços IP, que são publicadas por meio de DNS, e aceitas como fontes conhecidas e confiáveis de *spam*. Toda mensagem proveniente de um servidor de *e-mail* listado em uma RBL terá fortes indícios de ser categorizada como *spam*. Estas listas geralmente são disponibilizadas gratuitamente ou adquiridas por uma pequena taxa.

- Filtros *Bayesianos* - a filtragem *Bayesiana* também é baseada em cálculos estatísticos de probabilidade. Esta técnica leva em consideração o *feedback* dos usuários para treinar o filtro, de modo que possa ajustar-se dinamicamente às novas entradas. O filtro interpreta as mensagens avaliadas pelos usuários como *spam* e procura identificar algum tipo de padrão. Quando há uma correlação entre uma nova mensagem e um modelo detectado, são acrescentados pontos à classificação do conteúdo como *spam*.
- Listas negras e listas brancas - uma lista negra trata-se, efetivamente, de uma espécie de RBL local. Com funcionamento idêntico às RBLs, busca identificar um endereço de origem específico, domínio ou IP a partir do qual todas as mensagens devem ser bloqueadas. A única diferença substancial entre as listas negras e as RBL está no seu escopo de atuação, uma vez que todo e qualquer registro aplicado a elas afetam exclusivamente o domínio local onde a ferramenta de *AntiSpam* opera, não gerando nenhum impacto a usuários de outros domínios de *e-mail*. As listas brancas, em contrapartida, também buscam identificar um endereço de origem específico, domínio ou IP, porém com o objetivo de permitir qualquer *e-mail* oriundo destas fontes. Sua abrangência também está limitada ao escopo local.

As ferramentas de *AntiSpam* fazem uso destes artifícios de forma complementar, ou seja, são feitas em série: uma após a outra. Os resultados são somados em uma mesma variável, fator responsável por uma maior confiabilidade na hora de classificar uma mensagem como *spam*.

### 2.6.2 Antivírus de *e-mail*

Granier (2006) salienta que, atualmente os *spams* que apresentam um maior risco à segurança corporativa são aqueles que carregam algum tipo de vírus. Bhardwaj (2007) complementa ao afirmar que estes códigos maliciosos são muitas vezes enviados para destinatários de *e-mail* como anexos de mensagens. Assim que o destinatário clica no anexo, o vírus torna-se ativo e se instala em seu computador.

Uma vez infectada, ao levar-se em consideração a natureza do vírus, esta máquina poderá ser utilizada para enviar dados sigilosos aos *spammers* (remetentes de *spam*), para infectar outras máquinas ou ainda para servir como um novo remetente de mensagens falsas.

Os sistemas de antivírus de *e-mail* não operam diretamente com arquivos comprimidos ou em formato usual. Anterior à sua análise, os mecanismos de segurança desmontam a mensagem e, em muitos casos, descompactam os anexos. A partir deste momento, a varredura é feita de maneira semelhante aos dispositivos de antivírus convencionais.

Em virtude da elevada utilização de recursos computacionais nos processos de desmontagem da mensagem e de reconhecimento de padrões, a inspeção de vírus de *e-mail* é, estrategicamente, feita depois das mensagens já serem aprovadas pelas ferramentas de *AntiSpam*.

## 2.7 Soluções de Gerenciamento Unificado de Ameaças

Com a expansão da *Internet*, um número cada vez maior de empresas sofre ataques cibernéticos provenientes das mais variadas formas. Os custos destes ataques são altos, pois a violação de dados sigilosos e importantes pode representar um prejuízo de milhões de reais à companhia. É evidente que haja uma preocupação em evitar, ou pelo menos minimizar, os danos causados por eles.

Diferentes ataques requerem diferentes métodos de defesa. Uma medida amplamente utilizada caracteriza-se pela "defesa em camadas", onde inúmeras ferramentas de segurança (*firewall*, IDS/IPS, antivírus, entre outras) são utilizadas de forma complementar uma à outra. No entanto, esta técnica introduz seu próprio conjunto de problemas: a utilização de diferentes tecnologias pontuais de segurança não garante uma total integração direta entre elas e pode gerar uma diminuição na eficácia geral da solução. Também se soma o fato de aumentar significativamente os custos de segurança, a complexidade de gerência, a utilização de recursos computacionais e a latência média da rede.

Scarfone (2014) afirma que uma resposta do mercado ao problema da defesa em camadas foi a criação de ferramentas, que agreguem todos estes pontos díspares de soluções de segurança em um único produto, conhecidas como sistema de gerenciamento unificado de ameaças (*Unified Threat Management* - UTM). Criadas com o objetivo de proporcionar uma forma mais conveniente de implementar o conceito da defesa em camadas, uma vez que há um único produto para configurar, gerenciar e monitorar. Toda a inspeção e análise dos pacotes da rede são feitas apenas uma vez, e as informações são compartilhadas entre os múltiplos recursos de segurança para aumentar a precisão das detecções.

De maneira complementar, Tittel (2014) resume dispositivos UTM como uma plataforma de segurança de rede de base ampla, que representa o próximo estágio de evolução

para os *firewalls* tradicionais. Define uma gama de elementos de *hardware* e *software* para proteger redes corporativas embutidos em uma única solução integrada.

Os recursos de segurança que compreendem as soluções UTM não são novos, pois a maioria deles estão apresentados há muitos anos como soluções pontuais. Os principais mecanismos disponíveis nesta linha de produto são: *AntiSpam*, antivírus para *web* e *e-mail*, controle de aplicações, *firewall*, detecção/prevenção de intrusão, rede privada virtual e filtragem de conteúdo *web*. Os dispositivos de gerenciamento unificado de ameaças, atualmente, também estão expandindo suas funcionalidades para incluir recursos de segurança adicionais, tais como: balanceamento de carga, prevenção contra perda de dados (*Data Loss Prevention - DLP*) e gerenciamento de banda.

Inicialmente, os sistemas UTM foram criados para atingir empresas de pequeno e médio porte, onde havia uma escassez de recursos financeiros e de mão-de-obra especializada em segurança da informação. No entanto, com o passar do tempo, a ampla utilização destas ferramentas exigiu uma evolução natural para atender também as empresas de grande porte e elevada complexidade de gestão.

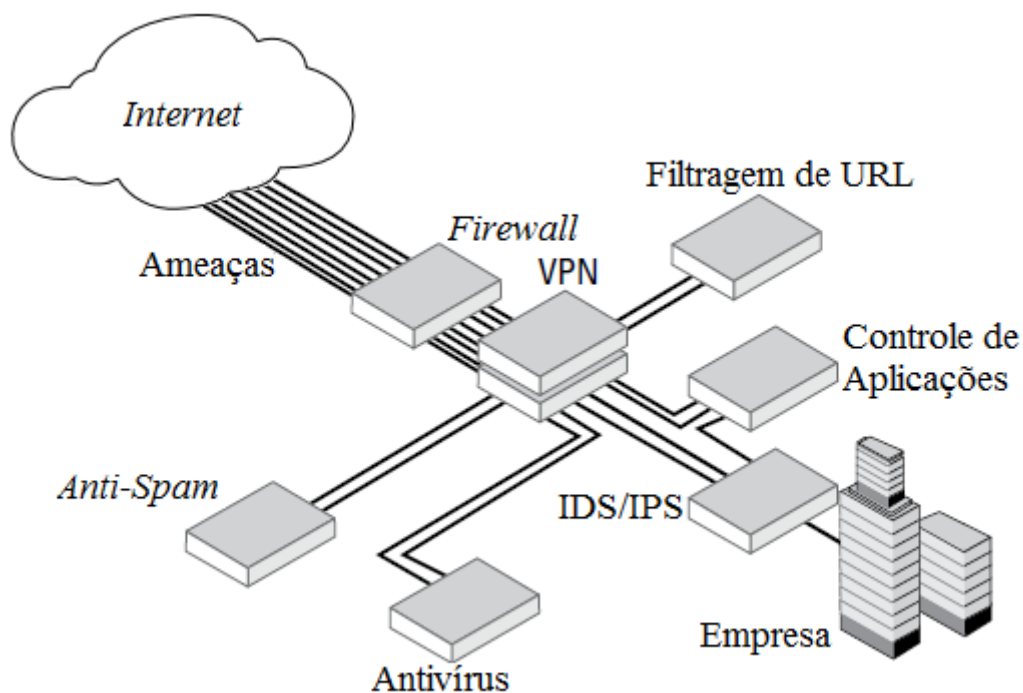
A arquitetura deste tipo de solução geralmente é apresentada na forma de *appliance* (*hardware + software*), onde os dispositivos físicos são preparados, desde o seu *core* de processamento até as interfaces de rede, para maximizar a *performance* das análises e detecções, fator responsável por uma maior estabilidade na rede onde atua. Os modelos baseados apenas em *software* requerem um servidor dedicado e de alto poder computacional para que as inspeções realizadas não resultem em um gargalo na velocidade geral da rede.

Equipamentos de segurança UTM geralmente são instalados de forma análoga a dispositivos de *firewall* convencionais, atuando diretamente nos limites da rede interna com o mundo externo (*Internet*) ou nas bordas entre diferentes segmentos da malha corporativa.

As Figuras 10 e 11 exprimem, respectivamente, a arquitetura organizacional de soluções de segurança baseadas na defesa em camadas e de gerenciamento unificado de ameaças.

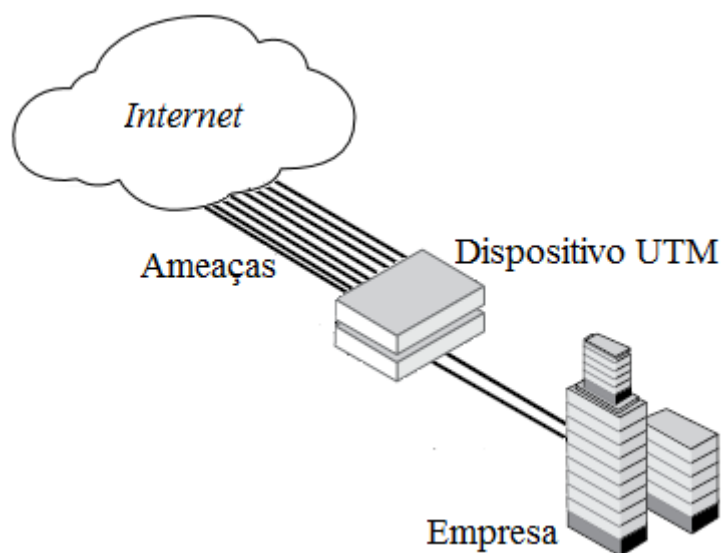


Figura 10 – Arquitetura organizacional de um sistema de defesa em camadas



Fonte: Adaptado pelo autor de Tittel (2014).

Figura 11 – Arquitetura organizacional de um sistema UTM



Fonte: Adaptado pelo autor de Tittel (2014).

Embora, à primeira vista, a utilização de sistemas UTM pode gerar um ponto central de falha, o que comprometeria toda a atividade da rede, muitos fabricantes implementam o conceito de alta disponibilidade (*High Availability* - HA). Tal *feature* consiste em dois

equipamentos idênticos em operação concomitante na modalidade ativo-passivo, onde o segundo dispositivo só entra em atividade caso haja alguma falha no principal.

As principais vantagens aplicadas aos sistemas de gerenciamento unificado de ameaças são:

- Garantia de compatibilidade entre os diferentes recursos de segurança.
- Diminuição de gastos na gestão da segurança corporativa.
- Maximização da eficiência das políticas de segurança.
- Centralização de *logs* e alertas.
- Facilidade na tomada de decisão diante a uma incidência de ataque ou ameaça à segurança.

Bigelow (2008) frisa que o verdadeiro desafio para utilizar soluções UTM é a configuração do produto. O planejamento prévio é crucial, pois é preciso compreender plenamente os dispositivos de redes, as aplicações utilizadas, os níveis e privilégios de acesso, as regras de negócio, enfim, toda a macroestrutura corporativa. Somente após este ponto é possível desenvolver um conjunto eficaz e eficiente das regras de segurança que irá abordar todas as necessidades do ambiente. Ele também destaca que as configurações aplicadas a um produto UTM são dinâmicas, pois mudam à medida que as aplicações, infraestrutura e necessidades de negócios evoluem.

## 2.8 Comparativo entre UTM e NGFW

Embora exista uma divisão suficientemente visível entre fabricantes de segurança no que se diz respeito às soluções de *Unified Threat Management* e *Next Generation Firewall*, os conceitos teóricos e os resultados práticos não se divergem de forma acentuada. O núcleo de soluções é explicitamente o mesmo, fator que inclusive dificulta a definição de cada escopo.

É notável que a diferença está mais ligada ao setor de *marketing*, onde alguns fabricantes se projetam como a “próxima geração de *firewalls*”, o que leva a crer que suas ferramentas são mais avançadas e eficientes que aquelas baseadas no conceito do gerenciamento unificado de ameaças. Plato (2012) destaca que esta separação de produtos não possui um cunho técnico e que somente justifica uma tentativa de fazer com que alguns fornecedores pareçam mais competitivos do que realmente são. Ele associa, metaforicamente, a bifurcação dos produtos a apenas “tons de cinza”.

A Figura 12 apresenta um quadro comparativo entre as funcionalidades embutidas em ferramentas UTM e NGFW.

**Figura 12 – Funcionalidades presentes em soluções UTM e NGFW**

Categoria	Produto	Firewall	IDS/IPS	Antivírus de gateway	Filtragem de URL	Controle de aplicações	Segurança de e-mail	VPN
<i>Next Generation Firewall</i>	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
<i>Unified Threat Management</i>	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
Adicionais	Cisco	Sim	Sim	Sim	Sim	Não	Sim	Sim
	Juniper	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Fonte: Adaptado pelo autor de Plato (2012).

É possível notar, a partir da análise do quadro acima, que tanto dispositivos NGFW quanto UTM possuem essencialmente as mesmas ferramentas de segurança.

### 3 MATERIAIS E MÉTODOS

O presente estudo possui dois objetivos a serem alcançados: o primeiro consiste na instalação de uma ferramenta baseada no conceito do gerenciamento unificado de ameaças em três organizações de diferentes portes (pequeno, médio e grande), além de compreender as análises, levantamentos e métodos utilizados antes, durante e após a implementação da solução; o segundo concentra-se em dimensionar o retorno sobre o investimento para cada estrutura, realizar a mensuração dos fatores que motivaram a escolha de um dispositivo UTM como ferramenta de segurança, bem como explicar o aumento gerado no nível geral de segurança de cada corporação.

Neste capítulo, dividido em cinco sessões, serão apresentados os cenários/ambientes, as ferramentas e os métodos de análise utilizados no estudo.

#### 3.1 Definição dos cenários de estudo

O Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE) usa o mesmo critério do Instituto Brasileiro de Geografia e Estatística (IBGE) no que se diz respeito ao número de funcionários para classificação do porte de uma determinada empresa, seja para fins bancários, ações de tecnologia, exportação ou outra aplicação qualquer. Esta diferenciação é representada na Figura 13.

**Figura 13 – Classificação do porte empresarial de acordo com o número de funcionários**

Categoria	Porte	Número de funcionários
Indústria	Micro	até 19
	Pequena	20 a 99
	Média	100 a 499
	Grande	mais de 500
Serviço	Micro	até 9
	Pequena	10 a 49
	Média	50 a 99
	Grande	mais de 100

Fonte: Elaborado pelo autor com base em SEBRAE (2015).

Com base nas definições acima citadas, três diferentes cenários reais serão utilizados para este estudo. Para garantir o sigilo das informações, os nomes das três empresas analisadas serão substituídos respectivamente por Empresa 1, Empresa 2 e Empresa 3.

Para facilitar a descrição de cada ambiente, os mesmos serão esquematicamente dispostos em uma grade, representada pela Tabela 3.

**Tabela 3 – Características dos ambientes de estudo**

Características	Empresa 1	Empresa 2	Empresa 3
Porte	Pequeno	Médio	Grande
Área de atuação	Escritório de contabilidade	Transporte de cargas	Instituto de educação
Localidade	Caxias do Sul - RS	São Leopoldo - RS	Osório - RS
Número de funcionários (aproximadamente)	21	92	110 + 700
Número de dispositivos gerenciados pelo UTM (aproximadamente)	35	138	880
Número de filiais	N/A	5	N/A
Métodos de interconexão	N/A	MPLS	N/A

Fonte: Elaborado pelo autor.

### 3.2 Justificativa da solução escolhida

Por se tratarem de ferramentas deveras complexas e robustas, os equipamentos UTM possuem um valor significativamente elevado para a utilização aplicada unicamente a estudos. Em virtude desta característica, para viabilizar a realização deste trabalho, foi realizada uma parceria com uma empresa lajeadense especializada como provedora de serviços gerenciados de segurança (*Managed Security Services Provider - MSSP*).

A empresa em questão trabalha exclusivamente com *appliances* de *firewall* UTM *Dell SonicWALL* e, por este motivo, o estudo foi realizado com a utilização desta linha de produtos.

Para atender os três cenários de análise, é necessária a utilização de três diferentes equipamentos. As especificações técnicas de cada modelo são detalhadas na Tabela 4.

**Tabela 4 – Descrições técnicas dos dispositivos UTM**

<i>Appliance</i> UTM	Empresa 1	Empresa 2	Empresa 3
Modelo	<i>Dell SonicWALL</i> SOHO	<i>Dell SonicWALL</i> TZ 300	<i>Dell SonicWALL</i> NSA 3600

Número de interfaces	5 portas 10/100/1000	5 portas 10/100/1000	12 portas 10/100/1000
<i>Performance de firewall</i>	300 Mbps	750 Mbps	3,4 Gbps
<i>Performance UTM (IMIX)</i>	60 Mbps	200 Mbps	900 Gbps
Número máximo de VPNs	10	10	800
Número máximo de conexões	10000	50000	325000
Suporte à alta disponibilidade	Não suportado	Ativo/Passivo sem sincronismo de sessão	Ativo/Passivo com sincronismo de sessão

Fonte: Elaborado pelo autor.

### 3.3 Análise da implementação da ferramenta UTM

Para efetuar a instalação dos dispositivos, será realizada uma série de análises em cada ambiente de estudo. O resultado desses levantamentos determinará as etapas e estratégias adotadas para a implementação da ferramenta.

Há uma divisão dos cuidados necessários no que se diz respeito a sua ordem cronológica. Essa separação é explanada nas subseções a seguir.

#### 3.3.1 Pré-instalação

- Análise das regras de negócio - definição dos setores críticos, bem como o entendimento dos acessos essenciais às atividades da corporação.
- Análise das regras de *firewall* - levantamento das regras (ACLs) já existentes e reestruturação de controles de acessos.
- Análise das regras de roteamento - mapeamento das regras de roteamento internas (entre as redes corporativas) e externas (saídas fixadas por um determinado *link* de *internet*, na existência de múltiplas opções).

### 3.3.2 Instalação

- Definição das regras de navegação - levantamento e determinação dos diferentes níveis de acesso à *Internet* (por setores ou cargos).
- Análise das exceções às regras - levantamento dos possíveis pontos que não estarão sob o controle do dispositivo UTM (servidores ou serviços específicos).

### 3.3.3 Pós-instalação

- Análise dos registros de *log* - monitoramento dos eventos gerados nos registros de *log* para detecção de possíveis pontos não percebidos durante a implementação da ferramenta.

## 3.4 Métodos de avaliação

A coleta dos dados e avaliação para o diagnóstico dos objetivos propostos baseiam-se na execução de duas diferentes linhas de pesquisa: análise comparativa e análise estatística. Há ainda um terceiro tipo de análise a ser realizado: trata-se da análise financeira, que busca determinar o tempo necessário para que o valor investido na solução seja completamente retornado.

### 3.4.1 Análise comparativa

Com a finalidade de mensurar o aumento do nível de segurança promovido pela implementação do dispositivo UTM, será realizada uma análise comparativa do inventário de vulnerabilidades presentes nas estruturas estudadas. Para gerar tal relacionamento, realizar-se-ão quatro testes em cada ambiente, dois deles antes da implementação da ferramenta UTM e dois depois. Para mapeamento das vulnerabilidades, será utilizado o *software Nessus*, da empresa *Tenable Network Security*, na sua versão 6.5.2.

- *Nessus* - é um *scanner* de vulnerabilidade de rede de código fechado (possui uma versão de demonstração) que usa a arquitetura *Common Vulnerabilities and Exposures* para facilitar a ligação cruzada entre as ferramentas de segurança compatíveis. Emprega a Linguagem de *Scripts* de Ataque *Nessus* (*Nessus Attack Scripting Language* - NASL), uma linguagem simples que descreve as ameaças individuais e potenciais ataques. Possui uma arquitetura modular, consistindo em

servidores centralizados que realizam varredura em clientes remotos, permitindo a interação do administrador (ROUSE, 2006).

Em cada etapa, serão realizados dois testes com a ferramenta *Nessus*. As coletas repetidas serão concatenadas. Após a obtenção das quatro amostras e da concatenação dos resultados, os dados serão comparados diretamente entre si.

Também se fará uso do programa *Dell SonicWALL Analyzer*, na sua versão 7.2, que coleta os arquivos de *syslog* dos dispositivos UTM e os sumariza em informações gerenciais e estratégicas, para gerar 30 (trinta) dias de relatórios das filtragens realizadas pelo antivírus de *gateway*.

É possível afirmar que o resultado gerado nestes processos se refere a um *benchmarking* entre o antes e o depois do quesito segurança de redes dos ambientes em estudo.

### **3.4.2 Análise estatística**

Com o intuito de obter a motivação primordial para a escolha de uma ferramenta UTM como solução de segurança (para cada diferente porte de empresa) será realizada uma pesquisa estatística com os gestores de TIC. A coleta de informações dar-se-á a partir de um formulário eletrônico (com o auxílio do *Google Docs*), contendo questões-chave para o entendimento dos fatores determinantes.

Além dos responsáveis pelos três ambientes estudados, para que a pesquisa tenha um número satisfatório de dados para análise, será novamente aproveitada a parceria com a MSSP lajeadense, pois o mesmo formulário será enviado a todo o seu portfólio de clientes. Desta forma, objetiva-se coletar um total mínimo de 100 (cem) amostras.

Após todos os dados serem computados em uma planilha eletrônica, serão processados e então dispostos em um gráfico demonstrativo em barras, que será utilizado para representar e visualizar o número de vezes que cada fator foi apontado. Serão construídos três gráficos, separados de acordo com o porte empresarial.

## **3.5 Análise financeira - Retorno sobre Investimento**

Segundo a Associação Brasileira de Marketing Direto (ABEMD), a pressão pela mensuração de resultados ante os investimentos realizados é crescente no mundo dos negócios de uma forma geral e, em especial, na comunicação e no marketing.

É possível afirmar que para o setor de TIC não é diferente. A justificativa de um investimento que visa melhorar a tecnologia de uma empresa (o que conseqüentemente



aumentará a sua competitividade) busca, antes de mais nada, medir a variável do *Return on Investment* (ROI).

Ainda de acordo com a ABEMD, o ROI define a relação entre quanto a empresa ganhou ou perdeu em relação a um determinado investimento.

Para a obtenção do ROI (em meses), para cada um dos três ambientes analisados, será utilizada a fórmula básica, conforme representada abaixo:

$$ROI = \frac{\textit{Quantia gasta com o investimento}}{\textit{Ganho obtido mensalmente}} \quad (1)$$

No caso dos três ambientes de estudo, o ganho obtido não será diretamente um aumento na receita da empresa, mas sim valores que deixam de ser perdidos (gastos) de maneira desnecessária.

A variável “ganho obtido mensalmente” será designada pelo somatório de inúmeros fatores particulares de cada cenário, tais como:

- Montante médio economizado pelo controle de navegação, baseado no valor-hora médio por funcionário, multiplicado pelo tempo médio gasto com conteúdos improdutivos.
- Montante médio economizado pela redundância VPN, baseado no valor médio perdido a cada hora de uma filial parada, devido às quedas do serviço de comunicação (*link*) MPLS.
- Montante médio economizado pela eficiência energética dos dispositivos UTM, além do montante economizado com inúmeros *hardwares* para prover as mesmas funções.
- Montante médio economizado pela utilização de comunicação VPN no lugar de circuitos MPLS.

Além desses fatores tangíveis, existem também os que são mais subjetivos, que sofrem maiores influências de externalidades, dificultando a sua inserção direta na variável “ganho obtido mensalmente”. O principal exemplo deste tipo de fator são os custos do vazamento não autorizado de informações críticas/estratégicas, que podem representar toda uma campanha de *marketing* (linha de produto), ou ainda ações judiciais de clientes ou fornecedores que possam vir a ser prejudicados.

## 4 RESULTADOS

Este capítulo destina-se à apresentação, explanação e discussão dos resultados oriundos das análises descritas anteriormente. Primeiro serão expostos os resultados coletados durante o processo de instalação da ferramenta UTM nos três ambientes de estudo. Após serão explanados os resultados do *benchmarking* das topologias antes e depois da implementação da solução UTM. Em seguida, serão apresentados os resultados do processo de obtenção dos fatores determinantes para a escolha de uma solução UTM nos diferentes portes empresariais. Por fim, será demonstrada a coleta do ROI de cada cenário analisado.

### 4.1 Implementação da ferramenta UTM

Os resultados obtidos a partir dos processos de instalação dos dispositivos UTM serão expostos separadamente, de acordo com o tamanho da infraestrutura envolvida.

Por questões de segurança, alguns octetos do endereçamento de IP externo foram substituídos pelo símbolo asterisco (\*), com o objetivo de manter anônima a identificação das empresas estudadas.

Para facilitar a tomada de decisão na etapa de parametrização das funcionalidades de filtragem de URL e de aplicação, em cada estrutura e por um período de 15 dias, foi mantido um dispositivo UTM configurado em modo *bridge* na borda externa à rede. Desta maneira, o equipamento não realizou qualquer tipo de bloqueio ou inspeção de pacote, apenas foi utilizado para coletar dados do tráfego de *Internet* (*sites* e aplicações).

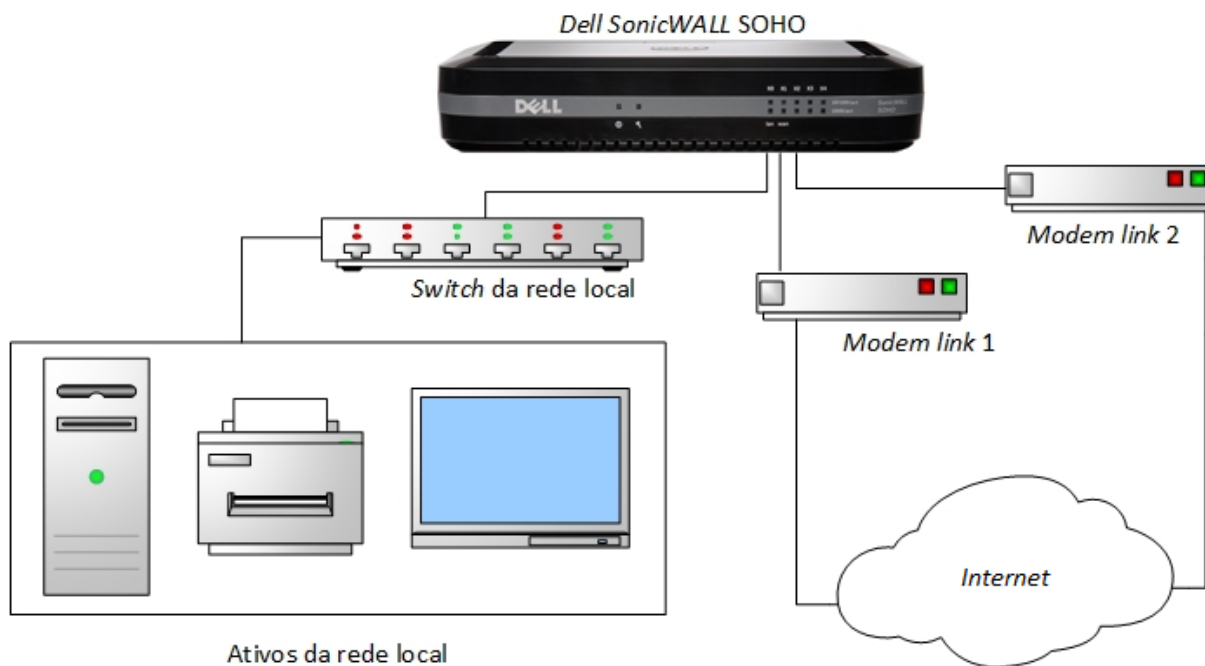
#### 4.1.1 Empresa 1 - Ambiente de pequeno porte

Por se tratar de uma estrutura reduzida, com poucos dispositivos e relativa simplicidade nas regras de negócio, o tempo compreendido para a instalação da ferramenta UTM foi de aproximadamente 1 (um) dia de trabalho, nos períodos da manhã e tarde, totalizando 8 (oito) horas de atividade.

Regras de negócio e exigências do coordenador de TIC: continuidade das atividades em situações de queda de um circuito de *Internet*; filtragem de conteúdo não produtivo (redes sociais, jogos, pornografia, entre outros); filtragem privilegiada para dispositivos de gerentes; acesso remoto aos servidores corporativos.

A Figura 14 representa a organização da rede na Empresa 1.

**Figura 14 – Estrutura organizacional de rede da Empresa 1**



Fonte: Elaborado pelo autor.

A partir das análises elencadas no item 3.3 do capítulo anterior, foram obtidas as seguintes etapas de execução:

- Configuração das interfaces do *appliance* - o dispositivo *Dell SonicWALL SOHO* foi configurado, em uma de suas interfaces (x0), com endereço IP 192.168.0.254 (máscara 255.255.255.0), sendo também designado como *gateway* desta faixa LAN. À próxima interface (x1) atribuiu-se os parâmetros de autenticação *Point-to-Point Protocol over Ethernet (PPPoE)*, que, por sua vez, recebeu o endereço IP 179.\*.114.\*. A placa de rede x2 foi parametrizada por *Dynamic Host Configuration Protocol (DHCP)*, onde obteve o endereço IP 177.\*.51.\*.
- Publicações (acessos externos) - foram criadas as *Network Address Translation (NATs)*, bem como as *ACLs* necessárias ao funcionamento externo do servidor de *Terminal Service* e do de gerenciamento de câmeras. As mesmas são mostradas na Tabela 5.

**Tabela 5 – NATs criadas na Empresa 1**

Origem	Destino externo	Destino Interno	Serviços (portas) externas	Serviços (portas) internas
Qualquer	179.*.114.*	192.168.0.100	TCP 3389	TCP 3389

---

Qualquer	179.*.114.*	192.168.0.108	TCP 37777	TCP 37777
----------	-------------	---------------	-----------	-----------

---

Fonte: Elaborado pelo autor.

- Regras de ACL - não foram realizadas configurações em nível de *firewall*. Manteve-se, por padrão, todas as portas liberadas de dentro para fora da rede. As regras de fora para dentro (WAN --> LAN) estão descritas no tópico anterior.
- Regras de roteamento - a infraestrutura possui apenas uma rede, não se fazendo necessária a configuração de quaisquer regras de roteamento. Apenas foi ativo o algoritmo de *failover* nos *links* de *Internet*, sendo que a saída principal ficou a da interface x1.
- Filtragem de URL - foram estipulados dois níveis de acesso à *Internet*: nível básico e nível privilegiado. O nível básico, no qual a grande maioria dos funcionários está associada, possui maior restrição nos acessos *web*. O nível privilegiado foi reservado para o servidor principal (ERP) e para os dispositivos utilizados pelos gerentes da empresa (PCs, *notebooks*, *tablets*, *smartphones* e afins). As Figuras 15 e 16 explanam, respectivamente, os níveis de acesso básico e privilegiado, de acordo com as categorias permitidas em cada um deles. Adicionalmente às categorias, criou-se uma lista de *sites* manualmente permitidos e negados.

**Figura 15 – Nível de acesso básico à Internet na Empresa 1**

**Select Forbidden Categories**

[Select all Categories](#)

<input checked="" type="checkbox"/> 1. Violence/Hate/Racism	<input type="checkbox"/> 23. Government	<input type="checkbox"/> 45. Travel
<input checked="" type="checkbox"/> 2. Intimate Apparel/Swimsuit	<input type="checkbox"/> 24. Military	<input type="checkbox"/> 46. Vehicles
<input checked="" type="checkbox"/> 3. Nudism	<input type="checkbox"/> 25. Political/Advocacy Groups	<input checked="" type="checkbox"/> 47. Humor/Jokes
<input checked="" type="checkbox"/> 4. Pornography	<input type="checkbox"/> 26. Health	<input type="checkbox"/> 48. Multimedia
<input checked="" type="checkbox"/> 5. Weapons	<input type="checkbox"/> 27. Information Technology/Computers	<input type="checkbox"/> 49. Freeware/Software Downloads
<input checked="" type="checkbox"/> 6. Adult/Mature Content	<input checked="" type="checkbox"/> 28. Hacking/Proxy Avoidance Systems	<input type="checkbox"/> 50. Pay to Surf Sites
<input checked="" type="checkbox"/> 7. Cult/Occult	<input type="checkbox"/> 29. Search Engines and Portals	<input type="checkbox"/> 51. N/A
<input checked="" type="checkbox"/> 8. Drugs/Illegal Drugs	<input checked="" type="checkbox"/> 30. E-Mail	<input type="checkbox"/> 52. N/A
<input checked="" type="checkbox"/> 9. Illegal Skills/Questionable Skills	<input checked="" type="checkbox"/> 31. Web Communications	<input type="checkbox"/> 53. Kid Friendly
<input checked="" type="checkbox"/> 10. Sex Education	<input type="checkbox"/> 32. Job Search	<input type="checkbox"/> 54. Advertisement
<input checked="" type="checkbox"/> 11. Gambling	<input type="checkbox"/> 33. News and Media	<input type="checkbox"/> 55. Web Hosting
<input checked="" type="checkbox"/> 12. Alcohol/Tobacco	<input type="checkbox"/> 34. Personals and Dating	<input type="checkbox"/> 56. Other
<input type="checkbox"/> 13. Chat/Instant Messaging (IM)	<input type="checkbox"/> 35. Usenet News Groups	<input type="checkbox"/> 57. Internet Watch Foundation CAIC
<input type="checkbox"/> 14. Arts/Entertainment	<input type="checkbox"/> 36. Reference	<input checked="" type="checkbox"/> 58. Social Networking
<input type="checkbox"/> 15. Business and Economy	<input type="checkbox"/> 37. Religion	<input checked="" type="checkbox"/> 59. Malware
<input type="checkbox"/> 16. Abortion/Advocacy Groups	<input type="checkbox"/> 38. Shopping	<input type="checkbox"/> 60. N/A
<input type="checkbox"/> 17. Education	<input type="checkbox"/> 39. Internet Auctions	<input type="checkbox"/> 61. N/A
<input type="checkbox"/> 18. N/A	<input type="checkbox"/> 40. Real Estate	<input type="checkbox"/> 62. N/A
<input type="checkbox"/> 19. Cultural Institutions	<input checked="" type="checkbox"/> 41. Society and Lifestyle	<input type="checkbox"/> 63. N/A
<input type="checkbox"/> 20. Online Banking	<input checked="" type="checkbox"/> 42. Gay and Lesbian Issues	<input type="checkbox"/> 64. Not Rated
<input type="checkbox"/> 21. Online Brokerage and Trading	<input type="checkbox"/> 43. Restaurants and Dining	
<input checked="" type="checkbox"/> 22. Games	<input type="checkbox"/> 44. Sports/Recreation	

Fonte: Elaborado pelo autor.

**Figura 16 – Nível de acesso privilegiado à Internet na Empresa 1**

**Select Forbidden Categories**

[Select all Categories](#)

<input type="checkbox"/> 1. Violence/Hate/Racism	<input type="checkbox"/> 23. Government	<input type="checkbox"/> 45. Travel
<input type="checkbox"/> 2. Intimate Apparel/Swimsuit	<input type="checkbox"/> 24. Military	<input type="checkbox"/> 46. Vehicles
<input checked="" type="checkbox"/> 3. Nudism	<input type="checkbox"/> 25. Political/Advocacy Groups	<input type="checkbox"/> 47. Humor/Jokes
<input checked="" type="checkbox"/> 4. Pornography	<input type="checkbox"/> 26. Health	<input type="checkbox"/> 48. Multimedia
<input type="checkbox"/> 5. Weapons	<input type="checkbox"/> 27. Information Technology/Computers	<input type="checkbox"/> 49. Freeware/Software Downloads
<input type="checkbox"/> 6. Adult/Mature Content	<input checked="" type="checkbox"/> 28. Hacking/Proxy Avoidance Systems	<input type="checkbox"/> 50. Pay to Surf Sites
<input type="checkbox"/> 7. Cult/Occult	<input type="checkbox"/> 29. Search Engines and Portals	<input type="checkbox"/> 51. N/A
<input type="checkbox"/> 8. Drugs/Illegal Drugs	<input type="checkbox"/> 30. E-Mail	<input type="checkbox"/> 52. N/A
<input type="checkbox"/> 9. Illegal Skills/Questionable Skills	<input type="checkbox"/> 31. Web Communications	<input type="checkbox"/> 53. Kid Friendly
<input checked="" type="checkbox"/> 10. Sex Education	<input type="checkbox"/> 32. Job Search	<input type="checkbox"/> 54. Advertisement
<input type="checkbox"/> 11. Gambling	<input type="checkbox"/> 33. News and Media	<input type="checkbox"/> 55. Web Hosting
<input type="checkbox"/> 12. Alcohol/Tobacco	<input type="checkbox"/> 34. Personals and Dating	<input type="checkbox"/> 56. Other
<input type="checkbox"/> 13. Chat/Instant Messaging (IM)	<input type="checkbox"/> 35. Usenet News Groups	<input type="checkbox"/> 57. Internet Watch Foundation CAIC
<input type="checkbox"/> 14. Arts/Entertainment	<input type="checkbox"/> 36. Reference	<input type="checkbox"/> 58. Social Networking
<input type="checkbox"/> 15. Business and Economy	<input type="checkbox"/> 37. Religion	<input checked="" type="checkbox"/> 59. Malware
<input type="checkbox"/> 16. Abortion/Advocacy Groups	<input type="checkbox"/> 38. Shopping	<input type="checkbox"/> 60. N/A
<input type="checkbox"/> 17. Education	<input type="checkbox"/> 39. Internet Auctions	<input type="checkbox"/> 61. N/A
<input type="checkbox"/> 18. N/A	<input type="checkbox"/> 40. Real Estate	<input type="checkbox"/> 62. N/A
<input type="checkbox"/> 19. Cultural Institutions	<input type="checkbox"/> 41. Society and Lifestyle	<input type="checkbox"/> 63. N/A
<input type="checkbox"/> 20. Online Banking	<input checked="" type="checkbox"/> 42. Gay and Lesbian Issues	<input type="checkbox"/> 64. Not Rated
<input type="checkbox"/> 21. Online Brokerage and Trading	<input type="checkbox"/> 43. Restaurants and Dining	
<input type="checkbox"/> 22. Games	<input type="checkbox"/> 44. Sports/Recreation	

Fonte: Elaborado pelo autor.

- Filtragem de aplicação - os bloqueios ativos na camada de aplicação (*layer 7* do modelo OSI) restringem-se às ferramentas de redes sociais, *softwares* de *download Peer-to-Peer* (P2P) e comunicadores instantâneos. Para a filtragem de aplicação também foi mantida a liberação dos equipamentos da gerência.

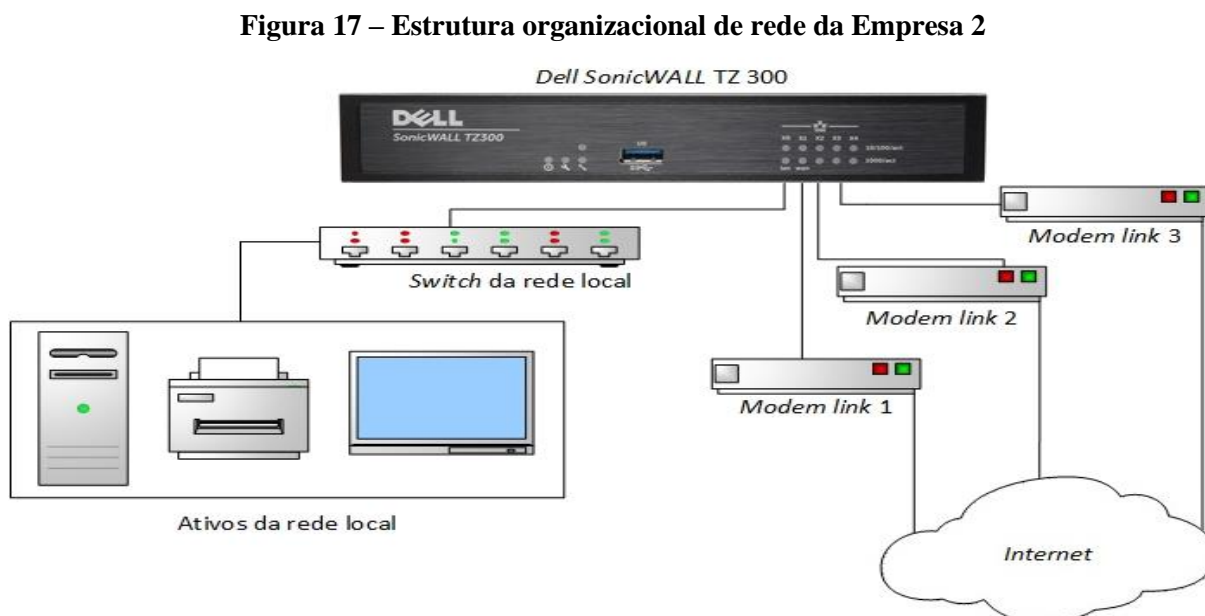
- Segurança de borda - neste ponto foram ativados, de maneira intercalada, os recursos de antivírus e *antispyware* de *gateway*, além dos sistemas de IDS/IPS.
- Monitoramento do arquivo de *logs* - após a conclusão de todas as configurações, realizou-se, por aproximadamente uma hora, a auditoria dos registros de *log*. Nenhum evento indesejado foi registrado, tal como: bloqueios indevidos, ações de falso/positivo nos mecanismos de segurança, acessos não autorizados ou lentidões na conexão geral da rede.

#### 4.1.2 Empresa 2 - Ambiente de médio porte

Em virtude de ser uma estrutura intermediária, com um considerável número de dispositivos e relativa complexidade nas regras de negócio, o tempo compreendido para a instalação da ferramenta UTM foi de aproximadamente 4 (quatro) dias de trabalho, nos períodos da manhã e tarde, totalizando 32 (trinta e duas) horas de atividade.

Regras de negócio e exigências do coordenador de TIC: alta disponibilidade para o servidor de ERP e DNS; gerência facilitada dos privilégios de acesso à *Internet* com a utilização da plataforma *Microsoft Active Directory* (AD); redundância automática dos circuitos de *Internet*; autenticação dos usuários via portal *web*; intercomunicação e navegação das filiais a partir da unidade matriz por meio de VPN IPsec; filtragem de conteúdo *web* em diferentes níveis.

A Figura 17 contextualiza a organização de rede na Empresa 2.



Fonte: Elaborado pelo autor.

A partir das análises elencadas no item 3.3 do capítulo anterior, foram obtidas as seguintes etapas de execução:

- Configuração das interfaces do *appliance* - ao dispositivo *Dell SonicWALL TZ 300* da unidade matriz foi atribuído, em sua interface x0, o endereço IP 192.168.0.1 (máscara 255.255.255.0), que por sua vez foi definido como *gateway* desta faixa LAN. A interface seguinte (x1) foi configurada com o endereço IP 200.\*.219.\* (máscara 255.255.255.248). Na sequência, a interface x2 foi parametrizada com o endereço IP 177.\*.253.\* (máscara 255.255.255.248). Por fim, a interface x3 recebeu o endereço IP 177.\*.212.\* (também com a máscara 255.255.255.248).
- Publicações (acessos externos) - foram configuradas as NATs e as ACLs exigidas para o funcionamento externo dos servidores de ERP, banco de dados e DNS. Para aumentar a disponibilidade do servidor ERP, o mesmo foi publicado a partir de dois circuitos distintos de *Internet*. Tais regras são esquematizadas na Tabela 6.

**Tabela 6 – NATs criadas na Empresa 2**

Origem	Destino externo	Destino Interno	Serviços (portas) externas	Serviços (portas) internas
Qualquer	177.*.212.*	192.168.0.7	TCP 6080	TCP 6080
Qualquer	177.*.212.*	192.168.0.7	UDP 9000	UDP 9000
Qualquer	177.*.212.*	192.168.0.7	UDP 9001	UDP 9001
Qualquer	200.*.219.*	192.168.0.7	TCP 6080	TCP 6080
Qualquer	200.*.219.*	192.168.0.7	UDP 9000	UDP 9000
Qualquer	200.*.219.*	192.168.0.7	UDP 9001	UDP 9001
Qualquer	200.*.219.*	192.168.0.15	TCP 10050	TCP 10050
Qualquer	200.*.219.*	192.168.0.15	TCP 10051	TCP 10051
Qualquer	200.*.219.*	192.168.0.15	TCP 5432	TCP 5432
Qualquer	200.*.219.*	192.168.0.18	TCP 8091	TCP 80
Qualquer	177.*.212.*	192.168.0.20	TCP e UDP 53	TCP e UDP 53
Qualquer	200.*.219.*	192.168.0.20	TCP e UDP 53	TCP e UDP 53
Qualquer	200.*.219.*	192.168.0.22	TCP 1433	TCP 1433



Fonte: Elaborado pelo autor.

- Regras de ACL - não foram realizadas configurações em nível de *firewall*. Manteve-se, por padrão, todas as portas liberadas de dentro para fora da rede. As regras de fora para dentro estão descritas no tópico anterior.
- Regras de roteamento - não foram necessárias regras de roteamento intra-rede, pois a topologia comportava apenas uma faixa de endereçamento LAN. Ativou-se o algoritmo de *failover* nos *links* de *Internet*, onde o *link* da interface x2 foi atribuído como principal, o da interface x3 como secundário e o da interface x1 como terciário. Por exigências de funcionamento e performance, foi criada uma rota de saída (que é automaticamente desativada em caso de falha do circuito) para que o servidor de ERP utilize o *link* da interface x3. Tal rota é representada na Figura 18.

**Figura 18 – Rotas criadas na Empresa 2**

Route Policies

View Style:  All Policies  Custom Policies  Default Policies

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
1	U_SRVRAS01	Any	Any	X3 Default Gateway	X3	100	19			 

Fonte: Elaborado pelo autor.

- Criação de usuários e grupos de acesso - Para maior escalabilidade e controle dos acessos *web*, a ferramenta UTM foi integrada à plataforma *Microsoft Active Directory* (AD), na qual foram criados três grupos: “G\_ACESSO-LIBERADO”, “G\_ACESSO-RESTRITO” e o “TI”. A identificação dos usuários é feita a partir de um *Captive Portal* diretamente no console do *appliance* que realiza a *query* de autenticação na base AD. A Figura 19 ilustra os grupos padrões do dispositivo, juntamente com os grupos importados do AD.



Figura 19 – Grupos de acesso da Empresa 2

#	Name	CFS Policy	Guest Services	Admin	VPN Access	Configure
1	Everyone					
2	Guest Services		✓			
3	Trusted Users					
4	Content Filtering Bypass	Filters bypassed				
5	Limited Administrators			Ltd.		
6	SonicWALL Administrators			Full		
7	SonicWALL Read-Only Admins			Rd-Only		
8	SSLVPN Services					
9	G_ACESSO-LIBERADO					
10	G_ACESSO-RESTRITO					
11	TI					

Fonte: Elaborado pelo autor.

- Filtragem de URL - em cumprimento à solicitação do gestor de TIC, houve a definição de três níveis de acesso à *Internet*: o nível restrito (associado ao grupo “G\_ACESSO-RESTRITO” - usuários em geral), o nível liberado (associado ao grupo “G\_ACESSO-LIBERADO” - usuários de gestores e supervisores) e o nível TI (associado ao grupo “TI” - destinado à utilização pela equipe de informática). A faixa de endereçamento IP compreendida entre 192.168.0.1 e 192.168.0.30 (utilizada exclusivamente por servidores) também foi associada à política “TI”. Também se fez uso de uma lista (global) branca e negra de *sites*.
- Filtragem de aplicação - o bloqueio na camada 7 foi ativado para jogos, comunicadores instantâneos, redes sociais, ferramentas multimídia (*streaming* de áudio e vídeo), P2P e aplicativos *mobile*. Somente os servidores foram mantidos fora deste filtro.
- Segurança de borda - a ativação das funcionalidades de IDS/IPS, *gateway* antivírus e *antispyware* deu-se de maneira escalonada, com constante análise dos arquivos de *logs*, a fim de diagnosticar algum bloqueio indesejado nas atividades da rede. Foram detectadas três estações de trabalho contaminadas por um *trojan* que representavam uma ameaça à segurança da rede. Tais dispositivos foram isolados para posterior formatação.

- Monitoramento do arquivo de *logs* - após o término da implementação da ferramenta UTM, realizou-se o acompanhamento do arquivo de *logs* por cerca de quatro horas. Nenhum evento anômalo foi registrado.
- Unidades filiais - para as unidades filiais foram configurados cinco equipamentos *Dell SonicWALL SOHO* com suas respectivas interfaces x0 nos endereços IP 192.168.20.1, 192.168.21.1, 192.168.22.1, 192.168.23.1, 192.168.24.1. As interfaces x1 e x2 foram todas configuradas por DHCP, pois os circuitos de *Internet* utilizados possuem endereço IP dinâmico. Configurou-se também uma VPN IPSec (redundante pelos dois links), designada para a intercomunicação das redes e para rotear o tráfego *web* das filiais pelo nó matriz, objetivando a centralização dos controles de navegação e a remoção do circuito MPLS.

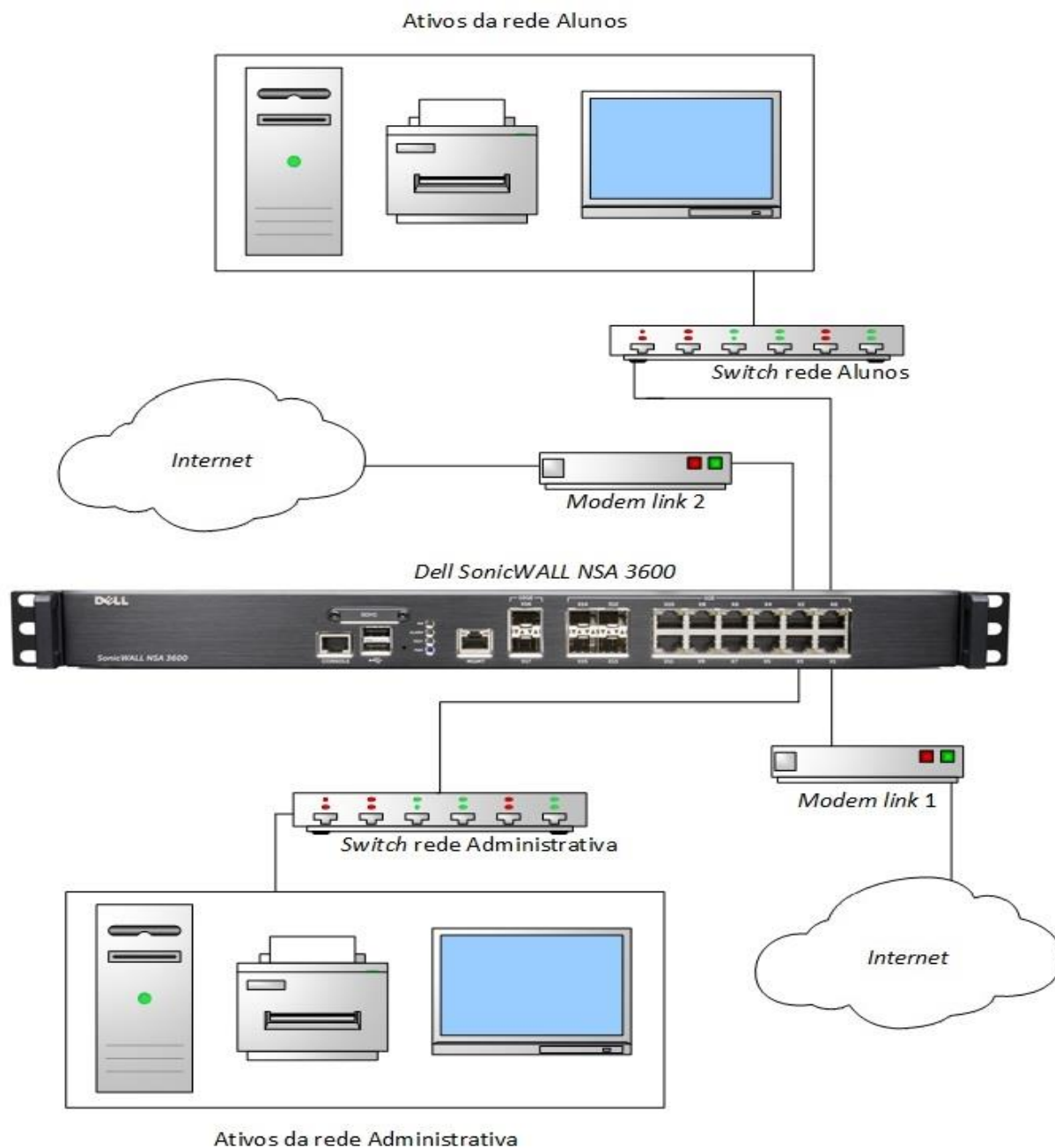
#### **4.1.3 Empresa 3 - Ambiente de grande porte**

Em decorrência do elevado grau de complexidade da estrutura de rede e das regras de negócio, aliados ao alto número de dispositivos, o tempo necessário para realizar a instalação de toda a solução UTM tratou-se de, aproximadamente, 7 (sete) dias de atividade, nos períodos de manhã e tarde, em um total de 56 (cinquenta e seis) horas.

Regras de negócio e exigências do coordenador de TIC: integração com múltiplos servidores controladores de domínio; gerenciamento do consumo de banda por servidores críticos (antivírus e atualizações de *Windows*); balanceamento automático entre os circuitos de *Internet* em situações de pico de utilização; controle de acesso entre a rede de alunos e a rede administrativa; autenticação de usuários via portal *web* para a rede alunos; autenticação automática de usuários para a rede administrativa; controle de acesso à *Internet* em múltiplos níveis; funcionamento independente dos recursos de proteção de borda (IDS/IPS, *gateway* antivírus e *antispyware*) para a rede alunos e administrativa; bloqueio de usuários facilitado.

A Figura 20 ilustra a organização da rede na Empresa 3.

**Figura 20 – Estrutura organizacional de rede da Empresa 3**



Fonte: Elaborado pelo autor.

A partir das análises elencadas no item 3.3 do capítulo anterior, foram obtidas as seguintes etapas de execução:

- Configuração das interfaces do *appliance* - o UTM *Dell SonicWALL NSA 3600* foi parametrizado, em sua interface x0, com o endereço de IP 10.1.0.10 (máscara 255.255.240.0) e foi atribuído como *gateway* da rede de alunos (LAN). A interface x1 foi definida com o endereço de IP 200.\*.227.\* (máscara 255.255.255.240). Em seguida, a interface x2 recebeu o endereço de IP 177.\*.3.\* a partir das configurações

de autenticação PPPoE. A próxima interface (x3) foi designada como *gateway* da rede administrativa (ADM) e obteve o endereçamento de IP 192.168.1.254 (máscara 255.255.252.0). A Figura 21 ilustra as configurações das quatro interfaces utilizadas.

**Figura 21 – Interfaces de rede da Empresa 3**

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		10.1.0.10	255.255.240.0	Static	1 Gbps Full Duplex	Alunos	
X1	WAN	Default LB Group	200.*.227.*	255.255.255.240	Static	1 Gbps Full Duplex	Embratel 20Mbps	
X2	WAN	Default LB Group	177.*.3.*	255.255.255.0	PPPoE	100 Mbps Full Duplex	INB 10Mbps	
X3	ADM		192.168.1.254	255.255.252.0	Static	1 Gbps Full Duplex		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X5	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		

Fonte: Elaborado pelo autor.

- Publicações (acessos externos) - foram configuradas as NATs e as ACLs exigidas para o funcionamento externo dos servidores de banco de dados, *web* e *Terminal Services*. As referidas regras estão apresentadas na Tabela 7.

**Tabela 7 – NATs criadas na Empresa 3**

Origem	Destino externo	Destino Interno	Serviços (portas) externas	Serviços (portas) internas
Qualquer	200.*.227.*	10.1.0.2	TCP 4005	TCP 3389
Qualquer	177.*.3.*	10.1.0.2	TCP 4005	TCP 3389
Qualquer	200.*.227.*	10.1.0.2	TCP 3000	TCP 3000
Qualquer	200.*.227.*	192.168.0.6	TCP 5000	TCP 80
Qualquer	177.*.3.*	192.168.0.7	TCP 80	TCP 80
Qualquer	200.*.227.*	192.168.0.22	TCP 5010	TCP 5432
Qualquer	200.*.227.*	192.168.1.6	TCP 4015	TCP 3389
Qualquer	200.*.227.*	192.168.1.8	TCP 4002	TCP 3389
Qualquer	200.*.227.*	192.168.1.202	TCP 8181	TCP 8181
Qualquer	200.*.227.*	192.168.1.234	TCP 80	TCP 80
Qualquer	200.*.227.*	192.168.1.234	TCP 81	TCP 81

Fonte: Elaborado pelo autor.

- Regras de ACL - Além das regras de ACL necessárias à publicação dos servidores anteriormente elencados, também foram criadas ACLs que liberam todas as portas da rede alunos (LAN) para a *Internet* (WAN), bem como da rede administrativa (ADM) para WAN. A intercomunicação entre a rede de alunos e administrativa foi completamente bloqueada, ficando restrita apenas ao serviço de DNS e a sincronização entre os servidores de AD. Além da regra que libera todas as portas da rede administrativa para a *Internet*, também criou-se uma regra destinada ao controle de banda dos servidores de antivírus e atualizações de *Windows* (WSUS), na qual, durante o período de expediente, a utilização máxima que estes dispositivos podem ter é de 3 Mbps do circuito de *Internet*. As ACLs da rede alunos para a rede administrativa e as da rede administrativa para a *Internet* estão dispostas, respectivamente, nas Figuras 22 e 23.

**Figura 22 – ACLs da rede alunos para rede administrativa na Empresa 3**

Firewall / Access Rules

Restore Defaults...

Access Rules (LAN > ADM)

View Style:  All Rules  Matrix  Drop-down Boxes

Add... Delete

#	From	To	Priority	Source	Destination	Service	Action	Users Ind.	Users Excl.	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable	Configure
<input type="checkbox"/> 1	LAN	>	ADM	1	Any	Any	DNS (Name Service)	Allow	All	None					<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2	LAN	>	ADM	2	INT-10.1.0.2-AD-ALLUNOS	INT-192.168.1.192-AD-ADM	Any	Allow	All	None					<input checked="" type="checkbox"/>	
<input type="checkbox"/> 3	LAN	>	ADM	3	INT-10.1.0.2-AD-ALLUNOS	INT-192.168.1.191-AD-ADM	Any	Allow	All	None					<input checked="" type="checkbox"/>	
<input type="checkbox"/> 4	LAN	>	ADM	4	Any	Any	Any	Deny	All	None					<input checked="" type="checkbox"/>	

Add... Delete

Clear Statistics Restore Defaults...

Fonte: Elaborado pelo autor.

**Figura 23 – ACLs da rede administrativa para *Internet* na Empresa 3**

Firewall / Access Rules

Restore Defaults...

Access Rules (ADM > WAN)

View Style:  All Rules  Matrix  Drop-down Boxes

Add... Delete

#	From	To	Priority	Source	Destination	Service	Action	Users Ind.	Users Excl.	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable	Configure
<input type="checkbox"/> 1	ADM	>	WAN	1	Servidores	Any	Any	Allow	All	None					<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2	ADM	>	WAN	2	Any	Any	Any	Allow	All	None					<input checked="" type="checkbox"/>	

Add... Delete

Clear Statistics Restore Defaults...

**Schedule**  
Servidores-Preferencia

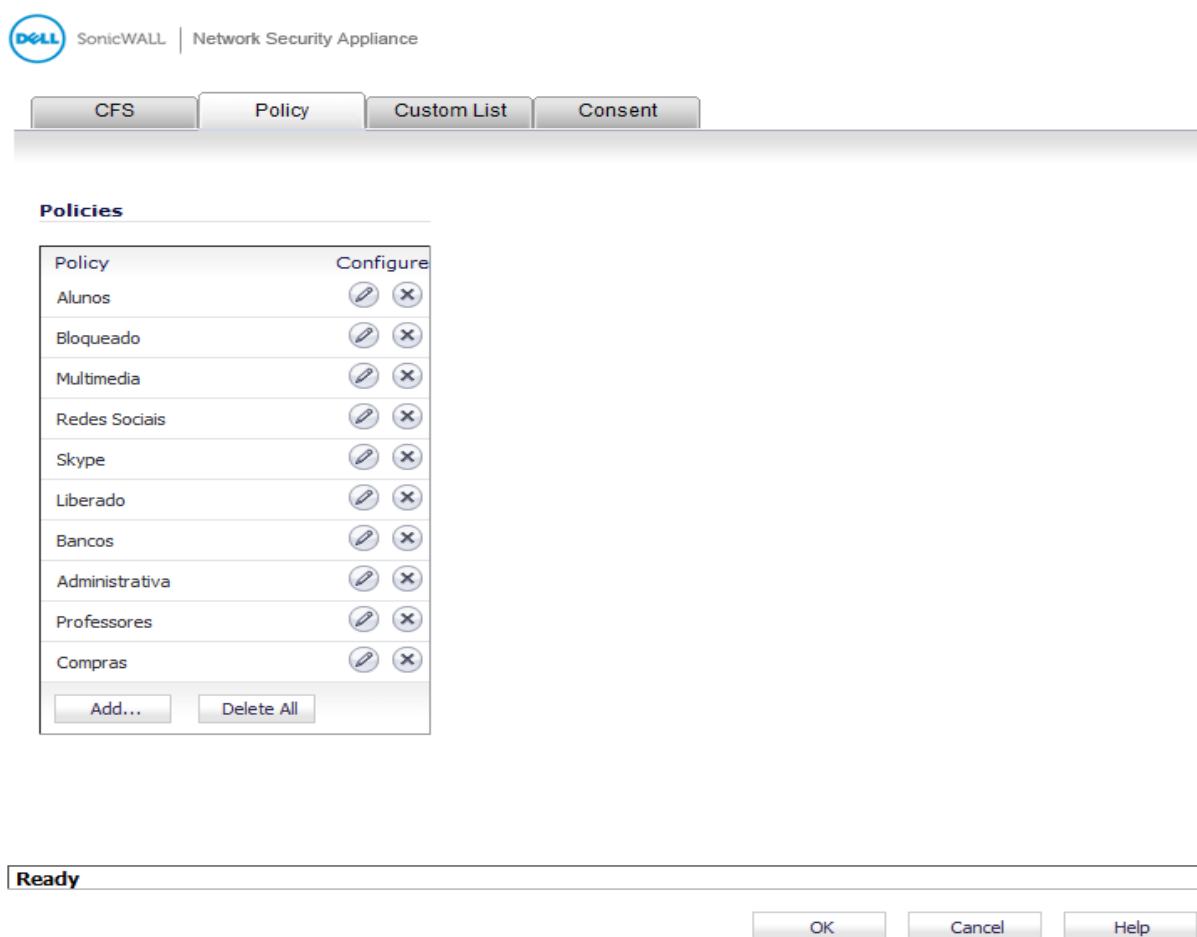
- M-T-W-TH-F 00:00 to 08:00
- M-T-W-TH-F 12:00 to 13:00
- M-T-W-TH-F 23:00 to 24:00
- S 00:00 to 08:00
- S 17:00 to 24:00
- SU 00:00 to 24:00

Fonte: Elaborado pelo autor.

- Regras de roteamento - as regras de roteamento para intercomunicação das redes alunos e administrativa são padrões entre as interfaces do *appliance*, porém respeitando as políticas estabelecidas nas regras de acesso (ALC). Foi ativado o algoritmo de balanceamento de carga *spillover*, que se caracteriza pela função de transbordo. Todo o tráfego é destinado ao *link* da interface x1 até que este atinja a marca de 15 Mbps de utilização. A partir deste ponto, o tráfego é balanceado para o *link* da interface x2. A faixa de endereços IP destinada ao setor de TI (192.168.1.1 até 192.168.1.20) foi fixada para sempre utilizar o *link* da interface x2. Os servidores endereçados entre os IPs 192.168.0.1 e 192.168.0.254 sempre utilizarão o circuito da interface x1 (salvo a exceção de queda no *link*), mesmo quando o algoritmo de *spillover* transbordar o restante do tráfego pelo circuito x2.
- Criação de usuários e grupos de acesso - a ferramenta UTM foi integrada a dois distintos servidores de AD, um situado na rede alunos e outro na rede administrativa, cada um em um domínio diferente. Na rede alunos, ativou-se a funcionalidade de *Captive Portal* para realizar a autenticação dos usuários. Já para a rede administrativa, optou-se pela instalação de um *software* (diretamente no servidor de AD), para identificar automaticamente o usuário que está utilizando determinada estação, de acordo com os registros de autenticação no controlador de domínio. A partir deste ponto, criaram-se nove diferentes grupos para gerência do tráfego *web*: "SW\_Alunos", "SW\_Bloqueado", "SW\_Multimedia", "SW\_Redes\_Sociais", "SW\_Skype", "SW\_Liberado", "SW\_Banking", "SW\_Administrativa" e "SW\_Professores".
- Filtragem de URL e aplicação - as funcionalidades de controle *web* e de aplicação foram associadas aos nove grupos importados do AD. Conteúdos de multimídia, redes sociais e comunicadores instantâneos foram liberados respectivamente para os grupos "SW\_Multimedia", "SW\_Redes\_Sociais" e "SW\_Skype". Somente os usuários membros do grupo "SW\_Banking" receberam privilégio de acesso a *sites*/aplicações de pagamentos *online*, bancos e instituições financeiras. As redes alunos e administrativa tiveram seus acessos básicos diferenciados, cada qual com um nível distinto de permissão, que, por sua vez, ficaram associados aos grupos "SW\_Alunos" e "SW\_Administrativa". Os professores possuem o mesmo nível de acesso dos alunos, porém com permissão de acesso a *sites* e aplicações de jogos e conteúdos de educação sexual. Os servidores em geral e os usuários do grupo "SW\_Liberados" (departamento de TI, diretor e supervisores) foram associados à

uma política de acesso totalmente liberada. Por fim, negou-se completamente o acesso à *Internet* para os membros do grupo “SW\_Bloqueado”. Aplicações de atualizações de software, jogos e P2P foram bloqueadas para todos os usuários (alunos e administrativa). Já a negação de aplicativos *mobile* foi ativada apenas para a rede administrativa. A Figura 24 expõe as diferentes políticas de acesso criadas na Empresa 3. Alguns *sites* foram manualmente cadastrados em uma lista de permitidos e outra de negados, que por sua vez foram associadas a todos os diferentes níveis de acesso.

**Figura 24 – Políticas de acesso da Empresa 3**



Fonte: Elaborado pelo autor.

- Segurança de borda - ativou-se as funcionalidades de controle de borda (IDS/IPS, *gateway* antivírus e *antispyware*) apenas na rede alunos e nos servidores de AD da rede administrativa. Tal ativação se deu de forma escalonada com constante análise dos arquivos de *logs*.

- Monitoramento do arquivo de *logs* - o último dia de instalação ficou todo dedicado ao acompanhamento do arquivo de *logs*. Nesta etapa detectou-se que o servidor de WSUS não estava conseguindo identificar as atualizações disponíveis, pois estava sendo barrado pela filtragem de aplicações. Optou-se então pela exclusão do endereço IP do servidor do filtro *layer 7*.

## 4.2 Comparativo entre os ambientes antes e após a implantação da ferramenta UTM

Para realizar o mapeamento dos serviços publicados (*port scan*) em cada ambiente, se utilizou a ferramenta *Nessus*. O *software* possui uma versão gratuita (é necessário apenas realizar um cadastro *online* na página do fabricante), que comporta as funcionalidades necessárias para o teste.

A aplicação foi parametrizada para mapear todas as portas TCP (1-65535) na faixa de endereçamento IP externo que mais possuía serviços publicados em cada topologia.

As duas capturas realizadas em cada estrutura (antes da ferramenta UTM) obtiveram exatamente o mesmo resultado. Desta forma, se registrou apenas uma amostra por empresa. Além das portas publicadas, também foi possível mapear que os endereços externos respondiam ao teste básico de *ping*. As Figuras 25, 26 e 27 ilustram, respectivamente, as coletas citadas.

**Figura 25 – Portas mapeadas antes da ferramenta UTM na Empresa 1**

Severity	Plugin Name	Plugin Family	Count
INFO	Nessus SYN scanner	Port scanners	2
INFO	Ping the remote host	Port scanners	1

Fonte: Elaborado pelo autor.



**Figura 26 – Portas mapeadas antes da ferramenta UTM na Empresa 2**

Severity	Plugin Name	Plugin Family	Count
INFO	Nessus SYN scanner	Port scanners	9
INFO	Ping the remote host	Port scanners	1

Fonte: Elaborado pelo autor.

**Figura 27 – Portas mapeadas antes da ferramenta UTM na Empresa 3**

Severity	Plugin Name	Plugin Family	Count
INFO	Nessus SYN scanner	Port scanners	9
INFO	Ping the remote host	Port scanners	1

Fonte: Elaborado pelo autor.

Após a implementação do dispositivo UTM, foram realizadas duas novas coletas em cada cenário e, novamente, os dados angariados neste segundo processo foram idênticos entre si. Logo, uma das amostras foi automaticamente descartada.

Mesmo com a utilização da ferramenta UTM, o *Nessus* conseguiu realizar a varredura das portas nos três ambientes. Porém vale ressaltar que em todos os mapeamentos o *appliance* identificou as tentativas sistemáticas de conexão (característica básica de um *port scan*) e registrou, via registro de *log*, conforme mostrado nas Figuras 28, 29 e 30.

**Figura 28 – Registros de logs de scan na Empresa 1**

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	10/21/2015 11:19:52.768	Alert	Intrusion Prevention	Probable port scan detected	191.191.197.186, 53733, X1 (admin)	179. * .114. * , 79, X1	TCP scanned port list, 23, 497, 548, 111, 443, 9100, 6000, 161, 1454, 79	
2	10/21/2015 11:19:52.768	Alert	Intrusion Prevention	Possible port scan detected	191.191.197.186, 7037, X1 (admin)	179. * .114. * , 9100, X1	TCP scanned port list, 23, 497, 548, 111, 443	

Fonte: Elaborado pelo autor.

**Figura 29 – Registros de logs de scan na Empresa 2**

Log View

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	10/22/2015 11:41:35.544	Alert	Intrusion Prevention	Probable port scan detected	191.191.197.186, 41414, X1, bfbc5ba.virtua.com.br (admin)	200. * .219. * , 48024, X1	TCP scanned port list, 47547, 47600, 47653, 47706, 47759, 47812, 47865, 47918, 47971, 48024	
2	10/22/2015 11:41:06.816	Alert	Intrusion Prevention	Possible port scan detected	191.191.197.186, 11962, X1, bfbc5ba.virtua.com.br (admin)	200. * .219. * , 18559, X1	TCP scanned port list, 18294, 18347, 18400, 18453, 18506	

Fonte: Elaborado pelo autor.

**Figura 30 – Registros de logs de scan na Empresa 3**

Log / Log Monitor

Filter View Src. IP

Filters: Display: Last 15 minutes Status Refresh: 60 sec

UTC Time	ID	Category	Priority	Message	Source	Destination	IP Protocol	Notes
01:16:10 Oct 23	82	Security Services	Alert	Possible port scan detected	191.191.197.186, 54286, X1	200. * .227. * , 17882, X1		TCP scanned port list, 17...
01:15:56 Oct 23	83	Security Services	Alert	Probable port scan detected	191.191.197.186, 62940, X1	200. * .227. * , 64525, X1		TCP scanned port list, 64...
01:15:03 Oct 23	82	Security Services	Alert	Possible port scan detected	191.191.197.186, 58359, X1	200. * .227. * , 17882, X1		TCP scanned port list, 62...

Fonte: Elaborado pelo autor.

A Figura 31 expõe, de forma mais detalhada, a coleta de portas no ambiente de pequeno porte mesmo após a implementação do dispositivo UTM.

**Figura 31 – Detalhamento das portas mapeadas na Empresa 1**

Empresa 1 - Depois  
CURRENT RESULTS: OCTOBER 21 AT 12:07 PM

Hosts > 179. \* .114. \* > Vulnerabilities

INFO Nessus SYN scanner

**Description**  
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.  
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

**Solution**  
Protect your target with an IP filter.

**Output**

Port 3389/tcp was found to be open

Port	Hosts
3389 / tcp	179. * .114. * ☑

Port 3777/tcp was found to be open

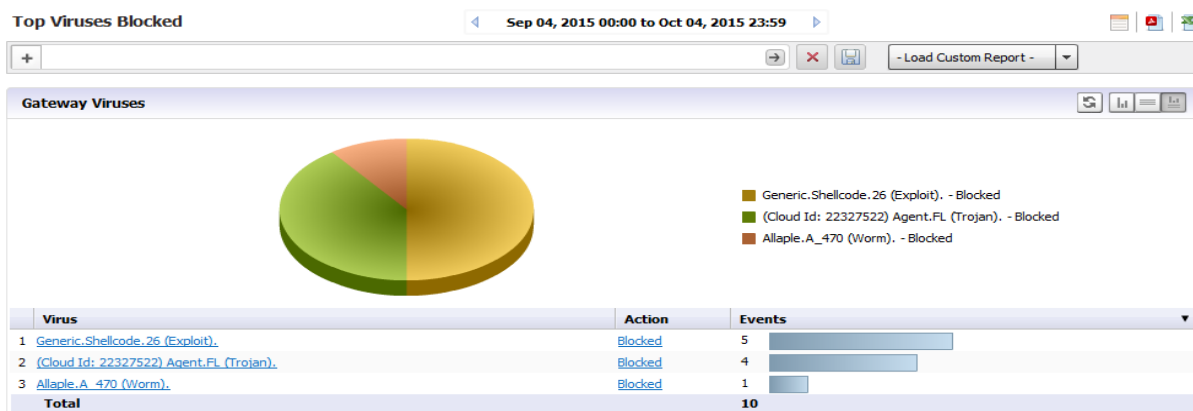
Port	Hosts
3777 / tcp	179. * .114. * ☑

Fonte: Elaborado pelo autor.

É possível analisar que, mesmo não havendo um bloqueio automático do *scan*, as ações não passaram despercebidas. Houve o registro de evidências juntamente com informações do endereço IP de origem, o que dá ao gestor de redes respaldo para tomada de decisões.

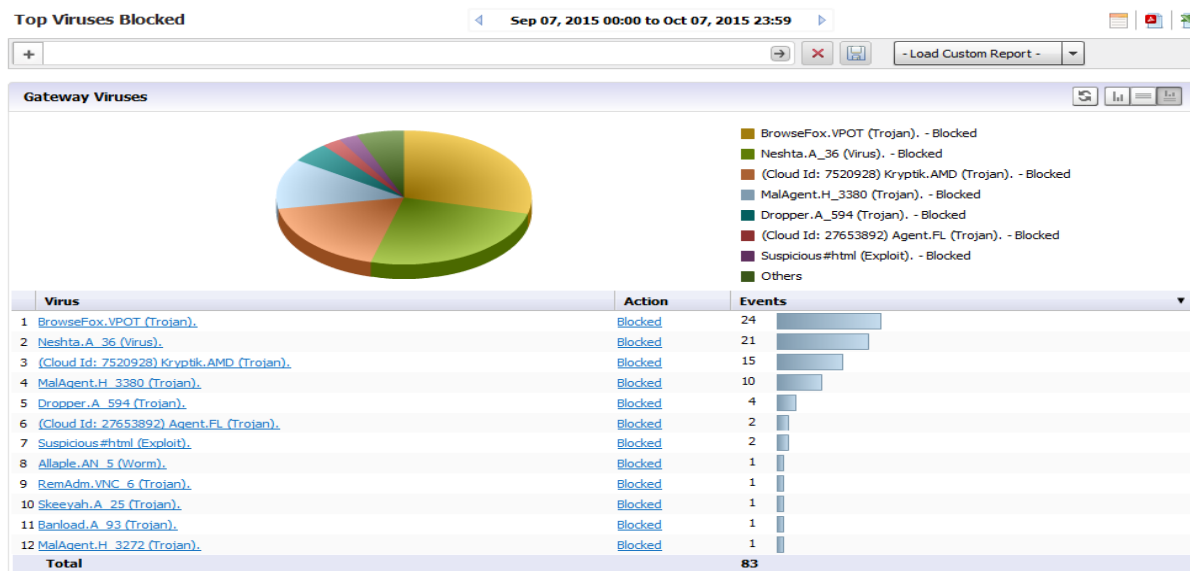
Com a utilização da aplicação *Analyzer*, foi possível coletar todos os registros de bloqueio (por parte do *appliance* UTM) a arquivos com conteúdos maliciosos, em cada um dos ambientes estudados, num intervalo de 30 (trinta) dias. O *software*, além de contabilizar o número de ocorrências, ainda discrimina cada tipo separadamente e gera um gráfico para facilitar a visualização das informações. Os resultados obtidos a partir das coletas do *Analyzer* são expostos pelas Figuras 32, 33 e 34.

**Figura 32 – Registro de vírus bloqueados na Empresa 1**



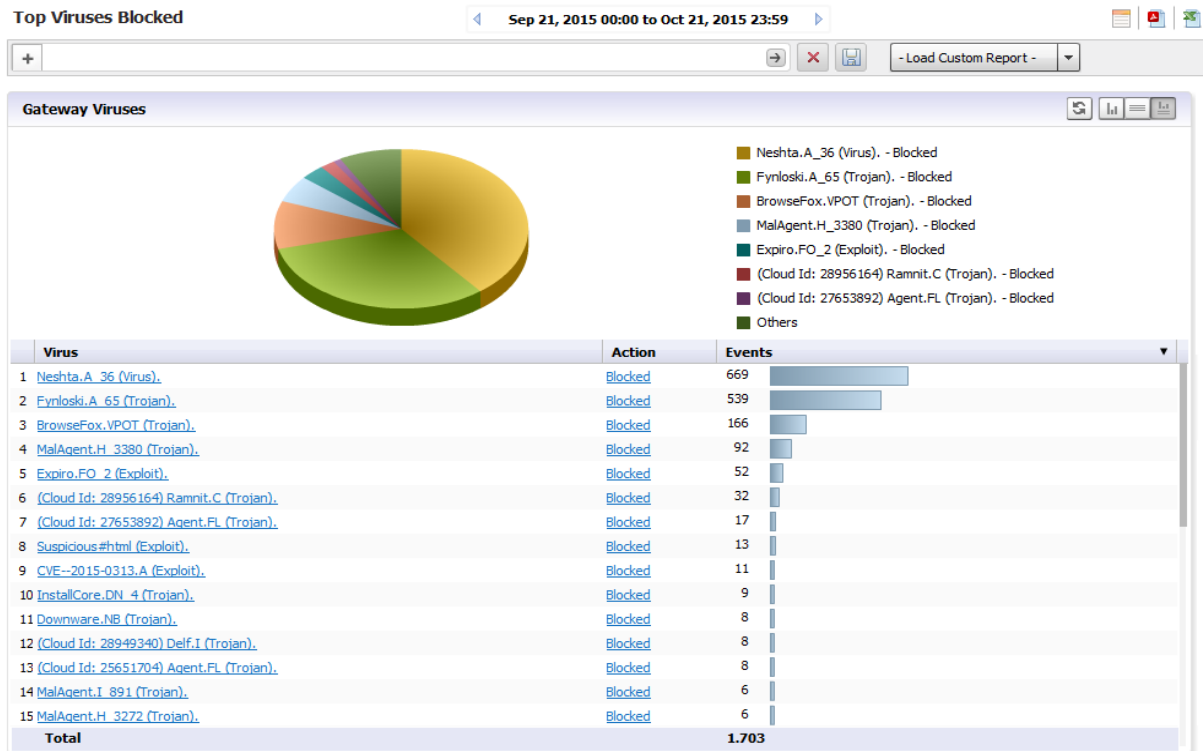
Fonte: Elaborado pelo autor.

**Figura 33 – Registro de vírus bloqueados na Empresa 2**



Fonte: Elaborado pelo autor.

**Figura 34 – Registro de vírus bloqueados na Empresa 3**



Fonte: Elaborado pelo autor.

É visível que, mesmo em uma análise de apenas 30 (trinta) dias, o número de ameaças que foram impedidas de penetrar nas infraestruturas estudadas foi muito significativo, principalmente nos cenários com um maior número de usuários.

### 4.3 Resultados estatísticos - fatores determinantes

Esta seção é destinada à apresentação dos resultados obtidos a partir dos dados coletados de um formulário *online* enviado aos três coordenadores de TIC das empresas estudadas. As informações nele contidas caracterizam a motivação de cada companhia pela escolha de uma ferramenta UTM como solução de segurança. Tal formulário encontra-se ao final deste documento, na forma de anexo.

Os dados serão dispostos de acordo com o porte de cada empresa e por ordem de relevância.

#### 4.3.1 Empresa 1 - Ambiente de pequeno porte

Com base nas necessidades do ambiente, os pontos elencados pelo responsável do setor de TIC, como determinantes para optar por uma ferramenta UTM como solução de segurança, foram:

- Filtragem de conteúdo (bloqueio de *sites* e aplicações).
- Balanceamento/Redundância de WAN (Utilização de múltiplos *links* de *Internet*).
- Segurança de borda (Antivírus de *gateway*, IPS/IDS, *antispyware*).
- Compatibilidade total entre os recursos oferecidos.

#### 4.3.2 Empresa 2 - Ambiente de médio porte

Dadas as regras de negócio do ambiente da Empresa 2, o coordenador de TIC elegeu os seguintes fatores:

- Interconexão de redes por VPN.
- Filtragem de conteúdo (bloqueio de *sites* e aplicações).
- Balanceamento/Redundância de WAN (Utilização de múltiplos *links* de *Internet*).

#### 4.3.3 Empresa 3 - Ambiente de grande porte

Para o gerente de TIC da Empresa 3, os pontos decisivos para optar por um dispositivo UTM como solução de segurança foram:

- Administração de segurança facilitada.
- Balanceamento/Redundância de WAN (Utilização de múltiplos *links* de *Internet*).
- Filtragem de conteúdo (bloqueio de *sites* e aplicações).
- Segurança de borda (Antivírus de *gateway*, IPS/IDS, *antispyware*).
- Compatibilidade total entre os recursos oferecidos.

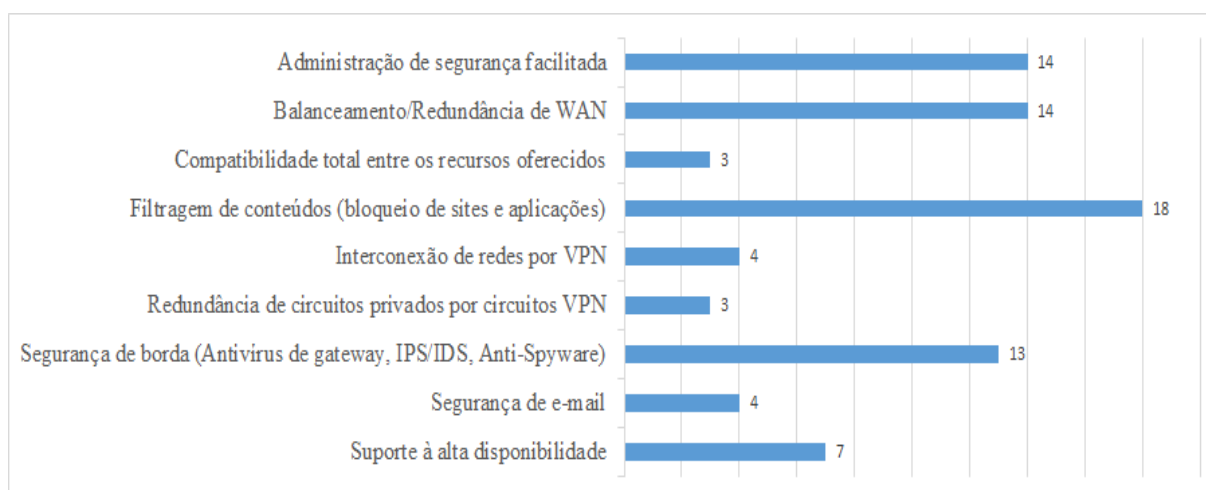
Além das informações coletadas dos três cenários de estudo, o mesmo formulário também foi disponibilizado a gestores de TIC de outras empresas que já utilizam ferramentas UTM para segurança de rede. Ao todo foram coletadas 106 amostras, utilizadas para construção dos gráficos apresentados abaixo.

#### 4.3.4 Fatores determinantes para empresas de pequeno porte

Do total de 106 amostras coletadas, 22 referem-se a empresas de pequeno porte. Dentre os fatores elencados por este segmento, destacam a filtragem de *sites* e aplicações, o balanceamento e redundância de circuitos de *Internet*, a administração de segurança facilitada e a segurança de borda.

A Figura 35 ilustra a quantidade de vezes que cada item foi selecionado como fator determinante à escolha de uma ferramenta UTM como solução de segurança para empresas de pequeno porte. Vale destacar que para cada coleta realizada foi possível selecionar múltiplos itens.

**Figura 35 – Fatores determinantes para empresas de pequeno porte**

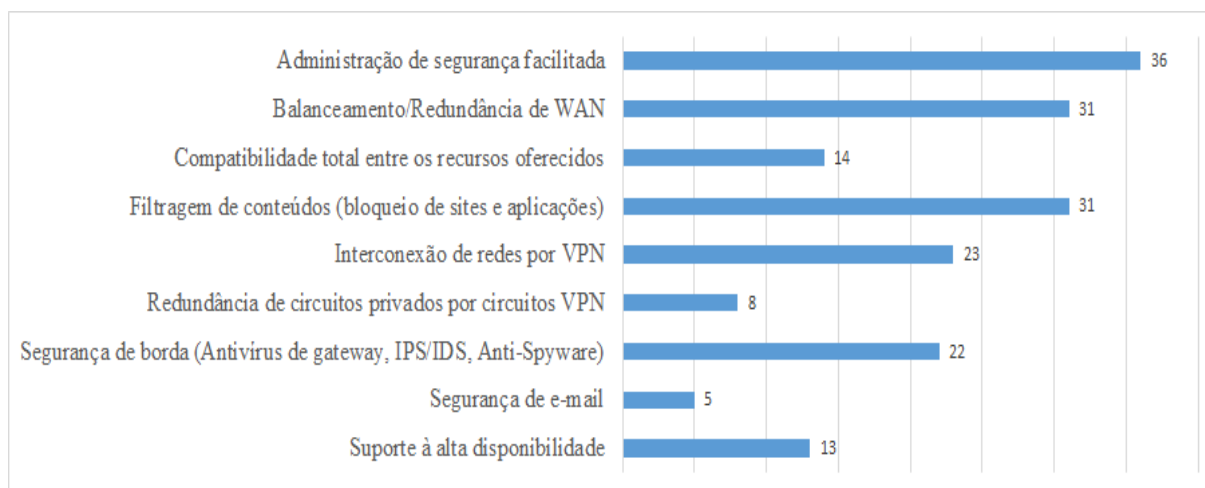


Fonte: Elaborado pelo autor.

#### 4.3.5 Fatores determinantes para empresas de médio porte

Ao todo foram coletadas 46 amostras referentes a empresas de médio porte. Para essa classificação, os fatores determinantes que receberam destaque foram: a administração de segurança facilitada, o balanceamento e redundância de circuitos de *Internet*, a filtragem *web* (*sites* e aplicações), a interconexão de redes através de circuitos VPN e a segurança de borda.

A Figura 36 representa a quantidade de vezes que cada item foi selecionado como fator determinante à escolha de uma ferramenta UTM como solução de segurança para empresas de médio porte.

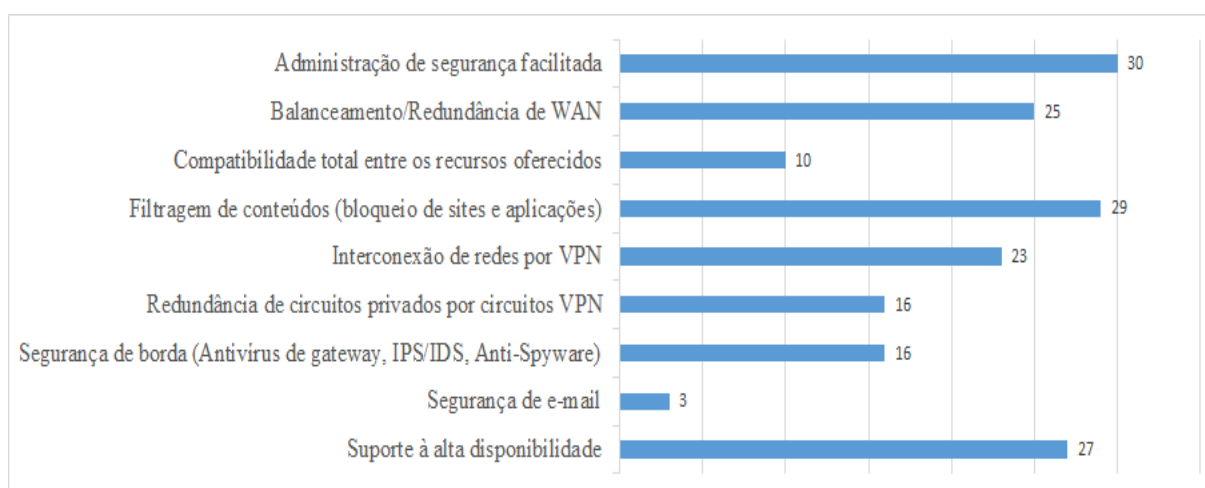
**Figura 36 – Fatores determinantes para empresas de médio porte**

Fonte: Elaborado pelo autor.

#### 4.3.6 Fatores determinantes para empresas de grande porte

Para empresas de grande porte foi coletado um total de 38 amostras, onde destacaram-se os seguintes fatores: a administração de segurança facilitada, a filtragem de conteúdos, o suporte à alta disponibilidade (*High Availability*), o balanceamento e redundância de circuitos de *Internet* e a interconexão de redes a partir de circuitos VPN.

A Figura 37 representa a quantidade de vezes que cada item foi selecionado como fator determinante para empresas de grande porte.

**Figura 37 – Fatores determinantes para empresas de grande porte**

Fonte: Elaborado pelo autor.

#### 4.4 Resultados financeiros - retorno sobre o investimento

Primeiramente serão explanados os custos totais envolvendo a aquisição dos equipamentos utilizados em cada ambiente, bem como os valores referentes ao licenciamento das funcionalidades de filtragem de conteúdo e segurança de borda (*Comprehensive Gateway Security Suite* - CGSS). Em seguida, serão calculados, com base na fórmula descrita na quinta seção do capítulo anterior, o ROI para os três cenários considerados no trabalho.

A Tabela 8 descreve os valores unitários (sem a realização do cadastro do registro de oportunidade junto ao fabricante) e os respectivos custos de licenciamento dos *appliances Dell SonicWALL SOHO, Dell SonicWALL TZ 300, Dell SonicWALL NSA 3600*.

**Tabela 8 – Custos da ferramenta UTM**

Modelo	Hardware + impostos	Licenciamento (CGSS - 3 anos)	Total
<i>Dell SonicWALL SOHO</i>	R\$ 4.124,06	R\$ 2.663,80	R\$ 6.787,86
<i>Dell SonicWALL TZ 300</i>	R\$ 7.464,04	R\$ 4.271,20	R\$ 11.735,24
<i>Dell SonicWALL NSA 3600</i>	R\$ 40.027,68	R\$ 25.190,20	R\$ 65.217,88

Fonte: Elaborado pelo autor.

Durante o período de 15 (quinze) dias antecedentes à instalação oficial das ferramentas UTM, os dados coletados com o funcionamento das mesmas em modo *bridge* além de facilitar a tomada de decisões na etapa de implementação, também foram utilizados para quantificar o tempo médio gasto com conteúdos não produtivos. Para a obtenção deste valor foi utilizado novamente o *software Dell SonicWALL Analyzer*. Tais informações foram diretamente utilizadas como componentes da variável “ganho obtido mensalmente” e são mostradas nas subseções a seguir.

##### 4.4.1 ROI - Empresa 1

Com a utilização da ferramenta *Analyzer*, foram obtidos os períodos gastos com os quinze *sites* mais acessados pela Empresa 1, e, a partir de uma análise do gestor de TIC, descartou-se o tempo utilizado em endereços pertinentes às atividades da organização.

A Figura 38 ilustra o relatório gerado pelo *Analyzer*.



**Figura 38 – Tempo gasto com conteúdos indevidos na Empresa 1**

Top Sites Aug 03, 2015 00:00 to Aug 18, 2015 23:59

Site IP	Site Name	Category	Browse Time	Hits	Transferred
2 31.13.73.3	facebook.com	Web Communications	10:31:42	8,190	436.69 MB
3 186.192.84.89	s2.qlbmq.com	News and Media	09:01:40	7,566	1.28 GB
5 201.31.84.13	googlevideo.com	Multimedia	06:54:52	7,167	3.29 GB
7 216.58.222.46	www.youtube.com	Web Communications	05:34:49	6,404	4.8 GB
8 189.86.41.80	googlevideo.com	Multimedia	04:34:42	5,837	1.57 GB
9 189.76.156.100	www.clicrbs.com.br	News and Media	04:02:16	5,437	550.38 MB
10 186.226.86.204	www.rbsdirect.com.br	News and Media	04:01:16	5,392	495.78 MB
12 186.192.80.5	voddownload.globo.com	News and Media	03:42:27	5,078	1.6 GB
13 179.184.23.16	rss.msn.com	News and Media	02:30:18	4,342	730.03 MB

Fonte: Elaborado pelo autor.

Com base nas informações acima citadas, chegou-se ao tempo total aproximado de 50,5 horas, que por sua vez foi duplicado para compreender o período de 1 mês. Em seguida, calculou-se o valor médio da hora de trabalho na Empresa 1, de acordo com as informações por ela fornecida, conforme mostra a fórmula abaixo:

$$Valor\ hora(R\$) = \frac{salário\ médio(R\$)}{carga\ horária\ mensal} \quad (2)$$

$$Valor\ hora(R\$) = \frac{1050}{220} = 4,77$$

Ao multiplicar o valor médio da hora trabalhada (R\$ 4,77) pelo total de horas gastas com conteúdos improdutivos, se obteve o montante de R\$ 482,04 por mês.

Também foi calculado o valor médio economizado com a eficiência energética do equipamento UTM. Para chegar a este resultado, se utilizou a fórmula básica do consumo energético:

$$Consumo(J) = potência(W) \cdot \Delta tempo(s) \quad (3)$$

No sistema internacional de unidades este resultado seria dado em *Joule*. Porém, em aplicações comerciais, a unidade utilizada é o quilowatt-hora (kWh). Por este motivo, os cálculos foram realizados diretamente com as variáveis no formato kWh.

A Tabela 9 apresenta um comparativo entre o consumo do antigo servidor utilizado pela Empresa 1 e do dispositivo *Dell SonicWALL SOHO*.

**Tabela 9 – Comparativo do consumo energético na Empresa 1**

	<i>Dell Power Edge T300</i>	<i>Dell SonicWALL SOHO</i>
Potência da fonte (kW)	0,49	0,024
Período de utilização (h)	720	720
Consumo mensal (kWh)	352,8	17,28
Valor do kWh (R\$)	0,71414047709	0,71414047709
Custo operacional mensal (R\$)	251,94	12,34

Fonte: Elaborado pelo autor.

Dados os valores de consumo de cada dispositivo, o montante mensal economizado com a eficiência energética da ferramenta UTM foi de R\$ 239,60. Para este cálculo utilizou-se apenas o valor médio do kWh do mês de setembro, desconsiderando os tributos fiscais (ICMS).

Para realizar todo o processo de implementação, o custo de instalação foi de R\$ 3.000,00. Por fim, o tempo necessário (em meses) para haver o equilíbrio entre o capital investido e o retorno gerado pela solução UTM foi de:

$$\text{ROI} = \frac{6.787,86 + 3.000}{482,04 + 239,60} = 13,56 \text{ meses} \cong 14 \text{ meses}$$

Após um período de três anos (validade da licença de CGSS) será necessário reinvestir o valor de R\$ 2.663,80, mas este terá um retorno ainda mais rápido.

$$\text{ROI} = \frac{2.663,80}{482,04 + 239,60} = 3,69 \text{ meses} \cong 4 \text{ meses}$$

#### 4.4.2 ROI - Empresa 2

Após o gestor de TIC da Empresa 2 validar as informações capturadas pelo *Analyzer*, se obteve um total aproximado de 16 horas perdidas com conteúdos improdutivos, conforme ilustra a Figura 39.

**Figura 39 – Tempo gasto com conteúdos indevidos na Empresa 2**

Top Sites Aug 12, 2015 00:00 to Aug 27, 2015 23:59

Site IP	Site Name	Category	Browse Time	Hits	Transferred
4 201.31.84.13	googlevideo.com	Multimedia	04:34:42	25,268	1.57 GB
5 201.86.233.221	www.youtube.com	Web Communications	04:02:16	12,687	3.29 GB
8 200.174.107.18	clickioqos.com.br	Games	03:42:27	1,901	553.31 MB
11 169.55.235.172	whatsapp.net	N/A	01:45:54	16,595	652.06 MB
14 31.13.85.2	facebook.com	Web Communications	01:05:52	8,898	307.17 MB
15 199.16.158.8	twitter.com	Social Networking	01:00:36	6,012	349.68 MB

Fonte: Elaborado pelo autor.

Este valor foi multiplicado por dois para obter o valor aproximado do período de um mês. Os valores informados pela Empresa 2, para média salarial aproximada, foi de R\$ 1.610,00 e carga horária de 220 horas mensais. Para este caso, o montante total economizado mensalmente com a filtragem de conteúdo foi de R\$ 234,18.

Utilizando a mesma fórmula para determinar o consumo energético descrita na seção anterior, a Tabela 10 apresenta um comparativo entre o antigo servidor utilizado pela Empresa 2 e do *appliance Dell SonicWALL TZ 300*.

**Tabela 10 – Comparativo do consumo energético na Empresa 2**

	<i>Dell Power Edge R200</i>	<i>Dell SonicWALL TZ 300</i>
Potência da fonte (kW)	0,345	0,024
Período de utilização (h)	720	720
Consumo mensal (kWh)	248,4	17,28
Valor do kWh (R\$)	0,71338904	0,71338904
Custo operacional mensal (R\$)	177,20	12,32

Fonte: Elaborado pelo autor.

Com base nos valores da tabela acima, o montante mensal economizado com a eficiência energética do dispositivo UTM foi de R\$ 164,88. Para este cálculo utilizou-se apenas o valor médio do kWh do mês de setembro, desconsiderando os tributos fiscais (ICMS).

Outro aspecto que incorporou a variável “ganho obtido mensalmente” foi o capital economizado pela utilização de circuitos VPN para interligação das filiais à matriz. A Tabela 11 resume os valores e as larguras de banda dos *links* MPLS e dos *links* ADSL (*Asymmetric Digital Subscriber Line*) de *Internet* que foram contratados para cada unidade. No nó matriz apenas foi realizado um aumento na largura de banda.

**Tabela 11 – Comparativo dos *links* MPLS e ADSL na Empresa 2**

	Filial A	Filial B	Filial C	Filial D	Filial E	Matriz
Banda MPLS (kbps)	512	512	512	512	512	2.048
Custo MPLS (R\$)	1.038,21	1.038,21	1.038,21	1.038,21	1.038,21	2.329,1
Banda <i>link</i> 1 (Mbps)	10	8	10	10	15	35
Custo <i>link</i> 1 (R\$)	89	99,50	69,90	75,10	71,99	159,90
Banda <i>link</i> 2 (Mbps)	5	5	10	8	10	20
Custo <i>link</i> 2 (R\$)	59,99	80,29	65,30	66,50	69,90	131,99

Fonte: Elaborado pelo autor.

Logo, o montante economizado com a utilização do circuito VPN foi de R\$ 6.480,79.

Para realizar todo o processo de implementação, o custo de instalação foi de R\$ 9.500,00. Por fim, o tempo necessário (em meses) para haver o equilíbrio entre o capital investido e o retorno gerado pela solução UTM foi de:

$$\text{ROI} = \frac{5 * 4.124,06 + 11.735,24 + 9.500}{234,18 + 164,88 + 6.480,79} = 6,08 \text{ meses} \cong 7 \text{ meses}$$

Após um período de três anos (validade da licença de CGSS) será necessário reinvestir o valor de R\$ 4.271,20 e para tal o retorno será em:

$$\text{ROI} = \frac{4.271,20}{234,18 + 164,88 + 6.480,79} = 0,62 \text{ meses} \cong 1 \text{ mês}$$

#### 4.4.3 ROI - Empresa 3

Para coletar as informações da Empresa 3, a partir da ferramenta *Analyzer*, foi criado um filtro para somente exibir dados da rede 192.168.0.0/22 (ADM), uma vez que os acessos da rede alunos não eram relevantes para o cálculo. Após a realização das devidas ponderações do

coordenador de TIC, o somatório de horas improdutivas foi de 173,5, que são expostas na Figura 40.

**Figura 40 – Tempo gasto com conteúdos indevidos na Empresa 3**

Site IP	Site Name	Category	Browse Time	Hits	Transferred
1 31.13.73.1	facebook.com	Web Communications	50:35:40	166.868	3,8 GB
3 64.233.186.141	app.snapchat.com	Web Communications	44:01:09	154.489	20,4 GB
4 199.27.75.246	audio-fa.spotify.com	Multimedia	41:21:46	112.975	22.01 GB
8 64.233.190.141	www.youtube.com	Web Communications	19:09:15	83.513	26.4 GB
10 186.215.194.12	googlevideo.com	Multimedia	11:48:33	75.843	38.86 GB
14 64.233.190.141	twitter.com	Social Networking	06:47:00	16.280	1,98 GB

Fonte: Elaborado pelo autor.

Novamente o valor obtido foi multiplicado por 2 para contemplar o período de 30 dias. As informações repassadas pela Empresa 3, para média salarial aproximada, foi de R\$ 2.070,00 e carga horária de 150 horas mensais. Neste cenário, o montante total economizado com os filtros de conteúdos foi de R\$ 4.788,60 mensais.

Os dados oriundos da fórmula do consumo energético para a Empresa 3 estão discriminados na Tabela 12.

**Tabela 12 – Comparativo do consumo energético na Empresa 3**

	<i>Dell Power Edge R410</i>	<i>Dell SonicWALL TZ 300</i>
Potência da fonte (kW)	0,480	0,250
Período de utilização (h)	720	720
Consumo mensal (kWh)	345,6	180
Valor do kWh (R\$)	0,7122619	0,7122619
Custo operacional mensal (R\$)	246,15	128,20

Fonte: Elaborado pelo autor.

Com as referências da tabela 12, a economia gerada com a eficiência energética do dispositivo UTM foi de R\$ 117,95. Para este cálculo utilizou-se apenas o valor médio do kWh do mês de setembro, desconsiderando os tributos fiscais (ICMS).

Para realizar todo o processo de implementação, o custo de instalação foi de R\$ 6.500,00. Por fim, o tempo necessário (em meses) para haver o equilíbrio entre o capital investido e o retorno gerado pela solução UTM foi de:

$$\text{ROI} = \frac{65.217,88 + 6.500}{4.788,60 + 117,95} = 14,61 \text{ meses} \cong 15 \text{ meses}$$

Após um período de três anos (validade da licença de CGSS) será necessário reinvestir o valor de R\$ 25.190,20 e para tal o retorno será em:

$$\text{ROI} = \frac{25.190,20}{4.788,60 + 117,95} = 5,13 \text{ meses} \cong 6 \text{ meses}$$

## 5 CONCLUSÃO

Com base no estudo realizado é possível determinar que, por se tratarem de ferramentas que englobam diversos conceitos de redes e segurança da informação, a instalação de uma solução UTM passa por um processo deveras complexo. Mesmo quando aplicadas a ambientes pequenos ou com uma infraestrutura consideravelmente simples, muitos aspectos requerem atenção para que não haja impactos negativos à empresa. Por atuarem diretamente na borda externa da rede, quaisquer falhas de projeto ou mesmo configurações incorretas durante o processo de análise e implementação, facilmente resultarão em uma interrupção do serviço de comunicação, que conseqüentemente geram diversos prejuízos à organização.

Também é possível afirmar que a utilização de ferramentas UTM, nos três cenários de estudo, expressou um aumento bastante significativo no nível geral de segurança das redes em questão. Mesmo não havendo um bloqueio automático do escaneamento de portas, sua execução foi devidamente detectada, fator este que garante ao gestor da rede embasamento para atuar diante de situações desta natureza. Outro ponto muito relevante foram as potencias ameaças barradas pelo antivírus de *gateway* e pela filtragem de *sites* e aplicações, que além de maximizarem a segurança da rede ainda geram uma economia financeira quando se considera o tempo economizado com conteúdos improdutivos.

A partir do estudo realizado foi possível observar que, mesmo para empresas de diferentes portes, há uma grande similaridade no que se diz respeito aos principais fatores determinantes no momento de optar por uma ferramenta UTM como solução de segurança para a rede. Os principais fatores elencados para todos os portes empresariais resumem-se à administração de segurança facilitada, à filtragem de conteúdos *web* e ao balanceamento e redundância de circuitos de *Internet*. Alguns fatores receberam relevância distinta de acordo com o tamanho da corporação envolvida. São eles: a segurança de borda (antivírus de *gateway*, IPS/IDS, *antispyware*) - para empresas de pequeno porte; a interconexão de redes por VPN - para empresas de médio porte e o suporte à alta disponibilidade (*High Availability*) - para empresas de grande porte.

Mesmo se tratando de equipamentos com valor de compra relativamente alto, nas três infraestruturas estudadas o retorno sobre o investimento se deu em um período inferior a dezoito meses (um ano e meio). O tempo necessário para que os benefícios gerados pela solução UTM ultrapasse os investimentos exigidos para sua compra e operação varia de acordo com os requisitos de cada ambiente. A filtragem *web* e de aplicações, juntamente com a eficiência energética dos dispositivos, representam uma economia direta aos cofres da organização. A substituição de circuitos MPLS por malhas VPN reduz de forma acentuada os custos de interconexão entre duas ou mais redes, sejam elas de uma mesma companhia ou de diferentes parceiros/fornecedores.

O presente documento apresentou o trabalho realizado como requisito direto à obtenção do grau de Bacharel em Engenharia da Computação. Todos os objetivos propostos foram alcançados. Além disso, o estudo contribuiu para formação de conhecimento e compreensão de um tema muito em voga no atual cenário de TIC, e que necessita ser veementemente difundido devido à sua grande utilização.

É possível citar como sugestão para trabalhos futuros, ou à continuidade do estudo realizado, a execução de experimentos que visam coletar os resultados de testes de *stress* feitos com diferentes ferramentas UTM. A submissão dos dispositivos UTM a vários tipos de cargas objetiva estudar e compreender o comportamento destes equipamentos quando aplicados a distintas situações reais de uma rede LAN. Outra possibilidade seria a realização de um estudo que vise a simulação de técnicas evasivas (*proxies*) aplicadas a soluções UTM, com o objetivo de obter a efetividade prática deste tipo de mecanismo de segurança.

## REFERÊNCIAS

- ALMEIDA, T. A.; YAMAKAMI, A. et. al. Redução de dimensionalidade aplicada na classificação de spams usando filtros bayesianos. **Revista Brasileira de Computação Aplicada**, Passo Fundo, v. 3, n. 1, p. 16-29, 2011.
- AMARAL, É. M. H.; BASTOS, C.; FIGUEIREDO, M. A.; LUNARDI, R. C.; SOUZA, A. M.; NUNES, R. C. **Análise Estatística Multivariada de Incidentes de Segurança em Redes de Computadores**, 2008. Disponível em: <[http://www.abepro.org.br/biblioteca/enegep2008\\_TN\\_STO\\_070\\_498\\_12168.pdf](http://www.abepro.org.br/biblioteca/enegep2008_TN_STO_070_498_12168.pdf)> Acesso em: 06 abr. 2015.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 17799**: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005b. 120 p.
- ASSOCIAÇÃO BRASILEIRA DE MARKETING DIRETO **Cálculo do ROI** Disponível em: <<http://www.abemd.org.br/pagina.php?id=73>> Acesso em: 04 jun. 2015.
- BHARDWAJ, P. K. **A+, Network+, Security+ Exams in a Nutshell** 1 ed. Sebastopol: Ed. O'Reilly Media, 2007. 787 p.
- BIGELOW, S. **Unified Threat Management: Migration and management techniques**, 2008. Disponível em: <<http://searchitchannel.techtarget.com/feature/Unified-threat-management-Migration-and-management-techniques>> Acesso em: 29 abr. 2015
- BRANDÃO, F. M. S. S.; OLIVEIRA, S. C. **Aplicação de Seamless MPLS nas Redes de Acesso** Pernambuco, 2012. Disponível em: <<http://www.fitec.org.br/wp-content/artigos/Aplicacao-Seamless-MPLS-nas-Rede-de-Acesso.pdf>> Acesso em: 11 mai. 2015.
- BRENTON, C.; HUNT, C. **Active Defense - A Comprehensive Guide to Network Security** 1 ed. Alameda: Ed. Sybex, 2001. 723 p.
- BRITO, S. H. B. **Wireshark na Análise de Tráfego e Protocolos em Redes**, 2013. Disponível em: <<http://labcisco.blogspot.com.br/2013/11/wireshark-na-analise-de-trafego-e.html>> Acesso em: 11 mai. 2015.
- CARMOUCHE, J. H. **IPsec Virtual Private Network Fundamentals** 1 ed. Indianápolis: Ed. Cisco Press, 2006. 480 p.
- CARTER, E.; HOGUE, J. **Intrusion Prevention Fundamentals** 1 ed. Indianápolis: Ed. Cisco Press, 2006. 312 p.
- CLARKE, J.; DHANJANI, N. **Network Security Tools** 1 ed. Sebastopol: Ed. O'Reilly Media, 2005. 352p.
- CONVERY, S. **Network Security Architectures** 2 ed. Indianápolis: Ed. Cisco Press, 2004. 792 p.
- DENT, K. D. **Postfix: The Definitive Guide** 1 ed. Sebastopol: Ed. O'Reilly Media, 2003. 264 p.



DEVLIN, P. **Unified threat management explained**, 2013. Disponível em: <<http://www.technologydecisions.com.au/content/security/article/unified-threat-management-explained-53439658>> Acesso em: 30 mar. 2015.

ENDORF, C.; SCHULTZ, E.; MELLANDER, J. **Intrusion Detection & Prevention** 1 ed. Chicago: Ed. McGraw-Hill, 2004. 388p.

FABRE, R. C. - **Métodos Avançados para Controle de Spam**. 2005. 94 p. Trabalho Final de Mestrado Profissional, Universidade Estadual de Campinas, Campinas, 2005.

Disponível em: <<http://www.las.ic.unicamp.br/paulo/teses/20050215-MP-Recimero.Cesar.Fabre-Metodos.avancados.para.controle.de.Spam.pdf>> Acesso em: 01 mai. 2015.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de Computadores, uma abordagem TOP-DOWN** 1 ed. Porto Alegre: Ed. AMGH Editora, 2013. 896 p.

FRAHIM, J.; SANTOS, O. **Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance** 1 ed. Indianápolis: Ed. Cisco Press, 2005. 840 p.

GARTNER IT Glossary, 2015. Disponível em: <<http://www.gartner.com/it-glossary/unified-threat-management-utm>> Acesso em: 27 mar. 2015.

GHEIN, L. DE **MPLS Fundamentals** 1 ed. Indianápolis: Ed. Cisco Press, 2006. 672 p.

GRANIER, T. B. **SPAM and Anti-SPAM**, 2006 Disponível em: <<http://www.sans.org/reading-room/whitepapers/email/spam-anti-spam-1776>>. Acesso em: 30 abr. 2015.

KNOX, T. A. **Technologies to Combat Spam**, 2003. Disponível em: <<http://www.sans.org/reading-room/whitepapers/email/technologies-combat-spam-1130>> Acesso em: 02 mai. 2015.

LAR, S. U.; LIAO, X.; REHMAN, A.; MA, Q. **Proactive Security Mechanism and Design for Firewall**, 2011. Disponível em: <<http://www.scirp.org/journal/PaperInformation.aspx?PaperID=6441#.VXSHzkb0-7A>> Acesso em: 03. mar. 2015.

LEHTINEN, R.; RUSSELL, D.; GANGEMI, G.T **Computer Security Basics** 2 ed. Sebastopol: Ed. O'Reilly Media, 2006. 312 p.

MENDES, D. R. **Redes de Computadores - Teoria e Prática** 1 ed. São Paulo: Ed. Novatec, 2007. 384 p.

MILLER, L. C. **Next-Generation Firewalls for Dummies** 1 ed. Indianápolis: Ed. Wiley Publishing, 2011. 68 p.

MORAES, A. F. DE **Segurança em redes: fundamentos** 1 ed. São Paulo: Ed. Érica, 2010. 264 p.

NAKAMURA, E. T.; DE GEUS, P. L. **Segurança de redes em ambientes cooperativos** 1 ed. São Paulo: Ed. Novatec, 2007. 488 p.

NMAP **Nmap Security Scanner** Disponível em: <<https://nmap.org/>> Acesso em: 03 jun. 2015.

NOONAN, W.; DUBRAWASKY, I. **Firewall Fundamentals** 1 ed. Indianápolis: Ed. Cisco Press, 2006. 408 p.

NORTHCUTT, S. **Spam and Flooding**, 2007. Disponível em: <[http://www.sans.edu/research/security-laboratory/article/spam-flooding#\\_\\_utma=216335632.364249024.1431318257.1431318257.1431318257.1&\\_\\_utmb=216335632.4.9.1431318731089&\\_\\_utmcc=216335632&\\_\\_utmcs=-&\\_\\_utmcz=216335632.1431318257.1.1.utmcsr=%28direct%29|utmccn=%28direct%29|utmcmd=%28none%29&\\_\\_utmv=-&\\_\\_utmk=174138977](http://www.sans.edu/research/security-laboratory/article/spam-flooding#__utma=216335632.364249024.1431318257.1431318257.1431318257.1&__utmb=216335632.4.9.1431318731089&__utmcc=216335632&__utmcs=-&__utmcz=216335632.1431318257.1.1.utmcsr=%28direct%29|utmccn=%28direct%29|utmcmd=%28none%29&__utmv=-&__utmk=174138977)> Acesso em: 01 mai. 2015.

OLIVEIRA, A. H. C. DE **Gerenciamento de túneis em ambiente mobile IP integrado a MPLS**. 2006. 168 p. Dissertação (Mestrado em engenharia) – Programa de Pós-Graduação em Engenharia Elétrica (PPGEE), Universidade de Brasília, Brasília, 2006.

PEIXINHO, I. C.; FONSECA, F. M.; LIMA, F. M. **Segurança de Redes e Sistemas**, 2013. Disponível em: <<http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas>> Acesso em: 17 mar. 2015.

PINHEIRO, J. M. S. **OSI: Um Modelo de Referência**, 2008. Disponível em: <[http://www.projetoderedes.com.br/artigos/artigo\\_osi\\_um\\_modelo\\_de\\_referencia.php](http://www.projetoderedes.com.br/artigos/artigo_osi_um_modelo_de_referencia.php)> Acesso em: 22 mai. 2015

PLATO, A. **UTM v NGFW - A Single Shade of Gray**, 2012. Disponível em: <<https://blog.anitian.com/utm-v-ngfw-a-single-shade-of-gray/>> Acesso em: 31 mar. 2015.

POKLADNIK, M.; SANTANDER, M. **UTM (Unified Threat Management) - Validating a UTM Device**, 2007. Disponível em: <[http://www.sans.edu/student-files/projects/200709\\_003.doc](http://www.sans.edu/student-files/projects/200709_003.doc) 2007> Acesso em: 01 jun. 2015.

ROBICHAUX, P. **Secure Messaging with Microsoft Exchange Server 2003** 1 ed. Redmon: Ed. Microsoft Press, 2004. 544 p.

ROUSE, M. **Nessus Definition**, 2006. Disponível em: <<http://searchnetworking.techtarget.com/definition/Nessus>> Acesso em: 03 jun. 2015.

SCARFONE, K. **Unified Threat Management - From Business Problem to Technical Solution** (parte 1), 2014. Disponível em: <[http://docs.media.bitpipe.com/io\\_11x/io\\_114747/item\\_863609/ISM\\_ITDC\\_Unified%20Threat%20Management\\_1\\_final.pdf](http://docs.media.bitpipe.com/io_11x/io_114747/item_863609/ISM_ITDC_Unified%20Threat%20Management_1_final.pdf)> Acesso em: 15 abr. 2015.

SCARFONE, K. **Unified Threat Management - From Business Problem to Technical Solution** (parte 2), 2014. Disponível em: <[http://docs.media.bitpipe.com/io\\_11x/io\\_114747/item\\_863610/ISM\\_ITDC\\_Unified%20Threat%20Management\\_2\\_final.pdf](http://docs.media.bitpipe.com/io_11x/io_114747/item_863610/ISM_ITDC_Unified%20Threat%20Management_2_final.pdf)> Acesso em: 15 abr. 2015.

SCHWARTZ, A. **SpamAssassin** 1 ed. Sebastopol: Ed. O'Reilly Media, 2004. 256 p.

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS **Critérios De Classificação De Empresas: EI - ME - EPP** Disponível em: <<http://www.sebrae-sc.com.br/leis/default.asp?vcdtexto=4154>> Acesso em: 03 jun. 2015.

SHAIKH, M. H.; KARLSON, I. S. **The Assessment of Employing Computational Intellection in Intrusion Detection Systems**, 2013. Disponível em <[http://www.cisjournal.org/journalofcomputing/archive/vol4no10/vol4no10\\_5.pdf](http://www.cisjournal.org/journalofcomputing/archive/vol4no10/vol4no10_5.pdf)> Acesso em: 30 mar. 2015.

SNYDER, J. **Evaluating Unified Threat Management Products for Enterprise Networks**, 2006. Disponível em: <<http://www.opus1.com/www/whitepapers/utm-eval.pdf>> Acesso em: 01 jun. 2015.

SOUZA, T. DA S. **IPSec - Internet Protocol Security** Rio de Janeiro, 2010. Disponível em: <[http://www.gta.ufrj.br/ensino/eel879/trabalhos\\_vf\\_2010\\_2/thiadgo/index.html](http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/thiadgo/index.html)> Acesso em: 10 abr. 2015.

SPEED, T.; ELLIS, J. **Internet Security: A Jumpstart for Systems Administrators and IT Managers** 1 ed. Burlington: Ed. Digital Press, 2003. 398 p.

TANENBAUM, A. S. **Redes de Computadores** 4 ed. Rio de Janeiro: Ed. Campus Elsevier, 2003. 946 p.

TITTEL, E. **Unified Threat Management for Dummies** 2 ed. Hoboken: Ed. Wiley Publishing, 2014. 68 p

## ANEXO A: FORMULÁRIO UTILIZADO PARA COLETA DOS FATORES DETERMINANTES

### ANÁLISE DA IMPLANTAÇÃO E UTILIZAÇÃO DE SISTEMAS DE GERENCIAMENTO UNIFICADO DE AMEAÇAS (UNIFIED THREAT MANAGEMENT – UTM) EM EMPRESAS DE DIFERENTES PORTES

Olá. Meu nome é Tiago Piazza, sou acadêmico do Centro Universitário UNIVATES - RS. Como requisito para a obtenção do grau de bacharel em Engenharia da Computação, estou realizando um estudo intitulado "ANÁLISE DA IMPLANTAÇÃO E UTILIZAÇÃO DE SISTEMAS DE GERENCIAMENTO UNIFICADO DE AMEAÇAS (UNIFIED THREAT MANAGEMENT – UTM) EM EMPRESAS DE DIFERENTES PORTES", que possui como um dos seus objetivos principais a detecção dos fatores decisivos para a escolha de ferramentas UTM como solução de segurança para cada porte de empresa. O formulário a seguir é anônimo e contém perguntas-chave que ajudarão a realizar importantes etapas deste Trabalho de Conclusão.

\*Obrigatório

1- Qual é o seu cargo de trabalho? \*

- Administrador de Redes
- Analista de Redes
- Coordenador de TI
- Especialista em Segurança da Informação
- Gerente de Telecomunicações
- Gerente de TI
- Outro:

2- Qual é o seu grau de decisão/influência quanto à escolha/contratação das soluções de segurança? \*

- Avalia
- Contrata/Compra
- Decide
- Especifica
- Precifica

3- Qual é o porte da empresa que você atua? \*

Classificação segundo o Instituto Brasileiro de Geografia e Estatística (IBGE).

- MICRO - (Indústria: até 19 funcionários; Serviço: até 9 funcionários)
- PEQUENA - (Indústria: de 20 a 99 funcionários; Serviço: de 10 a 49 funcionários)
- MÉDIA - (Indústria: de 100 a 499 funcionários; Serviço: de 50 a 99 funcionários)
- GRANDE - (Indústria: 500 ou mais funcionários; Serviço: 100 ou mais funcionários)

4- Dos diversos recursos encontrados em uma ferramenta UTM, quais deles você considerou mais importante quando comparou com outras soluções de segurança existentes no mercado? \*

- Administração de segurança facilitada
- Balanceamento/Redundância de WAN (Utilização de múltiplos links de Internet)
- Compatibilidade total entre os recursos oferecidos
- Filtragem de conteúdos (bloqueio de sites e aplicações)
- Interconexão de redes por VPN
- Redundância de circuitos privados por circuitos VPN
- Segurança de borda (Antivírus de gateway, IPS/IDS, Anti-Spyware)
- Segurança de e-mail (AntiSpam)
- Suporte à alta disponibilidade (High Availability)