Auxílio Multicritério à Decisão para seleção de um Firewall de rede para empresas de pequeno porte utilizando o método AHP

Vladimir da Silva Pereira Borgiani
vspnet2009@gmail.com
UFF

Marcilene de Fátima Dianin Vianna
marcilenedianin@gmail.com
UFF

Dalessandro Soares Vianna
dalessandrosoares@yahoo.com.br
UFF

Edwin Benito Mitacc Meza
emitacc@gmail.com
UFF

Resumo: Este artigo visa prover subsídios para a seleção de um firewall de rede de modo a estabelecer segurança de perímetro para empresas de pequeno porte, independentemente de sua área de atuação, utilizando o método de análise multicritério à decisão AHP – Processo Analítico Hierárquico. O trabalho foi desenvolvido com base em uma empresa provedora de serviços de telecomunicações em Macaé, RJ, onde a necessidade era proteger o tráfego de clientes conectados à Internet. As alternativas foram firewalls de entrada dos fabricantes Cisco, Watchguard, Fortinet e Dell SonicWall por serem de prévio conhecimento da equipe técnica da empresa e por possuírem assistência técnica no Brasil. O processo de seleção seguiu os critérios preço, serviços, capacidade e suporte.

Palavras Chave: AHP - Firewall - Segurança de rede - Decisão Multicritéri -

1. INTRODUÇÃO

Empresas de pequeno porte, independentemente de sua área de atuação, estão conectadas à Internet e, portanto, suscetíveis a ameaças cibernéticas dos mais variados tipos. Mais e mais empresas estão se tornando totalmente dependentes de sistemas de computador para suas operações do dia-a-dia (KIM; LEE, 2007). Além da proteção dos dados das empresas, a própria infraestrutura de acesso à Internet pode ser comprometida por ataques de negação de serviço. Esta indisponibilidade pode resultar em perdas financeiras e de reputação. Esses ataques demandam que o administrador de rede seja capaz de monitorar e reagir a quaisquer ameaças em potencial.

O firewall é um equipamento básico de proteção de perímetro de redes que evoluiu de um simples filtro de pacotes, permitindo bloquear tráfego IP entre redes, para um equipamento multiuso que protege contra diversos tipos de ataque (FRAHIM; SANTOS, 2010). Atualmente, serviços como redes privadas virtuais, criptografia, detecção e prevenção de intrusão, controle de aplicações, antivírus, segurança de e-mail, filtro de conteúdo web e autenticação são comuns em equipamentos de pequeno porte e, portanto, acessíveis para o consumidor leigo adquirir sem a necessidade de contratar um especialista para este fim.

A **Erro! Fonte de referência não encontrada.** demonstra a maneira genérica de conexão física de um firewall aos equipamentos internos da empresa e ao provedor Internet. A rede interna pode ter subdivisões denominadas zonas desmilitarizadas, no entanto o estudo não contempla explicação sobre esse modelo de implantação.

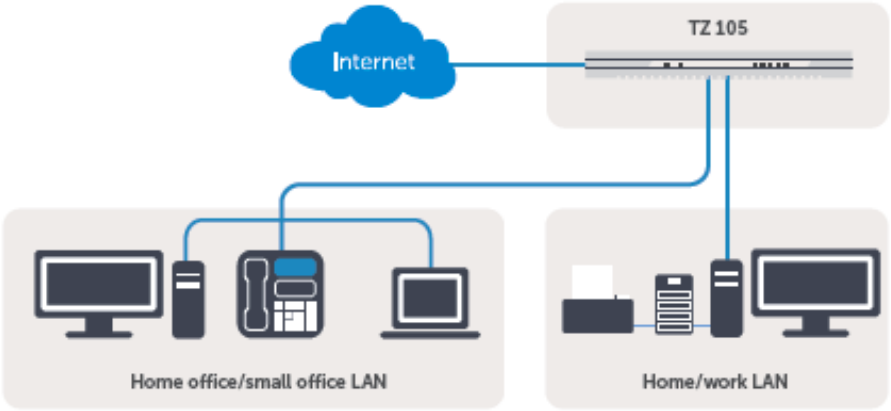

Figura 1: Topologia genérica de implantação.
Fonte: WALL, S. TZ Series, 2015.

A seleção de um equipamento para segurança de perímetro de rede é complexa devido aos diversos serviços de valor agregado que compõem os equipamentos dos vários fornecedores disponíveis no mercado. Cada empresa de pequeno porte possui necessidades muitos específicas que devem ser atendidas e, atualmente, a maioria dos equipamentos é capaz de atendê-las, seja implementado em software ou em hardware específico.

Comparar a importância de cada serviço em relação à capacidade e escalabilidade necessárias é importante visto que uma alta capacidade, por si só, não é significativa frente a um cenário em que todos os equipamentos se equiparam em capacidade. Do mesmo modo, escalabilidade perde importância na medida em que a necessidade de crescimento ao longo do

tempo pode ser absorvida pelo hardware já implantado e em operação, ou seja, escalabilidade deixa de ser um problema.

Estas empresas, geralmente, carecem de pessoal especializado na área de tecnologia da informação e acabam sendo guiadas pelos fornecedores, muitas vezes adquirindo equipamentos muito além de suas necessidades e, portanto, incorrendo em custos desnecessários.

O método AHP foi utilizado pelo fato de proporcionar uma ferramenta formal para comparação dos quesitos técnicos e permitir a quantificação de critérios mais subjetivos para o consumidor leigo em segurança da informação. Desse modo, espera-se contribuir para a elaboração de um método para escolha de equipamentos de segurança da informação que, com poucas adaptações, seja capaz de atender diversas demandas.

2. O MÉTODO AHP

O AHP – *Analytical Hierarchy Process* – é um método de Auxílio Multicritério à Decisão (AMD) utilizado na seleção de alternativas na presença de variados critérios. Estes critérios, muitas das vezes, podem apresentar um nível de incerteza tão alto que o processo decisório pode precisar reduzir esse grau de incerteza antes de continuar o processo (SAATY; VARGAS, 1987).

Ainda de acordo com Saaty e Vargas (1987), existem dois tipos de incerteza: a incerteza sobre o ocorrência dos eventos e a incerteza sobre os valores de julgamento para expressar as preferências. O primeiro tipo não pode ser controlado enquanto que o segundo depende da quantidade de informação disponível para o entendimento do problema.

A parte mais importante da construção e aplicação do método consiste na correta seleção dos critérios que realmente importam no processo de decisão (SAATY, 1994). Esses critérios e subcritérios são então arranjados em uma estrutura como a mostrada na Figura 2.

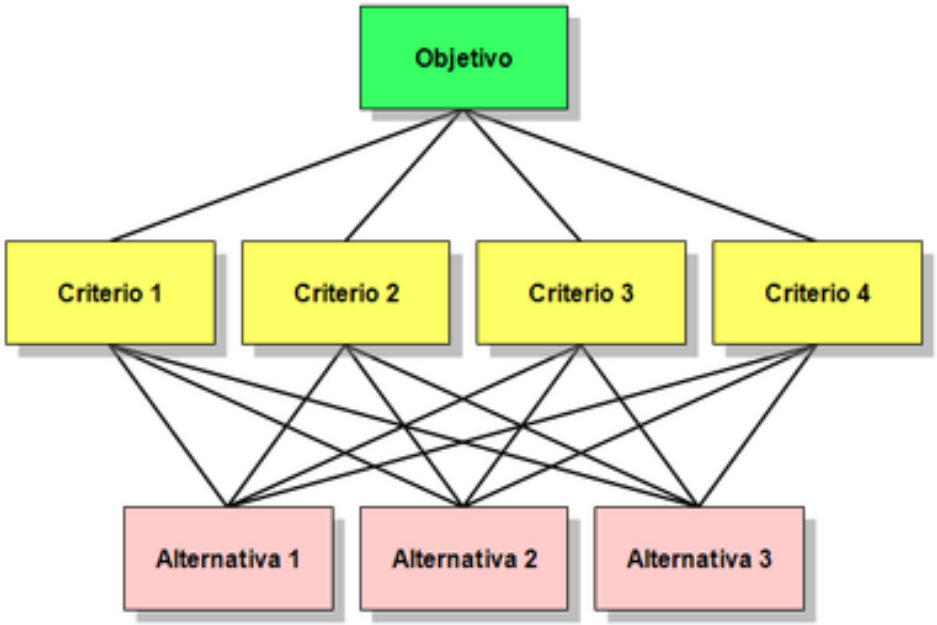

Figura 2: Modelo hierárquico AHP
Fonte: Modelo Analítico Hierárquico, 2015.

Seguindo a construção do modelo, as prioridades devem ser estabelecidas para cada critério de modo que sejam definidas as importâncias de cada um em relação aos demais. Quando muitas pessoas estão envolvidas no processo de priorização, encontrar o consenso pode ser difícil e uma matriz de importância de cada indivíduo julgador pode ser necessária para finalizar o debate (BASAK; SAATY, 1993).

A Figura 3 apresenta uma versão da escala fundamental de Saaty utilizada no método de comparação par a par (SAATY, 1994).

Intensidade de Importância	Definição	Explicação
1	Importância igual	As duas atividades contribuem igualmente para o objetivo
3	Pequena importância de uma sobre a outra	O julgamento favorece levemente uma atividade em relação à outra.
5	Importância grande	O julgamento favorece fortemente uma atividade em relação à outra.
7	Importância muito grande	O julgamento favorece muito fortemente uma atividade em relação à outra.
9	Importância absoluta	Mais alto grau de certeza de favorecimento de uma atividade sobre a outra
2,4,6,8	Valores intermediários entre julgamentos	Condição intermediária entre duas definições

Figura 3: Escala fundamental de comparação de Saaty.
Fonte: PAULA, B. L. de, CERRI, L. E. da S., 2012.

Após a definição das prioridades, chega a hora de ter certeza de que não existe inconsistência nos valores para julgamento. Um julgamento válido deve ter uma razão de consistência $RC \leq 0{,}1$ (XAVIER *et al.*, [s.d.]).

A fórmula para o cálculo do índice de consistência é $IC = \frac{\lambda_{max} - n}{n-1}$, onde n é o número de critérios e λ_{max} é o maior autovalor da matriz de comparação paritária, sendo calculado pela multiplicação da matriz de julgamentos pelo vetor de prioridades, dividindo-se o resultado obtido nessa multiplicação pelo vetor de prioridades.

O cálculo de *RC* é realizado dividindo-se *IC* por *CA* (Índice de consistência aleatória), que é tabelado. A Figura 4 apresenta os valores de consistência aleatória para cada quantidade de alternativas.

n	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
CA	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51

Figura 4: Índice Saaty de consistência aleatória.
Fonte: PAULA, B. L. de, CERRI, L. E. da S., 2012.

2.1. APLICAÇÃO DO MÉTODO AHP

A aplicação do método é genérica e se relaciona a qualquer pequena empresa que tenha conexão à Internet com capacidade até 100 Mbps. O estudo assume, também, que o gerenciamento do equipamento de segurança de informação é feito por funcionário próprio e com conhecimentos técnicos básicos em tecnologia da informação de modo que o aprendizado das tecnologias e serviços do novo equipamento seja gradativo, mas constante.

As alternativas de firewall definidas neste trabalho são: Cisco ASA 5505 (CISCO SYSTEMS, 2015), Watchguard Firebox T10 (JUDE, [s.d.]), Fortinet Fortigate 30D (FORTINET, 2015) e Dell SonicWall TZ 105 (WALL, 2014). Essas alternativas nascem do fato de que estes fornecedores são conhecidos do mercado brasileiro e possuem assistência local, em português, e foram pré-qualificados em uma primeira avaliação dos serviços necessários para uma empresa de pequeno porte como redes privadas virtuais, criptografia, filtragem de pacotes, gerenciamento via interface web e wireless embutido.

Para a escolha da melhor alternativa, foram considerados os seguintes critérios: preço, suporte, capacidade e serviços. O critério capacidade foi dividido em três subcritérios: conexões simultâneas, capacidade de tráfego e novas sessões por segundo. O critério serviços foi dividido em quatro subcritérios: vpn túneis, criptografia, gerenciamento e wireless. Os critérios foram selecionados dentre as principais funcionalidades utilizadas por equipamentos de segurança de perímetro por pequenas empresas.

2.2. AVALIAÇÃO DAS PRIORIDADES DOS CRITÉRIOS

A prioridade de cada critério, em relação aos demais critérios, é determinada com a utilização do software Expert Choice (EXPERT CHOICE, [s.d.]). Estas prioridades determinam quais critérios são mais importantes, ou seja, possuem maior peso em relação aos demais critérios.

A Figura 5 apresenta os pesos de cada critério e subcritério, além das prioridades globais das alternativas.

A Figura 6 apresenta os pesos dos critérios em ordem decrescente de importância, na qual percebe-se que o preço é o principal fator na avaliação. Isto deve-se ao fato de que, para o ambiente de pequenas empresas relevantes do estudo, a maioria dos firewalls de entrada possuem similar níveis de serviço, suporte e funcionalidades. O julgamento foi realizado por um especialista de segurança da informação da empresa onde o estudo foi realizado. Exceto pelos critérios preço, capacidade e serviço vpn, que foram analisados direta ou indiretamente, todos os outros critérios foram avaliados par a par.

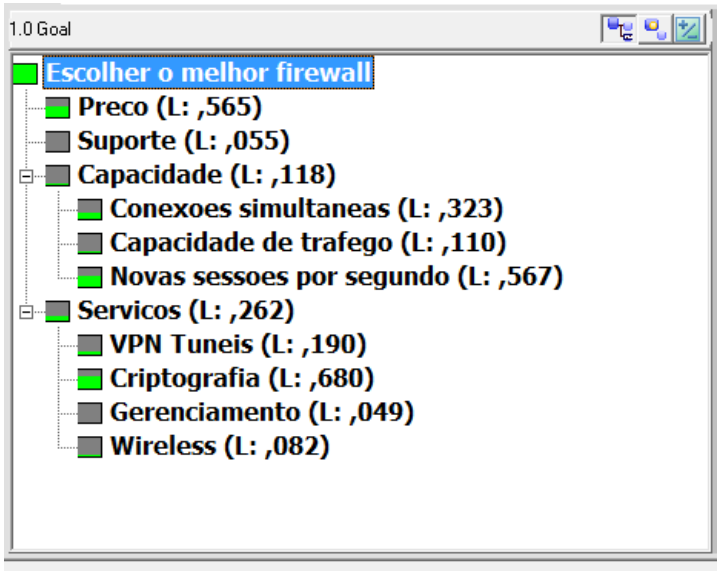

Figura 5: Prioridade dos critérios e subcritérios.

Figura 6: Pesos dos critérios.

A Tabela 1 apresenta os preços de firewall de entrada de cada fornecedor e os valores harmonizados e normalizados para servir como entrada para o software Expert Choice. A harmonização é utilizada para adequar a importância de cada critério de modo que o mesmo possa ser julgado diretamente, ou seja, quanto maior o valor, mais importante o critério. No exemplo do critério preço, o menor valor seria preferido (julgamento indireto). Dividir o somatório total pelo valor de cada critério adequa os dados à forma de julgamento direta. A normalização coloca os valores já harmonizados em percentual do todo, deixando clara a participação de cada critério.

Tabela 1: Harmonização e normalização do critério preço.

Modelo	*Preço (US$)*	*Harmonização*	*Normalização*
Cisco ASA 5505	$400,00	2,925	0,170
Fortigate 30D	$326,00	3,589	0,209
Watchguard T10	$200,00	5,850	0,341
SonicWall TZ 105	$244,00	4,795	0,279
Totais	$1.170,00	17,159	1,000

No critério suporte, foi solicitado que o especialista do domínio realizasse a comparação par-a-par. A análise levou em consideração a existência de suporte técnico local, facilidade em encontrar documentação online e quantidade de revendas do equipamento.

A Figura 7 apresenta a comparação, par a par, realizada pelo especialista do domínio, apresentando o ASA 5505 como de melhor desempenho no critério suporte.

	Dell SonicWall Tz 105	Cisco ASA 5505	Watchguard T10	Fortinet 30D
Dell SonicWall Tz 105		5,0	3,0	1,0
Cisco ASA 5505			7,0	3,0
Watchguard T10				3,0
Fortinet 30D	Incon: 0,02			

Figura 7: Critério Suporte avaliado par a par.

O critério capacidade foi subdividido em três subcritérios: quantidade de conexões simultâneas, capacidade de tráfego e quantidade de novas sessões por segundo. Essas são mais importantes pois demonstram não só o poder de processamento do equipamento, mas a escalabilidade e adaptabilidade do equipamento a mudanças repentinas no perfil de tráfego da rede a ser protegida.

A Tabela 2 apresenta o processo de normalização dos subcritérios componentes do critério capacidade, a saber, quantidade de conexões simultâneas, capacidade de tráfego e novas conexões por segundo.

Tabela 2: Normalização do critério capacidade.

	Capacidade		
Modelo	*Conexões simultâneas*	*Capacidade tráfego (Mbps)*	*Novas sessões por segundo*
Cisco ASA 5505	10000	150	4000
Fortigate 30D	200000	800	3500
Watchguard T10	7500	200	1000
SonicWall TZ 105	8000	200	1000
Totais	225500	1350	9500
Dados Normalizados			
Modelo	*Conexões simultâneas*	*Capacidade tráfego (Mbps)*	*Novas sessões por segundo*
Cisco ASA 5505	0,044	0,111	0,421
Fortigate 30D	0,887	0,593	0,368
Watchguard T10	0,033	0,148	0,105
SonicWall TZ 105	0,035	0,148	0,105
Totais	1	1	1

A Tabela 3 apresenta a normalização do subcritério vpn, que dimensiona quantos túneis criptografados cada equipamento suporta simultaneamente, em sua versão básica, assim como demonstra as avaliações par-a-par para os demais subcritérios do critério serviços. Apesar do subcritério criptografia apresentar todos os equipamentos com os mesmos pesos, a manutenção do mesmo na análise é necessária pois um dos objetivos é que este trabalho sirva de um modelo de referência para seleção de firewalls e não apenas resolver o problema descrito. O subcritério gerenciamento levou em consideração as formas existentes que o administrador teria para acessar, configurar e gerenciar o equipamento, a saber, linha de comando de texto, acesso através de navegador internet e aplicação específica criada pelo

fornecedor ou terceiros. O subcritério wireless levou em consideração se existe ou não a funcionalidade e se a mesma é opcional ou embutida na versão básica.

Tabela 3: Normalização e avaliação par-a-par do critério serviços.

	Serviços			
Modelo	*VPN*	*Criptografia*	*Gerenciamento*	*Wireless*
Cisco ASA 5505	10	3DES, AES	GUI / CLI /	Não
Fortigate 30D	20	3DES, AES	GUI / CLI / Application	Opcional
Watchguard T10	5	3DES, AES	GUI / CLI / Application	Opcional
SonicWall TZ 105	5	3DES, AES	GUI / CLI / Application	Nativo
Totais	40			
Dados Normalizados				
Modelo	*VPN*	*Criptografia*	*Gerenciamento*	*Wireless*
Cisco ASA 5505	0,25	1	1	1
Fortigate 30D	0,5	1	2	2
Watchguard T10	0,125	1	2	2
SonicWall TZ 105	0,125	1	2	3
Totais	1			

A Figura 8 mostra o julgamento do quesito vpn, realizado através de análise direta.

	Dell SonicWall Tz 105	Cisco ASA 5505	Watchguard T10	Fortinet 30D
Dell SonicWall Tz 105		2,0		
Cisco ASA 5505			2,0	
Watchguard T10				4,0
Fortinet 30D	Incon: 0,00			

Figura 8: Quantidade de tuneis para redes privadas virtuais.

As Figuras 9, 10 e 11 demonstram, respectivamente, os julgamentos dos subcritérios do critério serviços, realizados par a par.

	Dell SonicWall Tz 105	Cisco ASA 5505	Watchguard T10	Fortinet 30D
Dell SonicWall Tz 105		1,0	1,0	1,0
Cisco ASA 5505			1,0	1,0
Watchguard T10				1,0
Fortinet 30D	Incon: 0,00			

Figura 9: Algoritmos de criptografia disponíveis.

	Dell SonicWall Tz 105	Cisco ASA 5505	Watchguard T10	Fortinet 30D
Dell SonicWall Tz 105		2,0	1,0	1,0
Cisco ASA 5505			2,0	2,0
Watchguard T10				1,0
Fortinet 30D	Incon: 0,00			

Figura 10: Opções de gerenciamento do firewall.

	Dell SonicWall Tz 105	Cisco ASA 5505	Watchguard T10	Fortinet 30D
Dell SonicWall Tz 105		3,0	2,0	2,0
Cisco ASA 5505			2,0	2,0
Watchguard T10				1,0
Fortinet 30D	Incon: 0,00			

Figura 11: Funcionalidade wireless.

A Figura 12 mostra o resultado final, graficamente, com o equipamento Watchguard T10 como equipamento selecionado. Em segundo lugar, em um aparente empate, tem-se Fortigate 30D e SonicWall TZ 105, com Asa 5505 em último.

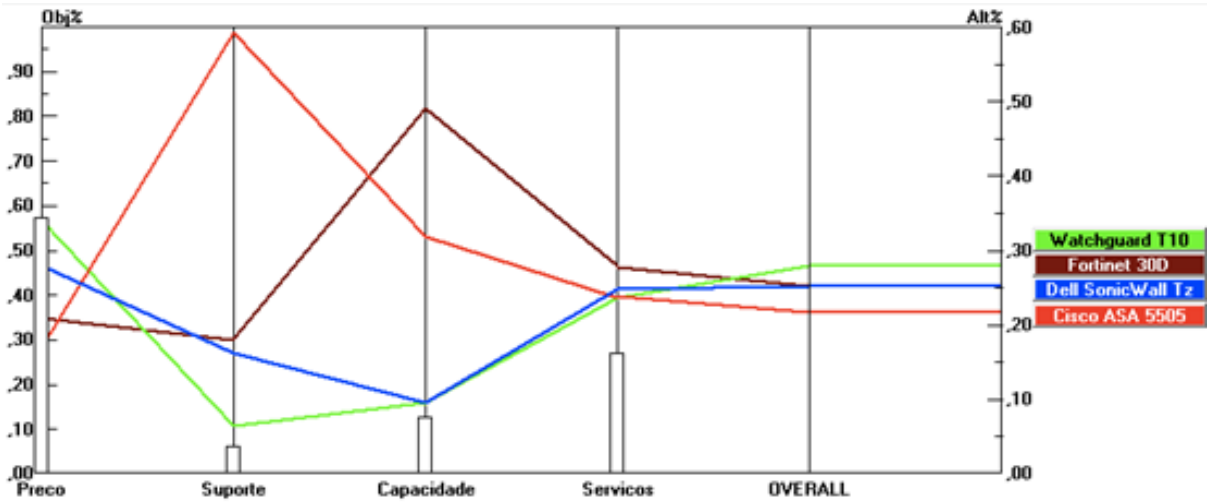

Figura 12: Prioridade global resultante.

A Figura 13 apresenta Fortinet como selecionado quando o critério mais importante passa a ser capacidade. Enquanto que a Figura 14 demonstra que o equipamento da Cisco seria o escolhido caso suporte tivesse a importância previamente associada ao critério preço.

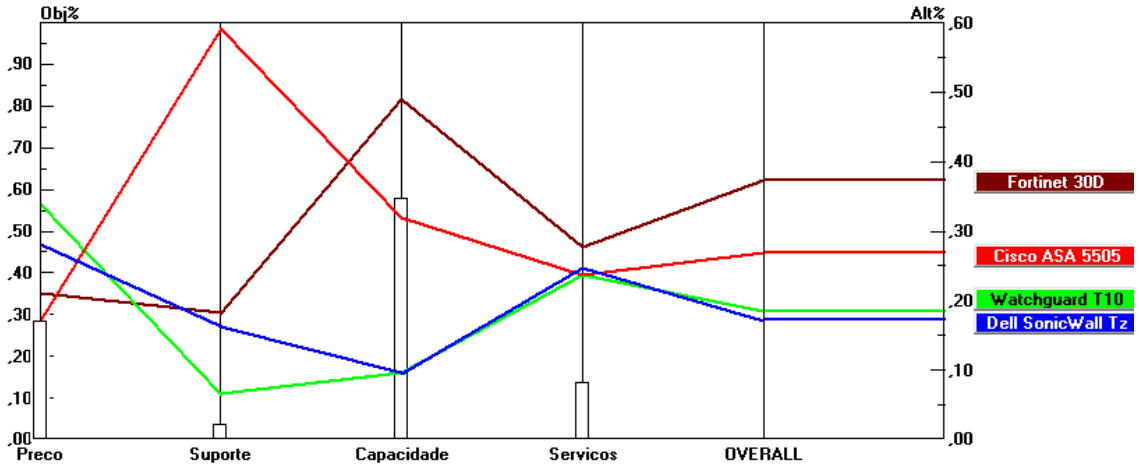

Figura 13: Resultado com critério capacidade com maior peso.

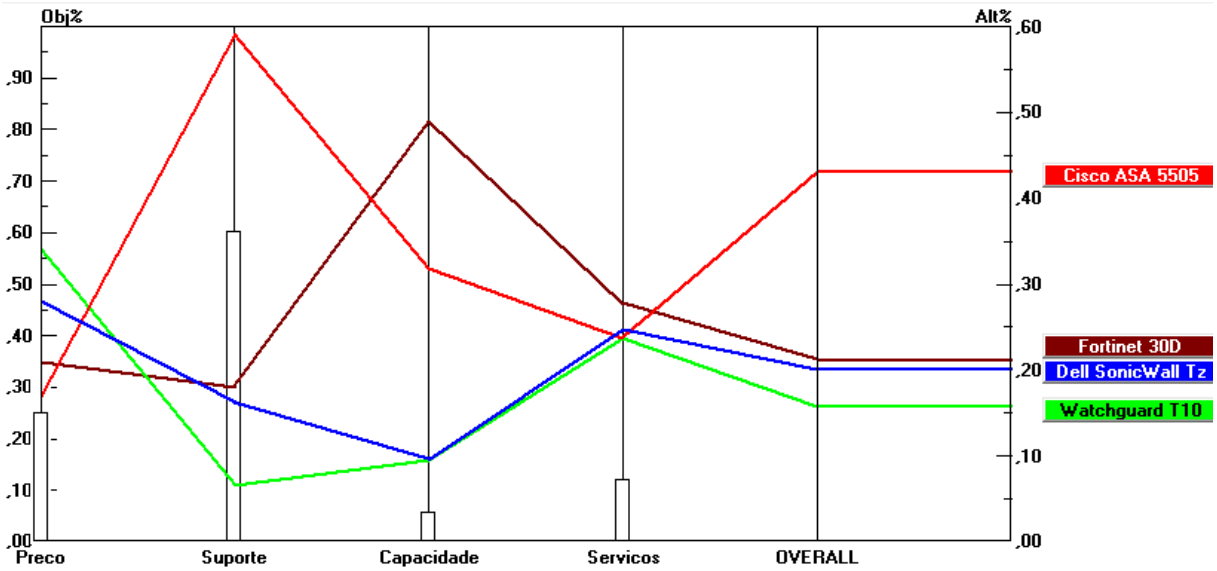

Figura 14: Resultado com critério suporte com maior peso.

3. CONCLUSÕES E TRABALHO FUTUROS

A escolha do firewall Watchguard Firebox T10 se deve ao fato de que preço foi o critério de maior importância na análise geral. Entretanto, a ferramenta utilizada permite uma rápida visualização das mudanças quando alteram-se os pesos de cada critério, tornando critérios antes sem importância em critérios decisivos.

É importante destacar que o método depende, exclusivamente, da melhor escolha dos pesos dos critérios e que os mesmos precisam se adaptar ao negócio para que a escolha faça sentido. Uma empresa pode necessitar que o peso das funcionalidades disponíveis seja maior do que o preço pelo simples fato de que a funcionalidade seja mandatória.

Recomenda-se a utilização de um número maior de critérios e subcritérios de modo a melhor definir a diferenciação entre as alternativas, ou seja, aumentar a diferença de importância entre as alternativas de modo a evidenciar a superioridade da escolha realizada.

4. REFERÊNCIAS

BASAK, I.; SAATY, T. Group decision making using the analytic hierarchy process. Mathematical and Computer Modelling, v. 17, n. 4-5, p. 101–109, 1993.

CISCO SYSTEMS. Cisco ASA 5505 Adaptive Security Appliance for Small Office or Branch Locations. Disponível em: <http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733510.html>. Acesso em: 6 set. 2015.

EXPERT CHOICE. No Title. Disponível em: <http://expertchoice.com/>. Acesso em: 6 jul. 2015.

FORTINET. FortiGate / FortiWiFi 30D Series. Disponível em: <http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-30D.pdf>. Acesso em: 7 set. 2015.

FRAHIM, J.; SANTOS, O. Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance. [s.l: s.n.].

JUDE, M. WatchGuard® Firebox® T10. Disponível em: <http://www.watchguard.com/docs/datasheet/wg_firebox_t10_ds.pdf>. Acesso em: 6 set. 2015.

KIM, S.; LEE, H. J. A study on decision consolidation methods using analytic models for security systems. Computers & Security, v. 26, n. 2, p. 145–153, 2007.

Modelo Analítico Hierárquico. Disponível em <http://www.wikiwand.com/es/Proceso_Analí tico_Jerárquico> Acesso em 5 set. 2015.

PAULA, B. L. de, CERRI, L. E. da S. Aplicação do processo analítico hierarquico (AHP) para priorização de obras de intervenção em áreas e setores de risco geológico nos municípios de Itapecerica da Serra e Suzano (SP). Geociênc. (São Paulo),vol.31, no.2, p.247-257. ISSN 0101-9082, 2012.

SAATY, T. How to make a decision: the analytic hierarchy process. Interfaces, v. 24, n. 6, p. 19–43, 1994.

SAATY, T. L.; VARGAS, L. G. Uncertainty and rank order in the analytic hierarchy process. European Journal of Operational Research, v. 32, n. 1, p. 107–117, 1987.

WALL, S. TZ Series. Disponível em: <http://www.sonicwall.com/br/pt/products/TZ-105.html#tab=specifications> Acesso em: 5 set. 2015.

XAVIER, B. M. *et al.* Auxílio multicritério a decisao para seleção de linguagem de programação usadas na construção de sistemas. [s.d.].