Uso de OSPF para convergência de túneis IPSec

Marcelo Tschanz Camocardi
IPT – Instituto de Pesquisas Tecnológicas
grupo.zender@gmail.com

Vanessa Pádua Muniz
IPT – Instituto de Pesquisas Tecnológicas
vanessa.padua@gmail.com

Dr. Alexandre Barbieri Sousa
IPT – Instituto de Pesquisas Tecnológicas
abarbieris@hotmail.com

***Resumo*— A busca pela alta disponibilidade é uma meta para diferentes tipos de empresas, principalmente para aquelas que possuem aplicações críticas para a continuidade de seus negócios. Porém, dispor de ambientes com altos índices de disponibilidade pode envolver grandes custos de aquisição e manutenção. Diante deste panorama, utilizar links não dedicados tende a ser uma realidade viável. Este artigo traz um estudo para avaliar disponibilidade e tempo de convergência utilizando-se de túneis IPSec sob links não dedicados com uso do protocolo de roteamento OSPF.**

I. INTRODUÇÃO

A suíte de protocolos *Internet Protocol Security* (IPSec) [2] se tornou um padrão em implementações que visam interligar localidades geograficamente distantes. Um dos grandes fatores que apoiam este padrão, é a interoperabilidade do IPSec permitindo, desta maneira, que o tunelamento através de *Virtual Private Network* (VPN) possa ocorrer entre diferentes fabricantes e soluções.

As VPNs são amplamente utilizadas em ambiente corporativo [9] possibilitando que o tráfego transite de maneira confiável entre diferentes unidades de negócio. Adicionalmente, as VPNs têm sido implantadas sob links *packet-switched – Asymmetric Digital Subscriber Line* (ADSL) - para prover alta disponibilidade de links dedicados [6], como por exemplo, *Multiprotocol Label Switching* (MPLS), aumentando desta maneira a resiliência da rede e do ambiente.

Para a convergência entre diferentes links, o roteamento se torna o fator chave [6]. Porém, atuar com o roteamento estático não seria a melhor abordagem em virtude da gerência das rotas. Para este artigo, foi escolhido o protocolo de roteamento dinâmico *Open Shortest Path First* (OSPF) por sua flexibilidade de configuração e demais características que serão descritas no decorrer deste artigo.

Com a convergência de tecnologias (voz, vídeo e dados), as operações e processos críticos das empresas, passam a ser realizadas através das conexões baseadas em IP, tornando imprescindível a disponibilidade das aplicações para a continuidade da empresa [6].

Solução de alta disponibilidade de links utilizando-se de conexões dedicadas tem dois fatores que podem leva a não adoção da mesma, sendo estas: 1. Custo elevado de links dedicados e 2. Dificuldade em ter 2 links dedicados de operadoras e circuitos diferentes.

A alternativa abordada neste artigo é a utilização de conexões compartilhadas do tipo ADSL ou Cable para atuar como *backup* das conexões dedicadas. Essa solução, mais econômica, torna possível a utilização de recursos de rede como protocolos de roteamento dinâmicos [9] em conjunto com a alta disponibilidade, além de trazer o fechamento dos três pilares de segurança: Confidencialidade, Integridade e Disponibilidade.

Outro ponto de atenção, é o tempo de convergência da rede que precisa ser aceitável, independente do tamanho da tabela de roteamento. Sabe-se que o tempo de convergência entre roteadores vizinhos, desde o inicio até sua finalização, pode ser rápido ou não, dependendo de fatores como protocolo utilizado, capacidade da conexão, mecanismos de autenticação, hardware entre outros.

Desta maneira, este artigo visa analisar o impacto na convergência de túneis IPSec sob links ADSL, utilizando-se do protocolo OSPF.

II. METODOLOGIA

Para demonstrar o tempo de convergência de redes utilizando-se de OSPF, foi realizado um experimento composto de duas etapas. A primeira etapa é a análise da funcionalidade da solução através do programa GNS3 (http://www.gns3.net), que emula roteadores, e outros ativos de rede, com o uso da imagem do próprio equipamento físico, ou seja, o comportamento dos roteadores (exceto questões de desempenho) poderá ser analisado de forma real. A segunda etapa consiste em realizar a medição dos tempos de convergência com equipamentos reais.

A análise do tempo de convergência será medido conforme as fases demonstradas na Figura 1.

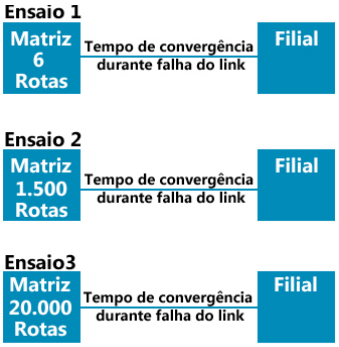

Figura 1. Diagrama de fases.

O cenário do experimento é composto da seguinte estrutura:

- Uma localidade denominada "Matriz" (Area 0) com 1 roteador central (*Core*) que possui seis rotas dinâmicas, aprendidas através de OSPF e 1 roteador de borda (ABR – Area Border Router), que faz a adjacência e troca de rotas entre roteadores vizinhos em localidades remotas (que serão descritas a seguir). Ambos vizinhos contam com conexões redundantes mas, apenas uma delas com tunelamento IPSec ativo.
- Duas Localidades Remotas denominadas "Filial 1" (Área 1) e "Filial 2" (Área 2). Ambas contam com os mesmos recursos de *hardware, software* e conexões redundantes até a "Matriz"

III. EXPERIMENTOS

Para minimizar o impacto de desempenho previsto nos roteadores de borda (ABR), o monitoramento ativo da conexão é realizado nos roteadores das Filiais "Filial 1" e "Filial 2", no qual cada localidade realizará a gerência de suas próprias conexões. Como resultado, o consumo de recursos de *hardware* no ABR será menor, proporcionando maior escalabilidade ao ambiente. Vale ressaltar, que este monitoramento pode ser feito no ABR porém, em virtude da sobrecarga, é recomendável que esta tarefa seja feita nos roteadores das filiais.

A seguir, são citados problemas que podem ocorrer e deverão ser mitigados antes da implantação deste ambiente.

- Se no mesmo roteador existirem duas conexões com dois túneis IPsec ativos simultaneamente, a vizinhança será fechada duas vezes com o mesmo vizinho, e pelo fato das conexões de túnel possuírem menor custo, o caminho que os pacotes tomarão não serão adequados e possíveis *loops* poderão ocorrer entre as interfaces virtuais.

- Em redes com conexões intermitentes poderá ocorrer o *flapping,* ou seja, a conexão se alterna entre o estado ativo e inativo. O mesmo acontece com os túneis e a vizinhança entre os roteadores, e como consequência ocorrerá aumento de processamento e alterações de topologia.

Em virtude do baixo custo e por suportar todas as funcionalidades requeridas para este ambiente, foram selecionadas as imagens de roteadores Cisco 2621.

As principais tarefas que os roteadores desempenham nesta topologia podem ser observadas na Figura 3.

Figura 3. Tarefas desempenhadas pelos roteadores das Filiais.

- Os eventos se desencadeiam quando o acesso a matriz se torna indisponível, seja por falha física ou lógica dos equipamentos.
- O monitoramento da disponibilidade da matriz é realizado através das ferramentas *IPSLA e tracking.* [4].
- As ações são tomadas com auxílio do recurso *event manager* [3].

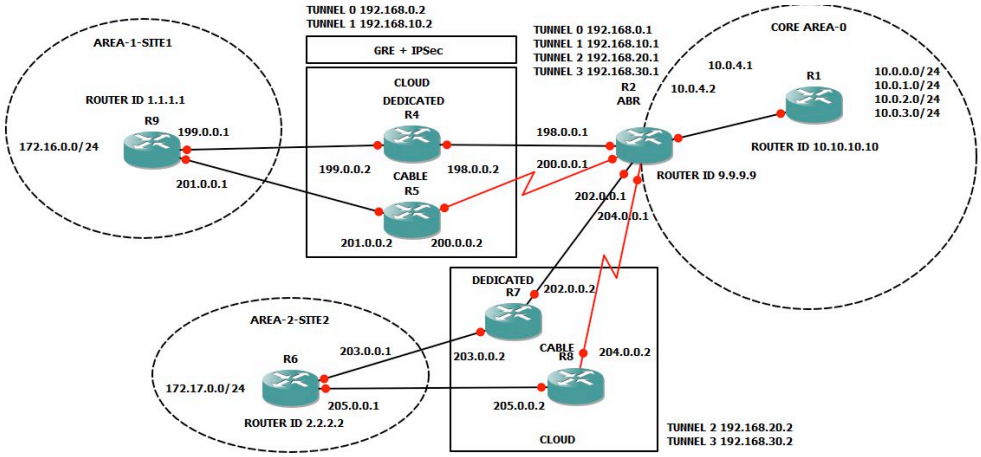

Figura 2. Topologia de Rede.

Para verificar a disponibilidade da localidade Matriz os comandos a seguir são utilizados:

```
ip sla monitor 1
type echo protocol ipIcmpEcho 198.0.0.2
timeout 1000
frequency 3
ip sla monitor schedule 1 life forever start-time now
!
track 1 rtr 1
```

Desta maneira, o endereço IP do ABR da matriz (198.0.0.2) é monitorado com frequência de 3 segundos e "timeout" de 1 segundo. O monitoramento começa a ser

realizado a partir do momento em que o equipamento é ligado. O comando "track" é responsável pelo alerta em caso de indisponibilidade.

```
event manager applet TUNNEL-1-LIGA
event syslog pattern "%TRACKING-5-STATE: 1 rtr 1 state Up->Down"
action 1.0 cli command "enable"
action 2.0 cli command "configure terminal"
action 3.0 cli command "interface tunnel 1"
action 4.0 cli command "no shutdown"
action 5.0 syslog msg "Tunnel 1 LIGADO"
action 6.0 cli command "end"
action 7.0 cli command "exit"
event manager applet TUNNEL-1-DESLIGA
event syslog pattern "%TRACKING-5-STATE: 1 rtr 1 state Down->Up"
action 1.0 cli command "enable"
action 2.0 cli command "configure terminal"
action 3.0 cli command "interface tunnel 1"
action 4.0 cli command "shutdown"
action 5.0 syslog msg "Tunnel 1 DESLIGADO"
action 6.0 cli command "end"
action 7.0 cli command "exit"
```

Quando o status se torna "*down*" é gerada uma mensagem de console no roteador. Este evento é capturado pelo *event manager* e a operação de ativação do túnel IPSec redundante é realizada de forma automatizada.

Para o processo de transferência do tráfego de uma interface para outra, é utilizado o comando "Track" em conjunto com o "Event Manager" e o "Action". Desta maneira, o "track" gera mensagens no terminal, em seguida o "Event Manager" captura essas mensagens e caso estas possuam "1 rtr 1 state Up->Down" os comandos informados nas linhas "action" para habilitar e desabilitar as interfaces de túnel do roteador serão realizados.

Na Figura 4 é demonstrado o fluxo das atividades quanto ao acesso dedicado até a matriz:

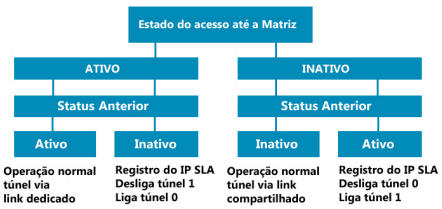

Figura 4. Fluxo de ações dinâmicas realizadas por evento nos roteadores das Filiais.

Para a análise e medição dos tempos de convergência, foram escolhidos roteadores de pequeno porte, sendo estes: Cisco 1841 para as Filiais e Cisco 2801 para a Matriz (ABR).

Através de um script em PHP (*Personal Home Page*) foram criadas rotas estáticas direcionadas para a interface *NULL 0* e redistribuídas para o processo OSPF, gerando assim 1500 rotas e 20.000 rotas consecutivamente. Para alterar as velocidades dos links foi utilizado o comando "clock rate" na interface serial, variando entre 512.000 bits por segundo a 2.000.000 bits por segundo.

Para simular tráfego, foi utilizado o programa Jperf. O tráfego foi gerado entre dois servidores, alcançando 70 conexões simultâneas em redes diferentes e roteadas através da técnica de *Inter Vlan Routing* (Roteamento entre redes virtuais) no ABR.

Os tempos de convergência foram medidos através do programa WinPing com frequência de mensagens a cada 1 segundo e timeout de 1 segundo. Através do *timestamp* foi possível identificar exatamente o tempo de indisponibilidade.

Na Figura 5 é ilustrado no WinPing, o comando ping sendo executado a partir da Filial 1 para a Matriz com o intuito de monitorar o tempo de indisponibilidade de acesso ao ambiente da Matriz.

```
1   Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:00.982
2   Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:01.980
3   Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:02.980
4   Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:04.039
5   Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:05.047
6   Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:06.036
7   Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:07.036
8   Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:08.095
9   Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:09.095
10  Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:10.094
11  Reply from 10.0.3.1 in   6 ms ; Bytes: 32 ; Time: 00:00:11.154
12  Reply from 10.0.3.1 in   7 ms ; Bytes: 32 ; Time: 00:00:12.152
13  TimedOut
14  TimedOut
15  DestinationHostUnreachable
16  DestinationHostUnreachable
17  DestinationHostUnreachable
18  DestinationHostUnreachable
19  DestinationHostUnreachable
20  DestinationHostUnreachable
21  DestinationHostUnreachable
22  DestinationHostUnreachable
23  DestinationHostUnreachable
24  DestinationHostUnreachable
25  DestinationHostUnreachable
26  Reply from 10.0.3.1 in   2 ms ; Bytes: 32 ; Time: 00:00:28.003
27  Reply from 10.0.3.1 in   2 ms ; Bytes: 32 ; Time: 00:00:29.063
28  Reply from 10.0.3.1 in   2 ms ; Bytes: 32 ; Time: 00:00:30.062
29  Reply from 10.0.3.1 in   2 ms ; Bytes: 32 ; Time: 00:00:31.123

Average of the response times = 5,06 ms
```

Figura 5. Retorno do Winping.

Como coleta de resultados do experimento, os seguintes dados foram obtidos:

Banda	Tabela de Roteamento	Carga ABR	Convergência Up → Down	Convergência Down → Up	Processamento ABR
512 kbps	6 rotas	70 Conexões 100 mbps	13 segundos	16 segundos	Entre 23% - 32%
512 kbps	1500 rotas	70 Conexões 100 mbps	17 segundos	11 segundos	Entre 25% - 29%
512 kbps	20000 rotas	70 Conexões 100 mbps	36 segundos	16 segundos	Entre 19% - 35 %
512 kbps	6 rotas	sem carga	13 segundos	10 segundos	Entre 0 % - 1 %
512 kbps	1500 rotas	sem carga	15 segundos	12 segundos	Entre 2 % - 4 %
512 kbps	20000 rotas	sem carga	35 segundos	16 segundos	Entre 6 % - 9%
1 mbps	6 rotas	70 Conexões 100 mbps	11 segundos	14 segundos	Entre 28 % - 35 %
1 mbps	1500 rotas	70 Conexões 100 mbps	14 segundos	13 segundos	Entre 12 % - 27 %
1 mbps	20000 rotas	70 Conexões 100 mbps	32 segundos	14 segundos	Entre 24% - 37 %
1 mbps	6 rotas	sem carga	12 segundos	11 segundos	Entre 0 % - 1 %
1 mbps	1500 rotas	sem carga	15 segundos	10 segundos	Entre 1 % - 4 %
1 mbps	20000 rotas	sem carga	24 segundos	19 segundos	Entre 2 % - 7 %
2 mbps	6 rotas	70 Conexões 100 mbps	17 segundos	13 segundos	Entre 23% - 31%
2 mbps	1500 rotas	70 Conexões 100 mbps	19 segundos	10 segundos	Entre 17 % - 26 %
2 mbps	20000 rotas	70 Conexões	26 segundos	23 segundos	Entre 27 % - 34 %

Tabela 1. Resultados alcançados

A partir destes dados foi possível observar que em ambientes com grande quantidade de rotas o tempo de convergência tende a aumentar, conforme demonstra o gráfico Figura 6.

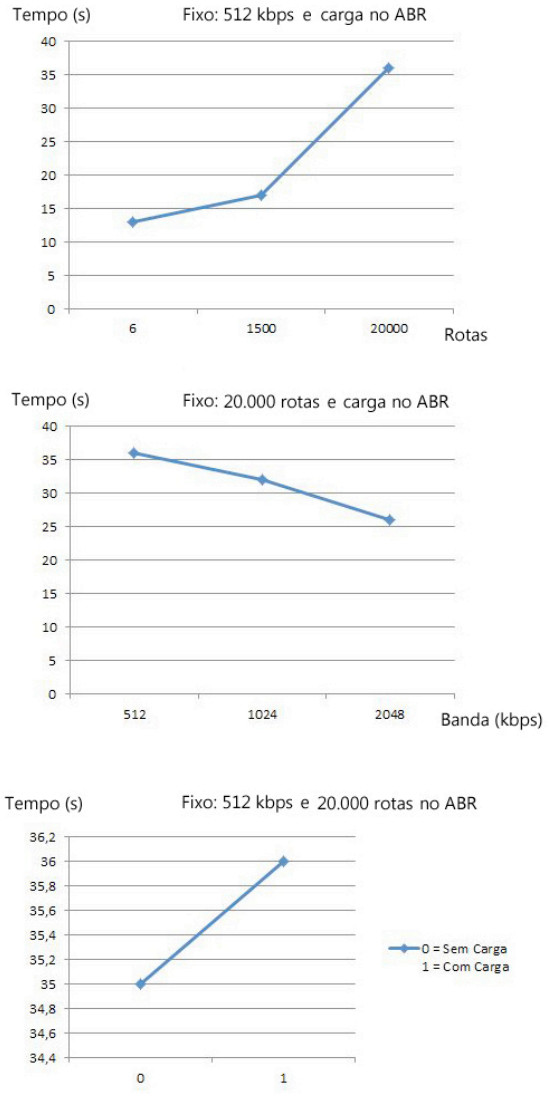

Figura 6. Gráfico com resultados do experimento

IV. CONCLUSÃO

Com a análise dos resultados alcançados, foi possível concluir que a solução atende a todos os cenários propostos com tempos de convergência abaixo de 36 segundos. Foram trabalhadas variações nas velocidades das conexões e mesmo com valores baixos, os tempos continuaram com pouca variação.

Adicionalmente, foi possível identificar que mesmo com uma grande quantidade de rotas e carga, o tempo de convergência não sofreu alterações sensíveis tornando a opção viável para ambientes de grande porte.

Desta maneira, o tempo de indisponibilidade de uma empresa que possui 2 links (dedicado e ADSL) para prover interconectividade e contingência de suas localidades, é mínimo e sendo aceitável para que os serviços corporativos sejam rapidamente reestabelecidos.

Como trabalhos futuros, é interessante uma análise deste experimento em ambientes com alto consumo de recursos de hardware dos roteadores envolvidos.

REFERÊNCIAS

[1] Aman Shaikh, *Student Member, IEEE*, Mukul Goyal, Albert Greenberg, *Member, IEEE*, Raju Rajan, and K.K. Ramakrishnan, *Member, IEEE* An OSPF Topology Server: Design and Evaluation IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 20, NO. 4, MAY 2002.

[2] Barylski, Marcin. On IPSec Performance Testing of IPv4/IPv6 IPSec Gateway. 1st International Conference on Information Technology, IT 2008, IEEE.

[3] Cisco IOS Embedded Event Manager (EEM). Disponível em <http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html> Acesso em 8 mar 2012.

[4] IP Service Level Agreements (IP SLAs). Disponível em <http://www.cisco.com/en/US/tech/tk920/tsd_technology_support_sub-protocol_home.html> Acesso em 8 mar 2012.

[5] Kini, Shrinivasa et al. Fast Recovery from Dual Link Failures in IP Networks. IEEE INFOCOM, 2009, IEEE.

[6] Kuboniwa, Akiko. IPsec-GW redundancy method with high reliability. Information and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium, 2010, IEEE.

[7] Kyriakos Manousakis, Anthony J. McAuley. Using Stochastic Approximation to Design OSPF Routing Areas that Satisfy Multiple and Diverse End-to-End Performance Requirements. 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, 2008, IEEE.

[8] Mikko Rtkanen, Marko Luoma. OSPF Flooding Process Optimization. High Performance Switching and Routing, 2005, IEEE.

[9] Okhravi, Johnson, Haines, Mayberry, Chan. Dedicated vs. Distributed: A Study of Mission Survivability Metrics. Military Communications Conference, 2011, IEEE.

[10] Song Wang, Hongbing Lv. A distributed object-based IPSec multi-tunnels concurrent architecture ICCP2011 Proceedings. International Conference on Computational Problem-Solving (ICCP), 2011, IEEE.