Estudo com protocolo IPv4, IPv6, OSPF e IPSec

Alexandre A. L. Lemos[1], Ítalo M. Faria[2]

[1]Faculdade de Computação – Universidade Federal de Uberlândia (UFU)
Uberlândia, MG - Brazil

[2]Faculdade de Engenharia Mecânica – Universidade Federal de Uberlândia (UFU)
Uberlândia, MG - Brazil

emaildoalexandre@ufu.br, imoraes@ufu.br

Abstract. *This work aims to explore the concepts and functioning of the IPv4 and IPv6 protocol along with the OSPF protocol. Methodologies and network simulations using the GNS3 simulator will be addressed to demonstrate the use of IPSec security authentication features and route disclosure.*

Resumo. *Este trabalho tem como objetivo explorar os conceitos e funcionamento do protocolo IPv4 e IPv6 junto do protocolo OSPF. Serão abordadas metodologias e simulações de rede utilizando o simulador GNS3 para demonstrar o uso de recursos de autenticação de segurança IPSec e divulgação de rotas.*

1. Introdução e metodologia

Internet se tornou uma parte importante da vida diária das pessoas em todo o mundo. Existem agora muitos dispositivos de rede que permitem que você se conecte a ele. Como tal, devem ser endereçados de alguma forma e, nas últimas décadas, o protocolo responsável por realizar esta função tem sido o IPv4. Atualmente, existe uma nova versão do protocolo IP, o IPv6, que também permite o endereçamento de dispositivos para que ambos possam coexistir no dispositivo. Portanto, este trabalho tem como objetivo explorar técnicas que proporcionem portabilidade entre as versões deste protocolo. A partir da criação de um cenário de simulação, será realizada uma técnica de migração de pilha dupla visando a convergência geral entre as duas versões do protocolo IP.

O protocolo de roteamento OSPF se enquadra na categoria de protocolo de roteamento de gateway interno dinâmico, que é responsável por encaminhar pacotes de rede da melhor maneira possível.

2. Estado da Arte

Para o desenvolvimento deste estudo, faz-se necessário introduzir o funcionamento do método utilizado. Esta introdução será realizada a seguir.

2.1. OSPF

Protocolo OSPF Como decidir o melhor caminho? Podemos fazer uma analogia sempre que saímos de casa para o trabalho ou a escola, temos duas ou mais possibilidades de um caminho, um mais curto e com muito trânsito, ou um mais longo mas mais suave. Dessa forma, escolhemos o protocolo de roteamento, aquele que leva em consideração o número de roteadores até a chegada do destino, também chamados de protocolos de vetor de

distância ou que me permitem chegar mais rapidamente dada a largura de banda, chamados de protocolos de estado de link ou Link State.

O OSPF funciona por meio de um programa denominado algoritmo Dijkstra, desenvolvido pelo cientista holandês Edsger Dijkstra, cuja função é manter um banco de dados contendo as mensagens recebidas de todos os outros roteadores. Quando um roteador recebe todas essas mensagens, ele cria seu banco de dados local, o OSPF usa o primeiro algoritmo de caminho mais curto aberto de Dijkstra para criar uma árvore SPF. A árvore SPF é então usada para preencher a tabela de roteamento IP com os melhores caminhos para cada rede. Para que essas informações sejam transmitidas por meio do protocolo de roteamento OSPF, precisamos entender certos tipos de mensagens trocadas entre roteadores configurados com o protocolo. Um conceito importante em redes configuradas com o protocolo de roteamento OSPF é a necessidade de cada roteador ter uma identificação para que se torne único na topologia.

Veja a figura abaixo, quando uma mensagem é enviada do PC1 para o Servidor.

Ao receber os pacotes, o roteador A1 tem dois caminhos a percorrer: o primeiro e mais óbvio diretamente para o A3 ou passar por A2 antes de chegar ao A3.

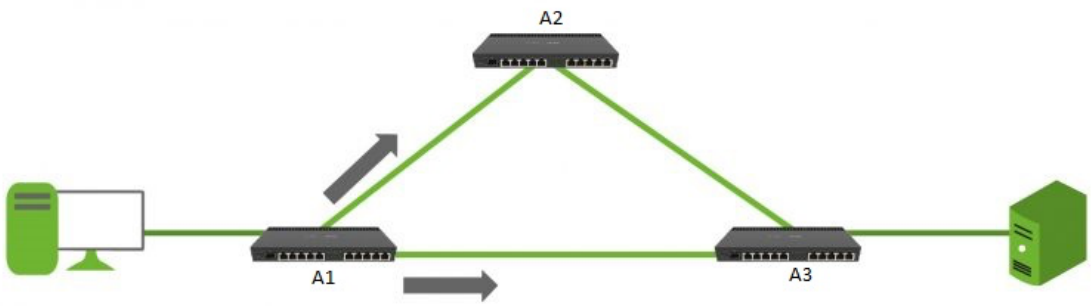

Figura 1. Exemplo de topologia de rede

Nesse caso, como tomar a decisão do melhor caminho? Eventualmente, podemos fazer uma analogia, ou seja, toda vez que saímos de casa para o trabalho ou para a escola, temos duas ou mais possibilidades de caminho, um mais curto, mas com muito trânsito, ou mais longo, porém, com mais fluidez.

Sendo assim, escolheremos aquele que permite chegar mais rápido considerando a banda, conhecidos como protocolos Link State ou Estado do Link.

2.2. IPSec

O IPSec é um protocolo de camada 3 projetado para suprir a falta de segurança de informações trafegando em rede pública. Basicamente o IPSec protege os pacotes IP de dados privados, encapsulando em outros pacotes IP para serem transportados. Há duas maneiras do IPSec ser implementado: modo túnel e modo transporte, sendo este último o modo nativo e o primeiro o utilizado neste projeto.

Dependendo do número de hosts conectados, o gerenciamento de chaves pode ser manual ou automático. O protocolo padrão para gerenciamento de chaves utilizado pelo IPSec é o Internet Key Exchange(IKE).

O IKE opera em duas fases:

Na fase 1, em meio inseguro, é estabelecido um canal seguro para realizar as operações do ISAKMP (Internet Security Association and Key Management Protocol). É executada uma vez para várias fases 2.

A fase 2 ocorre no canal seguro estabelecido na fase 1 e tem como objetivo definir as configurações da SA que irá proteger a conexão, tais como algoritmo de criptografia (DES, 3DES, AES), algoritmo de autenticação (MD5, SHA-1) e tempo de vida do AS (até 28.000 segundos). Esse processo pode ocorrer de tempo em tempo, conforme a vida útil do SA expira.

Para estabelecer uma comunicação por VPN utilizando IPSec são necessárias 4 fases: A primeira é definir o caminho para o IKE; A segunda é realizar a fase 1 do IKE, definindo um túnel seguro para a fase 2; A terceira é realizar a fase 2 do IKE, definindo os parâmetros para a associação de segurança(SA); O último passo é a transferência de dados, já utilizando o túnel seguro.

O túnel se encerra quando é finalizado manualmente ou o tempo de vida acaba. O encerramento pode ser configurado também a partir da ociosidade do meio ou a partir de uma certa quantidade de dados transmitidos.

3. Metodologia

O software de simulação utilizado foi o GNS3. Com ele foi possível criar instancias dos roteadores da Cisco, porém, um pequeno ajuste necessitou ser feito para que fosse possível instanciar o roteador com software MikroTik que consistiu em utilizar o VM Ware para simular uma máquina virtual de suporte para o GNS3.

Após a configuração do ambiente, decidiu-se pela utilização da topologia presente na figura 2, onde também são exibidas as interfaces utilizadas em cada roteador assim como seus endereços de IP.

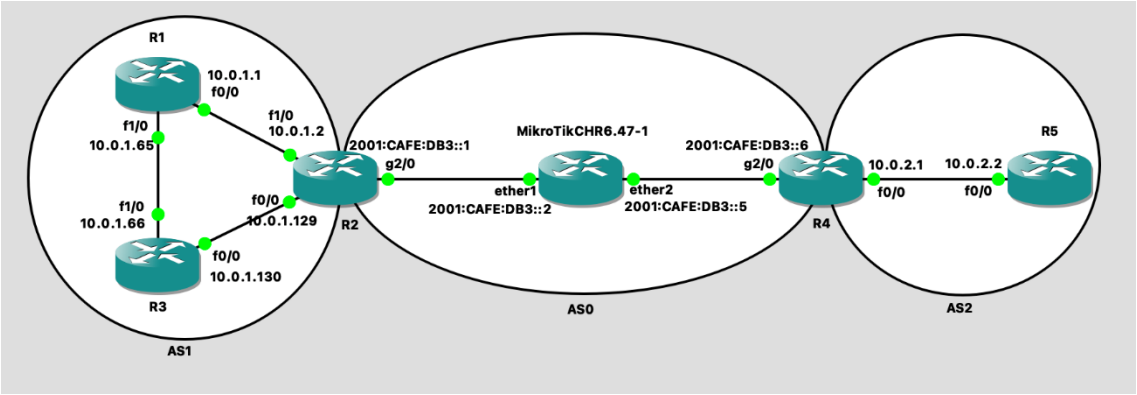

Figura 2. Topologia utilizada para o estudo

Os roteadores R1, R2 e R3 estão contidos em uma rede fechada (Área 1) e têm acesso às redes uns de outros, porém, o único roteador com acesso externo a essa rede é R2 e somente ele consegue se comunicar para fora da rede.

O Roteador R6 (MikroTik) faz parte de uma rede baseada em IPv6 e de seu próprio sistema (Área 0 - Backbone). Ele tem máscara de forma que apenas ele e mais dois dispositivos sejam conectados às suas subredes ("/126").

Os roteadores R4 e R5 estão em outra rede fechada (Área 2) e apenas R4 pode acessar a rede externa.

Existe um túnel protegido por IPSec com chave pré-compartilhada no backbone (Área 0: AS0) entre os roteadores R2 e R4. O túnel pode ser acessado navegando até o IP 2002::2 em R2 ou pelo IP 2002::1 através de R4.

Visto que a área 0 opera em IPv6 e as outras áreas em IPv4, existe também um túnel IPv4 sob IPv6 configurado manualmente a fim de permitir a comunicação bem-sucedida entre as áreas 1 e 2 e também a divulgação das rotas pelos roteadores de borda.

Nas tabelas 1 e 2 há um resumo da configuração efetuada em cada interface utilizada dos roteadores Cisco e MikroTik, respectivamente.

Tabela 1. Configurações dos roteadores Cisco

	f0/0	**f1/0**	**g2/0**
R1	10.0.1.1/26	10.0.1.64/26	-
R2	10.0.1.2/26	10.0.1.129/26	2001:CAFE:DB3::1/126
R3	10.0.1.130/26	10.0.1.66/26	-
R4	10.0.2.1/24	-	2001:CAFE:DB3::6/126
R5	10.0.2.2/24	-	-

Tabela 2. Configurações dos roteadores MikroTik

	ether1	**ether2**
R6 (MikroTik)	2001:CAFE:DB3::2/126	2001:CAFE:DB3::5/126

4. Resultados

Com a configuração dos roteadores, foi possível analisar a operação do OSPF e sua capacidade de publicar rotas por toda a rede. Fazendo um ping do roteador R5 na interface de IP 10.0.1.65 do roteador R1, é possível perceber que o OSPF propagou corretamente as rotas pelo IPv4. Além disso, é possível perceber que o OSPFv3 – utilizado para divulgar as rotas no IPv6 – também funcionou corretamente, uma vez que do roteador R2 é possível executar um ping bem sucedido à interface com IPv6 2001::CAFE:DB3::6 do roteador R4.

Quanto à implementação de túnel seguro com IPSec, a comunicação se deu de forma satisfatória. Analisando os pacotes capturados pelo software WireShark, é possível observar que existe uma comunicação privada e seus dados estão encriptados.

Durante a execução da configuração, foi encontrado um problema com o protocolo OSPF na divulgação da rota IPv4 da área 1 para a área 2. O problema foi identificado como a ausência da área de backbone (área 0), por onde os roteadores de borda deveriam fazer a divulgação de suas rotas entre as áreas. Ao configurar o túnel IPv4 sob IPv6, a área definida não foi a área 0, e sim a área 3. Desse modo, os roteadores de borda não faziam a divulgação por esse meio, a fim de evitar loops de rede. Ao alterar a área para 0, o protocolo funcionou corretamente de modo que a divulgação foi feita com sucesso.

5. Conclusão

Pôde-se concluir que o protocolo OSPF faz um ótimo trabalho divulgando rotas automaticamente dentro e fora das áreas, visto que se deve estar atento a como a configuração deve ser feita a fim de que rotas entre áreas sejam divulgadas por toda a rede.

O protocolo de segurança IPSec funciona perfeitamente bem e é uma alternativa muito boa para tráfego de informações sensíveis em redes não-seguras. Existe relativa facilidade na configuração e sua documentação é mais ampla, sendo mais fácil verificar problemas.

A elaboração deste projeto foi de extrema importância para aprofundar e fixar o conhecimento obtido durante as aulas teóricas, de modo que quando são encontrados problemas durante o desenvolvimento, isso força os estudantes a procurarem mais sobre o assunto, o que normalmente não aconteceria apenas com a parte teórica.

6. Referências

[1] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-man-tunls-xe.pdf

[2] https://www.cisco.com/c/pt_br/support/docs/ip/ip-version-6/25156-ipv6tunnel.html#t2

[3] https://wiki.mikrotik.com/wiki/Manual:IPv6/Address#Examples

[4] https://community.cisco.com/t5/networking-documents/configuration-example-site-to-site-vpn-for-ipv6-ipsec/ta-p/3134857

[5] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/ip6-route-ospfv3-xe.html

[6] https://www.cisco.com/c/pt_br/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

[7] https://www.youtube.com/watch?v=xSmVWsj98_Q

[8] https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1_2/vpn/vpn_ipsec2/vpn_ipsec/ipsec.html

[9] http://www.entelco.com.br/blog/roteamento-mikrotik-ospf-on-line-oficial/