Vpns e seus usos na computação moderna
Documentos e Resumo

Pedro Henrique Bufulin de Almeida [1], **Gabriel Solis Corrêa**[2],
TODO - Adicionar Nomes - Flávio Rech Wagner[1], **Jomi F. Hübner**[3]

[1]Faculdade de Computação – Universidade Federal de Uberlândia (UFU)
Caixa Postal 593 – CEP 38.400-902 – Uberlândia – MG – Brazil

gsolis.comp@gmail.com, TODO - Adicionem o email de vcs

Resumo. *Presente Artigo visa explorar as VPNs, seus usos na computação moderna e ferramentas relacionadas, além de conceituar o termo VPN. Serão realizados e documentados testes utilizando a ferramenta OpenVPN em um sistema de máquinas Ubuntu, hospedados nos servidores da Digital Ocean, para observar o funcionamento e as limitações de uma VPN.*

1. Introdução

2. Desenvolvimento

2.1. Configurado uma VPN utilizando OpenVPN

Para que seja possível implementar uma VPN como neste exemplo, você precisará de uma máquina rodando Ubuntu versão 18.04. Por questões de praticidade, não será visto com profundidade todo o processo de instalação das ferramentas que serão usadas, sendo algumas apenas mencionadas cabendo ao leitor descobrir como instalá-las. Além do servidor mencionado, o ideal seria ter uma outra máquina para ser a autoridade de certificação (CA), para evitar que um agressor capaz de se infiltrar no servidor consiga acessar a chave privada e assinar novos certificados.

2.2. Instalando os programas necessários

O primeiro passo é instalar o *OpenVPN* que está disponível nos repositórios padrão do ubuntu. Em seguida, instale *EasyRCA* tanto na máquina CA quanto no servidor que servira o VPN. O repositório deste programa encontra-se no github no mesmo repositório do *OpenVPN*. A versão a ser utilizada é a 3.0.8.

2.3. Configurando as variáveis e construindo o CA

No máquina que contém o CA, entre no diretório onde foi extraído o *EasyRCA*. copie o conteúdo do arquivo `vars.example` para um outro arquivo onde serão armazenadas as variáveis. Atualize os valores de acordo com suas informações, feche e salve o arquivo.

Dentro do da mesma pasta, existe um*script* chamado `easyrca`. Execute-o da seguinte maneira: `./easyrsa init-pki`. Isso irá iniciar a infraestrutura de chaves públicas no servidor CA. Se der tudo certo, deve surgir um diretório chamado `pki`. Em seguida, chame o script anterior novamente mas dessa vez com a opção `build-ca`. Isso irá construir a CA e criar dois arquivos importantes. Um deles é um certificado público que no contexto de uma VPN para informar ao servidor e ao cliente que ambos fazem parte da mesma rede. Isso serve como defesa de ataques do tipo *man-in-the-middle*

3. Discussão

4. Considerações Finais

5. Referências

Bibliographic references must be unambiguous and uniform. We recommend giving the author names references in brackets, e.g. [Knuth 1984], [Boulic and Renault 1991], and [Smith and Jones 1999].

The references must be listed using 12 point font size, with 6 points of space before each reference. The first line of each reference should not be indented, while the subsequent should be indented by 0.5 cm.

References

Boulic, R. and Renault, O. (1991). 3d hierarchies for animation. In Magnenat-Thalmann, N. and Thalmann, D., editors, *New Trends in Animation and Visualization*. John Wiley & Sons ltd.

Knuth, D. E. (1984). *The TEX Book*. Addison-Wesley, 15th edition.

Smith, A. and Jones, B. (1999). On the complexity of computing. In Smith-Jones, A. B., editor, *Advances in Computer Science*, pages 555–566. Publishing Press.