**ESQUEMA DE PLANO DE AULA PRÁTICA**

**TAREFA 8** "Construindo um Exemplo de VPN"

Tópico no Moodle “Rede Privada Virtual com OpenVPN”

Data:   
  
Tempo de Aula: 1,5 hora-aula  
  
Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Aluno\_2> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ASSUNTO**

Prática para se estudar como estabelecer uma VPN básica. O tópico é estudado através do uso do OpenVPN, uma ferramenta apropriada, um software livre que proporciona os meios necessários para estabelecimento de uma VPN.

A VPN estabelecida deve possuir todos os recursos de segurança para comunicação na Internet, tais como o uso de princípios de Diffie-Hellman, criptografia simétrica ou de chave pública e certificação digital.

**BIBLIOGRAFIA BÁSICA**

Página do OpenVPN, disponível em:<http://openvpn.net/>;

Página do OpenSSL, disponível em:<http://openssl.org/>;

Página do Prof. João Bosco Sobral, disponível em: <http://www.inf.ufsc.br/~bosco/ensino/ine5680/>

<http://invadindo.wordpress.com/servidor-vpn-com-openvpn/>

<http://www.vivaolinux.com.br/artigo/OpenVPN-+-Bridge-no-Ubuntu-Server>

<http://blogdonerd.com.br/2012/06/openvpn-servidor-ubuntu-e-clientes-windows-e-linux/>

**OBJETIVOS DA AULA**

Compreender como a segurança na comunicação de rede pode ser obtida, usando gateways VPNs instalados em ambientes de uma mesma organização, mas separados pela Internet.

Aplicar as condições para alcançar os requisitos de segurança de autenticação e confidencialidade na comunicação.

**SELEÇÃO DE CONTEÚDO – A PRÁTICA**

* Um conteúdo mínimo, consistindo de um roteiro de aula, com o OpenVPN, visando o objetivo acima, pode ser colocado como base de construção de uma VPN.

**MOSTRE SEU EXPERIMENTO (Deposite a tarefa no Moodle).**

* Criação de uma Autoridade Certificadora.
* Requisição e emissão de certificados digitais.
* Geração dos parâmetros Diffie-Hellman.
* Instalação e configuração da VPN.
* Execução e teste da VPN.

Para contemplar o conteúdo da aula prática, o aluno deverá seguir os passos, na ordem, inserindo os comandos no terminal Ubuntu Server.

**Configuração da VPN na VM Ubuntu Server**

1. $ cd /etc/ssl → Entrar no diretório etc/ssl
2. $ gedit openssl.cnf → abrir o arquivo de configuração openssl.cnf e localizar os parâmetros de [ CA\_defaults ], e alterar as linhas conforme o quadro 1:

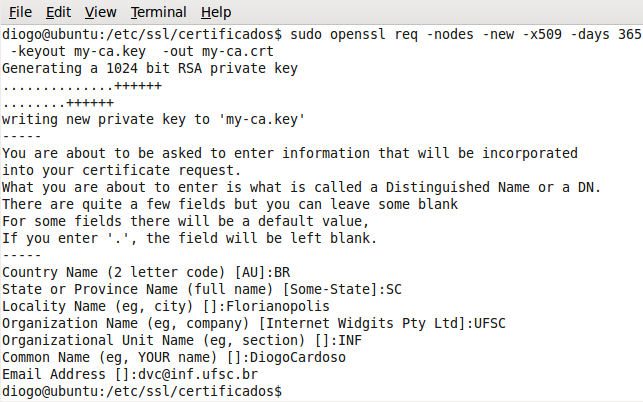
dir = /etc/ssl/certificados $ Where everything is kept

certificate = $dir/my-ca.crt $ The CA certificate

private\_key = $dir/my-ca.key $ The private key

Quadro 1: Modificações no arquivo openssl.cnf

1. $ mkdir certificados → criar o diretório "certificados"
2. $ cd certificados → acessar o diretório certificados
3. $ touch index.txt → Criar arquivo de índices;
4. $ echo ‘01’ > serial →Criar arquivo serial (pode-se usar o gedit e inserir “01” no arquivo);
5. $ openssl req -nodes -new -x509 -days 365 -keyout my-ca.key -out my-ca.crt → Gerar as chaves e certificados da CA - (preencher os dados requeridos, conforme modelo abaixo);   
    Modelo de dados para a geração de chaves no OpenVPN



1. $ openssl dhparam –out dh.pem 1024 → Gerar os parâmetros de Diffie-Hellman:
2. $ cd /etc/ssl/certificados → Acessar o diretório de certificados;
3. $ mkdir newcerts → Criar um novo diretório para os certificados da VPN;
4. $ openssl req -nodes -new -keyout vpn.key -out vpn.csr → Criar um novo par de chaves, agora para o certificado da VPN. (Preencher os dados como anteriormente e deixar as senhas em branco)
5. $ openssl ca -out vpn.crt -in vpn.csr → Registrar na entidade certificadora do servidor. (Y,Y);
6. $ cd /etc/openvpn → Acessar o diretório do OpenVPN (/etc/openvpn)
7. $ gedit vpn.conf → Criar o arquivo de configuração da VPN, e inserir os dados do quadro 2.

*dev tun*

*ifconfig 10.10.0.1 10.10.0.2*

*tls-server*

*dh /etc/ssl/certificados/dh.pem*

*ca /etc/ssl/certificados/my-ca.crt*

*cert /etc/ssl/certificados/newcerts/vpn.crt*

*key /etc/ssl/certificados/newcerts/vpn.key*

*port 5000*

*; user nobody*

*; group nobody*

*ping 15*

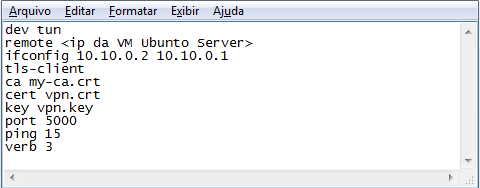
*verb 3*

Quadro 2: Modificações no arquivo vpn.conf

1. $ cd /etc/openvpn
2. $ openvpn --config vpn.conf → Carregar arquivo de configuração da VPN;
3. $ openvpn –daemon → Carregar o serviço do OpenVPN;
4. Configurar a placa de rede da VM para modo bridge;

**Configuração do Cliente VPN na VM Windows Server 2008**

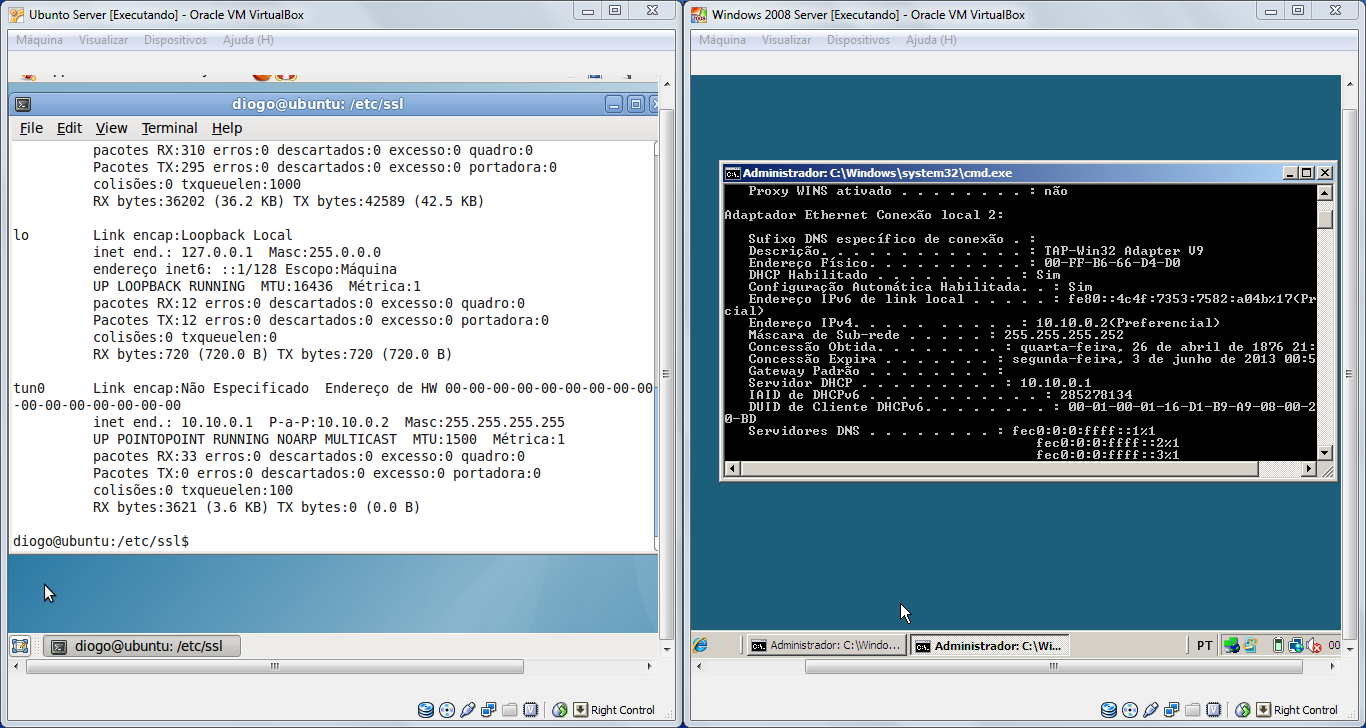
1. Copiar os arquivos (my-ca.crt, my-ca.key, vpn.crt, vpn.key, h.pem), criados no diretório /etc/ssl da VM Ubuntu Server, para o diretório c:/arquivos de programas/OpenVPN/config/ na VM Windows Server 2008;
2. Criar, utilizando o notepad, o arquivo de configuração vnp.ovpn, com as configurações abaixo na Figura 1:

  
Figura 1. Dados de configuração do arquivo vpn.ovpn

1. Configurar a placa de rede da VM para modo bridge;

Executar o OpenVPN-GUI e clicar em “connect” no menu do ícone instalado na bandeja do sistema.

O OpenVPN já está instalado nas VMs do Servidor DMC-NS e nas Máquinas Virtuais das estações da sala 01 do LIICT, tanto na Máquina Virtual Ubuntu Server, quanto na Windows Server 2008. A Figura 2 mostras a VPN funcionando entre as máquinas virtuais.

  
Figura 2. Mostrando a VPN funcionando entre as máquinas virtuais.

**AVALIAÇÃO DO APRENDIZADO**

1. Que tipos de VPN você pode construir ?

1. Que tipo de criptografia foi usada na sua VPN ?
2. Que protocolo foi utilizado na construção de sua VPN ?
3. Para que serviu Diffie-Helmann na construção da sua VPN ?
4. Em que situação seria melhor usar criptografia de chave pública ?

6. Nenhuma VPN [e totalmente segura. Então, devemos configurar com   
 cuidado todos os serviços necessários pata termos uma VPN estável e   
 sem riscos. Qual medida você tomaria, junto com seus gateways VPN,   
 para ter um mínimo de segurança necessária ?

**CONCLUSÃO**

Posteriormente, você deve ler o material sobre SSL, entregue em sala de aula, para entender melhor o funcionamento deste protocolo.

O SSL v3 chama-se TLS e é um protocolo que tende a substituir o SSL, possuindo segurança mais avançada.