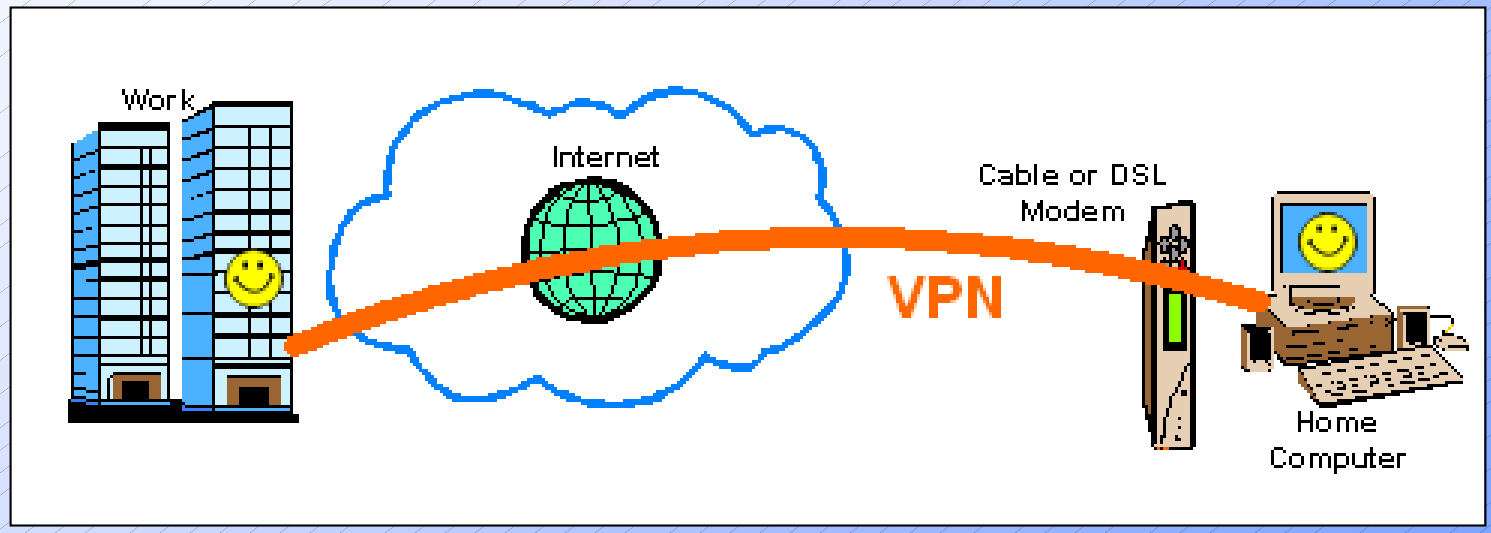
Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística
Pós-Graduação em Ciência da Computação

Virtual Private Network – VPN com Certificado Digital

Clytia Higa Tamashiro

Prof. João Bosco Mangueira Sobral

Virtual Private Network



Prática

- X.509
  - Biblioteca OpenSSL
- OpenVPN
  - Open source
  - OpenSSL
  - Segurança SSL/TLS
  - Interface de rede virtual TUN/TAP

Passos

- Criação da autoridade certificadora (AC)
- Requisição e emissão dos certificados digitais
- Geração dos parâmetros Diffie-Hellman
- Instalação e configuração da VPN
- Execução e teste da VPN

Criação da AC

- Edição do arquivo openssl.cnf
- Geração da chave privada e do certificado da AC
  - openssl req –new –x509 –keyout ca.key –out ca.crt –days 3650

Requisição e emissão dos certificados digitais

- Requisição do certificado
  - openssl req –new –keyout escritorio.key –out escritorio.csr
- Emissão do certificado
  - openssl ca –out escritorio.crt –in escritorio.csr

Parâmetros Diffie Hellman

- Criação dos parâmetros
  - openssl dhparam –out dh1024.pem 1024

Instalação e Configuração VPN

- Biblioteca OpenSSL e módulo TUN/TAP devem estar instalados
- Instalação OpenVPN
- Arquivos de configuração
  - office.conf
  - home.conf

Execução e Teste da VPN

- Inicialização da VPN
  - modprobe tun
  - openvpn – –config office.cnf
  - openvpn – –config home.cnf
- Teste da VPN
  - Ping
  - Programa socket em C
  - Sniffer

Referências

- OpenVPN: http://openvpn.net/
- OpenSSL: http://www.openssl.org/
- Sniffer APS: http://www.swrtec.de/swrtec/clinux/aps.php
- Stallings, William. Cryptography and Network Security. Principles and Practice. 2 ed., 1999.
- http://www.rnp.br/newsgen/9811/vpn.html
- http://www.homenethelp.com/vpn/