



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

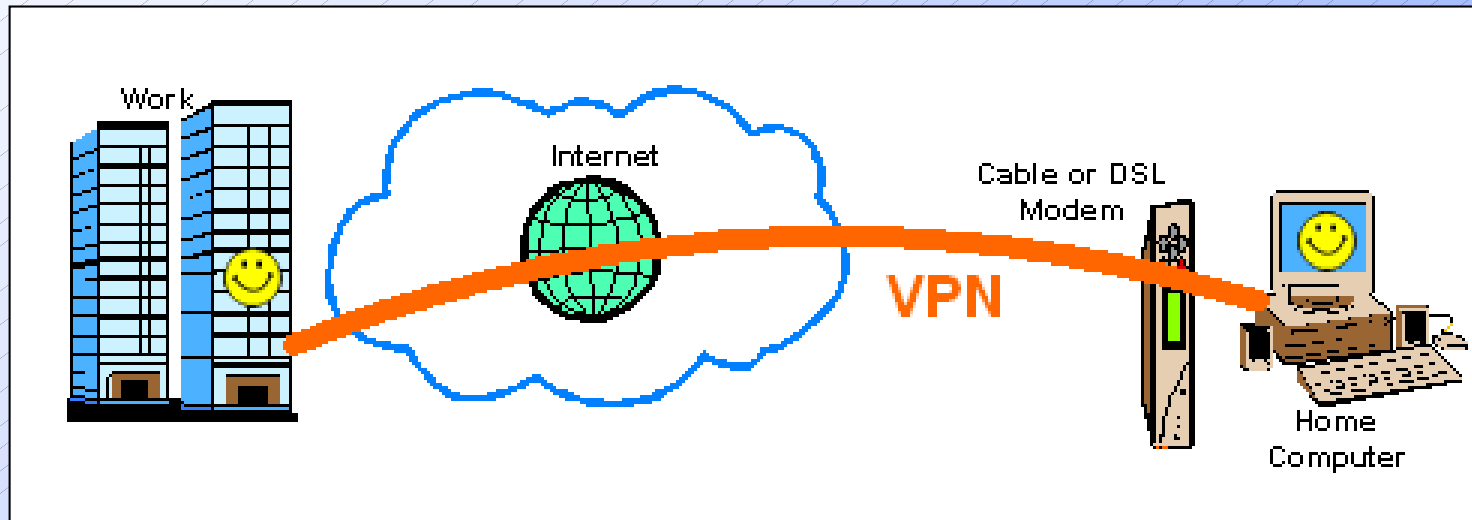
# **Virtual Private Network – VPN com Certificado Digital**

**Clytia Higa Tamashiro**

**Prof. João Bosco Manguiera Sobral**

# Virtual Private Network

---



# Prática

---

- X.509

- Biblioteca OpenSSL

- OpenVPN

- Open source
- OpenSSL
- Segurança SSL/TLS
- Interface de rede virtual TUN/TAP

# O termo VIRTUAL

---

- **Virtual**

Palavra que designa “parece existir, mas na realidade não existe”.

# Interface de rede virtual TUN/ TAP

---

- TUN Universal Driver.
- É um dispositivo de rede ponto-a-ponto **virtual**.
- O driver TUN foi projetado como suporte de baixo nível de kernel, para tunelamento IP.

# Interface de rede virtual TUN/ TAP

---

- TAP Universal Driver.
- É um dispositivo de rede Ethernet.
- O driver TAP foi projetado como suporte de baixo nível de kernel, para tunelamento Ethernet virtual.

# Interface de rede virtual TUN/ TAP

---

- Quais plataformas que dão suporte a TUN/TAP ?
  - Linux kernels: 2.2.x e 2.4.x
  - FreeBSD 3.x, 4.x e 5.x
  - Solaris 2.6, 7.0 e 8.0

# Interface de rede virtual TUN/ TAP

---

- Propósito:

O principal propósito do driver TUN/TAP é o tunelamento.

- Usado po VTUN

<http://vtun.netpdia.net>



# Interface de rede virtual TUN/ TAP

---

- Como o driver TUN/TAP trabalha ?

Um dispositivo de rede virtual pode ser visto como um simples ponto-a-ponto dispositivo ou um dispositivo Ethernet, ...

# Interface de rede virtual TUN/ TAP

---

- ... .. o qual ao invés de receber pacotes de um meio físico, recebe esses de um programa de usuário, ... ..

# Interface de rede virtual TUN/ TAP

---

- ... .. e ao invés de enviar pacotes via um meio físico, envia esses para um programa de usuário.

# Interface de rede virtual TUN/ TAP

---

- Qual é a diferença entre TUN driver e TAP driver ?

TUN trabalha com pacotes IP.

TAP trabalha como frames (quadros) Ethernet.

# Interface de rede virtual TUN/ TAP

---

VTUN

TCP/UDP

IP

TAP

Kernel

VTUN

TCP/UDP

IP

TAP

Kernel

# Tarefas

---

- Open VPN sobre Windows
- Open VPN sobre Linux
- VPN sem segurança.
- VPN com segurança:
  - VPN com chave simétrica
  - VPN com chave assimétrica

# 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/>