Comunicação Segura em Canais Inseguros com OpenVPN

Ricardo Kléber M. Galvão
(rk@ufrn.br)

Helder Jean Brito da Silva
(helder@info.ufrn.br)

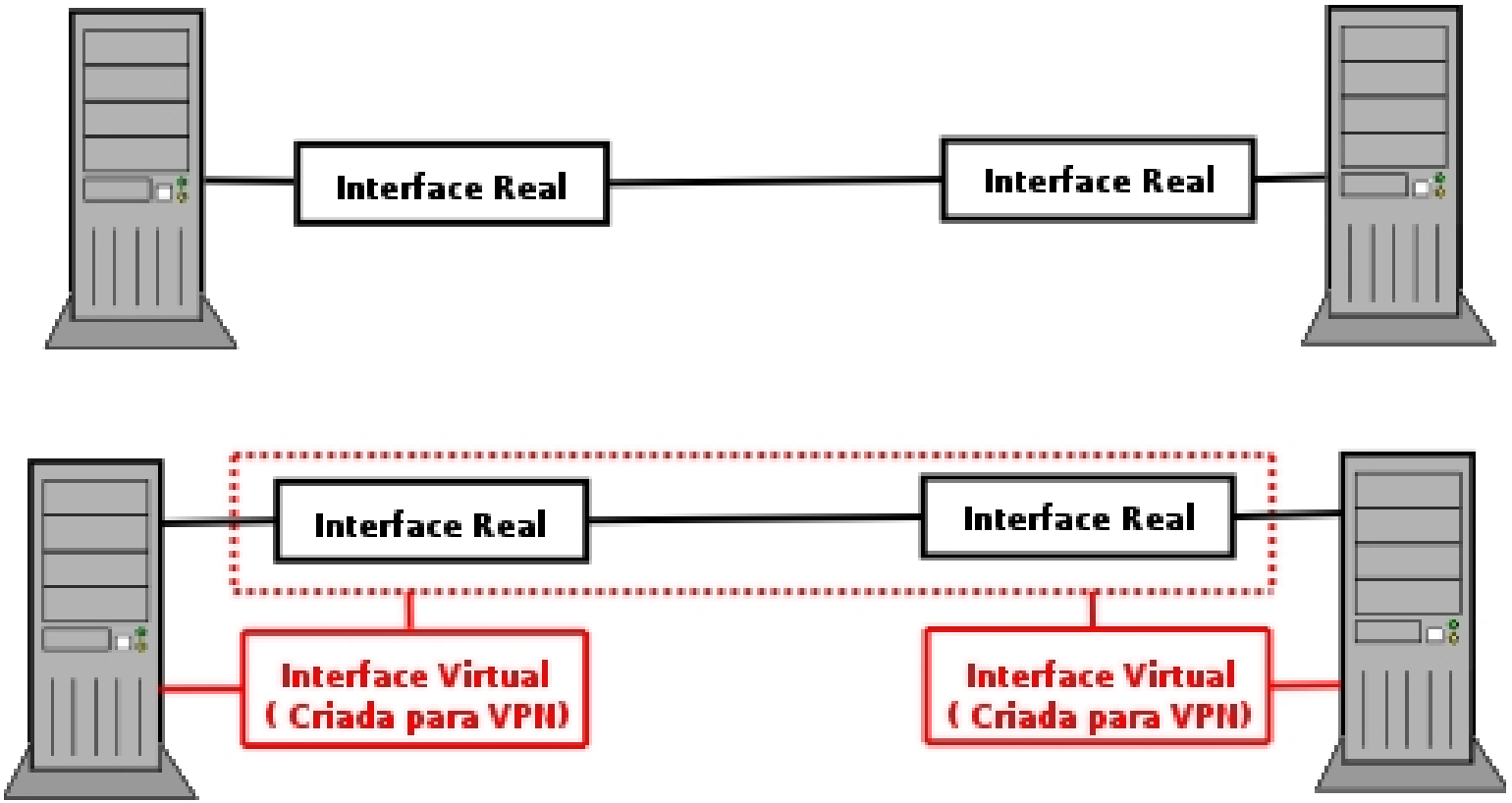
UFRN - SINFO NARIS
http://naris.info.ufrn.br

Núcleo de Atendimento e
Resposta a Incidentes de Segurança

VPNs (Redes Vituais Privadas)

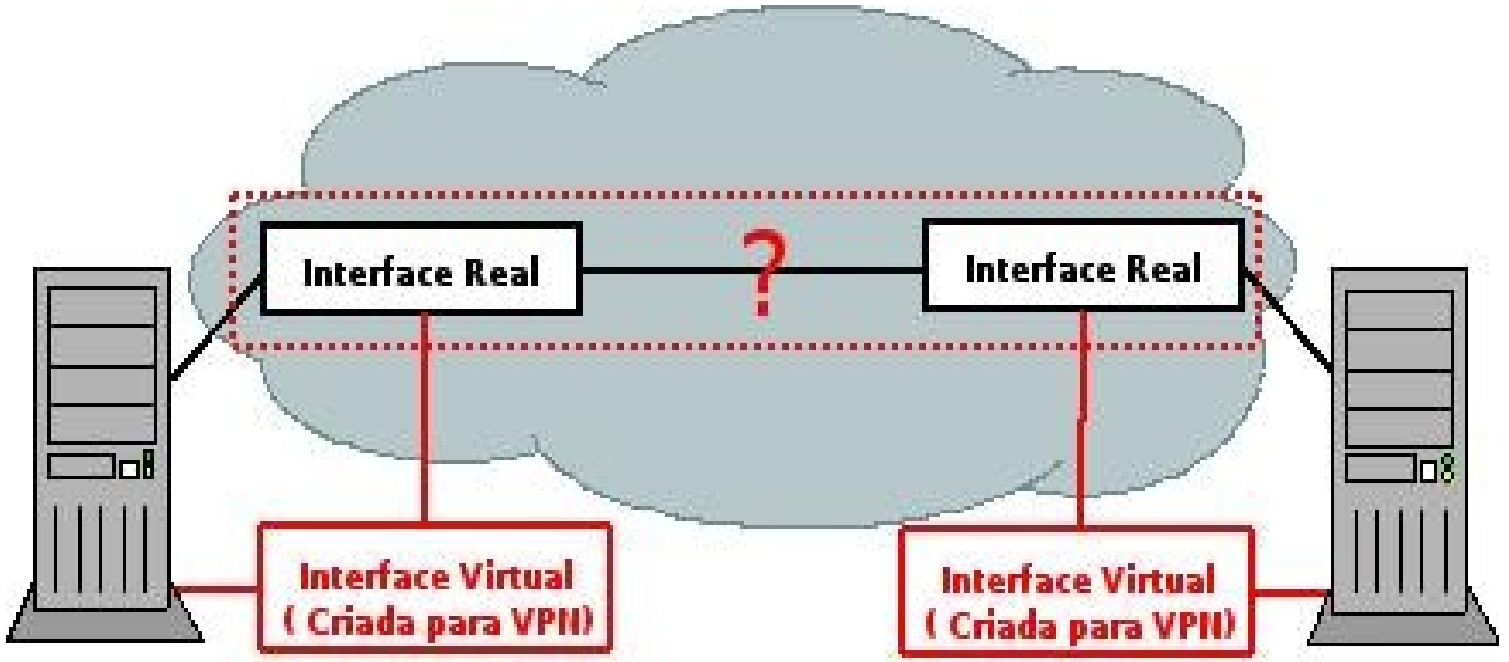
Contextualizando

- **Túneis virtuais**
  - Interfaces virtuais sobre interfaces reais



VPNs (Redes Vituais Privadas)
Contextualizando

- **Geralmente utilizadas em redes públicas** (Internet p.ex.)
  - Embora possa ser utiliza entre máquinas em uma rede privada



VPNs (Redes Vituais Privadas)
Contextualizando

Outras Características

- **Geralmente usam criptografia**
  - **Porém não necessariamente (túneis não encriptados)**
- **Podem utilizar, ainda, compactação**
  - **Redução do tráfego tunelado (aconselhável em links saturados)**
  - **Necessário avaliar retardo da compactação**

VPNs (Redes Vituais Privadas)
Contextualizando

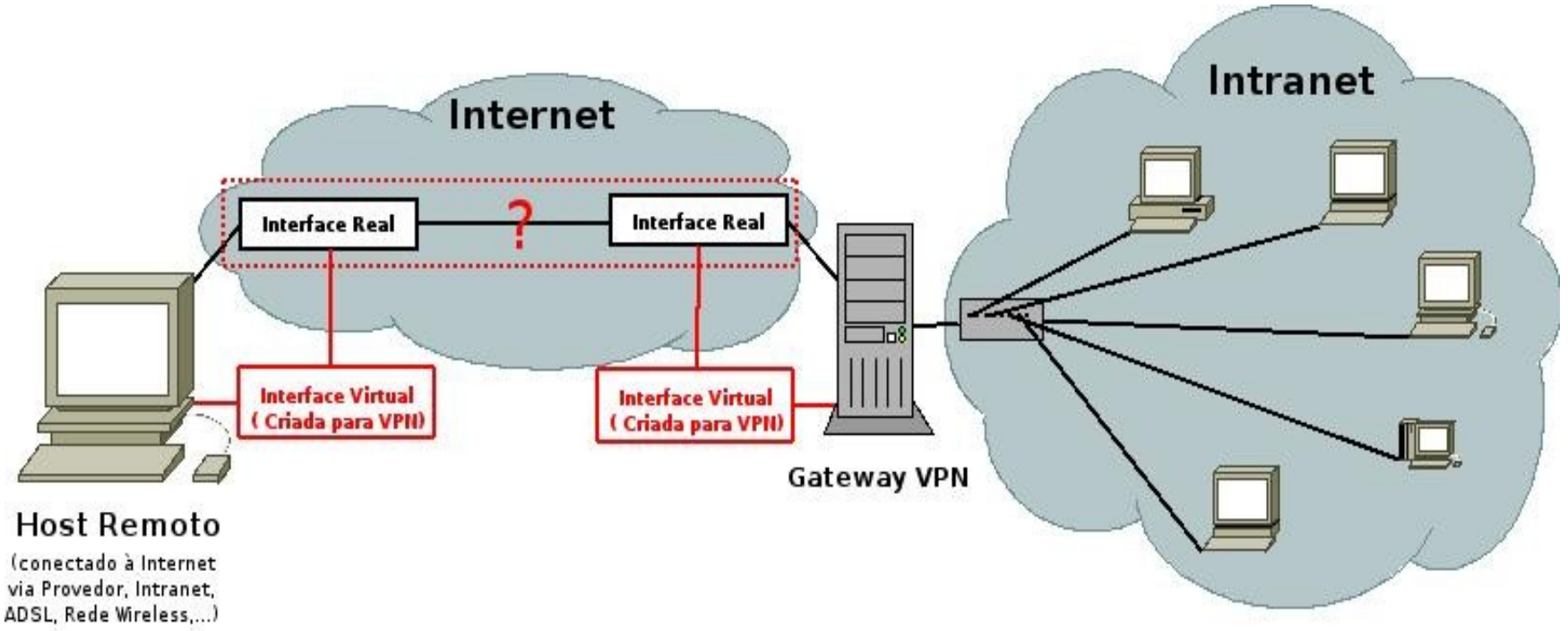
Vantagens de Utilização

- **Redes fisicamente separadas podem ser vistas logicamente como uma única rede**
  - **Facilitando a administração**
- **Com o uso da criptografia, têm-se canais seguros, mesmo sobre canais inseguros**
  - **Redução de custos (substituição de linhas privadas p.ex.)**
  - **Foco desta apresentação**

VPNs (Redes Vituais Privadas)

Cenários de Implementação

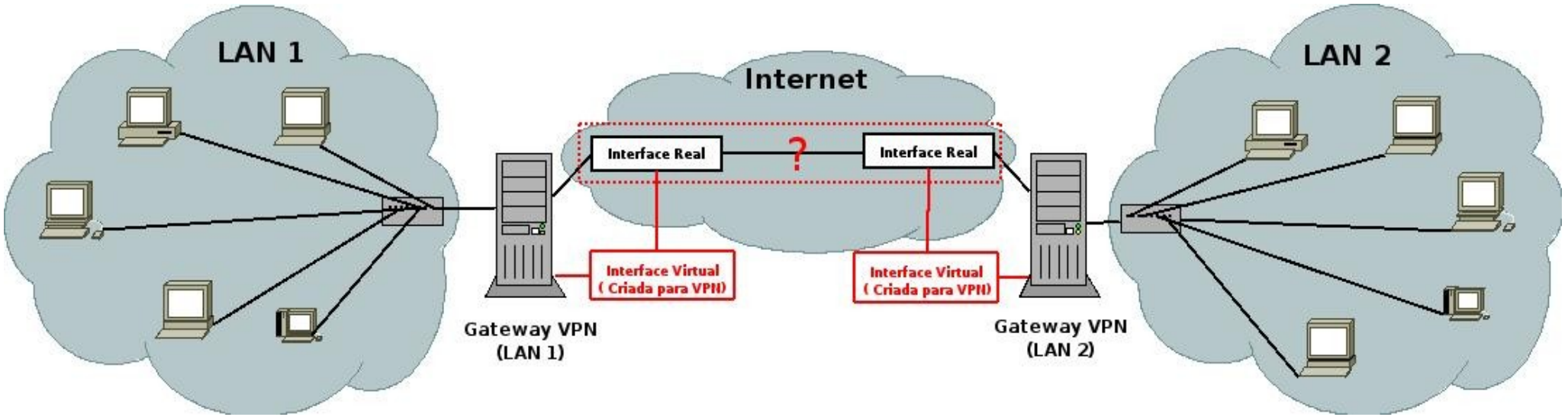
Acesso Remoto via Internet



VPNs (Redes Vituais Privadas)

Cenários de Implementação

Conexão de LANs

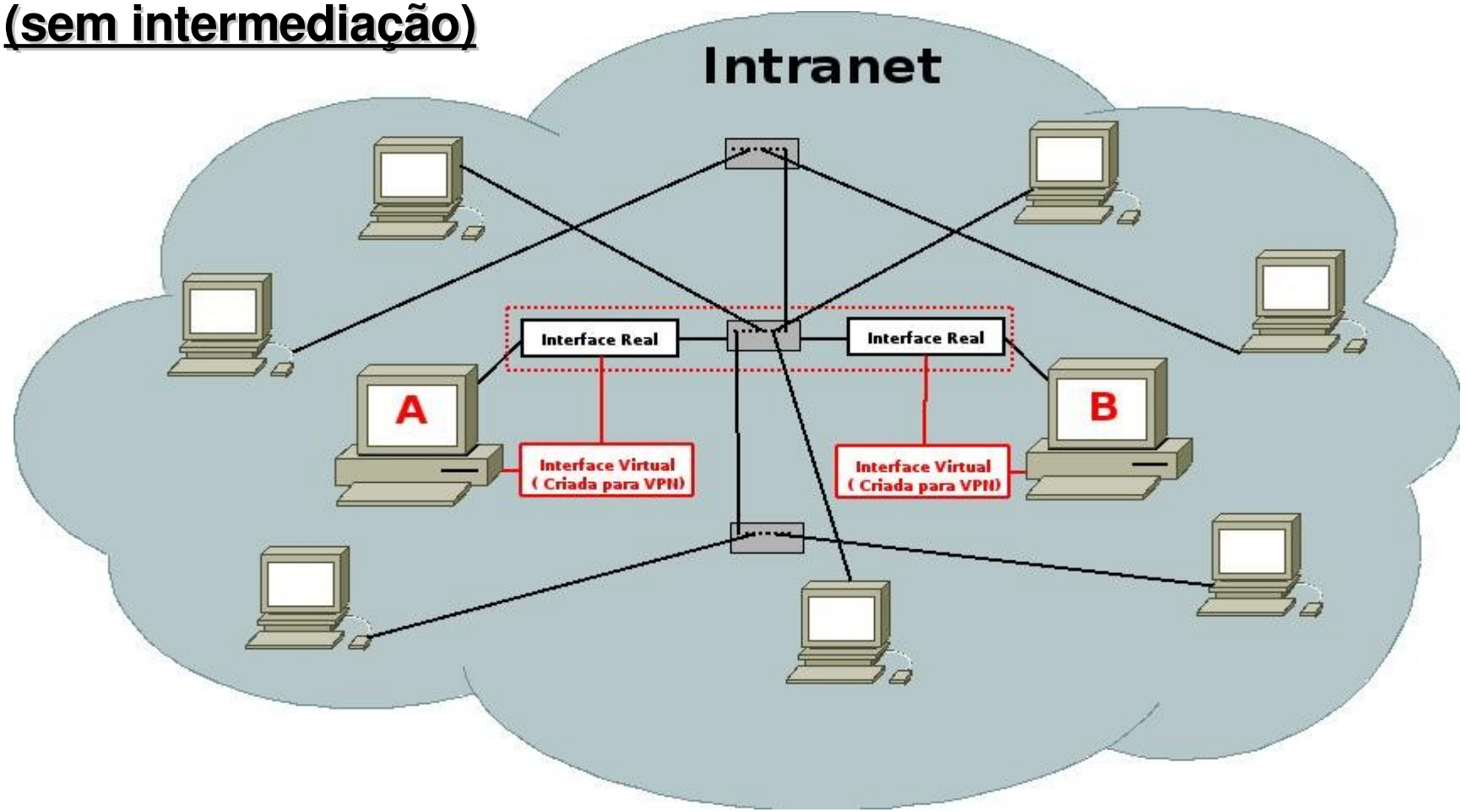


VPNs (Redes Vituais Privadas)

Cenários de Implementação

Conexão de Hosts em uma mesma Intranet

(sem intermediação)

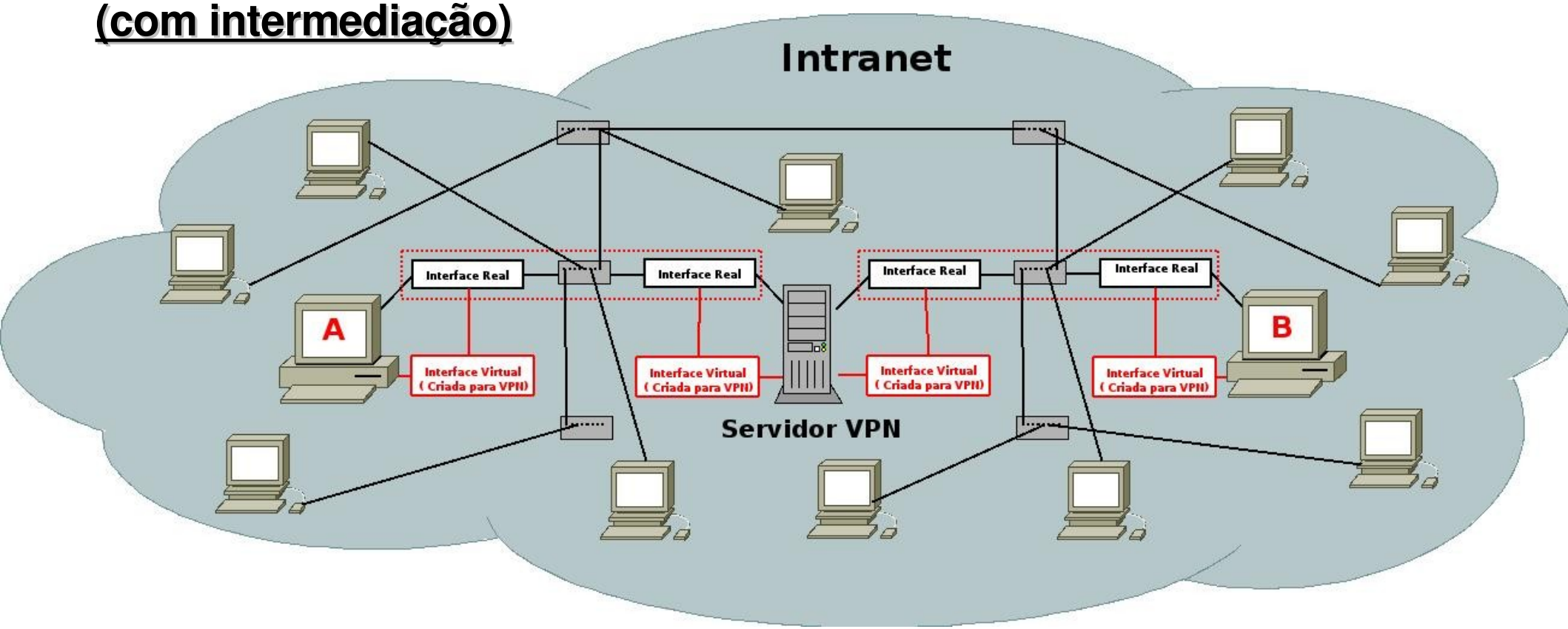


VPNs (Redes Vituais Privadas)

Cenários de Implementação

Conexão de Hosts em uma mesma Intranet

(com intermediação)



Softwares para Implementação de VPNs

FreeSwan

(www.freeswan.org)

Uso do IPSec para tunelamento

- Nativo no IPv6, necessário instalar no Ipv4
- Modificação nos cabeçalhos dos datagramas Ipv4
- Apresenta problemas para estações em mascaradas (NAT)
- Descontinuado (última versão (2.06) de 22/04/2004)
- Sucedido pelo OpenSwan (www.openswan.org)
- Voltado para VPNs entre LANs

Softwares para Implementação de VPNs

PPTP – Pont-to-Point Tunneling Protocol (www.pptp.org)

- Criado pela Microsoft
  - Nativo desde o Windows95
- Baseado no protocolo GRE (nível de rede)
  - Problemas com NAT e liberação em firewalls
- Criptografia de 128 bits
- Versões anteriores ao Windows 2000 sem patch = 40 bits

Softwares para Implementação de VPNs

Outras Opções:

- **Vtun – Virtual Tunnel** (http://vtun.sourceforge.net)
- **Cipe – Crypto IP Encapsulation** (http://sourceforge.net/projects/cipe-linux)
- **Vpnd – Virtual Private Network Daemon** (http://vpnd.dotsrc.org)
- **Tinc** (http://www.tinc-vpn.org)
- **Secvpn – Secure Virtual Private Network** (http://alioth.debian.org/projects/secvpn)
- **Yavipin** (http://yavipin.sourceforge.net)

OpenVPN

http://openvpn.net

Principais Características

- Utiliza os protocolos SSL/TLS
- Flexibilidade (uso de TCP ou UDP)
- Implementa todos os cenários apresentados
- Clientes também para Windows (texto ou gráfico)
- Uso de chaves ao invés de usuário/senha
- Plataformas: Linux, Windows (a partir do 2000), OpenBSD, FreeBSD, NetBSD, MacOS X e SunOS/Solaris

Instalação a partir do fonte:

- Baixar o fonte (Versão 2.0.9 de 01/10/2006):
  - `http://openvpn.net/release/openvpn-2.0.9.tar.gz`
- Descompactar em /usr/src e proceder instalação:
  - `./configure; make; make install`

Instalação no Linux Debian:

- `apt-get install openvpn`

OpenVPN

Arquivos Importantes

Servidor

- Arquivo de Configuração do Servidor
- Certificado da Entidade Certificadora (CA)
- Chave Pública da Entidade Certificadora (CA)
- Certificado do Servidor
- Chave Pública do Servidor

Cliente

- Arquivo de Configuração do Cliente
- Certificado da Entidade Certificadora (CA)
- Certificado do Cliente
- Chave Privada do Cliente

Scripts para Automatizar Tarefas

- **O processo de configuração inicial era o mais trabalhoso**
  - Geração dos parâmetros Diffie-Hellman (utilizado para a troca de chaves)
  - Geração manual e assinatura das chaves CA
  - Criação manual das chaves do servidor e dos clientes

- **Atualmente...**
  - Scripts (`/usr/share/doc/openvpn/examples/easy-rsa`)
  - Arq.Configuração (`/usr/share/doc/openvpn/examples/sample-config-files`)

Diretório Padrão e Cópia de Scripts e Arquivos:

- **Criação de diretório padrão:**
  - `mkdir /etc/openvpn`
- **Cópia dos scripts para o diretório padrão:**
  - `cd /etc/openvpn`
  - `cp /usr/share/doc/openvpn/examples/easy-rsa .`
  - `cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf .`

OpenVPN

Geração do Certificado e Chave da CA

- Editar o arquivo **vars** e personalizar informações:

```
export KEY_COUNTRY="BR"
export KEY_PROVINCE="RN"
export KEY_CITY="Natal"
export KEY_ORG="SINFO-UFRN"
export KEY_EMAIL="naris@info.ufrn.br"
```

- Carregar variáveis e gerar certificado da CA:

```
# . ./vars
# ./clean-all
# ./build-ca
```

Informar Common Name:

- CA-OpenVPN

Arquivos Gerados:

- ca.crt
- ca.key

OpenVPN

Geração de Certificado e Chave do Servidor

- **Executar o script para geração dos arquivos:**

```
# ./build-key-server server
```

- **Informar como Common Name: `server`**
- **Responder "`y`" na solicitação: "`Sign the certificate? [y/n]`"**
- **Arquivos gerados:**
  - `server.crt`
  - `server.key`

OpenVPN

Geração de Certificados e Chaves dos Clientes

- **Executar para cada cliente:**

```
# ./build-key nome_do_cliente
```

- **Informar como Common Name:** `nome_do_cliente`
- **Cada cliente deve ter um Common Name distinto**
- **Arquivos gerados:**
  - `nome_do_cliente.crt`
  - `nome_do_cliente.key`

Com estes procedimentos os clientes serão autenticados baseando-se apenas em seus certificados. Para utilizar autenticação baseada em certificado e senha, utilizar o script `build-key-pass`

OpenVPN

Geração dos Parâmetros Diffie-Helmann

- Executar o script para geração do arquivo:

```
# ./build-dh
```

- Arquivo gerado:
  - `dh1024.pem`
- Esta geração geralmente é demorada
- Para utilizar 2048 bits, modificar o arquivo `vars` antes de executar o script `build-dh`.

OpenVPN
Arquivos Importantes

Servidor

- Arquivo de Configuração do Servidor `server.conf`
- Certificado da Entidade Certificadora (CA) `ca.crt`
- Chave Pública da Entidade Certificadora (CA) `ca.key`
- Certificado do Servidor `server.crt`
- Chave Pública do Servidor `server.key`

Cliente

- Arquivo de Configuração do Cliente `client.conf`
- Certificado da Entidade Certificadora (CA) `ca.crt`
- Certificado do Cliente `nome_do_cliente.crt`
- Chave Privada do Cliente `nome_do_cliente.key`

OpenVPN

Arquivo de Configuração do Servidor

- Conteúdo do arquivo `server.conf`:

  `local 200.1.2.3` (ip do servidor)

  `port 1194` (porta padrão, porém configurável)

  `proto udp` (usar protocolo udp)

  `dev tun` (usar tap somente em vpns em nível de enlace)

  `ca ca.crt` (arquivo do certificado do CA)

  `cert server.crt` (arquivo do certificado do servidor)

  `key server.key` (arquivo da chave privada do servidor)

  `dh dh1024.pem` (arquivo com parâmetros Diffie-Helmann)

OpenVPN

Arquivo de Configuração do Servidor

- Conteúdo do arquivo `server.conf` (cont.):

```
server 10.8.0.0 255.255.255.0
```
(sub-rede da VPN)

```
push route 192.168.0.0 255.255.255.0
```
(clientes receberão rota para rede atrás do servidor)

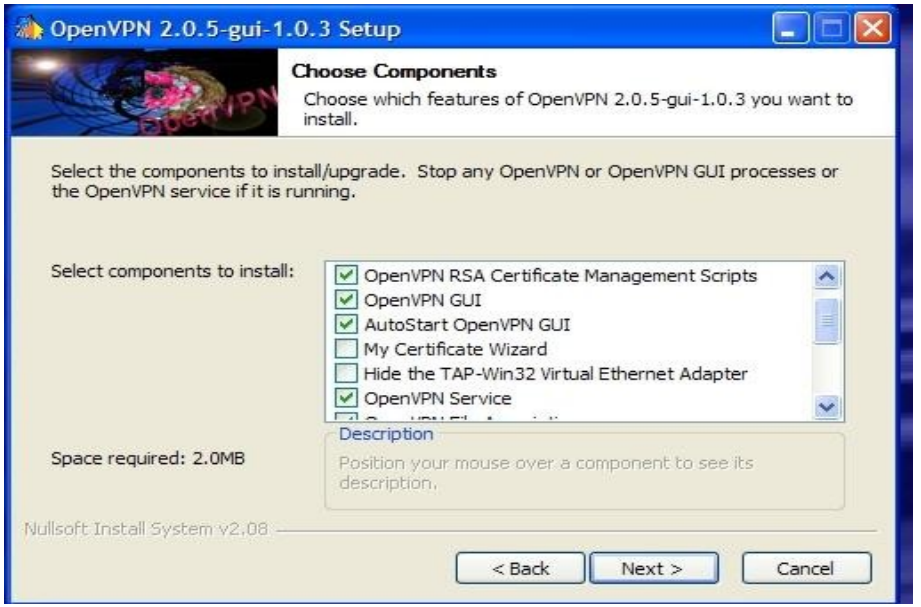
OpenVPN

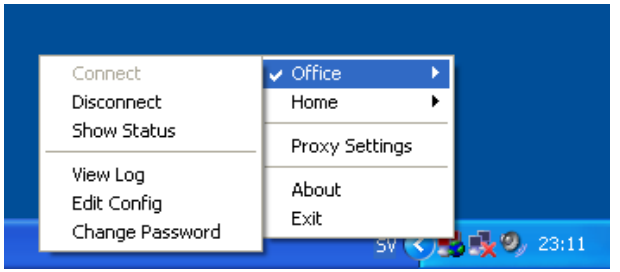
Arquivo de Configuração do Cliente

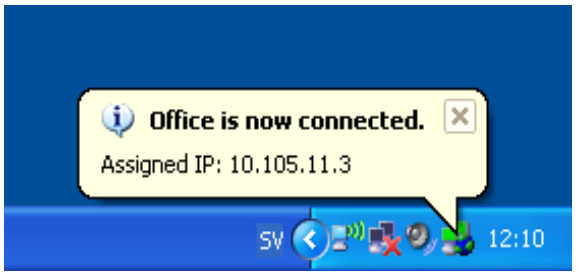
- **Conteúdo do arquivo client.conf:**

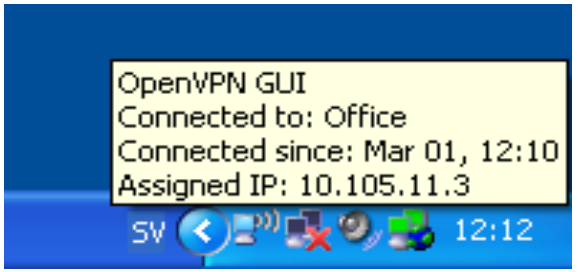
```
client  (informa que atuará como cliente na conexão)
dev tun  (usar tap somente em vpns em nível de enlace)
proto udp  (protocolo utilizado na VPN)
remote 200.1.2.3 1194  (endereço IP e porta do servidor)
ca ca.crt  (certificado do CA)
cert nome_do_cliente.crt  (certificado do cliente)
key nome_do_cliente.key  (chave privada do cliente)
```

OpenVPN
Windows GUI

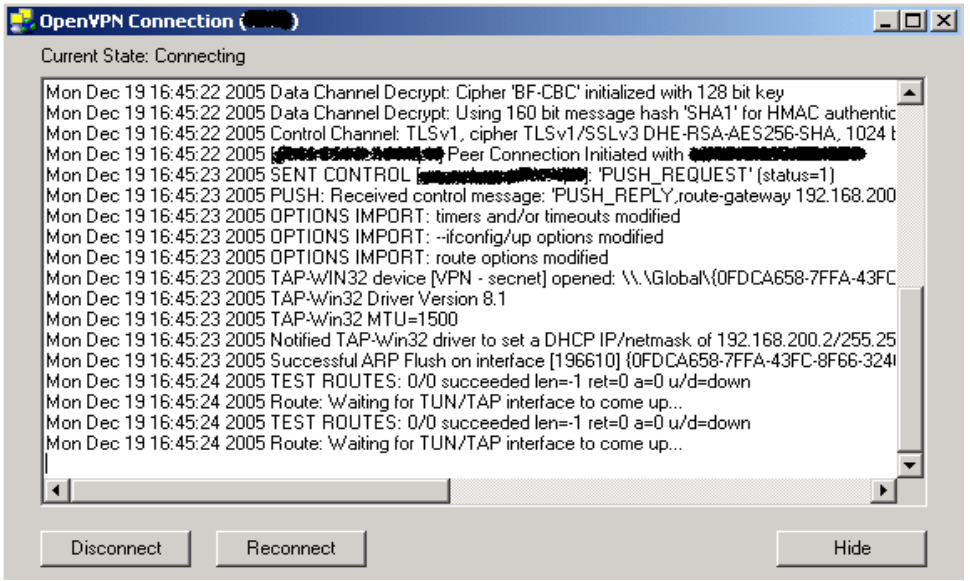


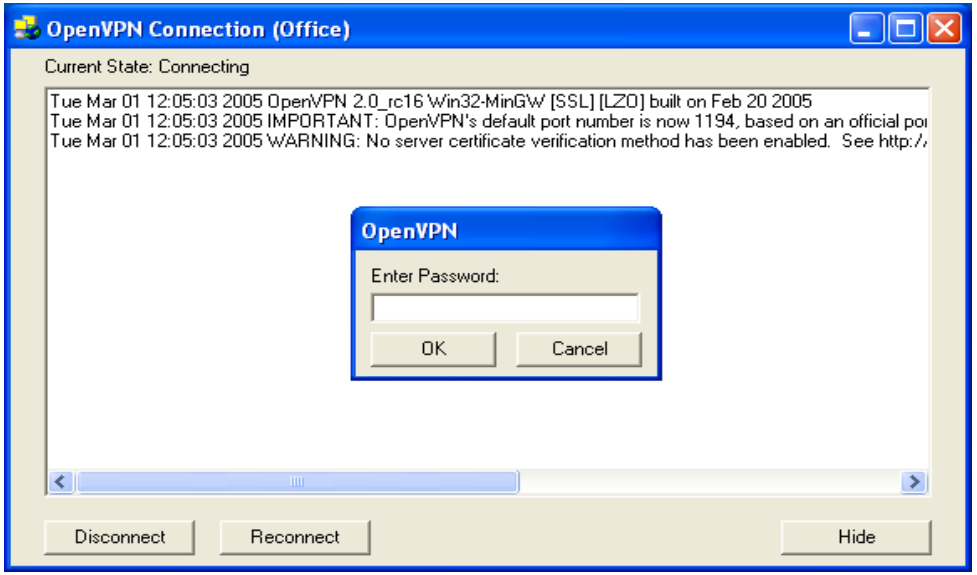






OpenVPN
Windows GUI





OpenVPN
Conectividade Total

- **Visualizando máquinas atrás de um cliente OpenVPN:**
  - **No arquivo de configuração do servidor (server.conf):**

```
client-config-dir ccd
route 192.168.100.0 255.255.255.255 (rede atrás do cliente)
```

  - **Criar um arquivo para cada cliente (dentro do sub-diretório ccd):**

```
mkdir /etc/openvpn/ccd/
touch /etc/openvpn/ccd/nome_do_cliente
```

  - **Cada arquivo informa a rota para sua rede interna:**

```
iroute 192.168.100.0 255.255.255.255 (rede atrás do cliente)
```

OpenVPN
Conectividade Total

- **Visualizando máquinas atrás de um cliente OpenVPN (cont.):**
  - **Com isso, mesmo redes atrás de clientes remotos com conexão não-permanente ficam disponíveis para acesso enquanto a VPN estiver ativa;**
  - **As rotas são inseridas somente quando o cliente estabelece a VPN e são removidas automaticamente quando a VPN é desfeita;**
  - **Desta forma um cliente remoto torna-se um gateway VPN para acesso de/para a sua rede interna.**

Uma opção deve, ainda. ser habilitada no arquivo de configuração do servidor para permitir a comunicação entre clientes VPN:

```
client-to-client
```

OpenVPN

Revogação de Certificados

- Executar o script para revogação do certificado:

```
# . vars
# ./revoke-full nome_do_cliente
```

- Verificar se o arquivo crl.pem gerado está no diretório de configuração do servidor
- Adicionar a linha abaixo no arquivo server.conf:
  - `crl-verify crl.pem`

OpenVPN
Outros Recursos

- VPNs em nível de enlace (túnel ethernet)
  - No arquivo de Configuração do servidor (server.conf):
    - Trocar a linha: `dev tun`
    - pela linha: `dev tap`
- Manter IPs de clientes nas próximas conexões:
  - No arquivo de Configuração do servidor (server.conf):
    - `ifconfig-pool-persist ipp.txt`
- Permitir mais de um cliente com mesmo certificado:
  - No arquivo de Configuração do servidor (server.conf):
    - `duplicate-cn`

OpenVPN
Outros Recursos

- **Limitando o número de clientes simultâneos**
  - **No arquivo de Configuração do servidor (server.conf):**
    - `max-clients 100` (neste caso limitando em 100)
- **Registrando logs em arquivo específico:**
  - **No arquivo de Configuração do servidor (server.conf):**
    - `log openvpn.log`

Concluindo...

- **Consolidação do OpenVPN**
  - **Flexibilidade e Robustez**
  - **GPL (General Public License)**
  - **Não exige mudanças em nível de rede**
- **Principal Desvantagem: Não oferece suporte a Win98**
- **Concorrente Direto: PPTP (nativo no Windows)**

> **"Nada é tão simples quanto parece,**
> **nem tão complicado quanto diz o manual"**
>
> ***(Corolário das Leis de Murph)***

Perguntas ???

Comunicação Segura em Canais Inseguros com OpenVPN

Ricardo Kléber M. Galvão
(rk@ufrn.br)

Helder Jean Brito da Silva
(helder@info.ufrn.br)

UFRN - SINFO NARIS
http://naris.info.ufrn.br

Núcleo de Atendimento e
Resposta a Incidentes de Segurança