



Network Service

Virtual Private Network (VPN)

Center of Electrical Engineering and Informatics
Federal University of Campina Grande

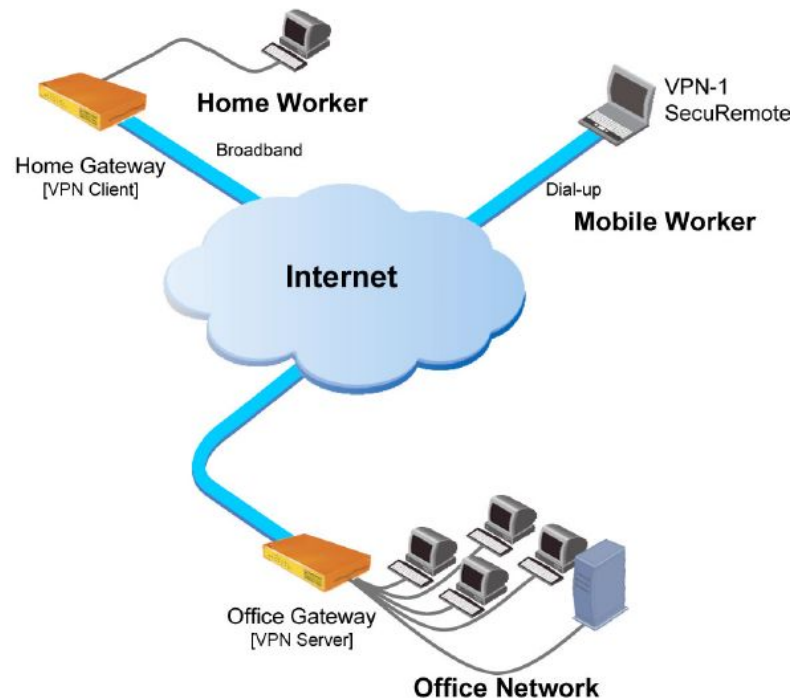


- Introdução à VPN
- Criando uma VPN
- Gerenciamento de VPN

- Uma empresa que precisa interligar suas filiais, como resolver?
 - Link via rádio
 - Link via cabo
 - Linha privada (LP)
- E se estiver em outra cidade, estado ou país?
- Como garantir a segurança?
 - VPN!

Conceito de VPN

- A VPN estabelece um túnel de comunicações seguro e criptografado entre o seu data center local e o seu VPC na Vivo CLOUD
- Ele permite que você estenda seus data centers diretamente para o Vivo CLOUD



- Acesso a VPN
 - Fornece conectividade remota aos funcionários e permite que eles usem o serviço de acesso VPN quando estão em viagens de negócios
- Intranet VPN
 - Conecta diferentes sites ou escritórios das empresas em uma rede pública usando conexões dedicadas
- Extranet VPN
 - Vincula parceiros ou organizações confiadas à intranet corporativa usando conexões dedicadas

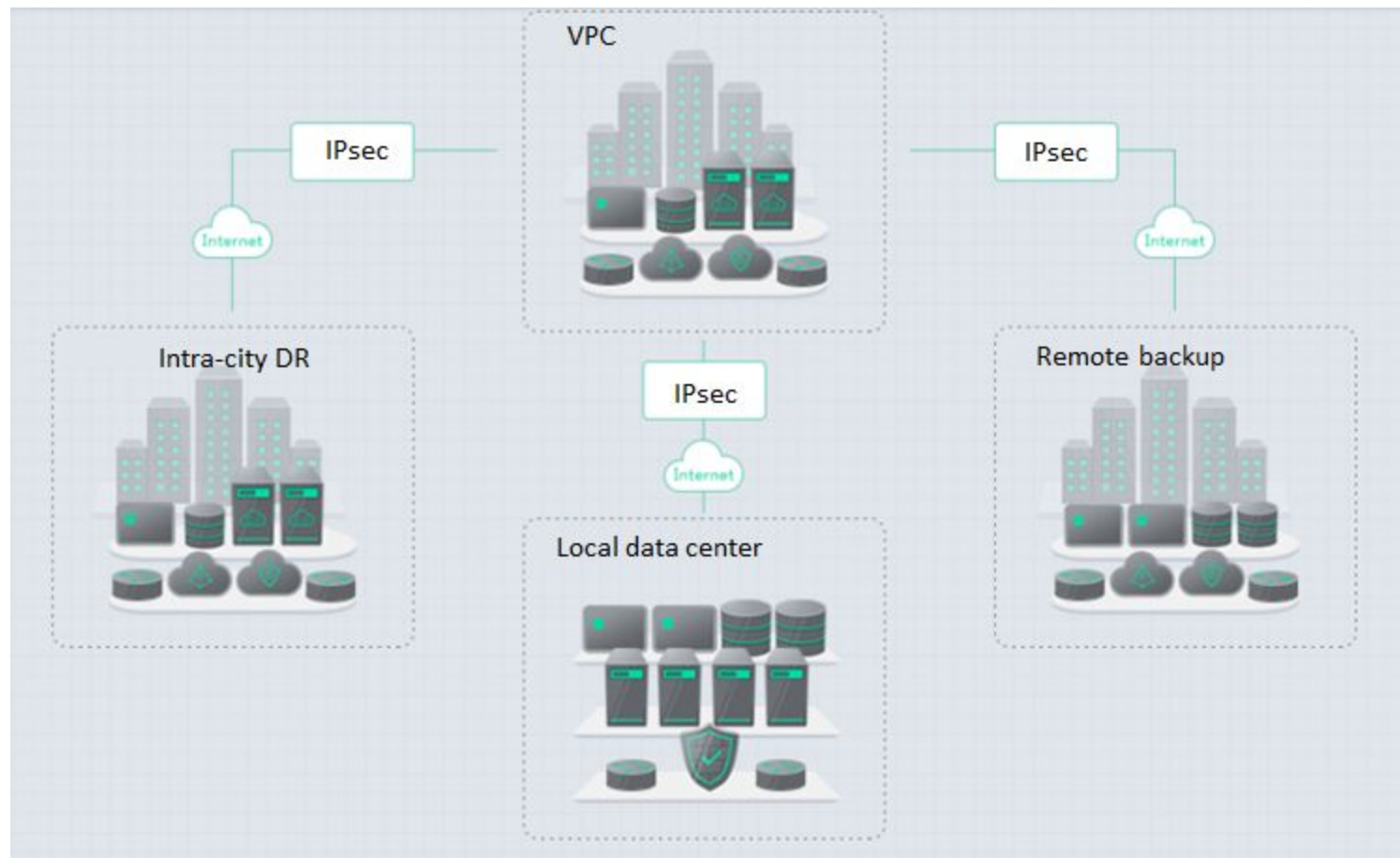
- VPN via tunelamento de camada 3
 - Funciona na camada de rede, como VPNs usando os protocolos GRE e IPsec. Atualmente, apenas a VPN IPsec é suportada
- VPN via tunelamento de camada 2
 - Funciona na camada de enlace de dados, como VPNs usando protocolos L2TP e PPTP

- O Internet Protocol Security (IPsec) é uma estrutura de padrões abertos desenvolvida pela Internet Engineering Task Force (IETF)
- O IPsec usa serviços de segurança criptográficos e algoritmos de hash para proteger as comunicações através de redes IP (Internet Protocol)
- O IPsec garante a integridade dos dados, a confidencialidade dos dados e a autenticação de origem dos pacotes de dados pela Internet
- O IPsec funciona na camada IP

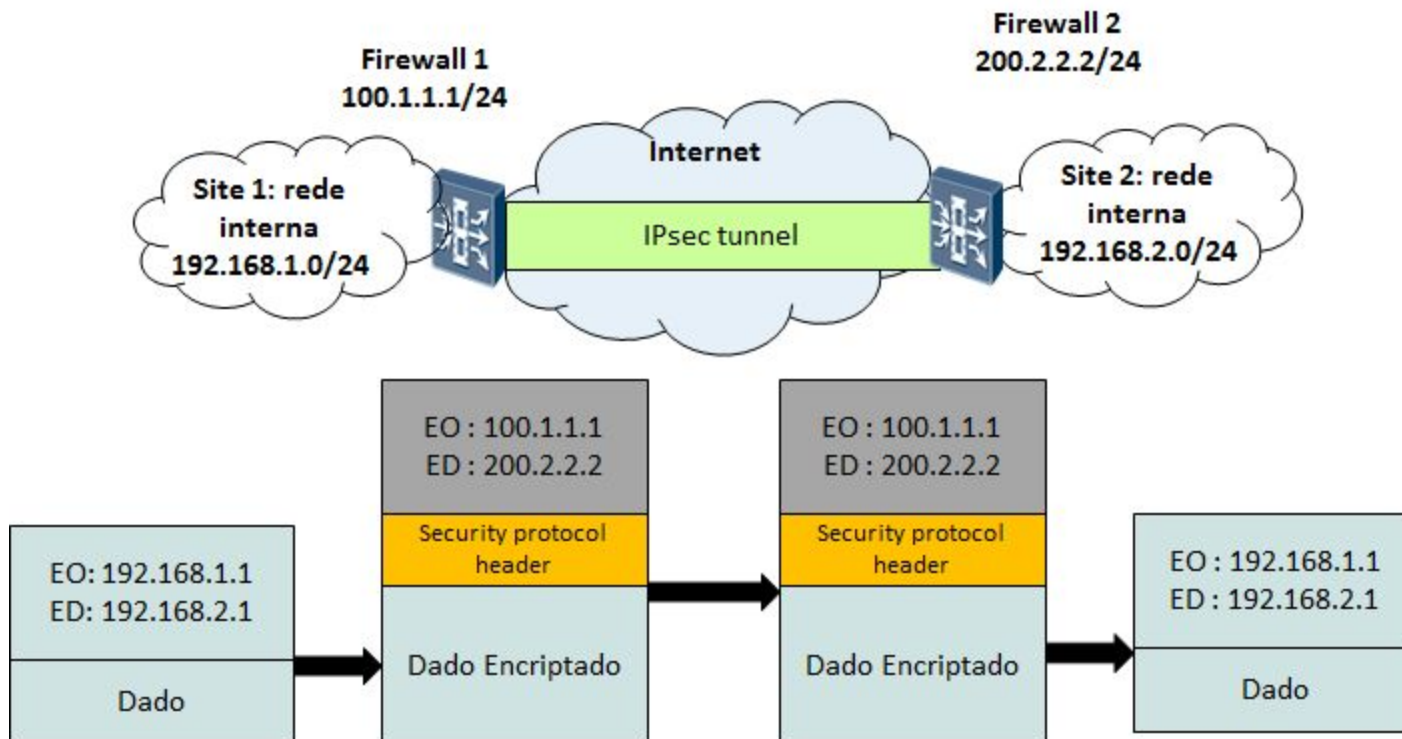
- O IPsec é um framework com vários protocolos, incluindo:
 - AH (Authentication Header) fornece integridade de dados e autenticação de origem de dados para datagramas IP
 - O ESP (Encapsulating Security Payload) fornece serviços de confidencialidade, autenticação de origem de dados e anti-interceptação na camada IP
 - A SA (Security Associations) registram a política e os parâmetros de política de cada túnel IPsec, incluindo protocolos usados para proteger pacotes de dados, modos de transcodificação, chaves e períodos de validade de chaves. As SAs são necessárias para as operações AH e ESP
 - O IKE (Internet Key Exchange) é usado para executar autenticação mútua e estabelecer e manter SA

- Estendendo seus aplicativos para a nuvem
 - Estabelecendo conexões VPN entre VPCs e seus data centers, você pode implantar aplicativos na Vivo CLOUD e serviços de banco de dados em seus data centers
- Estendendo sua rede de data center para a nuvem
 - Ao conectar a VPC e sua rede corporativa usando conexões VPN, você pode estender as capacidades de computação na camada de aplicativo, aproveitando a escalabilidade e a elasticidade da nuvem
- Implementando a recuperação remota de desastres (DR):
 - Com as conexões VPN, você pode implantar aplicativos na nuvem e em seus data centers, obtendo DR remoto

Arquitetura IPsec VPN



Exemplo de IPsec VPN



- Introdução à VPN
- Criando uma VPN
- Gerenciamento de VPN

Criando uma VPN



- É necessário um Data center com servidor VPN IPsec configurado
- Limite de 2 VPNs por região

1 Especificar detalhes

2 Confirmar especificações

3 Concluir

Informações básicas

Região **NA Mexico 1** Para selecionar uma região diferente, use o seletor de regiões no canto superior esquerdo da barra de menus principal.

* Nome

* VPC

* Sub-rede local **Usar Existente** Especificar CIDR

* Porta de ligação remota

* Sub-rede remota

* PSK

* Confirmar PSK

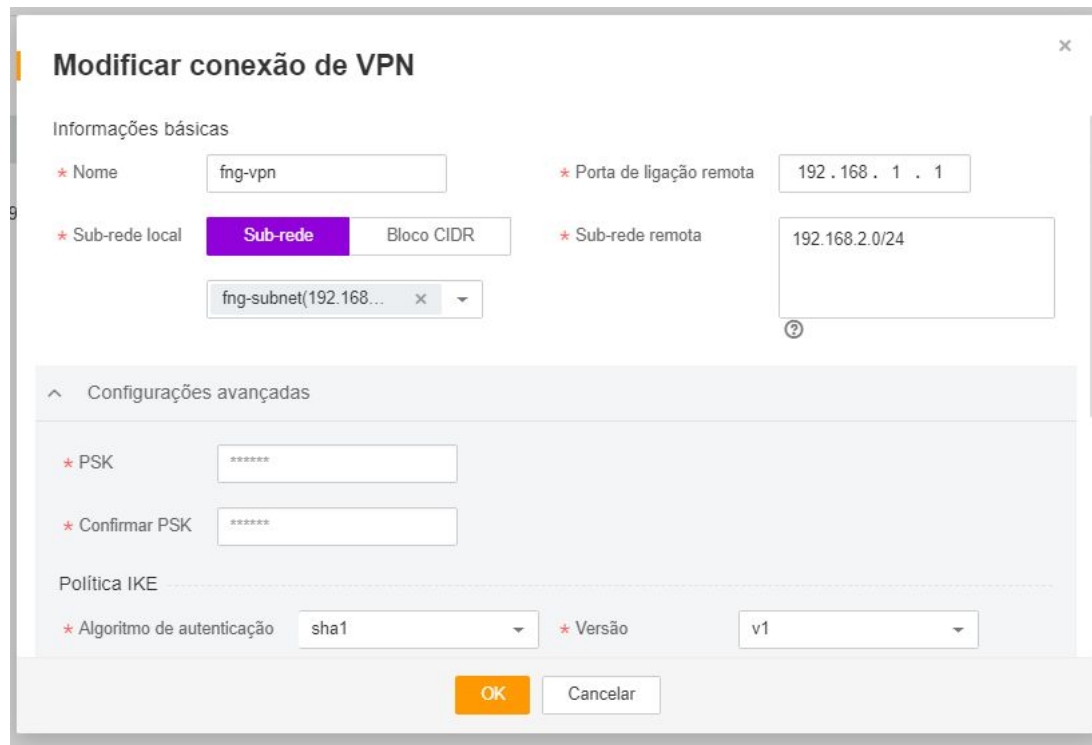
Configurações avançadas **Padrão** Personalizado

- Região
 - Localidade de VPN. Por exemplo, SA Brazil 1
- Nome
 - Identificador único por região. Exemplo: vpn-sp
- VPC
 - VPC que terá acesso a conexão VPN
- Sub-rede local
 - Sub-redes da VPC que podem se comunicar através da VPN
- Gateway remoto
 - Endereço IP público da VPN no seu datacenter ou na rede privada.

- Sub-rede remota
 - Sub-redes do seu datacenter ou rede privada para comunicação com o VPC. Deve ser diferente da **Sub-rede local**
- PSK (Pre-shared key)
 - Senha usada para se conectar na VPN. Deve ter entre 6 e 128 caracteres
- Política IKE
 - Algoritmos de criptografia e autenticação a serem usados na fase de negociação de um túnel IPsec.
- Diretiva IPsec
 - Protocolo, o algoritmo de criptografia e o algoritmo de autenticação a serem usados na fase de transmissão de dados de um túnel IPsec
- O IKE e IPsec devem ser idênticos no servidor e no cliente

- Introdução à VPN
- Criando uma VPN
- Gerenciamento de VPN

- Além de excluir uma VPN é possível modificar todos os parâmetros definidos na criação da mesma
- Inclusive a Chave Compartilhada, Política IKE e Diretiva IPsec



Modificar conexão de VPN

Informações básicas

* Nome: fng-vpn

* Porta de ligação remota: 192.168.1.1

* Sub-rede local: **Sub-rede** Bloco CIDR

fng-subnet(192.168... x

* Sub-rede remota: 192.168.2.0/24

Configurações avançadas

* PSK: *****

* Confirmar PSK: *****

Política IKE

* Algoritmo de autenticação: sha1

* Versão: v1

OK Cancelar

- Em caso de problemas de conexão é possível verificar facilmente os parâmetros definidos em busca de erros

Detalhes da política

Política IKE

Algoritmo de autenticação:	sha1	Versão:	v1
Algoritmo de criptografia:	aes-128	Ciclo de vida (sec):	86.400
Algoritmo DH:	group5	Modo de negociação:	main

Diretiva IPsec

Algoritmo de autenticação:	sha1	Protocolo de transferência:	esp
Algoritmo de criptografia:	aes-128	Ciclo de vida (sec):	3.600
Algoritmo DH:	group5		



Contact

Angelo Perkusich, D.Sc.

Professor, CEO

angelo.perkusich@embedded.ufcg.edu.br

+55 83 8811.9545

Hyggo Almeida, D.Sc.

Professor, CTO

hyggo.almeida@embedded.ufcg.edu.br

+55 83 8875.1894

Rohit Gheyi

Professor, Program Manager

rohit.gheyi@embedded.ufcg.edu.br

+55 83 8811 3339

