

# VPN as a Service

Stefano Nicotri  
INFN - Sezione di Bari

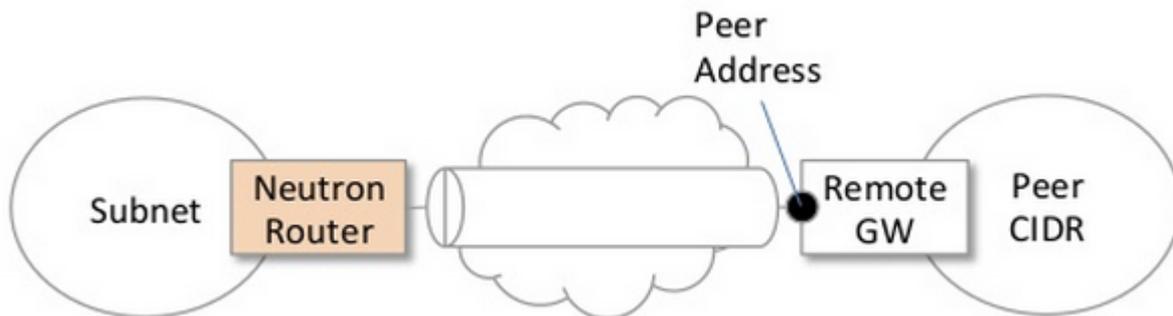
# Outline

- **Descrizione**
  - **VPN as a Service in OpenStack**
  - **Caratteristiche**
  - **Terminologia**
- **Installazione & configurazione**
- **Uso**
  - **Creazione di una IKE Policy**
  - **Creazione di una IPSec Policy**
  - **Creazione di un VPN Service**
  - **Creazione di una VPN Site Connection**

# Descrizione

# VPN as a Service in OpenStack

- Possibilità di connettere reti private, appartenenti a tenant diversi, tra di loro e con la rete pubblica
- connessione sicura
- Possibilità di connessione anche fra siti distribuiti geograficamente.



# VPN as a Service - Caratteristiche

- VPN Site-to-site
- uso della suite di protocolli **IPsec** (Internet Protocol **security**)
  - crittografia **3des**, **aes-128**, **aes-256** e **aes-192**
  - autenticazione **sha1**
  - transform protocol **ESP**, **AH** o **AH-ESP**
  - metodo di incapsulamento **tunnel** o **transport**
- crittografia attraverso **IKE policy** (Internet **Key Exchange**) v1
  - crittografia **3des**, **aes-128**, **aes-256** e **aes-192**
- Dead-Peer-Detection

# VPN as a Service - Terminologia

- **IKE Policy** - Internet Key Exchange Policy
  - identifica gli algoritmi di autenticazione e crittografia usati durante le fasi 1 e 2 della negoziazione di una connessione VPN
- **IPSec Policy** - IP Security Policy
  - identifica gli algoritmi di autenticazione e crittografia e il metodo di incapsulamento usati a connessione VPN stabilita
- **VPN Service** - Virtual Private Network Service
  - associa la VPN con un router e una subnet specifici
- **IPSec Site Connection**
  - specifica i dettagli della connessione site-to-site

# **Installazione & Configurazione**

# Installazione e configurazione

installare l'agente

```
# apt-get install openswan neutron-plugin-vpn-agent
```

configurare il file `/etc/neutron/vpn-agent.ini`

```
[DEFAULT]
interface_driver = neutron.agent.linux.interface.OVSInterfaceDriver

[vpnagent]
vpn_device_driver=neutron.services.vpn.device_drivers.ipsec.OpenSwanDriver

[ipsec]
ipsec_status_check_interval=60
```

aggiungere il plugin nel file `/etc/neutron/neutron.conf`

```
service_plugins = neutron.services.vpn.plugin.VPNDriverPlugin,neutron.services.loadbalancer.plugin.
LoadBalancerPlugin,neutron.services.firewall.fwaas_plugin.FirewallPlugin
```

# Installazione e configurazione

aggiungere il plugin nel file `/etc/neutron/neutron.conf`

```
[service_providers]
...
service_provider = VPN:Vpn:neutron.services.vpn.service_drivers.ipsec.IPsecVPNDriver:default
```

abilitare il servizio nella dashboard (`/etc/openstack-dashboard/local_settings`)

```
`enable_vpn' : True
```

far ripartire i servizi

```
# cd /etc/init.d
# for s in `ls neutron-*`; do service $s restart; done
# service apache2 restart
```

# Guida per l'installazione e la configurazione

<https://github.com/inf-n-bari-school/VPN-as-a-Service/wiki>

**Uso**

# VPN as a Service - Step-by-step

## Step 1 - Creare una IKE Policy per il tenant

The screenshot shows a dialog box titled "Add IKE Policy" with a close button (X) in the top right corner. Below the title bar is a tab labeled "Add New IKE Policy \*". The main area is divided into two columns. The left column contains several configuration fields: "Name \*" with the value "ike\_pol\_1"; "Description" with the placeholder "Additional information here..."; "Authorization algorithm \*" with a dropdown menu showing "sha1"; "Encryption algorithm \*" with a dropdown menu showing "aes-128"; "IKE version \*" with a dropdown menu showing "v1"; "Lifetime units for IKE keys \*" with a dropdown menu showing "seconds"; "Lifetime value for IKE keys \*" with a text input field containing "3600"; "Perfect Forward Secrecy \*" with a dropdown menu showing "group5"; and "IKE Phase1 negotiation mode \*" with a dropdown menu showing "main". The right column contains instructional text: "Create IKE Policy for current project." and "Assign a name and description for the IKE Policy.". At the bottom right of the dialog are two buttons: "Cancel" and "Add".

### Specificare

- algoritmo di autenticazione
- algoritmo di crittografia
- ...

# VPN as a Service - Step-by-step

## Step 2 - Creare una IPSec Policy

**Add IPSec Policy**

Add New IPSec Policy \*

**Name \***  
ipsec\_pol\_1

**Description**  
Additional information here...

**Authorization algorithm \***  
sha1

**Encapsulation mode \***  
tunnel

**Encryption algorithm \***  
aes-128

**Lifetime units \***  
seconds

**Lifetime value for IKE keys \***  
3600

**Perfect Forward Secrecy \***  
group5

**Transform Protocol \***  
esp

Create IPSec Policy for current project.  
Assign a name and description for the IPSec Policy.

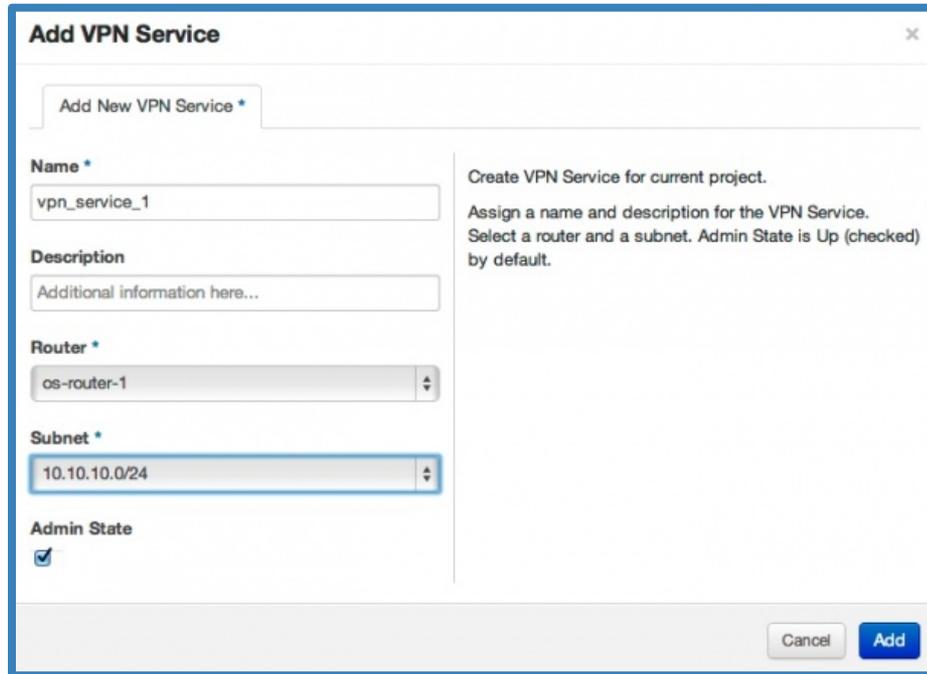
Cancel Add

### Specificare

- algoritmo di autenticazione
- metodo di incapsulamento
- algoritmo di crittografia
- transform protocol
- ...

# VPN as a Service - Step-by-step

## Step 3 - Creare un VPN Service



The screenshot shows a dialog box titled "Add VPN Service" with a close button (X) in the top right corner. Below the title bar is a button labeled "Add New VPN Service \*". The main area is divided into two columns. The left column contains form fields: "Name \*" with the value "vpn\_service\_1", "Description" with the placeholder "Additional information here...", "Router \*" with a dropdown menu showing "os-router-1", "Subnet \*" with a dropdown menu showing "10.10.10.0/24", and "Admin State" with a checked checkbox. The right column contains instructional text: "Create VPN Service for current project. Assign a name and description for the VPN Service. Select a router and a subnet. Admin State is Up (checked) by default." At the bottom right of the dialog are "Cancel" and "Add" buttons.

### Specificare

- nome
- router
- subnet associata

# VPN as a Service - Step-by-step

## Step 4 - Creare una VPN Site Connection

**Add IPsec Site Connection**

Add New IPsec Site Connection \* Optional Parameters \*

Name \*  
site1-to-site2

Description  
Additional information here...

VPN Service associated with this connection \*  
vpn\_service\_1

IKE Policy associated with this connection \*  
ike\_pol\_1

IPsec Policy associated with this connection \*  
ipsec\_pol\_1

Peer gateway public IPv4/IPv6 Address or FQDN \*  
192.168.82.10

Peer router identity for authentication (Peer ID) \*  
192.168.82.10

Remote peer subnet \*  
10.10.20.0/24

Pre-Shared Key (PSK) string \*  
cisco123

Cancel Add

### Specificare

- VPN Service associato (step 3)
- IKE Policy associata (step 1)
- IPsec Policy associata (step 2)
- IP pubblico o FQDN del gateway del router remoto
- subnet remota accessibile tramite questa connessione VPN
- stringa PSK preventivamente concordata con il sito remoto

***... ready to go ...***

***... enjoy!!***

**GRAZIE PER  
L'ATTENZIONE**