Tài liệu viết dựa trên bản thiết kế dành cho VNPaaS phiên bản đầu tiên ở bản phát hành Havana. Trong các bản cập nhập tiếp theo sẽ thêm tính năng và sửa một số bug, sẽ được cập nhập ở tài liệu.

Ở phiên bản đầu tiên, nhà phát hành thực hiện IKE với chế độ xác thực PSK thay vì sử dụng các chứng chỉ. Trong tương lai ở các bản cập nhập khác sẽ hỗ trợ xác thực dựa trên chứng chỉ.

**VPNaaS update:**

Bắt đầu từ phiên bản Havana:

**Liberty:** Start using reno to manage release notes.

**Mitaka:** Generation of sample Neutron VPNaaS configuration files.

### New Features

* Neutron VPNaaS no longer includes static example configuration files. Instead, use tools/generate\_config\_file\_samples.sh to generate them. The files are generated with a .sample extension.

**Newton:** Neutron VPNaaS is integrated with Guru Meditation Reports library.

### New Features

* Neutron VPNaaS services should respond to SIGUSR2 signal by dumping valuable debug information to standard error output.

**Pike:** Flavor framework integration.

### New Features

* Neutron VPNaaS is now integrated with Neutron flavor framework. Multiple VPN service providers might be configured at the same time. A flavor of service type VPN associated with a profile containing a driver is used to find the provider for a newly created VPN service.

### **Queens**: New Features

* VPNaaS support in neutron L3 agent is now implemented as L3 agent extension. We no longer have a separate binary neutron-vpn-agent. To enable VPNaaS support in L3 agent, ensure to specify vpnaas to the configuration extensions in [AGENT] section of the L3 agent config file.

### Upgrade Notes

* The separate L3 agent binary neutron-vpn-agent for VPNaaS support is dropped and VPNaaS support is now implemented as L3 agent extension. When upgrading your deployment to Queens, ensure to specify vpnaas to [AGENT] extensions configuration of the L3 agent config file and run neutron-l3-agent instead of neutron-vpn-agent.

### Bug Fixes

* The libreswan driver of neutron-vpnaas can now also work with Libreswan 3.19+ (bug [#1711456](https://launchpad.net/bugs/1711456)).

**Rocky:** Enable sha384 and sha512 auth algorithms for \*Swan drivers

### New Features

* Users can now specify sha384 and sha512 as the auth algorithm for both IKE policy and IPsec policy, when using \*Swan IPsec drivers.

### Upgrade Notes

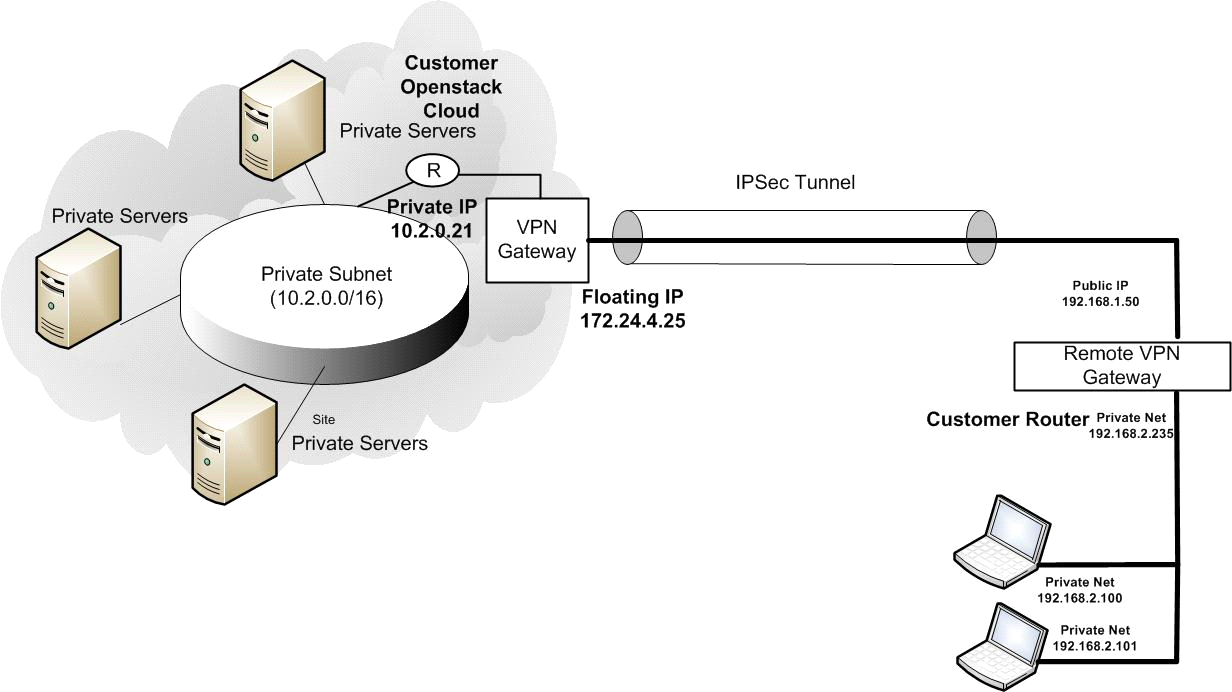
* The following drivers are removed due to the lack of maintainers of the drivers CiscoCsrIPsecDriver, FedoraStrongSwanDriver, VyattaIPsecDriver. Please refer the following [mailing list post](http://lists.openstack.org/pipermail/openstack-dev/2018-February/127793.html) for more detail.

### Bug Fixes

* The libreswan driver of neutron-vpnaas can now also work with Libreswan 3.19+ (bug [#1711456](https://launchpad.net/bugs/1711456)).

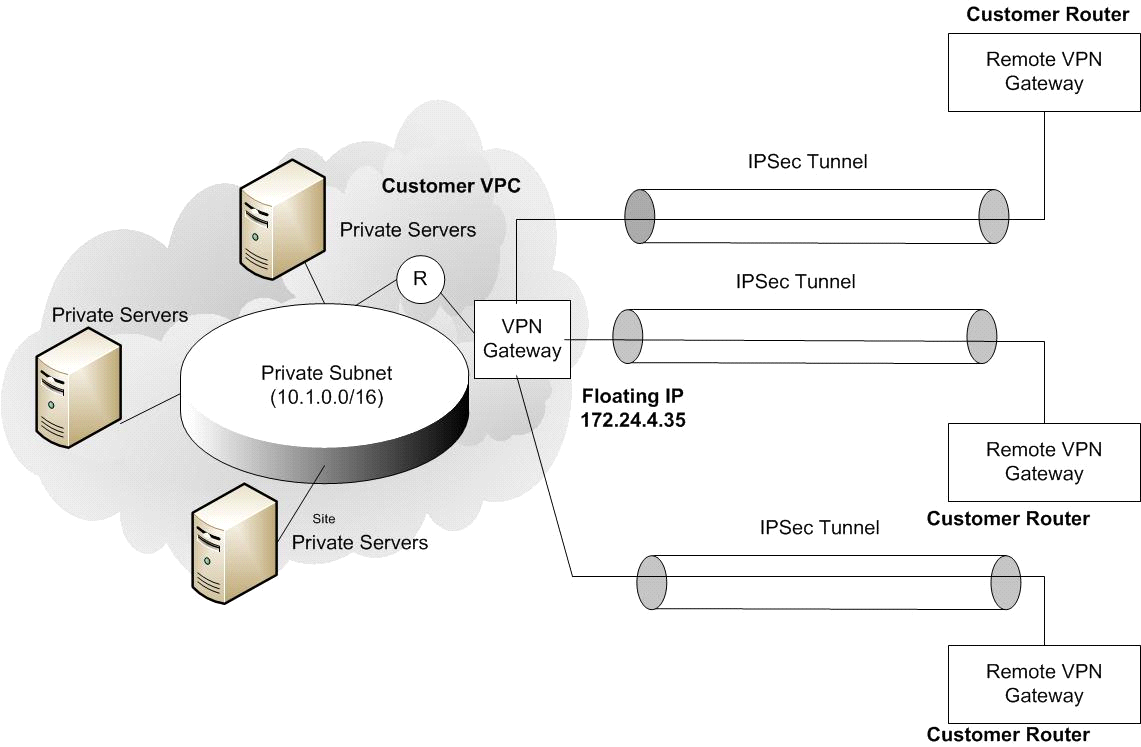
**IPsec Use Case**

**Single Connection**



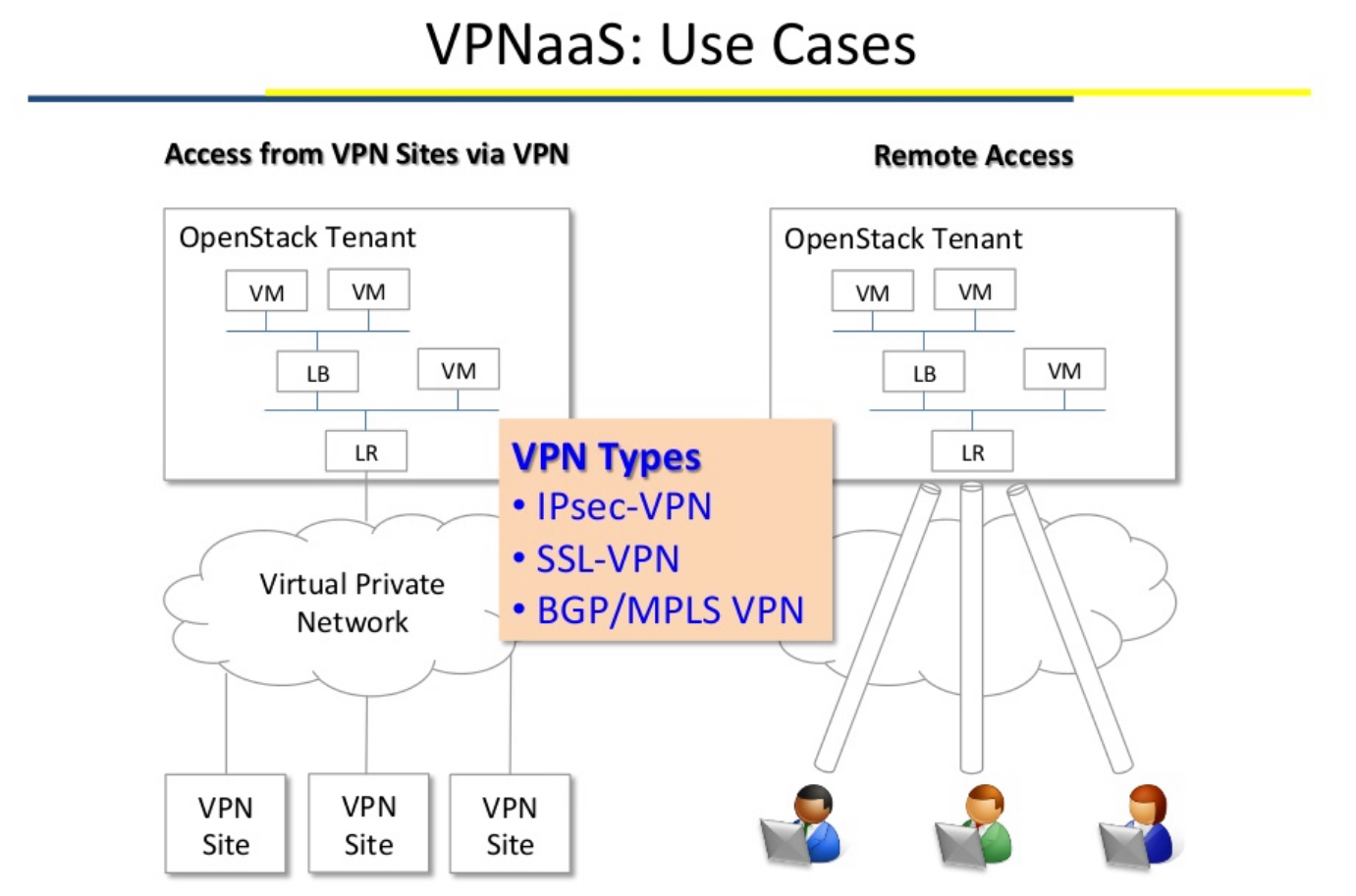
*Trong trường hợp tạo một kết nối*

**Multiple Connections**

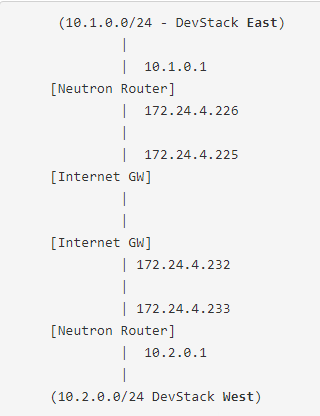


*Tạo nhiều kết nối VPN*

**VPNaaS Use Case**

****

- Khi người dùng muốn kết nối vào mạng nội bộ khác, 2 node DevStack có thể chung public network chỉ khác cổng. Sơ đồ mạng ở dưới bao gôm 2 node East và West



- Trong bài viết: <https://support.vccloud.vn/knowledge-base/su-dung-bizfly-cloud-vpnaas-de-ket-noi-bizfly-cloud-voi-vpc-aws/>

Có giới thiệu dịch vụ của Bizfly Cloud VPNaaS kết nối tới VPC AWS. Để tạo kết nối cần phải tạo 1 Virtual Private Gateway gắn với VPC cần kết nối sang. Tiếp theo tiến hành tạo VPN connection từ phía AWS gắn với VPG vừa tạo và thiết lập dải mạng phía bên cần kết nối.

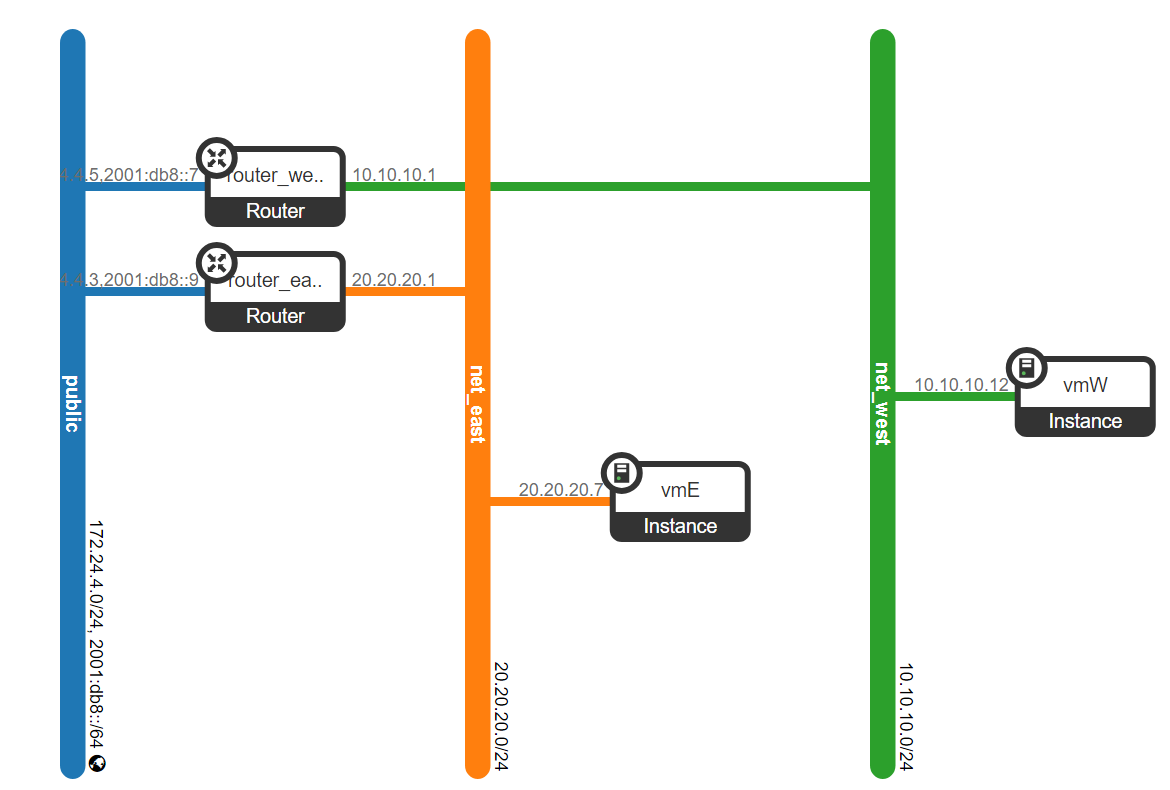
Sau đó tạo VPN connection phía cần kết nối.



*Mô hình cần tạo*

- Khi cần kết nối 2 private network cùng kết nối chung public network thông qua VPN

Ví dụ: netwok topology.



**Hướng dẫn cài đặt:** <https://github.com/phamngocsonls/SVTT/blob/phamngocsonls/SONPN/NetWorking/VPNaaS_install.md>

**Setting:**

## vpn-ikepolicy

Là giao thức thực hiện quá trình trao đổi khóa và thỏa thuận các thông số bảo mật như: thuật toán mã hóa được áp dụng, khoảng thời gian khóa cần được thay đổi . Sau khi thỏa thuận xong thì sẽ thiết lập “hợp đồng” giữa 2 bên, khi đó IPSec SA (Security Association) được tạo ra. SA là những thông số bảo mật đã được thỏa thuận thành công, các thông số SA này sẽ được lưu trong cơ sở dữ liệu của SA Ngoài ra IKE còn dùng 2 giao thức khác để chứng thực đầu cuối và tạo khóa: ISAKMP (Internet Security Association and Key Management Protocol) và Oakley.

– ISAKMP: là giao thức thực hiện việc thiết lập, thỏa thuận và quản lý chính sách bảo mật SA.

– Oakley: là giao thức làm nhiệm vụ chứng thực khóa, bản chất là dùng thuật toán Diffie-Hellman để trao đổi khóa bí mật thông qua môi trường chưa bảo mật

Lưu ý: Giao thức IKE dùng UDP port 500.

VPNasaS hỗ trợ 2 loại IKE: IKE và IKEv2

Phiên bản IKEv1 được giới thiệu vào năm 1998 và bị thay thế bởi IKEv2 7 năm sau. Sự khác biệt lớn nhất giữa IKEv2 và IKEv1 là giảm băng thông.

Tóm tắt so sánh:

1.IKEv2 không tiêu thụ nhiều băng thông như IKEv1.   
2.IKEv2 hỗ trợ xác thực EAP trong khi IKEv1 thì không.   
3.IKEv2 hỗ trợ MOBIKE trong khi IKEv1 thì không.   
4.IKEv2 đã tích hợp NAT traversal trong khi IKEv1 thì không.   
5.IKEv2 có thể phát hiện xem một đường hầm có còn sống hay không trong khi IKEv1 không thể.  
6. IKEv2 an toàn và nhiều tính năng hơn, đáng tin cậy hơn.

Xem thêm so sánh tại: <http://rockhoppervpn.sourceforge.net/techdoc_ikev1vsikev2.html>

Phương thức xác thực. Với các phiên bản cũ IKEpolicy chỉ hỗ trợ SHA1, ở các phiên bản gần đây bổ sung thêm sha384 và sha512

Với tùy chỉnh mặc định : neutron vpn-ikepolicy-create <name>

neutron vpn-ikepolicy-create [-h] [-f {shell,table}] [-c COLUMN]

[--variable VARIABLE] [--prefix PREFIX]

[--request-format {json,xml}]

[--tenant-id TENANT\_ID]

[--description DESCRIPTION]

[--auth-algorithm AUTH-ALGORITHM]

[--encryption-algorithm ENCRYPTION-ALGORITHM]

[--phase1-negotiation-mode PHASE1-NEGOTIATION-MODE]

[--ike-version IKE-VERSION]

[--pfs PFS]

[--lifetime unit=UNITS,value=VALUE]

NAME

* **NAME**: Friendly name of the IKEPolicy used in IPsec VPN Service Connections
* **description**: Friendly description of the IKEPolicy used in IPsec VPN Service Connections
* **tenant-id**: ID of the Tenant that owns the VPN Service.
* **auth-algorithm**: Authentication algorithm used in the IKEPolicy.
* **encryption-algorithm**: Encryption algorithm used in the IKEPolicy.
* **phase1-negotiation-mode**: Phase1 negotiation mode for IKE either 'Main' or 'Aggressive'.
* **lifetime**: String with lifetime specific parameters example: --lifetime "units=seconds,value=3600"
* **units**: Units for lifetime ('seconds' or 'kilobytes')
* **value**. Value for lifetime (non-negative integer).
* **ike-version**: Specify the ike\_version.
* **pfs**: Specify the Perfect Forward Secrecy.

## vpn-ipsecpolicy

Với tùy chỉnh mặc định : neutron vpn-ipsecpolicy-create <name>

**Authorization algorithm:** Mặc định sử dụng SHA1

**Encapsulation mode:** Hỗ trợ 2 chế độ tunnel và transport

**Encryption algorithm:** 3des, aes 128, aes 192, aes 256

**Transform Protocol:** esp, ah hoặc cả esp-ah

neutron vpn-ipsecpolicy-create [-h] [-f {shell,table}] [-c COLUMN]

[--variable VARIABLE] [--prefix PREFIX]

[--request-format {json,xml}]

[--tenant-id TENANT\_ID]

[--description DESCRIPTION]

--transform-protocol TRANSFORM-PROTOCOL

[--auth-algorithm AUTH-ALGORITHM]

[--encryption-algorithm ENCRYPTION-ALGORITHM]

[--encapsulation-mode ENCAPSULATION-MODE]

[--pfs PFS]

[--lifetime units=UNITS,value=VALUE]

NAME

* **NAME**: Friendly name of the IPsecPolicy used in IPsec VPN Service Connections
* **description**: Friendly description of the IPsecPolicy used in IPsec VPN Service Connections
* **tenant-id**: ID of the Tenant that owns the VPN Service.
* **auth-algorithm**: Authentication algorithm used in the IPsecPolicy.
* **encryption-algorithm**: Encryption algorithm used in the IPsecPolicy.
* **encapsulation-mode**: Encapsulation mode for IPsec tunnel either 'tunnel' or 'transport'.
* **transfrom-protocol**: IPsec Transform Protocol either 'ESP' or 'AH'.
* **lifetime**: String with lifetime specific parameters example: --lifetime "units=seconds,value=3600"
* **units**: Units for lifetime ('seconds' or 'kilobytes')
* **value**. Value for lifetime (non-negative integer).
* **pfs**: Specify the Perfect Forward Secrecy.

## vpn-service-create

Create a new vpnservice

neutron vpn-service-create [-h] [-f {shell,table}] [-c COLUMN]

[--variable VARIABLE] [--prefix PREFIX]

[--request-format {json,xml}]

[--tenant-id TENANT\_ID]

[--admin-state-down] [--name NAME]

[--description DESCRIPTION]

ROUTER

SUBNET

* **tenant-id**: ID of the Tenant that owns the VPN Service.
* **router**: Unique identifier of the Router (either 'name' or 'id') to which the VPN will be attached to.
* **subnet**: Unique identifier of the Subnet (either 'name' or 'id') to which the VPN will provide service. (\*)

## ipsec-site-connection-create

Create a new ipsec-site-connection object

Tùy chọn

neutron ipsec-site-connection-create [-h] [-f {shell,table}]

[-c COLUMN]

[--variable VARIABLE]

[--prefix PREFIX]

[--request-format {json,xml}]

[--tenant-id TENANT\_ID]

[--admin-state-down] --name NAME

[--description DESCRIPTION]

--peer-address PEER-ADDRESS

--peer-id PEER-ID --peer\_cidr

PEER-CIDRS

[--mtu MTU]

[--psk PSK]

[--initiator INITIATOR]

[--dpd DPD]

--vpnservice-id VPNSERVICE

--ikepolicy-id IKEPOLICY

--ipsecpolicy-id IPSECPOLICY

* **peer-address**: Remote Peer IP Address for the VPN Connection.
* **tenant-id**: ID of the Tenant that owns the VPN Service.
* **peer-id**: Peer identifier string.
* **peer\_cidr**: Remote Peer Subnet with mask in CIDR format.
* **mtu**: MTU for fragmentation
* **dpd**: String with the dpd attributes. Example: --dpd "action=hold,interval=30,timeout=120"
* **action**: Dead peer detection actions (action=hold, restart etc.,).
* **interval**: Dead peer detection interval.(interval=30)
* **timeout**: Dead peer detection timeout.(timeout=120)
* **route-mode**: Routing mode either 'static' or 'dynamic' - for first release only 'static supported.
* **auth-mode**: Authentication mode either 'PSK' or 'CERTS'
* **psk**: Peer identifier string.
* **initiator**: Initiator mode either 'bi-directional' or 'responder'.
* **vpnservice-id**: Unique Identifier to the VPN Service Object.
* **ikepolicy-id**: Unique Identifier to the IKE Policy Object.
* **ipsecpolicy-id**: Unique Identifier to the IPsec Policy Object.

**Ưu điểm:**

- VPNaaS trên OpenStack là một dịch vụ cung cấp kết nối VPN:

*- Giảm chi phí:*

Việc sử dụng một VPN sẽ giúp các công ty giảm được chi phí đầu tư và chi phí thường xuyên. Tổng giá thành của việc sở hữu một mạng VPN sẽ được thu nhỏ, do chỉ phải trả ít hơn cho việc thuê băng thông đường truyền, các thiết bị mạng đường trục và duy trì hoạt động của hệ thống. Giá thành cho việc kết nối LAN-to-LAN giảm từ 20 tới 30% so với việc sử dụng đường thuê riêng truyền thống. Còn đối với việc truy cập từ xa giảm từ 60 tới 80%.

- Linh hoạt trong vận hành và sử dụng:

Tính linh hoạt ở đây không chỉ là linh hoạt trong quá trình vận hành và khai thác mà nó còn thực sự mềm dẻo đối với yêu cầu sử dụng. Khách hàng có thể sử dụng kết nối T1, T3 giữa các văn phòng và nhiều kiểu kết nối khác cũng có thể được sử dụng để kết nối các văn phòng nhỏ, các đối tượng di động. Nhà cung cấp dịch vụ VPN có thể cung cấp nhiều lựa chọn cho khách hàng, có thể là kết nối modem 56 kbit/s, ISDN 128 kbit/s, xDSL, T1, T3

*- Mở rộng hệ thống:*

Do VPN được xây dựng dựa trên cơ sở hạ tầng mạng công cộng (Internet), bất cứ ở nơi nào có mạng công cộng là đều có thể triển khai VPN. Mà mạng công cộng có mặt ở khắp mọi nơi nên khả năng mở rộng của VPN là rất linh động. Một cơ quan ở xa có thể kết nối một cách dễ dàng đến mạng của công ty bằng cách sử dụng đường dây điện thoại hay DSL…Và mạng VPN dễ dàng gỡ bỏ khi có nhu cầu. Khả năng mở rộng băng thông là khi một văn phòng, chi nhánh yêu cầu băng thông lớn hơn thì nó có thể được nâng cấp dễ dàng.

*- Giảm thiểu các hỗ trợ kỹ thuật:*

Việc chuẩn hoá trên một kiểu kết nối từ đối tượng di động đến một POP của ISP và việc chuẩn hoá các yêu cầu về bảo mật đã làm giảm thiểu nhu cầu về nguồn hỗ trợ kỹ thuật cho mạng VPN. Và ngày nay, khi mà các nhà cung cấp dịch vụ đảm nhiệm các nhiệm vụ hỗ trợ mạng nhiều hơn thì những yêu cầu hỗ trợ kỹ thuật đối với người sử dụng ngày càng giảm.

*- Giảm thiểu các yêu cầu về thiết bị:*

Bằng việc cung cấp một giải pháp đơn cho các xí nghiệp truy cập bằng quay số truy cập Internet, VPN yêu cầu về thiết bị ít hơn, đơn giản hơn nhiều so với việc bảo trì các modem riêng biệt, các card tương thích (adapter) cho các thiết bị đầu cuối và các máy chủ truy cập từ xa. Một doanh nghiệp có thể thiết lập các thiết bị khách hàng cho một môi trường đơn, như môi trường T1, với phần còn lại của kết nối được thực hiện bởi ISP. Bộ phận T1 có thể làm việc thiết lập kết nối WAN và duy trì bằng cách thay đổi dải modem và các mạch nhân của Frame Relay bằng một kết nối diện rộng đơn có thể đáp ứng nhu cầu lưu lượng của các người dùng từ xa, kết nối LAN-LAN và lưu lượng Internet cùng một lúc.

*- Phục vụ nhu cầu thương mại:*

Các sản phẩm dịch vụ VPN tuân theo chuẩn chung hiện nay, một phần để đảm bảo khả năng làm việc của sản phẩm nhưng có lẽ quan trọng hơn là để sản phẩm của nhiều nhà cung cấp khác nhau có thể làm việc với nhau. Đối với các thiết bị và Công nghệ Viễn thông mới thì vấn đề cần quan tâm là chuẩn hoá, khả năng quản trị, khả năng mở rộng, khả năng tích hợp mạng, tính kế thừa, độ tin cậy và hiệu suất hoạt động, đặc biệt là khả năng thương mại của sản phẩm.

**Nhược điểm:**

- Ngay từ phiên bản đầu tiên ra mắt, VPNaaS sử dụng PSK để xác thực nhưng có hứa hẹn sẽ sử dụng chứng chỉ thay vì sử dụng PSK trong những phiên bản tiếp theo. Nhưng hiện tại VPNaaS vẫn đang sử dụng PSK. PSK phải được 2 bên trao đổi với nhau từ trước, có thể qua điện thoại, email, … có thể bị lộ gây mất an toàn. Ngoài việc bị lộ khóa PSK khi trao đổi ở môi trường bên ngoài, khóa PSK có thể bị lộ nếu kẻ tấn công sử dụng brute force để dò tìm khóa.

- Nhược điểm chung của các hệ thông VPN đều là tăng chi phí và kích thước gói tin khi kết hợp các phương thức đóng gói và mã hóa để tăng tính bảo mật dữ liệu, cũng làm ảnh hưởng tới tốc độ truyền dữ liệu.

**Biện pháp để tăng tính an toàn:**

**Đối với khóa PSK:**

* Ở trên đã nêu ra mối lo hại khi sử dụng PSK. Nếu không sử dụng chứng chỉ do bên tin cậy cấp, vẫn có thể sử dụng PSK để xác thực bằng cách sử dụng mật khẩu với độ dài > 30 kí tự bao gồm cả chữ cái, chữ số và thêm nhiều kí tự đặc biệt. Sử dụng mật khẩu với độ dài lớn ngăn chặn các cuộc tán công brute force, sử dụng các mật khẩu có nhiều kí tự đặc biệt, không liên quan tới thông tin cá nhân, liên quan, … giảm thiểu nguy cơ tấn công bằng từ điển. Để tăng tính an toàn của mật khẩu, có thể sử dụng công cụ tự tạo mật khẩu.
* Không sử dụng chung một khóa PSK cho nhiều kết nối.
* Sử dụng IKEv2 có thể tăng thêm tính an toàn hơn so với IKEv1, phiên bản IKEv2 mới và hỗ trợ nhiều tính năng đã nêu ở trên. Nhưng với các cuộc tấn công PSK, việc sử dụng IKEv2 thay cho bản IKEv1 không làm cho khắc phục nhược điểm này.

- Để dữ liệu được an toàn, tùy vào mục đích sử dụng có thể lựa chọn chế độ đóng gói tunnel hoặc transport:

* Đối với chế độ tunnel gói IP nguồn được đóng gói trong một IP Datagram và một IPSec header(AH hoặc ESP) được chèn vào giữa outer và inner header, bởi vì đóng gói với một "outer" IP Packet, chế độ Tunnle được có thể được sử dụng để cung cấp dịch vụ bảo mật giữa các IP Node đằng sau một VPN Getway. Thường được sử dụng khi dùng site-to-site trong VPN
* Đối với chế độ transport: Trong chế độ này một IPSec Transport Header(AH hoặc ESP) được chèn vào giữa IP Header và các Header lớp trên, thường được sử dụng cho client-to-site trong VPN
* Tùy vào mục đích và hiểu biết của người dùng có thể tùy chọn từng chế độ để tiết kiệm chi phí và an toàn

- Tùy vào từng mục đích, người dùng có thế dùng AH, ESP hoặc kết hợp cả 2 trong transform protocol. Chú ý, AH không hỗ trợ NAT vì AH bảo vệ toàn bộ gói tin, đi qua NAT sẽ làm thay đổi tính toàn vẹn của gói tin:

* Nếu cần đảm bảo rằng dữ liệu từ một nguồn được xác thực được truyền đi toàn vẹn, nhưng tính bảo mật là không cần thiết, thì hãy sử dụng giao thức AH. Điều này giúp tiết kiệm chi phí và băng thông bổ sung liên quan đến mã hóa ESP.
* Nếu bảo mật dữ liệu (quyền riêng tư thông qua mã hóa) là bắt buộc, thì phải sử dụng ESP. ESP có thể cung cấp xác thực và tính toàn vẹn cho các gói thông qua các thuật toán tương tự được sử dụng bởi AH.

****

AH, ESP, AH-ESP trong tunnel mode



AH, ESP, AH-ESP trong trasport mode

Use case, setting, install, advan/disadvantage, các case có thể sử dụng được, biện pháp để tăng tính an toàn, luồng triển khai thực tế với hệ thống

Luồng triển khai thực tế với hệ thống: