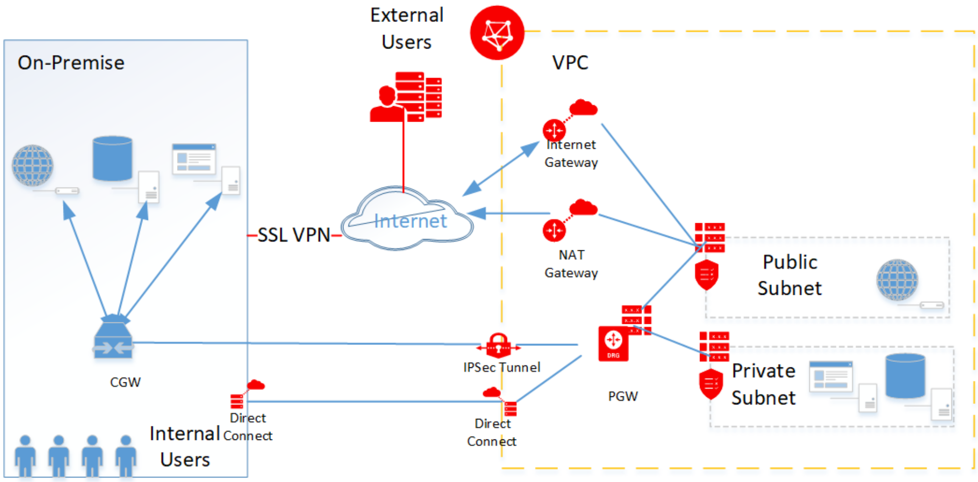
IPSec VPN

Aneel K. Kanuri

This whitepaper provides a technical reference of IPSec VPN. VPN connections are broadly used in the personal and professional world to secure communications over the Internet. The goal of this document is to give a clear understanding on the components involved behind the scenes of a VPN connection, as the packet travels from source to destination.



Background

IPSec VPN connections are very popular on personal computers and for all-sized organizations. It is very common to have multiple VPNs on a laptop or computer, each configured to a specific route. So, what exactly is a VPN? VPN stands for “Virtual Private Network.” As the name suggests, it creates a private network between the source and destination (often a remote resource). This will let the source communicate to the destination over a private IP as if they are on the same network. VPN also masks the source IP – which makes it difficult for hackers to track online activity from a specific computer.

There are two common VPN protocols that are often used – IPSec VPN and SSL VPN. IPSec VPN operates at Layer 3, and is often used to securely establish communication between two remote networks (rather than a single computer). SSL VPN operates at Layer 4-5, and information is encapsulated at Layer 6-7. SSL VPN offers more portability compared to IPSec VPN. This document further focusses on IPSec VPN keeping public cloud in the center of discussion.

IPSec VPN Use Cases

There are two use cases when an organization has a hybrid setup with their infrastructure shared between on-premise and a public cloud:

1. How do on-premise data-center resources access the resources deployed in cloud?
2. How can traveling consultants access resources deployed in the cloud, in a secure manner?

Let's get to the detail of these use-cases. In the first scenario, it is very common to have an application deployed in a public cloud but the dependent integrations are still left behind in an on-premises data-center. It is not ideal to have these two networks talk on public internet without any encryption. IPSec VPN comes into play here. It establishes a secure tunnel of communication between on-premise and public cloud (network to network). We will see in the next section on how this can be achieved.

The second scenario is common when there are traveling consultants who must connect to individual resources deployed in public cloud. There are two methods. These consultants can connect to on-premise using organization's VPN and then access the application deployed in public cloud over an IPSec VPN. This is a long route, and requires more network hops. The easiest way is to have an SSL VPN deployed on a compute instance in a public cloud, and advertise the application deployed in public cloud via that VPN connection. This SSL VPN is often a commercial software that has to be purchased, or an open source like Libreswan. Although SSL VPN is not further explored in this document, the above description will give you a good use case on where it can help.

IPSec VPN Setup

IPSec-VPN operates in two modes – IPSec VPN Tunnel Mode and Transport Mode.

IPSec VPN Tunnel Mode encrypts and authenticates an entire outgoing packet. After encryption, the packet is then encapsulated to form a new IP packet that has new header information. IPSec VPN Transport Mode encrypts only the actual payload of the packet, and the header information stays intact. This will make transport mode less secure than tunnel mode. Most public clouds support only Tunnel mode, which is more secure.

IPSec Tunnel is established by peering two remote networks. This is the step where trust is established between networks using a Pre-Shared Key (PSK). In a public cloud, a Customer Gateway is created where on-premise public endpoint IP address is provided. After that, a Virtual Private Gateway is created in the cloud to route the received traffic internally with in the cloud. CGW and VGW are pre-requisites to create a VPN connection.

A VPN connection can be established using a static routing or BGP dynamic routing. BGP routing uses a Border Gateway Protocol, and is preferred over static routing. Static Routing is best when there is a one-to-one relationship between source and destination networks. For static routing, a static route is defined during an IPSec connection creation.

By default, two tunnels are created for redundancy. Advise the customer to configure both the tunnels if supported on the customer router, then share the pre-shared keys with the customer.

After a few minutes, at least one of the tunnels will be up and running

Behind the Curtains

After a VPN connection is created and trust established, there are typically five steps that will happen when a data transfer is initiated.

1. Interesting Traffic initiates the IPSec process
2. IKE Phase 1
3. IKE Phase 2
4. Data Transfer
5. IPSec Tunnel Termination

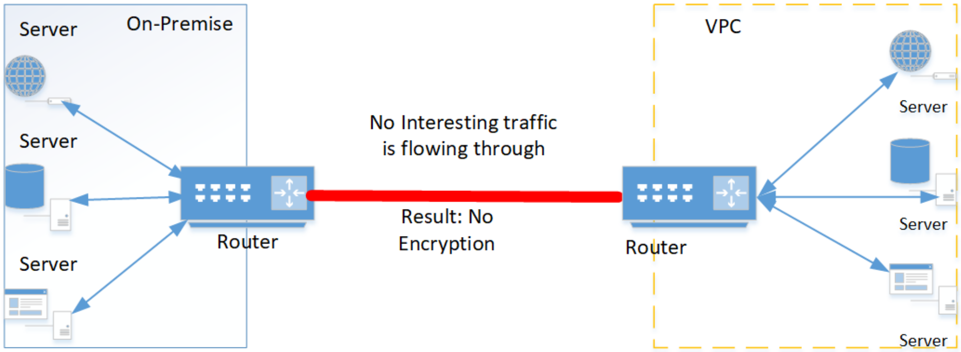


Fig 1.1: Initial state

1. Interesting Traffic: Any IP packet that is received by the router on source, which has a known destination, is marked as an interesting traffic. This will initiate the IPSec process.
2. IKE Phase 1: After receiving the interesting traffic, IKE Phase 1 is initiated. During this phase, source router will authenticate the peers to make sure they are actually who they claim they are. It negotiates and agrees on the methods of authentication and hashing used during the communication. Source or initiator will send the policies that it supports, and the destination will check for any matching policies before responding. Authentication usually uses DH exchange, with the end result of having matching shared secrets (PSK). After successful authentication, it creates a basic communication tunnel which is not fully encrypted.

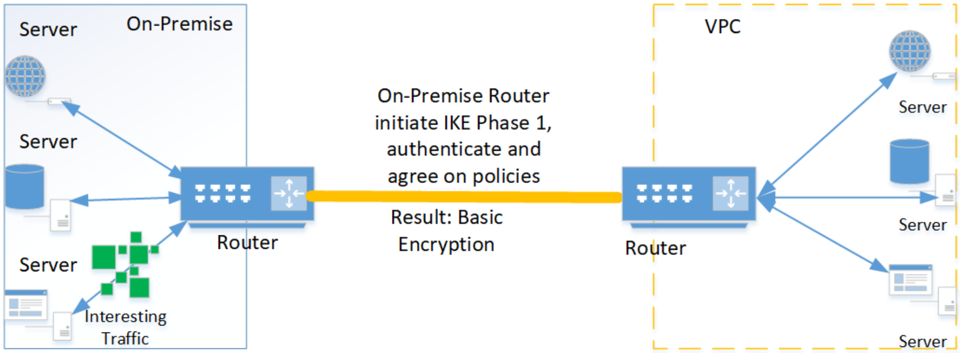


Fig 1.2: Interesting Traffic initiated IKE Phase 1

3. IKE Phase 2: IKE Phase 2 operates over the IKE Phase 1 tunnel. As IKE Phase 1 is already encrypted and has established a basic secure tunnel, it can now exchange sensitive information to create another security association – IPSec Security Association. If the tunnel exists for long time, it renegotiates IPSec Security Associations to ensure uninterrupted secure communication throughout the tunnel duration. A successful Security Association is the end of IKE Phase 2.

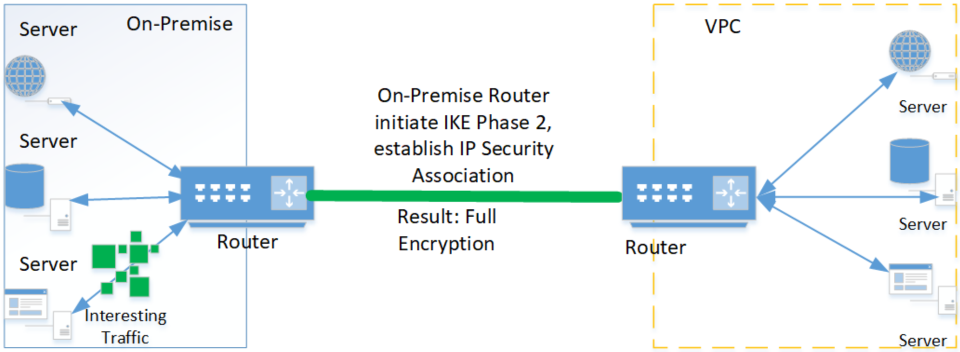


Fig 1.3: IKE Phase 2

4. Data Transfer: At the end of IKE Phase 2, there is a secure tunnel established between the network peers. Data can now be transferred securely in tunnel mode over an encrypted VPN tunnel.

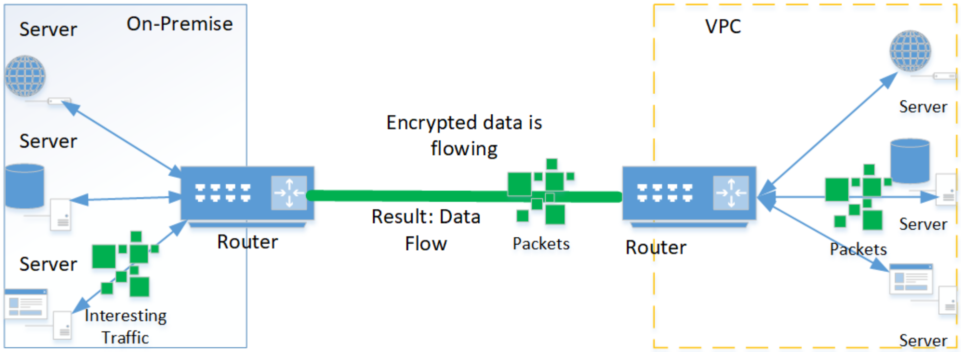


Fig 1.3: Data Flow

Tunnel Termination: When there is no interesting traffic or when a pre-defined timeout occurs, tunnel will be terminated. It is common to see that the tunnel is down after IPSec Tunnel Termination. With no extra manual effort, VPN tunnel will initiate steps from #1 to #3 when either router receives interesting traffic.

Pros and Cons

VPN looks like an attractive solution at first glance, but it does have a few drawbacks. The major drawback is that the speed of the VPN connection is dependent on the internet throughput if the other factors like vNIC model & speed are taken out of scope. This is fine with smaller / occasional workloads, but is not a reliable solution for network-intensive applications.

The best alternative is a Direct Connect / Fast Connect. The name may differ based on the chosen public cloud but the concept remains same. A Direct Connect is a direct wired connection between two networks. This is an expensive solution compared to VPN because this involves physical cabling. The expenses can be cut-down if a customer data center is co-located with one of the partners of a chosen public cloud, or if a major partner is located nearby the customer data-center. It is like running an Internet cable from a junction box near your house rather than running it from the ISP headquarters.

The advantage of Direct Connect is predictable speed between on-premise and the public cloud. Direct Connect usually comes with 1 Gbps / 10 Gbps with an increment of 1 Gbps speeds. A predictable speed is mandatory for many network-intensive applications. Data is not encrypted in transit while using a dedicated connection because it is not going through a public internet. However, encryption can be configured.

VPN is often used as a backup to Direct Connect connections. This will create a redundancy and keep the network available, at a reduced speed, when direct connect is down.

Conclusion

IPSec VPN Tunnel is a popular option in cloud migrations during the initial phase. VPN is less expensive and requires less time to setup when compared with Direct Connect. Although Direct Connect is a preferred option for network-intensive applications, they are often backed up by VPN connections. Because VPN is less expensive, it is often a common scenario to have redundant VPN connections back to on-premise data center. Zione Solutions, LLC has expertise in cloud networking, and can help you connect your on-premise to any public cloud for lift & shift or data center migrations.

Zione Solutions is highly experienced in data center migrations to public clouds like Oracle, GCP, AWS, and Azure. We have helped numerous customers in taking their first step towards the cloud, and have gained trust through our history of success. Our customers have benefited from our implementations which strictly follow a well-architected framework, and are extremely pleased with the performance, reliability, flexibility, and cost optimizations from the architectures designed by our team of experts. Our team includes certified AWS professionals, Oracle ACEs, and Oracle ACE Directors to assist in large data center migrations involving Oracle and non-Oracle workloads.