VMware Cloud on AWS: Direct Connect

VMware General

Table of contents

VMware Cloud on AWS: Direct Connect

Overview

Under normal circumstances, customers will access their SDDC via the public internet; either directly to VM public IP addresses, or to private addresses via IPSec VPN. Often times, customers wish to avoid using their public internet provider for connectivity to the SDDC. For these cases, AWS offers Direct Connect, which provides direct connectivity into an AWS region via private leased lines. With Direct Connect, users will define virtual interfaces (VIF) which allow them to connect to public or private resources within that Region. These VIFs come in 2 flavors: Public and Private.

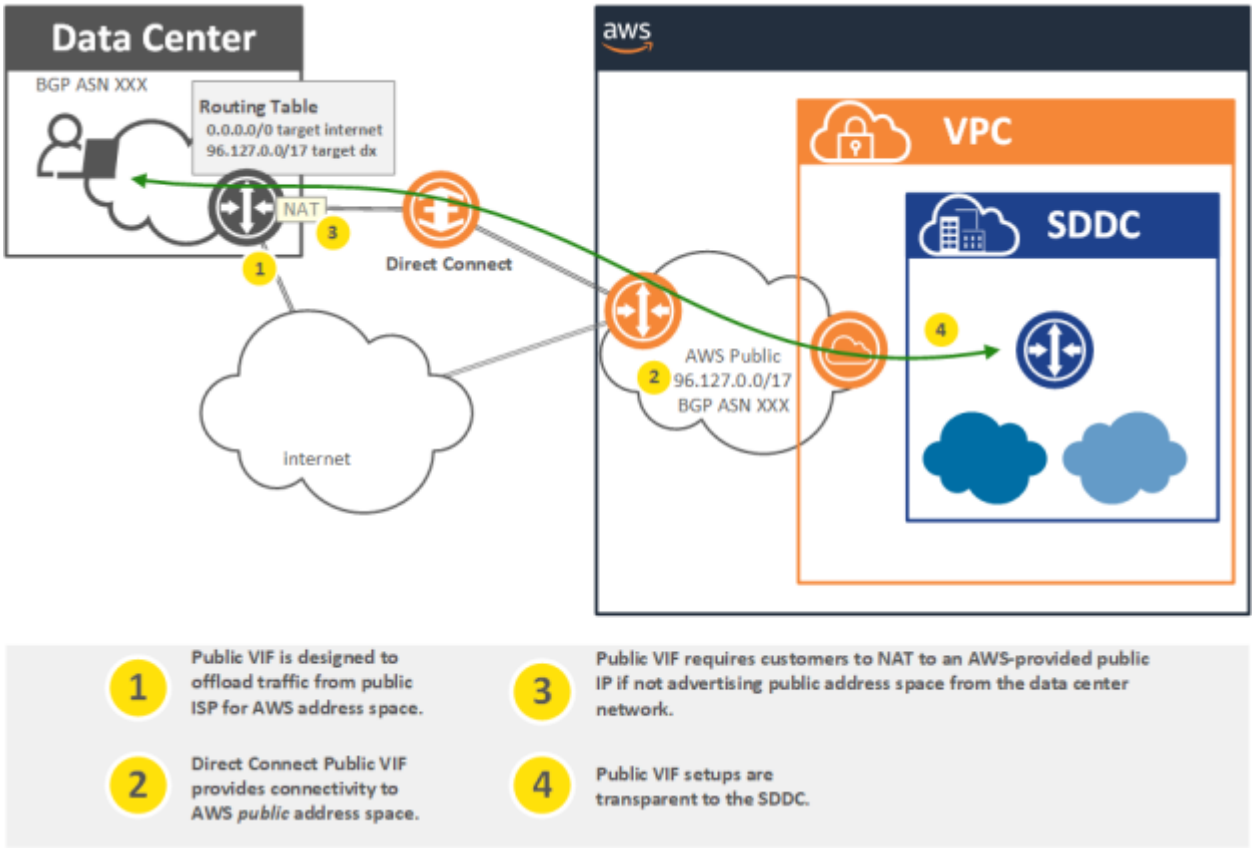
Public VIF enables the Direct Connect to be used for accessing the AWS public network. When Public VIF is used, the Direct Connect will become the preferred path for reaching AWS public IP addresses. This means that if IPSec VPN is being used to access the SDDC, then it will ride over the Direct Connect (assuming the VPN peering is done via the edge public IP).

Private VIF, on the other hand, enables Direct Connect to be used for accessing the private IP address space of a VPC. When a Private VIF is associated to an SDDC, then it becomes possible to access the SDDC directly without the need for IPSec VPN (although you can use IPSec VPN over Private VIF is so desired).

The next sections will explore this in more detail.

Public VIF

Public VIF enables a Direct Connect to be used for accessing the public IP address space of the AWS network. Normally, customers will have one or more public internet circuits over which they will receive either default routes, or specific BGP prefixes. These circuits are used to access the public IP address space which AWS advertises to its upstream internet providers. In this example, the on-premises router is receiving a default route to the internet.



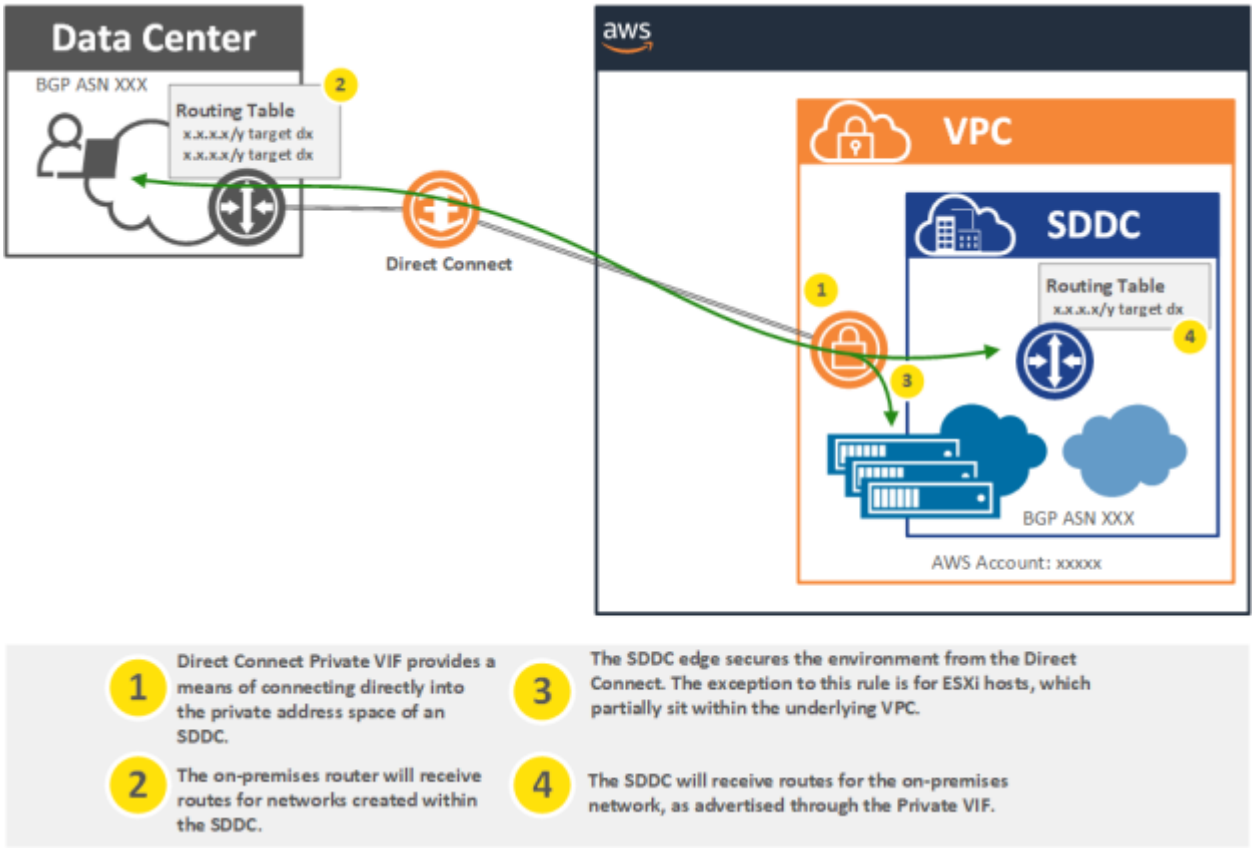
When Direct Connect is enabled, and a Public VIF created, AWS will begin to announce all of their public IP prefixes, via BGP, over the Direct Connect. In this example, due to the specific routes being advertised by AWS, the customer network will prefer the Direct Connect as its path toward AWS public address space. This effectively means that the Direct Connect will be used when connecting to the public IP addresses allocated to the SDDC; for example, the public interface of the edge or the Elastic IP of vCenter.

One important consideration when using Public VIF is to keep in mind that the on-premises network must also be reachable via its own public IP address space. For larger customers with their own public IP ranges and BGP ASN, they may choose to advertise this address space to AWS over the Direct Connect. Doing so will ensure that routing between the customer on-premises environment and AWS is symmetrical, and rides exclusively over the Direct Connect.

The typical AWS customer either does not have their own BGP ASN and public IP ranges, or does not want to advertise them over the Direct Connect. For these cases, customers may submit a request to AWS for a public IP. AWS will then allocate an IP from their own public address space which may be used by the customer for their end of the connection. It is important to note that in these cases customers must set up NAT such that all traffic originating from their end (which uses the Public VIF) is NAT-ted to that public IP. A common mistake is to forget to configure NAT, and in these cases, customers will end up routing traffic into the AWS public network which is sourced from their internal private IPs. In this scenario, AWS will drop the traffic, and the end result will be that AWS public address space will be unreachable from the customer environment.

Private VIF

The standard means of accessing the private address space of an SDDC is via IPSec VPN. This VPN creates a secure virtual tunnel directly between the customer on-premises and the SDDC, either over the public internet or atop Direct Connect Public VIF. Direct Connect Private VIF provides an alternative to IPSec VPN by enabling a direct routed path between the customer on-premises network and a VPC within the AWS environment.



An SDDC resides within a dedicated VPC which is owned by a master VMware account. Since the SDDC resides within a VPC, it is possible to terminate Direct Connect Private VIF directly to that VPC. In order to use Direct Connect with an SDDC, **customers must specifically link the Private VIF to the VMware AWS account used by the SDDC**. This account information is documented within the Network & Security tab of the SDDC within the VMC console.

Once the VIF has been terminated, the SDDC begins advertising routes through the Private VIF via BGP. The customer on-premises router should also be configured to advertise routes (representing the customer private address space) to the SDDC. As a general rule, the best practice is to advertise specific routes into the Direct Connect from the on-premises network instead of advertising a default route.

As seen above, the edge routers of the SDDC are in-path for Direct Connect. This means that gateway firewalls are enforcing security and that the security policies of the SDDC must be configured to permit connectivity to and from the on-premises environment.

There is one important exception to this rule. Since the ESXi hosts themselves reside at the base-layer of the infrastructure, two of their interfaces are directly connected to Subnets of the underlying VPC. Specifically, the management and vMotion interfaces. For these interfaces, the path through the Direct Connect will bypass the edge routers of the SDDC. This means that security between the on-premises network and the ESXi hosts must be enforced on the on-premises side of the Direct Connect. Again, this scenario only applies to Direct Connect Private VIF and does not apply to users of IPSec VPN.

Authors and Contributors

Author: Dustin Spinhirne