Enabling Cloud Native VPN/ Encryption Options Over Dedicated Cloud Connectivity Paths

When implementing a dedicated connection into the public cloud through ExpressRoute to Microsoft Azure or Direct Connect to Amazon Web Services, the security of the transport path is part of a security risk assessment to minimize the risk of any potential man-in-the-middle attack.

Azure and AWS have published details on how to use VPN services through their respective dedicated cloud connectivity options:

- Configure a site-to-site VPN over Microsoft Peering
- Establish a VPN Using AWS Direct Connect

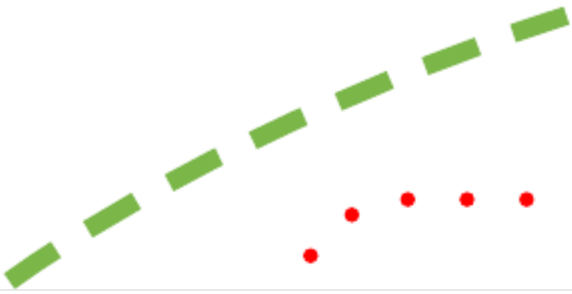
But what about using a Megaport as your connectivity partner for your ExpressRoute or Direct Connect? What can Megaport provide beyond the private pathway to the cloud?

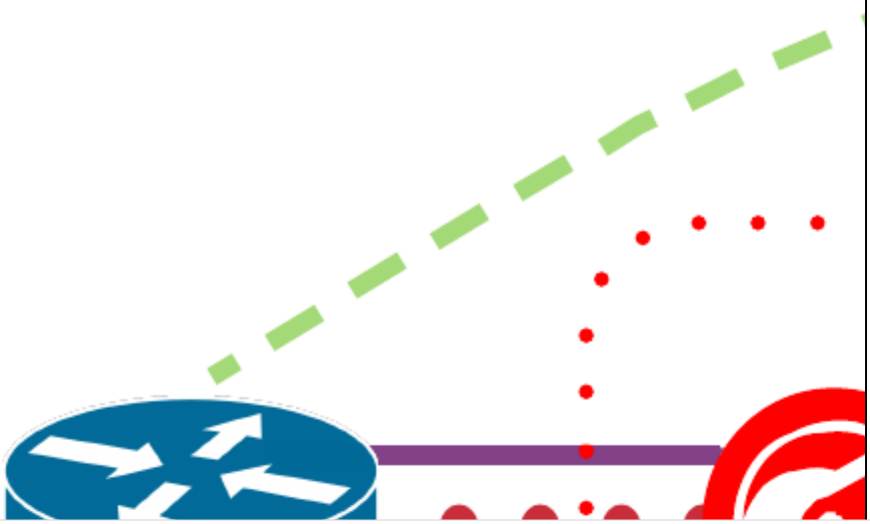
This topics reviews several scenarios leveraging dedicated cloud connectivity, including:

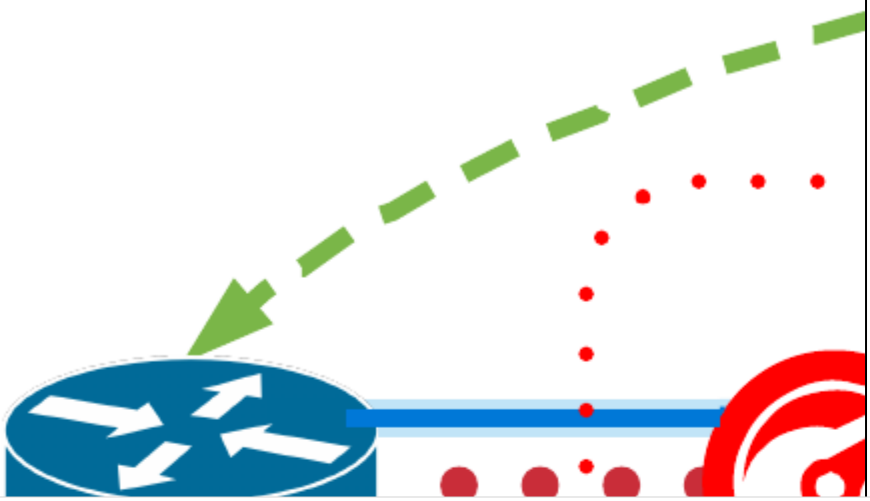
- **Scenario 1:** IPsec VPN – Azure ER Microsoft Peering or AWS DX Public VIF
- **Scenario 2:** IPsec VPN via Megaport Cloud Router (MCR) – Azure ER Microsoft Peering or AWS DX Public VIF

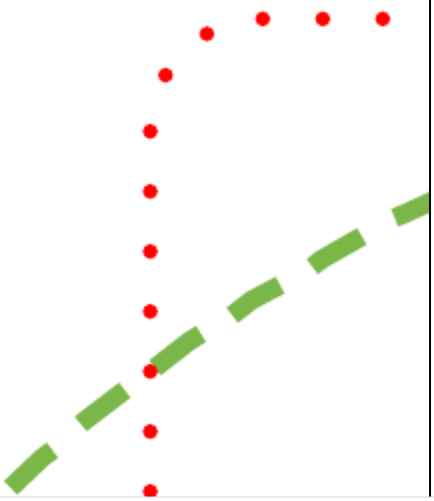
- **Scenario 3:** IPsec VPN – Azure ER Private Peering or AWS DX Private VIF with Network Virtual Appliance (NVA) in Azure or AWS
- **Scenario 4:** IPsec VPN – Multicloud with Network Virtual Appliance (NVA) in Azure and AWS

Scenario 1	Scenario 2	Scenario 3	Scenario 4

Scenario 1
IPsec VPN - Microsoft Peering or Public VIF
Prerequisites
• Owned public IP addresses that can be assigned to use Microsoft Peering and Public **Note:** If public IP addresses are not owned, use MCR (Scenario 2). • On-premises network appliance that supports IEEE 802.1ad (Q-in-Q) – specifically fo **Note:** If 802.1ad is not supported, use MCR (Scenario 2). • Owned network appliance capable of IPsec.
Megaport Technology Required
Megaport
Megaport Cloud Router (MCR)
Virtual Cross Connect (VXC)


Scenario 2
IPsec VPN through MCR - Microsoft Peering or Public VIF. This solution is suitable for organizations that do not own public IP addresses.
Prerequisites
• Customer owned network appliance capable of IPsec.
Megaport Technology Required
Megaport
Megaport Cloud Router (MCR)
Virtual Cross Connect (VXC)


Scenario 3
IPsec (or other) VPN - Private Peering or Private VIF with Network Virtual Appliance (NVA
Prerequisites
• Customer (on-premises) network appliance that supports IEEE 802.1ad (Q-in-Q) – sp **Note:** If 802.1ad is not supported, use MCR (Scenario 2) but use private peering or a • Customer owns IPsec-capable network appliances on-premises and in the cloud.
Megaport Technology Required
Megaport
Megaport Cloud Router (MCR)
Virtual Cross Connect (VXC)


Scenario 4
IPsec (or other) VPN - Multicloud with Network Virtual Appliance (NVA) in Azure and AW This solution is suitable for organizations with on-premises infrastructure that is not geogr
Prerequisites
• Customer owns IPsec-capable network appliances on-premises and in the cloud.
Megaport Technology Required
Megaport
Megaport Cloud Router (MCR)
Virtual Cross Connect (VXC)


Last update: