VPC Shared VS multi-VPC: choosing the best suits for your organization

29 September 2023 - 8 min. read

Advanced Networking | *Amazon VPC* | *governance and compliance* | *Landing Zone*

Introduction

As we saw in the last article, when it comes to network infrastructure for our Landing Zone, we no longer think only about the Transit Gateway but about a broader range of possibilities. The real question we need to ask ourselves now is when to use one approach over another, understanding the benefits or drawbacks this decision will bring with it. In the course of this article, we will try to outline the advantages and disadvantages of each solution and, subsequently, provide you with some small examples of use cases for each of these solutions.

Use Cases

After understanding the various possibilities we have for configuring our landing zone network, let's explore some potential scenarios that will help us determine which approach suits our case and needs. Below, we will attempt to present three possible scenarios and together, we will assess which of the options fits the described scenario. Please remember that you may have specific requirements not covered in this article; what we are providing are simply guidelines to assist you in making your decisions without imposing strict rules.

Shared VPC use case

Let's consider the most common scenario: a company that has decided to leverage the cloud for its entire infrastructure and has likely increased the number of its accounts over the years. For our hypothetical company, topics like the Landing Zone, cost

management, and centralization of core services have become part of their daily routine.

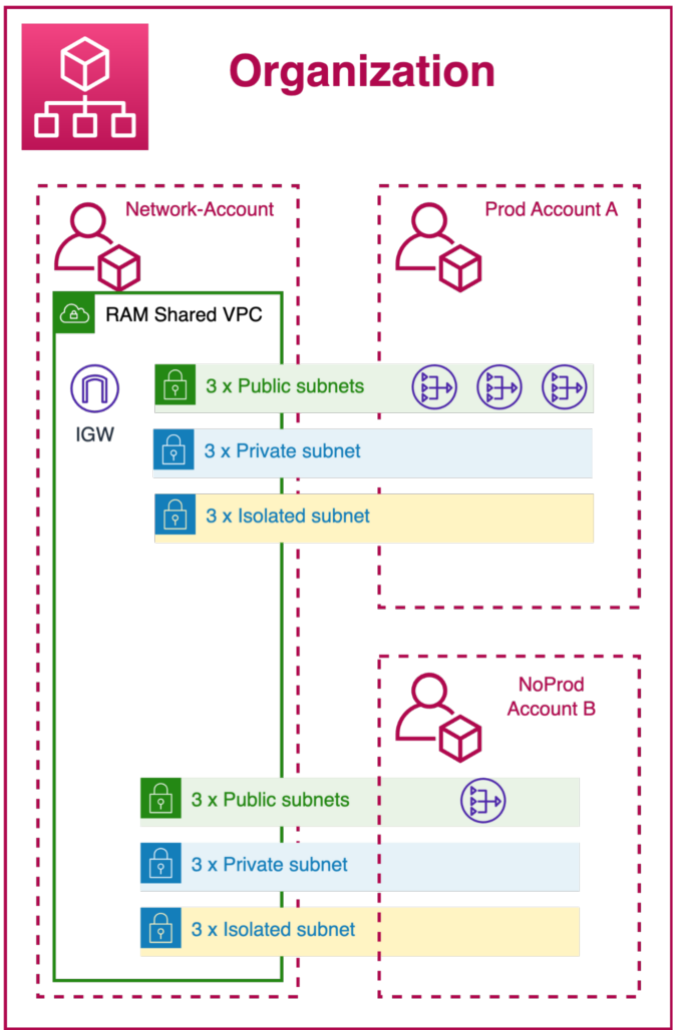
Unfortunately, IT hasn't grown at the same pace as applications and business needs, often leading to struggles with excessive overhead in managing their infrastructure. In this case, among all the available options, a single shared VPC could be the missing piece that enhances the daily operations of our IT department, without giving up the scalability and compliance benefits commonly seen in a well-structured Landing Zone.

Unlike a Transit Gateway, with this solution, we can manage the network of all accounts directly from a centralized console in our "network account." As explained in the previous article, when we refer to the "network account," we mean an AWS account within our Organization dedicated to creating the VPC and all its subnets, which will later be shared with various accounts.

Being able to modify routes, create new subnets, and manage cross-account traffic directly from a console will save us a significant amount of time that would otherwise be spent switching accounts using assumeRole or our SSO portal if we're federated with our IDP. While multi-account management has become commonplace for such companies, saving significant time helps us focus on more critical issues like security and segregation.

Another advantage of this solution is the segregation of permissions related to network resources in the application accounts. By managing VPC ownership within our centralized account, we can limit IAM permissions for users working on various accounts, ensuring that incorrect configurations do not create security vulnerabilities in our network.

If we want to add another piece to our hypothetical company, we can say that the various applications present in our accounts often need to communicate with each other to exchange valuable information necessary to provide a quality service to potential customers. If you've been in this situation, you'll know that in these cases, extra-VPC costs tend to be one of the main causes of high bills. Remember that on AWS, traffic within a VPC and traffic passing between VPCs (even in the same AWS region) have significantly different costs. If there's also a Transit Gateway between the VPCs, the costs increase further.



In this case, as well, a single shared VPC with AWS RAM will help us reduce all these additional costs. Our packet traffic, even when moving from one subnet to another or from one account to another, will always remain within our single VPC, avoiding the additional costs mentioned earlier.

As a side note on this situation, if during our journey on AWS, we decided to implement Attribute-Based Access Control (ABAC) as an access management methodology, this decision may not work well with this network architecture. The simplest solution would be to re-tag the resources once the subnets are shared.

Transit Gateway use case

Before we talked about a medium-sized company that built its infrastructure in the cloud, now we're discussing a large multinational company that is undergoing cloud migration to modernize its applications. Compared to the previous example, the number of IT employees and network management personnel is certainly higher. We can also imagine that each company making up our conglomerate will have its dedicated IT and may have different ways of working. In this case, the Single Shared VPC would likely cause problems due to the numerous stakeholders involved in its

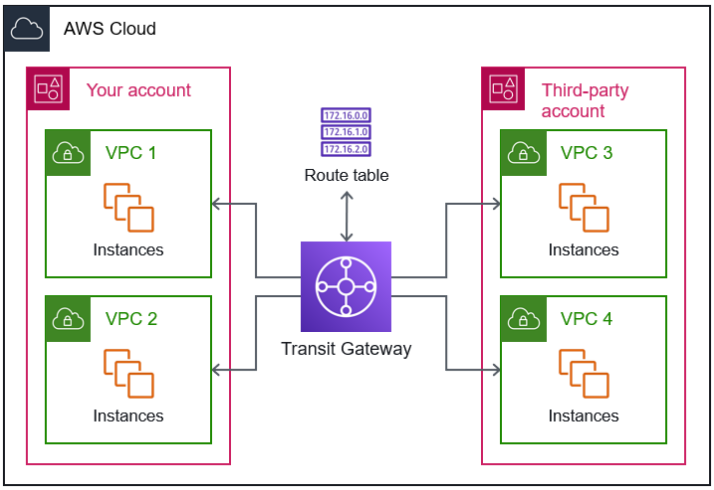
configuration. The wiser choice falls on the Transit Gateway approach and the creation of at least one VPC in each of our AWS Organization accounts. As in the other example, here too, we will have a central account where the Transit Gateway will reside, which probably will only be accessible to some IT managers or individuals with particular technical expertise. For all other accounts, individual IT departments will be free to create internal routes, DHCP reservations, network ACLs, and whatever else is needed to ensure the company's daily operations run smoothly.

The Transit Gateway is the most advantageous choice in this context because, most likely, for our Landing Zone, we have yet to opt for a single region but for several. This decision may have been made to bring the company's offices scattered around the world closer to the data centres where the VMs reside, thus minimizing latency as much as possible.

Such a multi-region implementation would not be possible using the VPC Shared method because, relying on a "regional" service like RAM, we can use shared subnets with our accounts only if we are in the same original Region of the VPC.

Another situation that leads us to this solution is the possibility of routing all S2S VPNs from our on-premise locations to the Cloud through the Transit Gateway. This operation is necessary to allow IT administrators to work effectively on the numerous virtual machines in their machine park.

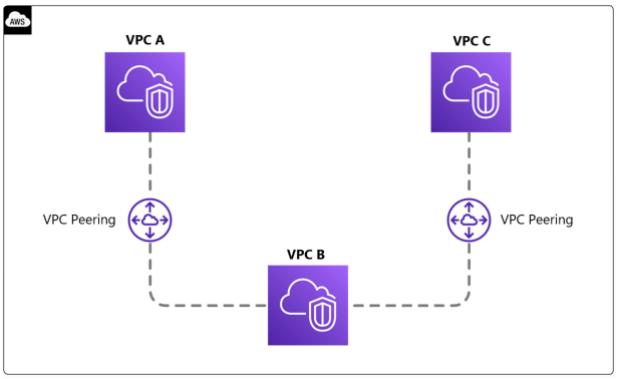
As described in the Transit Gateway section of the previous article, all traffic and routing can be managed by modifying the routing tables assigned to each Transit Gateway Attachment. We need to configure the routes so that each on-premise location can only reach its respective AWS account. This would also lead to a reasonably high level of security in case a malicious actor attempted "Lateral Moving" within our network. Unfortunately, if this approach relies solely on configuring routing tables, it might be more cumbersome to address these issues with the Shared VPC. Since all subnets communicate with each other and cannot create more exclusive routes (within the routing tables) than our CIDR, the only way to segregate each group of subnets would be to adopt very stringent network ACLs.



VPC Peering use case

After discussing medium and large enterprises, the last scenario to address is emerging businesses, such as small companies or startups. We can think of this company as being in its early stages, and after taking its initial steps into the cloud, it has decided to create a simplified Landing Zone. When thinking about these types of companies, we shouldn't imagine a global presence, a vast number of accounts, a complex compliance policy, or a dedicated IT department. The two main factors to consider in designing our landing zone for such scenarios are cost and ease of management.

If we are looking for network infrastructure that aligns with these two principles, the choice inevitably falls on VPC Peering. The simplicity of this feature, which is often excluded from the pool of possible solutions, makes it the perfect candidate in this case to best meet our clear and well-defined needs.



In this scenario, our Landing Zone will consist of a very small number of accounts, omitting accounts typically used for security and auditing management. Even the network account is superfluous and can be easily disregarded.

With VPC peering, we can establish communication between our two applications that have been deployed on separate accounts (or perhaps developed at different times) with just a few clicks. While using peering won't allow us to employ complex and elaborate features as we could with a Transit Gateway, in our case, this won't be an issue since network management won't be one of our primary concerns at this stage of our AWS development.

Unfortunately, peering won't be a permanent solution if we plan to expand our company and AWS organization in the coming years. The primary drawback of this solution is its scalability, which loses its simplicity principle and adds a lot of management overhead as the number of accounts grows.

However, this could serve as a transitional phase to establish our presence in the cloud before adopting a more structured solution like VPC Sharing or Transit Gateway.

Conclusion

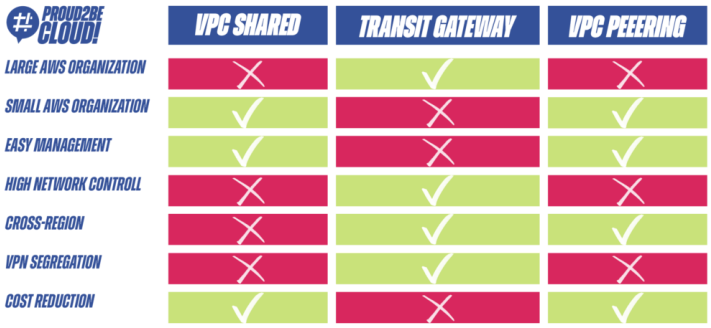
As always, it's time to conclude based on what we've discussed in the last two articles about centralized networking in a Landing Zone and the various possible infrastructures.

We've seen that each of the various options provided by AWS has its advantages, disadvantages, and specific use cases. It would be difficult to say which of these solutions is the best because, as often happens, the answer is "it depends." The first step is certainly to understand the needs of our company and the values we want to uphold during the creation of the Landing Zone. As has been emphasized many times on this blog, designing a Landing Zone is something that needs to be studied in detail and tailored to the requirements, much like a custom-tailored suit.

Let's also remember that a well-designed infrastructure will accompany us on the growth path of our company. Therefore, let's aim to design a solution that can grow in tandem with our needs and, consequently, with the growth of our Landing Zone on AWS.

Once we've determined the structure our Landing Zone will adopt, it will be necessary to engage with the stakeholders of our applications to understand their perspective and any needs we may have overlooked or not considered. Remember that a

customized infrastructure that allows everyone to work efficiently and securely is always the path to follow during the design and renewal phases.



About Proud2beCloud

Proud2beCloud is a blog by beSharp, an Italian APN Premier Consulting Partner expert in designing, implementing, and managing complex Cloud infrastructures and advanced services on AWS. Before being writers, we are Cloud Experts working daily with AWS services since 2007. We are hungry readers, innovative builders, and gem-seekers. On Proud2beCloud, we regularly share our best AWS pro tips, configuration insights, in-depth news, tips&tricks, how-tos, and many other resources. Take part in the discussion!

Riccardo Fragnelli

DevOps @ beSharpI was born on-prem as a Dev before landing on the “Cloud side of IT”. With AWS I discovered a whole new branch of IT that fascinates me more and more; I’m always ready for the next big thing!I’m the fussiest man I know on earth and quite lazy. I like spending my free time jumping between video games and RPGs.
