Table of Contents

Abstract ............................................................................................................................................ 1
Abstract .................................................................................................................................... 1
Introduction ...................................................................................................................................... 2
AWS hybrid connectivity building blocks ............................................................................................... 3
AWS hybrid connectivity services ................................................................................................. 3
Hybrid network connection ......................................................................................................... 4
  Site-to-Site Virtual Private Network (VPN) ............................................................................. 4
  AWS Direct Connect ........................................................................................................... 4
Hybrid connectivity type and design considerations ................................................................................ 6
  Connectivity type selection ......................................................................................................... 7
    Time to deploy .................................................................................................................. 7
    Security ............................................................................................................................ 9
    Service-level agreement (SLA) .......................................................................................... 10
    Performance .................................................................................................................... 11
    Cost ................................................................................................................................ 13
  Connectivity type selection summary .................................................................................. 15
Connectivity design selection ..................................................................................................... 16
  Scalability ........................................................................................................................ 16
  Connectivity models ......................................................................................................... 18
  Reliability ........................................................................................................................ 27
Customer-managed VPN and SD-WAN .............................................................................................. 33
  Definition ........................................................................................................................ 33
  Impact on design decisions ................................................................................................. 33
  Requirement definition ....................................................................................................... 33
  Technical solutions ........................................................................................................... 34
Example Corp. Automotive use case ................................................................................................... 35
  Architecture selected by Example Corp. Automotive .......................................................... 40
Conclusion ....................................................................................................................................... 42
Contributors .................................................................................................................................... 43
Further reading ................................................................................................................................ 44
Document revisions .......................................................................................................................... 45
Notices ............................................................................................................................................ 46
Hybrid Connectivity

Publication date: September 22, 2020 (Document revisions (p. 45))

Abstract

Many organizations need to connect their on-premises data centers, remote sites, and the cloud. A hybrid network connects these different environments. This whitepaper describes AWS building blocks and the key things to consider when deciding which hybrid connectivity model is right for you. To help you determine the best solution for your business and technical requirements, we provide decision trees to guide you through the logical selection process.
Introduction

A modern organization uses an extensive array of IT resources. In the past, it was common to host these resources in an on-premises data center or a colocation facility. With the increased adoption of cloud computing, IT resources are delivered and consumed from cloud service providers over a network connection. In some cases, organizations have opted to migrate all existing IT resources to the cloud. In other cases, organizations maintain IT resources both on premises and in the cloud. In both cases, a common network is required to connect on-premises and cloud resources. Coexistence of on-premises and cloud resources is called hybrid cloud and the common network connecting them is referred to as a hybrid network. Even if your organization keeps all of its IT resources in the cloud, it may still require hybrid connectivity to remote sites.

There are several connectivity models to choose from. Although choice of options adds flexibility, selecting the best option requires analysis of the business and technical requirements, and elimination of options that are not suitable. Requirements can be grouped together across considerations such as: security, time to deploy, performance, reliability, communication model, scalability, and more. Once requirements are carefully collected, analyzed, and considered, network and cloud architects identify applicable AWS hybrid network building blocks and solutions. To identify and select the optimal model(s), architects must understand advantages and disadvantages of each model. There are also technical limitations that might cause an otherwise good model to be excluded.

To simplify the selection process, this whitepaper guides you through each key consideration in a logical order. Questions used to collect requirements are listed under each consideration. The impact of each design decision is identified along with possible solutions. Decision trees are presented for some of the considerations as a method to aid decision-making process, eliminate options, and understand the effect of each decision. The whitepaper also applies the whole connectivity model selection and design process to a scenario covering a hybrid use case. It helps you to see how the end-to-end process is executed in a practical example.

This whitepaper is intended to help you select and design the most optimal hybrid connectivity model. This whitepaper is structured as follows:

- **Hybrid connectivity building blocks** - overview of AWS services used for hybrid connectivity.
- **Connectivity selection and design considerations** - definition of each connectivity model, how each impacts the design decision, requirement identification questions, solutions, and decision trees.
- **A customer use case** - an example of how to apply the considerations and decision trees in practice.
AWS hybrid connectivity building blocks

From the hybrid connectivity architecture point of view, there are three primary components that construct the building blocks of a hybrid network connectivity architecture:

**AWS hybrid connectivity services** – these services represent the abstraction layer of the AWS Cloud networking components. They handle the connectivity and routing to the customer infrastructure in AWS and are running on highly scalable and reliable AWS infrastructure.

**Hybrid network connection** – this component refers to the connection from the on-premises networking edge device to the AWS Cloud (it can be physical connection such as AWS Direct Connect, or an overlay connection such as a Site-to-Site (S2S) VPN)

**On-premises customer gateway device (CGW)** – this networking device must meet AWS technical requirements and perform IP routing and forwarding.

*Note*
For connections to Direct Connect with port speeds of 1 Gbps or higher, your customer gateway device needs to meet the requirements listed under the Prerequisites section of the Direct Connect user guide.

*Note*
For Site-to-Site VPN, the customer gateway device can be a physical or software appliance. For more information about tested network devices by AWS, see Your customer gateway device in the Site-to-Site VPN User guide.

Because this whitepaper focuses on the selection and design of the hybrid connectivity, the following topics provide a brief definition of each of the connectivity types with a link to the respective documentation for further details. We recommend that you have a good understanding of the content covered in the AWS whitepaper, Amazon Virtual Private Cloud Connectivity Options.

AWS hybrid connectivity services

The AWS network services provide an abstraction layer to highly scalable and available networking components. They play an essential role to enable and facilitate building hybrid networking solutions. At the time of this whitepaper writing, there are three primary service endpoints:

- **AWS Virtual Private Gateway (VGW)** is a regional service, that is highly available, in that it contains a redundant component within a VPC across multiple Availability Zones. It offers distributed IP routing and forwarding at the VPC level. In other words, it acts as the gateway for the VPC to communicate with your remote networks such as on-premises networks. VGW is capable of terminating AWS Site-to-Site VPN connections as well as Direct Connect private virtual interfaces (VIF).

- **Direct Connect gateway (DXGW)** is a globally available resource. You can create the DXGW Direct Connect gateway in any public AWS Region and access it from any other public AWS Regions (except the Beijing and Ningxia Regions in China). A Direct Connect connection can be linked to an AWS DXGW via private or transit VIF. DXGW can be associated with either VGW (directly to a VPC) or can be associated with AWS Transit Gateway.
• **AWS Transit Gateway** is a highly available and scalable regional service that enables you to connect VPCs and on-premises networks through a central hub over Site-to-Site VPN and/or Direct Connect. Conceptually, an AWS Transit Gateway acts like a virtual cloud router. AWS Transit Gateway is highly available by design. It is built on AWS Hyperplane, the Network Function Virtualization platform that underpins many other AWS services, like Network Load Balancer and NAT Gateway. To learn more about the AWS Hyperplane, see the AWS re:Invent session, Another Day, Another Billion Flows. Because it is a logical object, AWS Transit Gateway provides a centralized abstraction layer, where you can create and manage connectivity rules and routing control, which helps to simplify the manageability of the network solution. AWS Transit Gateway enables you to scale your connection throughput with equal cost multi-path (ECMP) routing support over multiple Direct Connect connections or Site-to-Site VPN tunnels. For some common use cases see AWS Transit Gateway examples.

---

**Hybrid network connection**

**Site-to-Site Virtual Private Network (VPN)**

A site-to-site IPsec VPN enables two different networks (sites) to communicate in a secure manner over an untrusted transport such as the internet. From a hybrid connectivity point of view the VPN connection is established between an on-premises site and Amazon Virtual Private Cloud (Amazon VPC). There are two options to establish a Site-to-Site VPN with AWS:

• **AWS Managed Site-to-Site VPN (S2S VPN):** Is a fully managed and highly available VPN service. See AWS Managed VPN for more information. Also, you can optionally enable acceleration for your Site-to-Site VPN connection. See Accelerated Site-to-Site VPN connections

• **Software Site-to-Site VPN (Customer-managed VPN):** Unlike the AWS Managed VPN, with this VPN connectivity option, the customer is responsible for provisioning and managing (configuration, patching, upgrading, licensing) the entire VPN solution. This typically involves running a VPN software (open source or commercial) on an EC2 instance, or it could be a VPN virtual appliance from AWS Marketplace, including SD-WAN solutions. For more information, see Software Site-to-Site VPN.

**AWS Direct Connect**

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated and private network connection from your premises to AWS. See AWS Direct Connect

There are two types of Direct Connect connections: dedicated and hosted connection. See AWS Direct Connect connections for more information.

• **AWS Direct Connect Virtual Interface (VIF):** Virtual interface is logical interface built on top of the physical connection. There are three primary types of VIFs: Private VIF, Public VIF and Transit VIF. See AWS Direct Connect virtual interfaces for more information. Figure 1 illustrates hybrid connectivity model that uses Private and Public VIFs. Public VIF in particular, is used to access all AWS public services, such S3, DynamoDB, as well as public EC2 IP ranges. Public VIF provides the ability to reach any AWS public IP, including AWS S2S VPN endpoints. VPN over public VIF is a common connectivity option for scenarios that require encryption in transit for the Direct Connect (DX) connection.

**Note**

Hosted Virtual Interface (Hosted VIF) is another option that technically offers connectivity to AWS resources. It can refer to either a VIF assigned to a different AWS account than the AWS account which owns the AWS Direct Connect connection. Also, it can refer to a VIF provided by an AWS Direct Connect partner. AWS no longer allows new partners to offer this model, for more information see Hosted Virtual Interfaces (Hosted VIF).
Figure 1 – AWS Direct Connect Private and Public VIFs
Hybrid connectivity type and design considerations

This section of the whitepaper covers the considerations that impact your choices when selecting a hybrid network to connect your on-premises environments to AWS. It follows a logical thought process to support you selecting the most optimal hybrid connectivity solution. The considerations impacting your design are categorized into two types:

- Considerations that impact your connectivity type
- Considerations that impact your connectivity design

Connectivity type considerations will support you deciding between using an internet-based VPN or Direct Connect. Connectivity design considerations will support you deciding how to set up the connections.

The following considerations that impact your connectivity type are covered: time to deploy, security, SLA, performance and cost. After reviewing those considerations, and how they impact your design choices, you will be able to decide if using an internet-based connection or Direct Connect is recommended to meet your requirements.

The following considerations that impact your connectivity design are covered: Scalability, Communication Model, Reliability and third-party SD-WAN integration. After reviewing those considerations, and how they impact your design choices, you will be able to decide the optimal logical design that meets your requirements.

The following structure is used to discuss and analyze each of the selection and design considerations:

- **Definition** – Brief definition of what is the consideration.
- **Impact on design decision** – How the consideration impacts the design choices.
- **Requirement definition** – Provides a set of questions that enable you to collect the requirements associated with the consideration.
- **Technical solutions** – Solutions to address the requirements associated with the consideration.
- **Decision tree** – For some considerations or a group of considerations, a decision tree is provided to help you select the optimal hybrid network solution.

The considerations impacting your hybrid network design are covered in an order where the output of one consideration is considered as part of the input for the subsequent consideration. As illustrated in Figure 1, the first step is to decide on the connectivity type, followed by refining it with the design selection considerations.

Figure 1 demonstrates the two consideration categories, the individual considerations and the logical order in which the considerations are covered in the subsequent sub-sections. Those are the essential considerations when making a hybrid network design decision. However, if the targeted design does not require all these considerations, you can focus on the ones that are relevant to your requirements.
Connectivity type selection

This sub-section of the whitepaper covers the considerations that impact your connectivity type selection.

The following considerations are going to be covered: time to deploy, security, SLA, performance and cost. After covering the considerations, we then provide a summary and a decision tree which demonstrates how those considerations together help you decide between using an internet-based VPN or Direct Connect as your connectivity type.

Topics
- Time to deploy (p. 7)
- Security (p. 9)
- Service-level agreement (SLA) (p. 10)
- Performance (p. 11)
- Cost (p. 13)
- Connectivity type selection summary (p. 15)

Time to deploy

Definition

From a design selection thought process, this is typically the first consideration you need to look at to determine the options you have. This consideration is related with how long you must establish the connectivity with AWS. You need to consider if you need to establish the connectivity within hours, days, weeks, or months. This will influence your decision to use an internet-based connection, a private and dedicated connection or a private connection provided as a managed service by a service provider or AWS Direct Connect Partner.

Impact on design decision

Depending on how long you have before the connection needs to be established will impact if you need to leverage existing links or if you have time to engage service providers to provision new links that can meet your connectivity requirements.
You also need to consider if the connection is required for a long period of time such as when your company will operate for months or years in a hybrid mode or if the connection is required for a temporary purpose. Temporary refers to the need of a connection to achieve certain goal within a defined period of time of usually up to a few weeks. For example, temporary test and development environment in the cloud that needs connection to on-premises during the test and development period only, or for performing data processing in the cloud for a given period of time only.

**Requirement definition**

- What is the required timeline for the deployment? Hours, days, weeks, or months?

**Technical solutions**

When you have hours or a few days to establish connectivity with AWS, you will most likely need to use a link that already exists. For most customers, this means using their existing on-premises internet connection. On top of this connection, you would establish a Site-to-Site VPN to AWS.

When you have a few weeks, in addition to leveraging an internet-based connection, you can look into working with an AWS Direct Connect Partner to establish connectivity with AWS. AWS Direct Connect Partners (APN) help you establish network connectivity between AWS Direct Connect locations and your data center, office, or colocation environment. Certain AWS Direct Connect Partners are approved to offer Direct Connect Hosted Connections. Hosted Connections are usually provisioned faster than Dedicated Connections. When providing a Hosted Connection, in most cases, the AWS Direct Connect Partner leverages their existing physical interconnection to AWS. The AWS Direct Connect Partner will provision each Hosted Connection over a network link between themselves and AWS that is shared by multiple customers.

When you have several weeks to months, in addition to the options mentioned previously, you can look into establishing a dedicated private connection with AWS. AWS Direct Connect Dedicated Connections are facilitated by service providers and AWS Direct Connect Partners. You can contact AWS Direct Connect Partner to learn more about their specific capabilities (connection speed and type). It is common for service providers to install a router (or other network devices) at the customer's premises as well as in the direct connect location to facilitate a Direct Connect Dedicated Connection. Depending on the service provider, location of your site and other physical factors, the installation of a Direct Connect Dedicated Connection can take from several weeks to a few months. Refer to Getting started with AWS Direct Connect for more details.

If you already have your network equipment installed in the same colocation facility where the AWS Direct Connect location exist then you can establish an AWS Direct Connect Dedicated Connection within days. After you request the connection, AWS makes a Letter of Authorization and Connecting Facility Assignment (LOA-CFA) available to you to download, or emails you with a request for more information. The LOA-CFA is the authorization to connect to AWS, and is required by your network provider to order a cross connect for you.

<table>
<thead>
<tr>
<th>Connectivity Type</th>
<th>Provisioning Time</th>
<th>DX Dedicated Connection when you already have equipment within DX location</th>
<th>Direct Connect Hosted Connections</th>
<th>Direct Connect Dedicated Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>internet-based connectivity</td>
<td>Hours to days</td>
<td>Days</td>
<td>Few weeks</td>
<td>Several weeks to months</td>
</tr>
</tbody>
</table>

8
Note
The provided provisioning time guidelines are based on our experience working with customers and may vary. However, when taking into consideration your site location, proximity to direct connect location and pre-existing infrastructure, your service provider or AWS Direct Connect Partner can advise you on the precise provisioning time.

Security

Definition
This section refers to the security considerations that influence the hybrid connectivity type selection. These considerations are:

- transport type – internet or private network connection
- encryption in transit

Impact on design decision

Your security requirements and policies might permit use of internet or require a private network connection between AWS and your company network. They also impact the decision, if encryption in transit must be provided by the network or if performing encryption at application layer is acceptable.

Requirement definition

- Do your security requirements and policies allow the usage of encrypted connections over the internet to connect to AWS or mandate the usage of private network connections?
- When leveraging private network connections, does the network layer have to provide encryption in transit?

Technical solutions

If you can leverage the internet, then AWS Site-to-Site VPN could be used to create encrypted tunnels between your network and your Amazon VPCs or AWS Transit Gateways over the internet. Extending your SD-WAN solution into AWS over the internet may also be an option if you are leveraging an internet-based connection. The Customer-managed VPN and SD-WAN section later in this whitepaper cover the specific considerations for SD-WAN.

If you require the usage of a private network connection between AWS and your company network, then AWS recommends the usage of AWS Direct Connect Dedicated Connections or Hosted Connections. If encryption in transit is required over the private network connection, then you should establish a Site-to-Site VPN over Direct Connect.

<table>
<thead>
<tr>
<th>Site-to-Site VPN</th>
<th>Direct Connect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>Over the internet</td>
</tr>
<tr>
<td>Encryption in transit</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Service-level agreement (SLA)

Definition

Enterprise organizations often require a service provider to specify an SLA for each service the organization may consume. The organization in turn builds its own service(s) on top and may offer their own consumers an SLA. The SLA is important as it describes how the service is provided, operated, and it often includes specific measurable characteristics such as availability. Should the service break the defined SLA, a service provider usually offers a financial compensation under the SLA. The SLA defines the type of measure, the requirement, and measurement period. As example, refer to uptime target definition under AWS Direct Connect SLA.

Impact on design decision

SLA can be a non-negotiable consideration that can force other tradeoffs. If the connectivity is not available, resources running in the cloud could not be accessed. If a formal SLA with applicable service credits for the connectivity is required, appropriate connectivity to satisfy this requirement should be selected.

It could be possible that only a subset of cloud resources requires an SLA, such as the ones used for production applications. Other environments such as development and testing may not require SLAs. This is where a mix of connectivity options could be considered.

Requirement definition

- Is hybrid connectivity connection SLA with service credits required?
- Does the entire hybrid network need to adhere to the uptime target?

Technical solutions

Connectivity type – internet connectivity as underlying transport doesn’t provide an SLA. While great care is taken to have multiple links in place with diverse set of Service Providers (ISPs), control of network resources outside the respective administrative domain of AWS or single ISP is simply not possible. There is limited amount of traffic engineering a cloud provider can do once the traffic exit the border of their network.

AWS Direct Connect offers a formal SLA with service credits. This is the recommended transport if an SLA is required. AWS Direct Connect SLA lists specific minimal configuration requirements for each uptime target such as number of AWS Direct Connect locations, connections, and other configuration details. The failure to satisfy the requirements means that service credits cannot be offered should the service breach defined SLAs. At the time of writing, dedicated AWS Direct Connect links are required at a minimum of 2 locations. Make sure to review the requirements as they may change overtime.

Importantly, even if the service selected to provide the hybrid connectivity is configured to meet the SLA requirements, the rest of the network may not provide the same level of SLA. The AWS responsibility ends at the AWS Direct Connect location, more specifically at the AWS Direct Connect port. Once traffic is handed over to your organization's network, it is no longer the responsibility of AWS. If you use a service provider between AWS and your on-premises network, connectivity is subject to SLA between yourself and the service provider, if applicable. Keep in mind that entire hybrid network is just as good as the weakest part of it when designing hybrid connectivity.

AWS Direct Connect partners also offer AWS Direct Connect connectivity. The partner may offer an SLA with service credits based on their product offering up to the demarcation point with AWS. The option should be evaluated and further researched directly with APN Partners. Refer to the APN list for more details.
Logical design: In addition to the connectivity type you also have to consider other building blocks as part of your overall design. As example, AWS Transit Gateway has its own SLA as does AWS S2S VPN. You might be using AWS Transit Gateway for scale and AWS S2S VPN for security reasons but both have to be designed in a certain way to be eligible for service credits with each respective service.

**Connectivity type selection based on the SLA Decision Tree**

**Performance**

**Definition**

A definition of performance is how well something does its intended function. In the content of this whitepaper, we have hybrid connectivity which has intended function of delivering network traffic between on-premises network and the AWS Cloud. There are multiple factors which influence network performance such as latency, packet loss, jitter, and bandwidth. Depending on applications requirements the importance of each of these factors can vary.

**Impact on design decision**

Based on your application requirements, you need to identify and prioritize the network performance factors that impact your application behavior and user experience. To give further context, we define key factors which impact your connectivity type selection:

- Bandwidth – the maximum data transfer rate of a connection.
- Throughput – the successful transfer rate over a network path which an application can achieve.
- Traffic flow – a flow represents a single, point-to-point network connection between a source and destination.
- Latency – the time taken for a packet to go from source to destination over a network connection.

Having a lot of bandwidth, doesn’t mean that application can use all of it and achieve required throughput. VPNs can restrict throughput due to tunneling overheads. An application might require the use of multiple traffic flows in parallel if it is hitting a per-flow bandwidth limit. Some application might require deterministic performance over a high-bandwidth connection, while others may require both deterministic performance and high bandwidth.
For example, business requirements might state that certain activity must complete within a defined amount of time. Perhaps a backup window has a duration of four hours or a batch processing job must be completed before the start of business hours. The business requirements lead to an understanding of the technical requirements. How much data needs to be copied during the backup window and the throughput required to achieve it. Virtual desktop infrastructure (VDI), where a user interacts with an interface streamed as image over a network connection is sensitive to latency. Delay between input and resulting action can affect user experience. Other applications may not operate well even when latency is low if there is an occasional jitter. Jitter means there is an unpredictable delay. Voice-based applications are susceptible to poor voice quality due to jitter.

**Requirement definition**

- What are the most critical network performance factors for your applications?
- What is the required throughput? (e.g., 10Gbps symmetric)
- What is the maximum acceptable latency between AWS and on-premises network? (AWS can recommend a Direct Connect location selection but does not provide latency guarantees)
- What is the maximum acceptable network variance, or jitter?

**Technical solutions**

When predictable latency and throughput are required, Direct Connect is the recommended choice. Bandwidth could be selected based on throughput requirements. We recommend using Direct Connect when a customer requires a more consistent network experience than internet-based connections. It also provides deterministic performance. Private VIF and transit VIF both support jumbo frames (9001 and 8500 bytes, respectively), which reduce number of packets and overheads through the network and can improve throughput.

Using a VPN over AWS Direct Connect adds encryption. However, it reduces MTU size, which might reduce throughput. For more information about technical capabilities, see Traffic engineering.

Note that AWS Transit Gateway allows customers to horizontally scale the number of VPN connections and throughput accordingly with equal-cost multi-path routing (ECMP). For more information, see Traffic engineering.

Another option is to use a Site-to-Site VPN over the internet. Bandwidth available over internet has been steadily growing over the years. While it is an attractive option due to low cost and is almost universally accessible; keep in mind that performance over the internet is best effort but it can provide high bandwidth considering your on-premises access speed. Internet weather events, congestion, increased latency periods are not unusual. AWS does offer a solution with Accelerated Site-to-Site VPN connections, which can mitigate some of the downsides of the internet. The Accelerated Site-to-Site VPN uses AWS Global Accelerator which allows VPN traffic to enter AWS network as early as possible and as close as possible to the customer gateway device. This option helps organizations optimize their VPN over the internet. It optimizes the network path, using the congestion-free AWS global network to route traffic to the AWS Site-to-Site VPN endpoint. You can use an accelerated VPN connection to avoid network disruptions that might occur when traffic is routed over the public internet.
Cost

Definition

In the cloud, the cost of hybrid connectivity includes cost of provisioned resources and usage. Cost of provisioned resources is measured in units of time, such as hourly. Usage is for data transfer and processing, usually measured in gigabytes (GB). Other costs includes the cost of connectivity to the AWS network point of presence. If your network is within the same colocation facility, it might be as little as the cost of a cross connect. If your network is in different location, there will be a service provider and/or Direct Connect partner costs involved.

Impact on design decisions

Organizations try to maximize efficiency and reduce cost. An optimal hybrid connectivity solution has to meet business and technical requirements at the lowest cost possible. If connectivity is provisioned with just enough bandwidth to meet requirements, it optimizes for current cost. However, it might be hard and costly to scale the connectivity if requirements change. Another aspect to consider is that at-scale, private connectivity can often be cheaper even with the higher cost of provisioned resources, including service provider cost. This is because data transfer cost per GB over Direct Connect is cheaper than over the internet. For example, if you have bandwidth-heavy workloads that you want to run on AWS, Direct Connect reduces your network costs into and out of AWS in two ways. First, by transferring data to and from AWS directly, you can reduce your bandwidth commitment to your internet service provider. Second, all data transferred over your dedicated connection is charged at the reduced Direct Connect data transfer rate rather than internet data transfer rates.

With AWS, you can elastically adjust your usage up and down. If you are using a network service provider for connectivity between on-premises and a Direct Connect location, your ability to change your bandwidth commitments is based on your contract with the service provider. AWS can deliver your traffic to any AWS Region, except China, from any AWS network point of presence using AWS backbone. This capability has many technical benefits over using just internet to access remote AWS Regions. There is a data transfer cost premium for using AWS backbone. If there is an AWS Transit Gateway in the traffic path, it adds data processing cost per GB.

Finally, AWS charges for data egress with hybrid connectivity solutions. Optimal application design keeps data processing within AWS and minimizes unnecessary data egress. Data ingress to AWS is free. This
means that any use case that sends a lot of data to AWS is very economical from the data transfer cost perspective.

Note: As part of the overall connectivity solution, in addition to the AWS connection cost, you should also consider cost of the end-to-end connectivity. This includes service provider cost, cross connects, and racks and equipment within a Direct Connect location (if required).

**Requirement definition**

- How much data do you anticipate to send to AWS per month?
- How much data do you anticipate to send from AWS per month?
- Is this connectivity temporary or permanent?

**Technical solutions**

If you are not sure whether you should use internet or private connectivity at this point, calculate a breakeven point before Direct Connect becomes cheaper than using internet. If the volume of data means that Direct Connect is cheaper, and you require a permanent connectivity, Direct Connect is the optimal connectivity choice.

If the connectivity is temporary and internet meets other requirements, it could be cheaper to use AWS Site-to-Site VPN over internet due to elasticity of the internet. This choice assumes that you have sufficient internet connectivity in your on-premises network.

If you are within a facility that has Direct Connect, you can establish a cross connect to AWS. This means using a dedicated connection that comes at fixed sizes. Direct Connect partners offer further bandwidth granularity and smaller sizes, which could optimize your connectivity cost. For example, you can start at 50Mbps hosted connection vs 1Gbps dedicated connection.

With AWS Transit Gateway you can share your VPN and Direct Connect connections with many VPCs. While you are charged for the number of connections that you make to the AWS Transit Gateway per hour and the amount of traffic that is processed by the AWS Transit Gateway, it simplifies management and reduces number of VPN connections and VIFs required. Lower operational overhead yield benefits and cost savings that can easily outweigh the additional cost of AWS Transit Gateway data processing. Optionally, you can consider a design where AWS Transit Gateway is in the traffic path to most VPCs but not all. This approach avoids the AWS Transit Gateway data processing fees for use cases where you require a transfer of very large amounts of data into AWS. For more information, see Connectivity Models (p. 18).

Another approach is to combine Direct Connect as a primary path and use AWS Site-to-Site VPN over the internet as backup and failover path. While technically feasible and cost effective, this solution has technical challenges, discussed in Reliability, and can be difficult to manage. AWS does not recommend it for highly critical workloads.

The last approach is a customer-managed VPN or SD-WAN deployed in Amazon EC2 instances. Compared to AWS Site-to-Site VPN, this approach can be cheaper at scale if many tunnels, each with low-bandwidth needs, are required. There is also a management overhead, the cost of licensing, and the cost of EC2 resources for each virtual appliance to consider.

<table>
<thead>
<tr>
<th>Category</th>
<th>Customer-managed VPN or SD-WAN</th>
<th>AWS S2S VPN</th>
<th>AWS Accelerated S2S VPN</th>
<th>AWS Direct Connect Hosted Connection</th>
<th>AWS Direct Connect Dedicated Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires customer</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

14
<table>
<thead>
<tr>
<th>Category</th>
<th>Customer-managed VPN or SD-WAN</th>
<th>AWS S2S VPN</th>
<th>AWS Accelerated S2S VPN</th>
<th>AWS Direct Connect Hosted Connection</th>
<th>AWS Direct Connect Dedicated Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>internet connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provisioned resources cost</td>
<td>EC2 instance and software licensing</td>
<td>AWS S2S VPN</td>
<td>AWS S2S VPN and AWS Global Accelerator</td>
<td>Applicable capacity slice of port cost</td>
<td>Dedicated port cost</td>
</tr>
<tr>
<td>Data transfer cost</td>
<td>Internet rate</td>
<td>Internet rate or Direct Connect rate</td>
<td>Internet with data transfer premium</td>
<td>Direct Connect rate</td>
<td>Direct Connect rate</td>
</tr>
<tr>
<td>Transit Gateway</td>
<td>Optional</td>
<td>Optional</td>
<td>Required</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Data processing cost</td>
<td>N/A</td>
<td>Only with AWS Transit Gateway</td>
<td>Yes</td>
<td>Only with AWS Transit Gateway</td>
<td>Only with AWS Transit Gateway</td>
</tr>
<tr>
<td>Can be used over AWS Direct Connect?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 1 – Cost effectiveness comparison

**Connectivity type selection summary**

The considerations discussed thus far focused on the connectivity type selection. The following decision tree provides a summary of the considerations covered in the preceding sections. For details about each consideration refer to the associated consideration section.
Hybrid Connectivity AWS Whitepaper
Connectivity design selection

This sub-section of the whitepaper covers the considerations which impact your connectivity design selection. Connectivity design includes the logical aspects as well as how to design and optimize the hybrid connectivity reliability.

The following considerations are covered: scalability, connectivity models, reliability, and customer-managed VPN and SD-WAN.

Topics
- Scalability (p. 16)
- Connectivity models (p. 18)
- Reliability (p. 27)

Scalability

Definition

Scalability refers to the size of the solution. This size can be related to the entire solution or to a specific component(s) of it.

When designing a solution and hybrid networking connectivity in particular, you need to consider the current size, as well as the anticipated growth of the solution. This growth can be either an
organic growth of a solution, or might be related to a merger and acquisition type of scenarios, where the size can be increased dramatically within a short period of time. In the context of a hybrid network connectivity design, scalability refers to the design's ability to support the current and future requirements related to:

- Number of on-premises sites to be connected to AWS
- Number of AWS Regions to be used
- Number of Amazon VPCs within each Region
- Number of routes to be exchanged
- Bandwidth requirements

Impact on the design

The understanding of the current and the anticipated future scale requirements is critical, because it will influence the decision with regard to the optimal connectivity option selection and design. To be able to analyze the connectivity options in relation to the targeted solution scale, first we need to identify what are the influencing factors that need to be considered as part of the scale analysis when selecting and designing a hybrid connectivity solution architecture. The following list summarizes the key elements that impact the design decision regarding scale:

- **Number of Amazon VPCs** – The number of VPCs that need to be connected to an on-premises site(s). Different connectivity options have limits that need to be taken into consideration at the decision-making stage.
- **Number of AWS Regions to be used** – For multi-Region architectures, it’s important to identify the required number of Regions to connect or anticipated to be connected to an on-premises site. This helps to minimize unexpected limitations in terms of the supported number of Regions to connect to, and major design changes.
- **Number of on-premises sites to be connected to AWS** – The number of sites to be connected to AWS impacts the decision of how many connections are required to be set up that will influence the entire hybrid connectivity design. From a logical design point of view, this also has implications on the routing complexity, such as number of BGP peering sessions.
- **The number of advertised prefixes** – This element is related to the control plane aspect (IP routing). Because different AWS services have different quotas, the required scale of IP routing information (routes) to be advertised to or from AWS can influence the design decision.
- **Bandwidth** – In the context of scalability, this refers to the ability of a connection or link to support increased bandwidth capacity. For example, from 1G to 10G over same fiber link, or more VPN bandwidth capacity by adding more VPN Tunnels.

Note: Depending on the targeted solution architecture, not all of the preceding elements need to be taken into consideration. However, they can serve as the foundational elements to identify scalability requirements of most common hybrid network solutions. This whitepaper focuses on the hybrid connectivity selection and design. Therefore, the preceding scale elements are mainly focused on the hybrid connectivity selection and design. Nevertheless, we recommend that you look at the big picture. Therefore, we further recommend that you expand the scale consideration of the hybrid connectivity to the VPC’s networking architecture. For more information about the selected hybrid connectivity design, see the AWS whitepaper Building a Scalable and Secure Multi-VPC AWS Network Infrastructure.

Requirement definition

- What is the current or anticipated number of VPCs which require connectivity to on-premises site(s)?
- Are these VPCs deployed in a single AWS Region or multiple Regions?
- How many on-premises sites need to be connected to AWS?
• How many customer gateway devices (e.g. routers) you have per site that need to connect to AWS?
• How many routes are expected to be advertised to Amazon VPCs as well as the number of expected routes to be received from AWS side?
• Is there a requirement to increase bandwidth to AWS overtime?

**Technical solutions**

To address scale requirements as part of the hybrid connectivity design, ideally it should be combined with the connectivity model design. Therefore, Connectivity models (p. 18) incorporate scale as part of the targeted connectivity model design.

The following are recommended best practices to minimize scale complexity of hybrid network connectivity design:

• Use route summarization to reduce the number of routes advertised to and received from AWS. This indicates that a structured IP addressing scheme needs to be planned ahead of time that ultimately will simplify the use of route summarization. You should design this with traffic engineering in mind. For more information, see Traffic engineering (p. 28).
• Minimize the number of BGP peering sessions by using DXGW with VGW or AWS Transit Gateway, where a single BGP peering session can provide connectivity to multiple VPCs.

**Connectivity models**

**Definition**

Connectivity models refer to the communication pattern between on-premises networks and cloud resources in AWS. Cloud resources can be deployed within an Amazon VPC within a single AWS Region or across multiple Regions. AWS services, such as Amazon S3 and DynamoDB, can have a public endpoint in a single Region or in multiple Regions.

**Impact on the design decision**

The connectivity model is typically driven by the required communication or traffic pattern. That is essential to be identified and taken into consideration at the early design planning and decision stage.

**Defining the requirements**

• Is there a requirement for cross-VPC communication to be enabled (within a Region and/or across Regions)?
• Is there any requirement to access AWS public endpoints directly from on-premises?
• Is there a requirement to access AWS services using VPC endpoints from on-premises?

**Technical solution**

The following are some of the most common connectivity model scenarios. Each connectivity model covers requirements, attributes, and considerations.

Note: As highlighted earlier, this whitepaper is focused on the hybrid connectivity between on-premises networks and AWS. For further details on the design to interconnect VPCs, see the AWS whitepaper Building a Scalable and Secure Multi-VPC AWS Network Infrastructure.
AWS Accelerated Site-to-Site VPN – AWS Transit Gateway, Single AWS Region.

This model is constructed of the following:

- Single AWS Region
- AWS Managed Site-to-Site VPN connection with AWS Transit Gateway
- Accelerated VPN enabled

![AWS Cloud diagram showing connectivity model attributes](image)

*Figure 1 – AWS Managed VPN – AWS Transit Gateway, Single AWS Region*

**Connectivity model attributes**

- Provides the ability to establish more optimized VPN connection performance over the public internet, by using **AWS accelerated Site-to-Site VPN connections**. This routes traffic from your on-premises network to an AWS edge location that is closest to your customer gateway device.
- Provides the ability to achieve higher VPN connection bandwidth by configuring multiple VPN tunnels with ECMP.
- Can be used for connecting from one or multiple (high scale) numbers of remote sites.
- Offers automated failover, with dynamic routing (BGP).
- With AWS Transit Gateway connected to VPCs, all the connected VPCs can share the VPN connection. Also, full or partial mesh connectivity can be achieved between the VPCs. With AWS Transit Gateway, you can control the desired communication model among the VPCs. For more information, see How transit gateways work.
- Offers flexible design options to integrate third-party security and SD-WAN virtual appliances with AWS Transit Gateway. For more information, see Centralized network security for VPC-to-VPC and on-premises to VPC traffic.

**Scale considerations**

- Up to 50 Gbps of bandwidth with multiple IPsec VPN tunnels and ECMP configured. Each traffic flow will be limited to the maximum bandwidth per VPN tunnel.
Hybrid Connectivity AWS Whitepaper
Connectivity models

- **Hundreds** of VPCs can be connected per AWS Transit Gateway.
- For information about other scale limits, such as number of routes, see Site-to-Site VPN quotas.

**Other considerations**

- Additional AWS Transit Gateway processing cost for data transfer between on-premises data center and AWS.
- Security groups in a remote VPC cannot be referenced over AWS Transit Gateway. If security group referencing is a requirement, we recommend that you consider VPC peering. However, VPC peering adds operational complexity to build and manage a large number of VPC point-to-point peering at scale.

**AWS DX – DXGW with VGW, Single Region**

This model is constructed of the following:

- Single AWS Region
- Dual AWS Direct Connect Connections to independent DX locations
- AWS DXGW directly attached to the VPCs using VGW
- Optional usage of AWS Transit Gateway for cross-VPC communication

![AWS DX – DXGW with VGW, Single AWS Region](image)

**Figure 1 – AWS DX – DXGW with VGW, Single AWS Region**

**Connectivity model attributes**

- Provides the ability to connect to VPCs and/or DX connection(s) in other Regions in the future
- Offers automated failover, with dynamic routing (BGP)
- With AWS Transit Gateway connected to VPCs, full or partial mesh connectivity can be achieved between the VPCs. With AWS Transit Gateway, you can control the desired communication model among the VPCs. For more information, see How transit gateways work.

**Scale considerations**
Hybrid Connectivity AWS Whitepaper

Connectivity models

• 100 routes per Private VIF
• Up to 10 VPCs can be connect per DXGW over a single BGP session. If more VPCs need to be connected, additional DXGWs can be added to facilitate the connectivity at scale.
• Additional AWS Direct Connect connections can be added as desired.
• For more information about the scale limits, such as the number of supported prefixes, or the number of VIFs per DX connection type (dedicated or hosted), see AWS Direct Connect quotas.

Other considerations

• Does not incur AWS Transit Gateway-related processing cost for data transfer between AWS and on-premises networks.
• Security groups of a remote VPC can't be referenced over AWS Transit Gateway. If security group referencing is a requirement, we recommend that you consider VPC peering.
• VPC peering can be used instead of AWS Transit Gateway to facilitate the communication between the VPCs. However, this adds operational complexity to build and manage large number of VPC point-to-point peering at scale.
• If cross-VPC communication is not required, neither AWS Transit Gateway nor VPC peering is required in this connectivity model.

AWS DX – DXGW with VGW, Multi-Regions, and AWS Public Peering

This model is constructed of the following:

• Multiple AWS Regions
• Dual AWS Direct Connect Connections to independent DX locations
• Single on-premises data centers with dual connections to AWS
• AWS DXGW directly attached to no more than 10 VPCs using VGW
• Optional use of AWS Transit Gateway for Inter-VPC and Inter-Region communication
Hybrid Connectivity AWS Whitepaper
Connectivity models

Figure 1 – AWS DX – DXGW with VGW, Multi-Regions, and Public VIF

Connectivity model attributes

- AWS DX public VIF is used to access AWS public services, such as Amazon S3 and DynamoDB, directly over the AWS DX connections.
- Provides the ability to connect to VPCs and/or DX connection(s) in other Regions in the future.
- With AWS Transit Gateway connected to VPCs, full or partial mesh connectivity can be achieved between the VPCs.
- Cross-VPC and Cross-Region VPC communication is facilitated by AWS Transit Gateway peering.

Scale considerations

- 100 routes per private VIF
- Up to 10 VPCs can be connect per DXGW over a single BGP session. If more VPCs need to be connected, additional DXGWs can be added to facilitate the connectivity at scale.
- Additional AWS DX connections can be added as desired.

Other considerations

- Does not incur AWS Transit Gateway-related processing costs for data transfer between AWS and on-premises networks.
- Security groups of a remote VPC cannot be referenced over AWS Transit Gateway. If security group referencing is a requirement, VPC peering can be considered.
- VPC peering can be use instead of AWS Transit Gateway to facilitate the communication between the VPCs. However, this adds operational complexity to build and manage large number of VPC point-to-point peering at scale.
- If cross-VPC communication is not required, neither AWS Transit Gateway nor VPC peering is required in this connectivity model.
AWS DX – DXGW with AWS Transit Gateway, Multi-Regions, and AWS Public Peering

This model is constructed of the following:

- Multi AWS Regions
- Dual Direct Connect connections to independent DX locations
- Single on-premises data center with dual connections to AWS
- AWS DXGW with AWS Transit Gateway
- High scale of VPCs per Region

![Figure 1 – AWS DX – DXGW with AWS Transit Gateway, Multi-Regions, and AWS Public VIF](image)

**Connectivity model attributes**

- AWS DX public VIF is used to access AWS public resources, such as Amazon S3 and DynamoDB, directly over the AWS DX connections.
- Provides the ability to connect to VPCs and/or DX connection(s) in other Regions in the future.
- With AWS Transit Gateway connected to VPCs, full or partial mesh connectivity can be achieved between the VPCs.
- Cross-VPC and Cross-Region VPC communication facilitated by AWS Transit Gateway peering.
- Offers flexible design options to integrate third-party security and SD-WAN virtual appliances with AWS Transit Gateway. For more information, see Centralized network security for VPC-to-VPC and on-premises to VPC traffic.

**Scale considerations**
• The number of routes to and from AWS Transit Gateway are limited to the maximum supported number of routes over a Transit VIF. Inbound and outbound numbers vary. For more information about scale limits and support for the number of routes, see AWS Direct Connect quotas. We recommend route summarization to avoid going over this limit.

• Scale up to thousands of VPCs per AWS Transit Gateway over a single BGP session to DXGW, assuming the provided performance by the provisioned AWS DX connection(s) is sufficient.

• Single Transit VIF per AWS DX.

• Additional AWS DX connections can be added as desired.

Other considerations

• Incurs additional AWS Transit Gateway processing cost for data transfer between AWS and on-premises site.

• Security groups of a remote VPC cannot be referenced over AWS Transit Gateway. If security group referencing is a requirement, we recommend that you consider VPC peering.

• VPC peering can be use instead of AWS Transit Gateway to facilitate the communication between the VPCs. However, VPC peering adds operational complexity to build and manage a large number of VPC point-to-point peering at scale.

• A single DXGW can support up to three AWS Transit Gateways. If more TGWs are required, additional DXGW need to be added. For more information, see the following connectivity model.

AWS DX – DXGW with AWS Transit Gateway, Multi-Regions (more than 3)

This model is constructed of the following:

• Multi AWS Regions (more than 3)

• Dual on-premises data centers

• Dual AWS Direct Connect Connections across to independent DX locations per Region

• AWS DXGW with AWS Transit Gateway

• High scale of VPCs per Region

• Full mesh of peering between AWS Transit Gateways
Connectivity model attributes

- Has the lowest operational overhead
- Uses AWS DX public VIF to access AWS public resources, such as Amazon S3, with DynamoDB directly over the AWS DX connections.
- Provides the ability to connect to VPCs and/or DX connection(s) in other Regions in the future.
- Has the ability to achieve full or partial mesh connectivity between the VPCs, with AWS Transit Gateway connected to VPCs.
- Cross-Region VPC communication is facilitated by AWS Transit Gateway peering.
- Offers flexible design options to integrate 3rd party security and SD-WAN virtual appliances with AWS Transit Gateway. See: Centralized network security for VPC-to-VPC and on-premises to VPC traffic.
Scale considerations

- The number of routes to and from AWS Transit Gateway are limited to the maximum supported number of routes over a Transit VIF (inbound and outbound numbers vary). For more information about the scale limits, see AWS Direct Connect quotas. We recommend route summarization to avoid going over this limit.
- Scale up to thousands of VPCs per AWS Transit Gateway over a single BGP session per DXGW (assuming the provided performance by the provisioned AWS DX connections is sufficient).
- Up to three AWS Transit Gateways can be connected per DXGW.
- If more than three Regions need to be connected using AWS Transit Gateway, then additional DXGWs are required.
- Single Transit VIF per AWS DX
- Additional AWS DX connections can be added as desired.

Other considerations

- Incurs additional AWS Transit Gateway processing cost for data transfer between on-premises site and AWS.
- Security groups of a remote VPC cannot be referenced over AWS Transit Gateway. If security group referencing is a requirement, we recommend that you consider VPC peering.
- VPC peering can be use instead of AWS Transit Gateway to facilitate the communication between the VPCs. However, this adds operational complexity to build and manage large number of VPC point-to-point peering at scale.

The following decision tree covers the scalability and communication model considerations:
along with the number of required VPC to be connected to the VPN connection(s) to help you to make the decision.

**Reliability**

**Definition**

Reliability refers to the ability of a service or system to perform its expected function when required. Also, the reliability of a system can be measured by the level of its operational quality within a given timeframe. On the other hand, resiliency refers to the ability of a system to recover from infrastructure or service disruptions, dynamically and reliably.

For more details about how availability and resiliency are used to measure reliability, see the AWS Well-Architected Framework, *Reliability Pillar*.

**Impact on the design decision**

The following are the primary aspects that can influence the design decision:

- **The required level of availability** – The availability of a connection to AWS needs to be evaluated. This would be based on the level of criticality to the business with regard to the connected on-premises site, criticality of the resources access in AWS site and the impact magnitude of a downtime on the business.

- **The required level of resiliency** – Evaluate the impact of a downtime duration. There are use cases that demand minimum downtime. Examples include financial services, and critical infrastructure management services.

Similarly, if the redundant network components (for example, links or network devices) are not reliable enough to provide the expected function on their own, such as connection performance, then this means low resiliency to failures. This would result in poor and degraded user experience.

**Requirements definition**

- What is the impact magnitude on the business in case of a connectivity failure to AWS?
- What is the required level of availability (up time target, e.g., 99.9%) per on-premises site that need to be connected to AWS?
- From a business point of view, does the cost following a connectivity failure to AWS outweigh the cost of deploying a highly reliable connectivity model to AWS?
- Is the cost in anyway the primary limiting factor to the business?

**Technical Solution**

Reliability of a hybrid network connection depends on several factors, such as security, operational excellence, etc. However, the primary factor is resiliency. Therefore, resiliency is the primary focus of this section.

First, it is important to note that not every hybrid network connectivity solution or business requires a high level of reliability. That's why we recommend that you evaluate first, so that you are able to identify where a high level of reliability is needed. In some scenarios, a primary site may require reliable (redundant and resilient) connections because the downtime has higher impact on the business. Regional sites, however, may not require same level of reliability due to the lower impact on the business in case of a failure event. We recommend that you refer to the AWS Direct Connect Resiliency...
**Recommendations**. This resource explains the AWS best practices for ensuring high resiliency with AWS Direct Connect design.

To achieve a reliable hybrid network connectivity solution in the context of resiliency, the design needs to take into consideration the following aspects.

**Redundancy**

Redundancy aims to eliminate any single point of failure in the hybrid network connectivity path, including but not limited to; network connections, edge network devices, redundancy across Availability Zones, AWS Regions, and DX locations, as well as power sources to the devices, etc. For the purpose and scope of this whitepaper, redundancy focuses on the network connections, edge devices (for example, customer gateway devices), AWS DX location, and AWS Regions (for multi-Region architectures).

**Reliable failover components**

In some scenarios, a system might be available (functioning) but it is not performing its functions at the minimum required level. From an operational quality point of view, the system may not be delivering the intended service or performing a function reliably even it is technically available. Such a situation is very common, following a failover event, to a redundant component (for example, redundant network link). This is where a reliable redundant component can help to mitigate or eliminate such situation and make the overall design more resilient.

**Failover time**

Failover time is another key aspect of resiliency, because you might have a redundant component or connection. However, following a failure event of the primary component, it takes long time for the secondary component to start taking over, or even requires manual configuration update by administrator. This typically leads to a less resilient solution even though there is redundant component in the design.

As part of the hybrid network connectivity, one of the key metrics that a cloud and network architect need to consider is the failure detection time. This is an important aspect because you might have a routing design or protocol tuned to fail over very quickly, however, this failover operation won’t be triggered fast if the failure itself is not reported fast enough to the routing protocol.

There are many techniques to speed up the failure detection, depending on things like connectivity type and physical medium. With AWS hybrid connectivity, if you are using VPN, you might need to look into VPN dead peer detection. If you are working with AWS DX connection, you need to look at Bidirectional Forwarding Detection (BFD), which helps to achieve a faster routing re-convergence time, and will result in a higher solution resiliency. Note that Asynchronous BFD is automatically enabled for DX virtual interfaces on the AWS side. However, you must configure your router for asynchronous BFD to enable it for your connection. For more information, see How do I enable BFD for my DX connection?

In addition, you must consider the on-premises network side, because if there is any routing protocol deployed, peering with multiple CGWs, this routing protocol needs to converge as well. Each routing protocol has its own convergence speed, and recommended tuning timers to achieve fast and stable convergence time.

**Traffic engineering**

Traffic engineering, in the context of resilient hybrid network connectivity design, aims to address how traffic should flow over multiple available connections in both normal and failure scenarios. Therefore, we recommend that you follow the concept of “design for failure,” where you need to look at how the solution will operate in different failure scenarios and whether it will be acceptable by the business or not. This section discusses some of the common traffic engineering use cases that aim to enhance the overall resiliency level of the hybrid network connectivity solution.
To design an effective traffic engineering solution, you need to have a good understanding of how each of the AWS networking components (Amazon VPC and gateways), handle IP routing in terms route evaluation and selection, as well as the possible mechanisms to influence the route selection. The figure below illustrates a summarized version of how the IP routing decision is made at different level within AWS from the VPC to the networking gateways components.

**Figure 1 – Routing evaluation within Amazon VPC and associated gateways**

**Note**
In the VPC route table, you might reference a prefix list that has additional route selection rules. For more information about this use case, see Route priority. AWS Transit Gateway route tables also support prefix lists but, once applied, they get expanded to specific route entries.

**Dual Site-to-Site VPN connections with more specific routes example**

This scenario is based on a small on-premises site connected to a single AWS Region via redundant VPN connections over the internet to the AWS Transit Gateway. The traffic engineering design is depicted in the figure 13. It shows how, using traffic engineering, you can influence the path selection, that increases the hybrid connectivity solution reliability by:

- Providing resilient hybrid connectivity – redundant VPN connection that provides same performance capacity, automated failover by using dynamic routing protocol (BGP), speed up connection failure detection by using VPN dead peer detection.
- Providing performance efficiency – configure ECMP per VPN connection to AWS Transit Gateway, helps to maximize the overall VPN connection bandwidth. Also, (optionally) by advertising different more specific routes along with the site summary route helps to distribute the load over the two VPN connections.
Figure 1 – Dual Site-to-Site VPN connections with more specific routes example

Dual on-premises sites with multiple DX connections example

The scenario illustrated in the figure 14 shows two on-premises data center sites located in different geographical Regions. They are connected to AWS using the Maximum Resiliency connectivity model (described in the AWS Direct Connect Resiliency Recommendations) using AWS DX with DXGW and VGW. These two on-premises sites are interconnected to each other over a data center interconnect (DCI) link.

One of the on-premises IP prefixes (192.168.0.0/16) that belongs to remote branch sites is advertised from both on-premises data center sites. The primary path for this prefix should be Corporate data center 1. Traffic to and from the remote branch sites will failover to Corporate data center 2 in a failure event of data center 1 or both DX locations. Also, there is site-specific IP prefix for each data center. These prefixes need to be reached directly and via the other data center site in case of both DX locations failure.

By associating BGP Community attributes with the routes advertised to AWS DXGW, you can influence the egress path selection from AWS DXGW side. With these values, you can control the value of the BGP Local_Preference attribute that is to be assigned to the advertised route. For more information refer to AWS DX Routing policies and BGP communities.

In addition, to maximize the reliability of the connectivity at the AWS Region level, each pair of AWS DX connections configure with ECMP, where both can be utilized at the same time for data transfer between each on-premises site and AWS.
With this design, the traffic flows destined to the on-premises networks (with the same advertised prefix length and BGP community) will be distributed across the dual DX connections per site using ECMP. However, if ECMP is not required across the DX connection, the same concept described in Routing policies and BGP communities can be used to further engineer the path selection at a DX connection level.

**Note**

If there are security devices in the path within the on-premises data centers, these devices need to be configured to allow traffic flows leaving over one DX link and coming from another DX link (both links utilized with ECMP) within the same data center site.

### VPN connection as a backup to AWS DX connection example

In some scenarios, VPN can be selected to provide a backup hybrid network connection to an AWS DX. Typically, this type of connectivity model is driven by cost, because it provides lower level of reliability to the overall hybrid connectivity solution for the reasons discussed earlier in this whitepaper, such as indeterministic performance over the internet. There is no SLA that can be obtained for a connection over the public internet. It is a valid and cost-effective connectivity model, and should be used when cost is the top priority consideration and there is limited budget, or possibly as an interim solution until a secondary DX to be provisioned. Figure 15 illustrates the design of this connectivity model.

One key consideration to be taken into account is that, with this design, where both the VPN and DX connections are terminating at the same AWS Transit Gateway, the VPN connection can advertise higher number of routes than the ones that can be advertised over a DX connection connected to AWS Transit Gateway via DXGW. For more information, see [Allowed prefixes interactions](#). This may result in asymmetric routing situation, in cases where more specific routes are advertised over the VPN connection. One simple way to avoid such issue is to configure route filtering at the customer gateway device CGW for the routes received from the VPN connection where, for example, only the summary route(s) is accepted.
**Note**

To create the summary route on the AWS Transit Gateway, specify a static route in the AWS Transit Gateway route table to an arbitrary attachment that you don’t plan to delete anytime soon, so that it is sent along the more specific routes. Otherwise if the CGW filters specifics, it will not see the aggregate routes.

From AWS Transit Gateway routing table point of view, the routes for the on-premises prefix received from the AWS DX connection (via DXGW) and from VPN, both are with the same prefix length and propagated dynamically over BGP. Following the route evaluation order of AWS Transit Gateway (in which routes received over Direct Connect have a higher preference than the ones received over dynamic Site-to-Site VPN), the path over the AWS Direct Connect will be the preferred way to reach the on-premises network(s).

![Diagram of AWS Cloud depicting Hybrid Connectivity](image)

**Figure 1 – VPN connection as a backup to AWS DX connection example**

The following decision tree guides you through making the desired decision for achieving a resilient and reliable hybrid network connectivity. For more information see Using the AWS Direct Connect Resiliency Toolkit to get started.
Customer-managed VPN and SD-WAN

Definition

Connectivity to the internet is a commodity, and available bandwidth continues to increase every year. Some customers choose to build a virtual WAN on top of the internet instead of building and operating a private WAN. A software-defined wide area network (SD-WAN) through intelligent use of software allows companies to rapidly provision and centrally manage this virtual WAN. Other customers choose to adopt traditional self-managed site-to-site VPNs.

Impact on design decisions

SD-WAN and customer-managed VPNs can run over internet or AWS Direct Connect. SD-WAN or any software VPN overlay, is as reliable as the underlying network transport. Therefore, the considerations discussed earlier in this whitepaper with regard to reliability and SLA, are applicable here. For instance, building an SD-WAN overlay over the internet will not offer the same reliability if built over an AWS Direct Connect.

Requirement definition

- Do you use SD-WAN in your on-premises network?
- Are there specific features you require that are only available on certain virtual appliances used for VPN termination?
Technical solutions

We recommend integrating SD-WAN with AWS Transit Gateway. AWS Transit Gateway Connect enables native integration of SD-WAN appliances into AWS. You can seamlessly extend your SD-WAN edge into AWS using standard protocols, such as Generic Routing Encapsulation (GRE) and Border Gateway Protocol (BGP). It provides you with added benefits, such as improved bandwidth, and supports dynamic routing with increased route limits, thus removing the need to set up multiple IPsec VPNs between the SD-WAN appliances and Transit Gateway. Each GRE tunnel can have bandwidth up to 5 Gbps.

AWS can act as a hub or a spoke for SD-WAN sites. AWS backbone can be used to connect different SD-WAN hubs deployed in AWS with a highly reliable and performant network. SD-WAN solutions support automated failover through any available path, additional monitoring, and observability capabilities in a single management pane. Extensive use of automated configuration allows for rapid provisioning and visibility, compared to traditional WANs. Still, use of tunneling and encryption overheads do not compare to dedicated, high-speed fiber links used in private connectivity.

In some cases, you might choose to use a virtual appliance with VPN capability. Reasons for selecting a self-managed virtual appliance include technical features and compatibility with rest of your network. When you select a self-managed VPN or an SD-WAN solution that uses a virtual appliance deployed in an Amazon EC2 instance, you are responsible for the operational management, such as high availability and failover between virtual appliances. While those design considerations increase your operational responsibility, they also could provide you more flexibility. The features and capabilities of the solution depend on the virtual appliance you select.

AWS Marketplace contains many VPN virtual appliances that customers can deploy on Amazon EC2. We recommend that you start with AWS managed Site-to-Site VPN. If that doesn’t meet your requirements, look at other options. The management overhead of virtual appliances is your responsibility.
Example Corp. Automotive use case

This section of the whitepaper demonstrates how the considerations, requirement definition questions, and decision trees are used to help you decide on the optimal hybrid network design. Identifying and capturing requirements is important because they are used as input to the decision trees. Capturing requirements at the beginning avoids further design iterations. When requirements are understood up front, there is less of a chance that you will have to pause a project altogether and place valuable resources on hold while you revisit the design.

We will use Example Corp. Automotive as the illustrative customer throughout this section. They are looking to initially deploy their first analytics project on AWS. The analytics project is focused on analyzing data from cars manufactured by the company and other datasets that already exist in the company’s data centers.

Initially, the company’s architecture group thinks that they will need an AWS account, an Amazon VPC, and few subnets to host production, and development environments. The project team is eager to get started and they requested access to a development environment as soon as possible. Their plan is to go into production in three months.

Example Corp. Automotive also plans to use AWS for several additional projects, such as migrating their enterprise resource planning (ERP) systems, Virtual Desktop Infrastructure (VDI), and another 20 applications from on-premises to AWS over the next six months. Some of the requirements for additional projects are still being defined, but it is clear that their AWS Cloud use is anticipated to grow.

The architecture team decided to use the approach outlined in this whitepaper. They used the requirement definition questions outlined under each consideration to capture the inputs to make their design decisions.

They start with requirements related to the connectivity type that are summarized in the following table.

<table>
<thead>
<tr>
<th>Connectivity type selection considerations</th>
<th>Requirement definition questions</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to Deploy</td>
<td>What is the required timeline for the deployment? Hours, days, weeks, or months?</td>
<td>Dev/Test: 1 week Production: 3 months</td>
</tr>
<tr>
<td>Security</td>
<td>Do your security requirements and policies allow the usage of encrypted connections over the internet to connect to AWS or mandate the usage of private network connections?</td>
<td>Dev/Test: Site-to-Site VPN acceptable Production: private network required</td>
</tr>
<tr>
<td></td>
<td>When leveraging private network connections, does the network layer have to provide encryption in transit?</td>
<td>No, application layer encryption will be used.</td>
</tr>
<tr>
<td>SLA</td>
<td>Is hybrid connectivity SLA with service credits required? (yes/no)</td>
<td>Dev/Test: No Production: Yes</td>
</tr>
<tr>
<td></td>
<td>What is the uptime target? (e.g., 99.9%)</td>
<td>Dev/Test: N/A. Production: 99.99%</td>
</tr>
</tbody>
</table>
Table 1 – Example Automotive Corp connectivity type requirements

Based on requirements received, the architecture team followed the connectivity type decision tree from Figure 1. The decision tree allowed the architecture team to decide on the connectivity type for the development and test environment as well as for the production environment.

For the production environment, they considered the immediate as well as the upcoming requirements. As illustrated in Figure 1, for development and test, Example Corp. Automotive will establish a site-to-site VPN over the internet. For production they are going to work with a service provider to connect their corporate network with Direct Connect. Example Corp. Automotive initially considered using a Direct Connect Hosted Connection. However, due to the requirements for an AWS provided SLA, they selected Direct Connect Dedicated Connections.
After deciding on the connectivity type, the next step is to capture the requirements that impact the connectivity design selection. This is related to the logical design, such how the connections are configured and which AWS services to use in order to support business and technical requirements.

To capture the scalability and communication model requirements, the architecture team used the requirement definition questions from the associated sections of this whitepaper. The requirements related with those two considerations are summarized in the following table.

<table>
<thead>
<tr>
<th>Connectivity design selection considerations</th>
<th>Requirement definition questions</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability</td>
<td>What is the current or anticipated number of VPCs which require connectivity to on-premises sites?</td>
<td>2 initially, growing to 30 in 6 months</td>
</tr>
<tr>
<td></td>
<td>Are these VPCs deployed in a single AWS Region or multiple Regions?</td>
<td>Single Region</td>
</tr>
<tr>
<td></td>
<td>How many on-premises sites need to be connected to AWS?</td>
<td>2 data centers</td>
</tr>
<tr>
<td></td>
<td>How many customer gateway devices (e.g., routers) do you have, per site, that need to connect to AWS?</td>
<td>2 routers per data center</td>
</tr>
<tr>
<td></td>
<td>How many routes are expected to be advertised to AWS VPCs as well as the number of expected</td>
<td>Routes to be advertised to AWS: 20 routes. Routes to be received from AWS: 1 /16 route.</td>
</tr>
<tr>
<td>Connectivity design selection considerations</td>
<td>Requirement definition questions</td>
<td>Answers</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>routes to be received from AWS side?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is there any plan to consider bandwidth increase of the connection to AWS, in the near future?</td>
<td>Dev/Test: 100 Mbps. Production: 500 Mbps growing to 2 Gbps.</td>
</tr>
<tr>
<td>Connectivity Design Models</td>
<td>Is there a requirement for inter-VPC communication to be enabled (within a Region and/or across Regions)?</td>
<td>Yes, within an AWS Region</td>
</tr>
<tr>
<td></td>
<td>Is there a requirement to access AWS public endpoints services directly from on-premises?</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Is there a requirement to access AWS services using VPC endpoints from on-premises?</td>
<td>No</td>
</tr>
</tbody>
</table>

*Table 2 – Example Corp. Automotive connectivity design inputs*

Based on inputs, the architecture team followed the decision tree in the Connectivity Design Model, shown in the preceding table. After anticipating that the number of VPCs are going to grow from 2 to 30 in the next six months, the architecture team decided to use AWS Transit Gateway as the termination gateway for the connection as well as for inter-VPC routing. They’ll use independent AWS Transit Gateways to terminate the VPN connection used for development, testing, and the production connectivity with AWS Direct Connect.

The use of separate AWS Transit Gateways makes change management simpler and provides a clear demarcation between dev/test and production environments. For the production, AWS Direct Connect gateway is required due to AWS Transit Gateway. Public VIF will be used for access to AWS public endpoint services. Figure 2 illustrates the path taken on the decision tree based on requirements collected.
After deciding on the solution to meet the scalability and communication model requirements, the next step is to capture the requirements associated with reliability. This is related with the required level of availability and resilience.

To capture the reliability requirements, the architecture team used the requirement definition questions from the associated section of this whitepaper. The requirements are summarized in the following table.

<table>
<thead>
<tr>
<th>Connectivity design selection considerations</th>
<th>Requirement definition questions</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability</td>
<td>What is the impact magnitude on the business in case of a connectivity failure to AWS?</td>
<td>Dev/Test: Low. Production: High.</td>
</tr>
<tr>
<td></td>
<td>From a business point of view, does the cost following a connectivity failure to AWS outweigh the cost of deploying a highly reliable connectivity model to AWS?</td>
<td>Dev/Test: No. Production: Yes.</td>
</tr>
</tbody>
</table>

*Table 3 – Example Automotive Corp reliability inputs*

Based on inputs received, the architecture team followed the decision tree from the reliability considerations sections covered previously in this whitepaper. After considering the uptime target of 99.99% for the production connectivity and the high business impact if a service interruption event were to happen, the architecture team decided to use two Direct Connect locations and have two links from each on-premises data center to each Direct Connect location (four links in total). The VPN connectivity used for development and testing will also use two VPN connections for additional redundancy. Using traffic engineering techniques, connectivity will be configured as follows:
• For development and testing, traffic is going to be load balanced using ECMP over the two tunnels going to the primary data center. This allows for higher throughput. The tunnels going to the secondary data center will be used in case of failure of the primary tunnels.
• For production, the latency between on-premises and AWS over either one of the direct connect locations is very similar. In this case, they decided to load balance the traffic between AWS and on-premises over the two connections going to the primary data center. Similarly, for on-premises systems running in the secondary data center, traffic is going to be load balanced between the two connections to the secondary data center. In case of failure of the connections, BGP will facilitate an automated failover.

Figure 3 illustrates the path taken on the decision tree based on requirements collected.

![Diagram of decision tree](image)

**Figure 3 – Example Corp. Automotive reliability decision tree**

**Architecture selected by Example Corp. Automotive**

The following diagram illustrates the architecture selected by Example Corp. Automotive after collecting the requirements and navigating the decision trees covered in the previous sections of this whitepaper. It uses AWS Site-to-Site VPN over the internet, terminating on AWS Transit Gateway for development and testing. It then uses AWS Direct Connect with Direct Connect gateway and a second AWS Transit Gateway for the production traffic. AWS Transit Gateway is used for Inter-VPC routing.

From a data path perspective, the VPN tunnels for the primary data center are used as primary paths for development and testing, with the tunnels to the secondary data center used as failover paths. For the production traffic, all connections are used simultaneously. Traffic from AWS prefers the most optimal network connection based on the data center in which the on-premises system is located. Example Corp. Automotive uses similar traffic engineering techniques to prefer appropriate path when traffic is sent to AWS, ensuring that symmetric traffic paths are used to minimize the use of the corporate network between primary and secondary on-premises data centers.
Figure 4 – Example Corp. Automotive selected hybrid connectivity model
Conclusion

Once an organization makes a decision to use the AWS Cloud, a hybrid connectivity model is almost always required. To provide the connectivity, a hybrid network can be built with the most applicable and optimal solution following the connectivity model selection process outlined in this whitepaper. The process consists of considerations arranged in a logical order. The order closely resembles a mental model followed by a seasoned network and cloud architect. Within each group of considerations, decision trees allow for rapid connectivity model selection even with limited input requirements. You might find that some considerations lead to the selection of mutually exclusive solutions. In those cases, as a decision maker, you might need to compromise on some requirements and select the most optimal solution that meets your business and technical requirements.
Contributors

Contributors to this document include:

- Marwan Al Shawi, Solutions Architect, Amazon Web Services
- Santiago Freitas, Head of Technology, Amazon Web Services
- Evgeny Vaganov, Specialist Solutions Architect – Networking, Amazon Web Services
- Tom Adamski, Specialist Solutions Architect – Networking, Amazon Web Services
Further reading

- Building a Scalable and Secure Multi-VPC AWS Network Infrastructure
- Hybrid Cloud DNS Options for Amazon VPC
- Amazon Virtual Private Cloud Connectivity Options
- Amazon Virtual Private Cloud Documentation
- AWS Direct Connect Documentation
- What's the difference between a hosted virtual interface (VIF) and a hosted connection?
Document revisions

To be notified about updates to this whitepaper, subscribe to the RSS feed.

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor update (p. 45)</td>
<td>Fixed broken links.</td>
<td>March 22, 2022</td>
</tr>
<tr>
<td>Initial publication (p. 45)</td>
<td>Whitepaper first published</td>
<td>September 22, 2020</td>
</tr>
</tbody>
</table>
Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2022 Amazon Web Services, Inc. or its affiliates. All rights reserved.