AWS Whitepaper

Cross-Domain Solutions with AWS

Cross-Domain Solutions with AWS: AWS Whitepaper

Table of Contents

Abstract **1**
Abstract 1
Introduction **2**
What is a Cross-Domain Solution? **3**
One-Way Transfer Device 3
Multidomain Data Guard 3
Traditional Deployment 3
How Is a Cross-Domain System Different from Other Security Appliances? **5**
When is a Cross-Domain System Required? **6**
Connecting Cloud-to-Cloud Infrastructure **7**
Amazon VPC 7
Amazon EC2 8
Amazon S3 8
AWS Diode 8
Connecting On-Premises Infrastructure **9**
AWS Direct Connect 9
AWS Advantages for Secure Workloads **10**
Cost 10
Elasticity 10
Purpose-Built Infrastructure 10
Auditability 11
Security and Governance 11
Sample Architectures **12**
Both Security Domains are in the Cloud 12
Deploying a CDS through the Internet or AWS Direct Connect 13
Deploying a CDS across Multiple Regions 15
Conclusion **17**
Contributors **18**
Further Reading **19**
Document history **20**
Notices **21**

Cross-Domain Solutions on AWS

Publication date: **February 2, 2021** (*Document history*)

Abstract

Many corporations, government entities, and institutions maintain multiple security domains as part of their information technology (IT) infrastructure. For the purposes of this document, a security domain is an environment with a set of resources accessible only by users or entities who have permitted access to those resources. The resources are likely to include the resource network fabric, as defined by the security domain's policy.

Some organizations' users need to interact with multiple domains simultaneously. Or a system or user within one security domain needs to communicate directly or obtain data from a system or user in a separate security domain. For security domains with highly sensitive data, organizations can deploy a cross-domain solution (CDS) to allow data transfer between security domains while also helping to ensure the integrity of the domain's security perimeter.

Introduction

To control access across security domains, it's common to employ a specialized hardware solution such as a cross-domain system (CDS) to manage and control the interactions between two security boundaries. When security domains extend across data centers or expand into the cloud, you can encounter additional challenges when including the hardware solution you want in your architecture.

You are not limited to any vendor solution to deploy a CDS on the AWS Cloud. However, one challenge is that you cannot place your own hardware within an AWS data center. This requirement is part of the AWS commitment to maintain security within AWS data centers. As part of the growing need to move data within cloud-based security domains, AWS provides an AWS Service to allow moving data within security domains.

This whitepaper provides best practices for designing hybrid architectures where AWS services are incorporated into one or more security domains within a multidomain environment and to describe a best practice of using a cloud-based CDS service.

What is a Cross-Domain Solution?

The Committee on National Security Systems (CNSS) defines a CDS as a form of controlled interface that enables manual or automatic access or transfer of information between different security domains. We discuss two CDS types in this whitepaper: a one-way transfer (OWT) device, and a multi-domain data guard.

One-Way Transfer Device

An OWT device allows data to flow in a single direction from one security domain to another. A common implementation of an OWT device uses a single strand of fiber-optic cable. To ensure data flows only in one direction, the OWT uses a single optical transmitter. The optical transmitter is placed on only one end of the fiber optic cable (for example, the data producer). The optical receiver is placed on the opposite end (for example, the data consumer). Because they only transfer data in one direction, OWT devices are often referred to as diodes, like the semiconductors of the same name.

Multidomain Data Guard

A multidomain data guard is a specialized system that enables bidirectional data flow between security domains. A common implementation of a multidomain data guard is a single server running a trusted, hardened multi-level operating system with multiple network interface cards (NICs). Each NIC provides a physical demarcation for a single security domain. The multidomain data guard inspects all data transmitted between domains to ensure that the data remains in compliance with a unique rule set that is specific to the guard's deployment.

Traditional Deployment

Figure 1 shows a traditional cross-domain solution deployment between two security domains. Security Domain A is connected to Security Domain B using a CDS. If the CDS is an OWT device, resources deployed in Network A can communicate to resources deployed in Network B by sending data through the CDS. If instead, the CDS is a multidomain data guard, resources in either security domain can communicate with the other security domain by sending data through the CDS. In the following example, the CDS is administrated and physically located within the protections of Security Domain B.

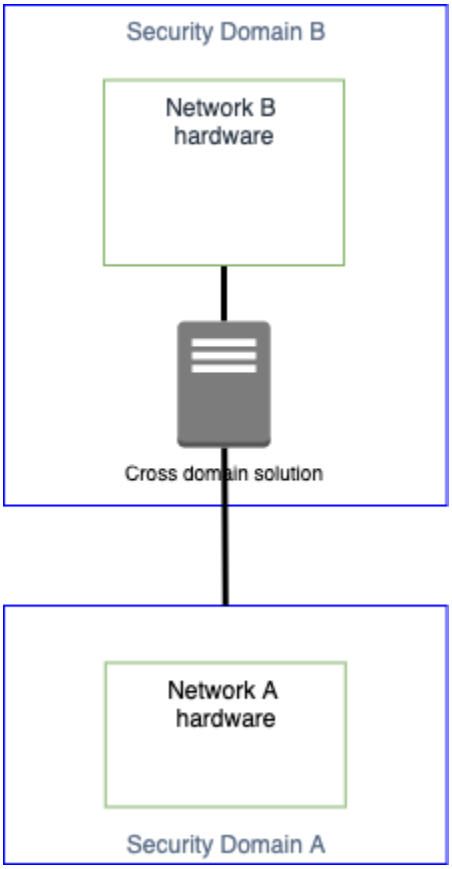

Figure 1: Traditional CDS deployment

How Is a Cross-Domain System Different from Other Security Appliances?

A CDS differs from other security appliances such as firewalls, web application firewalls (WAFs), and intrusion detection or prevention systems. In addition to providing physical, network, and logical isolation between domains, cross-domain solutions offer additional security mechanisms. These additional mechanisms include virus scanning, auditing and logging, and deep content inspection in a single solution. When the CDS is included in a larger security program, these capabilities help prevent both exploitation and data leakage. By design, CDS systems are intended to fail data passing if anything is suspect or not recognizable in the flow.

When is a Cross-Domain System Required?

A business decision to employ a CDS should evaluate the high cost of ownership involved with integration, procurement, and maintenance. Be aware that a high degree of customization is often required for each individual CDS deployment.

You would often deploy a CDS due to regulatory or policy requirements, or in situations where inappropriate access to data would cause significant impact to your organization. Because of these reasons, the CDS is an integral component of the architecture and may even be required to achieve an Authority to Operate (ATO) from your organization's security and compliance program.

Once an ATO is achieved, it can be cumbersome to make changes to a CDS configuration (for example, altering the message rule set) without affecting the ATO's approval. If these drawbacks outweigh the additional security provided by a CDS, you should consider another option, like a WAF.

Connecting Cloud-to-Cloud Infrastructure

AWS provides service offerings to help you transfer information from one AWS Cloud Region to another. Many of the services AWS offers are common for on-premises as well as in the cloud. The following sections describe some of the key services that AWS offers, including:

- Amazon Virtual Private Cloud (Amazon VPC)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Simple Storage Service (Amazon S3)
- AWS Diode

> **Note**
>
> As of paper publication in December 2020, AWS Diode has the sole purpose of directly supporting the US Government, in that it controls data flowing to AWS classified regions. Commercial entities can use the service, to supply the US Government with their data or services. Commercial entities cannot use the service in any other way. For information about how to determine current availability, see AWS Diode.

Amazon VPC

Amazon VPC lets you provision a logically isolated section of your AWS environment so that you can launch resources in a virtual network you define. You have complete control over your virtual networking environment, including the selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. The network configuration for a VPC is easily customized using multiple layers of security, including security groups and network access control lists (ACLs). The security layers control access to Amazon EC2 instances in each subnet. Additionally, you can create a hardware virtual private network (VPN) connection between your corporate data center and your VPC, and leverage AWS as an extension of your corporate data center.

Amazon EC2

Amazon EC2 is a web service that provides secure, resizable compute capacity in the cloud. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

Amazon S3

Amazon S3 provides cost-effective object storage for a wide variety of use cases, including cloud applications, content distribution, backup and archiving, disaster recovery, and big data analytics. Customers can use Amazon S3 to store and protect objects in transit by using SSL or client-side encryption. Data at rest in Amazon S3 can be protected by using server-side encryption (you request Amazon S3 to encrypt your object before saving it on disks in its data centers, and decrypt it when you download the objects) and/or using client-side encryption (you encrypt data client-side and then upload the data to Amazon S3). Using client-side encryption, you manage the encryption process, the encryption keys, and related tools.

AWS Diode

AWS Diode is a cloud-based CDS service that provides scalable and reliable delivery of data from one cloud security domain to another. It provides you with complete control of your transfer options, including an API, and runs as a service within Amazon's proven infrastructure. The service runs completely within the AWS infrastructure but is accessible from on-premises services using Amazon S3 as the storage location for the data being transferred. The AWS Diode service workflows follow the ICD-503 Risk Management Framework (RMF). This results in an approved System Security Plan (SSP) and successful Joint Test Team (JTT) assessment using the NIST 800-53rev4 controls. This significantly eases the onboarding to AWS Diode service.

For more information on AWS Diode, reach out to your account Solutions Architect or Enterprise support member. You can also email the diode team at awsdiode@amazon.com.

> **Note**
>
> As of paper publication in December 2020, AWS Diode has the sole purpose of directly supporting the US Government, in that it controls data flowing to AWS classified regions. Commercial entities can use the service, to supply the US Government with their data or services. Commercial entities cannot use the service in any other way.

Connecting On-Premises Infrastructure

AWS provides service offerings to help you connect your existing on-premises infrastructures. As noted earlier, you can use many of the same services on premises. One service that is useful for on-premises is AWS Direct Connect.

AWS Direct Connect

Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment. AWS Direct Connect enables you to establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This enables you to use the same connection to access public resources, such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within Amazon VPC using private IP address space, while maintaining network separation between the public and private environments.

You can reconfigure virtual interfaces at any time to meet your changing needs.

AWS Advantages for Secure Workloads

The AWS Cloud provides several advantages if you want to deploy secure workloads using a CDS. The AWS Cloud has a cloud scale CDS service to support cloud-to-cloud communications. This service is accredited as part of the AWS infrastructure services, and allows for fast onboarding and familiar API that work with your existing cloud capabilities. The AWS Cloud also supports a myriad of secure interconnect options to allow your on-premise services and data to take advantage of cloud capabilities and scale.

Cost

Pay only for the storage and compute consumed for your workloads. Amazon S3 offers multiple storage classes you can use to control the cost of storage objects, based on the frequency and availability required at the object level. Eliminate the costs associated with data duplication, data fragmentation, system maintenance, and upgrades. Provision compute resources for specific jobs and stop paying for the compute resources when the jobs are complete.

Elasticity

Scale as workload volumes increase and decrease, paying only for what you use. Reduce large capital expenditures by no longer guessing what levels of storage and compute are required for your workloads. The ability to scale resources is not limited to just meeting demand. Workload owners can also use the scalability value of AWS by scaling up compute resources for time-sensitive jobs.

Purpose-Built Infrastructure

You tailor AWS purpose-built tools to your requirements and scaling and audit objectives, in addition to supporting real-time verification and reporting with internal tools such as AWS CloudTrail, AWS Config, and Amazon CloudWatch. These tools are built to help you maximize the protection of your services, data, and applications. This means as an AWS customer, you can spend less time on routine security and audit tasks, and focus on proactive measures that can continue to enhance security and audit capabilities of your AWS environment.

Auditability

AWS manages the underlying infrastructure, and you manage the security of anything you deploy in AWS. As a modern platform, AWS enables you to formalize the design of security, as well as audit controls, through reliable, automated, and verifiable technical and operational processes that are built into every AWS customer account. The increased automation & visibility capability available in the AWS Cloud can help you move to a continuous assurance model rather than relying on point-in-time assessments.

Security and Governance

The AWS Compliance Program helps you to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS Cloud infrastructure, compliance responsibilities are shared between AWS and the customer. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance Enablers build on traditional programs. This helps you establish and operate in an AWS security control environment. The IT infrastructure that AWS provides is designed and managed in alignment with security best practices and numerous security accreditations.

Sample Architectures

The following sections outline different architectures for transferring data across security domains. These samples focus on where the source security domain data resides and the desired destination security domain. Some of the samples show the use of customer-owned CDS equipment. But as data moves from on-premises to cloud-based models, the needs for these may disappear and allow different architectures to replace the legacy model. The models are organized as follows:

- Both of the security domains are in the cloud
- The source security domain is the cloud and the destination domain is on-premises
- Both the source and the destination domains are in the cloud, but the customer wants to manage and maintain the CDS component at its location

Both Security Domains are in the Cloud

AWS Diode provides a service to allow native cloud-friendly transfer of data from one cloud security domain to another. The advantage of this service is that you do not need to maintain or manage the cross-domain system (which is a costly endeavor both in manpower and time). The AWS Diode service supports moving multiple file types as well as the option to move compiled code in support of CI/CD pipelines. The following image depicts the service architecture:

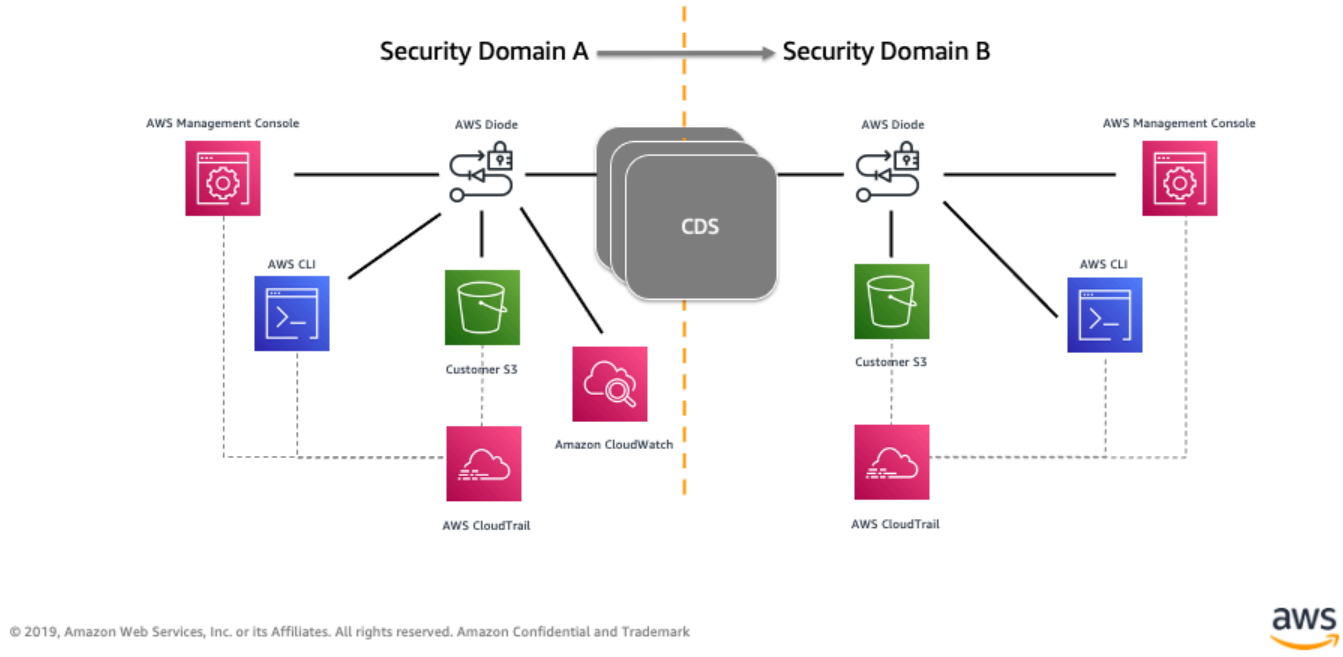

Figure 1 – Cloud Native CDS

This service works entirely within the cloud security domains and provides the added benefit of cloud APIs that move your data when you want it moved. Because it is a cloud-based service, you do not need to worry about scaling it to support your workload or managing all the complexities and auditing needs of CDS devices. The service is interfaced directly to all the standard auditing in the cloud and provides an ease of use like Amazon EC2 or Amazon S3. For customers who are more interested in getting their data moved versus running a CDS, this service provides the high-speed backbone to move your critical data.

Again, this option is most attractive when your data is in the cloud and needs to move to the cloud in another security domain.

You can set up your CDS in many ways. The following examples describe some of the more common architectures in use.

Deploying a CDS through the Internet or AWS Direct Connect

Figure 2 shows two on-premises customer networks that are connected by a CDS using the traditional deployment. In this configuration, Security Domain A is extended to provide

connectivity to an Amazon VPC in the AWS Cloud, while Security Domain B exists solely within the customer's data center. The connectivity between Security Domain A and an Amazon VPC can be done using a secure IPSec tunnel or using AWS Direct Connect as depicted.

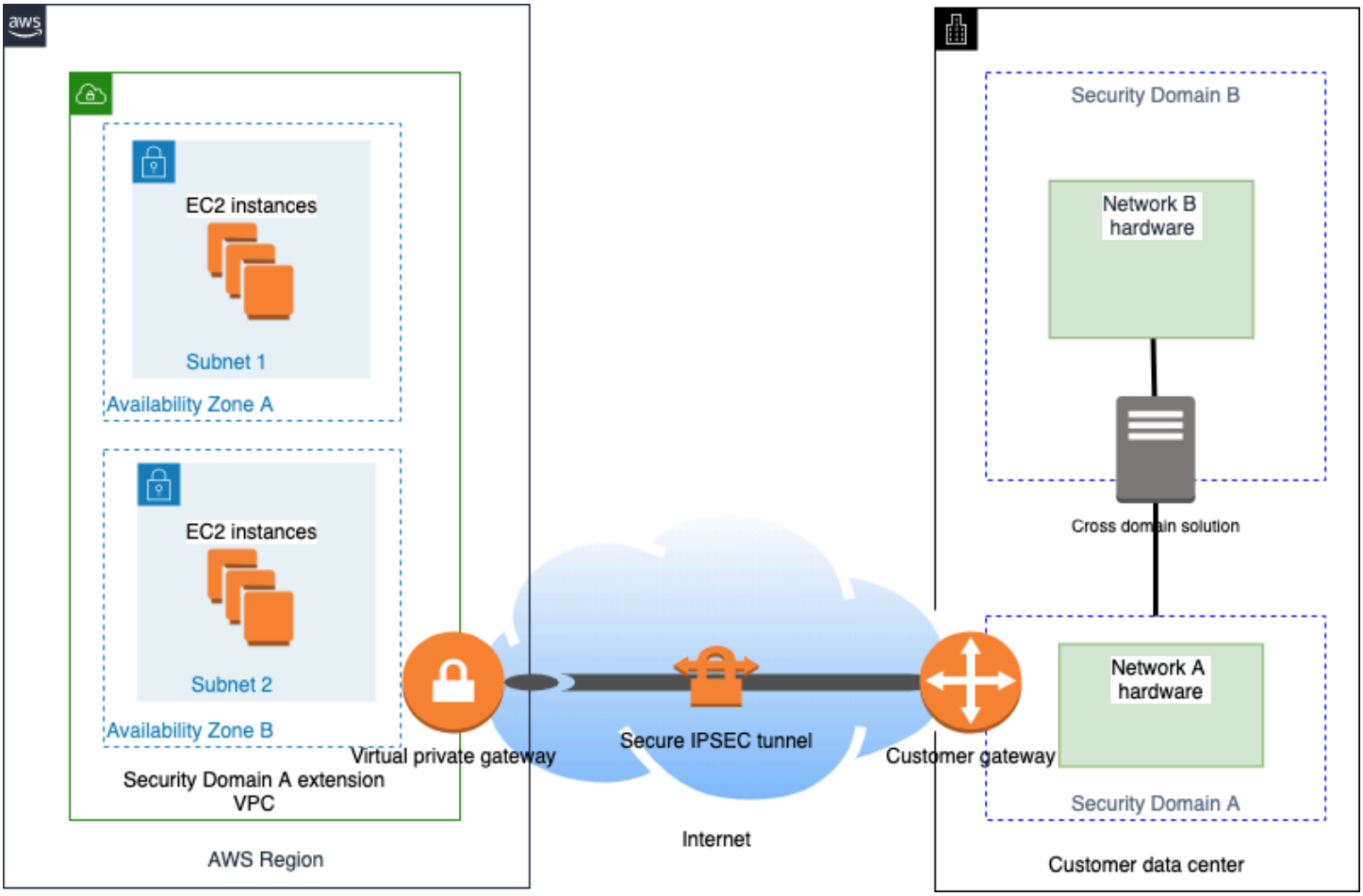

Figure 2 – Deploying a CDS through the internet

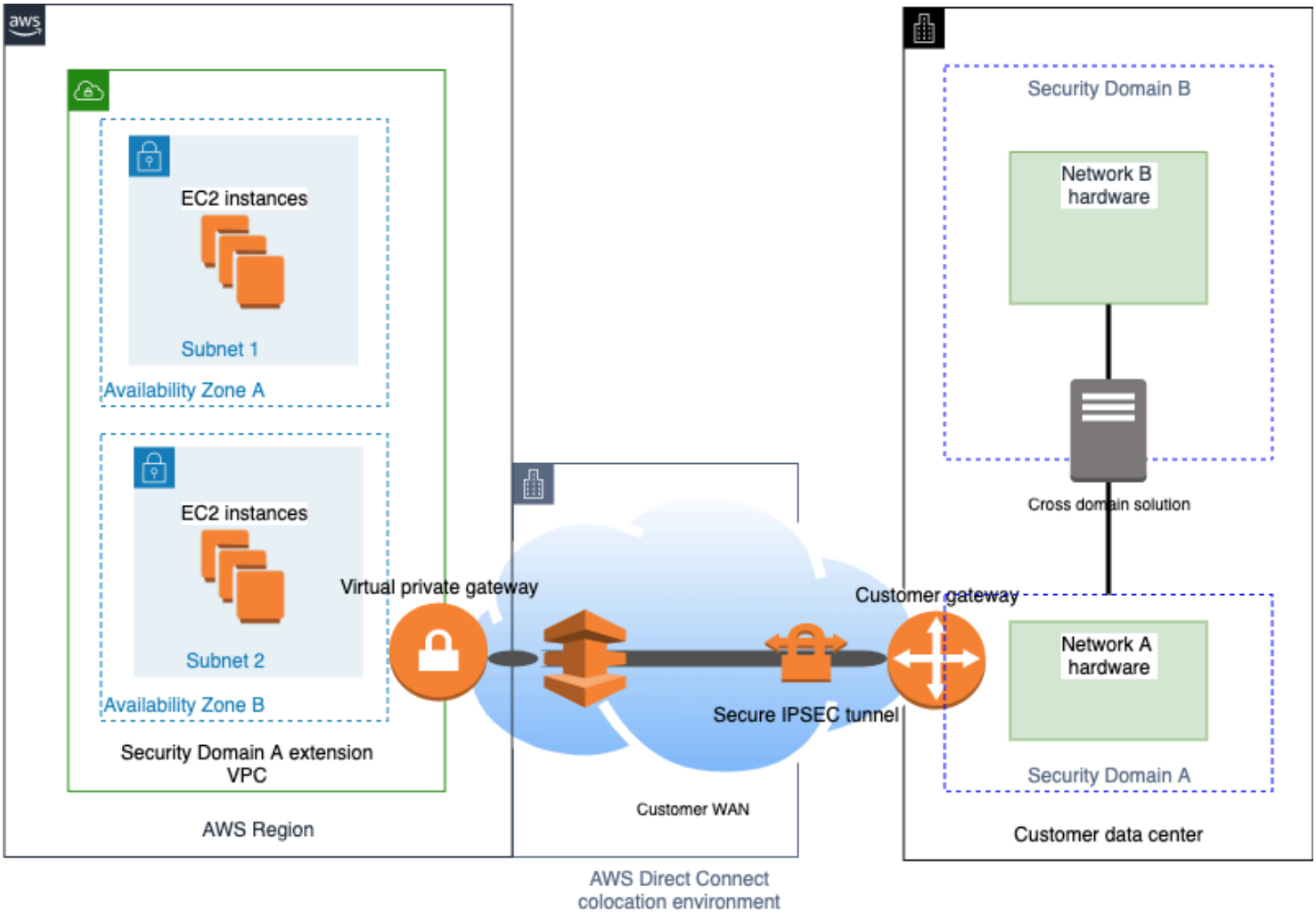

Figure 3: Deploying a CDS through IPSEC or Direct Connect

A secure IPSEC tunnel encapsulates data crossing the Internet between on-premises infrastructure and the customer's VPC. Additional security mechanisms, such as a WAF or an intrusion detection system (IDS), can be deployed within Security Domain A for added protection from Internet-facing systems. Because Amazon VPC is an extension of Security Domain A, Amazon EC2 instances launched within Amazon VPC can communicate with resources in Security Domain B through the CDS.

Deploying a CDS across Multiple Regions

Figure 4 shows two individual security domains connected to two separate AWS Regions. As shown earlier in Figure 2, the security domains are extended by using a combination of Direct Connect and a secure IPSEC VPN tunnel. All data flowing between the security domains flows from AWS to the customer's data center first, where it is inspected by the CDS before flowing back to AWS.

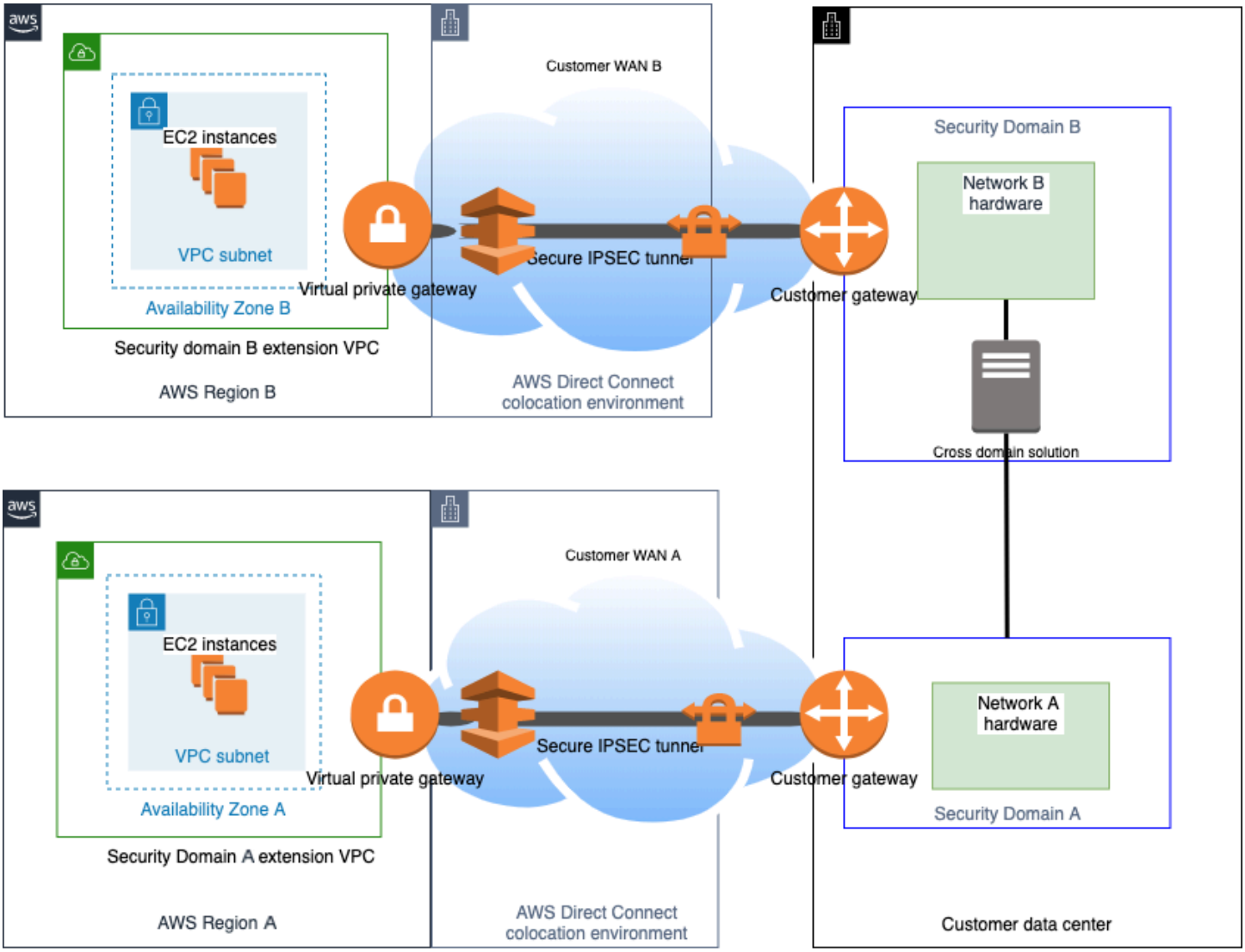

Figure 4: Deploying a CDS across multiple regions

Conclusion

Organizations with workloads across multiple security domains can leverage all the benefits that AWS services offer by using AWS Diode, AWS Direct Connect, VPN, cross-domain hardware, and a colocation approach. Organizations can select the hardware needed to meet their security domain transfer requirements, and extend resources that live in other AWS Regions or on-premises locations. In addition to the ability to connect resources across security domains, AWS offers a wide variety of tools that you and your organization can leverage to help meet security and compliance requirements of workloads hosted within AWS.

Contributors

The following individuals and organizations contributed to this document:

- Andrew Lieberthal, Solutions Architect, AWS Public Sector Sales-Var
- Tony Dahbura, Principal Technologist, AWS CDS Team

Further Reading

For additional help, please consult the following sources:

- Amazon VPC Network Connectivity Options
- AWS Architecture Center – Best Practices for Security, Identity & Compliance
- Intro to AWS Security

Document history

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

Change	Description	Date
Added information	This document now covers the AWS Diode service. This service provides a CDS service in the cloud.	February 2, 2021
Initial publication	Whitepaper first published	December 12, 2016

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.