Cross-Domain Solutions on AWS

December 2016

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. 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.

Contents

Introduction 1

What is a Cross-Domain Solution? 1

- One-Way Transfer Device 1
- Multidomain Data Guard 2
- Traditional Deployment 2

How Is a Cross-Domain Solution Different from Other Security Appliances? 3

When is a Cross-Domain Solution Required? 4

Connecting On-Premises Infrastructure 4

- Amazon VPC 4
- AWS Direct Connect 5
- Amazon EC2 5
- Amazon S3 5

AWS Advantages for Secure Workloads 6

- Cost 6
- Elasticity 6
- Purpose-Built Infrastructure 6
- Auditability 6
- Security and Governance 7

Sample Architectures 7

- Deploying a CDS via the Internet 7
- Deploying a CDS via AWS Direct Connect 8
- Deploying a CDS across Multiple Regions 9
- Deploying a CDS in a Colocation Environment 11

Conclusion 11

Contributors 12

Further Reading 12

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's network fabric, as defined by the security domain's policy.

Some organization's 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, a cross-domain solution (CDS) can be deployed to allow data transfer between security domains while ensuring 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 solution (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 particular 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.

This whitepaper provides best practices for designing hybrid architectures where AWS services are incorporated as one or more security domains within a multidomain environment.

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. Two types of CDS are discussed in this whitepaper, a one-way transfer (OWT) device and a multidomain 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 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 (e.g., data producer) and the optical receiver is placed on the opposite end (e.g., data consumer). OWT devices are often referred to as diodes due to their ability to transfer data only in one direction, similar to the semiconductor of the same name.

Multidomain Data Guard

A multidomain data guard enables bidirectional data flow between security domains. A common implementation of a multidomain data guard is a single server running a trusted, hardened 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 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 via 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 via the CDS. In the following example, the CDS is administrated and also physically located within the protections of Security Domain "B".

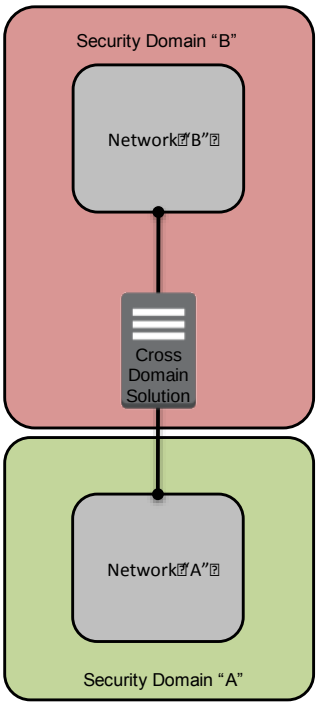

Figure 1: Traditional CDS deployment

How Is a Cross-Domain Solution 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, such as virus scanning, auditing and logging, and deep content inspection in a single solution. In

combination, when the CDS is included in a larger security program, these capabilities help prevent both exploitation and data leakage.

When is a Cross-Domain Solution 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 a data breach would be catastrophic 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 (e.g., alter the message rule set) without affecting the ATO's approval. If these drawbacks outweigh the additional security provided by a CDS, you should consider other options such as WAFs.

Connecting On-Premises Infrastructure

AWS provides service offerings to help you connect your existing on-premises infrastructures. The following sections describe some of the key services that AWS offers, including: Amazon Virtual Private Cloud (Amazon VPC), AWS Direct Connect, Amazon Elastic Compute Cloud (Amazon EC2), and Amazon Simple Storage Service (Amazon S3).

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. 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.

AWS Direct Connect

Using Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment. Direct Connect enables you to establish a dedicated network connection between your network and one of the 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.

Amazon EC2

Amazon EC2 is a web service that provides 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. Objects stored in Amazon S3 can be protected 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 Advantages for Secure Workloads

The AWS Cloud provides several advantages if you want to deploy secure workloads using a CDS.

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. Eliminate large capital expenditures by no longer guessing what levels of storage and compute are required for your workloads. Scaling resources is not limited to just meeting demand. Workload owners can also leverage 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 through the use of internal tools such as AWS CloudTrail,[1] AWS Config,[2] and Amazon CloudWatch[3]. 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 cloud simplifies system use for administrators and those running IT, and makes your AWS environment much simpler to audit sample testing, as AWS can shift audits toward a 100 percent verification versus traditional sample testing.

Security and Governance

AWS Compliance enables 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. 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

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

Deploying a CDS via the Internet

Figure 2 shows two on-premises customer networks that are connected by a CDS using the traditional deployment, as shown earlier in Figure 1. 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.

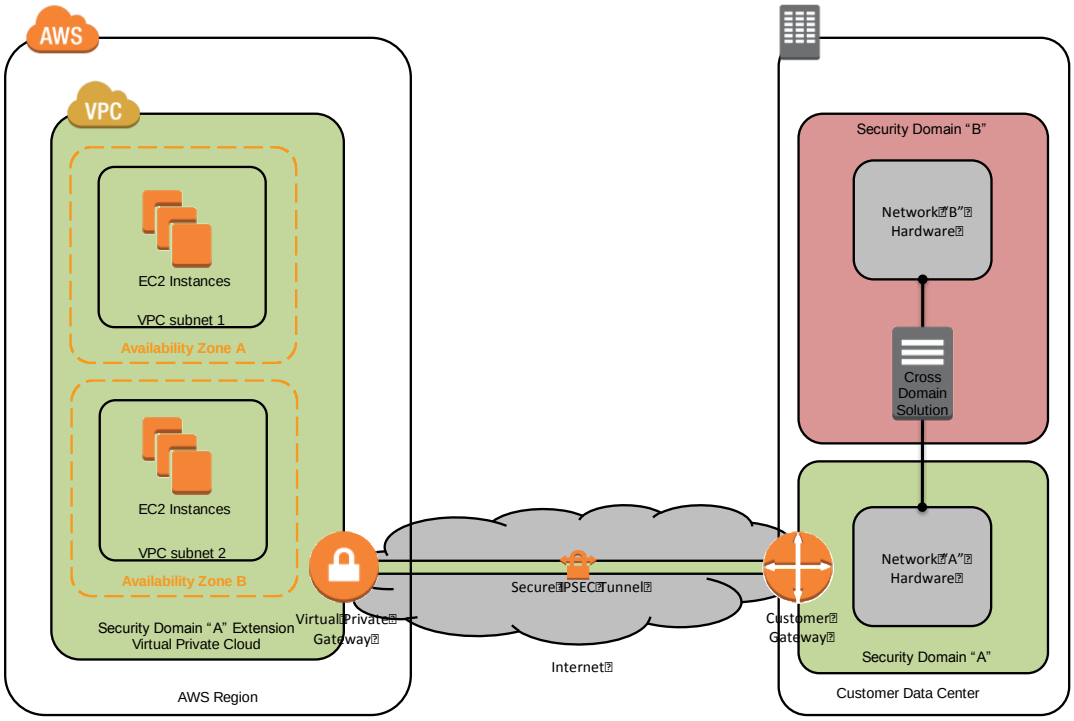

Figure 2: Deploying a CDS via the Internet

The customer is using the Internet as a WAN to connect to the Amazon VPC. 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" via the CDS.

Deploying a CDS via AWS Direct Connect

Figure 3 shows a similar deployment to Figure 2, but Direct Connect is used instead of the Internet to provide the WAN connectivity for extending Security Domain "A" to Amazon VPC.

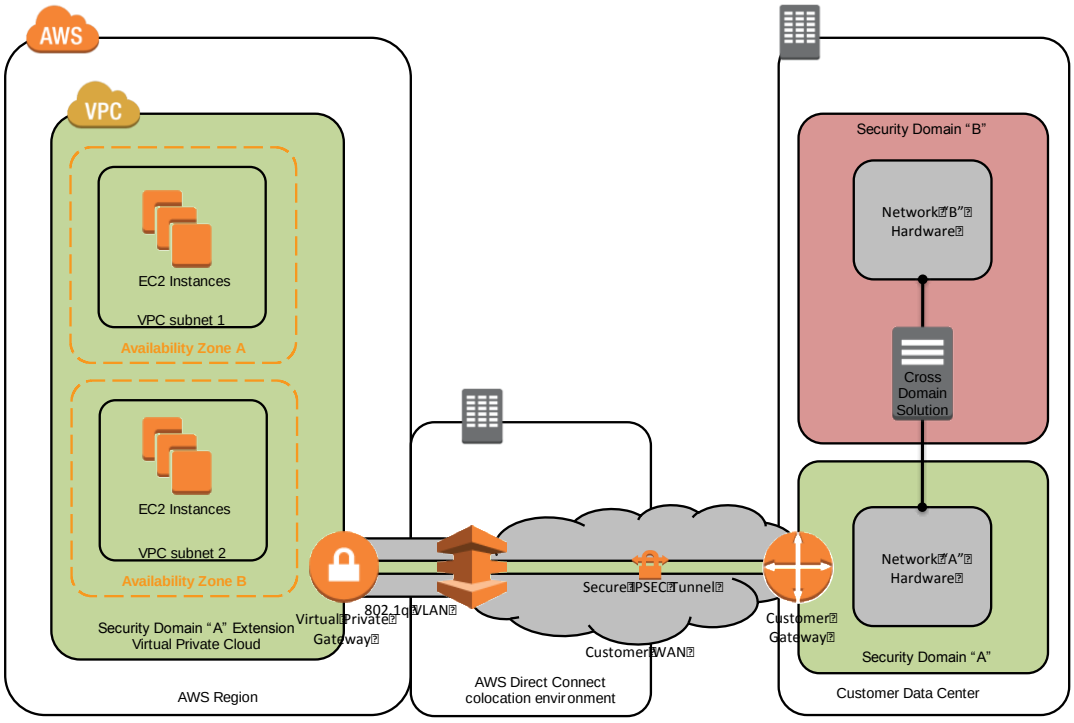

Figure 3: Deploying a CDS via Direct Connect

Direct Connect gives you greater control and visibility of the WAN network path required to connect to Amazon VPC. Using Direct Connect also reduces the threat vector posed by the Internet. All data flowing between your data center and AWS Regions is doing so across your procured communication links.

Deploying a CDS across Multiple Regions

Figure 4 shows two individual security domains connected to two separate AWS Regions. As shown earlier in Figure 3, 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.

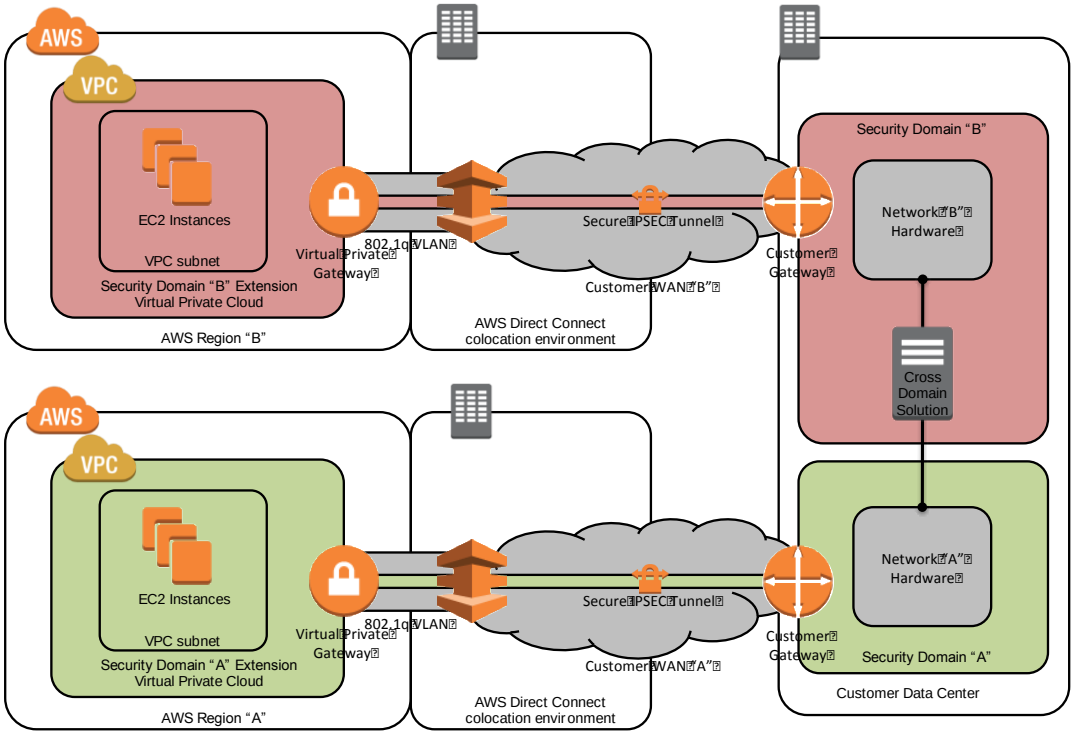

Figure 4: Deploying a CDS across multiple regions

You should implement a multiregion deployment when the unique capabilities of an individual AWS Region apply to only a single security domain. For example, an entity might choose to provision an Amazon Redshift data warehouse in one of the AWS Regions in the European Union (EU) to comply with data locality requirements, while also maintaining a production data processing cluster in a US-based region to comply with FedRamp requirements. Even though these two systems are deployed in separate geographic locations to comply with separate compliance programs and regulations, they still might have a requirement to communicate and share an approved subset of data. Deploying a CDS between these two security domains might be an acceptable way to share data while maintaining the integrity of the security domain's boundary.

Deploying a CDS in a Colocation Environment

Figure 5 depicts an additional potential configuration using space at colocation environments. In Figure 5 the CDS is still deployed in a customer-controlled area that is leased from the colocation facility provider. Figure 5 shows a fully off-premises implementation that includes a CDS.

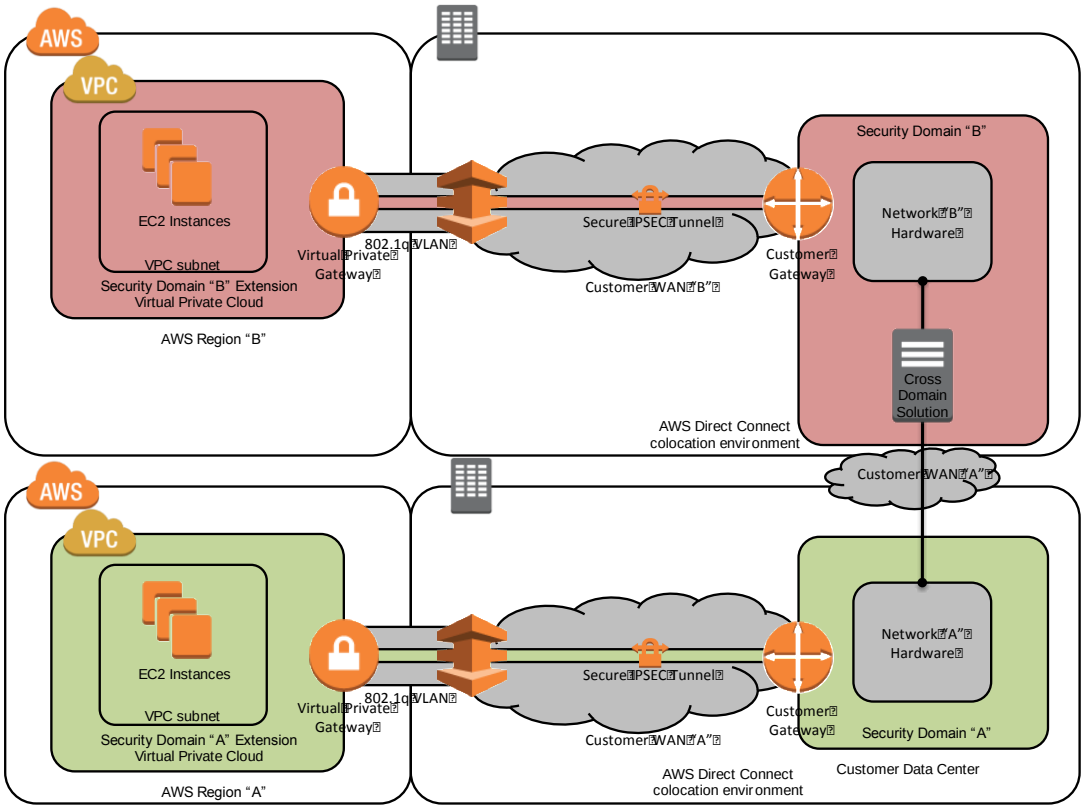

Figure 5: Deploying a CDS in a colocation environment

Conclusion

Organizations with workloads across multiple security domains can leverage all the benefits that AWS services offer by using Direct Connect, VPN, cross-domain hardware, and a colocation. 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 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

Further Reading

For additional help, please consult the following sources:

- Amazon VPC Network Connectivity Options[4]
- AWS Security Best Practices[5]
- Intro to AWS Security[6]
- Overview of AWS[7]

Notes

[1] https://aws.amazon.com/cloudtrail/

[2] http://aws.amazon.com/config

[3] http://aws.amazon.com/cloudwatch

[4] http://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf

[5] http://do.awsstatic.com/whitepapers/aws-security-best-practices.pdf

[6] https://do.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf

[7] http://do.awsstatic.com/whitepapers/aws-overview.pdf