Defining and Implementing Effective Cloud Security Architecture in Amazon Web Services

Published 27 September 2016 - ID G00308604 - 55 min read

ARCHIVED This research is provided for historical perspective; portions may not reflect current conditions.

By Analysts Mike Morrato

Supporting Key Initiative is Cloud Security

AWS has placed significant investment, effort and development into its security services within its cloud offering. This assessment examines the real-world applicability of AWS security offerings and explains how IT security architects can create a strong network security architecture within AWS.

More on This Topic
This is part of an in-depth collection of research. See the collection:

- Guide to Gartner's Research on IaaS Security

Overview

Key Findings

- AWS offers a strong and comprehensive set of features across multiple security domains to protect data, workloads and servers. Introduction or expansion of major security initiatives such as data protection, key management (especially bring your own key), identity and access management (IAM), and audit/logging functionality improves AWS's security ecosystem.

- In addition to the AWS-provided security features, the AWS Marketplace features a significant number of third-party security tools and platforms. These include security features such as network, data protection, key management, IAM and host/endpoint security.

- When designing a security infrastructure on AWS, critical differences must be taken into account. For example, "bump in the wire" security appliances, Switched Port Analyzer (SPAN) ports/virtual

LAN access control list (VACL) capture or Level 1/Level 2 networking elements are not available to deploy in AWS.

Recommendations

- When building a zoning and segmentation plan around security, use virtual private clouds (VPCs), security groups and network ACLs to create and define it.
- Combine the security features offered by VPCs with other elements such as network logging and analysis, distributed-denial-of-service prevention, host protection and third-party/OEM virtual security instances to create and continuously refine a robust security architecture program.
- Do not try to replicate an existing security architecture program at AWS on a 1:1 basis. There are opportunities to improve existing security architecture elements as well as flexibility to insert and utilize features that are specific to a cloud environment.
- Take advantage of the AWS-provided security tools, which will integrate with or extend the functionality of existing enterprise security architecture elements. AWS CloudTrail, Amazon CloudWatch, VPC Flow Logs, AWS Config and other tools add additional security functionality and should not be overlooked.

Analysis

Gartner clients frequently inquire not only about infrastructure as a service (IaaS)/cloud security in general, but also about specifics in how to secure aspects of their cloud deployments at AWS. Over the past 18 months, Gartner has fielded over 500 interactions with clients specific to security within AWS. While AWS advertises itself as a robust cloud provider, it frequently talks about its world-class security features. AWS even goes so far as to imply that enterprise data can be more secure within the AWS boundaries than within an enterprise's own data center. Clients frequently ask about the difference between marketing-driven announcements and real-world applicability of these security features. This assessment examines those claims while covering and focusing on creating a strong network security architecture within AWS. It also discusses key management and data protection, identity and access management, and logging/monitoring functionality.

Outside of the most stringent of security requirements, AWS customers can maintain a strong security posture within AWS that is equal to or better than what they have deployed in their own enterprise data centers. Use cases that align with this stance include stand-alone IaaS instances or extension of the enterprise data center in a hybrid fashion (aka hybrid IT). For enterprise customers considering AWS who are worried about traditional security functions, Amazon has put together a strong family of tools and features. For those features not offered directly by AWS, an ecosystem of technology partners exists to augment and enhance beyond what AWS offers. Enterprises taking advantage of these features, assuming proper implementation, will end up with a strong sense that their data and workloads are well-protected. There are exceptions to the rule. Technologies that traditionally work at Layers 1 or 2 currently do not work in AWS's environment. This includes packet capture/forensic network security appliances (such as packet sniffers, threat intelligence traffic analyzers, Layer 2 firewalls and stand-alone intrusion prevention systems [IPSs] in bridged mode).

To log and view network traffic and transactional data, AWS has provided alternative methods (such as AWS IAM, AWS CloudTrail, Amazon CloudWatch and VPC Flow Logs). However, many enterprises have forensic tools and security requirements that focus on network packets. They write policy around those packets and use forensic tools to capture and examine those packets. Because clouds do not work in a manner consistent with that way of thinking, customers have to evolve their thinking about how to secure data, how to gather that data and how to examine it. This will be an ongoing challenge for some enterprise customers of cloud services, but it is not a fault of the cloud itself.

According to Gartner's "In-Depth Assessment of Amazon Web Services," (https://www.gartner.com/document/code/301366?ref=grbody&refval=3454732) AWS provides solid security foundations, including:

- Documentation
- Customer-controlled firewalls/access control lists (network ACLs; security groups)
- Comprehensive compliance certifications and reports
- Encrypted data stores
- Encryption key management (AWS Key Management Service)
- Network traffic logging (VPC Flow Logs)
- Secure Sockets Layer (SSL)-secured endpoints
- Broad role-based authorization controls for all services (through AWS IAM)

Table 1 spells out what is included, and what is not included, in this assessment.

Table 1: Scope of Analysis and Coverage

Area of Coverage ↓	Out of Scope for This Analysis ↓
Network security architecture and design	Industry/regulatory security compliance
Other native security features in AWS	Available compliance features at AWS

Area of Coverage ↓	Out of Scope for This Analysis ↓
Key management and data protection	Options/methods to validate/audit Elastic Compute Cloud (EC2) configurations
Identity and access management	Expanded analysis of Amazon CloudWatch, AWS CloudTrail, and other logging and auditing functions
Logging and monitoring basics	Vendors offering complementary products in this space

Source: Gartner (September 2016)

Responsibility Model

Before an organization enrolls with AWS and begins any sort of deployment, it needs to understand how the roles and responsibilities work and who is responsible for what. For more information, see AWS's "Shared Responsibility Model." (https://aws.amazon.com/compliance/shared-responsibility-model/)

AWS customers are strongly encouraged to understand the concept of shared responsibility because it is frequently misunderstood. Failure to understand who is responsible for what could lead to a security incident for the customer. Using the IaaS model as an example, the customer is responsible for virtually all aspects of its environment outside of the physical equipment and the operating system. For example, AWS is in charge of the physical servers and their virtualization software within EC2. Customers are responsible for the instance image, the software on that instance, the configuration of the instance and so on. Likewise, AWS is in charge of the actual network infrastructure, but the customers are in charge of their own virtual cloud and the logical network definitions within it.

When looking at security, knowing what the customer is responsible for and what AWS manages is critical and must not be ignored. Figure 1 represents an example of security architecture domains. The "IaaS" column represents the provider. The "Customer" column represents the customer of the IaaS provider. A low responsibility means the party is responsible for the basic operation and availability. A high responsibility means the party is responsible for the configuration and management, as well any compliance or regulatory concerns. Joint means that there are shared responsibilities that fall on both parties. Some examples:

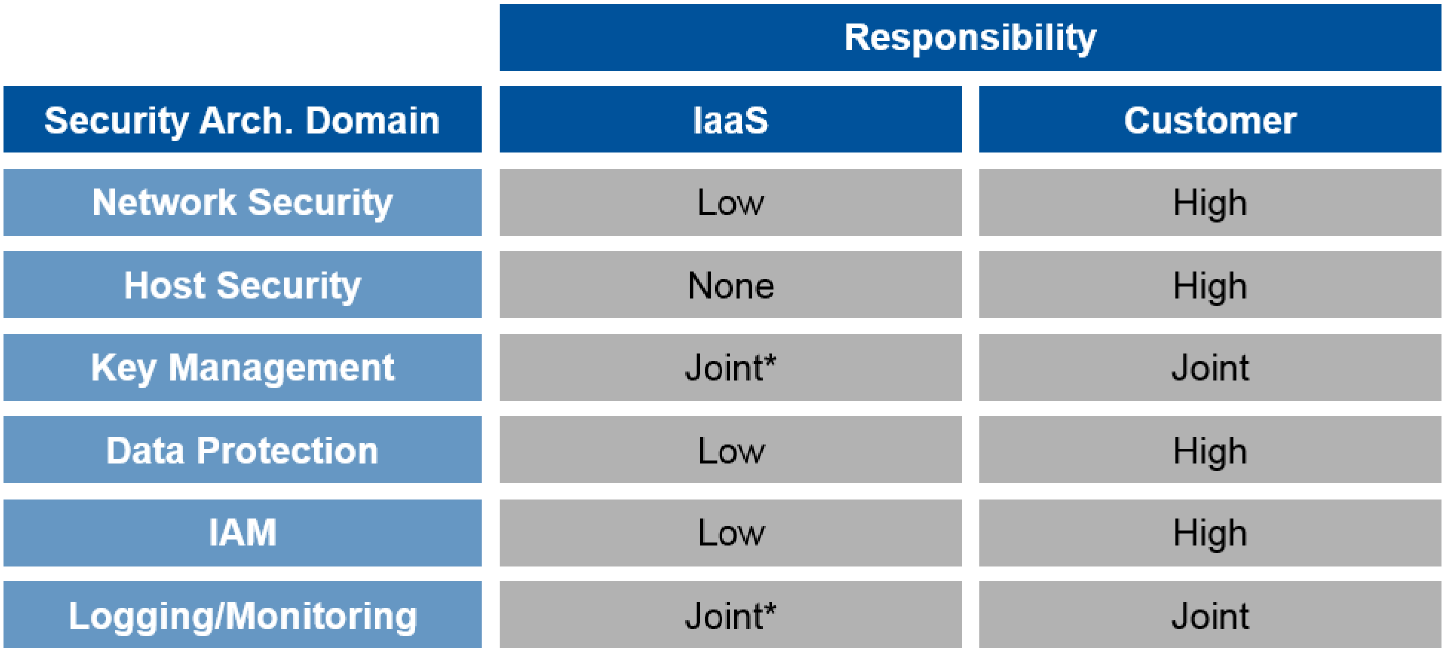
- **Example 1:** When looking at network security, AWS is responsible for the actual infrastructure that the customer's environment runs in. That includes:
  - Hypervisors
  - Physical network infrastructure

  - Features available for customers to use
  - Support for issues that arise outside of a customer's environment but are impacting that environment (such as outages or availability issues)

  The customer is responsible for their security policy, defining security boundaries, implementing their own required security features and products and so on.

- **Example 2:** In this scenario, a few services have joint responsibility, and AWS has to go beyond just providing an API or service. Take Amazon CloudWatch, AWS's monitoring service, as an example. AWS must develop and make the service available as well as provide the infrastructure to run it. However, AWS also has to integrate Amazon CloudWatch with its other offerings. Maintaining the availability of the service and protecting the integrity of the data produced is a critical responsibility. Customers are still responsible for enabling, configuring and managing Amazon CloudWatch, so ultimately, they still "own" a lot of the responsibility. However, in the case of logging and key management through AWS Key Management Service (KMS), responsibility and ownership exist on both sides.
- **Example 3:** With regard to AWS KMS, the customer is responsible for the actual keys and generation of them. The customer is also responsible for applications and/or users that make use of those keys. If a key is compromised or needs to be rotated, the customer is responsible. AWS, however, has a number of responsibilities regarding the AWS KMS service. This includes:
  - The securing of the keys between customers
  - Ensuring the integrity of the overall key solution
  - Ensuring secure replication of keys across global regions (as AWS KMS operates globally, not just within a region)

Figure 1. Responsibility Model Within AWS



	Responsibility	
Security Arch. Domain	IaaS	Customer
Network Security	Low	High
Host Security	None	High
Key Management	Joint*	Joint
Data Protection	Low	High
IAM	Low	High
Logging/Monitoring	Joint*	Joint

** Note: For key management and logging/monitoring, AWS actually manages the overall operation of AWS KMS and Amazon CloudWatch solutions. Customers manage their instances of each, but AWS has a degree of control over how these services work, what they integrate with and what data is available to each. Furthermore, certain features of both are region-specific and may not be globally available as of September 2016.*

Source: Gartner (September 2016)

Although assigning a joint value to key management and logging functions may come across as splitting hairs, the criticality of those services forces AWS to assume a degree of responsibility that differs from the network. In the event of a network failure, the network is resilient enough to get around that failure in most cases. A misconfigured Border Gateway Protocol (BGP) entry is unlikely to cause a security incident. Though there could be an outage, clouds are designed to allow for self-healing and, frequently, with alternative paths around that failure.

With logging, a missed event delivered to a customer's bucket could be the difference between identifying a security event and missing it altogether. The integrity of logging data is critical to any successful forensics or audit event. Likewise, storing and managing encryption keys is not a task for the lighthearted. These are essentially the "keys to the kingdom." Any security lapse of AWS KMS would have far-reaching implications.

Although AWS offers a service for customers to use, and although customers are 100% responsible for their own use of AWS KMS, AWS plays a major role in the overall security of the AWS KMS. AWS KMS operates globally as compared with regional solutions like AWS CloudHSM or customer-managed solutions from providers like Oracle, Okta and Ping. Maintaining synchronicity, along with security and availability, at a global level makes Amazon a partner, even if implicitly, in the AWS KMS space.

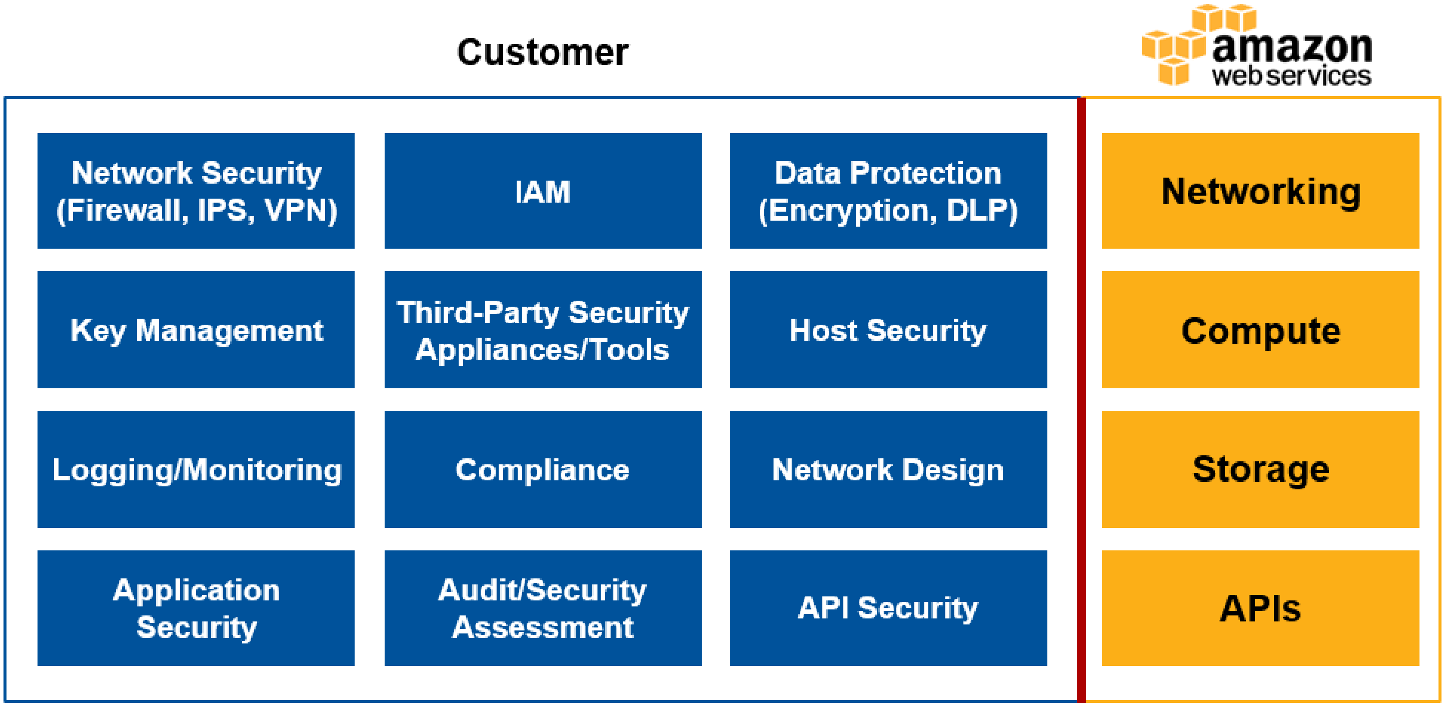
In an effort to give customers as much control as possible and autonomy of their instances, cloud providers manage the underlying systems that provide the networking, compute and storage functions. AWS is no different in that regard. What is currently different is the breadth of features and functions that are offered to customers. AWS does manage pieces and parts behind the scenes, but most of the configuration details are left to the customer. For example, although AWS provides the network and the protocols, customers define and configure how the network behaves and functions within their VPCs. AWS's responsibility is more about uptime, securing the underlying infrastructure and providing features that enable customers the ability to deliver their services through an IaaS infrastructure.

Customers have a significant number of tools and features at their disposal. Starting with the networking, they can define Layer 3 boundaries and design how their network looks as well as how instances can or cannot connect to each other. When it comes to security, customers can configure services across multiple security domains including:

- Network security
- Identity and access management
- Data protection
- Key management
- Host security
- Logging and monitoring

When examining the shared responsibility model and looking at it in terms of individual elements of a security program, customers can examine the shared responsibility model (see Figure 2) and know what to expect when it comes to ownership and what they are required to manage.

Figure 2. Shared Responsibility Model



Customer			amazon web services
Network Security (Firewall, IPS, VPN)	IAM	Data Protection (Encryption, DLP)	Networking
Key Management	Third-Party Security Appliances/Tools	Host Security	Compute
Logging/Monitoring	Compliance	Network Design	Storage
Application Security	Audit/Security Assessment	API Security	APIs

Source: Gartner (September 2016)

AWS ultimately becomes responsible for things like:

- The physical network
- Available CPU cycles
- Storage capacity and availability
- APIs to access functions or reporting telemetry

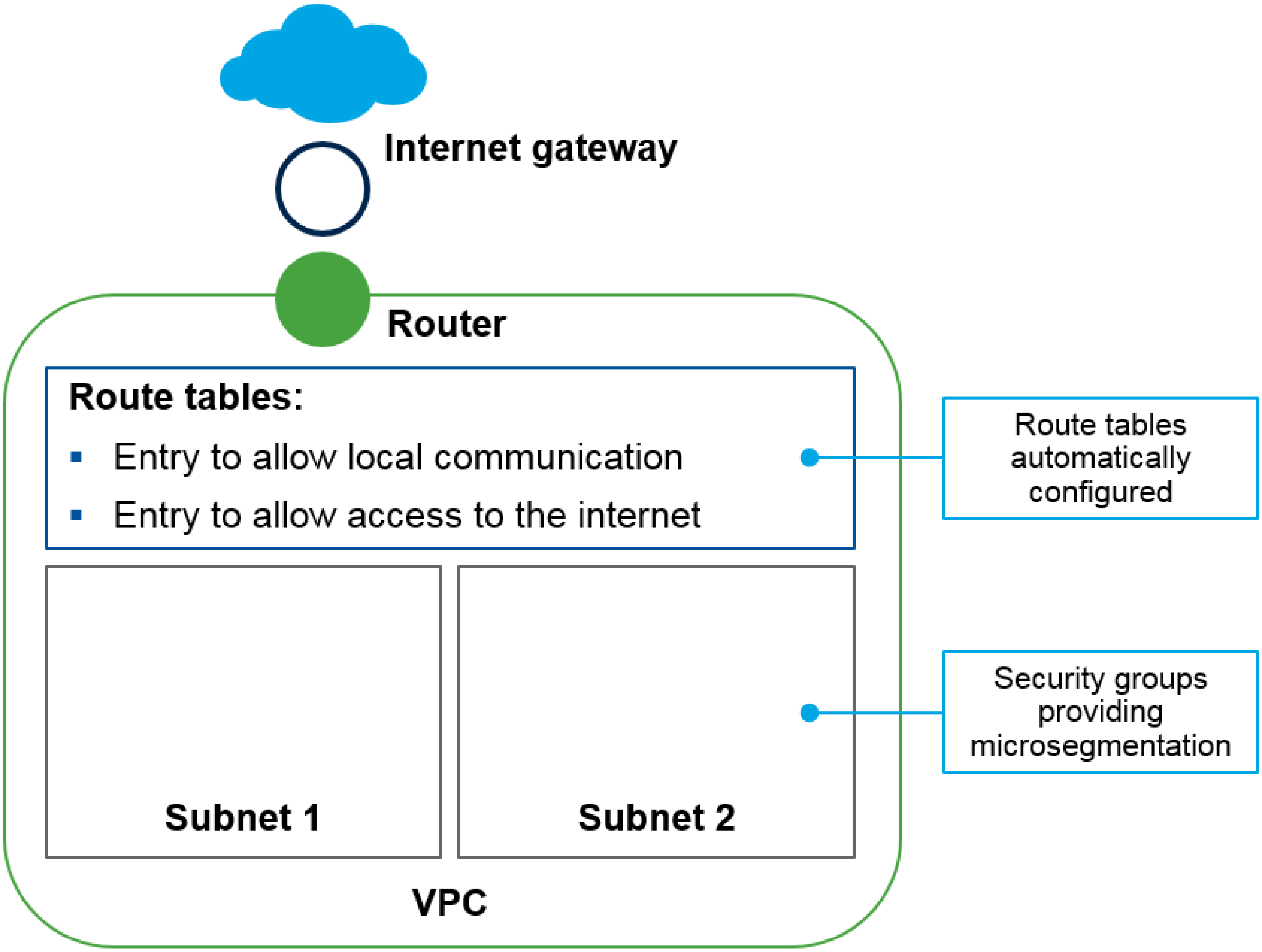
A majority of AWS's responsibility is around availability and accessibility. In the case of host instances, beyond providing a compatible image, AWS assumes no control, input or visibility as to how the instance is managed or run. Customers are responsible for either the logical configuration of those assets (such as with networking or instance specifics) or how those resources are manipulated and used to meet their own business needs.

Amazon VPCs, Security Groups and Network ACLs

Amazon virtual private clouds are the primary network construct at AWS. They are essentially a logical IaaS tenant dedicated to a customer. Amazon VPCs define the boundaries of a customer's environment. From a security concept, the Amazon VPC act as the most basic provider of network layer security. Amazon VPCs, however, are not analogous to anything in the traditional security space when it comes to network segmentation. Amazon VPCs themselves, while containing network elements, are more than just a network, so equating them to virtual routing and forwarding (VRF) or

VLANs would be inappropriate. Amazon VPCs commonly contain network and compute elements and can run third-party virtual images/appliances for those who procure and deploy them. The security practitioner needs to consider Amazon VPCs as the cloud tenant in which their environment runs Amazon VPCs can also be considered zones at the macro level. However, security groups and IP segmentation within the Amazon VPC work better at the micro level (see Figure 3).

Figure 3. A Generic Amazon VPC


Internet gateway
Router
Route tables:
▪ Entry to allow local communication
▪ Entry to allow access to the internet
Route tables automatically configured
Subnet 1
Subnet 2
Security groups providing microsegmentation
VPC

Source: Gartner (September 2016)

Customers can create up to five Amazon VPCs without any interaction between them and AWS. Amazon does allow customers to create more than five VPCs, but justification needs to be given via a web form. Customers may have a number of reasons to have more than one Amazon VPC. These include development versus production environments, separating lines of business/business units, or to "air gap" groups of workloads that are not related to one another and have no need to communicate with each other. By default, if a customer were to create more than one Amazon VPC, they could not talk to each other through AWS's infrastructure. Customers can create links between Amazon VPCs, but they must be done so manually and explicitly permit the traffic flow between Amazon VPCs.

Within an Amazon VPC, a customer uses security groups to define additional security boundaries within the Amazon VPC. Security practitioners should think of security groups as equivalent to security zones in a traditional data center. They are admittedly a bit more complex than that, but they serve the purpose of giving instances assigned to them a similar security profile as far as network connectivity goes. Security groups act as a sort of firewall for Amazon EC2 instances. They define what traffic is and is not allowed to and from an instance at the network layer. While security groups are most often associated with subnets, there is actually little relationship between the two, which is a major strength of security groups. Security groups are actually assigned to Amazon EC2 instances, and up to five different groups can be assigned to a single instance. Up to 500 security groups can be defined per VPC.

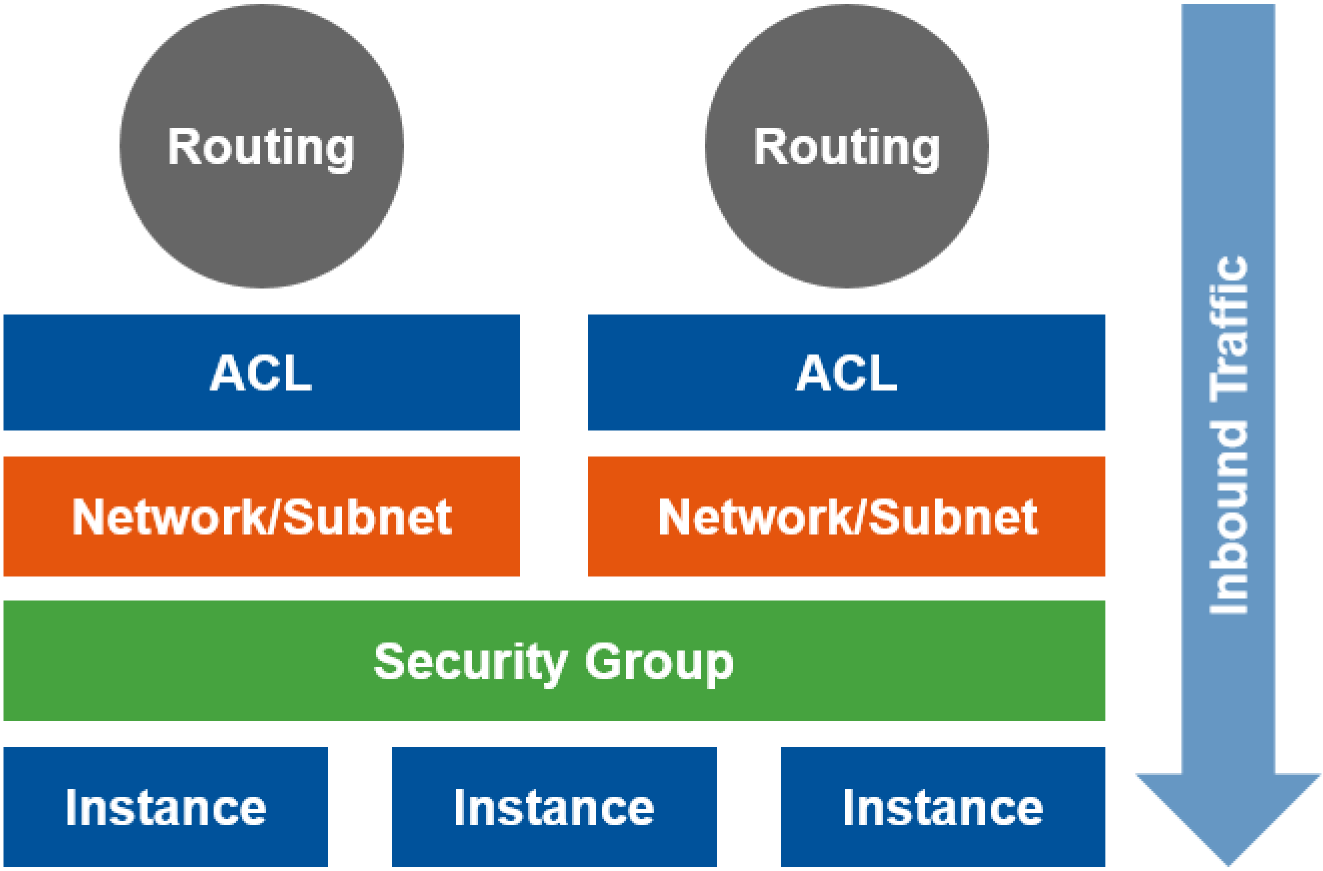
When comparing security groups with traditional firewalls, looking specifically at the L3/L4 rule sets that most security practitioners are familiar with, Gartner sees security groups as an equivalent control. In past discussions of cloud security, the focus was on having adequate controls. However, in the case of security groups — given their function and flexibility — they are equivalent in nature. Of course, next-generation firewall (NGFW) appliances offer added functionality, such as IPS, VPNs, URL filtering and malware prevention, among others, but other than IPS, they are typically end-user-facing enforcement tools that are not always required in a cloud environment, but can be deployed if necessary.

When working with security groups, customers need to keep the following in mind:

- No network traffic is allowed inbound to the instance, by default. All network traffic rules and policies must be explicitly defined.
- The default outbound rule allows all traffic to leave the instance. Customers are encouraged to configure the security group to limit outbound connectivity.
- Security groups are stateful in operation. Only the initiating side of the connection needs to be configured. Any backflow traffic is allowed once the session is established.
- Instances within the same security group cannot talk to each other, by default. In other words, just because two instances are in the same security group does not mean they can communicate with each other directly.

The other security controls within Amazon VPCs are network-based ACLs. These are stateless packet filters applied at Layer 3 hops within a customer's environment. The ACLs operate in a manner very similar to a traditional router or switch within an enterprise data center. Whereas the security groups dictate policy at the interface and instance level, ACLs operate at the network level. Customers should be aware that there is a default network ACL that permits all traffic (see Figure 4).

Figure 4. Security Flow Within an Amazon VPC



Source: Gartner (September 2016)

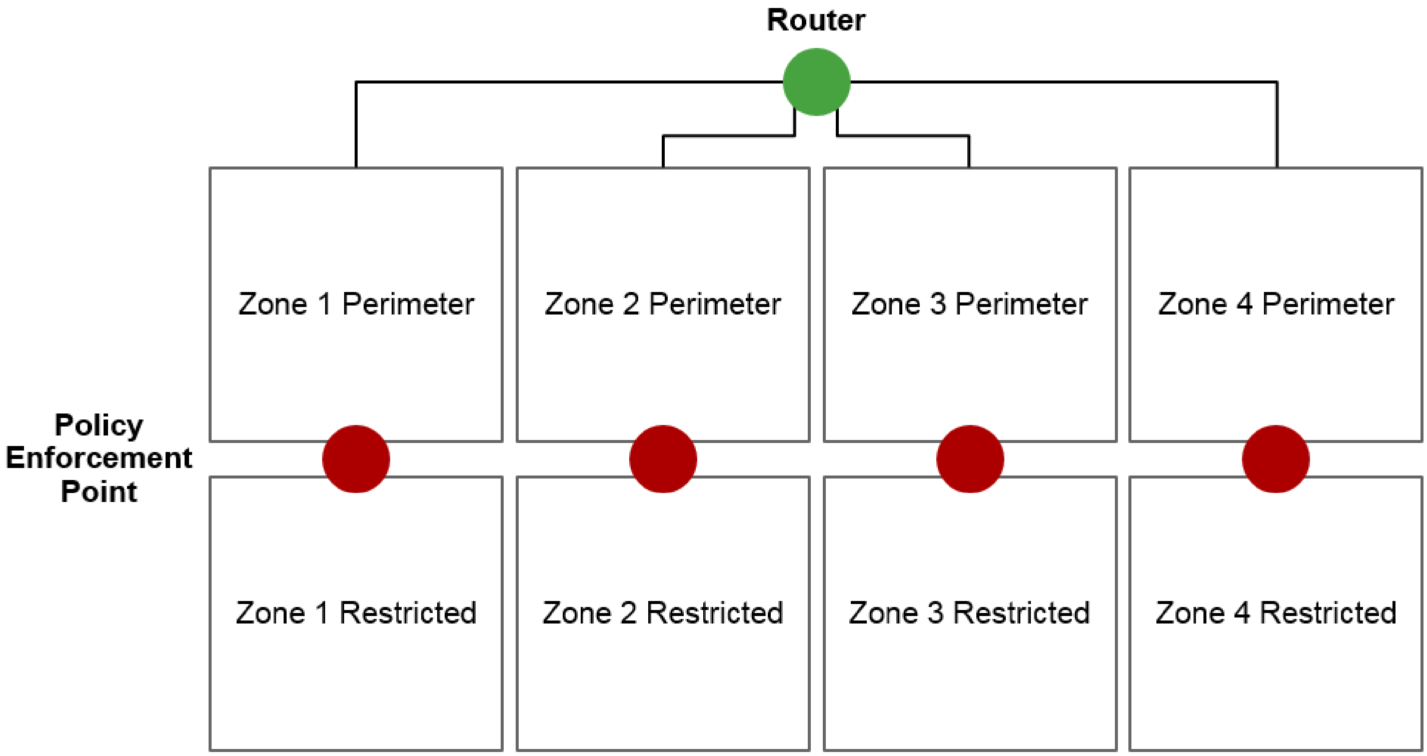
Amazon VPCs offer significant flexibility for environmental separation. Security groups provide internal segmentation and policy definition at the host level. Network ACLs control network traffic as it moves through the VPC. Combined, these features define and create a basic network security architecture that will be sufficient for a vast majority of enterprises when utilizing a cloud environment. Some customers may require the addition of IPS, DLP, antivirus or other network and host-based controls to accommodate their own security policy or regulatory burden, but those features are available from third parties. Traditional NGFW providers like Palo Alto Networks and Check Point also have offerings in this space, as do traditional software security vendors like Trend Micro and Sophos. Endpoint controls may also compensate for the lack of specific security features available from AWS, such as malware defense. If AWS-provided network security tools are insufficient for the organization deploying inside of AWS, NGFW platforms are available to deploy as a virtual appliance.

These components allow for very creative implementations of zoning architectures and manage access control at the network level in a manner similar to firewalls, routers and switches in the enterprise data center. Note that there is no Layer 2 switching, which would allow for features such as private VLANs and VLAN/port-based ACLs. However, few Gartner clients cite the lack of those feature abilities a reason not to adopt AWS or to worry about security. Furthermore, creative use of security groups can be used to limit host-to-host communication, providing an equivalent but obviously functionally different (L2 VLAN tags versus IP-based network rules) alternative to private VLANs. While there are differences between how these security elements are implemented and operate within Amazon EC2 infrastructure, security professionals should not have policy or design issues implementing a network security policy akin to what they currently do in on-premises environments.

Creating Multizoned Environments

As an example of a security zoning architecture, Figure 5 represents a multizone security architecture diagram that is possible in AWS. In this example, stateless network ACLs are deployed at the virtual router (green circle). Stateful rule sets are deployed at the policy enforcement points (PEPs) between the perimeter and restricted zones with security groups. The network ACL performs the initial filtering of traffic at the zone level using a macro level of enforcement. Within each zone, security groups should be used to apply specific access security controls at the micro level. Using a model similar to this allows AWS to have security policy flexibility without necessarily sacrificing security posture.

Figure 5. Amazon VPC Multizone Design Example



Source: Gartner (September 2016)

A question often asked by Gartner clients is, "How many zones/segments do I need?" Or, in the case of AWS, "Do I need multiple Amazon VPCs?" There is no generic answer to this question, and a few considerations — such as security requirements and how duties, workloads and functions are separated/managed — all come into play. Generically speaking, one strong recommendation is to zone instances into what is internet accessible (such as presentation/web servers) and what is not (such as database and middleware servers). This allows a more granular security policy to be applied at both zone egress points. It also reduces exposure for those services that are not internet accessible and would require, in most circumstances, the compromising of instances in the presentation layer in order to be attacked directly themselves.

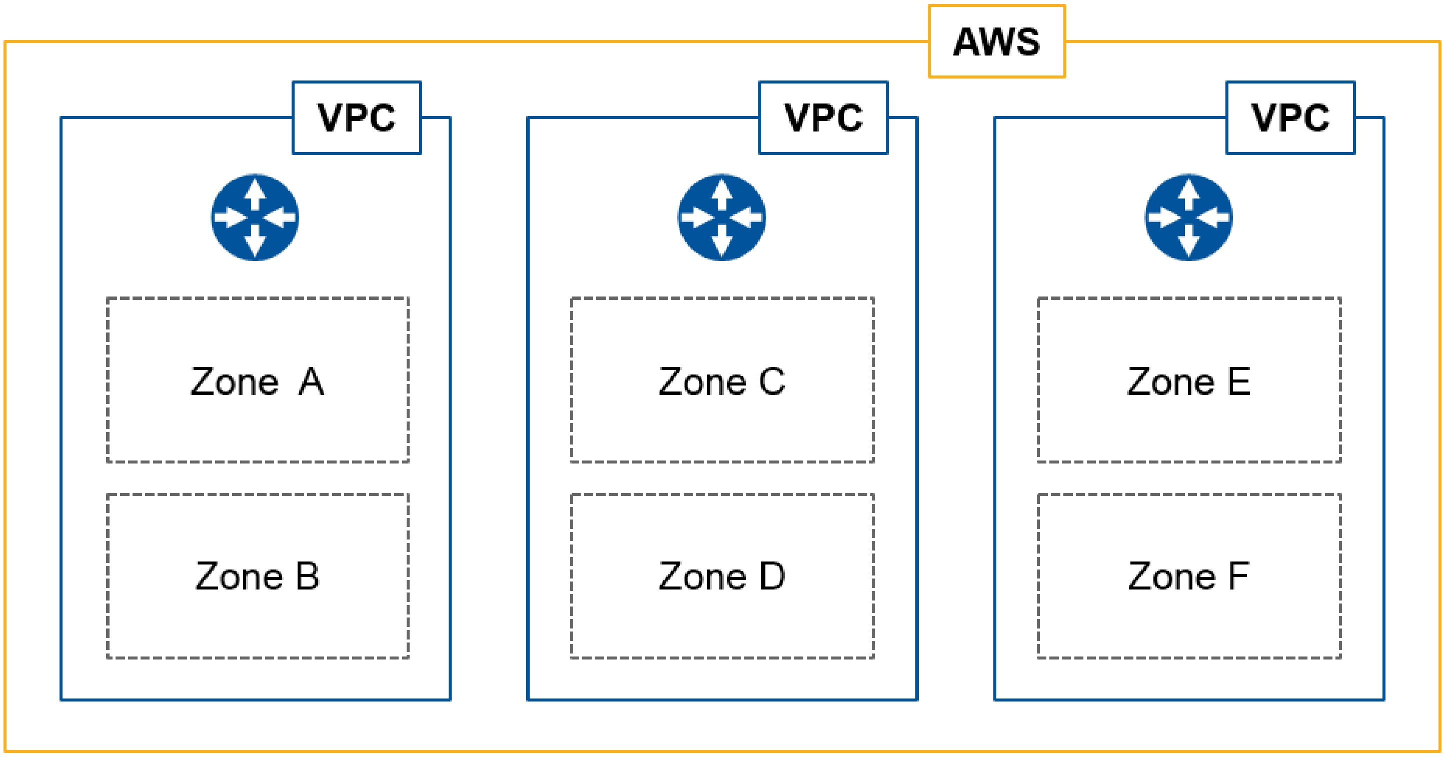
Using Multiple Amazon VPCs

Customers often have additional segmentation needs that go beyond just simple zoning within a tenant. In the case of development versus production, multiple VPCs should be used to completely isolate both environments. This same logic can be applied to segmenting lines of business or completely separate operating environments. Additionally, each VPC is capable of having different administrative privileges to separate ownership and responsibility duties. At the individual VPC level, specific security architectures are deployed to further define and refine the policies.

Another consideration with multiple VPCs is the concept of a single administrative domain versus multiple administrative domains. Using production versus test as an example, VPCs are managed flexibly. There can be different user administrators for each VPC, even allowing for different users for elements within VPCs. Adopting a model like this, if it fits within one's AWS IAM design and policy to permit it, allows customers to limit the fallout from account abuse. It also puts walled gardens (from an IAM standpoint) around what user accounts can and cannot affect between VPCs or elements between VPCs. This could just as easily apply to the concept of using VPCs to differentiate between lines of business or business units and having different users manage their respective environments.

One other consideration for a multi-VPC design is making use of a "utility" or "services" VPC. Most networks need common features such as DNS, Network Time Protocol (NTP), Trivial File Transfer Protocol (TFTP; although not likely needed in cloud deployments) and so on. These are the type of services that enable applications and users to perform their required functions, but they are not accessible by third parties/external users. Instead of deploying these in each VPC, they could be colocated in a services tier, and each VPC can then leverage those services centrally. The alternative would be to deploy those services in each VPC, which in turn could increase complexity as well as the number of instances/services inside of each VPC. Using a services tier in this manner, with a dedicated VPC, could have the added benefit of minimizing the attack surface by making these critical services inaccessible to outside users and only accessible from the other VPCs directly (see Figure 6).

Figure 6. Multi-VPC Architecture



Source: Gartner (September 2016)

Extending the Data Center With Amazon VPCs

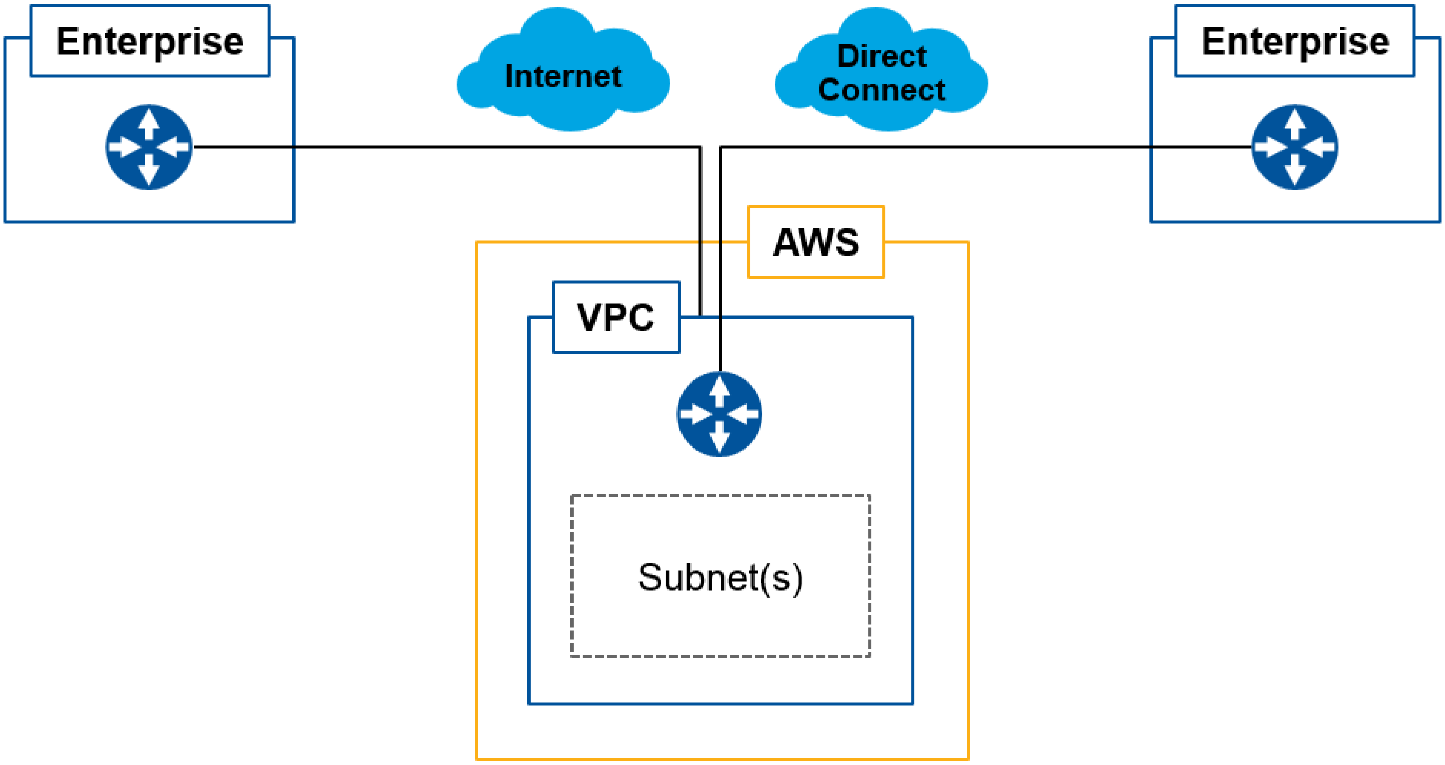
Reviews of customer interactions at Gartner, as well as case studies publicly supplied by AWS, show that an increasing number of enterprises are using Amazon EC2 for data center extension, also known as hybrid IT. The two reoccurring themes that show up when analyzing the data are:

- The need to rapidly deploy new solutions
- Lack of space or function in the existing data center

With these and other use cases, concern about security between the enterprise data center and the VPC are common. Most of the security fears around data protection or a threat actor using the VPC as a "back door" into the enterprise data center do not have the evidence to back them up, at least not from the cloud provider side. User configuration errors that lead to exposing data or assets will continue to be a problem moving forward. Cloud versus traditional data center does not immediately change the exposure if the security policy is designed properly. Simple tasks such as preventing internet-sourced IP addresses from traversing the VPN or WAN link back to the enterprise minimize one aspect of the risk involved with using a cloud provider like AWS to infiltrate the enterprise. Customers should design their cloud operations around secure instances and not necessarily around a secure network. This concept is different from the security policy applied to the ingress point for an enterprise data center, but the result should be very similar in application.

AWS allows two ways to connect between a customer's VPC and its enterprise data center. The first and most common method is via an internet-based VPN. Customers would create an IPsec tunnel between an endpoint in their data center and the virtual router at AWS. The other option is to utilize a direct/private WAN connection. Both options provide a mechanism for secure connectivity as well as preserving the integrity and confidentiality of data that is moving between the customers VPC and their enterprise data center. AWS Direct Connect's primary value is around availability and predictability, but some Gartner clients use it as an additional layer of confidentiality versus a VPN over the public internet (see Figure 7).

Figure 7. VPC Connectivity Options



Source: Gartner (September 2016)

Whether it is VPN or AWS Direct Connect over a private WAN, extending the data center to a cloud provider like AWS is a proven method over trying to package an application and/or its data and then redeploying in a "greenfield" manner within AWS (although there may be conditions that require that type of migration). This facilitates activities like migrating apps to the cloud in a secure and controlled fashion. It also allows for time-sensitive expansion of critical functions or helps alleviate space/power/cooling constraints that would otherwise delay new projects.

AWS Identity and Access Management

In-depth discussion of general IAM concepts are out-of-scope for this document. Because there is other research specific to IAM through Gartner, you are encouraged to reference that material for leading practices in that space. The focus here is on IAM capabilities at AWS and their place in a security architecture program.

Some existing Gartner research on this includes (may not be available based on subscription level):

- *"How to Choose Between On-Premises and IDaaS Delivery Models for Identity and Access Management" (https://www.gartner.com/document/code/296572?ref=grbody&refval=3454732)*
- *"Building a Risk-Aware IAM Environment With Identity Analytics" (https://www.gartner.com/document/code/273300?ref=grbody&refval=3454732)*
- *"The Emerging Architecture of Modern Identity" (https://www.gartner.com/document/code/272486?ref=grbody&refval=3454732)*

Identity and access management is another area where AWS shows strength and provides value to the customer. For most enterprises, Amazon has the IAM tools that are generally sufficient for most enterprises. For those use cases where the customer doesn't feel comfortable with AWS's integrated IAM tools, there are a number of third-party IAM providers available in the marketplace that they may be more familiar or comfortable with. AWS does offer a federated model that can integrate with most IAM toolkits including Active Directory. AWS also offers its own directory service, a connector for Active Directory, and an identity broker (AWS Directory Service).

The decision as to what to use, if at all, comes down to an enterprise's IAM architecture and policy. Active Directory integration will make a lot of sense and likely be the easiest mechanism for integration. Unfortunately, AD also carries a lot of concern for customers. AWS customers are encouraged to evaluate their IAM policies and choose the AWS solution that best aligns with those policies. If AWS offerings are not sufficient or lack the requirements of the IAM programs at the enterprise, Gartner encourages AWS customers to look into the marketplace for other IAM providers or to work with their existing IAM provider for solutions tailored toward AWS operations.

AWS Directory Service supports many of the key features demanded by security architects, including multifactor authentication, audit trails for actions performed by individual logins, and specific roles and permissions per ID. User accounts within AWS Directory Service have a great depth of customization available to them such as:

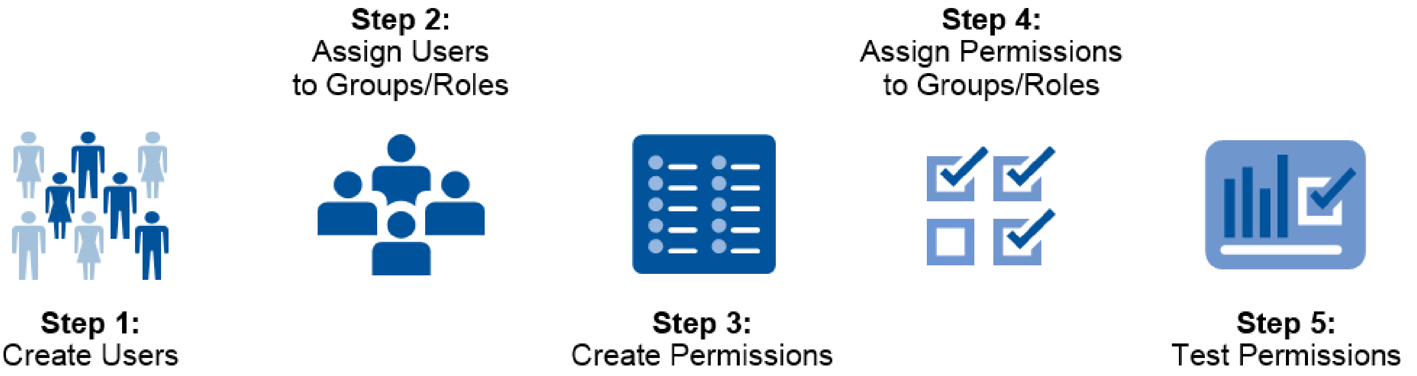
- API access
- Management of individual networks, instances or platforms
- Service roles for add-on products that the customer deploys within EC2

The Active Directory Connector and identity broker are best used by enterprises that want to leverage their existing IAM platforms and to either directly connect to Active Directory or use a token service to translate between enterprise roles and AWS roles.

Within AWS IAM, AWS offers managed policies and in-line policies. On top of that, there are also AWS-defined managed policies and customer-defined managed policies. A managed policy is applied to multiple users, group and/or roles. Much like Active Directory groups, this is a group policy that a user is assigned to that has specific groupwide permissions. The account just inherits those permissions. In-line policies are applied directly to the user account and are specific to just that user. The rules defined in an in-line policy are incapable of being shared or used with other users. Instead, a duplicate policy would need to be created and customized for additional users.

Although there is no immediate constraint on the number of elements in a policy, there is a limit on the overall size in order to maintain and protect the service. A powerful feature, managed policies can support multiple iterations to facilitate both rollback in the event of a permissions problem or testing to ensure the new rules work as expected. With managed policies, IAM administrators apply up to 10 different policies to users, groups and/or roles. To really make the math interesting, while a user can have 10 policies attached to them, a user can also be a member of up to 10 groups, and each group can have an additional 10 policies attached. The point is that AWS has made this feature flexible enough that it will meet IAM policy needs in most cases (see Figure 8).

Figure 8. IAM Process Flow



Source: Gartner (September 2016)

The flexibility of AWS IAM allows customers to create very specific and exact rules and roles that satisfy most enterprise needs and concerns. An example where it may not work is when a federated model is used between the enterprise and AWS, but the enterprise side lacks definition of user roles or is an otherwise flat structure. Another example where this may not work is where the enterprise both refuses to expose their AD environment to external parties and cannot map internal users into AWS IAM roles, or they are using an IAM provider that does integrate with AWS's native offerings.

Users can be limited to individual elements or services within the environment. Users can be granted power over large swaths of the infrastructure as well. These IAM policies apply to instances, networks, security tools and value-added services provided by Amazon. AWS does allow for multifactor authentication using OTPs/tokens.

In addition to the flexibility that roles, groups and permissions have with regard to granting or denying access to resources at AWS, additional features enhance the offering to meet specific needs of the enterprise (see Table 2).

Table 2: Selected AWS IAM Features Available to AWS Customers

Features ↓
Access advisor — used to help define least privilege needed for accounts
Service last accessed — lists the last use of the account; good for removing stale accounts
Strong/minimum password policy
Multifactor authentication
Credential rotation
Policy conditions — limit requests by IP as well as unique identifier (user ID)/password; require MFA for select services
Monitoring — lists who, what and when for the purpose of monitoring and auditing
Policy generator — wizard for creating unique or specific permissions from lists

Source: Gartner (September 2016)

There is a default "root" account when a customer enrolls with AWS. This root account has full permissions over most aspects of the environment and can be secured before instances are created and the network is configured. Use role-specific accounts that facilitate separation of duties instead because this helps limit access to those services an administrator needs to do their job.

Gartner strongly encourages AWS customers to lock down their root account immediately. This includes using multifactor authentication, enrollment in privileged access management tools and logging of all actions taken by the root account. This account has the ability to create, delete or modify any aspect of the customer's account. Abuse of this account could lead to service disruption, potential billing surprises or manipulation of assets within AWS, including data exfiltration, deletion, modification and so on.

AWS Key Management Service and AWS CloudHSM

Another area of security concern for many enterprises is around encryption and key management. Amazon offers two services to address the needs of those customers in the form of AWS Key Management System and AWS CloudHSM. These are different services, and although they overlap in certain areas, one is global in nature and the other is tied to an Amazon EC2 instance or series of instances within a region (see Table 3). AWS provides AWS KMS as a base function of a customer's service. The AWS CloudHSM service is a for-fee service.

Table 3: AWS CloudHSM and AWS KMS Comparison

↓	AWS CloudHSM ↓	AWS KMS ↓
Key Generation	AWS	AWS
Where Keys Are Used	AWS + enterprise DC (if necessary)	Only AWS
How Keys Are Used	Customer apps, APIs	Management, apps, APIs, signatures, SDKs, customer apps
Operational Responsibility	Customer	AWS
Integration With AWS Services	Limited	Yes
End-User Costs	Per HSM	Base + add-ons available
Control	Customer	Customer + AWS

Source: Gartner (September 2016)

The primary goal of the AWS KMS and AWS CloudHSM revolves around encryption. The AWS CloudHSM is a managed hardware solution (the customer is directly responsible for managing the keys however) whereas the AWS KMS is a managed encryption service. Both services support customers who provide their own keys. They also allow customers to generate new keys. Keys can be disabled in both services should a key become compromised or no longer needed. Both also have audit trails associated with them and report into AWS CloudTrail upon usage. Customers should be aware that there are costs associated for usage of either system, as well as at certain transaction levels.

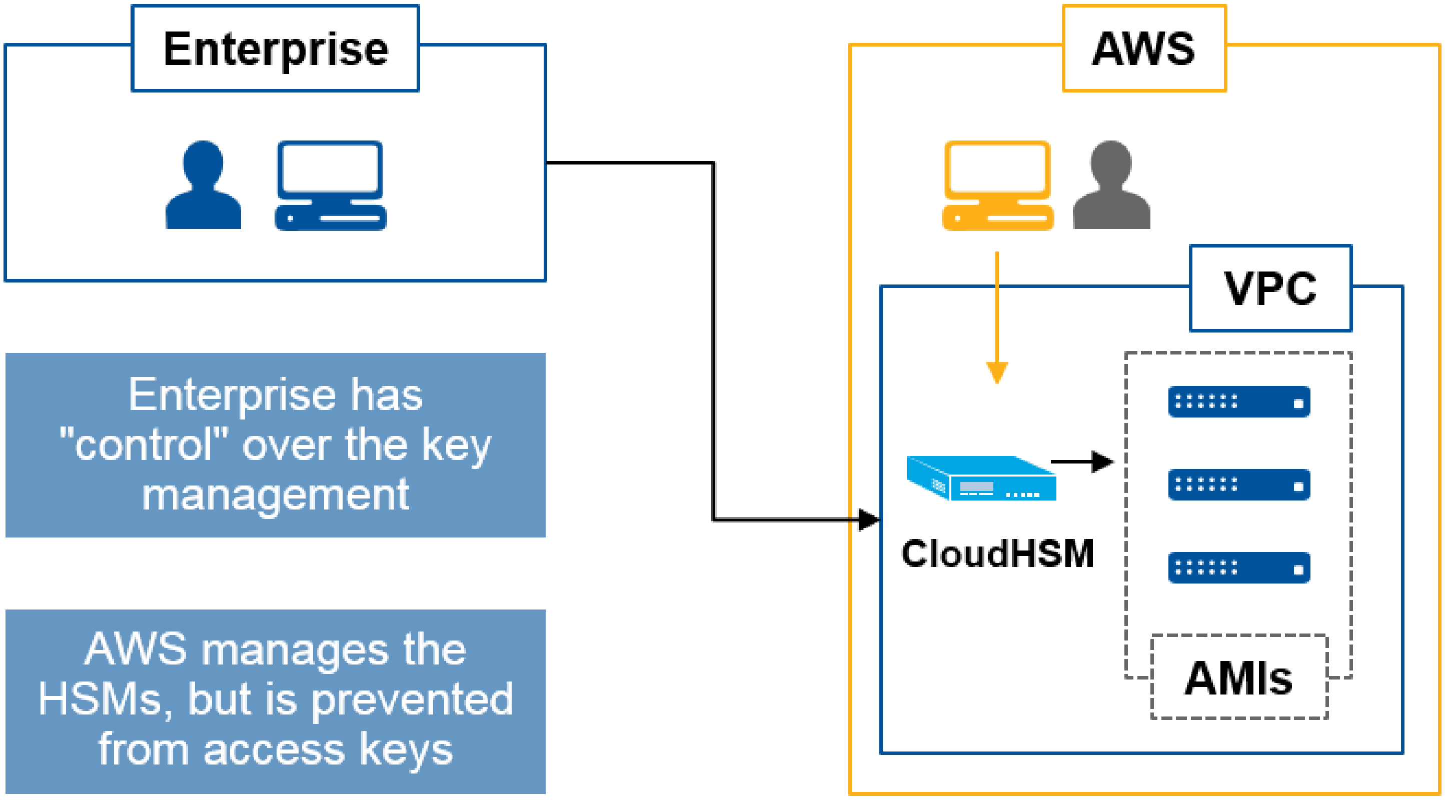
One of the bigger concerns articulated by enterprises has been around ownership and access to the keys. With the AWS CloudHSM, only customers have access to their keys while they are at rest. When in use, they might be exposed to the cloud provider. Depending on the mode in which AWS CloudHSM is deployed, Amazon does not have access to customer keys when used (this applies to certified third parties as well). AWS does not have access to Customer Master Keys in the case of AWS KMS.

Gartner's "Enabling High-Risk Services in the Public Cloud With IaaS Encryption" (https://www.gartner.com/document/code/259591?ref=grbody&refval=3454732) noted:

> **Properly implemented infrastructure as a service (IaaS) encryption solutions do not provide 100% confidentiality for your data, and even encryption keys are exposed in cleartext in cloud-based server memory. Therefore, organizations must be aware of potential attack scenarios and the residual risks.**

AWS CloudHSM is most often used with regulatory requirements such as PCI, but there are other regulatory bodies that may also require it. There may be other contractual requirements that make AWS CloudHSM an attractive offering, but the AWS CloudHSM is best used when the customer wants to have 100% control over the keys and how they are used. Because the CloudHSMs are the responsibility of the customer after they are provisioned, it is advisable that customers set them up in a redundant fashion. Unlike AWS KMS, the AWS CloudHSMs are not redundant by default, and during an outage, this could affect operations and uptime. AWS manages the physical hardware, but the customer is responsible for making sure the platform is not oversubscribed or burdened. Customers also need to keep in mind that, because the AWS CloudHSMs are specific to a region, there could be latency involved for those who utilize multiple regions, which also requires the security policy to reflect key operations between regions (see Figure 9).

Figure 9. AWS CloudHSM Design


Enterprise
AWS
VPC
CloudHSM
AMIs
Enterprise has "control" over the key management
AWS manages the HSMs, but is prevented from access keys

Source: Gartner (September 2016)

AWS KMS is a more robust platform and has a larger potential impact for customers, but it may not meet regulatory or contractual requirements due to its shared nature. While individual customer keys cannot be accessed directly by AWS or by other customers, the shared nature of AWS KMS platform may be an impediment to adoption by some enterprises. AWS KMS does allow for concepts such as:

- Key rotation
- Giving friendly names to individual keys
- Deep integration with the AWS IAM features
- Integration with most of the AWS add-on services, such as Elastic Block Store (EBS), Relational Database Service (RDS) and Simple Email Service (SES) S3

This makes AWS KMS a much more desirable service than AWS CloudHSM when regulatory requirements are not in the picture. AWS KMS is also widely available across multiple regions, which gives it an availability and accessibility advantage over AWS CloudHSM. However, because AWS KMS is a shared service, there could be differences in performance throughout the day.

A few other key details around AWS KMS:

- Centralized management for all key operations
- Audit trail in AWS CloudTrail includes users, time, date, data and which keys were used
- High availability across regions
- Support for bring your own key (BYOK)
- Limit of 1,000 keys per region (can be increased, if justified)

DDoS Protection

Not all AWS customers will need to worry about distributed denial of service (DDoS) protection. Those using AWS in a hybrid IT model without making the AWS portions of their operations internet accessible would not generally need to worry about DDoS attacks on their AWS components. Even those who are internet accessible, depending on the service they are offering and the impact downtime would have on them, would need to immediately plan on DDoS mitigation. However, those who are building their service model on top of AWS and have availability SLAs with their customers — or those who cannot afford being taken offline due to the impact of a DDoS attack — should consider adopting at least some components of DDoS mitigation.

Although AWS has sufficient capacity within each reason to absorb the impact of most DDoS attacks, customers should still invest in protection mechanisms to maintain the uptime of their instances and prevent disruption. AWS has features that can assist in maintaining uptime and potentially reducing the load caused by DDoS attacks. Those features are:

- **Auto Scaling:** This feature allows an instance to "expand" to meet incoming demand. This could include bringing up other instances of the impacted workload in the current or other regions. When the attack subsides, the on-demand instances would be turned off automatically. Note that Auto Scaling is a paid feature, so there are costs associated with it, and depending on the size and length of the attack, it can end up being costly. Customers should carefully consider the use of this feature against the cost of downtime or interruption.

- **Amazon CloudFront:** This is AWS's content delivery network (CDN) and is useful for web content, APIs, video or other web assets. However, customers should be aware of the pricing of this service because a DDoS attack could potentially send a customer to a higher pricing tier.

- **AWS Elastic Load Balancing (ELB):** While not directly involved in DDoS mitigation (as in it does not scrub traffic), it works with Auto Scaling, Amazon Route 53 and AWS VPCs to redirect traffic and optimize resource utilization.

- **Amazon Route 53:** This is AWS's DNS solution and can be used to redirect traffic, perform health checks, work with Auto Scaling to bring up new instances based on load, and work with ELB to manage and engineer traffic in an attempt to optimize it.

- **Security Groups:** This limits access to an instance using only the ports needed. The attack traffic would likely still make its way into a customer's VPC. Writing a compact and concise security group ACL could limit the attack surface and reduce the chance that a DDoS attack would actually make it all the way back to the targeted instance. Note, however, that firewalls are not DDoS mitigation devices. The goal here is to limit the number of exposed services or open ports that could be targeted.

- **Amazon EC2 instances:** Depending on the operating system, these may also support rate limiting within their own firewalls, although there could be an input/output (I/O) bottleneck in those cases, so this should not be relied upon as a first line of defense.

AWS has stated that null routing is the option of last resort. AWS also offers security architects and engineers to assist customers with designing and implementing solutions that protect a customer's infrastructure. Gartner's "DDoS: A Comparison of Defense Approaches" (https://www.gartner.com/document/code/268154?ref=grbody&refval=3454732) tackles some of the issues cloud customers face in detail and is recommended reading for those worried about DDoS attacks in general.

Using security groups and instance/OS-level rate limiting is recommended as a standard practice, provided customers properly understand their traffic patterns. Rate limiting is a mixed bag if improperly implemented because it can self-DoS a service if sized incorrectly. Flow accounting is a good method of assessing what is "normal" as far as traffic patterns and transactions go. Application logs could also provide some insight. This allows a customer to both tailor policy and identify what needs to be protected as it relates to DDoS attacks.

One major consideration to look at with some of the features are the costs involved. DDoS mitigation is not without cost. Because some AWS services are based on transaction numbers or bandwidth usage, implementing these features may come with a hefty price. Customers will need to weigh their need for availability versus the cost of maintaining that availability. Like many cloud service options, these are easy to implement without considering their financial impact.

Outside of AWS directly, some external providers also offer DDoS mitigation for AWS environments. Providers like Imperva, through its Incapsula product, and Neustar offer services for DDoS protection for AWS customers. AWS customers who are concerned about DDoS but are unfamiliar with DDoS mitigation are encouraged to reach out to external providers as well as AWS security architects to identify the best solution for their environment.

Logging and Monitoring

A key component of any security architecture program is the ability to log and monitor the environment. Telemetry data can inform security practitioners about the effectiveness of their policy and where changes need to be made. This same data is also critical to forensic investigations and can be used to spot security incidents. Logging of telemetry data, API usage, account usage and actions performed, and flow accounting should be important parts of any AWS implementation.

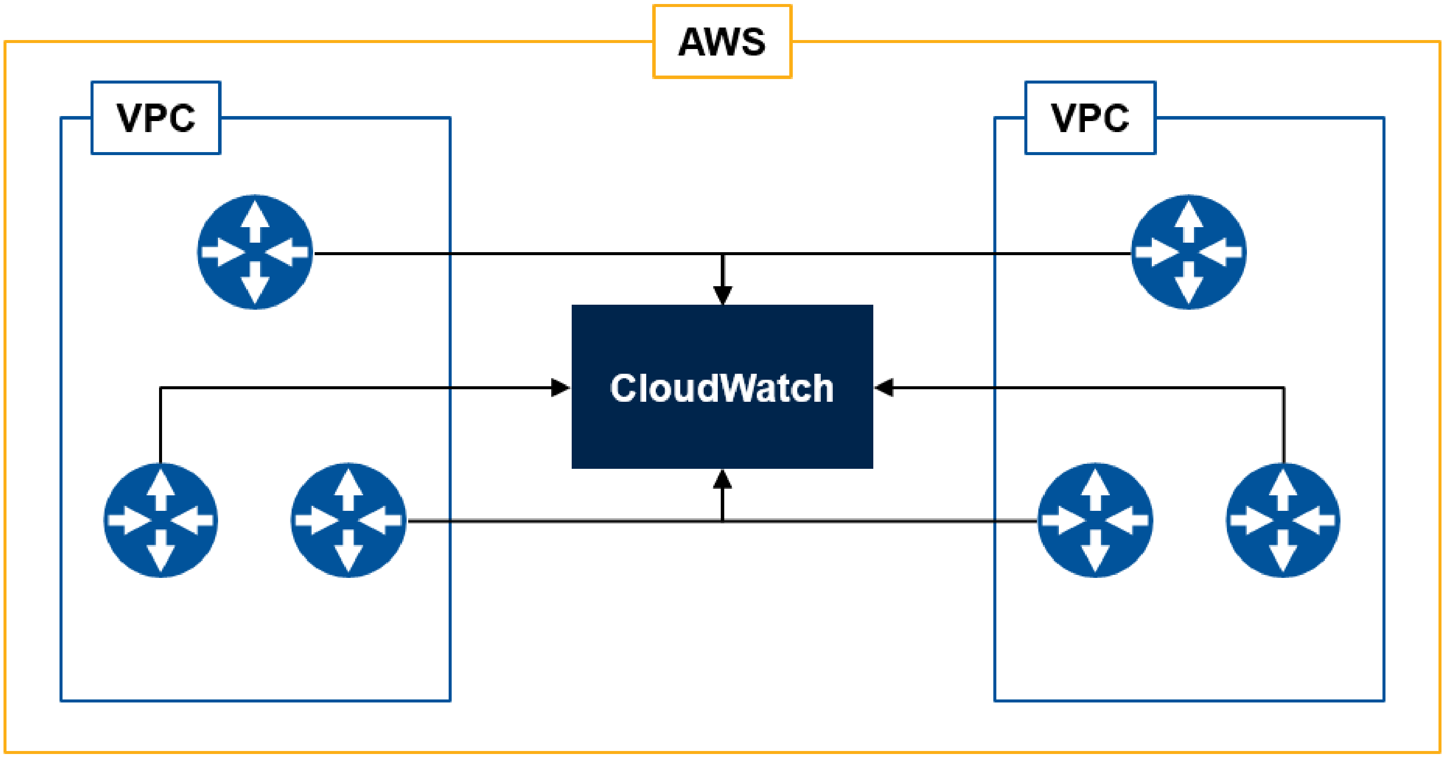
Amazon CloudWatch is the central monitoring service made available within AWS. It's actually much more than just a log collection tool because it can also track metrics, alarm on conditions set by the customer, monitor instance resources and perform health checks. Individual instances and even applications within instances can be configured to forward their logs into Amazon CloudWatch. It would be inappropriate, however, to equate Amazon CloudWatch with a security information and event management (SIEM) tool. There are some overlapping features, such as alarms, that are set off when conditions are met, and there is some limited monitoring capability. However, these should not be confused with more traditional security analytics.

Instead, Amazon CloudWatch is a logging and monitoring service that can and should be used not only to evaluate performance of the overall environment, but also to evaluate the effectiveness of the policies deployed. Because Amazon CloudWatch is a real-time monitoring service, one obvious use case is for troubleshooting where a problem might exist. In a security context, customers can also use Amazon CloudWatch to identify potential security violations or attacks in progress.

Customers should integrate any AWS IAM features into Amazon CloudWatch and take advantage of the audit trail it provides. The concept here is that, when a user performs an action, it is logged by the user ID, the time and what action was performed. Logging IAM actions into Amazon CloudWatch is one way to identify credential misuse or actions performed that may not have been intended by a user. Naturally, this also extends to stolen credentials and intentionally malicious activity. Another strength of integrating AWS IAM actions into Amazon CloudWatch is through the AWS Config utility. This can allow easy backing out or reversing of changes that negatively affect the environment or violate security policy.

AWS CloudTrail is an important service that monitors and logs API calls. AWS CloudTrail reports on API calls done via command line interface (CLI), the web interface and individual services. Because API calls can carry a lot of power within AWS, Gartner recommends that AWS CloudTrail be set up not only to log API calls itself, but also to log those API calls and usage into Amazon CloudWatch. Much like AWS IAM, this is an audit trail that can be used to identify the who, what and when. Along with AWS Config, Amazon CloudWatch can be used to reverse changes if they end up violating security policy (see Figure 10).

Figure 10. Amazon VPC Flow Logs With Amazon CloudWatch



Source: Gartner (September 2016)

A recent addition to AWS is VPC Flow Log accounting. This is an AWS feature that is similar to Cisco's NetFlow or the industry-standard IPFIX that reports on flow accounting within the VPC. Flow logs should be brought into Amazon CloudWatch so that traffic patterns can be assessed and analyzed and so security policy can be modified to fit new trends or to address policy requirements that were missed. Flow accounting has proven effective at the network layer to document and analyze traffic behaviors, and Gartner advises AWS customers to take advantage of the concept.

That said, in conversations with Gartner clients, usability issues are a reoccurring theme with VPC Flow Logs. Because they are not formatted similarly to NetFlow or IPFIX datasets, bringing that data into third-party flow analyzers has not been easy. A financial services client indicated that it had to write its own software to massage the data from the VPC Flow Logs into a format that could be used by its flow analytics software. Another client in the software development space eventually had to discontinue use of VPC Flow Logs because it could not make effective use of the data as it was presented.

When analyzing the feature, Gartner does see value in the VPC Flow Logs but understands the formatting issues they can present. AWS customers are advised to at least evaluate VPC Flow Logs to see if, individually, they can make use of the data. Again, flow logging is a powerful way to see what traffic is traversing one's network and to help identify areas where policy needs to be adjusted. However, because the format is not equivalent to that of IPFIX or NetFlow, without further work, the VPC Flow Logs may not be usable by all customers. As an alternative, third-party vendors such as Dome9 can analyze and visualize the VPC Flow Logs. Other vendors, such as Splunk and FlowTraq, can convert and massage the data into formats that are usable by existing enterprise toolsets.

Gartner's "How to Monitor the Security of Public Cloud Resources" (https://www.gartner.com/document/code/273118?ref=grbody&refval=3454732) is recommended for a more detailed assessment of monitoring in environments like AWS. One of the document's key recommendations is pertinent in this case and needs to be kept in mind when planning on monitoring and logging requirements:

> **In general, plan on doing more monitoring in public cloud environments due to less control over the computing stack. Compensate for lack of visibility from the layers of the stack that CSP controls by performing additional monitoring from the layers you control.**

Third-Party AWS Marketplace

AWS offers security solutions out of the box that meet the demands and requirements of most enterprise customers. However, because some security professionals and executives are still not convinced about the state of public and hybrid cloud native security, AWS provides the AWS Marketplace, where traditional vendors (Cisco, Palo Alto Networks, F5, Check Point and others) offer virtual appliances or security software. It is also a place where up-and-coming or cloud-specific solutions providers sell AWS-specific solutions. While research shows that most AWS customers will maintain their relationships with OEM vendors both within their enterprise data center and at AWS, the AWS Marketplace offers solutions and platforms that can complement or help complete technical security requirements of enterprises. In many cases, these solutions will enhance the security posture of AWS-deployed services and software.

Use of AWS Marketplace solutions does change how customers manage their AWS environment. These solutions are not always represented in the dashboard, could lack API access, are not managed via the CLI and may not participate in AWS features like Amazon CloudWatch, AWS Config and others. This means customers may face a fractured management structure within AWS. Although not always the case, this could create a suboptimal management situation. From a security aspect, this means that security policy may not be consistent or that visualizing and managing policy between AWS native applications and third-party offerings may need yet another tool for reconciliation. Gartner does not advise against the use of AWS Marketplace offerings, but instead that customers choose their tools carefully while keeping an eye on the complexity and integration issues that may arise from such combinations.

Table 4 provides some examples of third-party providers.

Table 4: Examples of Third-Party Providers in the AWS Marketplace, by Function

Infrastructure ↓	IAM ↓	Data Protection ↓	Key Management ↓
Fortinet	Okta	Trend Micro	Vormetric
Imperva	OneLogin	Gemalto	Voltage Security
Cisco	Bitium	CloudLock	Townsend Security
Palo Alto Networks	SAP	CipherCloud	Covata
Check Point	SecureAuth	Symantec	Druva

Source: Gartner (September 2016)

Note that inclusion in the above table is not an endorsement by Gartner related to their assigned function. Rather, it's simply an acknowledgement that these providers exist in the marketplace.

Differences From the Enterprise Data Center

There are some important feature exclusions and differences in operation between a service like AWS and a traditional data center, especially when it comes to networking and security. In order to design a security architecture program, practitioners need to be aware of these differences. Some of these differences make it difficult, if not impractical, to replicate features from the enterprise data center in a cloud environment like AWS. Using a cloud infrastructure allows for customers to rethink how they do security and leave longstanding, suboptimal solutions behind in favor of a more agile and flexible deployment into a cloud environment. Notable differences include:

- IPv6 is not routed within VPCs. There is no option to natively forward IPv6 traffic inside of a VPC.
- For VPNs between the enterprise data center and a VPC, IPv6 is not supported. Only IPv4 tunnels can be established.
- Layer 1 and 2 "bumps in the wire," such as L2 firewalls, in-line IPS, DLP, packet captures and similar solutions are not supported natively. Some Gartner clients have mentioned the creative use of network address translation (NAT) in order to simulate Layer 2 in-line appliances, but this is not equivalent to a Layer 1 or Layer 2 security appliance.
- Third-party NGFW can be deployed into the VPC, which in turn offers IPS functionality for the customer. However, these all work in a Layer 3 deployment only. This generally requires a different way of visualizing and implementing particular security services as compared with how it might be done in the enterprise data center. Also, this may prevent certain functions from working at a network level (for example, packet captures).
- Although a longer discussion is outside of the scope of this paper, cloud environments place more value on instance security than network security. That is not to say that the enterprise data center does not make use of endpoint security agents. However, in a cloud environment, endpoint security at both the OS and application layer, as well as host protection mechanisms, carry more value than traditional security tools (firewall, IPS, network DLP and so on) due to differences in the cloud.
- By default and design, VPCs do not route traffic between each other. Customers must explicitly define any inter-VPC communication and create VPC peering configurations before any inter-VPC communication can occur.
- Path isolation technologies like private VLANs, VRFs, label switching, Generic Routing Encapsulation (GRE) tunnels and IP-in-IP are not supported. However, there are third-party platforms from the likes of Cisco, Check Point and F5 that do support and provide a few technologies like this, but none of them is native to AWS.
- Configuration errors can cause an environment to "fail open." Because there are no wires or switches in the traditional sense, user error can lead to security controls being bypassed at the click of a button. Care must be taken to ensure that the difference in cloud network configuration and subsequent changes do not bypass the controls that protect the customer assets and environment.

Another point to consider is that, with AWS, customers have a flexible and dynamic environment that is not constrained by legacy concepts or technology. For example, Layer 1 and 2 solutions came about mostly due to legacy needs and the desire to avoid redesigning the network in order to offer particular security features that an enterprise deemed necessary. Some of those requirements are not applicable to IaaS environments and should not be replicated if at all possible. Using a service from AWS allows enterprises to rethink how they do security. It provides an opportunity to optimize their security mindset specific to cloud environments and ideally reduce the security complexity that has accompanied years of building on top of existing security solutions.

Strengths

- AWS has been built with security in mind and continues to develop additional security features. When it comes to security requirements, except for the most demanding of customers, AWS offers enough native functionality in the form of network policy, data protection, key management, logging and monitoring, and attack mitigation for a comprehensive security architecture program to be executed.

- For many enterprises, the security features offered by AWS will be adequate, if not equivalent to, those found in the enterprise data center, without the need to adopt third-party solutions. In the cases where enterprise customers do not feel that AWS's offerings alone meet their needs, there is an ecosystem of third-party solution providers in the security space to bridge the gaps.

- VPCs, Security Groups and network ACLs provide an equivalent security solution, as compared with traditional firewalls, that simplifies how policies are defined and implemented compared with the traditional enterprise data center.

- The Key Management Service and IAM solutions are feature-rich and have the capabilities many enterprises will need to migrate or extend their data center into the cloud.

- Amazon provides APIs for many of its security features, eliminating the need to log in to the AWS console or CLI. API calls can be embedded in existing network management system (NMS)/operations support system (OSS) platforms and support strong authentication.

Weaknesses

- The omission of Layer 1 and Layer 2 security "bump-in-the-wire" options (such as packet capture, private VLANS, packet decoding and forensics) may limit what some customers can deploy. There may be regulatory requirements that mandate investigations of suspicious or malicious traffic. The lack of these features will inhibit that type of activity at the network level.

- The versatility of security solutions are a positive thing, but are potentially overwhelming for customers. While some examples in the documentation can handhold customers, many features such as the KMS and AWS Directory Services have a steep learning curve to them, preventing customers from taking full advantage of what they offer.

- The encryption and key management components of a data protection program are well-represented and highly functional within AWS. However, there is a gap. There are no native data or asset classification tools and an obvious absence of data loss prevention options. These features are available through the AWS Marketplace, and through vendors like McAfee and Symantec, but it would be beneficial to customers to have some of this functionality be native.

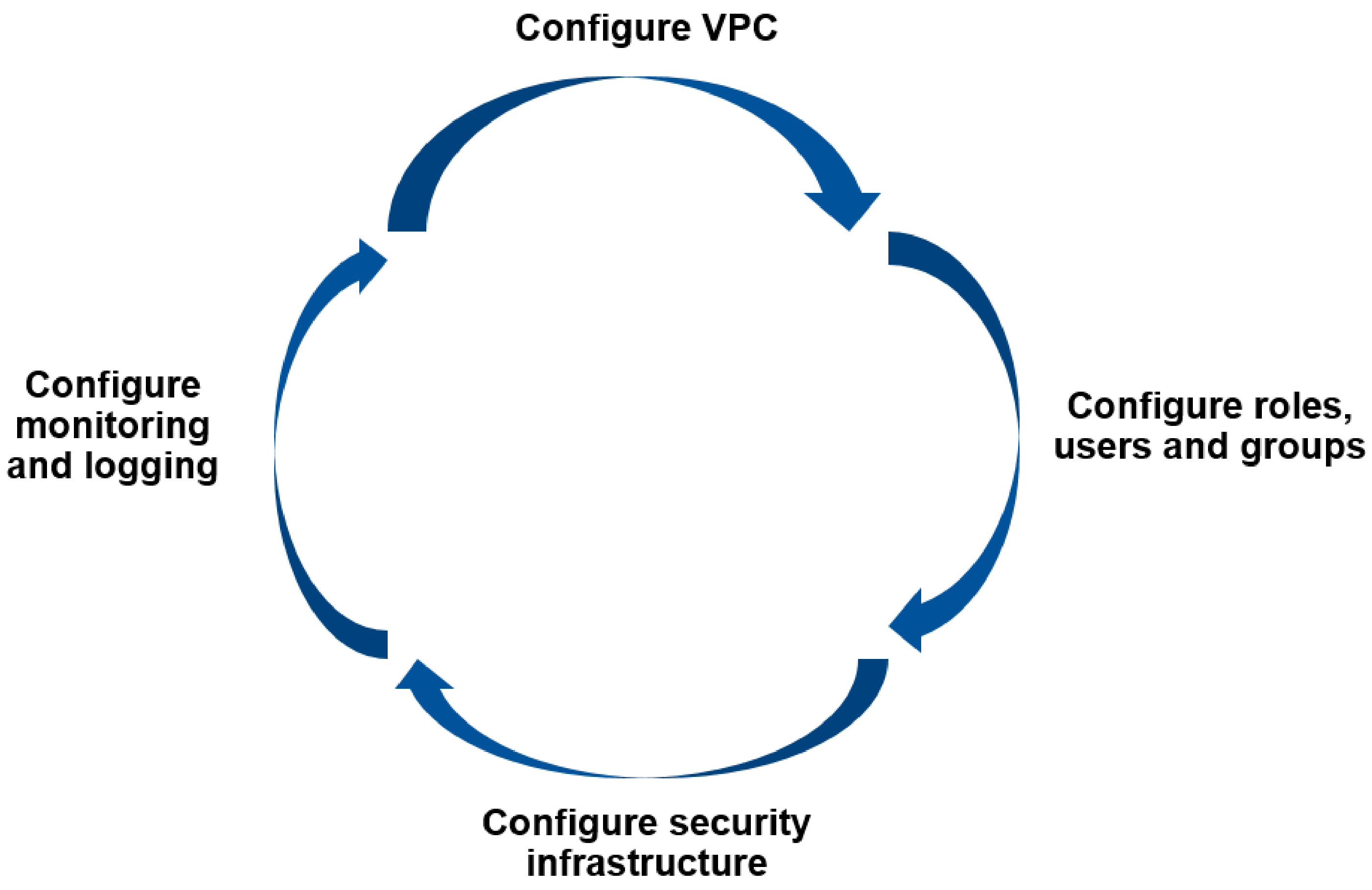
Guidance

Do Not Duplicate Enterprise Security Architecture

Amazon VPCs, along with security groups and network ACLs, are flexible enough that they mimic traditional switching and security infrastructure in many ways. Granted, there is no concept of Layer 2 networking and features, but some of those features, like private VLANs (PVLANs), can be mimicked by creative use of security groups. Other features, such as Address Resolution Protocol (ARP) security or Dynamic Host Configuration Protocol (DHCP) protection, have shown yet to be necessary in cloud environments.

New networks can be initialized without affecting other networks, and security policy can be changed on the fly without the need for an outage window. That doesn't mean that change control isn't necessary. If anything, change control may be even more important in the cloud because of the lack of physical infrastructure that could limit the fallout of a "bad" change. AWS provides much more flexible security elements (see Figure 11). It is not constrained by legacy security design and implementation concepts. Enterprise customers have an opportunity to rethink how they design and implement security policy in a manner that is more efficient than what is being done today in the traditional data center.

Figure 11. Security Architecture Life Cycle at AWS


Configure VPC
Configure roles, users and groups
Configure security infrastructure
Configure monitoring and logging

Source: Gartner (September 2016)

Be careful not to overarchitect and overdesign Amazon VPCs; keep the architecture as simple as possible. Instead of focusing on trying to build a secure network, aim for building a network of secure instances. The network will always play a critical role in overall enterprise security. The evolution of endpoint protection options and the consolidation of key network security features into common hardware/software should allow for much more simplistic security designs and operations.

Document all requirements before configuring VPCs and the associated security controls. Schedule the change (you still need change control), but do not forget to audit that change. Make sure the changes to an element do not have the unintended effect of modifying other elements and do not break communication flows elsewhere. Take advantage of AWS features like AWS Config to see what changes have occurred, who performed them and when it happened. VPCs and the networks within can become unruly quickly unless design disciplines are enforced. Much like the explosion of VMs in the enterprise, new networks can rapidly be deployed and create a difficult environment to troubleshoot and operate. Integrate security management and operations with AWS IAM to ensure only the required accounts can manage the network.

With the ability to create multiple VPCs, create one strictly for testing and validation. New policies and design changes are implemented and tested much easier than in a traditional physical environment. Customers will see the impact of changes in a sandbox and have the ability to modify and validate them before pushing them into production.

Explore and Test the Capabilities of AWS IAM Service

Enterprise customers will likely underestimate the capabilities of AWS's IAM. Whether it is through Active Directory or identity broker, or leveraged through AWS Directory Services, the level of detail that goes into the roles and groups are very powerful. With careful management, customers can effectively restrict which of their users can access functions and services at the individual command level. While this is not a new concept by itself, command-level authorization has always been difficult to manage and maintain. Using the automated and guided tools to evaluate what permissions an account needs, and if that account has too little or too much, greatly simplifies account management. The ability to audit individual accounts, the commands they have issued or resources they have accessed, as well as general account activity, are powerful tools for IAM administrators.

Do not use the AWS root account. Customers should create a new administrative account and apply account monitoring, privileged access management and strong password security, including multifactor authentication (MFA) to the root account. All other administrative accounts should follow suit because AWS provides simple tools to achieve these tasks. The root account, however, needs to be highly secured and locked down because abuse of root could lead to data exfiltration, creation/deletion of instances, modification of security policies, and deploying/suspension of additional AWS services or AWS Marketplace solutions.

Use managed policies instead of in-line policies. Managed policies are assigned to multiple users, groups and/or roles. They allow for very granular controls and support iterations of each control set. By using nested policies, customers can implement a "least privilege" policy across all of their AWS infrastructure from a central console. When integrated with Amazon CloudWatch, another AWS service, a comprehensive audit trail is also provided.

Use the AWS CloudHSM and/or AWS Key Management Service

For customers looking for PCI compliance, AWS CloudHSM does meet their key management requirements. It also provides the appropriate encryption standards to complete an audit. While there are many other considerations when looking at PCI, AWS CloudHSM is compliant with PCI Data Security Standard (DSS) Level 1, as well as International Organization for Standardization (ISO) 27017 and 27018.

Customers not requiring PCI should still invest time and run a pilot on the AWS KMS against their existing key management system, if they have one. AWS KMS is a central part of API access and data encryption options, and unlike the AWS CloudHSM, it is available in multiple regions at once. If customers are nervous about generating keys at AWS, they can generate their own keys with their existing key management platform and import that to Amazon.

When using the KMS, a good practice is to utilize key rotation, which can help blunt the impact of a lost or stolen key. Customers should also integrate AWS KMS with Amazon CloudWatch to log all key access, including the user, time and specific key that was used. Amazon CloudWatch provides a strong audit trail for all key use and can help quickly identify misuse or compromise when combined with AWS IAM policies. AWS KMS can also be managed via API, which in turn allows customers to manage their AWS KMS from existing network management tools and instrumentation.

Use Logging and Monitoring

Gartner strongly encourages customers to, at a minimum, utilize Amazon CloudWatch to centrally collect logs within AWS before, if necessary, exporting them to the enterprise SIEM or log collection/management system. If management and monitoring are being done with APIs, AWS CloudTrail should also be a firm requirement in the logging and monitoring area, and AWS CloudTrail should be feeding its data into Amazon CloudWatch. Using VPC Flow Logs is optional, but given the visibility they provide into network traffic within a VPC, they should be explored as yet another source of security and network intelligence.

Plan for DDoS Protection

While the immediate threat of DDoS is mitigated by moving to a cloud provider, a targeted attack can still take down a public-facing server. Customers should invest time and testing into getting the security groups as specific as possible. From there, leveraging Amazon Route 53 to perform health and load checks and identify potential problems is advised. Customers who have strict uptime and availability requirements should also look into Amazon CloudFront, a CDN provided by AWS, to move content away from an individual instance. Last, while keeping an eye on costs, Gartner recommends using Auto Scaling to bring up additional instances to manage the load from a DDoS attack and integrating AWS ELB into the network path. Combined, these services provide a resilient solution that should prevent most targeted DDoS attacks from taking down a customer's environment.

While DDoS services from the marketplace are available, customers should first look into what is offered natively within AWS. Anti-DDoS services built into WAF, NGFW and other stateful appliances are generally inadequate for attacks beyond a few gigabits per second and could make any targeted attack worse. They also could cause a false positive with Amazon Route 53 and AWS ELB, causing unnecessary resources to become active and increasing the customer's financial cost. If customers are not comfortable with DDoS mitigation, there are external providers that do offer a managed DDoS mitigation service.

The Details

AWS documentation is arranged and sorted by feature or service. It does not tend to have comprehensive architecture or design documents that look at the overall picture. It does have engineers and architects available to help customers come up with end-to-end solutions. Below is a list of important links that document how features discussed in this document work and how they are configured.

- Security Home (https://aws.amazon.com/security/)
- VPCs (https://aws.amazon.com/vpc/)
- Security Groups (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html)
- Network ACLs (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)
- AWS IAM (https://aws.amazon.com/documentation/iam/)
- AWS CloudHSM (https://aws.amazon.com/cloudhsm/details/)
- KMS (https://aws.amazon.com/documentation/kms/)
- Amazon CloudFront (https://aws.amazon.com/cloudfront/)
- Amazon Route 53 (https://aws.amazon.com/documentation/route53/)
- Auto Scaling (https://aws.amazon.com/documentation/autoscaling/)

Evidence

This assessment stems from Gartner inquiries that took place from January 2015 through June 2016 and included more than 500 participants. Other sources of information came from:

- AWS vendor briefings (13 April 2016, 11 May 2016, 19 May 2016)
- AWS webinars (10 May 2016 and 2 June 2016)
- VPC Security (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html)
- AWS Security Portal (https://aws.amazon.com/security/security-resources/)
- AWS KMS Documentation (https://aws.amazon.com/documentation/kms/)

Document Revision History

Implementing Effective IaaS Cloud Security in Amazon Web Services - 7 November 2014 (https://www.gartner.com/document/code/260748?ref=ddrec)

Recommended by the Author

In-Depth Assessment of Amazon Web Services (https://www.gartner.com/document/3096719?ref=ddrec&refval=3454732)

Managing Identities, Privileges, Access and Trust Primer for 2016 (https://www.gartner.com/document/3187123?ref=ddrec&refval=3454732)

Network Security Architectures for Virtualized Data Centers (https://www.gartner.com/document/3109819?ref=ddrec&refval=3454732)

How to Monitor the Security of Public Cloud Resources (https://www.gartner.com/document/3102228?ref=ddrec&refval=3454732)

Recommended For You

In-Depth Assessment of Oracle Cloud Infrastructure IaaS, July 2018 (https://www.gartner.com/document/3884666?ref=ddrec&refval=3454732)

How to Develop a Business Case for the Adoption of Public Cloud IaaS (https://www.gartner.com/document/3893869?ref=ddrec&refval=3454732)

Enhancing Operations Automation With Serverless Computing (https://www.gartner.com/document/3892975?ref=ddrec&refval=3454732)

2019 Planning Guide for Cloud Computing (https://www.gartner.com/document/3891095?ref=ddrec&refval=3454732)

IAM Is Vital for Successful Application Migration to IaaS (https://www.gartner.com/document/3895269?ref=ddrec&refval=3454732)

It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."