



CSP Provided Security Services

CSP Provided Security Services



All public cloud providers offer basic services with their own implementation techniques and pricing models.



Customer needs to stitch multiple services together



Security design in each cloud will be different.



Customer demands consistency, clean design and simple operation



The “Shared Responsibility” is Customer’s Responsibility at the end






































































References

<https://aws.amazon.com/blogs/security/update-of-aws-security-reference-architecture-is-now-available/>

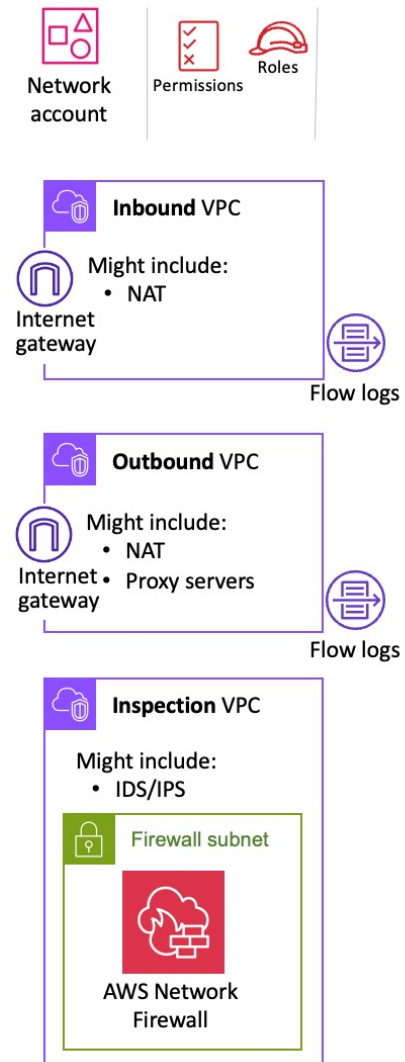
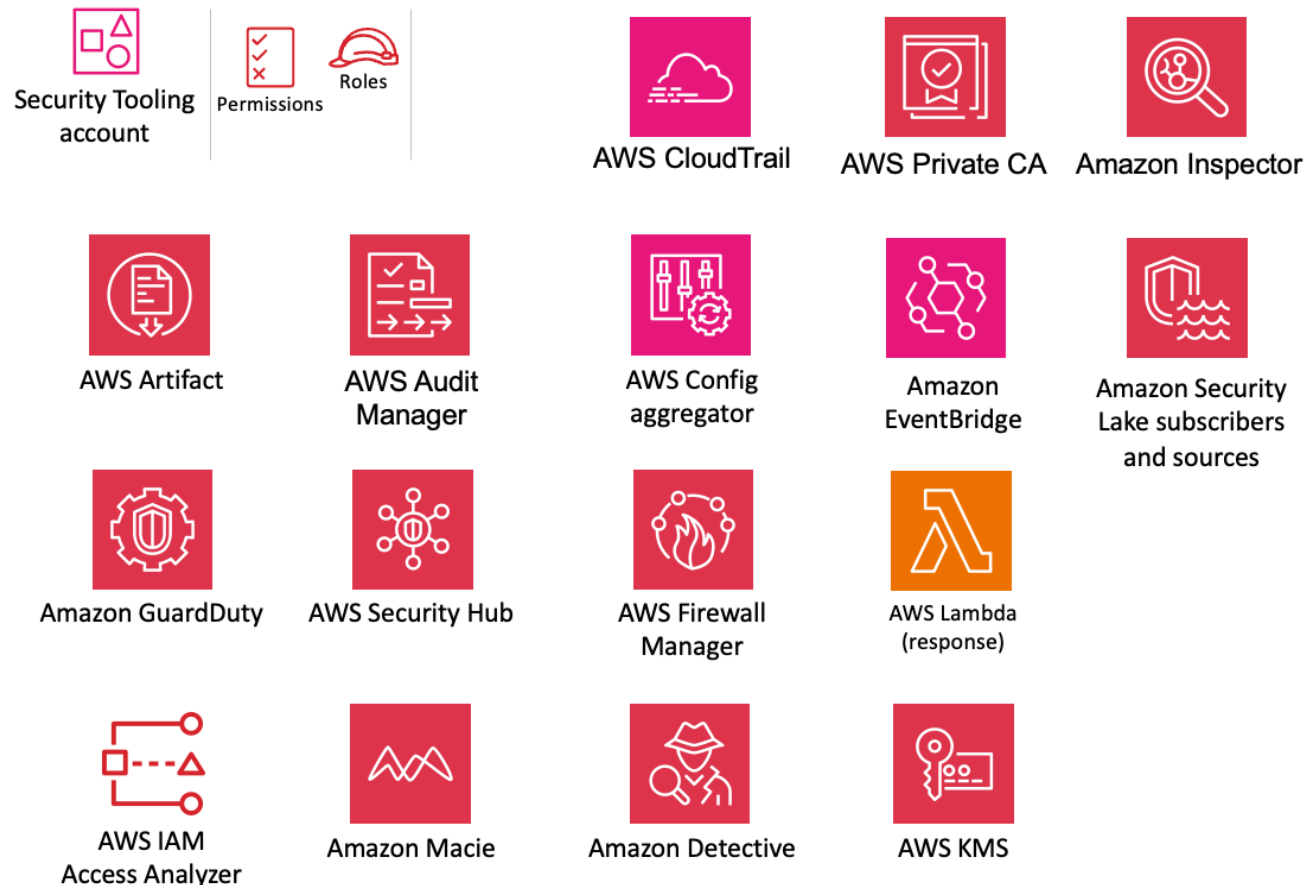
<https://azure.microsoft.com/en-us/solutions/network-security>

<https://aviatrix.com/resources/aviatrix/security-is-up-to-you-when-it-comes-to-cloud-security-don-t-rely-on-your-csp>

<https://cloud.google.com/docs/get-started/aws-azure-gcp-service-comparison>

aws	Azure	Google Cloud	AVIATRIX CE Aviatrix Certified Engineer
 Elastic Compute Cloud (EC2)	 Virtual Machine	 Compute Engine	
 Elastic Kubernetes Service (EKS)	 Azure Kubernetes Service (AKS)	 Google Kubernetes Engine (GKE)	
 Lambda	 Azure Functions	 Cloud Functions	
 Simple Storage Service (S3)	 Blob Storage	 Cloud Storage	
 Elastic Block Store	 Managed Disk	 Persistent Disk	
 Elastic File System	 File Storage	 File Store	
 Virtual Private Cloud	 Virtual Network	 Virtual Private Cloud	
 Route 53	 DNS	 Cloud DNS	
 Elastic Load Balancing	 Load Balancer	 Cloud Load Balancing	
 Web Application Firewall	 Web Application Firewall	 Cloud Armor	
 RDS	 SQL Database	 Cloud SQL	
 DynamoDB	 Cosmos DB	 Firebase Realtime Database	
 Redshift	 Synapse Analytics	 BigQuery	
 Elastic MapReduce	 HDInsight	 Dataproc	
 Kinesis	 Streaming Analytics	 Dataflow	
 SageMaker	 Machine Learning	 Vertex AI	
 Glue	 Data Factory	 Data Fusion	
 EventBridge	 Event Grid	 Eventarc	
 Simple Queuing Service	 Storage Queues	 Pub/Sub	
 Simple Notification Service	 Service Bus	 Firebase Cloud Messaging	
 CloudWatch	 Monitor	 Cloud Monitoring	
 CloudFormation	 Resource Manager	 Deployment Manager	
 IAM	 Active Directory	 Cloud Identity	
KMS	Key Vault	Cloud KMS	

Design and deploy security in single cloud is a challenge



* Don't underestimate the cost implications

Design and deploy security in multiple clouds is even more challenging

Use-Case(s)	AWS Service	Azure Service
Users to control access to services and resources	<u>Identity and Access Management (IAM)</u>	<u>Azure Active Directory</u>
Protect Internet-facing web applications from common exploits.	<u>Web Application Firewall</u>	<u>Web Application Firewall</u>
Ingress and Egress Firewall for web and non-web traffic East/West and North/South Firewall for web and non-web traffic	<u>AWS Network Firewall</u>	<u>Firewall</u>
Detect threats from on-premises and in the cloud locations.	<u>GuardDuty</u>	<u>Microsoft Sentinel</u>
Protection from distributed denial of services (DDoS) attacks.	<u>Shield</u>	<u>DDos Protection Service</u>
L4 Security to allow or block traffic going to EC2/VM	Security Group	Network Security Group

* Don't underestimate the cost implications

Design and Deploy Security in Multiple Clouds Could be Worse

Use-Case(s)	AWS Service	Azure Service
Normalize and correlate network data for analysis of risky activity.	<u>Amazon Security Lake</u>	<u>Azure Sentinel</u>
On-prem connectivity with security	<u>Direct Connect MACSec</u>	<u>Express Route with MACSec</u>
Logging and Monitoring	<u>CloudWatch</u> , <u>Cloud Trail</u> , <u>VPC Flow Logs</u> , <u>AWS Network Manager</u>	<u>Azure Monitor</u> , <u>Network Watcher</u>
Aggregates security alerts from CSP and partner products	<u>AWS Security Hub</u>	<u>Azure Security Center</u> <u>Microsoft Defender for Cloud</u>
IPSec Encryption for Network Data in Transit	<u>S2S VPN with VGW</u>	<u>S2S VPN with VNG</u>
Network Segmentation (VRF)	Manual route table management	Manual UDR management

* Don't underestimate the cost implications



Aviatrix Certified Engineer (ACE)
<https://aviatrix.com/ACE>



COMMUNITY
<https://community.aviatrix.com>