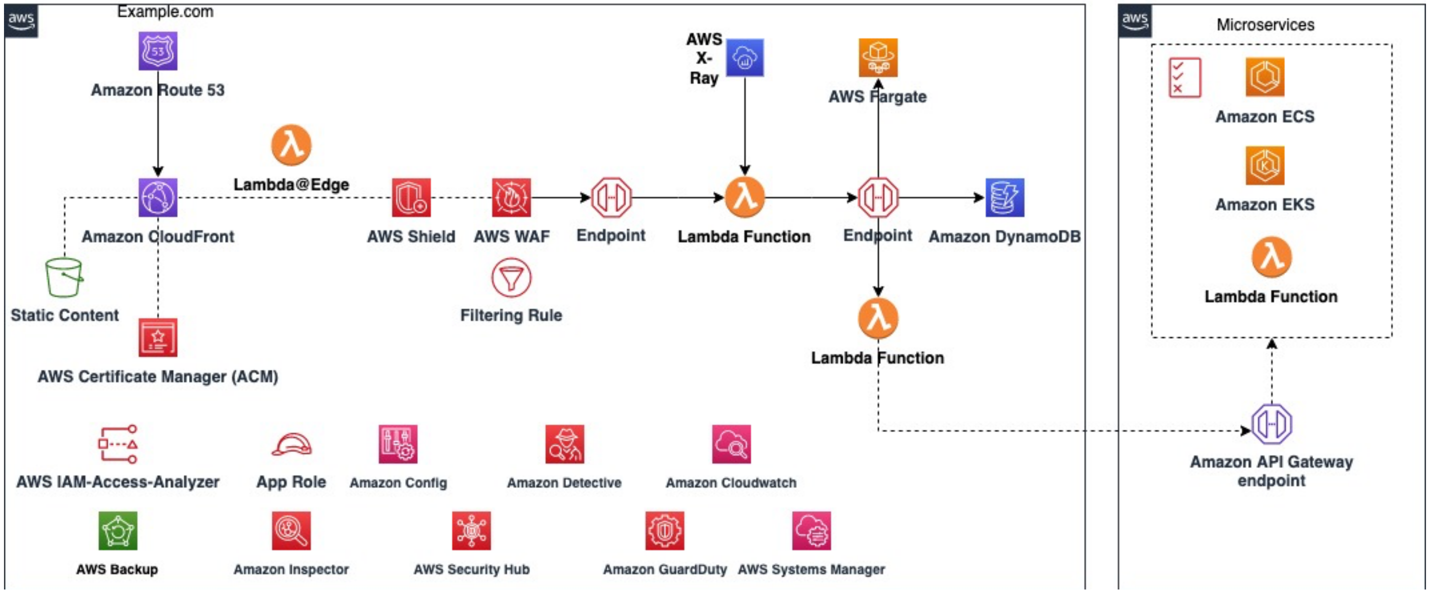
TIC 3.0 AWS Overlay Reference - Containers and Abstracted Services



Overview

The above diagram illustrates at a high level how different AWS services and partner solutions can help with TIC 3.0 compliance for web applications hosted with containerized or abstracted services. The diagram is not meant to serve as a complete and exact illustration for implementation guidance. For exact implementation guidance, please refer to the AWS documentation for each service, respectively, or reach out to your AWS account team or preferred partner.

In this scenario, static content of the web application is hosted on Amazon CloudFront and Amazon S3. Dynamic content consists of microservices developed using Amazon ECS, Amazon EKS or AWS Fargate with a DynamoDB database. The microservices expose endpoints using Amazon API Gateway. These microservices are deployed within the same account or another account. The endpoints are protected using AWS Shield and AWS WAF.

The table below further breaks down how various services in the above diagram support different TIC security capabilities as listed in CISA's *Trusted Internet Connections 3.0, TIC Core Guidance Volume 3: Security Capabilities Catalog*. We start out with Universal Capabilities and then add additional capabilities based on the scenario above, for example by describing how different AWS networking services support Networking Policy Enforcement Point (PEP) Capabilities.

Universal capabilities

TIC Security Capability	Service	How the service provides the capability	TIC Objective
Backup and Recovery	AWS Backup	Centrally deploy data protection policies to configure, manage, and govern backup activity across your company's AWS accounts and resources.	Ensure Effective Response, Ensure Service Resiliency
	AWS Config	Continuously monitors and records AWS resource configurations; comprehensive snapshot of all resources and their configuration attributes provides a complete inventory of resources for use in recovery processes.	Ensure Effective Response
Central Log Management with Analysis	Amazon VPC Flow Logs	Enable capture of information about the IP traffic going to and from network interfaces in VPC.	Protect Traffic Integrity; Ensure Effective Response
	AWS Cloudtrail	Track user activity and API usage.	Ensure Effective Response
	AWS Network Firewall	Monitor network traffic and traffic filtering done by the stateful rule groups in Network Firewall firewalls.	Ensure Service Resiliency; Ensure Effective Response
	Amazon Cloudwatch Logs	Centralize logs from all of your systems, applications, and several AWS services in a single, highly scalable service.	Ensure Effective Response
	Amazon Route 53	Queries that DNS resolvers forward to Route 53.	Ensure Effective Response

	Resolver Query Logs		
	Amazon Route 53 Public Zone Logs	Information about the public DNS queries that Route 53 receives.	Ensure Effective Response
	AWS Service Logs - Cloudwatch; AWS Service Logs - S3	AWS services such as Amazon RDS publish logs to CloudWatch Logs, whereas services such as Application Load Balancer publishes logs to S3.	Protect Traffic Integrity; Ensure Effective Response
Configuration Management	AWS CloudFormation	Model, provision, and manage AWS and third-party resources using declarative statements in YAML or JSON.	Ensure Effective Response, Ensure Service Resiliency
	AWS Config	Continuously monitor and record AWS resource configurations.	Ensure Effective Response
	AWS Lambda	Use AWS Lambda functions to evaluate whether AWS resource configurations comply with custom Config rules.	Ensure Effective Response
	AWS Systems Manager	Enable reporting and workflows for managing application configuration and infrastructure on AWS and on premises.	Ensure Effective Response
	Amazon Cloudwatch	Collect and track metrics, collect and monitor log files, and set alarms to detect anomalous behavior.	Ensure Effective Response
Resilience	Application Load Balancer	Automatically distributes incoming application traffic across multiple targets and virtual appliances in one or more Availability Zones (AZs).	Ensure Service Resiliency
	AutoScaling	Monitors your applications and automatically adjusts capacity to maintain steady, predictable performance.	Ensure Service Resiliency, Manage Traffic
Vulnerability Management	Amazon Inspector	Automatically discover and quickly route vulnerability findings in near real time to the appropriate teams.	Ensure Service Resiliency; Ensure

			Effective Response
	AWS Systems Manager	Systems Manager Automation runbooks remediate Amazon Inspector findings using resource tags and Amazon Inspector finding severity.	Ensure Service Resiliency, Ensure Effective Response
Patch Management	AWS Systems Manager	Systems Manager Patch Manager automates the process of patching managed nodes with both security related and other types of updates for both operating systems and applications.	Ensure Service Resiliency, Ensure Effective Response
Enterprise Threat Intelligence	Amazon GuardDuty	Continuously monitor AWS accounts and workloads for malicious activity and deliver detailed security findings for visibility and remediation.	Ensure Service Resiliency; Ensure Effective Response
Dynamic Threat Discovery	Amazon GuardDuty	Expose threats using anomaly detection, machine learning, behavioral modeling, and threat intelligence feeds from AWS and third-parties.	Ensure Service Resiliency; Ensure Effective Response
Inventory	AWS Config	Continuously monitor and record AWS resource configurations;	Ensure Effective Response
	AWS Systems Manager	AWS Systems Manager Inventory provides visibility into AWS computing environment and collect *metadata* from managed nodes.	Ensure Effective Response
Policy Enforcement Parity	AWS Config	AWS Config rules and conformance packs can be used to identify deviations from desired configurations; Remediation of those deviations can be automated using AWS Lambda.	Ensure Service Resiliency; Ensure Effective Response
	AWS Lambda	Use AWS Lambda functions to evaluate whether AWS resource configurations comply with custom Config rules.	Ensure Service Resiliency; Ensure

			Effective Response
	AWS Systems Manager	AWS Systems Manager Compliance centralizes all relevant operational data including software inventory, and patch compliance status for a clear view of infrastructure compliance and performance.	Ensure Service Resiliency; Ensure Effective Response

Web PEP Capabilities

TIC Security Capability	Service	How the service provides the capability	Objective
Break and Inspect	AWS Marketplace	Access AWS Partner solutions such as firewalls by replacing the AWS Network Firewall with a Gateway Load Balancer. These solutions offer the ability to break and inspect traffic. As an alternative solution, set up VPC Traffic Mirroring on instances behind and Application Load Balancer, which terminates the TLS, and stream packages to an inspection solution.	Protect Traffic Integrity
Domain Resolution Filtering	Route 53 Resolver DNS Firewall	Block DNS-level threats for DNS queries going out from the VPC with domain name filtering rules and lists of domain names to allow or block. Customize responses for the DNS queries that are blocked.	Manage Traffic
Filtering	AWS Shield	AWS Shield (Standard version) offers DDoS protection. Shield Advanced adds integration with AWS WAF.	Manage Traffic, Ensure Service Resiliency
	AWS WAF	Filter malicious content by means of rule groups, both managed and custom, to block content like cross-site scripting and SQL injection.	Manage Traffic, Protect Traffic Integrity. Ensure Service Resiliency

	AWS Network Firewall	Filter content with Suricata compatible IPS rules.	Manage Traffic, Protect Traffic Integrity
	AWS Marketplace	The AWS Marketplace offers solutions from leading partners.	Manage Traffic, Protect Traffic Integrity

Networking PEP Capabilities

TIC Security Capability	Service	How the service provides the capability	Objective
Access Control	AWS Network Firewall	Filter traffic at the perimeter of the VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect.	Manage Traffic
	AWS WAF	Control how protected resources respond to HTTP(S) web requests through the central components such as Web ACLs, Rules and Rule Groups.	Manage Traffic
	Amazon VPC: Security Groups	Security Groups are stateful firewalls at the instance level such as EC2 instances, RDS databases, and Application Load Balancers.	Manage Traffic
	Amazon VPC: Network ACLs	Network Access Control Lists are stateless firewalls at the subnet level.	Manage Traffic
Internet Address Deny listing	AWS Network Firewall	Use managed rule groups such as Domain list rule groups to block HTTP(S) traffic to domains identified as low-reputation, or that are known or suspected to be associated with malware or botnets. Create deny rules for specific IPs.	Manage Traffic
	AWS WAF	Provides fine-grained control over HTTP(S) web requests for protected resources. Use criteria like IP address origin of the request, country of origin of the request and much more.	Manage Traffic

	Amazon VPC: Network ACLs	Subnet level firewall that allows deny rules for specific IPs or ranges of IPs and protocols.	Manage Traffic
Host Containment	AWS Systems Manager	Use Incident Manager, a capability of AWS Systems Manager, to help triage incidents faster and return applications to normal.	Manage Traffic, Ensure Effective Response
	Amazon VPC: Security Groups	Security Groups begin as an implicit Deny for all traffic. Change the security groups manually or with automation to block traffic for impacted hosts, rendering the host contained.	Manage Traffic, Ensure Effective Response
	Amazon VPC: Network ACLs	Network ACLs contains hosts at a subnet level by denying all traffic to the subnet.	Manage Traffic, Ensure Effective Response
	Amazon VPC	Configure an "Isolation VPC", ideally in a separate account and effectively instrumented to handle compromised instances, that are spun up to do forensic analysis on them.	Manage Traffic, Ensure Effective Response
Network Segmentation	Amazon VPC	Split the environment up in multiple subnets with VPC, either as "Public" or "Private" subnets. Public subnets have direct Internet access. Private subnets are inaccessible from the Internet.	Manage Traffic, Ensure Service Resiliency
Micro-segmentation	AWS Private Subnet	Private subnets are a part of AWS VPC. Private subnets are inaccessible from the Internet.	Manage Traffic, Ensure Service Resiliency
	AWS Public Subnet	Public subnets are a part of AWS VPC. Private subnets are accessible from the Internet via public IP addresses.	Manage Traffic, Ensure Service Resiliency
	AWS Firewall Subnet	Firewall subnets can be either private or public subnets. These subnets are dedicated to firewall appliances for simplified configuration and routing as well as improved security.	Manage Traffic, Ensure Service Resiliency

Resiliency PEP Capabilities

TIC Security Capability	Service	How the service provides the capability	Objective
Distributed Denial of Service Protections	AWS Shield	AWS Shield Standard tier focuses on Layer 3 and 4 attacks. Advanced tier provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF.	Manage Traffic, Ensure Service Resiliency
	AWS WAF	Protect against DDoS attacks with custom AWS WAF rules written to match the signature of the attack and to block those requests.	Manage Traffic, Ensure Service Resiliency
Regional Delivery	AWS Global Infrastructure	In many cases designing a workload to span across multiple availability zones within a region will be sufficient to have a resilient and performant workload. Multi-region setups may be beneficial in certain disaster recovery scenarios to separate backups or failover systems with several hundred miles.	Ensure Service Resiliency
	Amazon API Gateway	Amazon API Gateway provides a regional endpoint intended for clients in the same region. When a client running on an EC2 instance calls an API in the same region, or when an API is intended to serve a small number of clients with high demands, a regional API reduces connection overhead	Ensure Service Resiliency
Elastic Expansion	Application Load Balancer	The Application Load Balancer (ALB) is a managed service that automatically scales according to needs.	Ensure Service Resiliency
	Amazon EC2 Auto Scaling	The application servers sit behind the ALB and scale horizontally by means of an auto-scaling group.	Ensure Service Resiliency
	Amazon CloudFront	Cache certain information closer to the users. This improves the overall user experience and can reduce the load on your application servers.	Manage Traffic, Ensure Service Resiliency

	Amazon RDS	Scales horizontally by adding additional read replicas. Scale the database vertically by adding more CPU or memory if more write capacity is needed.	Ensure Service Resiliency
	AWS Fargate Auto Scaling	AWS Fargate automatically increases or decreases your desired container task count by integrating Amazon ECS on Fargate with Amazon CloudWatch alarms and Application Auto Scaling	Ensure Service Resiliency
	AWS Lambda Scaling	AWS Lambda provides a serverless compute service that can scale from a single request to hundreds of thousands per second using concurrency and transactions per second	Ensure Service Resiliency
	Amazon API Gateway	Provides throttling at multiple levels including global and by service call to manage traffic to back-end applications effectively and ensure service resiliency; Also provides caching to improve performance and reduce traffic sent to the back end.	Manage Traffic, Ensure Service Resiliency

Intrusion Prevention PEP Security Capabilities

TIC Security Capability	Service	How the service provides the capability	Objective
Intrusion Detection and Prevention Systems	AWS Network Firewall	Provide active traffic flow inspection to identify and block vulnerability exploits using signature-based detection. Perform web filtering that can stop traffic to known bad URLs and monitor fully qualified domain names.	Manage Traffic

Data Protection PEP Security Capabilities

TIC Security Capability	Service	How the service provides the capability	Objective
Access Control	AWS Identity and Access Management	Access to data in an S3 bucket can be controlled with IAM.	Manage Traffic, Protect Traffic Confidentiality
	Resource Policies	Access to data in an S3 bucket can be controlled with Resource Policies.	Manage Traffic, Protect Traffic Confidentiality
	Amazon CloudFront	Access to S3 from CloudFront is controlled with “origin access control (OAC)”, which ensures that the data in the S3 bucket can only be access from the intended CloudFront distribution.	Manage Traffic
	AWS Secrets Manager	For access to a database such as Aurora MySQL from an application or via a bastion host, access can be controlled via Secrets Manager, storing and rotating credentials.	Protect Traffic Confidentiality
Protections for Data at Rest	AWS KMS	Create, manage, and control cryptographic keys across applications and more than 100 AWS services including options to import or create and manage your own keys.	Protect Traffic Confidentiality, Protect Traffic Integrity
Protections for Data in Transit	AWS Certificate Manager	Provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources.	Protect Traffic Confidentiality, Protect Traffic Integrity