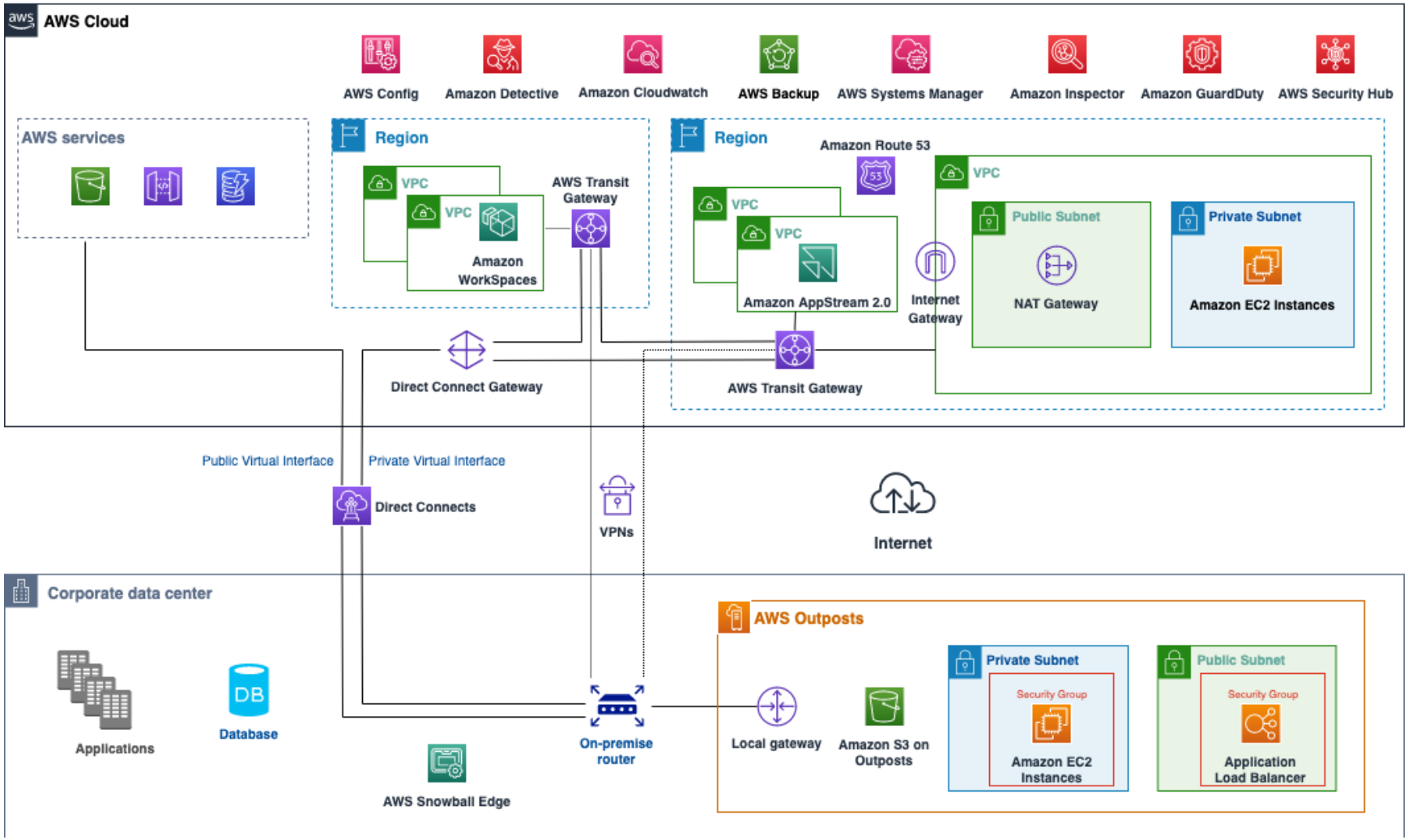
TIC 3.0 AWS Overlay Reference - Hybrid/Edge Scenario



The above diagram illustrates at a high level how different AWS services and partner solutions can help with TIC 3.0 compliance for edge driven solutions. 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, workloads consist of solutions tightly integrated across the corporate data center and AWS. An online example is a service like Amazon AppStream 2.0 or Amazon WorkSpaces (an Amazon VDI solution), to which you can connect securely via AWS Direct Connect or AWS VPN. Networking is simplified with AWS Transit Gateway and Direct Connect Gateway services. An example of an offline solution could be AWS Snowball Edge for edge computing in remote locations or for large data transfers to and from your data center. Another example is AWS Outposts, which is an AWS rack installed directly into your data center for close proximity. Identity can be integrated by extending an on-premises Active Directory into the AWS cloud by using AWS Directory Service.

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	Ensure Effective Response

		and their configuration attributes provides a complete inventory of resources for use in recovery processes.	
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. Place this in each VPC or in a Central Inspection VPC to monitor traffic to/from on-premise.	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 Resolver Query Logs	Queries that DNS resolvers forward to Route 53.	Ensure Effective Response
	Amazon Route 53Public 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 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 anomolous behavior.	Ensure Effective Response
	AWS Organizations	Centrally manage your environment, apply guardrails across accounts, and centrally secure and audit your environment.	Ensure Effective Response
Resilience	AWS Transit Gateway	Acts as a highly available router between the Internet facing Hub VPC and all other (private) VPCs across accounts. Simplifies in-Region and inter-Region distributing encrypted traffic across the AWS network rather than the public Internet, as well as being hub for connecting to on-premise VPNs and Direct Connect connections.	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 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
Strong Authentication	AWS Directory Service	Set up Managed AD in AWS or use AD Connector to leverage your on-premises Microsoft Active Directory in AWS.	Protect Traffic Integrity. Ensure Service Resiliency

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
	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

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
	AWS Virtual Private Network	Allow direct access to a secure enclave or web application with a traditional VPN connection.	Manage Traffic, Protect Traffic Integrity
	AWS Direct Connect	Create a dedicated connection between your corporate network and AWS to connect securely to both private networks and public services.	Manage Traffic
	AWS Transit Gateway	Acts as a highly available router between the Internet facing Hub VPC and all other (private) VPCs across accounts. Simplifies in-Region and inter-Region distributing encrypted traffic across the AWS network rather than the public Internet, as well as being hub for connecting to on-premise VPNs and Direct Connect connections.	Ensure Service Resiliency, Manage Traffic
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
Regional Delivery	AWS Global Infrastructure	In many cases designing a workload to span across multiple availability zones within a region will be suffient 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
	AWS Transit Gateway	Acts as a highly available router between the Internet facing Hub VPC and all other (private) VPCs across accounts. Simplifies in-Region and inter-Region distributing encrypted traffic across the AWS network rather than the public Internet, as well as being hub for connecting to on-premise VPNs and Direct Connect connections.	Ensure Service Resiliency, Manage Traffic
	AWS Snowball Edge	Store content locally with additional compute capability, both online and offline. Secure transfer of data at scale to and from AWS.	Protect Traffic Integrity, Ensure Service Resiliency
	Amazon Outposts	Extend AWS into your data center. Allows you to meet data sovereignty requirements and tight integration with on-premise applications.	Ensure Service Resiliency, Manage Traffic
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

Enterprise PEP Capabilities

TIC Security Capability	Service	How the service provides the capability	Objective
Security Orchestration, Automation, and Response	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
	AWS Step Functions	Create automated workflows, including manual approval steps, for security incident response.	Ensure Effective Response
	AWS Lambda	Automatically respond to events from AWS Config, AWS Step Functions and other AWS security tools.	Ensure Effective Response
	AWS Systems Manager	Orchestrate, automate, and respond with features such as Incident Manager, Automation, Change Manager, and Run Books.	Ensure Effective Response
Virtual Private Network	AWS Virtual Private Network	Allow direct access to a secure enclave or web application with a traditional VPN connection.	Manage Traffic, Protect Traffic Integrity
Application Container	Amazon AppStream 2.0	Provide secure, reliable, and scalable access to applications and non-persistent desktops from any location while storing data securely on AWS.	Manage Traffic, Ensure Service Resiliency
	Amazon WorkSpaces	Provide a secure, managed Desktop-as-a-Service (DaaS) to your end users for both Linux and Windows desktops while storing data on AWS.	Manage Traffic, Ensure Service Resiliency

Remote Desktop Access	Amazon WorkSpaces	Provide a secure, managed Desktop-as-a-Service (DaaS) to your end users for both Linux and Windows desktops while storing data on AWS.	Manage Traffic, Ensure Service Resiliency
	Amazon AppStream 2.0	Provide secure, reliable, and scalable access to applications and non-persistent desktops from any location while storing data securely on AWS.	Manage Traffic, Ensure Service Resiliency
	AWS Systems Manager Sessions Manager	Provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.	Manage Traffic, Ensure Service Resiliency

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 withResource Policies.	Manage Traffic, Protect Traffic Confidentiality
	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