Traffic Control

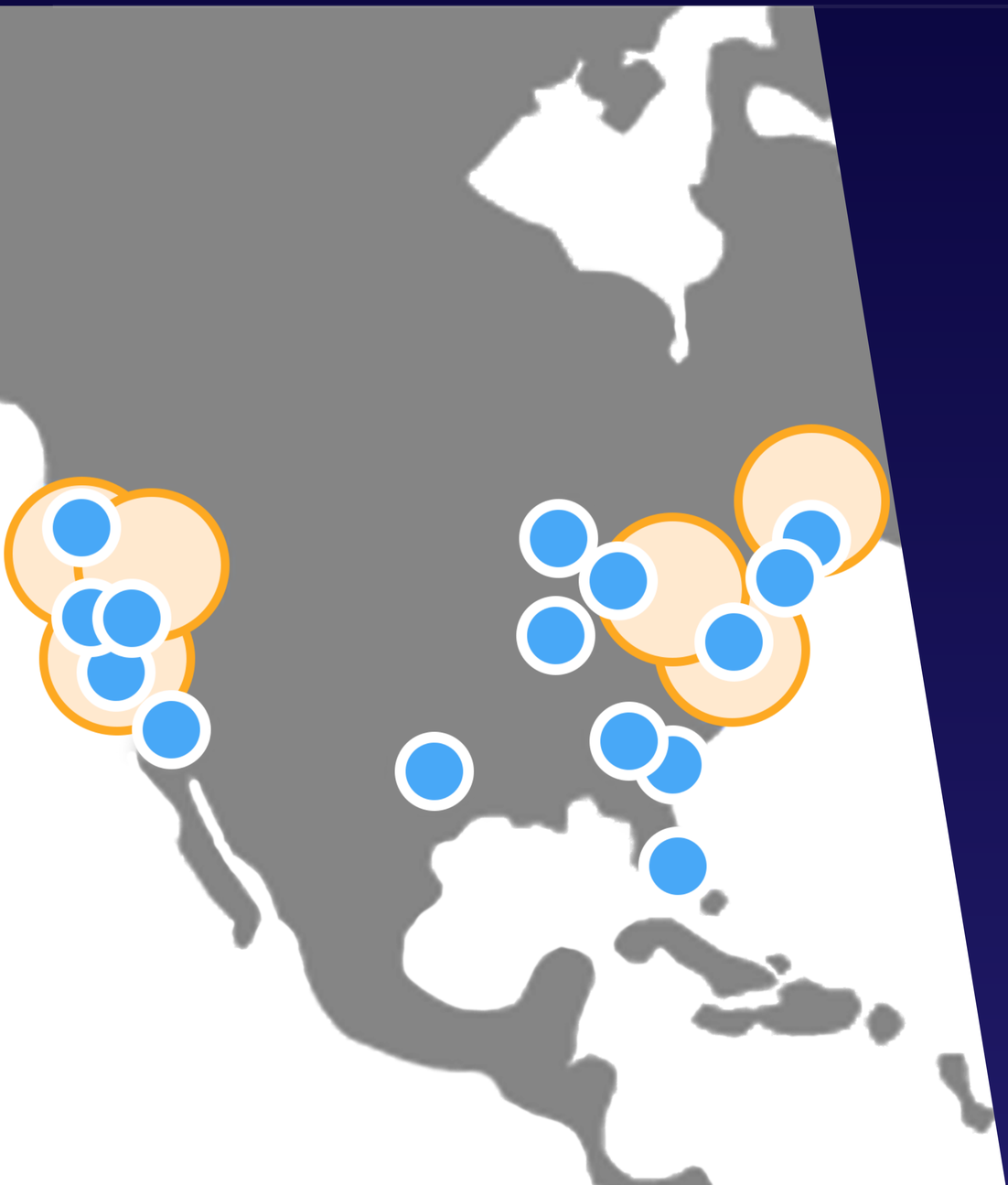
Steven Moran
TECHNICAL INSTRUCTOR

Let In What You Want, Keep Everything Else Out

Incoming network traffic can be filtered in several ways:

- Filtering by traffic properties.
  - What kind of traffic is allowed?
- Filtering by requestor identity.
  - Who is allowed to send requests?
- Filtering by destination is controlled by route tables.

Let In What You Want, Keep Everything Else Out



AWS provides a number of built-in and optional features and services residing at Edge Locations and Regions that can be used to identify both legitimate and unwanted traffic.

AWS Shield

- Managed DDoS protection service.
- Hosted at all CloudFront, Global Accelerator, and Route 53 edge locations.
- Covers approximately 96% of known layer 3 and 4 attacks.

AWS Shield – Pricing Tiers

- Standard is automatically provided to all AWS customers at no charge.

- Advanced is a paid service that provides:
  - Additional protection for select services
  - Detailed monitoring
  - WAF at no charge
  - 24×7 DDoS response team
  - EDoS (economic denial of sustainability) coverage

AWS Web Application Firewall (WAF)

- Allow, deny, or count HTTP/HTTPS requests using ACLs.
- Applicable to API Gateway, CloudFront, and Application Load Balancer.
- New version of AWS WAF released in November 2019.
  - All WAF resources created beforehand are “AWS WAF Classic”.
  - Resources for the new version are “AWS WAF”.
  - ACLs can be migrated from classic to current.

AWS Web Application Firewall (WAF) – ACL Components

- **Conditions** are used to identify request content of interest:
  - Cross-site scripting
  - Country of origin
  - IP address
  - Size of request properties
  - SQL queries
  - String/regex
- Each condition contains one or more filters.
- Multiple condition filters are OR-ed.

AWS Web Application Firewall (WAF) – ACL Components

- **Rules** contain one or more conditions.
  - Specify if traffic should match or not match condition filters.
  - Multiple conditions are AND-ed.

- Rules can be *normal* or *rate-based*.

AWS Web Application Firewall (WAF) – ACL Components

- Customers may purchase **managed rule sets** to be used alongside customer-created rules.

AWS Web Application Firewall (WAF) – ACL Components

- **ACL**s contain one or more rules.
  - Rules are set to either allow, deny, or count matching requests.
  - Multiple rules are processed in the order listed in the ACL.
  - Default action applies to requests that match no rules.
- Rate-Based rules only apply their action after a set number of requests are received
  - Limits may be for all traffic or bound to conditions
  - Request counts for limits are reset every 5 minutes

AWS Web Application Firewall (WAF) – ACL Components

- ACLs may be associated with ALBs, API Gateway APIs, and CloudFront distributions.
- While an ACL remains associated, it may only be further associated with other objects of the same type.
- ALB and API associations become region-restricted.

AWS Web Application Firewall (WAF) – Pricing

- Per ACL, per month.
- Per Rule, per month.
- Per 1 million requests.
- Managed rule prices are set by the seller.

AWS Web Application Firewall (WAF) – ACL Quota Limits

- Per account, per region:
  - 50 ACLs
  - 100 rules
  - 5 rate-based rules
  - 100 of each condition type *except*...
  - 10 regex conditions (cannot be increased)
- Maximum of 10 conditions per rule.
- Maximum of 10 rules per ACL.

Route 53

- Public-hosted zones are...public.
- Use private-hosted zones for internal use.
- Geolocation routing policies can deflect name–resolution requests from selected areas.

CloudFront

- Content in CF distributions are inherently public.
- Ensure all traffic is sent to CF distribution and not to origin data source.
  - Resolve traffic to distribution DNS name.
  - S3 bucket origins - restrict traffic using CF Origin Access Identity.
  - Custom origins - only accept requests that include signed URLs, cookies, or custom headers added by CF distribution.

CloudFront

- CF distributions support geo restriction.
- Choose to either whitelist or blacklist countries.
- Optional custom error message for blocked requests.

Simple Storage Service

- Avoid enabling public access.
- Use the correct type of authentication for your authorizations:
  - IAM permissions require IAM authentication
  - Bucket policies and ACLs do not require IAM authentication
- Require signed URLs.
- Use bucket policy conditions.

Simple Storage Service

- S3 service is natively accessed via the internet.
- VPC gateway endpoints allow access from VPCs in the same region.
  - Access can be restricted by both S3 bucket policies and gateway endpoint policies.

Simple Storage Service

- S3 Access Points allow the creation of customized access points for an S3 bucket.
- Each access point:
  - Has a unique host name
  - Has distinct permissions and network controls
  - Can be limited to VPCs
- Can be managed by AWS Organizations SCPs.

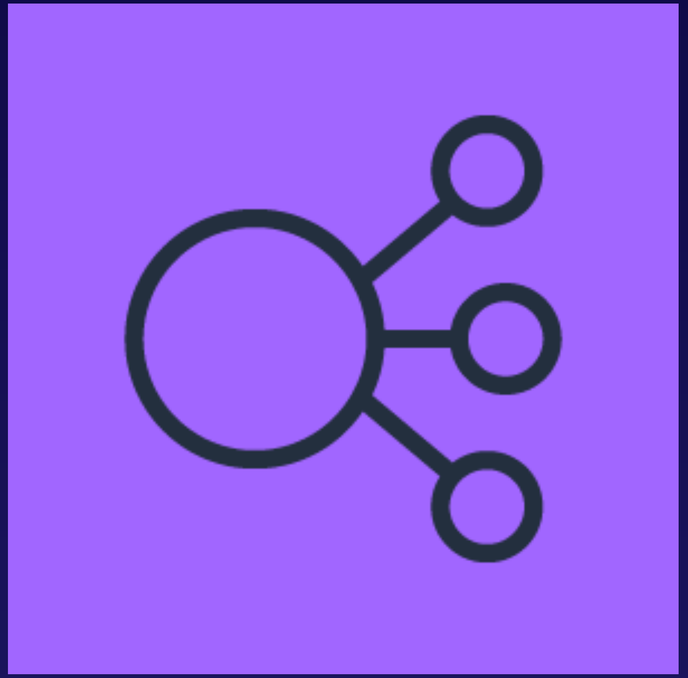
VPC NACLs and Security Groups

- NACLs:
  - Applied to subnets
  - Only one per subnet
  - Rules processed in sequence
  - Have explicit deny
  - Only recognize IP traffic properties
  - Stateless

- Security Groups
  - Applied to ENIs
  - Up to five per ENI
  - Rules processed collectively
  - No explicit deny
  - Can identify source and destination security groups
  - Stateful

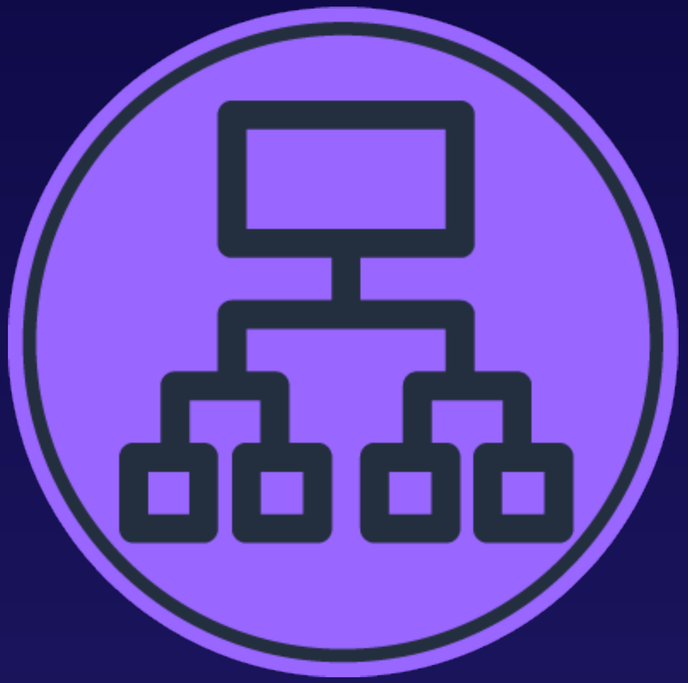
Elastic Load Balancer

- Only accepts traffic matching a configured listener.
- Protected by VPC security groups.

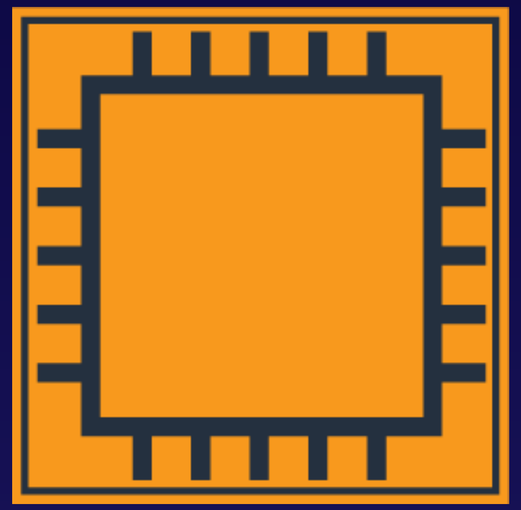


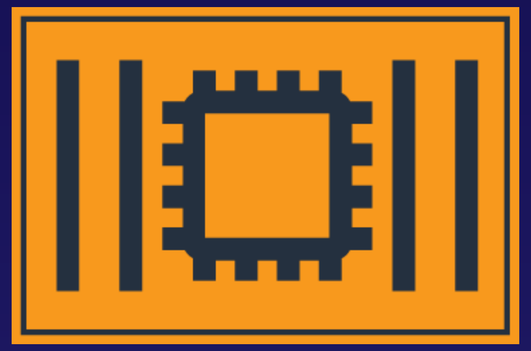
Application Load Balancer Built-in Authentication

- Authentication can be offloaded from the application to ALB.
- Traffic matching a listener rule is sent to a configured identity provider (IdP).
- Supported methods include:
  - OIDC-compliant IdPs
  - Well-known social IdPs
  - Amazon Cognito user pools
  - SAML
  - LDAP
  - Microsoft AD



EC2 and Container Instances





- Limited only by what the instance OS can support.
- May provide features that comparable, AWS-managed services do not.
- Services hosted on instances are the customer's responsibility to maintain.

Fast Takeaways

Using AWS-managed services shifts responsibility towards AWS.

Filtering by authentication may involve connection to external services.

Eliminating unwanted traffic earlier in the cycle reduces workload on your end application.