AWS re:Invent

NET413-R

Elastic Load Balancing: Best practices for securing your applications

Sathya Ramaseshan
Senior Product Manager
AWS Load Balancing
Amazon Web Services

David Ward
General Manager
AWS Load Balancing
Amazon Web Services

Related breakouts

NET407-R Get the most from Elastic Load Balancing for different workloads

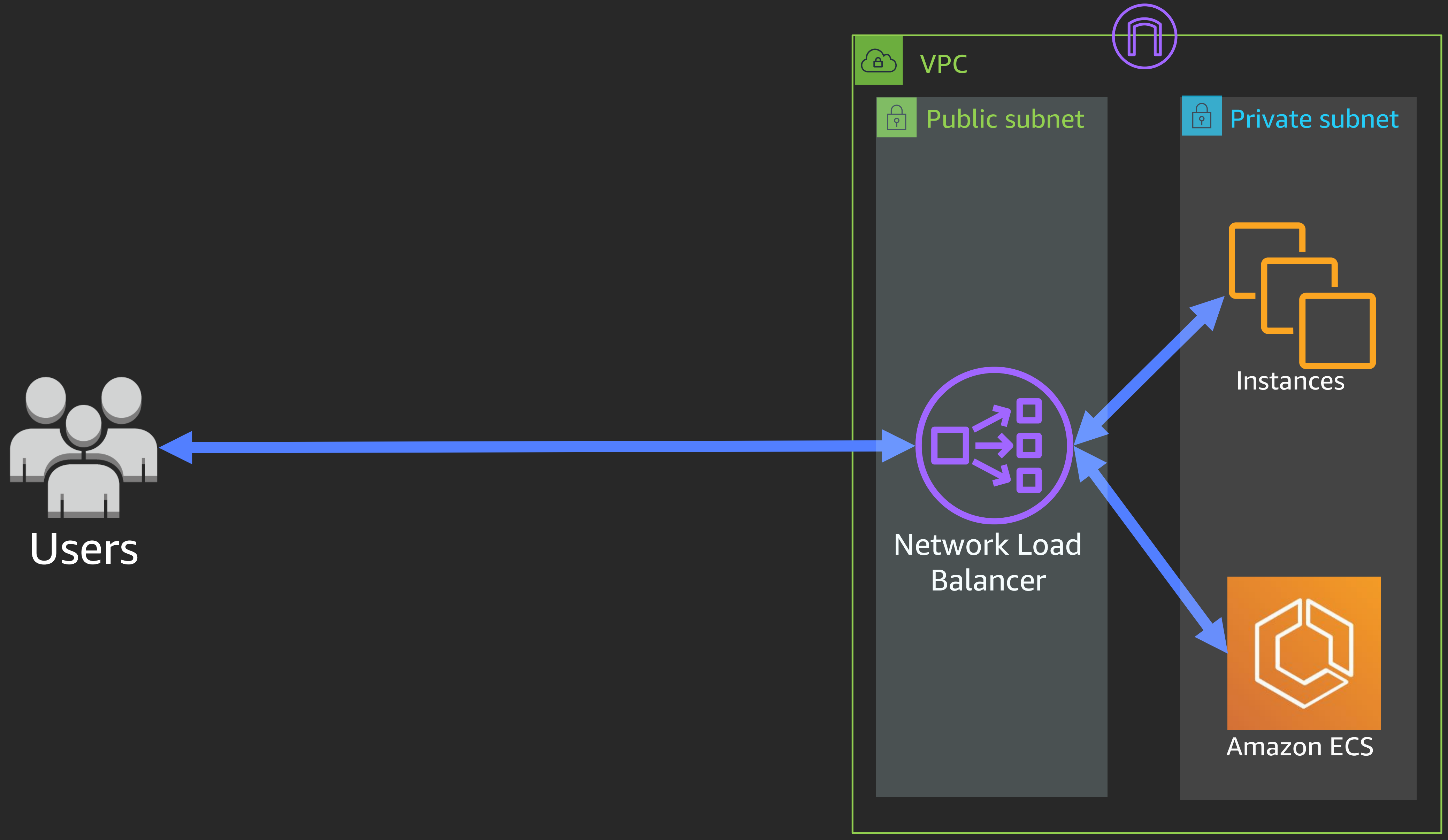
- Tuesday, Dec 3, 7:00 PM - 8:00 PM – Aria, Level 1 West, Bristlecone 9 Red
- Wednesday, Dec 4, 8:30 AM - 9:30 AM – Bellagio, Grand Ballroom 5 Black

NET203-L Leadership session: Networking

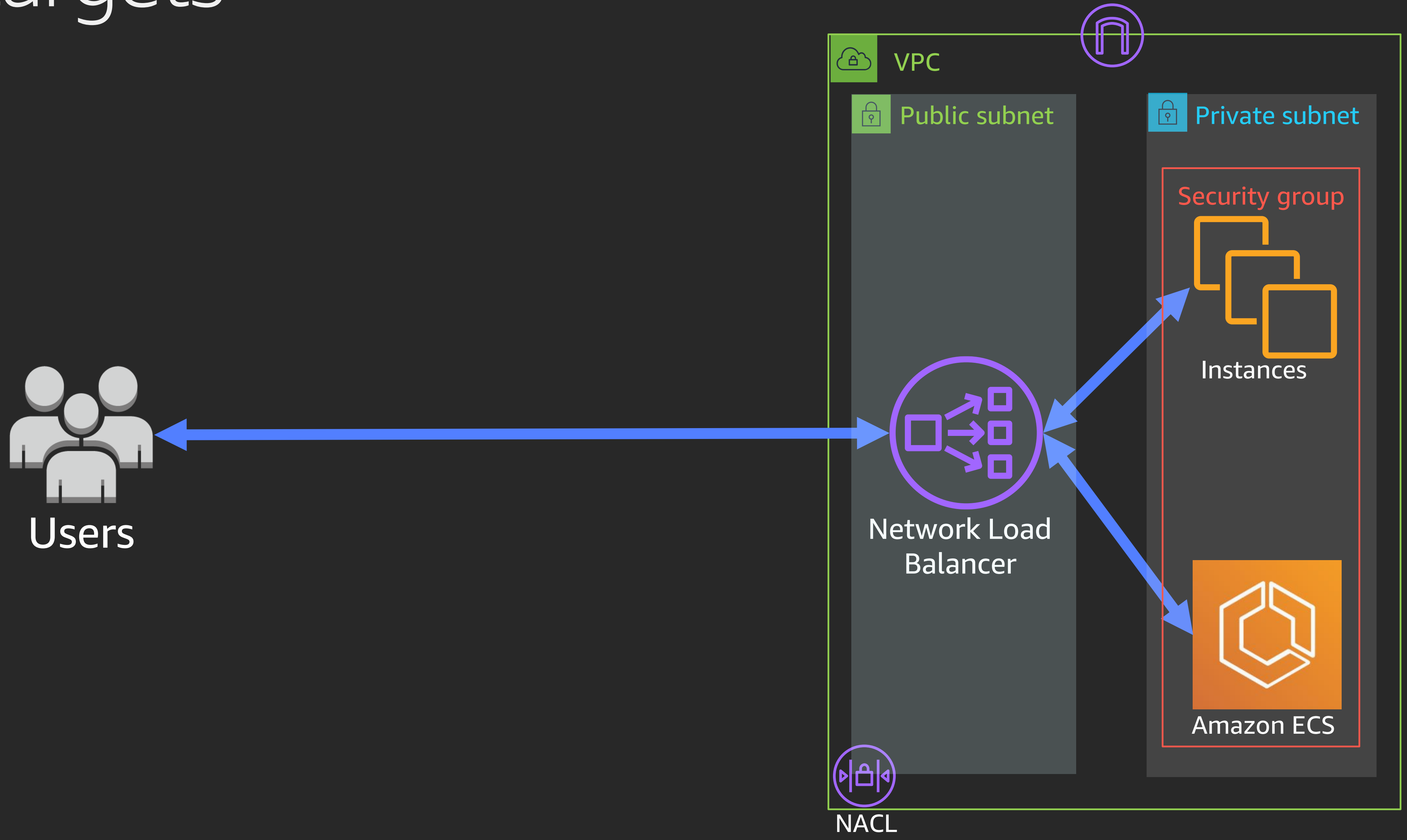
- Wednesday, Dec 4, 11:30 AM - 12:30 PM – MGM, Level 3, Premier Ballroom 309

Building defense in depth using NLB for your applications

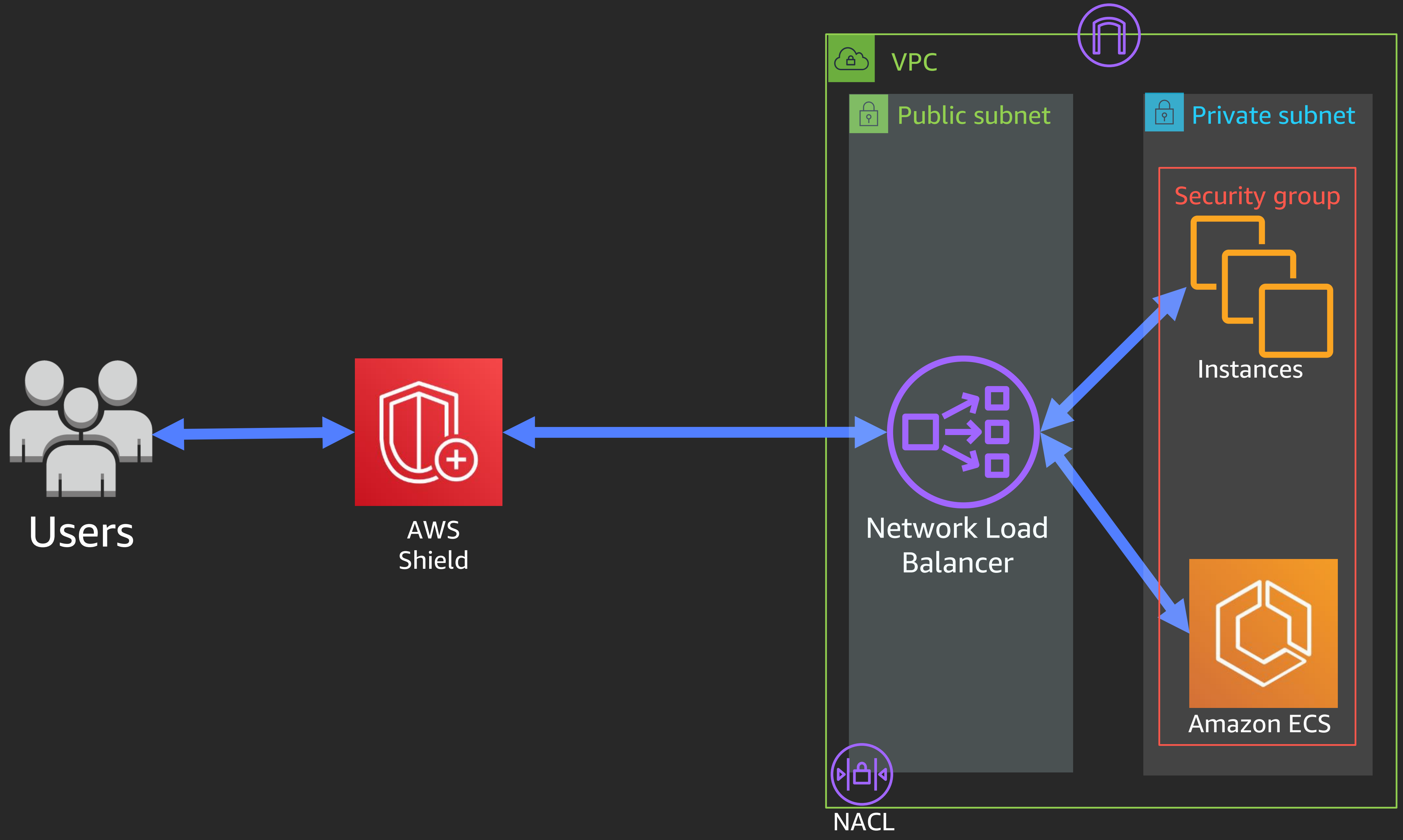
Build secure applications with NLB



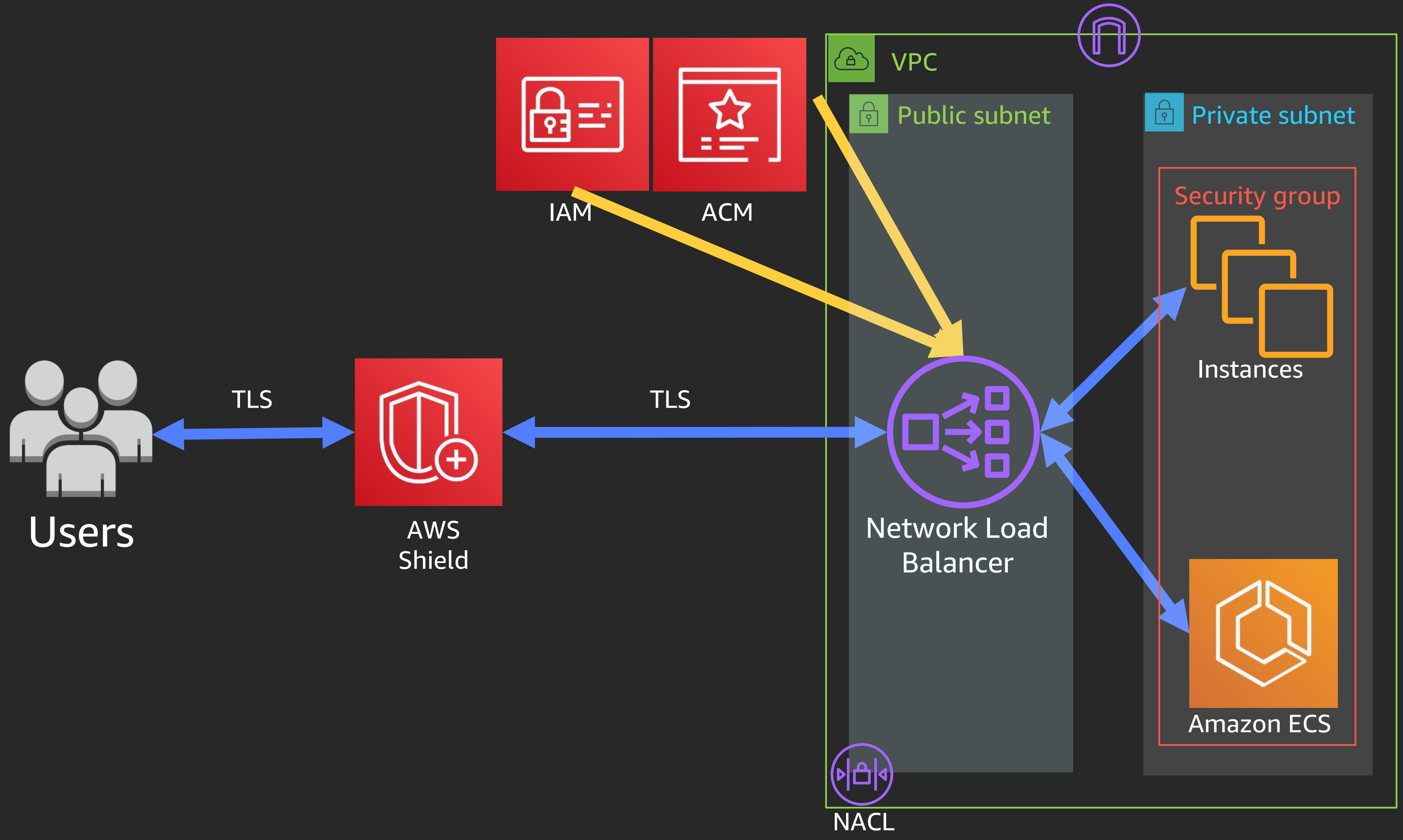
Control traffic in/out of your load balancer and targets



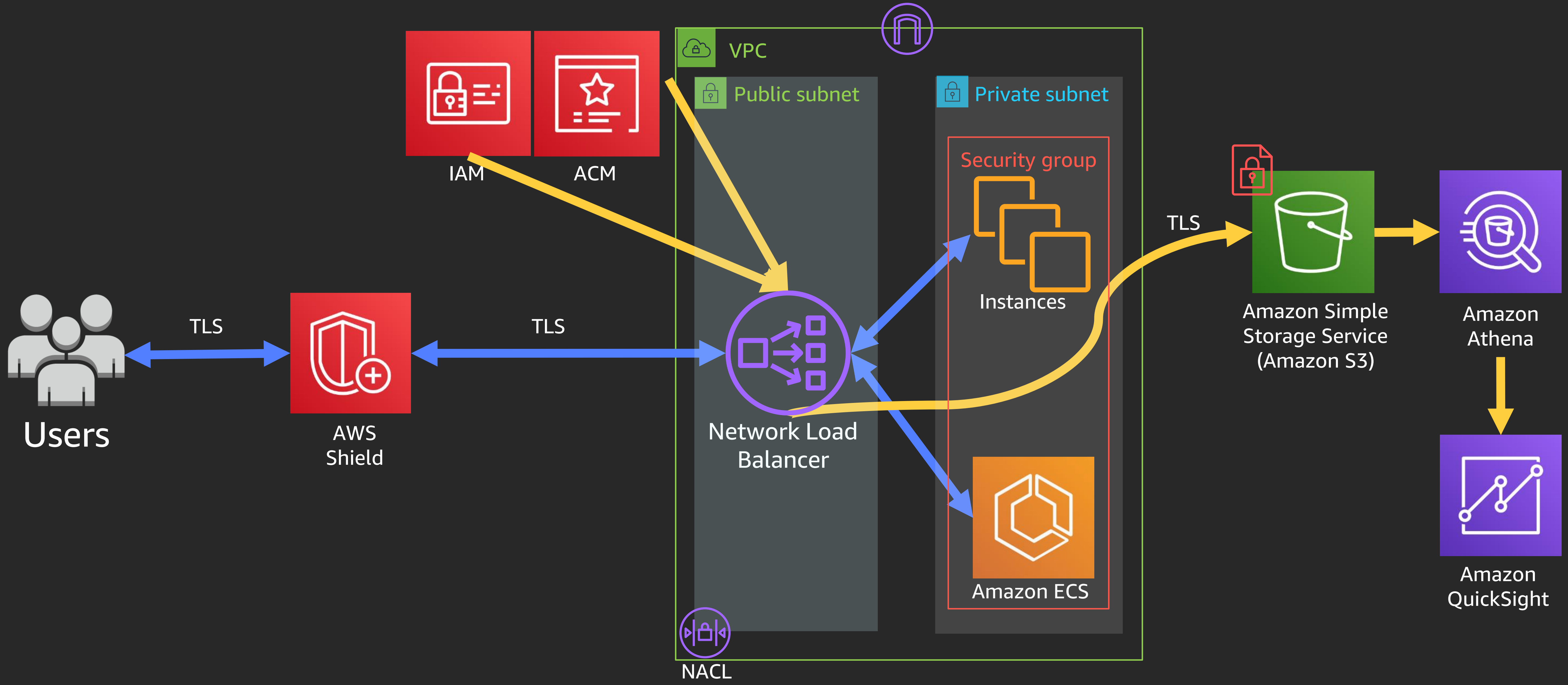
Enable layer 3/4 protection seamlessly



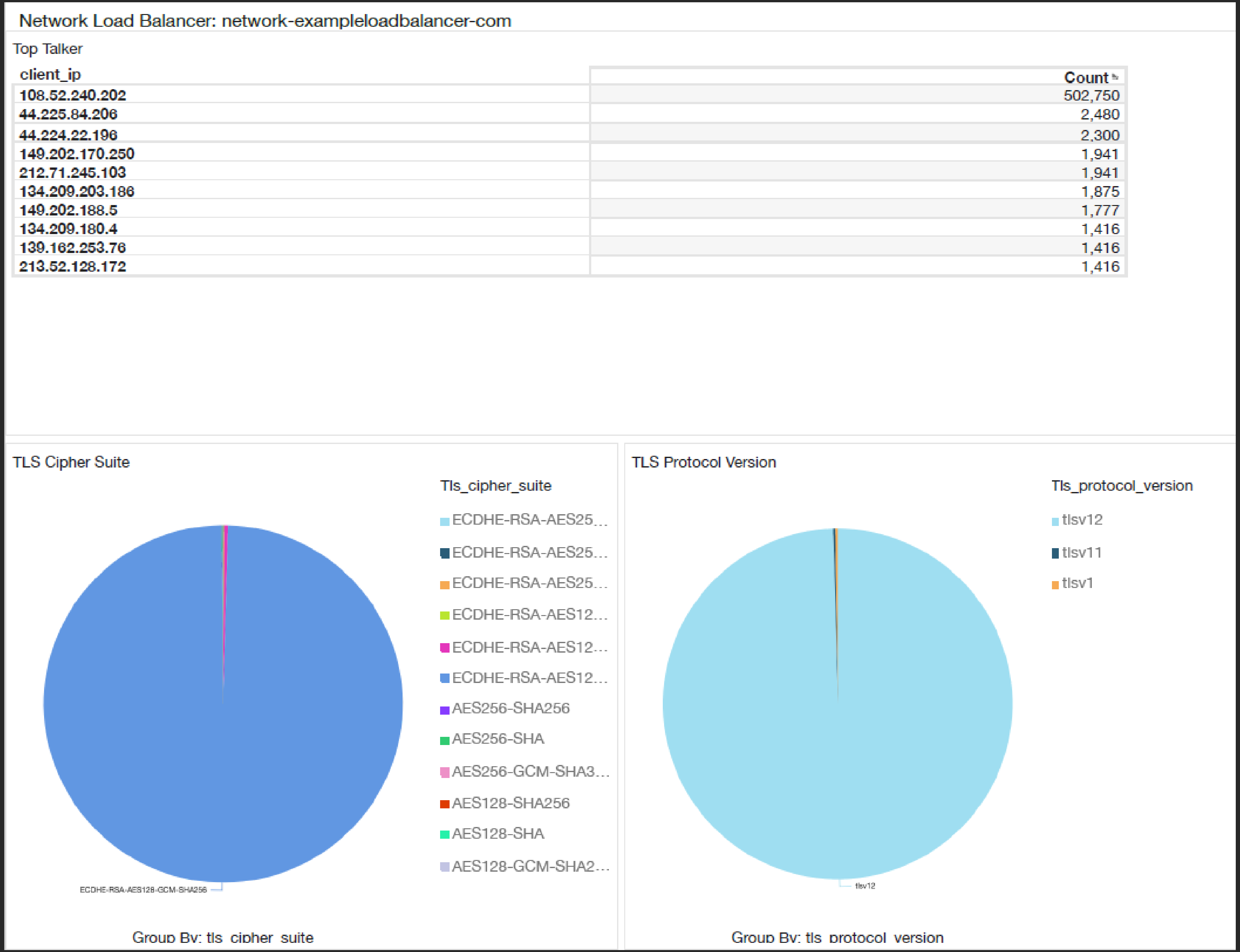
Offload TLS to encrypt traffic to your application



Analyze your traffic patterns using access logs



Example TLS Access logs dashboard from QuickSight



Network Load Balancer: network-exampleloadbalancer-com

Top Talker

client_ip	Count
108.52.240.202	502,750
44.225.84.206	2,480
44.224.22.196	2,300
149.202.170.250	1,941
212.71.245.103	1,941
134.209.203.186	1,875
149.202.188.5	1,777
134.209.180.4	1,416
139.162.253.76	1,416
213.52.128.172	1,416

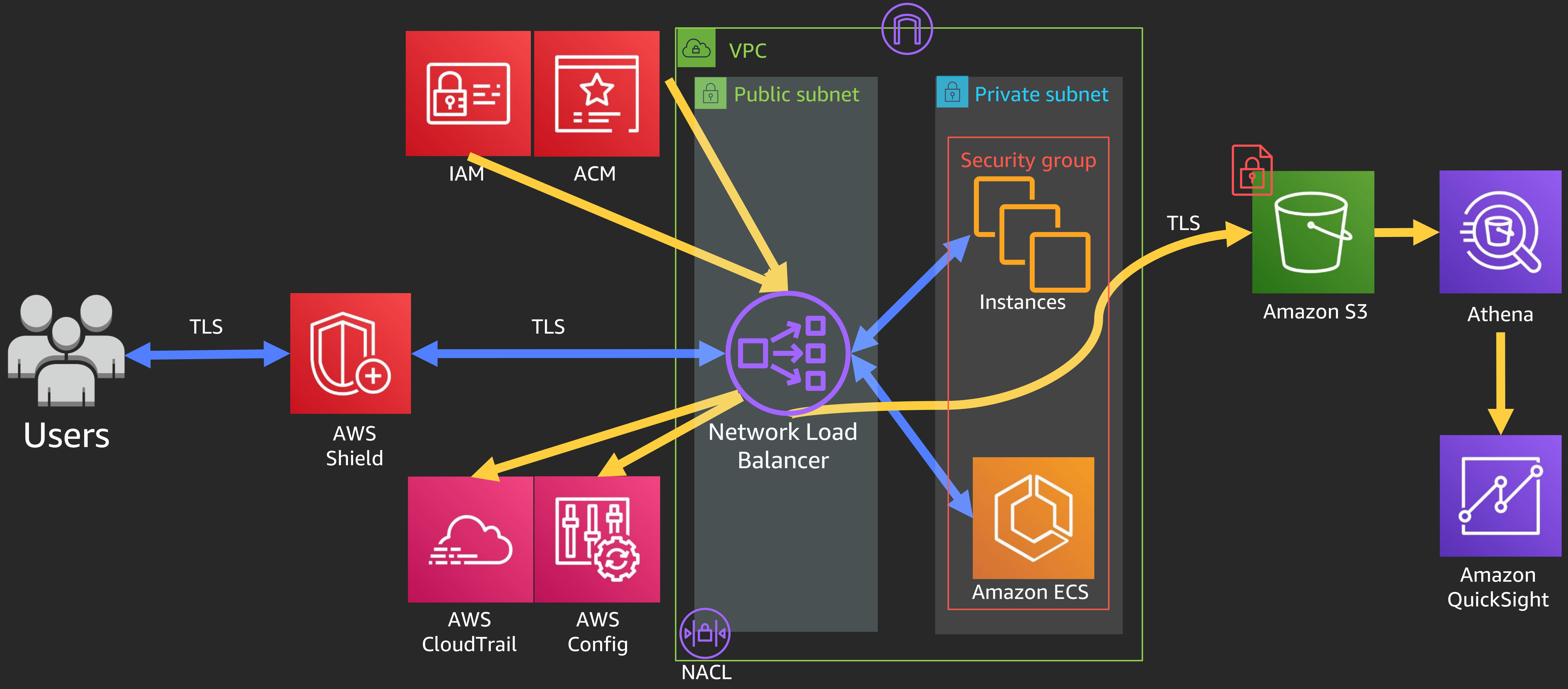
TLS Cipher Suite

Group By: tls_cipher_suite

TLS Protocol Version

Group By: tls_protocol_version

Meet your application's compliance requirements

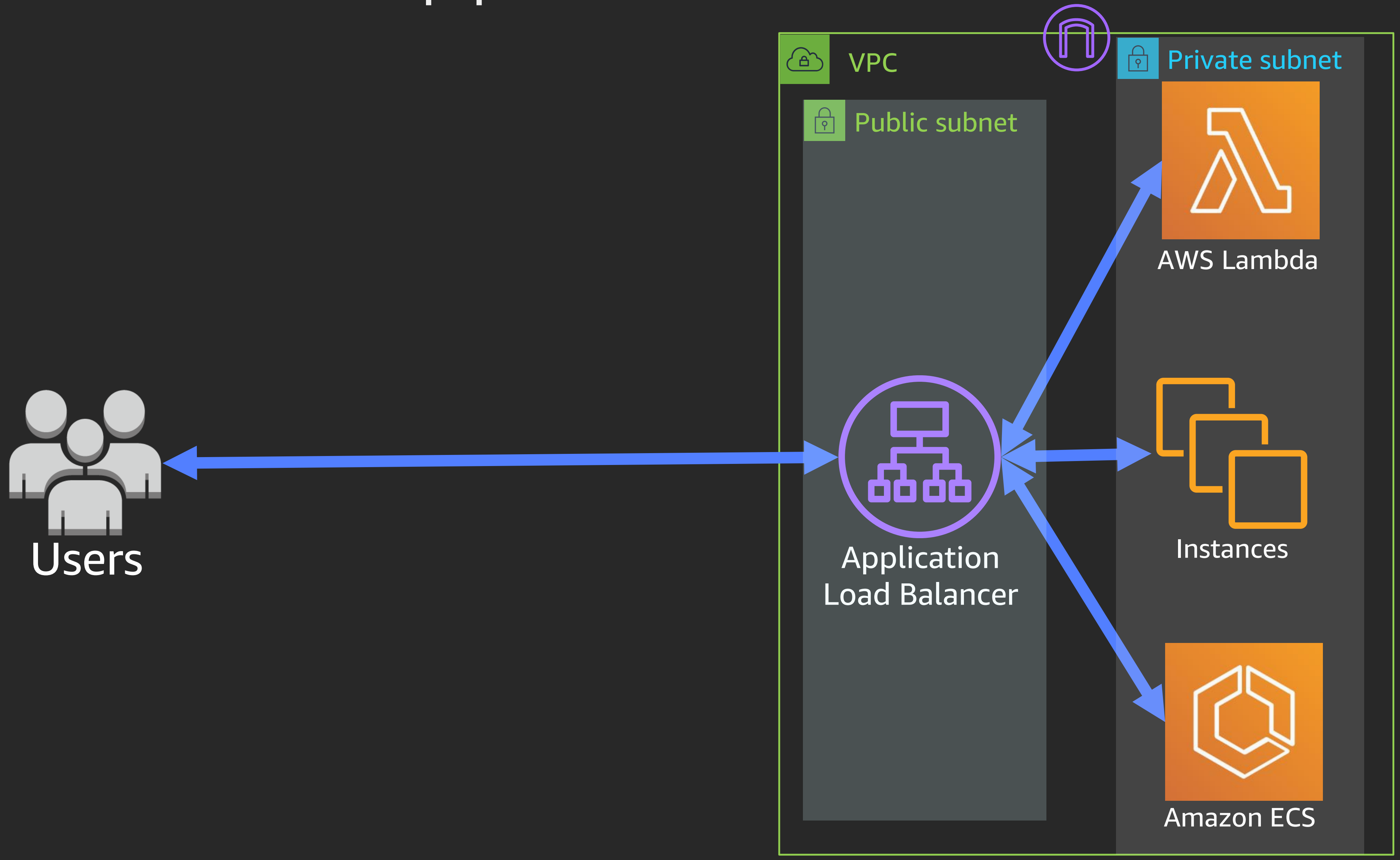


Building defense in depth using ALB for your applications

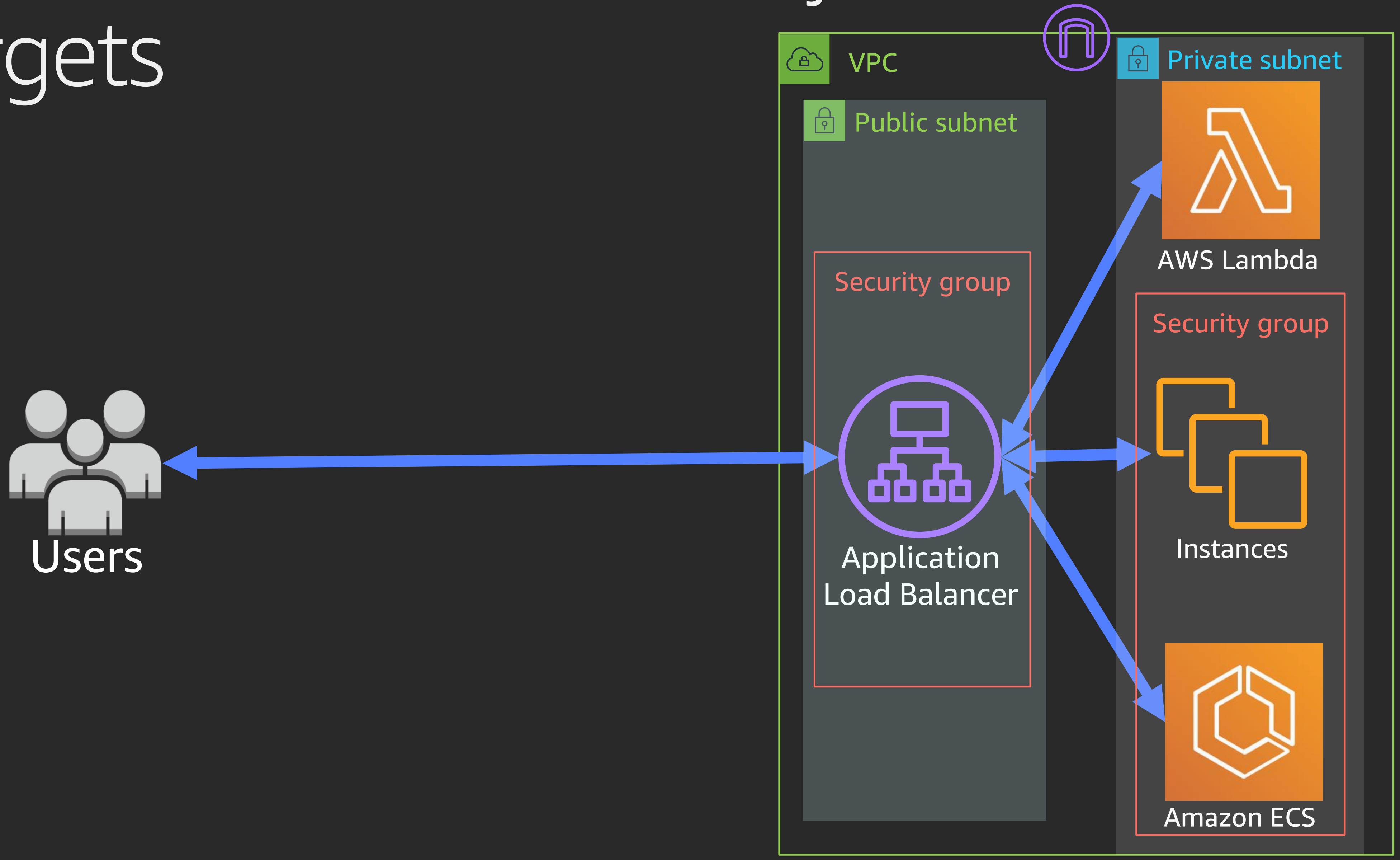
AWS re:Invent

aws

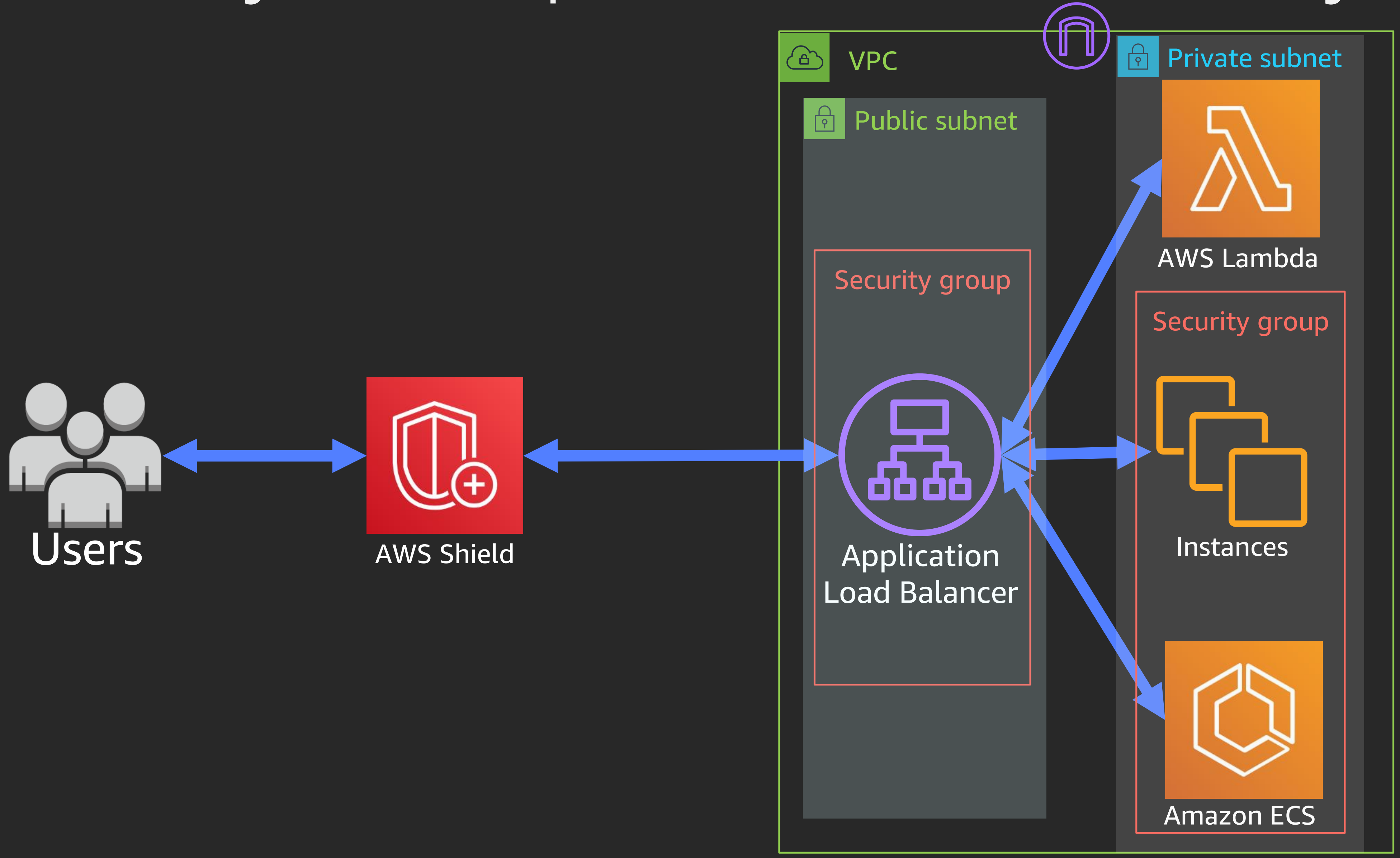
Build secure applications with ALB



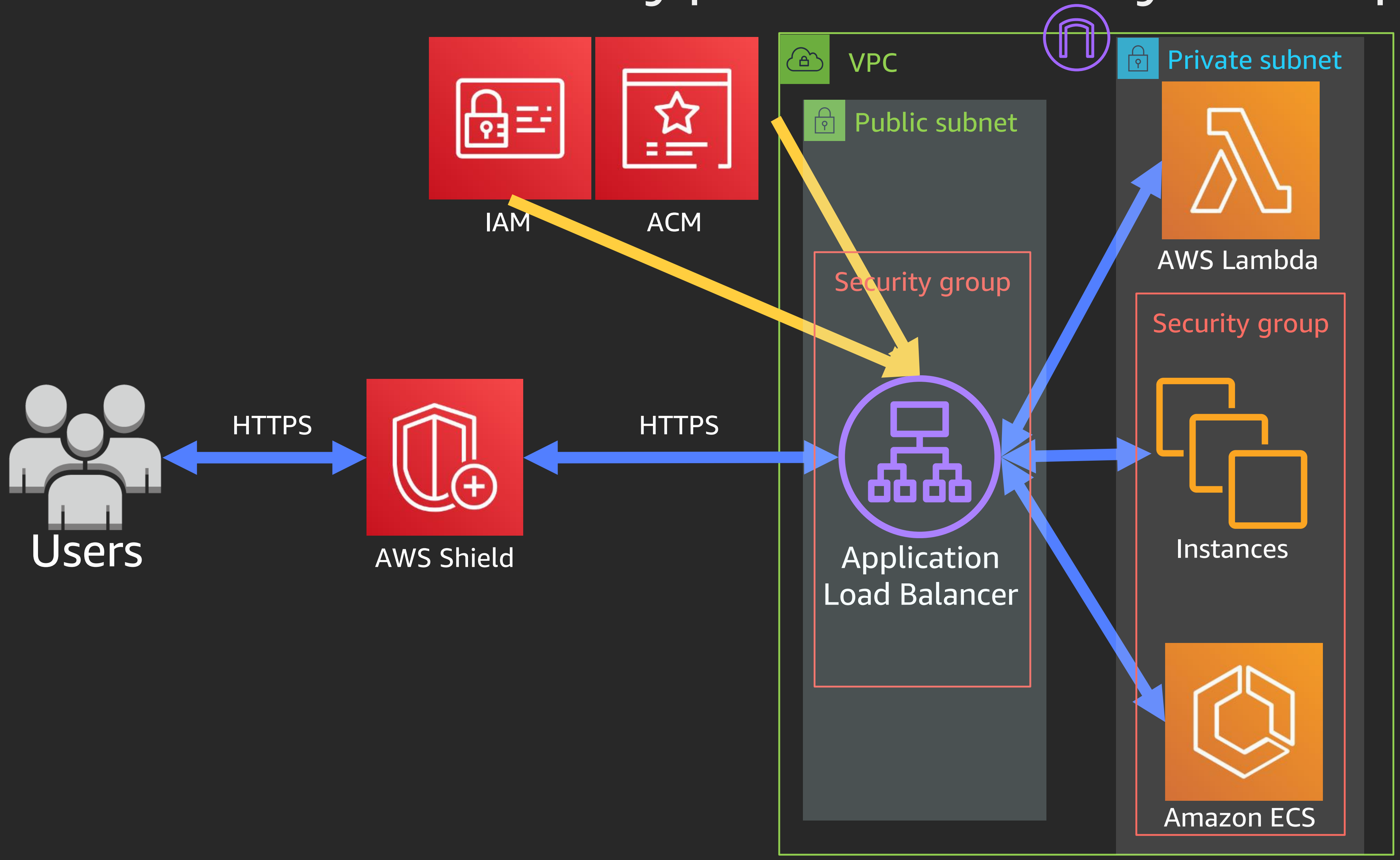
Control traffic in/out of your load balancer and targets



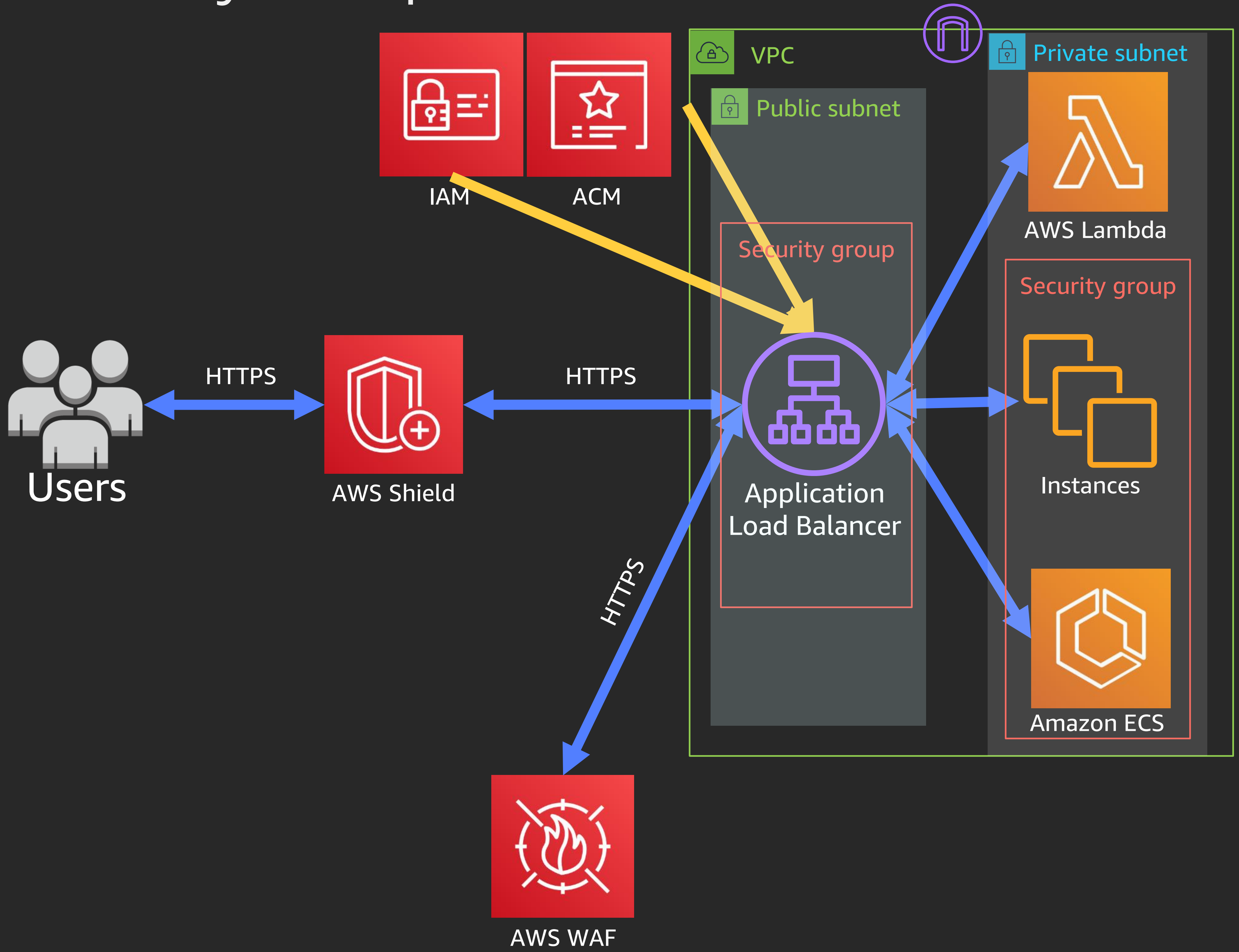
Enable layer 3/4 protection seamlessly



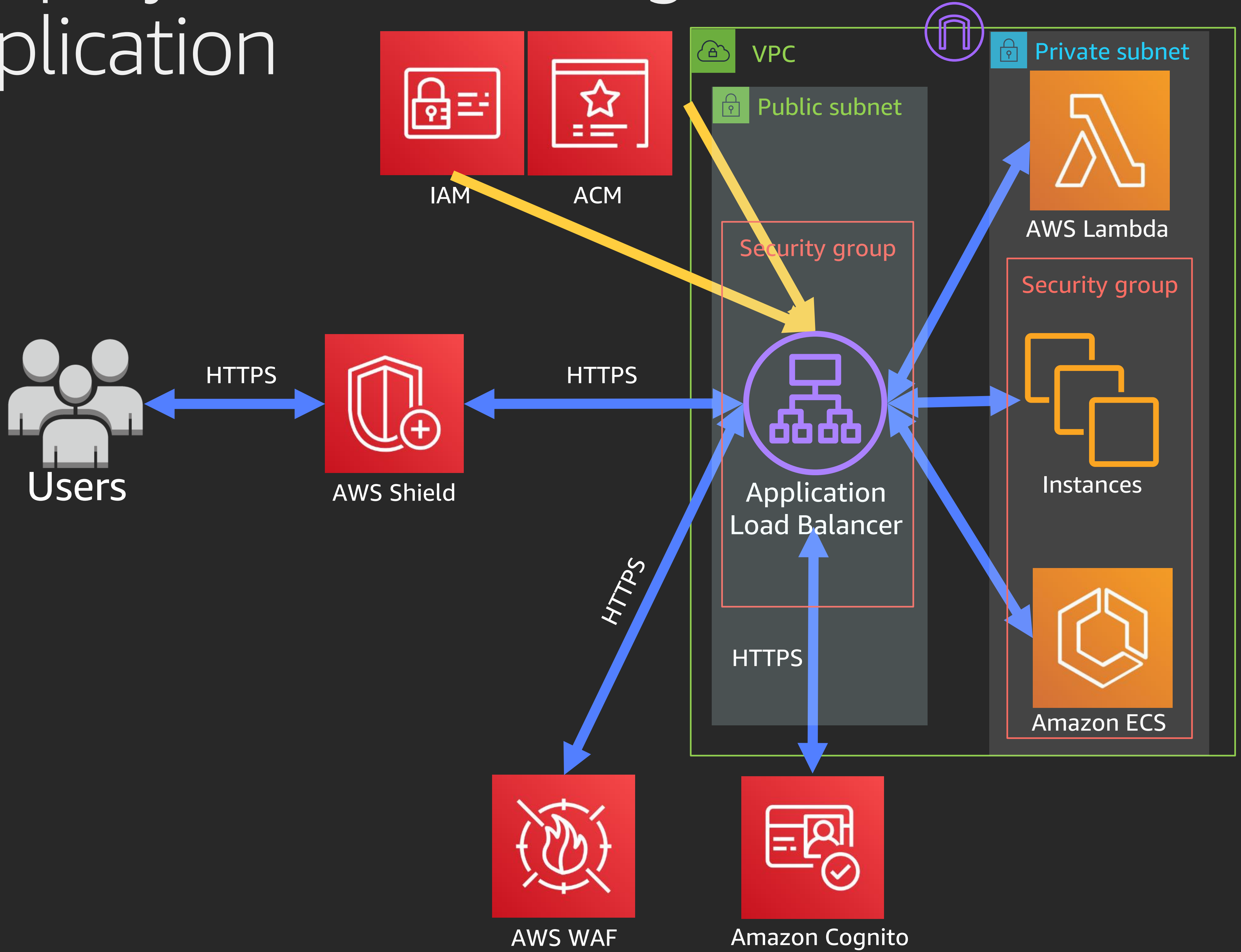
Offload TLS to encrypt traffic to your application



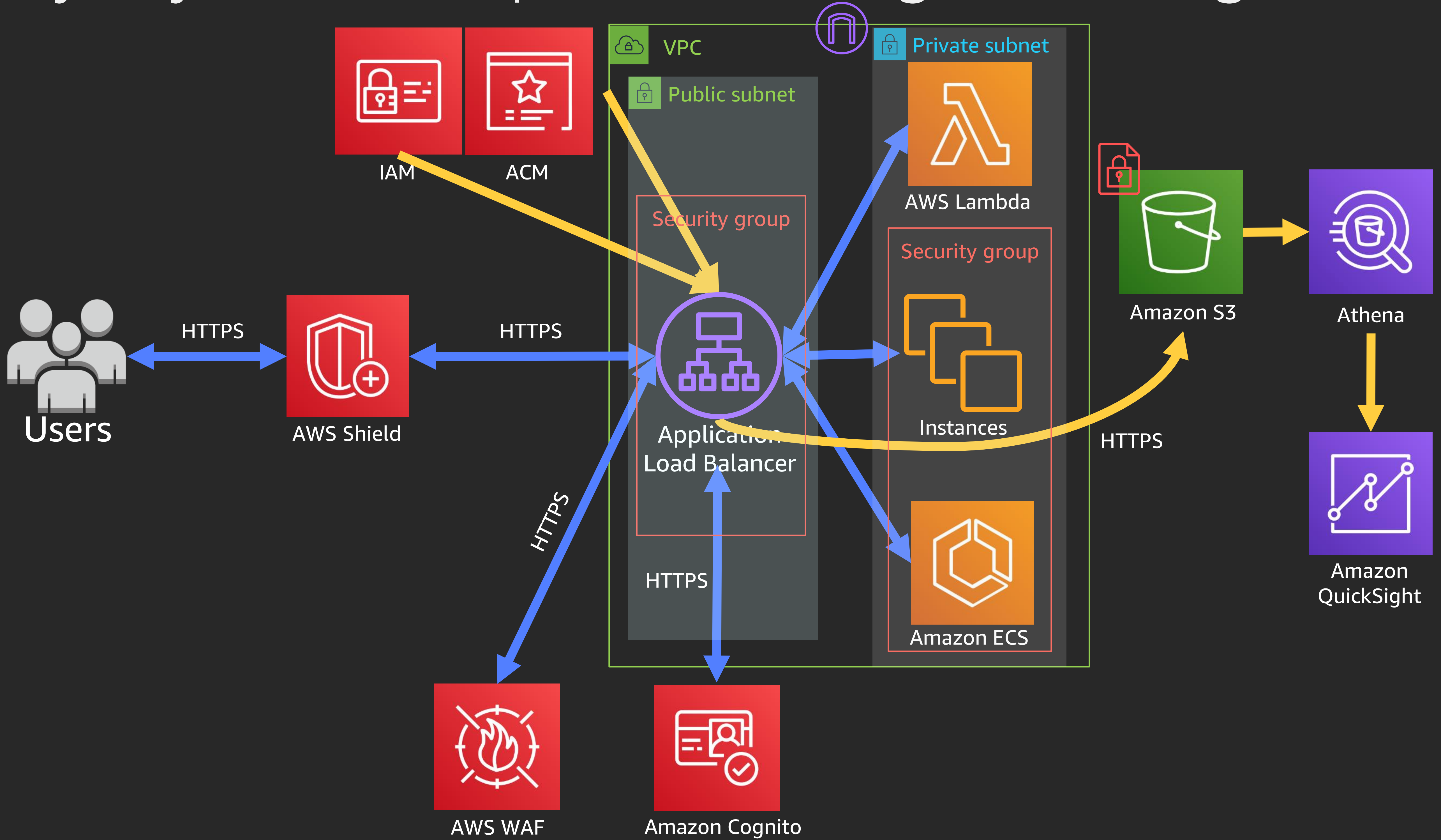
Enable layer 7 protection with AWS WAF



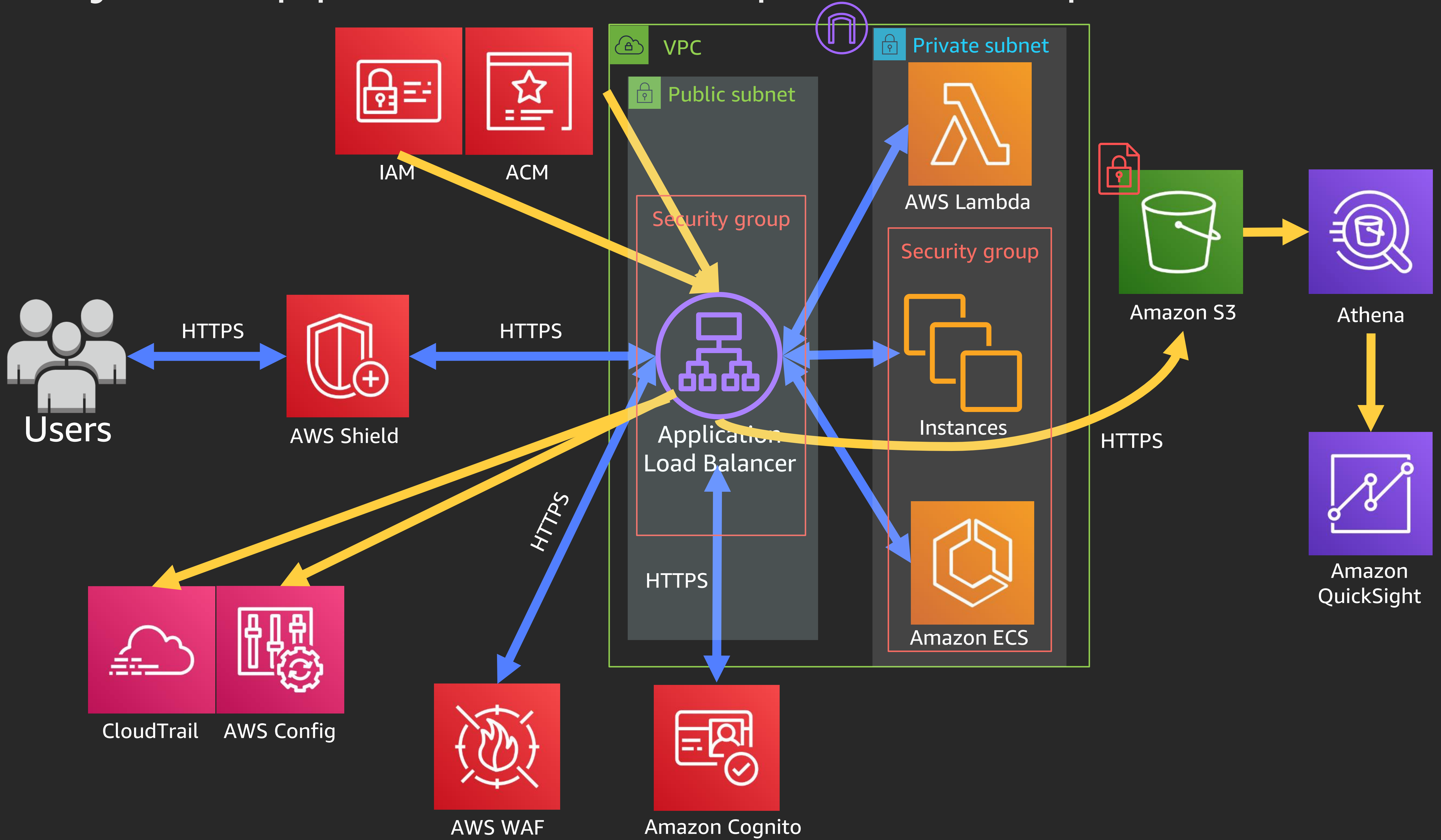
Simplify authenticating users' access to your application



Analyze your traffic patterns using access logs



Meet your application's compliance requirements



TLS on NLB/ALB

TLS features on NLB/ALB

Features	NLB	ALB
Source IP preservation	Yes	Yes – XFF header
Predefined policies	Yes	Yes
SNI	Yes	Yes
ALPN	No	Yes – Client to ALB
Session resumption	Tickets (Regional)	Tickets and session ID
RSA Certs > 2K	No	Yes
EC Certs	No	Yes – IAM only
TLS to target	Yes	Yes

Considerations to determine TLS settings

Types of clients

Types of targets

Compliance needs

Number of applications behind load balancer

Simplifying user login with ALB authentication

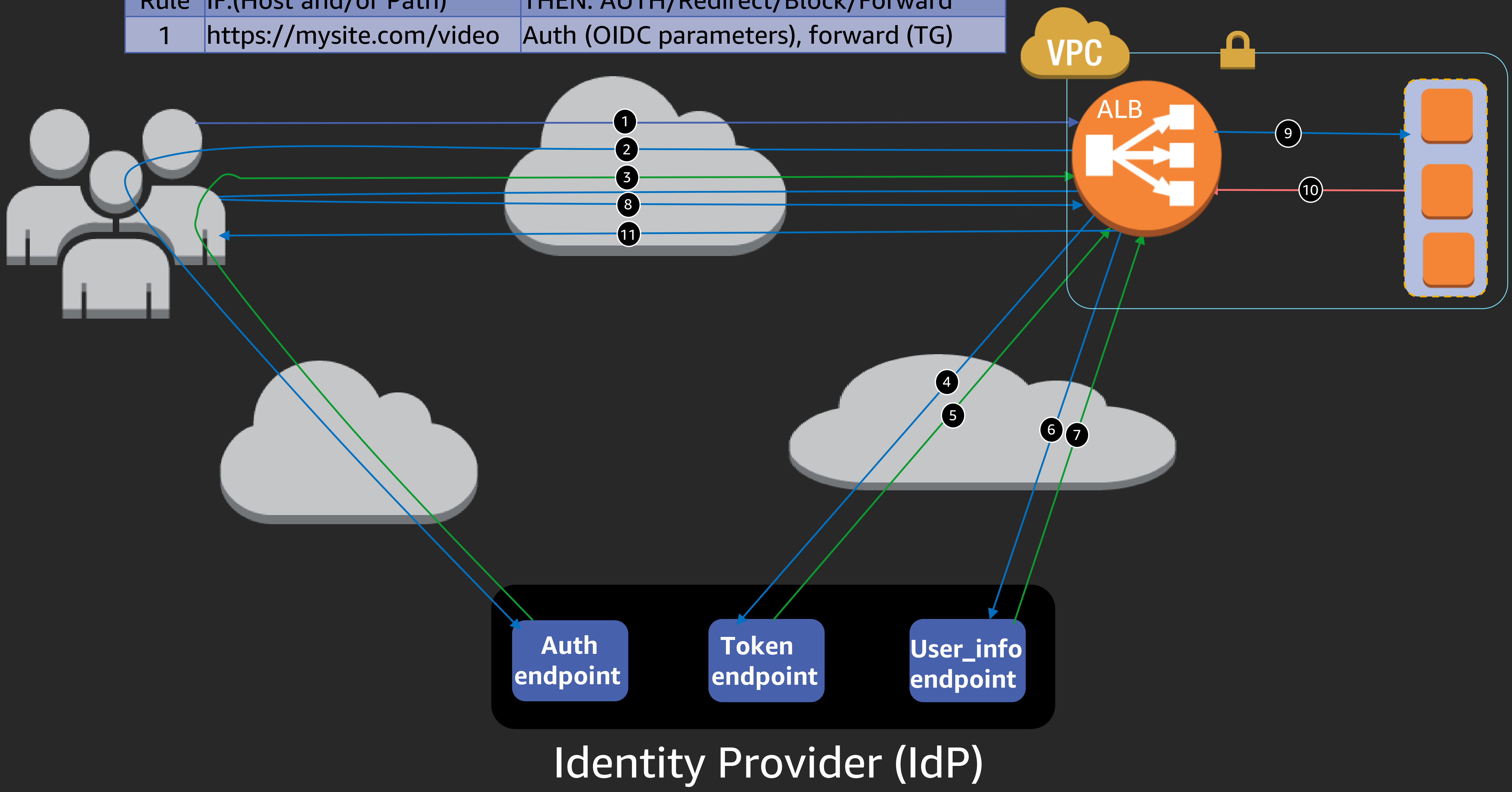
Authentication in ALB

Secure authentication and single sign-on experience across your applications

- ALB implements the role of a “Relying Party" as defined by the OpenID Connect spec
- Support for authorization code grant flow
- Native integration with any OIDC supported IdP
- Seamless integration with Amazon Cognito
  - Authenticate with corporate identities using SAML, LDAP, Microsoft AD, or OIDC
  - Authenticate with federated identities based on public IDPs (Facebook, Google, Amazon, Okta)
- Implemented through listener rules that simplifies authorization in the backends

Authentication workflow in ALB

Rule	IF:(Host and/or Path)	THEN: AUTH/Redirect/Block/Forward
1	https://mysite.com/video	Auth (OIDC parameters), forward (TG)



1) User sends HTTPS request to a website hosted behind Auth enabled ALB
2) ALB checks for Auth session cookie and redirects the user to IdP if it is missing
3) After authenticating with IdP, user is redirected back to ALB with authorization CODE
4) ALB authenticates the CODE and sends to token endpoint
5) Token endpoint exchanges CODE for ID token, Access Token
6) ALB sends Access Token to user_info endpoint
7) User_info endpoint exchanges Access Token for user claims
8) ALB redirects the user with AWSELBAuthSessionCookie to original URI
9) ALB validates cookie and forwards user info to targets in the "X-AMZN-OIDC-*" HTTP headers set
10) Target sends response back to ALB
11) ALB sends final response to user

Learn networking with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate networking skills

Free digital courses cover topics related to networking and content delivery, including Introduction to Amazon CloudFront and Introduction to Amazon VPC

Validate expertise with the
AWS Certified Advanced Networking - Specialty exam

Visit aws.amazon.com/training/paths-specialty

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.

Appendix

TLS on NLB/ALB

TLS on ALB/NLB

Makes client-to-server communication thru load balancer secure by default

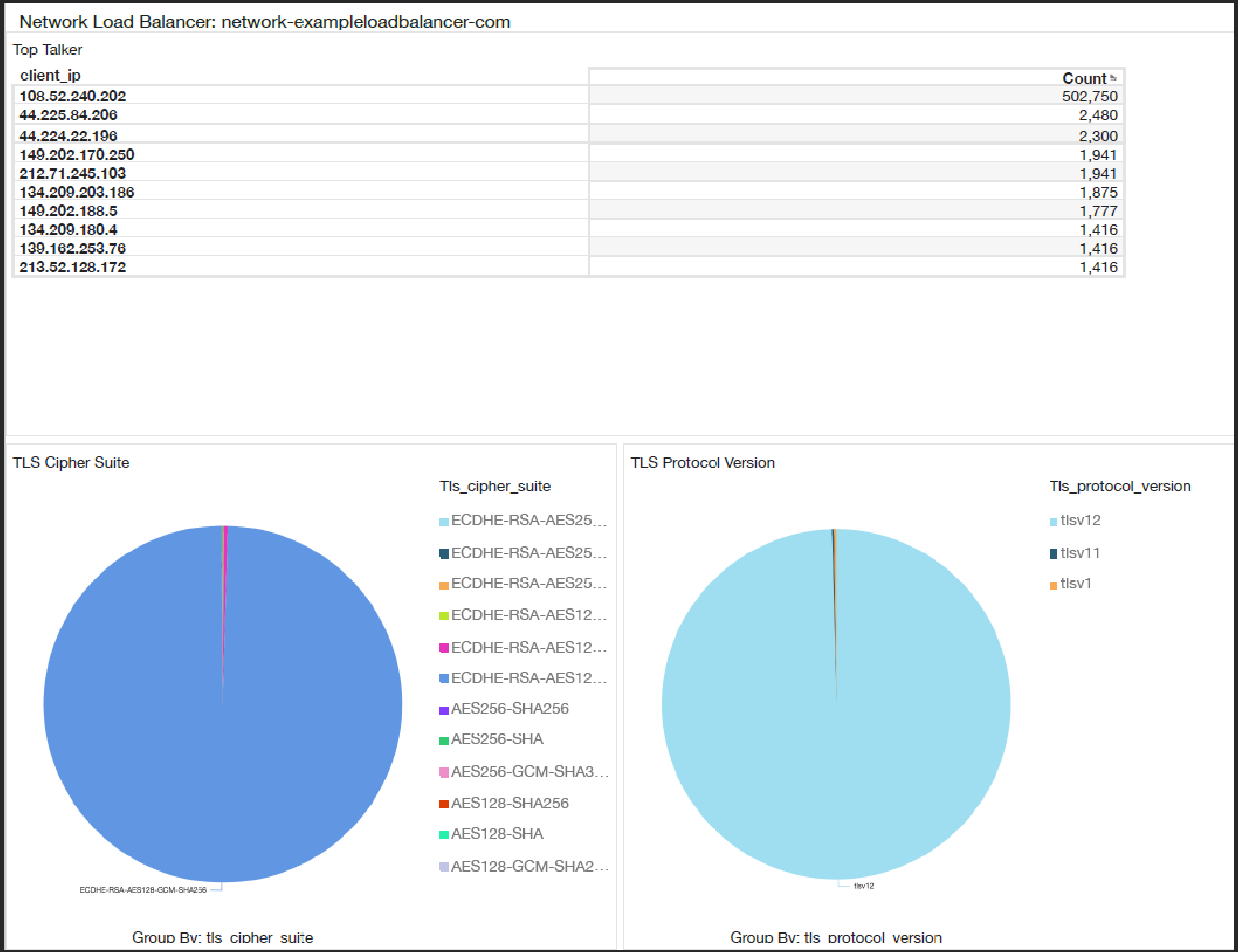
Application data is encrypted in transit

Improved PCI compliance

Fleets patched to handle zero day vulnerabilities

Visibility through metrics and access logs

Example TLS Access logs dashboard from QuickSight



Network Load Balancer: network-exampleloadbalancer-com

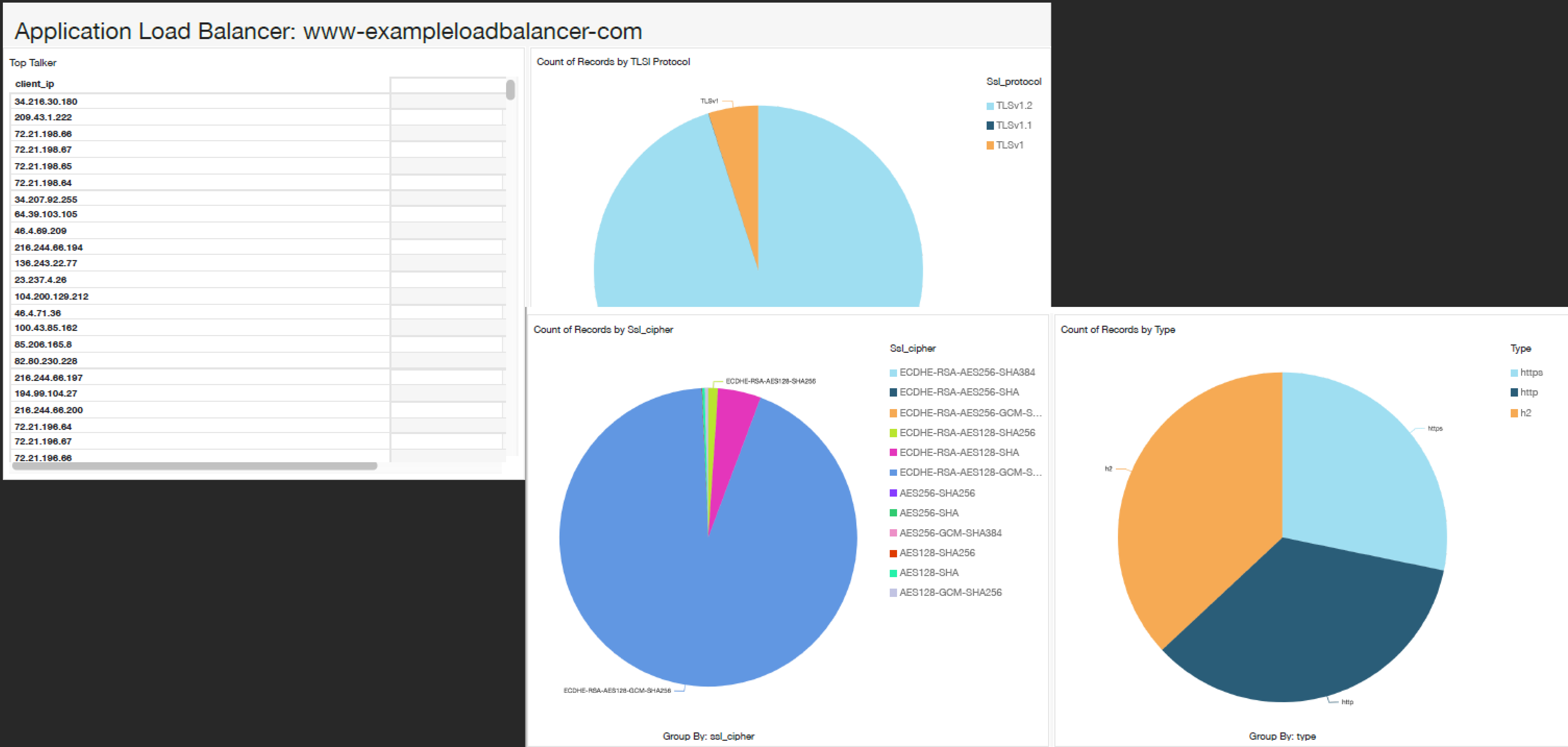
Top Talker

client_ip	Count
108.52.240.202	502,750
44.225.84.206	2,480
44.224.22.196	2,300
149.202.170.250	1,941
212.71.245.103	1,941
134.209.203.186	1,875
149.202.188.5	1,777
134.209.180.4	1,416
139.162.253.76	1,416
213.52.128.172	1,416

TLS Cipher Suite

TLS Protocol Version

Example TLS Access logs dashboard from QuickSight



Application Load Balancer: www-exampleloadbalancer-com

Top Talker

client_ip
34.216.30.180
209.43.1.222
72.21.198.66
72.21.198.67
72.21.198.65
72.21.198.64
34.207.92.255
64.39.103.105
46.4.69.209
216.244.66.194
136.243.22.77
23.237.4.26
104.200.129.212
46.4.71.36
100.43.85.162
85.206.165.8
82.80.230.228
216.244.66.197
194.99.104.27
216.244.66.200
72.21.196.64
72.21.196.67
72.21.196.66

Count of Records by TLSl Protocol

Count of Records by Ssl_cipher

Count of Records by Type

Simplifying user login with ALB authentication

AWS re:Invent

aws

Amazon Cognito configuration

```
[{
    "Type": "authenticate-cognito",
    "AuthenticateCognitoConfig": {
        "UserPoolArn": "arn:aws:cognito-idp:region-code:account-id:userpool/user-pool-id",
        "UserPoolClientId":"abcdefghijklmnopqrstuvwxyz123456789",          //ID of the Amazon Cognito user pool client
        "UserPoolDomain": "userPoolDomain1",                               //Domain prefix or FQDN of Amazon Cognito user pool
        "SessionCookieName": "my-cookie",                                  //Configure ALB Authentication Cookie Name
        "SessionTimeout": 3600,                                            //Configure ALB Authentication session length (1s – 7days)
        "Scope": “openid",                                                 //Set of user claims requested from IDP. Must include ID token
        "AuthenticationRequestExtraParams": {                              //Query Params (String-to-String) to include in redirect to IDP
                "display": "page",
                "prompt": "login"
        },
       "OnUnauthenticatedRequest": "deny | allow | authenticate"           //Behavior on Unauthenticated Requests
    },
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-id:targetgroup/target-group-name/target-group-id",
    "Order": 2
}]
```

Native OIDC configuration

```
[{
    "Type": "authenticate-oidc",
    "AuthenticateOidcConfig": {
        "Issuer": "https://idp-issuer.com",                                //IDP Endpoint
        "AuthorizationEndpoint": "https://authorization-endpoint.com",     //Endpoint to get Authorization Code
        "TokenEndpoint": "https://token-endpoint.com",                     //Endpoint to get ID and Access Token
        "UserInfoEndpoint": "https://user-info-endpoint.com",              //Endpoint to get user claims
        "ClientId": "abcdefghijklmnopqrstuvwxyz123456789",                 //OAuth2.0 Client ID configured in IDP shared with ALB
        "ClientSecret": "123456789012345678901234567890",                  //OAuth2.0 Client ID configured in IDP shared with ALB
        "SessionCookieName": "my-cookie",                                  //Configure ALB Authentication Cookie Name
        "SessionTimeout": 3600,                                            //Configure ALB Authentication session length (1s – 7days)
        "Scope": “openid",                                                 //Set of user claims requested from IDP. Must include ID token
        "AuthenticationRequestExtraParams": {                              //Query Params (String-to-String) to include in redirect to IDP
                "display": "page",
                "prompt": "login"
        },
       "OnUnauthenticatedRequest": "deny | allow | authenticate"          //Behavior on Unauthenticated Requests
    },
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-id:targetgroup/target-group-name/target-group-id",
    "Order": 2
}]
```

Info Received in HTTP Headers by Backends

- `x-amzn-oidc-accesstoken`: Access token from the token endpoint (plain text)
- `x-amzn-oidc-identity`: Subject field from the user info endpoint (plain text)
- `x-amzn-oidc-data`: User claims in JWT format (base64 URL encoded)
  - Header

    ```
    {
    "alg": "algorithm",
    "kid": "12345678-1234-1234-1234-123456789012",
    "signer": "arn:aws:elasticloadbalancing:region-code:account-id:loadbalancer/app/load-balancer-name/load-balancer-id",
    "iss": "url",
    "client": "client-id",
    "exp": "expiration“
    }
    ```

  - Payload

    ```
    {
    "sub": "1234567890",
    "name": "name",
    "email": "alias@example.com",
    ...
    }
    ```

Analyzing load balancer access logs

Monitoring using load balancer access logs

Access logs are pushed every 5 minutes to configured S3 bucket

Access logs are encrypted in transit to Amazon S3 and can be encrypted at rest

Athena can be used to query access logs to understand traffic patterns

Amazon QuickSight can be used to create dashboards for TLS vs. non TLS traffic, certificates/ciphers used, and assessing session resumption

Auditing your load balancers

Examining your load balancer activity

Using resource and tag-based permission to implement fine-grained access controls on load balancer resources using AWS Identity and Access Management (IAM) policies

Integration with CloudTrail enables capture of all API calls made to the load balancers to create a record of actions taken by a user, role, or an AWS service

Integration with AWS Config captures changes to load balancer configurations and notifies account owners