



Understanding & securing cloud resources

Using a layered approach

Ruskin Dantra

Solutions Architect, AWS

Ratan Kumar

Principal Solutions Architect, AWS

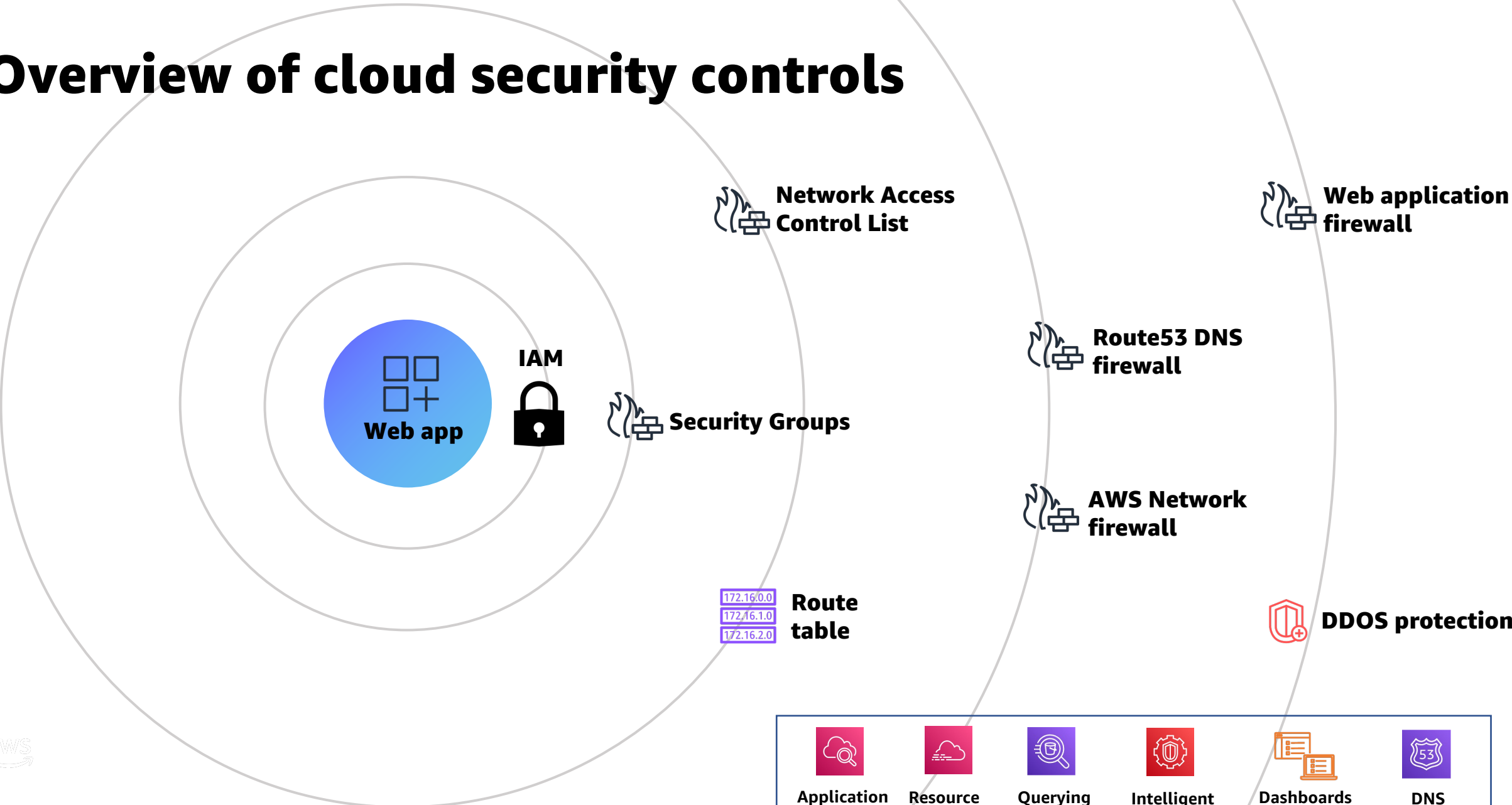
Agenda

- Overview of cloud security controls
- Discuss Demo Application Architecture
- Demo: Apply Security Controls
- Q&A

Disclaimer

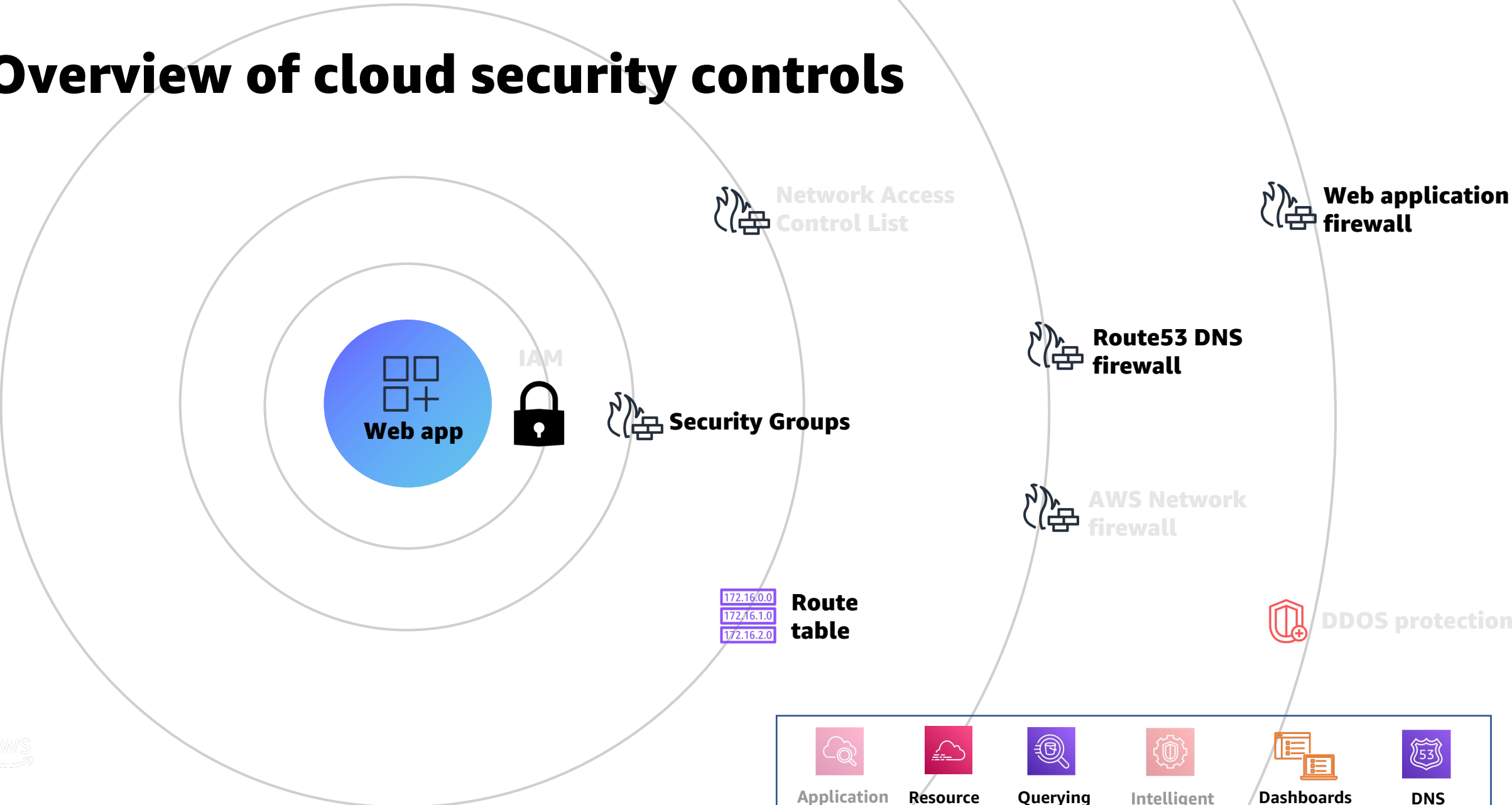
We work for Amazon Web Services (AWS), material presented here is our own opinion. Although care has been taken to ensure a vendor agnostic session, we might sometimes refer to services offered by AWS to reinforce a principle.







Overview of cloud security controls



					
Application logs	Resource access logs	Querying Logs	Intelligent threat detection	Dashboards	DNS query logs

Overview of cloud security controls



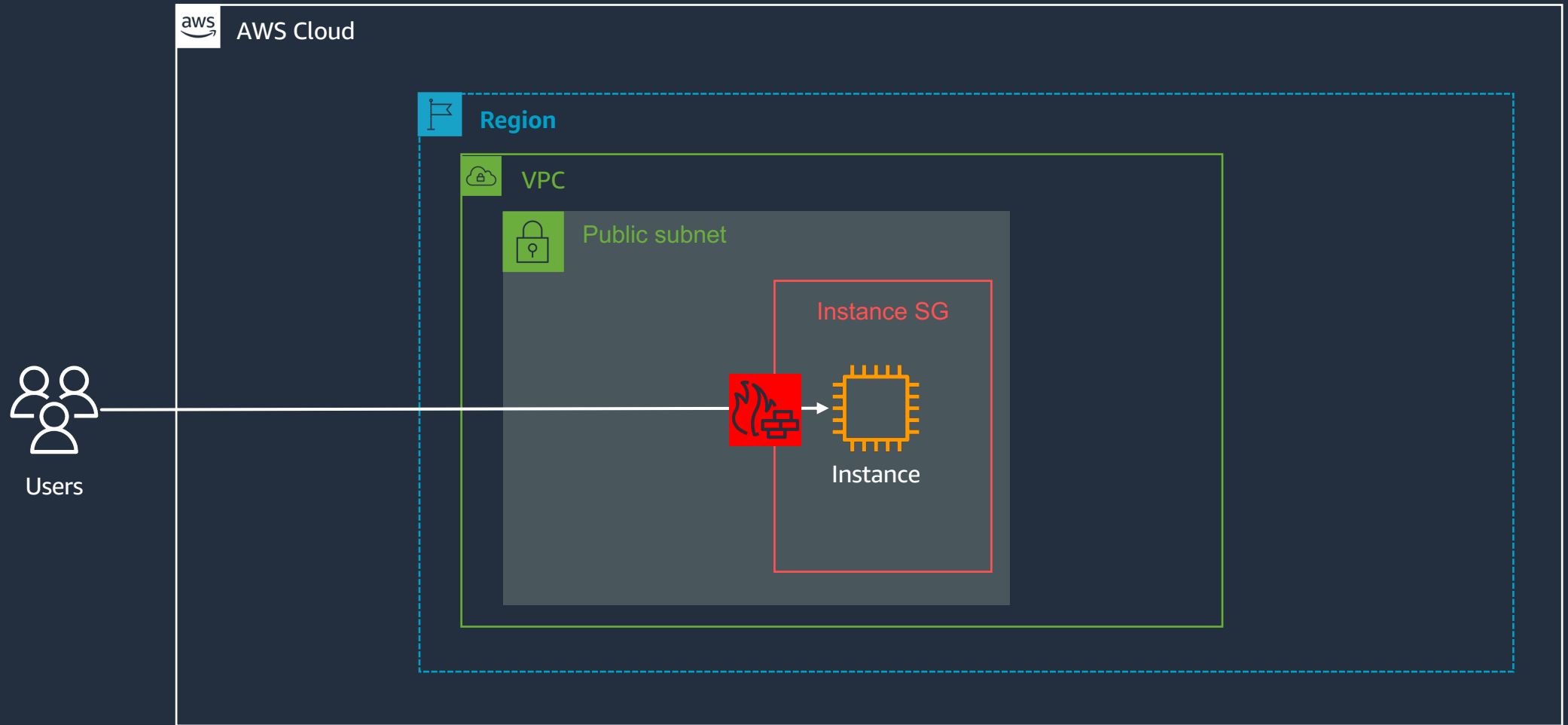
					
Application logs	Resource access logs	Querying Logs	Intelligent threat detection	Dashboards	DNS query logs

Discuss the Architecture

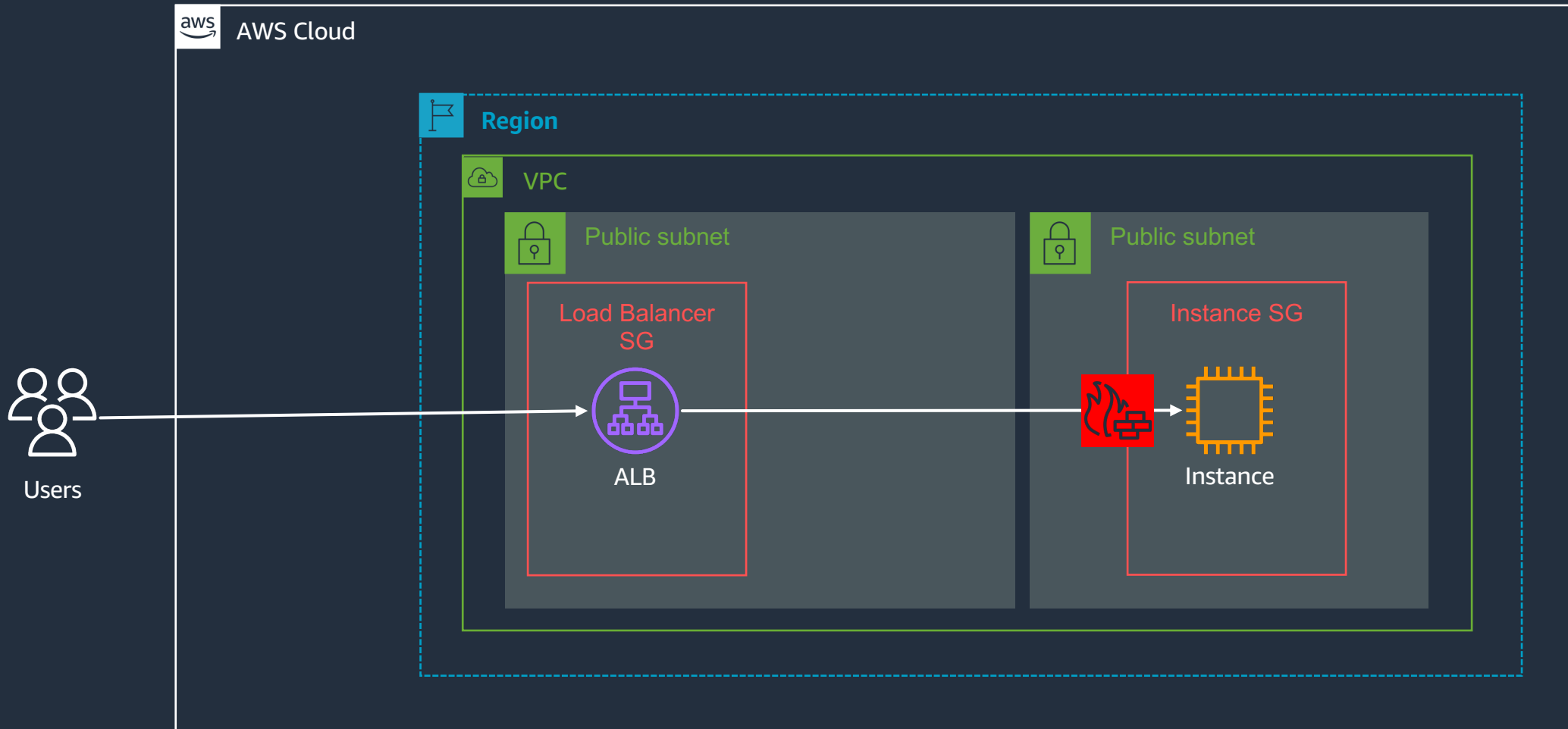


<https://bit.ly/owaspnzday2023>

OWASP Juice Demo App



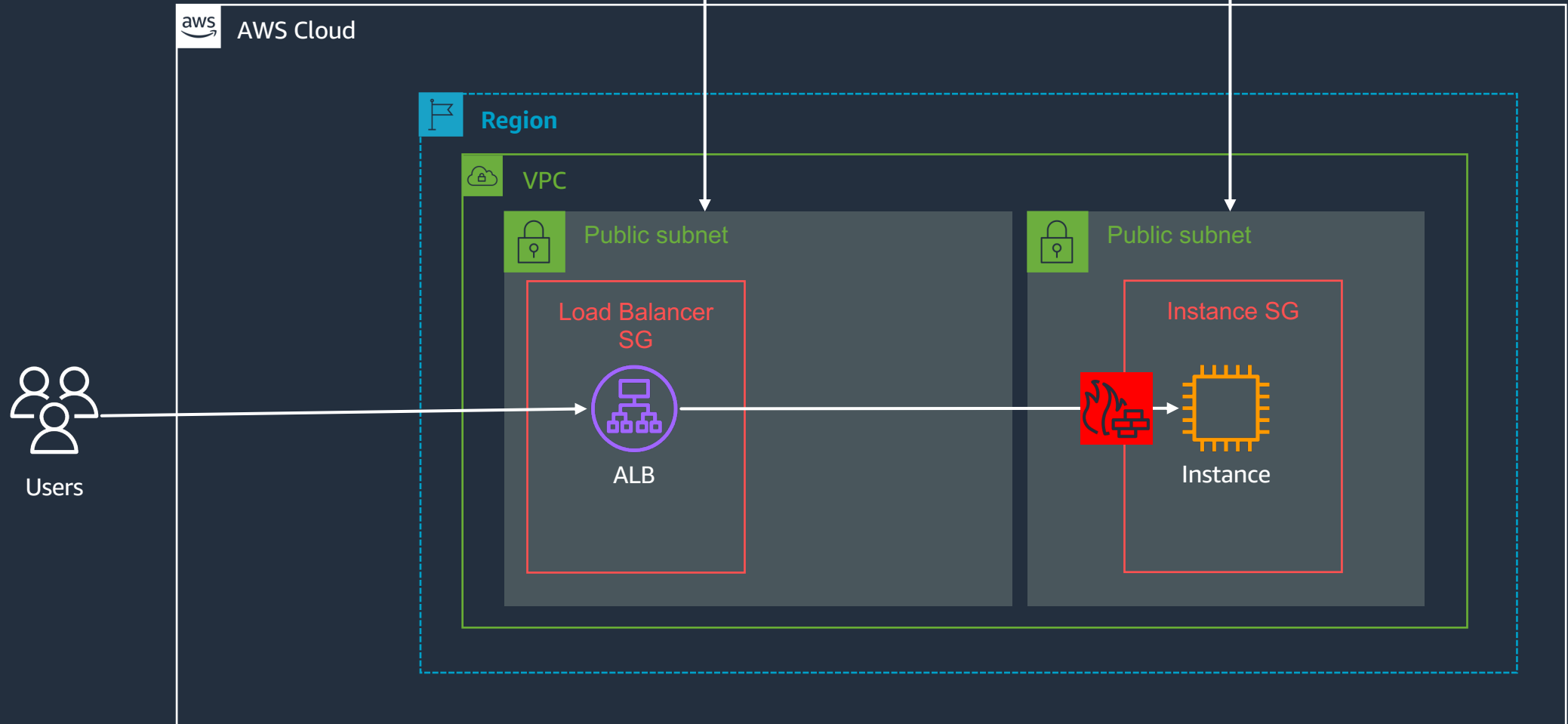
Add firewall rules to restrict direct internet access



Restrict inbound internet access

Destination	Next hop
10.10.0.0/16	local
0.0.0.0/0	Internet GW

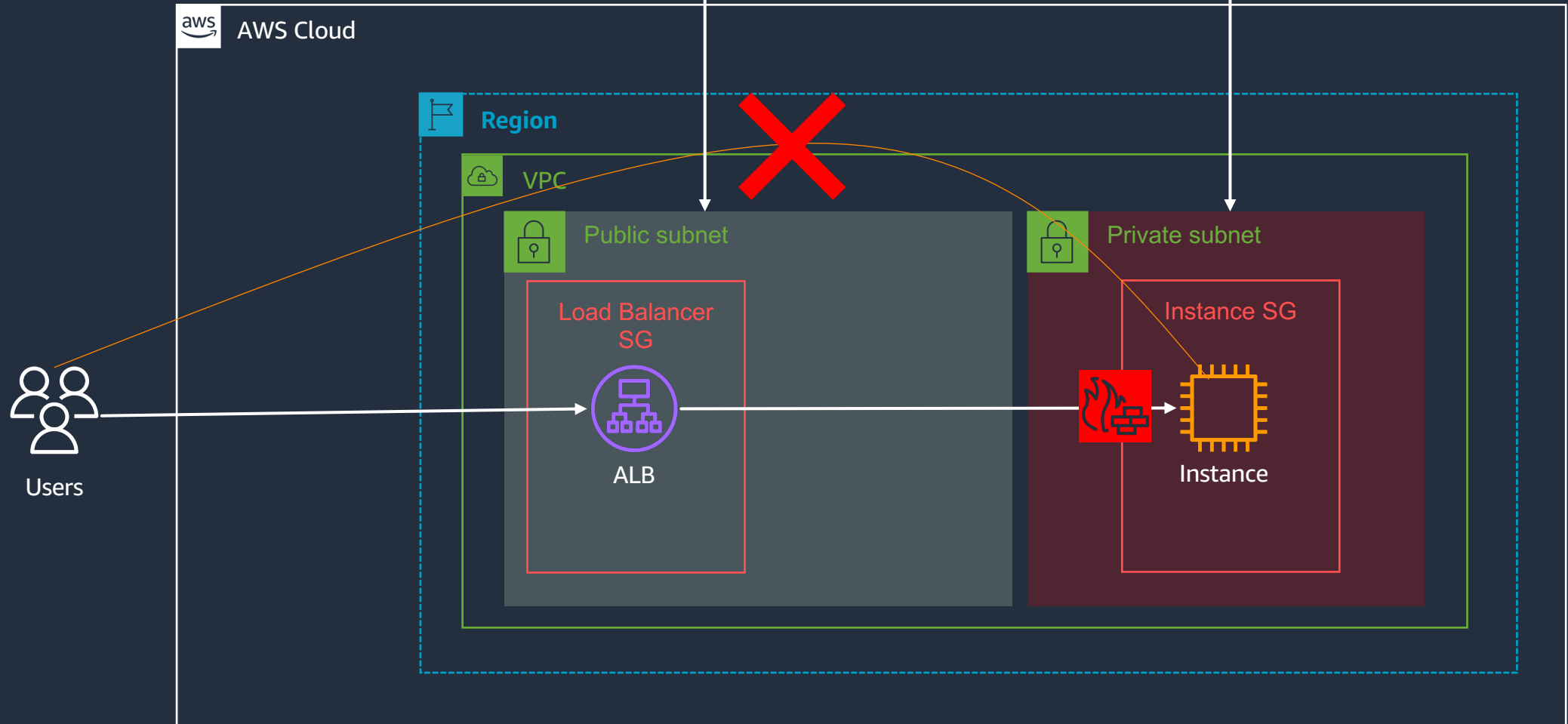
Destination	Next hop
10.10.0.0/16	local
0.0.0.0/0	Internet GW



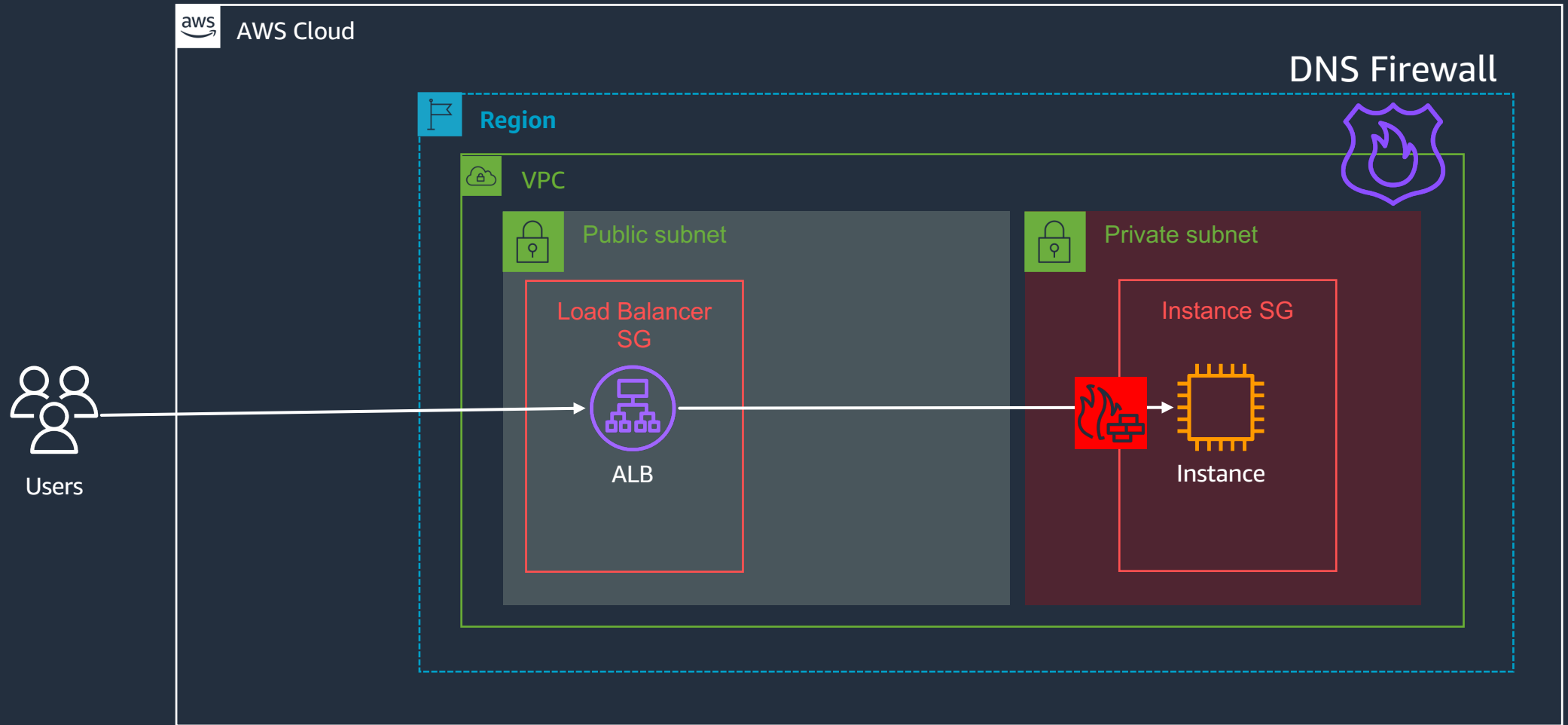
Restrict inbound internet access

Destination	Next hop
10.10.0.0/16	local
0.0.0.0/0	Internet GW

Destination	Next hop
10.10.0.0/16	local
0.0.0.0/0	NAT GW



Protecting against DNS data exfiltration

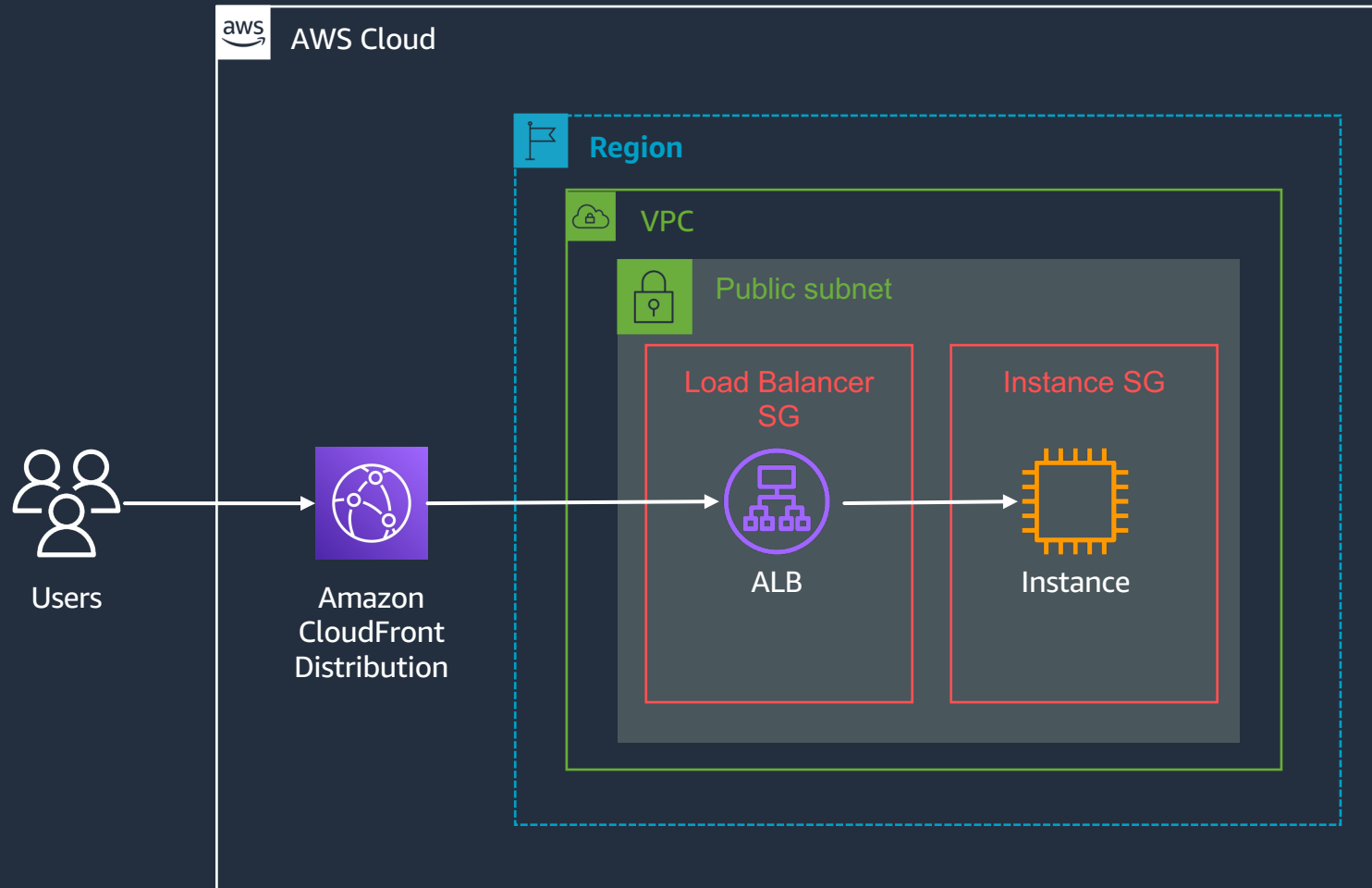


Managed services

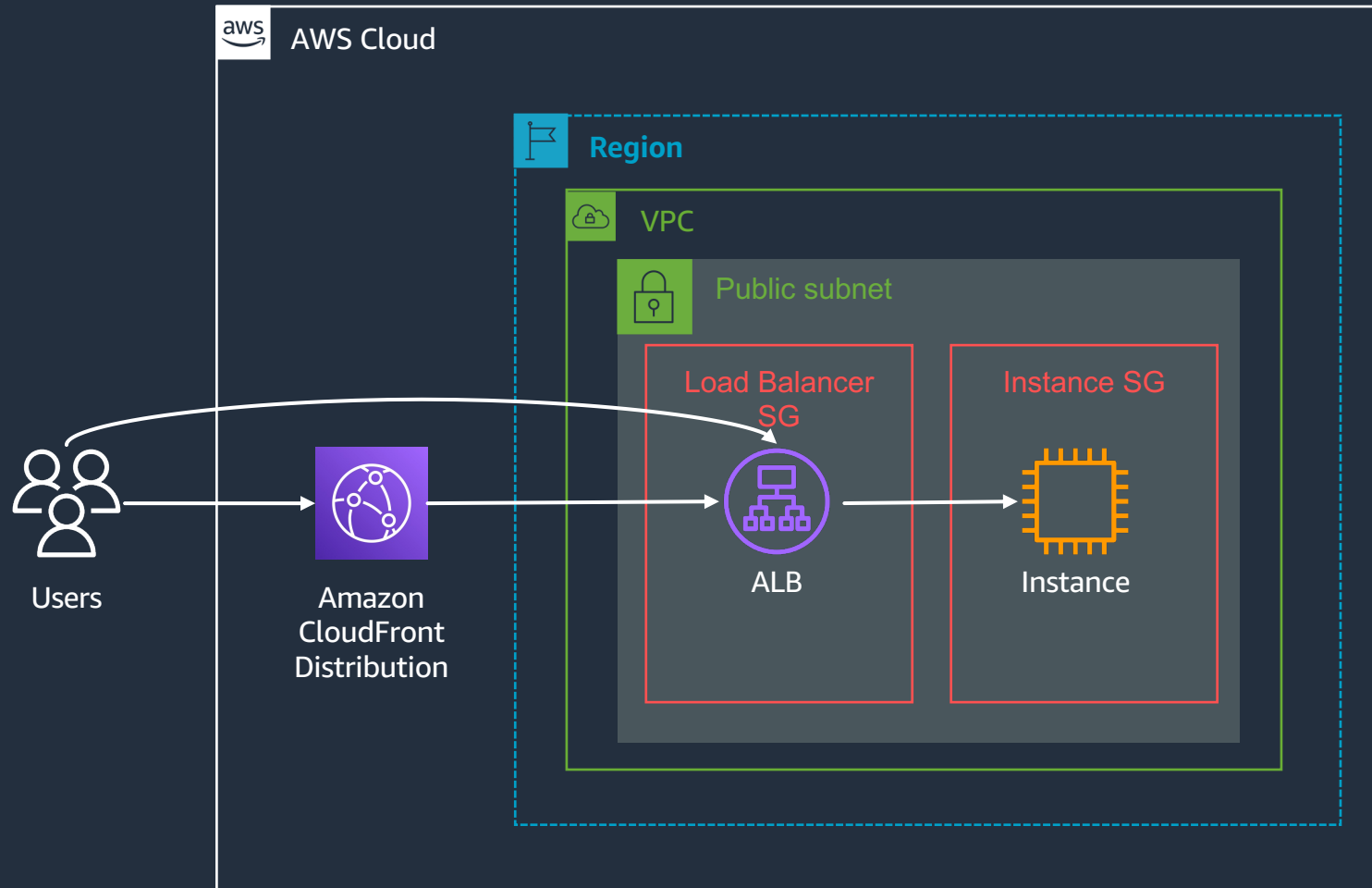


<https://bit.ly/owaspnzday2023>

Application architecture – Recap



Application architecture – Bypass CF



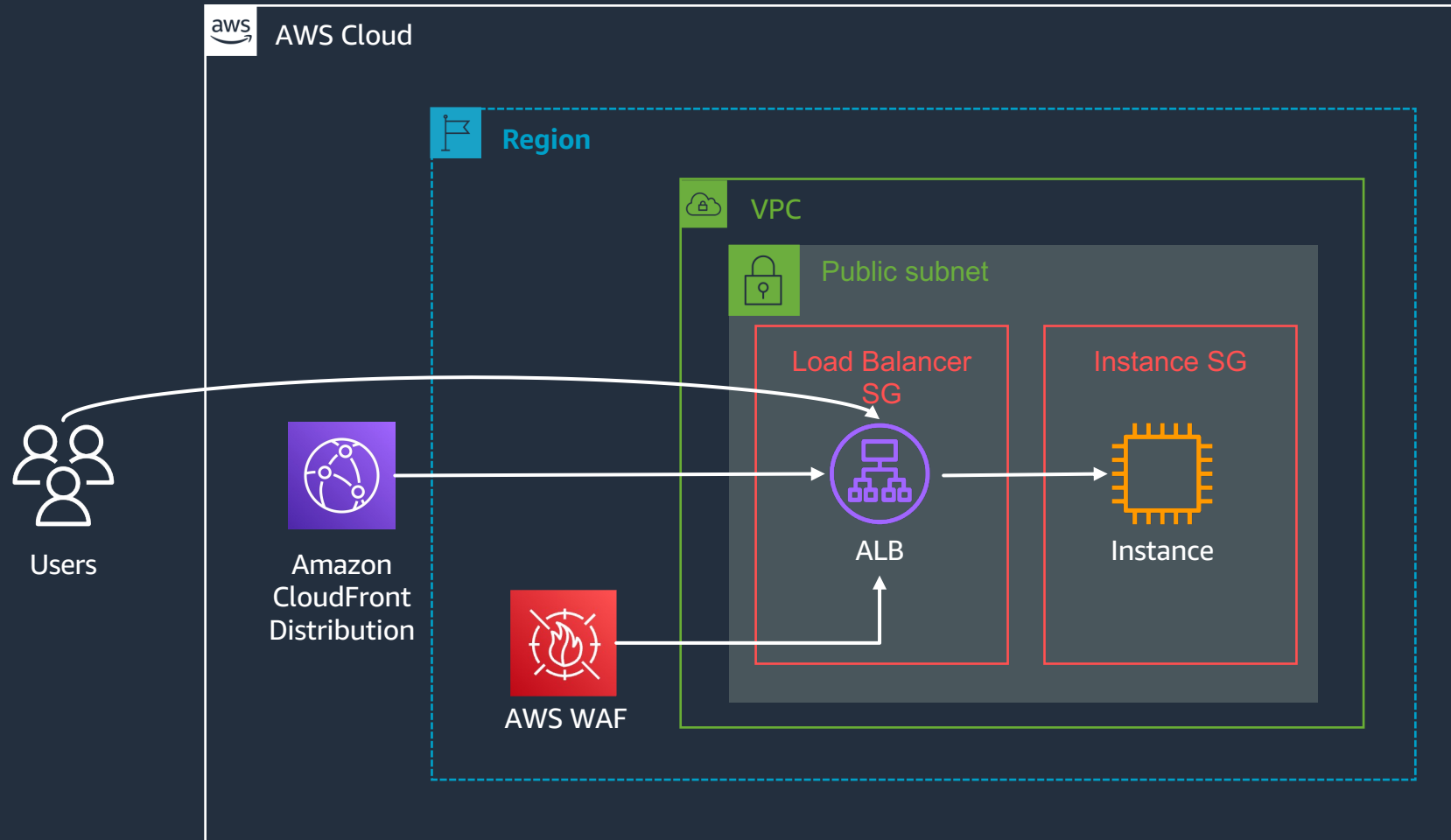
Demo – ALB



Demo – WAF



Application architecture – WAF







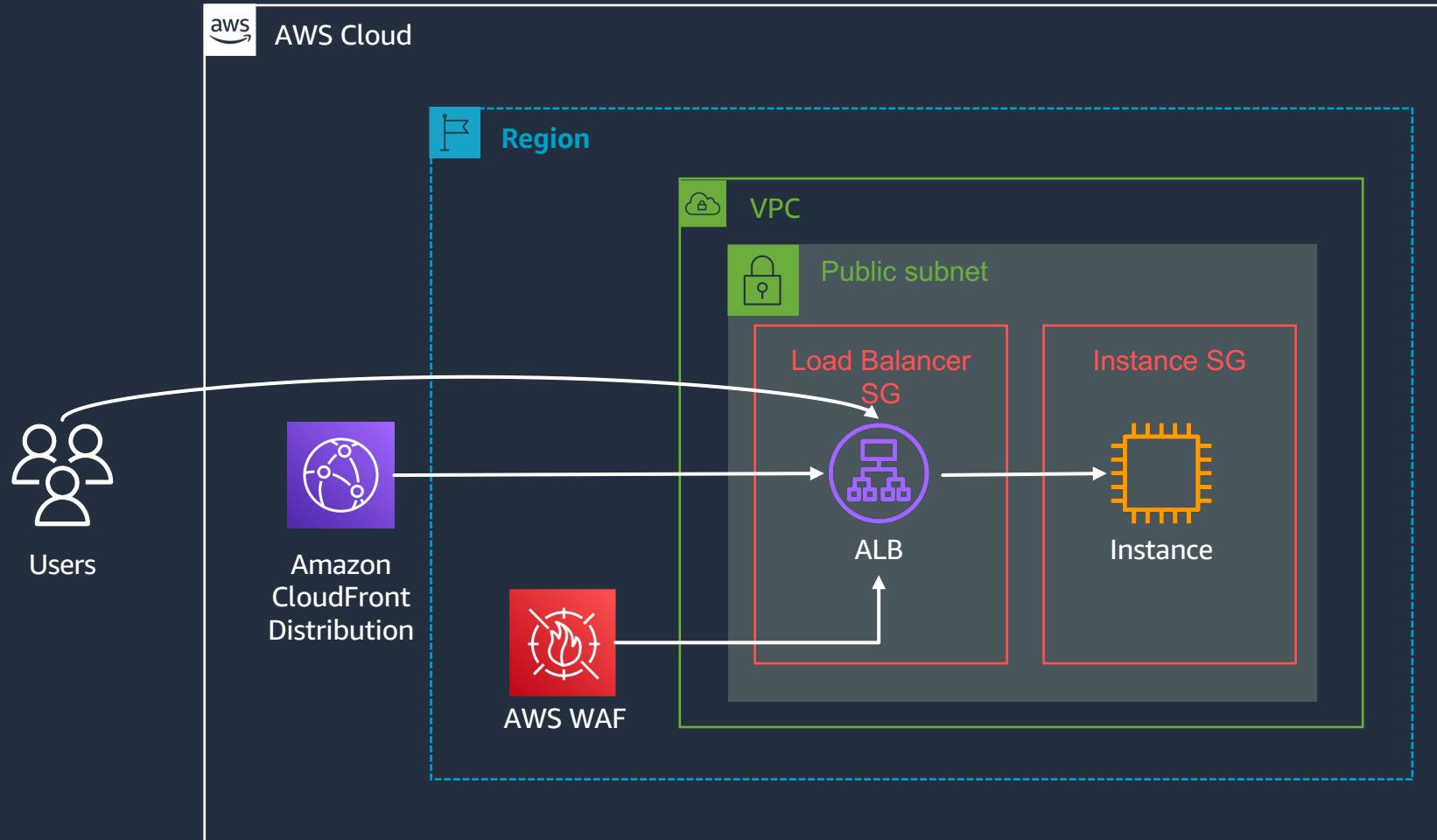
WAF – Protecting your asset

- IP based protection
- Geographic match protection
- Change default action to BLOCK

Demo – CloudFront



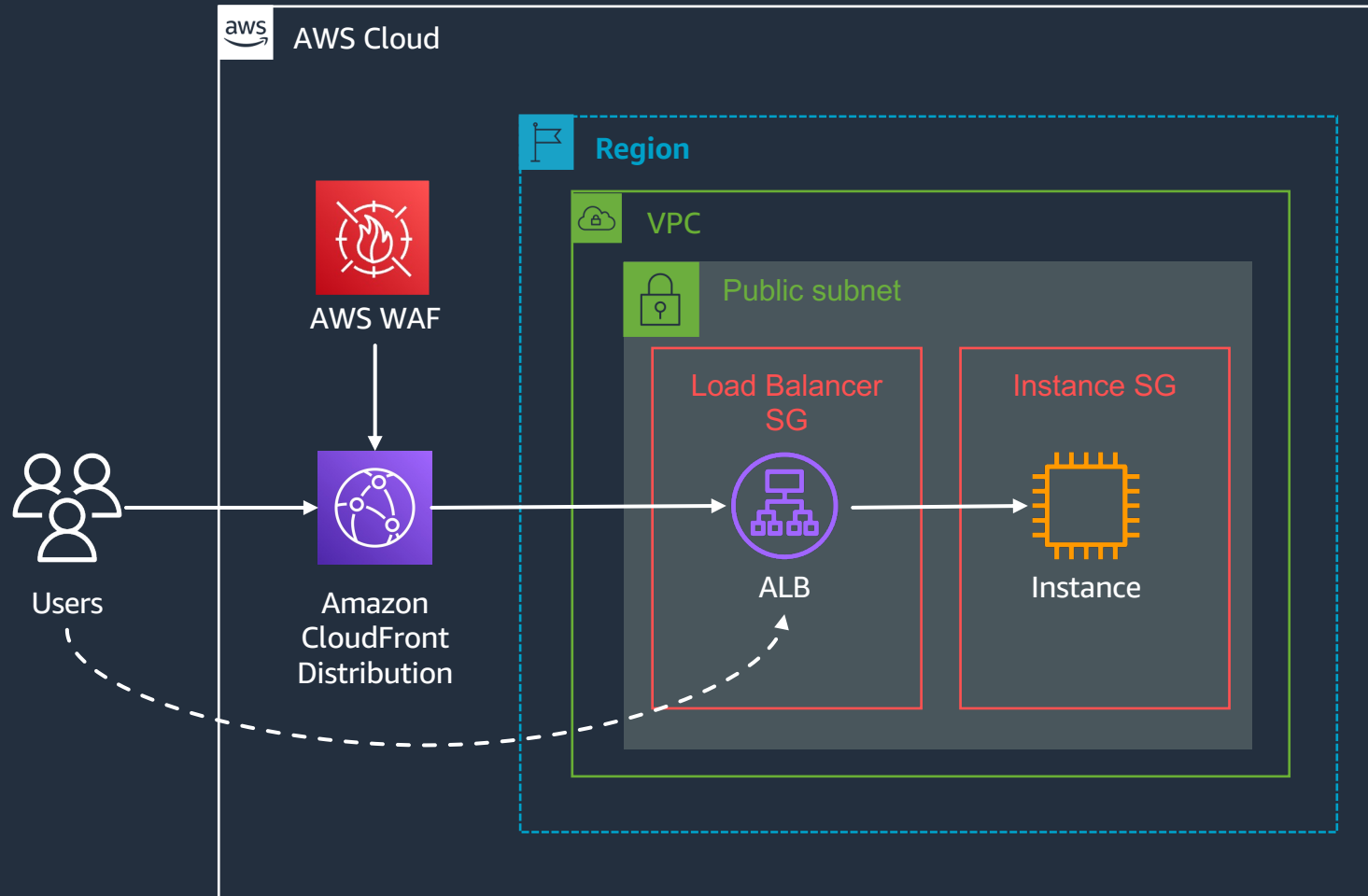
Application architecture – Recap



Demo – CloudFront & WAF



Application architecture – CF & WAF



Demo – WAF SQLi

Summary

- Consider all threat vectors
- Secure in layers
- Trust but verify
- Automation
- Dashboards are great but alerts are better

Questions?



Feedback -

<https://www.pulse.aws/survey/XFVF8VIW>





Thank you!

Ruskin Dantra

Ratan Kumar