AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

Welcome

Welcome to this workshop! Today we will cover practical guidance for designing and building secure Amazon VPCs. We’ll briefly cover the basics, such as subnets, security groups, routing, and flow logs, but the main focus will be on the range of additional services and features that AWS offers that help you operate securely.

The workshop will use an interactive, scenario-based approach, walking through a series of challenges that are based on real-world situations. To solve them, you’ll have to use a number of AWS services, such as AWS Network Firewall, Amazon Route 53 Resolver DNS Firewall, AWS Systems Manager, Traffic Mirroring, AWS WAF, AWS PrivateLink, and more. All the examples given will follow best practices for Amazon VPC security, design, and management, and we provide plenty of links to additional reading and learning content throughout the workshop.

NET308-R

Building secure VPCs and integrating them into your network

Laura Caicedo (she/her)

Solutions Architect Manager
AWS

Matt Johnson (he/him)

Chief Technologist, UK Public Sector
AWS

Getting started

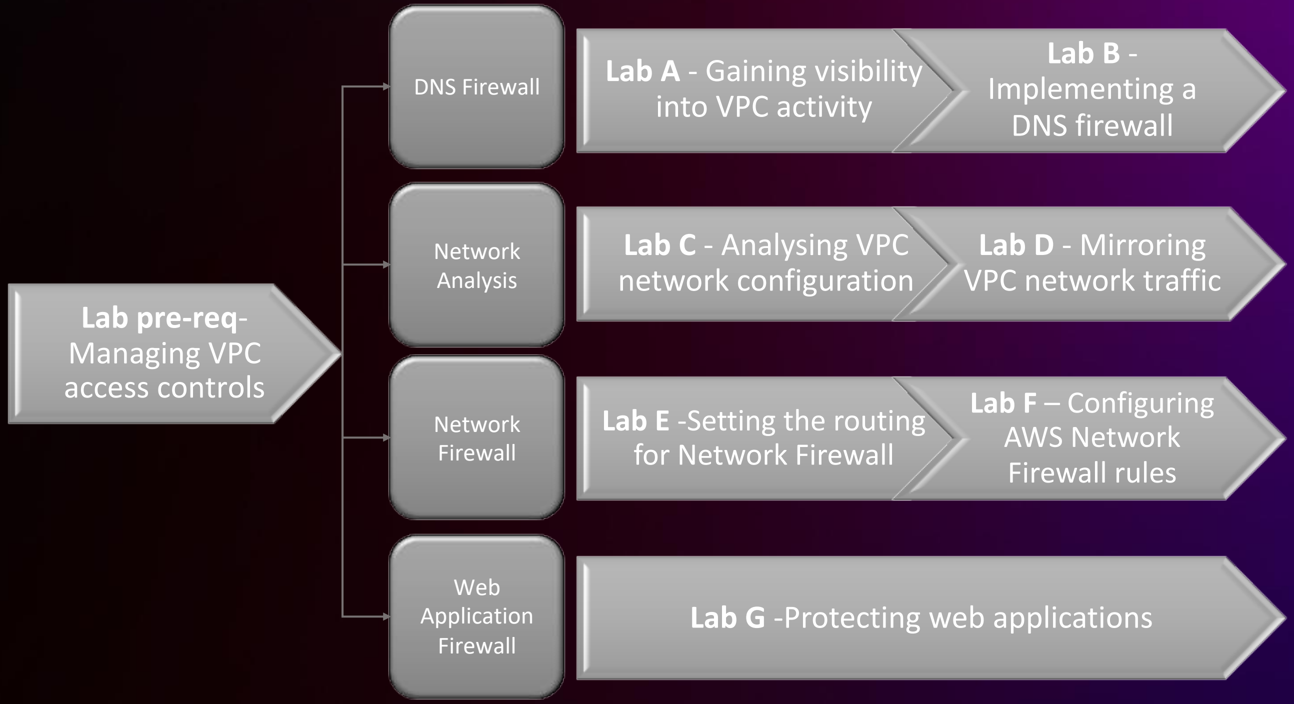
- Lab guide: https://tinyurl.com/securevpc
- Hash code:
- Attendees need to bring their own laptop or share with a partner

---

- This a 300-level workshop
- We assume you have previous knowledge about security groups, subnets, and basic routing

Intro

- Scenario-based workshop (4 tracks)
- Each scenario will have an overview of the challenge, desired outcomes, and some suggested starting points
- Two ways of solving: you’re free to explore and get to the desired outcome alone or use our step-by-step walkthrough to help you on your way
- You can start with any track depending where you want to dive deep; tracks are not dependent on the previous one

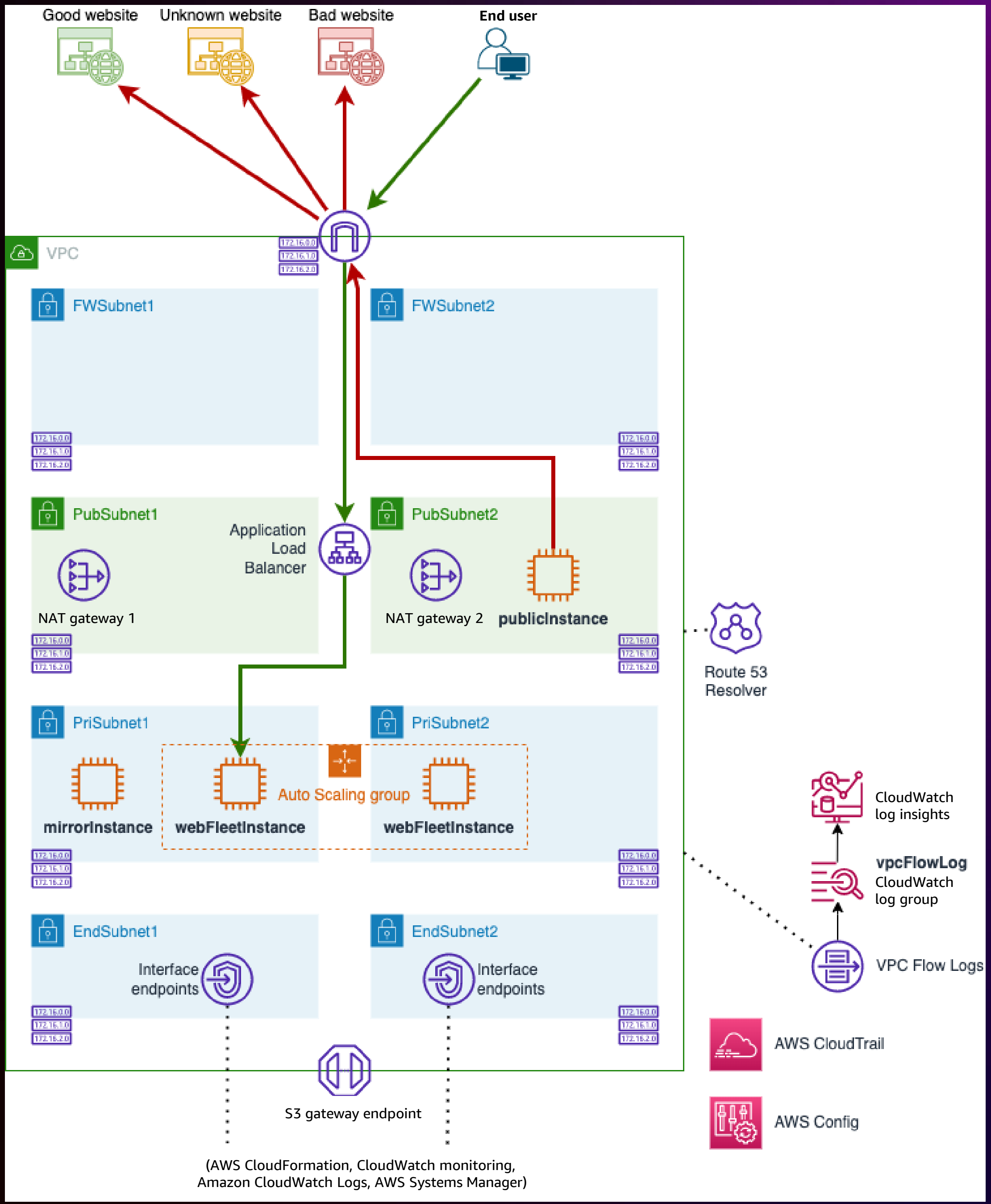


Lab pre-req- Managing VPC access controls
DNS Firewall
Lab A - Gaining visibility into VPC activity
Lab B - Implementing a DNS firewall
Network Analysis
Lab C - Analysing VPC network configuration
Lab D - Mirroring VPC network traffic
Network Firewall
Lab E -Setting the routing for Network Firewall
Lab F – Configuring AWS Network Firewall rules
Web Application Firewall
Lab G -Protecting web applications

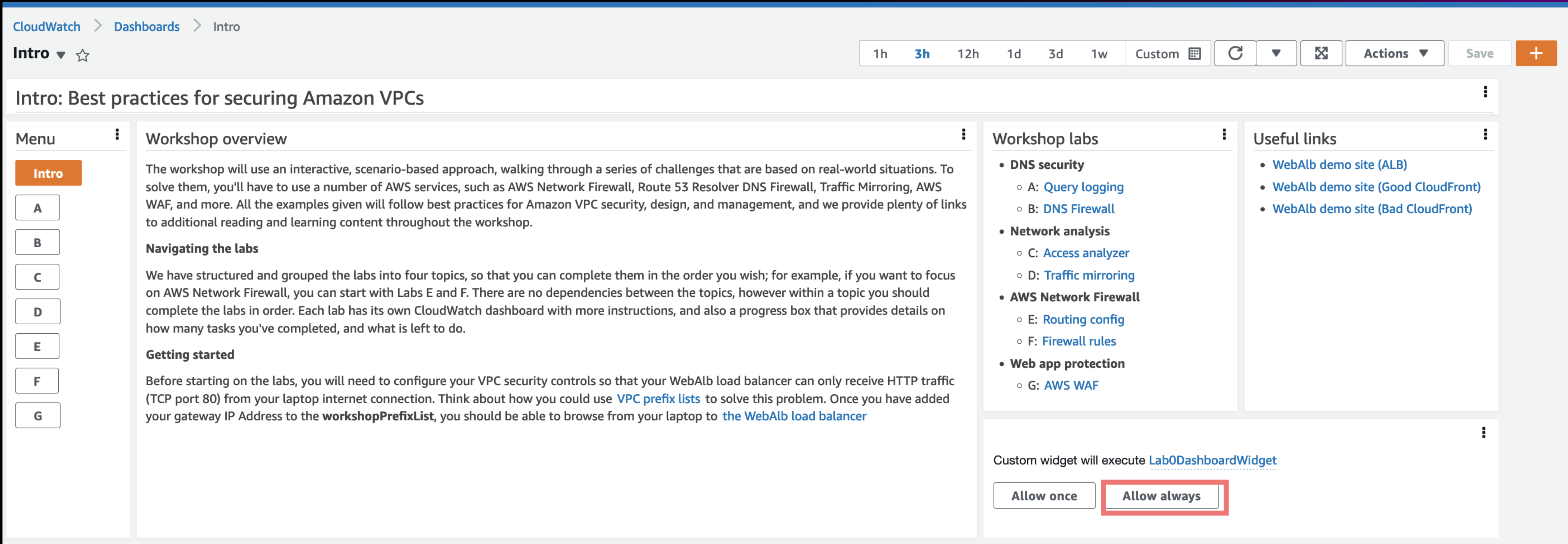
Lab architecture

Pre-deployed infrastructure

- Single VPC with public and private subnets
- PrivateLink endpoints, NAT gateway, internet gateway
- Internet-facing Application Load Balancer, EC2 instances (NGNIX)
- And other things that we will mention in the **pre-deployed infrastructure** of each lab



CloudWatch dashboard



Intro: Best practices for securing Amazon VPCs

Menu

Workshop overview

The workshop will use an interactive, scenario-based approach, walking through a series of challenges that are based on real-world situations. To solve them, you'll have to use a number of AWS services, such as AWS Network Firewall, Route 53 Resolver DNS Firewall, Traffic Mirroring, AWS WAF, and more. All the examples given will follow best practices for Amazon VPC security, design, and management, and we provide plenty of links to additional reading and learning content throughout the workshop.

Navigating the labs

We have structured and grouped the labs into four topics, so that you can complete them in the order you wish; for example, if you want to focus on AWS Network Firewall, you can start with Labs E and F. There are no dependencies between the topics, however within a topic you should complete the labs in order. Each lab has its own CloudWatch dashboard with more instructions, and also a progress box that provides details on how many tasks you've completed, and what is left to do.

Getting started

Before starting on the labs, you will need to configure your VPC security controls so that your WebAlb load balancer can only receive HTTP traffic (TCP port 80) from your laptop internet connection. Think about how you could use VPC prefix lists to solve this problem. Once you have added your gateway IP Address to the **workshopPrefixList**, you should be able to browse from your laptop to the WebAlb load balancer

Workshop labs

- **DNS security**
  - A: Query logging
  - B: DNS Firewall
- **Network analysis**
  - C: Access analyzer
  - D: Traffic mirroring
- **AWS Network Firewall**
  - E: Routing config
  - F: Firewall rules
- **Web app protection**
  - G: AWS WAF

Useful links

- WebAlb demo site (ALB)
- WebAlb demo site (Good CloudFront)
- WebAlb demo site (Bad CloudFront)

Custom widget will execute Lab0DashboardWidget

Thank you!

Laura Caicedo

lauramcai

laura-caicedo

Matt Johnson

mjwork

Mhjwork

Please complete the session survey in the **mobile app**