

Protecting Network and Host-level Boundaries

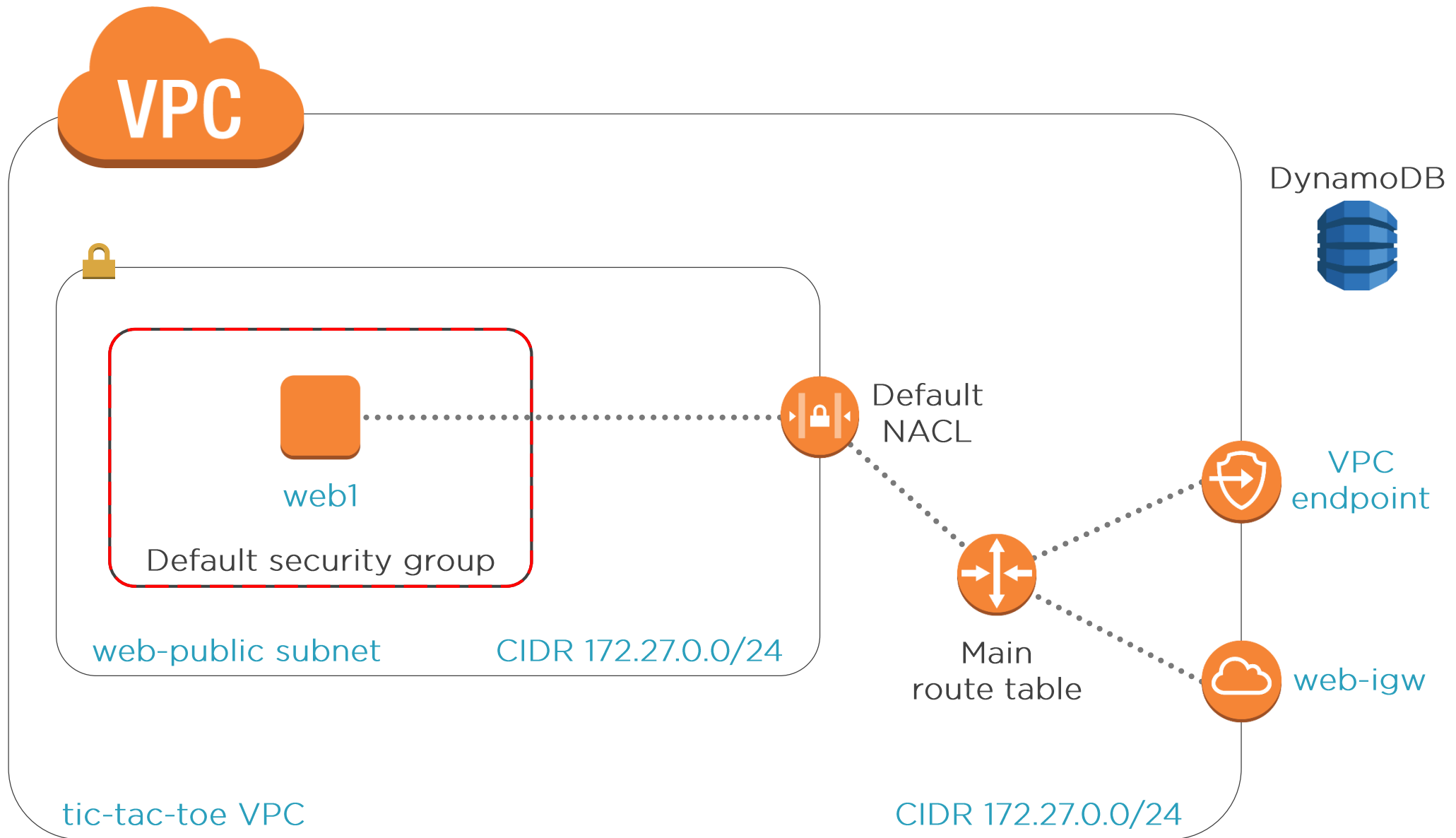


Ben Piper

AWS CERTIFIED SOLUTIONS ARCHITECT

<https://benpiper.com>







AWS Networking Deep Dive: Virtual Private Cloud (VPC)



Module Overview



Creating a public subnet

Creating and using an IAM
instance profile

Using SSH key pairs

Using VPC endpoints

Network access control lists



Demo



Create the tic-tac-toe VPC

Create internet gateway

Add default route

Reconfigure default security group



Demo



Create IAM role to allow access to DynamoDB

Role will contain a trust policy to allow EC2 instances to assume the role

Launch instance and attach instance profile



Demo



SSH into instance using OpenSSH client

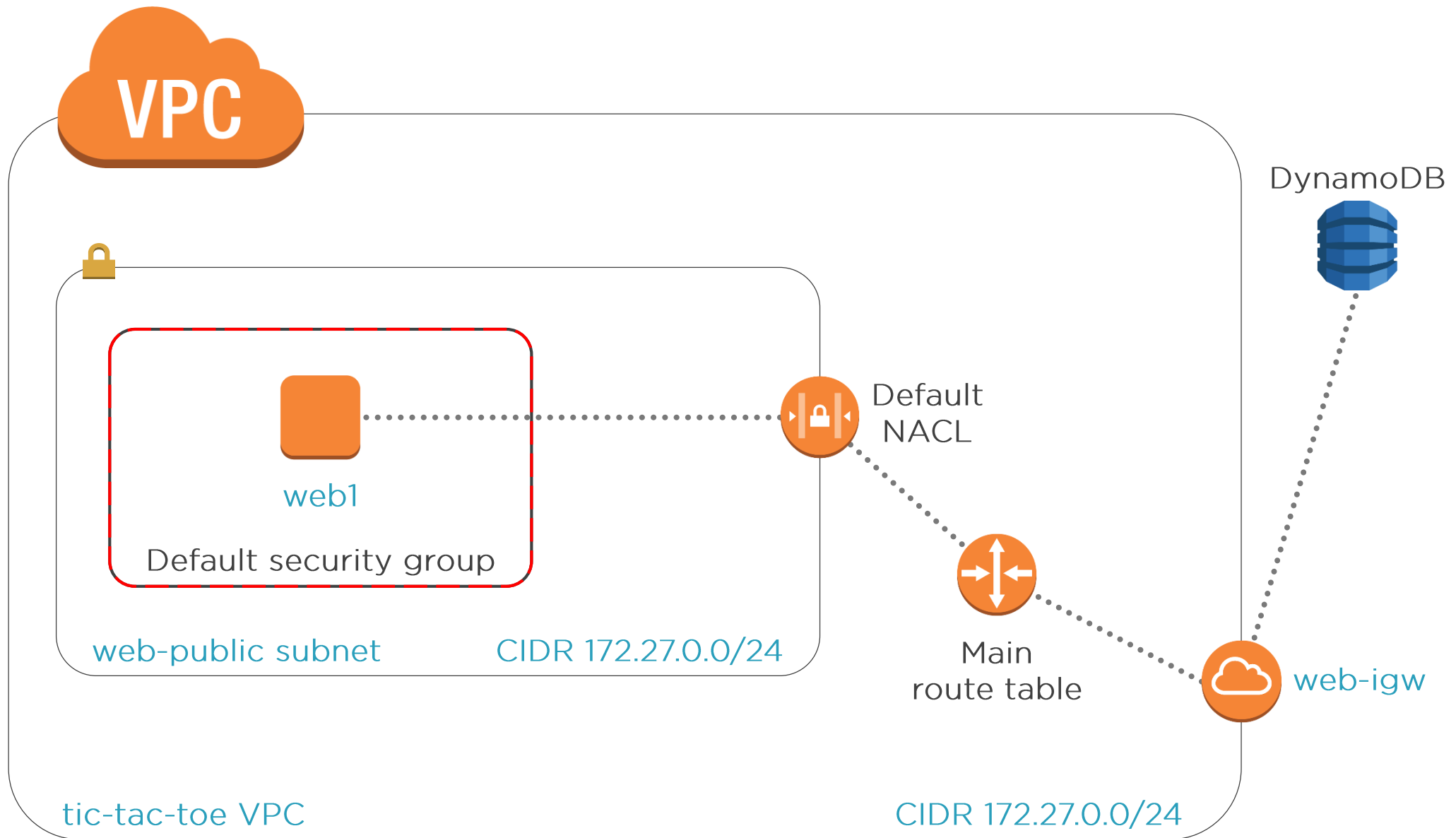
Linux comes with the client installed

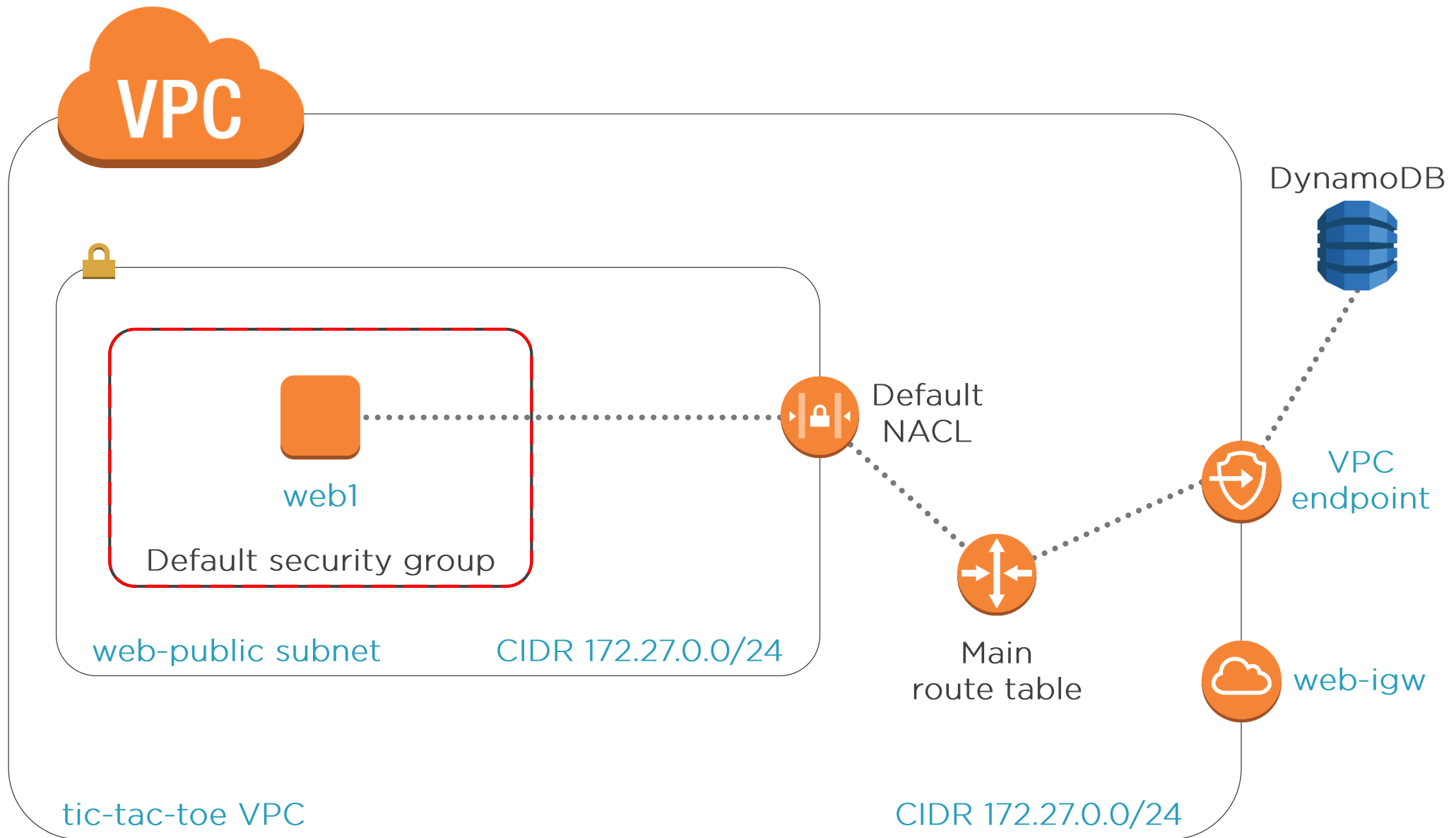
Windows 10 comes with the client installed as of the April 2018 update



Using VPC Endpoints







Demo



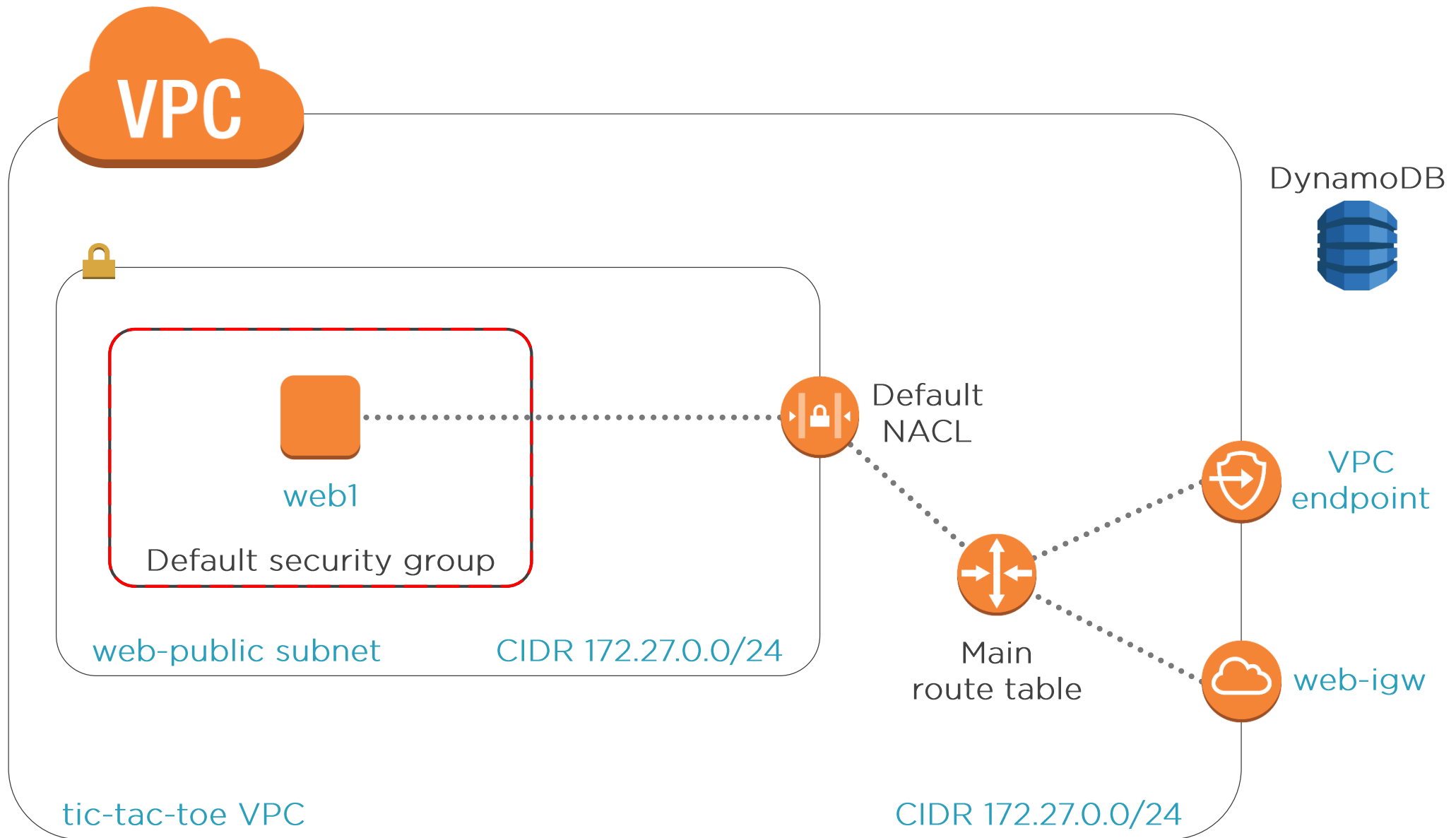
Block outbound internet access from the instance

Configure VPC endpoint



Network Access Control Lists





Security Group vs. NACL

Security group

Instance level

Stateful

Unnumbered rules

NACL

Subnet level

Stateless

Numbered rules



Demo



Explore the structure of NACL rules

Reconfigure the default NACL



Summary



A public subnet has a default route to an internet gateway

Use an IAM instance profile to grant an instance access to an AWS service

Decide whether to connect to AWS endpoints via the internet or a VPC endpoint

Security groups and network access control lists act as firewalls but differ in significant ways





Coming up Next

Protecting data at rest



Understanding CloudTrail



Event Types

Management

Configuration changes to AWS services

Reading resources

Logging into the management console

Assuming a role

Data

Access to S3 objects

Lambda function execution





CloudTrail logs are stored in S3
Limit what you log to control costs

Demo



Analyze event logs that CloudTrail stores by default

Configure CloudTrail to log all management write events



CloudTrail vs. CloudWatch Logs



CloudTrail vs. CloudWatch Logs

CloudTrail

Logs AWS actions

Stores logs in S3

CloudWatch Logs

Aggregates logs from CloudTrail *and* non-AWS sources

Provides interface to view and search logs



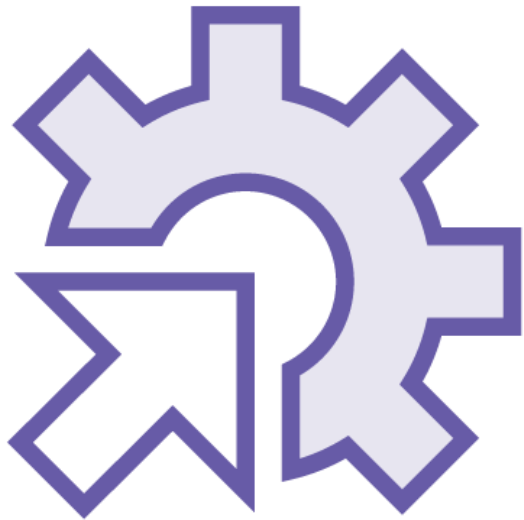
Configuring CloudWatch Logs



Create a CloudWatch Logs log group to store CloudTrail logs



Configuring CloudWatch Logs



Create IAM service role

- Contains inline service policy that grants CloudTrail permissions to send logs to CloudWatch Logs
- Contains trust policy that allows CloudTrail to assume the role

Role is an IAM principal for CloudTrail to use to authenticate to CloudWatch Logs

Demo



Create a log group in CloudWatch Logs

Create an IAM role for CloudTrail
to assume

Browse and search logs in
CloudWatch Logs



Demo



Create CloudWatch alarm to trigger
when CloudTrail logs a
management event



Searching Logs with Athena



Why Athena?

You don't want to use
CloudWatch Logs

You want to search the
contents of S3 objects





Athena uses SQL

You must provide the schema

AWS provides the schema for
CloudTrail logs

Demo



Select the S3 bucket containing the objects to search

Create a table in Athena

Run queries against CloudTrail logs



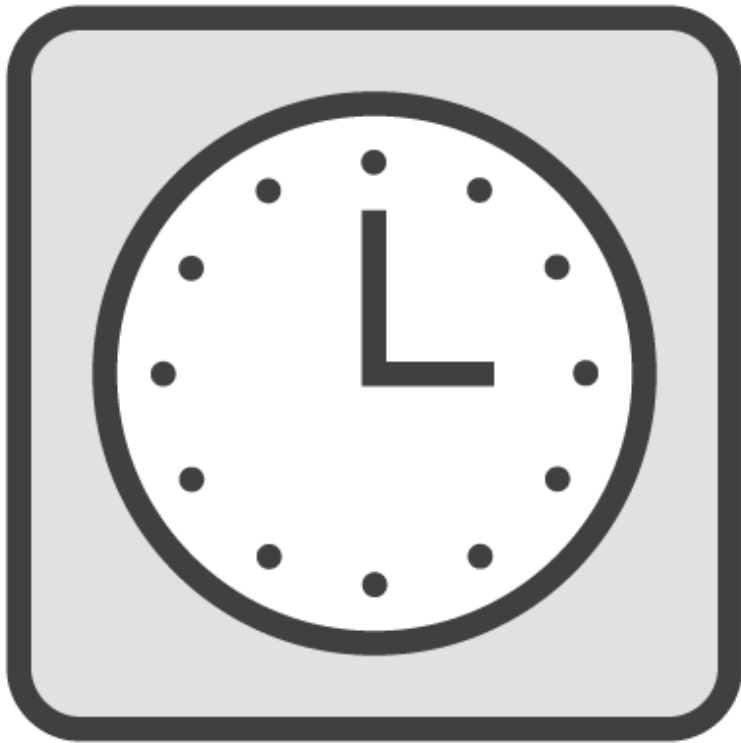
Tracking Configuration Changes in AWS Config



Events and Configuration States



AWS Config



Tracks configuration changes over time

Records changes in S3

Notifies of changes