

## Requirements

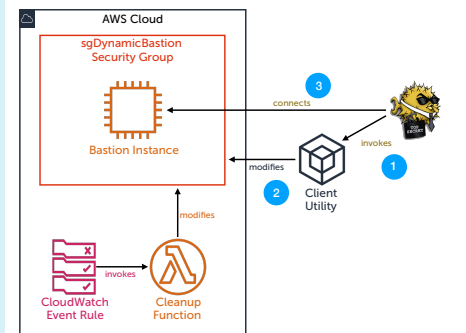
- › Not listening to 0.0.0.0/0
- › Support remote users on dynamic IPs
- › Assume API keys
- › Self-cleaning
- › Low-friction
- › Simple

## Solution

## High-Level

- › CloudFormation — template VPC
  - › bastion instance
  - › two security groups, dynamic and static
  - › IAM role for editing the dynamic security group
  - › Lambda + CloudWatch event rule
- › A small amount of code
  - › user utility
  - › Lambda function
- › A small amount of SSH configuration

## In AWS



## The Code

- › Lambda function
  - › Periodic execution
  - › Evaluates rule descriptions in dynamic group
  - › Deletes expired (or invalid) rules
- › User utility
  - › Requires API keys (with relevant policy attached)
  - › Inserts user's current public IP into dynamic security group when run
  - › SSH configuration runs this utility before connecting
- › Written in Go
  - › Uses the AWS API
  - › Static binary

## Demo & Walkthrough



# Questions...

## Links

- › <https://github.com/kirasystems/bastion-security>
- › CloudFormation, Go code, documentation
- › Freely adaptable



## Contact Us!



support@kirasystems.com



+1 888 710 3454



kirasystems.com