

Monitoring & Testing Networks on AWS

Using native tools

Hitarth Asrani

About Me

- Hitarth Asrani, AWS Cloud DevOps Engineer @ Leaven/CCL (Part of Spark Business Group) ~ 2 years in October
- 6 X AWS Certified. Talk to me after if you want to learn more about AWS Certification
- Spent the last year building and debugging a complex network for one of my clients.
- Held back trying to go Swimming during the Cyclone. It just seems wrong...

Agenda

10-15 mins talk, around 15 mins live demo

Introduction/Quick Recap of networking on AWS.

Monitoring networks using Cloudwatch and other tools on AWS

Testing your networks using 3 (or 4) different tools

Live Demo

Q&A / End

Networking on AWS Recap

VPC - Virtual Private Cloud

Subnets - segmented pieces of your VPC

Route Tables - Rules/Routes for your subnets or VPCs

Security Groups - set of rules for inbound and outbound traffic applied on resources



Monitoring Networks

Logs + (Cloudwatch or S3) = Fancy Charts

- Cloudwatch is your central place for anything monitoring on AWS
- VPC Flow logs capture ...
- AWS Network Firewall can log to S3 or CW.
- Cloudwatch Contributor insights
- S3 + Athena can give you insights into logs on S3

Flow log settings

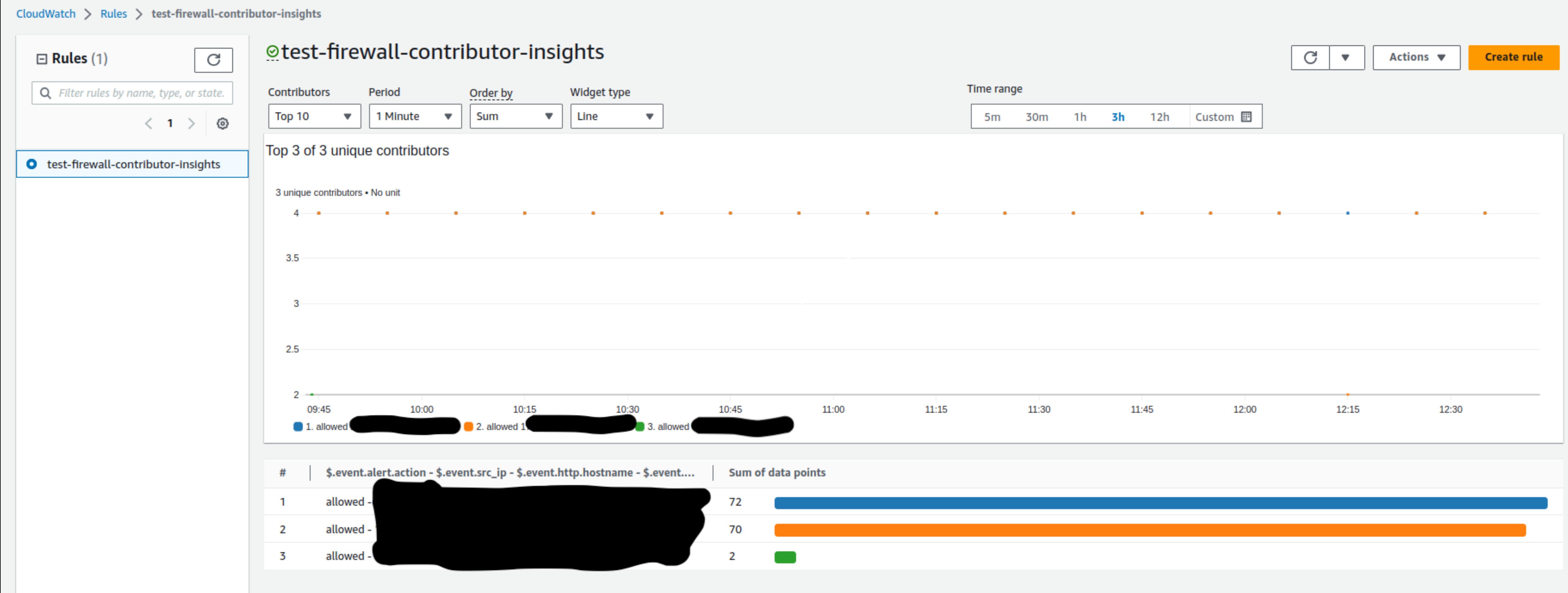
Name - *optional*
test-flow-log

Filter
The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).
 Accept
 Reject
 All

Maximum aggregation interval [Info](#)
The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.
 10 minutes
 1 minute

Destination
The destination to which to publish the flow log data.
 Send to CloudWatch Logs
 Send to an Amazon S3 bucket
 Send to Kinesis Firehose in the same account
 Send to Kinesis Firehose in a different account

CloudWatch Contributor Insight Example



Testing Networks - I

VPC Reachability Analyser

Path ID: nip-07aa36fc008c73fe

| Summary <small>Info</small> | | |
|---------------------------------|---|---|
| Path ID nip-07aa36fc008c73fe | Last analysis date July 6, 2023, 16:23 (UTC+12:00) | Reachability status ✖ Not reachable |
| Source i-08e63b72ba98d5254 | Source account ID 893548939888 | Destination i-0398b9c4f78e29bee |
| Destination port - | Protocol TCP | |

eni-0e09140186c025049

| | | |
|------------------------------------|------------------------------|------------------------------------|
| Attached To i-0398b9c4f78e29bee | VPC vpc-099fd31a9d803f91f | Subnet subnet-02e59fc2b08d92570 |
|------------------------------------|------------------------------|------------------------------------|

ENI_SG_RULES_MISMATCH:
None of the ingress rules in the following security groups apply: sg-070f0457aab82a80d. See [sg-070f0457aab82a80d](#).

- Testing suite under AWS Network Manager
- Test connectivity between a source resource and destination resource
- Price per analysis (ap-se-2) - \$0.10
- Troubleshoot, verify and automate verification of connectivity

Testing Networks - II

VPC Network Access Analyser

- Understand network access on your resources.
- Verify that this meets your security requirements
- Demonstrate Compliance

Network Manager > Network Access Scopes > nis-0a02bf937c2cd6bd7

nis-0a02bf937c2cd6bd7 / network-tgw-access

Summary [Info](#) [Actions ▾](#) [Analyze](#)

| | | |
|--|----------------------------|------------------------------|
| Network Access Scope ID nis-0a02bf937c2cd6bd7 | Name network-tgw-access | Description Access to tgw |
|--|----------------------------|------------------------------|

[▶ Network Access Scope definition](#)

[Latest analysis](#) [Past analyses](#) [Tags](#)

Analysis details [Export findings ▾](#) [Delete analysis](#)

| | | | | |
|---|---|---|---|----------------------------------|
| Analysis ID nisa-0a6f38eac8f1c379d | Last analysis date July 6, 2023, 15:49 (UTC+12:00) | Last analysis result Findings detected | Analysis status Complete | Network Interfaces analyzed 6 |
|---|---|---|---|----------------------------------|

Testing Networks - III

TGW Route Analyser

- AWS Transit Gateway - connect VPCs from multiple internal and external accounts to your AWS environment.
- How do you test this?
- VPC -> Network Manager -> Create a Global Network -> Route Analyser

The screenshot shows the AWS Network Manager Route Analyzer interface. The navigation path is: Network Manager > Global networks > test-global-network > Transit gateway network > Route Analyzer. The Route Analyzer tab is selected. The configuration form is titled "test-global-network Route Analyzer" and includes the following fields:

| Source | Destination |
|---|--|
| Transit gateway demo-tgw | Transit gateway demo-tgw |
| Transit gateway attachment ss-vpc-attach | Transit gateway attachment tgw-attach-0075e8ea9da95ad88 |
| IP address IPv4 or IPv6 address 10.1.130.92 | IP address IPv4 or IPv6 address 10.0.132.113 |

Below the configuration fields are two checkboxes:

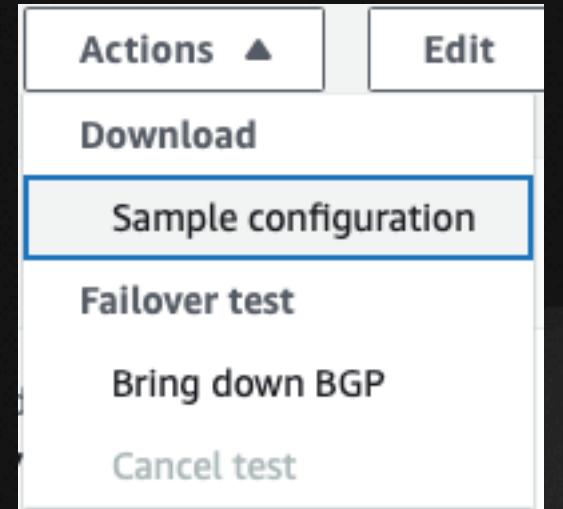
- Include return path in results
- Middlebox appliance? [Info](#) If selected, state those that are known in the results

You can visualize and monitor your Transit Gateway(s) from the AWS Network Manager [Info](#). Register your Transit Gateway by creating a global network [Info](#) to get started.

Bonus {not in the live demo :(}

Failover testing your Direct Connect connections

- I didn't know this until recently.
- Test virtual interfaces
- You can failover-test your Direct Connect connections.
- This is probably one of your acceptance criteria for a HA connection between your on-prem and AWS.
- https://docs.aws.amazon.com/directconnect/latest/UserGuide/resiliency_failover.html



Start failure test

⚠ Failure testing puts the virtual interface in a down state and will cause an outage if you have not configured redundancy. Failure testing will put virtual interface dxvif-fh5uteas in an induced failure state by putting its BGP peerings into a down state.

Test maximum time (minutes) - *optional*

Valid ranges are 1 - 4320 minutes. The default time is 180 minutes.

To confirm the test, type *Confirm* in the field below.

Cancel **Confirm**

Live Demo Time

Thank You

Find me - “Hitarth Asrani” on LinkedIn