Improve Elastic Cloud security with AWS PrivateLink and IP filtering

Shubha Anjur Tupil (Cloud PM)
Pieter Humphrey (Cloud PMM)
Agenda

1. What are traffic filters on Elastic Cloud?
2. What problems do they solve for customers?
3. Pricing, Subscriptions, and Data Transfer
4. Getting started and Demo
5. Summary
What are traffic filters?

**IP filtering** - control the inbound IP addresses or address ranges that can access your Elastic Cloud deployments

**AWS PrivateLink** - Secure connection between Elastic Cloud VPC and AWS services via private endpoints, (versus routing to public endpoints for AWS services)
Why are traffic filters important?

Security comes in layers

• Principle of least privilege

• Traffic filters add network layer security controls

• Address concerns around secure connectivity and peering options
Why is AWS PrivateLink important?

- Simplifies network management and access controls: use security groups and IAM policies to manage access to PrivateLink endpoints
- Connect via a private IP address
- PrivateLink is the preferred connection type for AWS services
Why is IP filtering important?

- PrivateLink securely connects a Customer VPC to private AWS services endpoints
- IP filtering operates on any network, on any cloud provider, restricting access based on IP address range(s).
- Common InfoSec requirement
So... how is it priced?

- Available to all Elastic Cloud subscription tiers
- No additional charges from Elastic
  - AWS PrivateLink incurs additional expenses on the customer’s AWS account, directly paid to Amazon.
  - Per VPC endpoint per AZ ($/hour) + Per GB data processed ($).
  - AWS has a pricing calculator on their website.
Mythbusters: PrivateLink and Data transfer charges

Will AWS PrivateLink help you save on data transfer costs?

- Talk to your AWS Representative about their data transfer pricing →

- What have we learned so far?
  - It’s similarly priced to intra-region data transfer charges.
  - But if you are using a NAT gateway, it is cheaper.
Getting Started with Traffic Filters

1. Setup AWS infrastructure
   - PrivateLink Endpoint
   - DNS record (optional)

2. Setup Elastic Cloud
   - Make PrivateLink Filter
   - Make IP Filter

3. Apply filter to deployment(s)
   - Make once, apply anywhere
   - Apply one or both
Demo Time
Roadmap and more resources

Coming Soon:
Azure Private Link

Coming later: Private Service Connect for Google Cloud

Learn More:
- Elastic’s Release Blog
- Traffic Filters Documentation
- Signup today at cloud.elastic.co
Key takeaways

Improved security posture

AWS PrivateLink

• Secure connection between Elastic Cloud VPC and AWS services via private endpoints
• More for security versus cost savings in most cases

IP Filtering

• Works on any cloud provider, any network
• Allow/deny based on IP address or IP address range

Available in all cloud subscriptions
Thank You

Search. Observe. Protect.