CISCO
SECURE

At a Glance
Cisco Public

Network Monitoring in AWS Virtual Private Cloud Environments

Using cloud servers and network infrastructure clearly provides many significant and well-known benefits. However, many companies needed additional network monitoring capabilities.

Why is this? When you operate your own switches and routers, you have tools like mirror ports and NetFlow data, which can be used to analyze overall security and performance. In a cloud environment, these options have not been available. Additionally, monitoring network traffic on cloud servers traditionally required an agent-based approach where each machine needed to have software installed to collect traffic records. This approach simply doesn't work if the machine can't run the software agent.

Now there's a new option for Amazon Web Services (AWS) customers who operate virtual private cloud (VPC) networks. AWS recently introduced VPC Flow Logs, which facilitate logging of all the IP traffic to, from, and across your network. These logs are stored as records in special Amazon CloudWatch log groups and provide the same kind of information as NetFlow data.

Specifically, AWS VPC Flow Logs contain the following information:

- Which IP entities are communicating inside and outside the VPC
- Which protocols (such as TCP and UDP) are being used
- How much traffic is sent and received by each entity
- Whether the flow was allowed or blocked by the security policy

VPC Flow Logs + entity modeling = improved security monitoring

Perhaps the most significant advantage is that you can use VPC Flow Logs as the input for entity modeling. Now, Secure Cloud Analytics (formerly Stealthwatch Cloud) can automatically retrieve VPC Flow Logs as a primary or supplementary data source for entity modeling. This means you can now monitor network activity in a cloud environment and increase your security.

Using VPC Flow Logs for security monitoring in a virtual private cloud environment provides multiple advantages over previous techniques:

- Now there is no need to deploy monitoring agents to each of the Amazon Elastic Compute Cloud (EC2) instances in the VPC environment.
- Machines that cannot run an agent, such as some Windows server or private Redshift clusters, can be monitored transparently.
- Traffic records do not need to be routed out of the VPC through an intermediate host. Machines that don't need to connect to the Internet don't need to send their data outside the private network.

For more information

Learn more about Secure Cloud Analytics can use VPC Flow Logs to protect your cloud environment at https://www.cisco.com/go/secure-cloud-analytics.