observable networks

Observable Networks is now a part of Cisco.

amazon web services Partner Network
ADVANCED TECHNOLOGY PARTNER

Network Monitoring in AWS Virtual Private Cloud Environments

Observable's Dynamic Endpoint Modeling security solution can automatically retrieve VPC Flow Logs as a primary or supplementary data source.

Using cloud servers and network infrastructure clearly provides many significant and well-known benefits. However, until very recently, they did come with one major disadvantage: Very limited 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. Amazon recently introduced VPC Flow Logs, which enable logging of all the IP traffic to, from, and across your network. These logs are stored as records in special CloudWatch Log groups and provide the same kind of information as NetFlow data.

Specifically, AWS VPC Flow Logs contain the following information:

- Which IP endpoints 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 endpoint
- Whether the flow was allowed or blocked by the security policy

Learn more about network monitoring in AWS virtual private cloud environments

- **The Observable blog:** We have written a few articles related to AWS VPC Flow Logs. Please visit the Observable blog for more information: https://observable. net/blog/
- **Observable setup guide:** To learn more about using VPC Flow Logs with our Dynamic Endpoint Modeling solution, please, download our setup guide: https://observable.net/storage/docs/ObservableNetworks-AWS-EC2-and-VPC-DeploymentGuide.pdf
- **Dynamic Endpoint Modeling:** For more on Observable's Dynamic Endpoint Modeling, please visit https://observable.net/solution/
- **Free trial:** To get even better visibility into your network, please sign up for our free Dynamic Endpoint Modeling trial: https://observable.net/trial/

VPC Flow Logs + endpoint modeling = improved security monitoring.

Perhaps the most significant advantage is that VPC Flow Logs can be used as the input for endpoint modeling. Now, Observable's Dynamic Endpoint Modeling security solution can automatically retrieve VPC Flow Logs as a primary or supplementary data source. 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 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.

Observable Networks hopes to see VPC Flow Logs evolve to provide even richer data about network traffic and hope other providers create even more of these tools to their customers.

Learn more at www.observable.net.

observable networks

Observable Networks is now a part of Cisco.

CISCO

For further information contact us at **info@observable.net** or visit **www.observable.net**