TECH BRIEF

SKYBOX SECURITY AND AMAZON WEB SERVICES

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud in a virtual network that you define. You have control over your virtual networking environment, including IP address range, creation of subnets and configuration of route tables and network gateways. Additionally Amazon VPC offers multiple layers of built-in security and a virtual private network (VPN) connection to your corporate datacenter.

But it's important to remember, while Amazon is responsible for the security of the AWS Cloud, your are responsible for the security of the data within your Amazon VPC.

AWS and VPC represent a shift in network design and implementation, replacing your need to manage any physical hardware (and IP addresses) with purely logical management tasks. However, network security, auditing and compliance requirements of typical network infrastructure are still important areas of focus.

The Skybox® Security platform can be easily configured to connect with your Amazon VPC to give you seamless visibility across your on-prem network and the cloud. By ingesting Amazon VPC data into your Skybox solution, you have the means to assess the security controls of your cloud-based assets and analyze both east-west and north-south traffic.

This also helps extend traditional security tasks such as access analysis, policy analysis and vulnerability management from on-prem networks to the cloud, ensure workloads within Amazon VPC are properly secured and compliant.

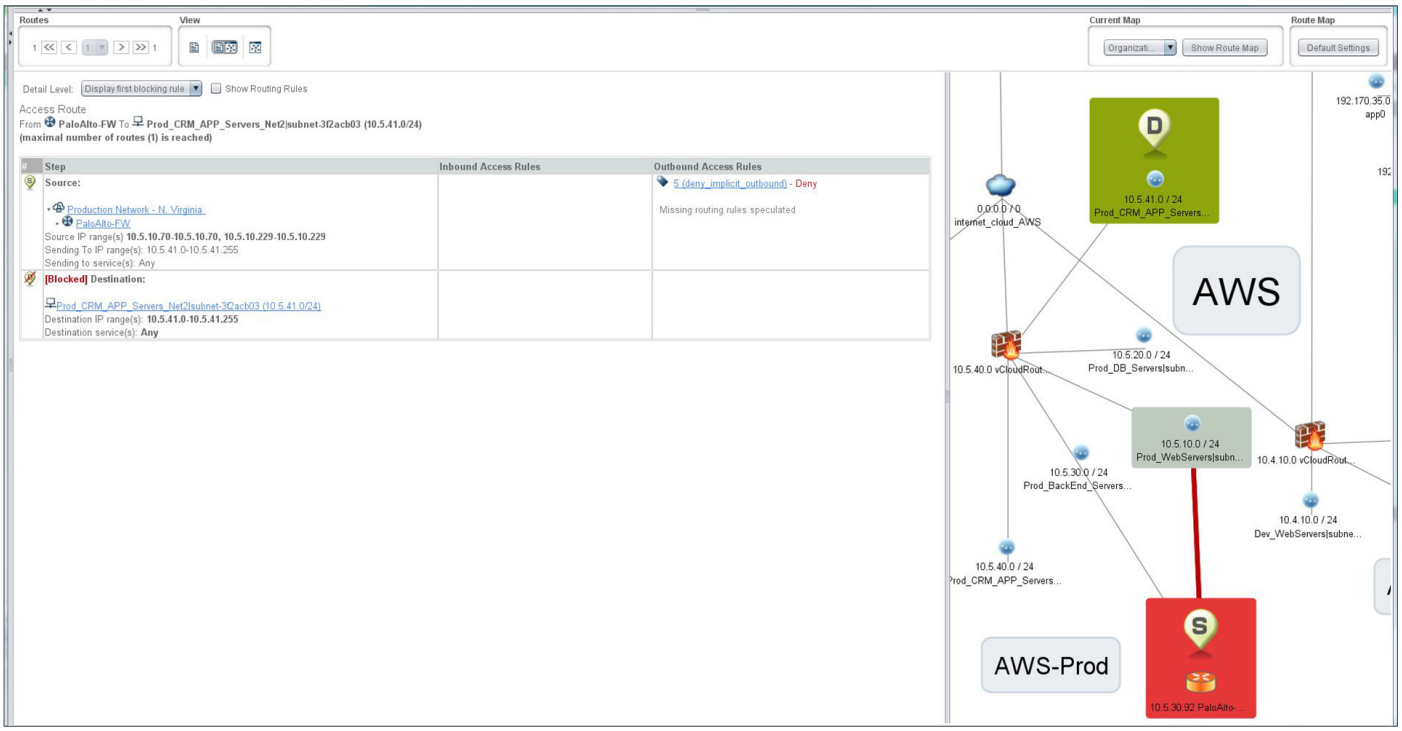
Connecting Skybox with AWS VPC is easy: simply select the "AWS connector" task in Skybox to automatically collect data for your specific AWS cloud(s) using the AWS API.

Skybox will automatically collect and import collected AWS VPC data into the Skybox model:

- Gateways (virtual private cloud connections, internet gateways, customer gateways)
- Routers (route tables)
- Access control lists
- Network address translation
- Elastic load balancing
- Subnets
- Security group
- Assets (virtual machines)

After the data is gathered, Skybox adds it to the network model and maps each VPC, visualizing the internal details. Skybox models the virtual firewalls that represent entry/exit points for the cloud containing routing to the network and NAT for public addresses to internal addresses. Network and asset information is also created using **security tags**. In addition, Skybox incorporates vulnerability and threat information into this model to understand how attacks might play out within a network or how such risks are shared between the on-prem network and the cloud.

The Skybox® Security Suite provides you the capabilities you need to visualize your network, assess your security controls and demonstrate compliance whether you networks are physical, public or private clouds or a mix of all three.



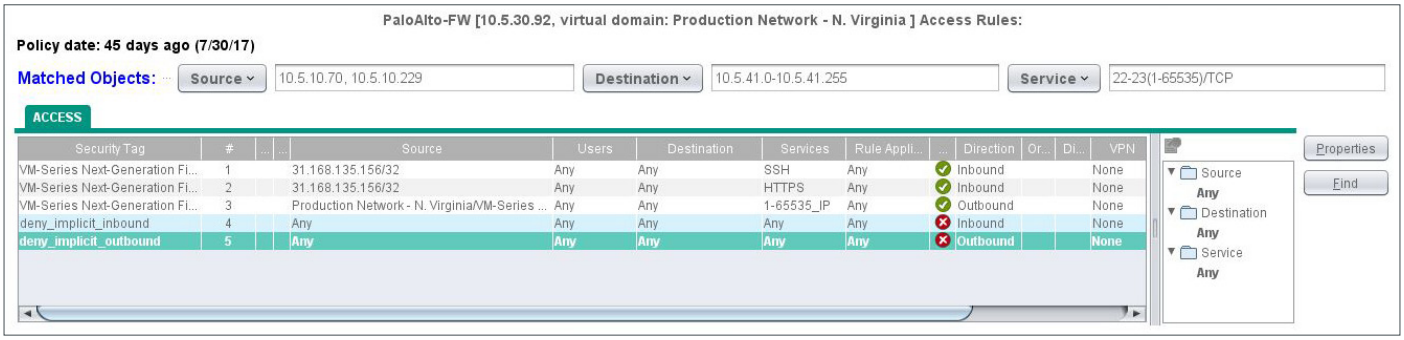


FIG 1 and 2: An example of a Skybox® Access Analyzer query in the Skybox Network Assurance module. (Upper) A model of a blocked access path and related security controls. (Lower) Drill-down of rules controlling access.

The Skybox® Security Suite provides you the capabilities you need to visualize your network, assess your security controls and demonstrate compliance whether you networks are physical, public or private clouds or a mix of all three.

To learn more about how Skybox can help you manage security in your hybrid cloud infrastructure, visit our website: **www.skyboxsecurity.com**.

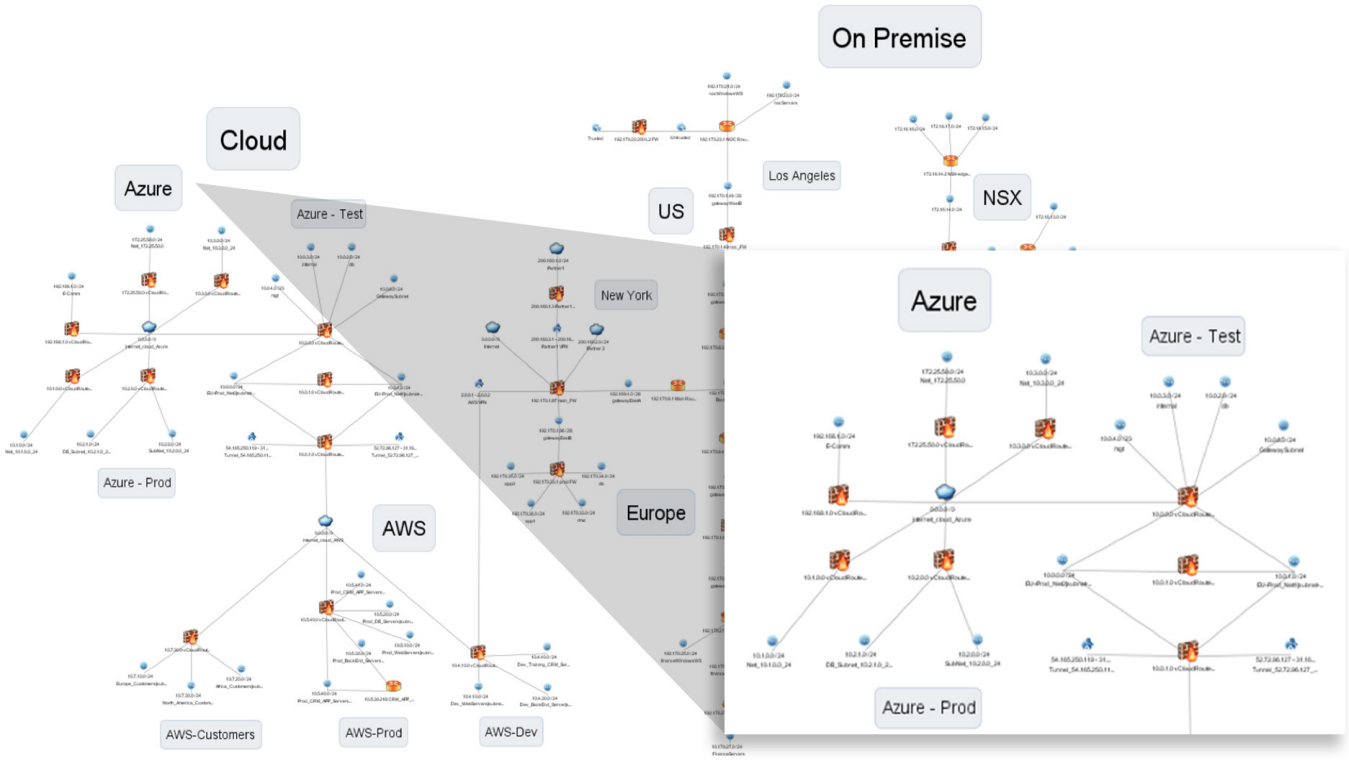


Fig. 3: The Skybox model showing on-prem, virtual and cloud networks as well as the network connections and security controls between them.

ABOUT SKYBOX SECURITY

At Skybox, we remove complexities from cybersecurity management. By integrating data, delivering new insights and unifying processes, we help you control security without restricting business agility. Our comprehensive solution unites security perspectives into the big picture, minimizes risk and empowers security programs to move to the next level.