TECH BRIEF

SKYBOX SECURITY AND AZURE

SECURING DATA WITHIN YOUR AZURE VNET

Microsoft Azure Virtual Network (VNet) lets you provision a logically isolated section of the Microsoft Azure 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, The Azure Virtual Network 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 Microsoft is responsible for the security *of* the Azure Cloud, you are responsible for the security of the data *within* your Azure VNet.

Azure VNet represents 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 concerns, auditing and compliance requirements of typical network infrastructure still remain.

The Skybox® Security platform can be easily integrated with your Azure VNet to give you seamless visibility across your physical, virtual and multi-cloud networks. By integrating Azure VNet 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 physical network security tasks such as access analysis, policy analysis and vulnerability management to the cloud.

Skybox integrates easily with Azure VNet; simply select the "Azure connector" task to automatically collect data for your specific Azure cloud(s) using the Microsoft Azure API.

Skybox will automatically collect and import it to the Skybox network 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 VNet, 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**.

Skybox also incorporates vulnerability and threat information into this model to understand how attacks might play out within or between networks. An example of a Skybox™ Access Analyzer query in the Skybox® Network Assurance module is demonstrated on this page.

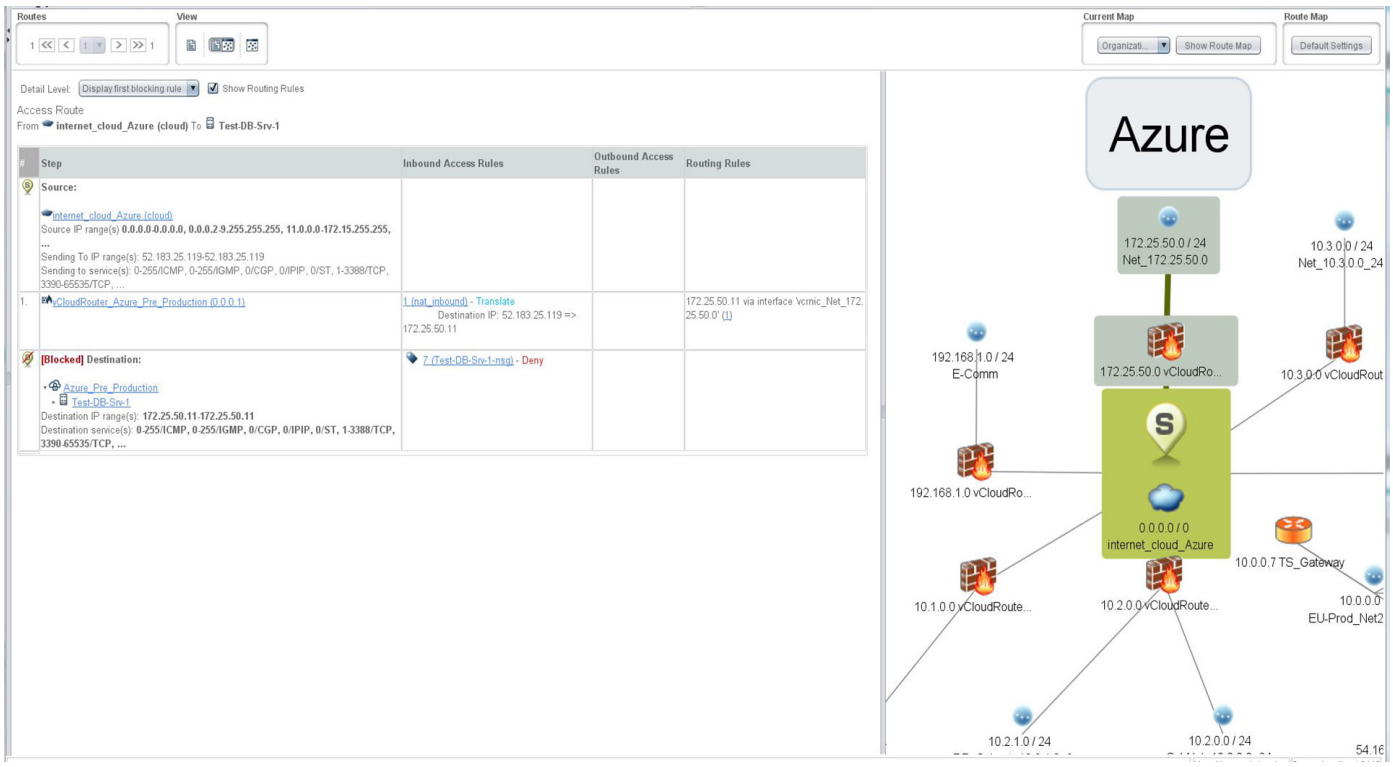

Fig. 1: A model of a blocked access path and related security controls.

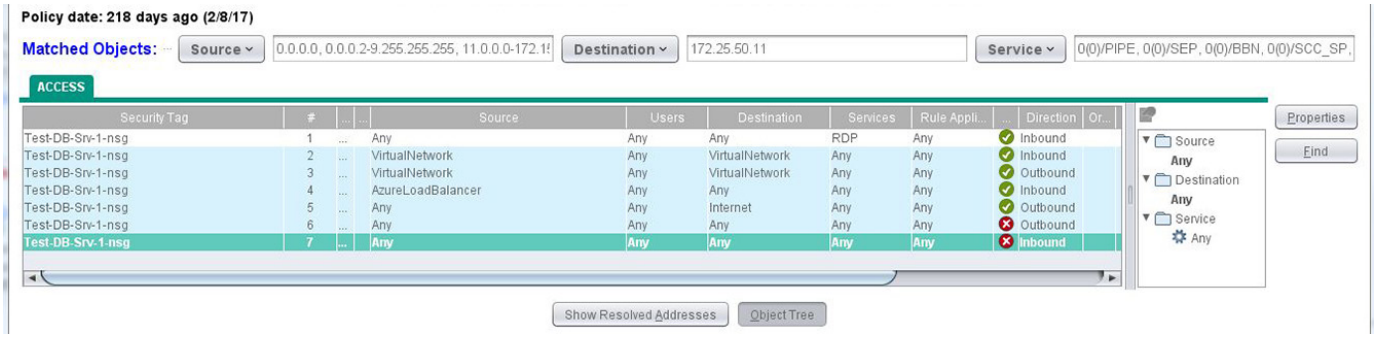

Fig. 2: Drill-down of rules controlling access.

The Skybox® Security Suite provides you the capabilities you need to visualize your network, assess your security controls and demonstrate compliance whether your networks are physical, virtual or both.

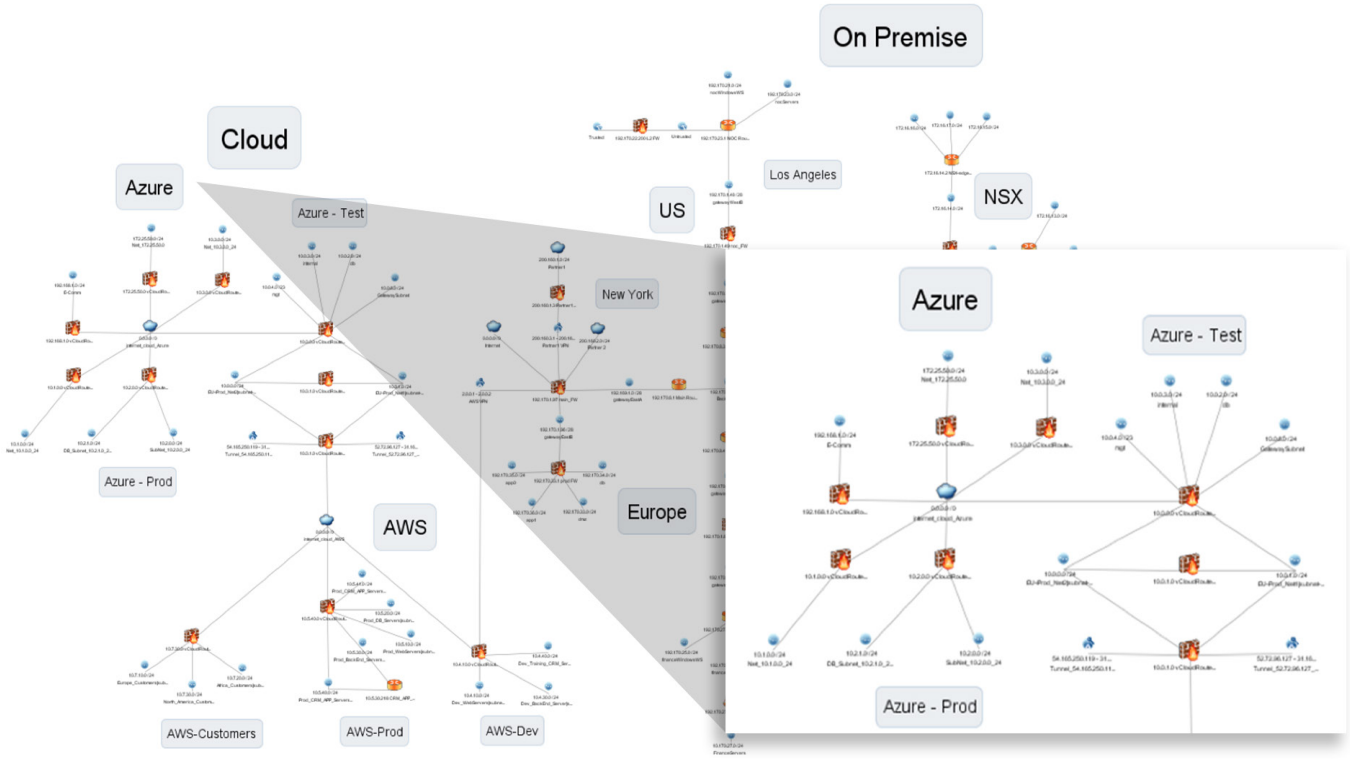

Fig. 3: The Skybox model showing physical, virtual and multi-cloud networks as well as the network connections and security controls between them.

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.

www.skyboxsecurity.com