NetBrain® Integrated Edition 10.0

Public Cloud Support

Version 10.0 | Last Updated 2021-01-27

Copyright ©2004-2021 NetBrain Technologies, Inc. All rights reserved.

Contents

1. Public Cloud Support

As more and more IT workloads are being moved to the public cloud, operating the public cloud environment becomes a very changeling task for IT specialists. Even if the automation and agility during the provisioning process have been greatly improved, it is not the same when it comes to the manageability of the pubic cloud environment. The main challenges of managing public cloud consists of the following aspects:

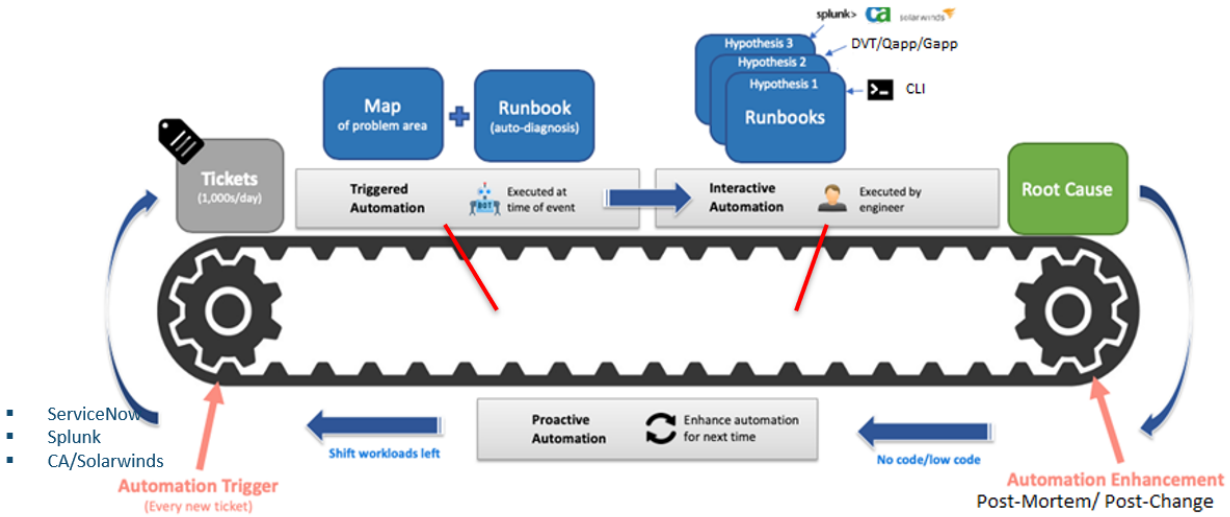
- **Lack of visibility**: agile provision of cloud resources makes visibility difficult using the traditional manual method.
- **Huge number of accounts and subscriptions**: to comply with the security requirements, you may have huge number of accounts and subscriptions that used by different teams, managing all resources scattered in all these accounts and subscriptions bring huge management burden to the team when it comes to the troubleshooting cloud issues.
- **Multi-cloud and hybrid-cloud environments**: East-West Traffic supporting key application often traverse physical data center, SDN data center and public cloud. You may also have different public cloud providers to prevent vendor lock-in. As a result, a lot of organizations bring multiple public cloud providers into their production use and you will need to understand different cloud provider's uniqueness.
- **Collaboration within different teams and customers**: as the application that traverses through your network may involves multiple teams: network team, security team, cloud team server team and application team. When problem occurs, you may need to involve all the related teams together to figure out the root cause.

The need to have the visibility into the public cloud becomes very critical. In the R10 version we have built the support for AWS and Azure and the support consists of the following areas:

- **Auto Discovery:** with NetBrain's auto discovery function, NetBrain is able to discover public cloud resources and update the data periodically by leveraging the benchmark function.
- **Review network data and config with dynamic mapping**: like the way we do for traditional network and SDN network, we use API to access the public cloud environment and provide the data model which you can easily build the map based on the data model. The system has the ability to periodically retrieves the data from public cloud providers and update the data model accordingly.
- **Map application dependency across end-to-end network**: with the ability to build the data model for public cloud, SDN, SD-WAN, and also the traditional network, NetBrain is able to provide you the path analysis function across the entire network. NetBrain can check the routing table/security group/network ACL for all the networking objects along the path and display the checking result details.
- **SPOG access through cloud-native and 3rd party cloud management tools**: NetBrain has the ability to use Data View Template to display the cloud infrastructure data from AWS API, display the cloud monitoring data from AWS Cloud Watch and Azure monitoring, and also we can integrate with any of your cloud monitoring tools, Datadog, Splunk, Dynatrace for example, to overlay the monitoring metrics/logging information on the NetBrain map.
- **Automate Troubleshooting with Runbook**: The support for Runbook Automation is also expanded to Runbook Automation natively, with the support for public cloud, you are able to build different Runbooks according to your public cloud troubleshooting scenarios and can leverage the Automation within NetBrain's entire automation reference workflow.

With all these functions built for public cloud, operating public cloud network which consisting hundreds of even thousands of public cloud account becomes easier. The reference workflow for the hybrid/multi-cloud

network remains the same to give you unified workflow for the entire network. We'll use the following diagram to help you understand the workflow of using NetBrain to troubleshoot the ticket in your hybrid/multi-cloud environment:

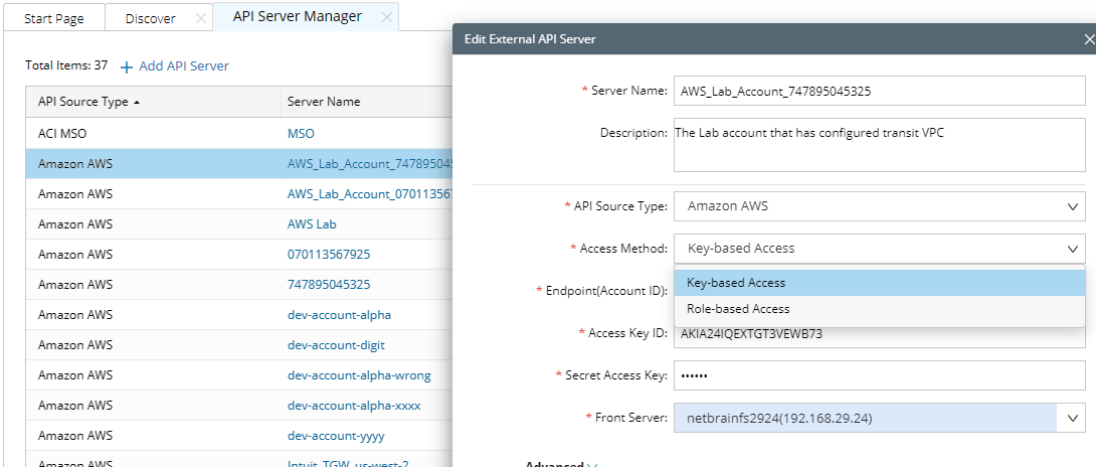


- **Tickets Creation**: when a ticket is created in ServiceNow or Remedy, it can send the event to NetBrain system for integration.
- **Triggered Automation**: Upon receiving the event, NetBrain system can take the input (device name, source and destination IP addresses of your traffic flow) to create the map for the problem area, the similar concepts can be applied to hybrid/multi-cloud environment, NetBrain is able to map the entire network work hence it will help you gain the visibility of the entire network. Runbook automation is also supported in cloud environment and the automation can be used to analyze the hypothesis of the root cause in real time.
- **Interactive Automation**: the map created during the event and also the runbook analysis results can be leveraged by different teams (network team, cloud security team, application team) to collaborate and analyze the problem. NetBrain can help you troubleshoot the problem with the following functions:
    - **Data View Template**: you can leverage DVT to view the cloud monitoring information and also the metrics from other cloud management systems, such as Datadog, Splunk.
    - **Runbook Analysis**: you can leverage different Runbooks to execute different tasks according to your public cloud architecture and different use cases.
    - **Data Comparation**: since NetBrain captures valuable historical data of your cloud environment, you can compare the data in historical security groups/route tables/Network ACLs etc.
    - **Incident Portal/Function portal**: you can use the portal to share the findings with other teams who don't have access to the NetBrain environment.
- **Problem resolution and Post-mortem/post-change:** After the problem is resolved, you can create the Runbook to share the troubleshooting knowledge so next time when a similar problem happens, the root cause can be identified much quicker.

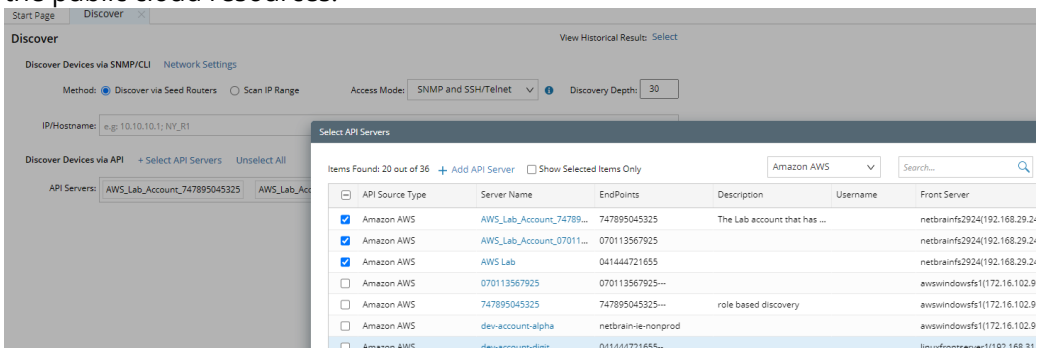
1.1. Discover Public Cloud Resources

To discover the public cloud resources, you will need to have the related API access to public cloud providers. The general steps for setting public cloud access are as follows:

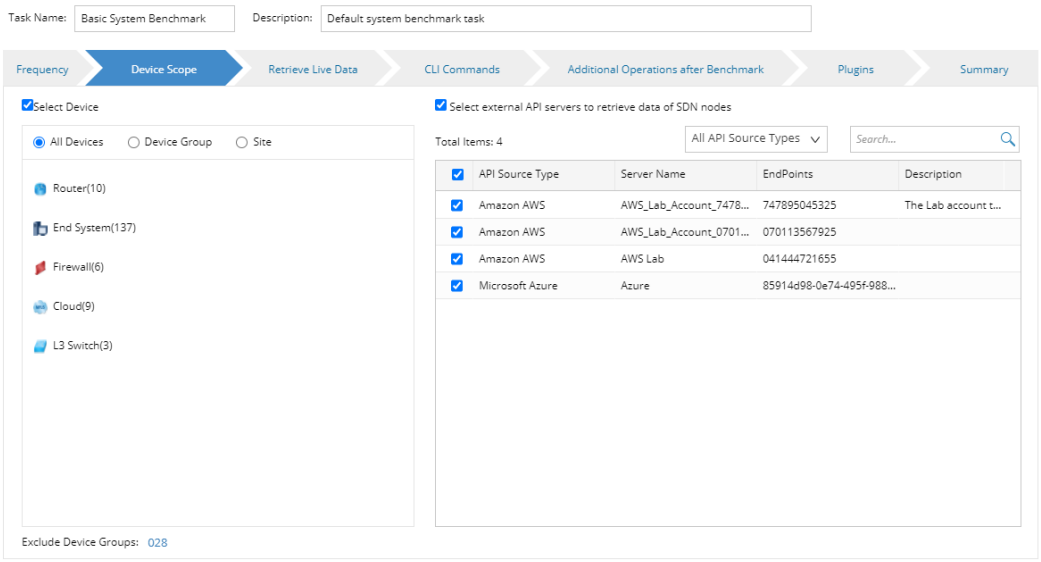
1. **Setting up API access**: you will need to use either key-based access or role-based access method to discover public cloud resources.



2. **Discover Public Cloud resources:** run the discovery function with the specified accounts to discover the public cloud resources.



3. **Setting up benchmark tasks**: you will need to set up benchmark tasks to retrieve the public cloud resources periodically.



For the complete instruction on how to set up the API access and discover the public cloud resources, please refer to the following document:

- AWS Quick Setup Guide
- Azure Quick Setup Guide

NetBrain's discovery and benchmark functions can periodically capture the public cloud configuration status and update the data model accordingly.

At current stage, the AWS support mainly focuses on the networking objects and the pertaining objects. The following is a complete list of all supported networking objects:

- AWS Supported Networking Objects
- Azure Supported Networking Objects

1.1.1.AWS Supported Networking Objects

ITEMS	SUPPORTED TECHNOLOGY DETAILS	MAP	TOPOLOGY	PATH
VPC	• Security Group • Network ACL • ENI Interface details per VPC • VPC Sharing across Multiple Accounts • VPC Route Table • Ingress Routing	Yes	Yes	Yes
VPC PEERING	• VPC Peering within Same Accounts • Cross Account VPC Peering	Yes	Yes	Yes
INTERNET GATEWAY	• Private to Public IP Mapping Table	Yes	Yes	Yes

VIRTUAL PRIVATE GATEWAY	• Virtual Route Table (based on NetBrain's unique algorithm) • Cloudhub function • Site-2-Site VPN details	Yes	Yes	Yes
ELB (ALB/NLB)	• Target Group ○ IP/Instance as targets • Listener Table	Yes	Yes	Yes
NAT GATEWAY	• ENI interfaces provisioned for VPCs	Yes	Yes	Yes

AWS DIRECT CONNECT (DX ROUTER SUPPORT)	• Virtual Route Table for DX Router
	• Virtual Interfaces details
	  ○ Private virtual interface
	  ○ Transit virtual interface
	• Traffic engineering (As Path prepend, local preference for BPG community).
	• DX Connection details
	• LAG details
		Yes	Yes	Yes

DIRECT CONNECT GATEWAY	• Virtual Route Table • Allowed Prefix for VGW/TGW • Cross Account association to VGW/TGW	Yes	Yes	Yes
TRANSIT GATEWAY	• Transit Gateway attachments • Transit Gateway route tables • Transit Gateway associations • Transit Gateway propagation • Transit Gateway peering • ENI interfaces provisioned for VPCs • Transit Gateway sharing for VPC attachments	Yes	Yes	Yes
EC2 INSTANCE	• EC2 Data Details • Network Interface Details • Security Groups	Yes	Yes	Yes
NETWORK VIRTUAL APPLIANCES **(ASAV, CSR1000V, VEDGE ETC.)**	• Relationship to EC2 hosts • EC2 details	Yes	Yes	Yes
VPC ENDPOINT (GATEWAY ENDPOINT)		Yes		
VPC ENDPOINT (INTERFACE ENDPOINT) - PRIVATELINK	• ENI interfaces provisioned for VPCs	Yes		

1.1.2.Azure Supported Networking Objects

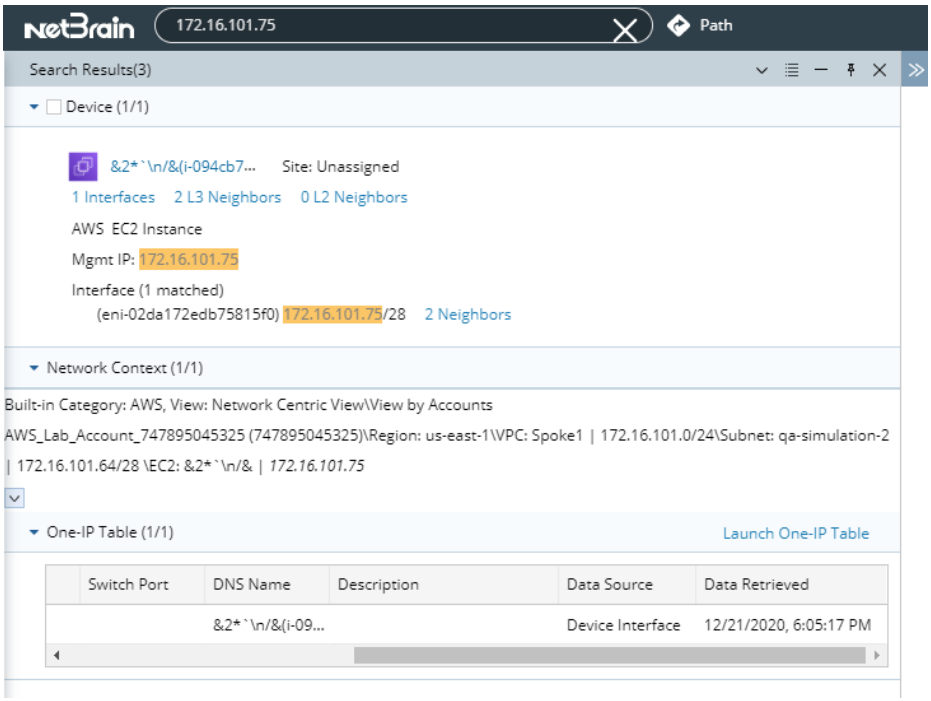
ITEMS	SUPPORTED TECHNOLOGY DETAILS	MAP	TOPOLOGY	PATH	UNSUPPORTED FEATURES
VIRTUAL MACHINE (VM)	• VNIC Interface details • VM Device details • Network Security Group (Interface Level)	Yes	Yes	Yes	
VIRTUAL NETWORK (VNET)	• Network Security Group (Subnet Level) • Application Security Group • Across Multiple Accounts • Across Multiple subscription • User Defined Route Table (UDR) • VNet Peering Table • VNIC Effective Route Table • Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes	
VNET PEERING	• VNet Peering within the same subscription • VNet Peering across Multiple subscriptions • VNet Peering within the same Account/Tenant • VNet Peering across Multiple Account/Tenant	Yes	Yes	Yes	
VIRTUAL NETWORK GATEWAY (VPN/EXPRESSROUTE GATWAY)	• VPN/ExpressRoute Gateway device details • Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes	
AZURE LOAD BALANCER (PUBLIC)	• Device details • Inbound NAT Rules Table • Load Balancing Rule Table • Outbound Rules Table • Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes	

AZURE LOAD BALANCER (INTERNAL)	• Device details • Inbound NAT Rules Table • Load Balancing Rule Table • Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes	
NAT GATEWAY	• Device details • NAT Table • Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes	
AZURE FIREWALL	• Device details • Network Rule Collection Table • DNAT Rule Collection Table • Application Rule Collection Table • Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes	
APPLICATION GATEWAY	• Device details • Listener Table • Rules Talbe • Http Setting Table • Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	NO	• OSI Layer 7 Path (URL/Http/Https)
NETWORK VIRTUAL APPLIANCES **(ASAV, CSR1000V, VEDGE ETC.)**	• Relationship to Virtual Machine host • Virtual Machine details	Yes	Yes	Yes	
INTERNET CLOUD	• Device details	Yes	Yes	Yes	• NCT route table • Path Originated from Internet
MPLS CLOUD	• Device details • Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes	
PRIVATE LINK		No	No	No	
PUBLIC SERVICE		No	No	No	

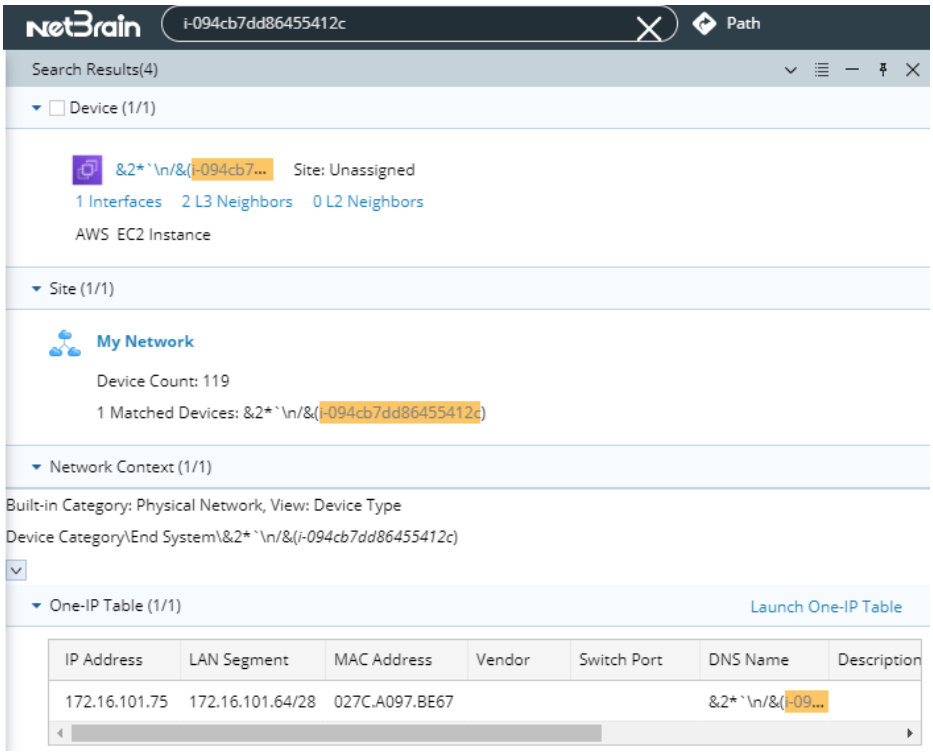
1.2. Map Public Cloud Resources

After your public cloud and on-prem networks are discovered, you will be able to view the related public cloud resources. There are different ways to view the related public cloud resources:

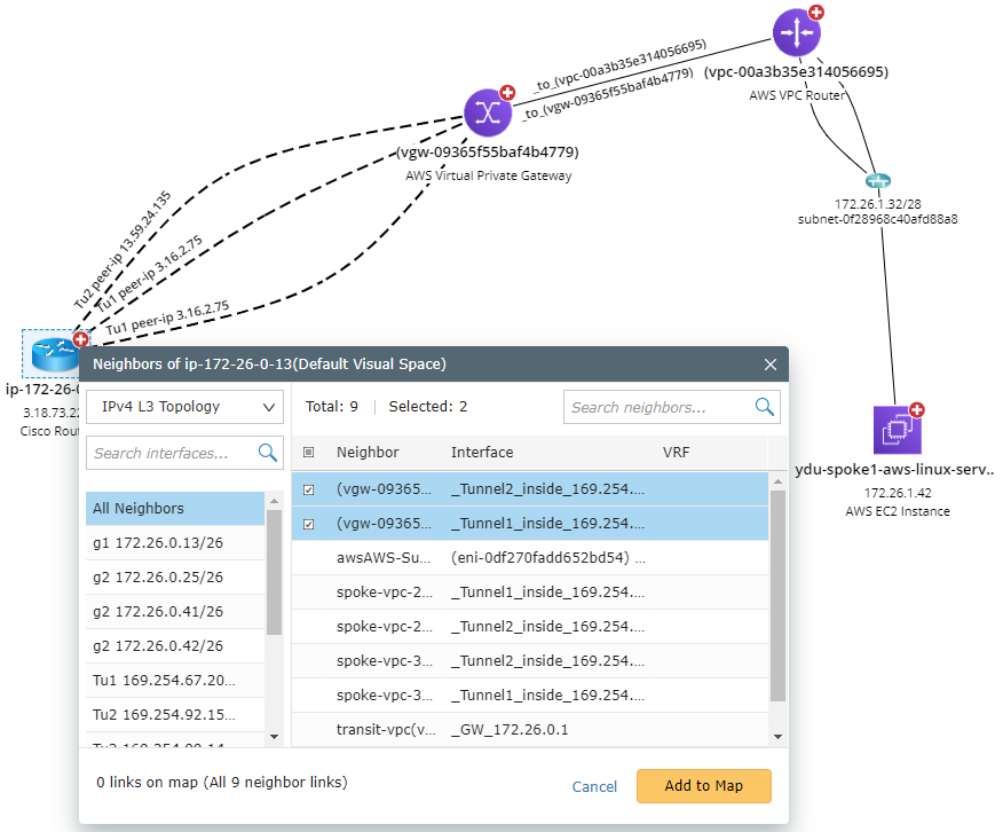
- **Network Pane**: network page gives you the resource view for a specific technology, whether that is your traditional network, SDN network or public cloud environment, we will cover more details in the following chapters.
- **Global Search**: through the global search, you can search for specific public objects with their name/ID, as the name and ID are searchable in the global search, this will help you quickly identify where the resource is located at and create maps based on the search results.
    - **Search by IP**



    - **Search by ID**



- **Map**: another way to find your public cloud resources is through the extend neighbor function, if you have your On-Prem devices connected to the public cloud environment, you can use the extend neighbor function to extend the neighbors.



1.2.1.AWS Network Tree

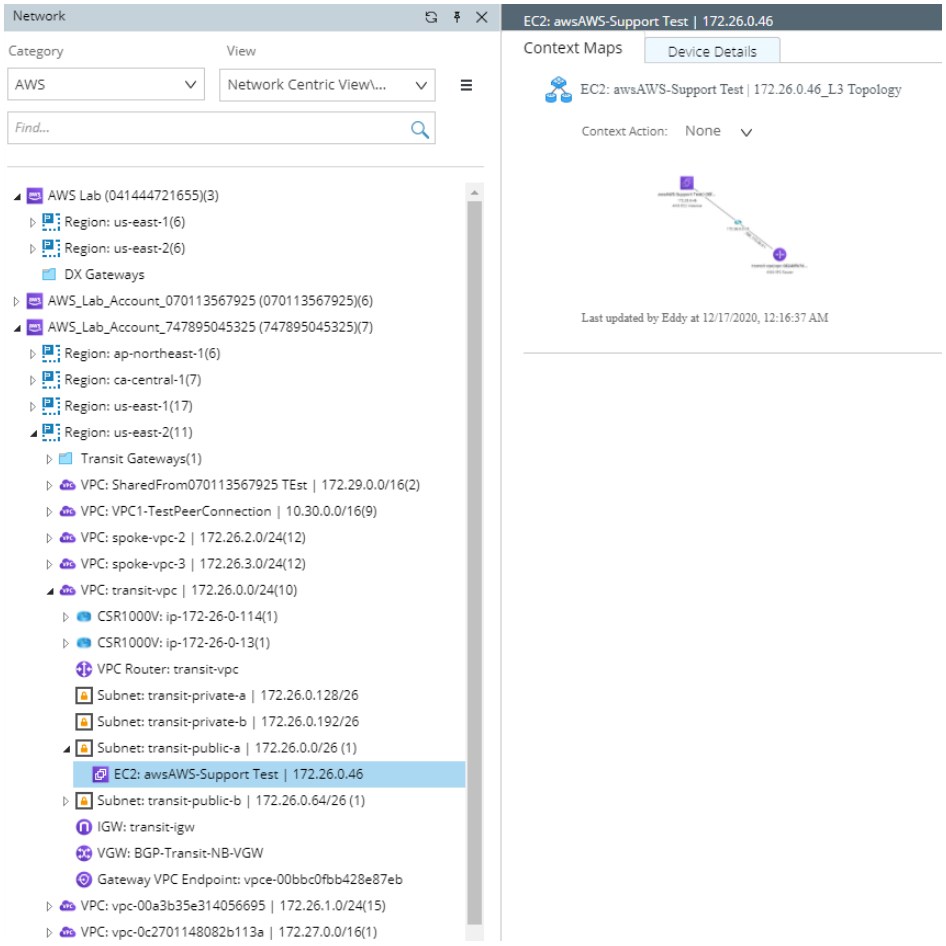
In the example below, you will have access to all of your accounts discovered in a single view:

Below is one hieratical view for the AWS resources:

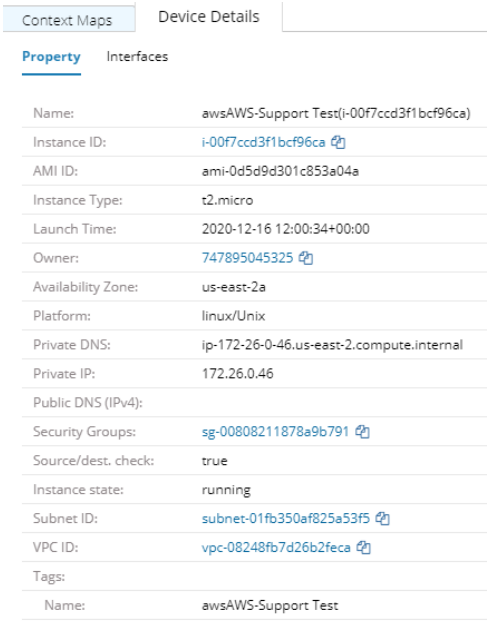
Account > Region > VPC > Subnet

You will also find the other networking objects as listed based on their hierarchy.

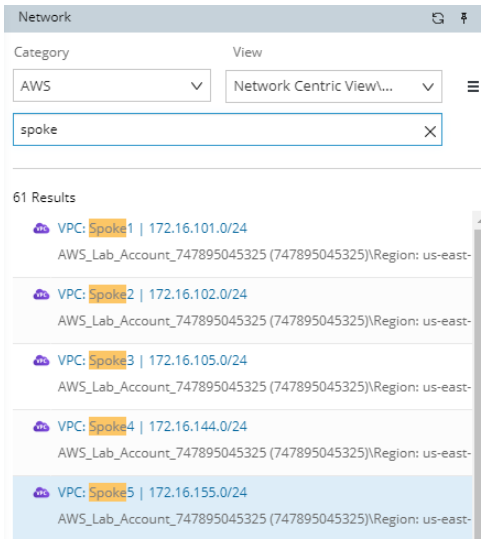
- Transit gateway is listed under regions as transit gateway is a reginal service that resides within a certain region.
- AWS direct connect gateways are logical components that can interconnect VGW and TGW from different regions, so they are listed under account.
- AWS direct connect router is a physical device that resides in certain direct connect locations, so it's listed under region.



From the details pane you can view the details for each object and the hyperlink will take you to the AWS console directly.

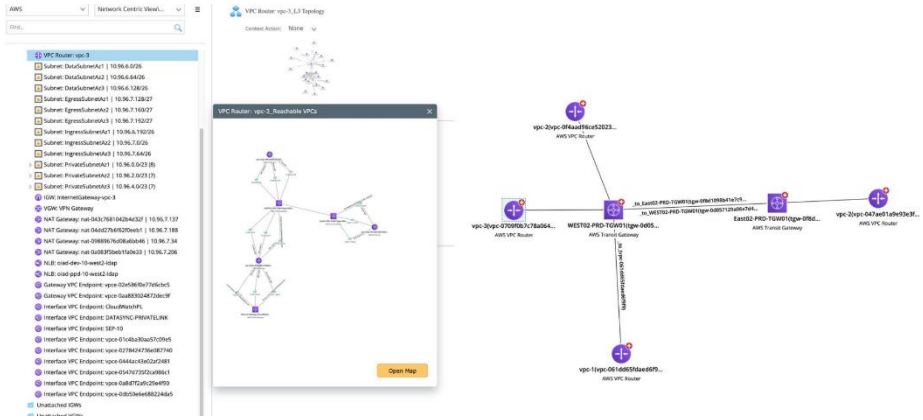


You can use the search function to view all matched results.



1.2.1.1. VPC Reachability Context Map

The following context map is to help you understand the reachability from VPC via the transit gateway.



1.2.2.Azure Network Tree

In the example below, you will have access to all of your tenants discovered in a single view:

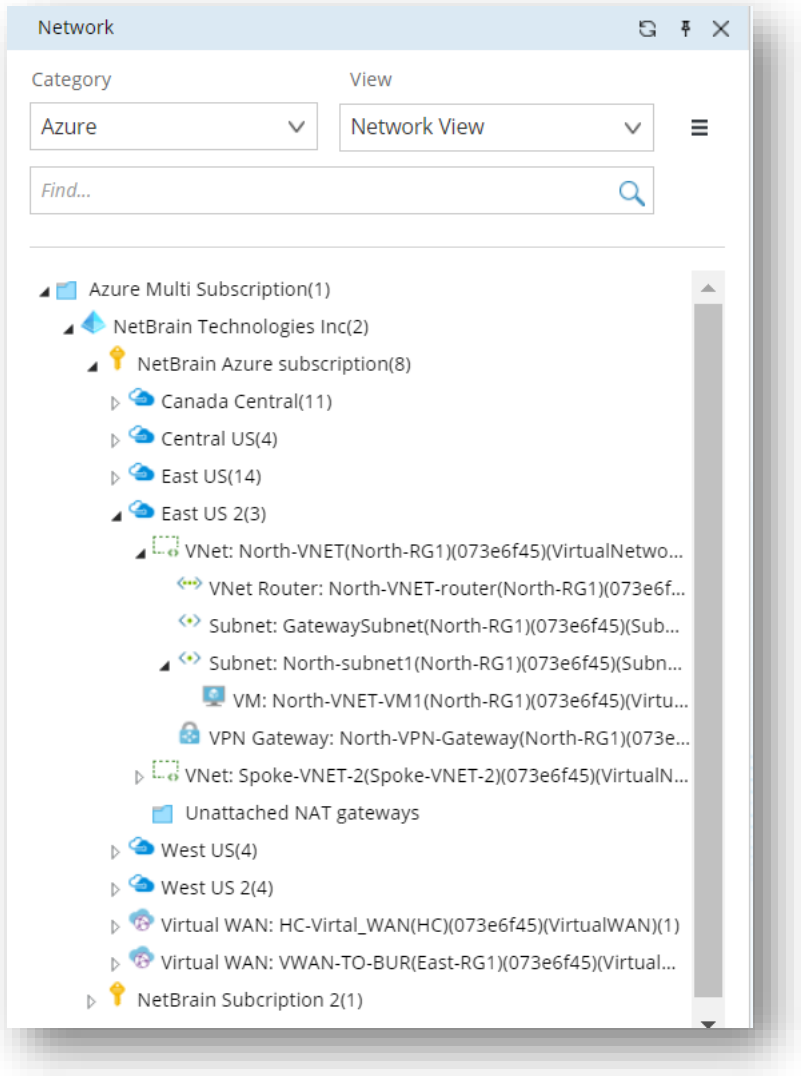
Below is an example of hieratical view for the Azure resources:

- Level 0: Tenant
  - Level 1: Subscription
    - Level 2: Region
      - Level 3: VNet
        - Level 4: Virtual Network Distributed Router
        - Level 4： Subnet
          - Level 5: Virtual machines
        - Level 4: VPN Gateway
        - Level 4: Express Route Gateway
        - Level 4: Application Gateway
        - Level 4: Azure Load Balancer(Internal)
        - Level 4: NAT Gateway
        - Level 4: Azure Firewall
      - Level 3: MSEE
      - Level 3: Azure Load Balancer (Public)
      - Level 3: Unassigned NAT Gateway
    - Level 2: Virtual WAN
      - level 3: Virtual WAN Hub
        - level 4: VPN Gateway for vHub
        - level 4: Express Route Gateway for vHub
        - level 4: Azure Firewall

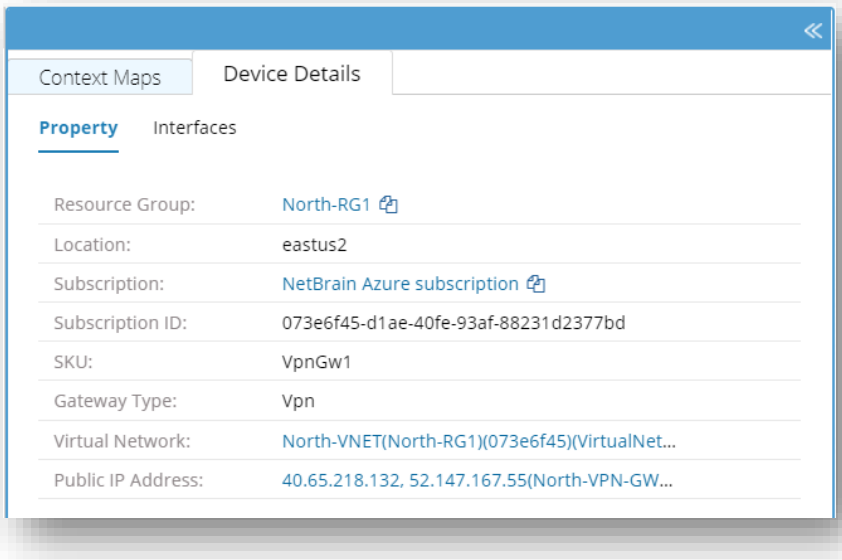
You can find the network objects listed in this hierarchy tree.

- The virtual network as a parent node to include sub node virtual network distributed router and subnet.
  - The virtual network distributed router is a NetBrain conceptual compoent to simulate virtual network as a network object to build relationship with other resources that belong to this virtual network.

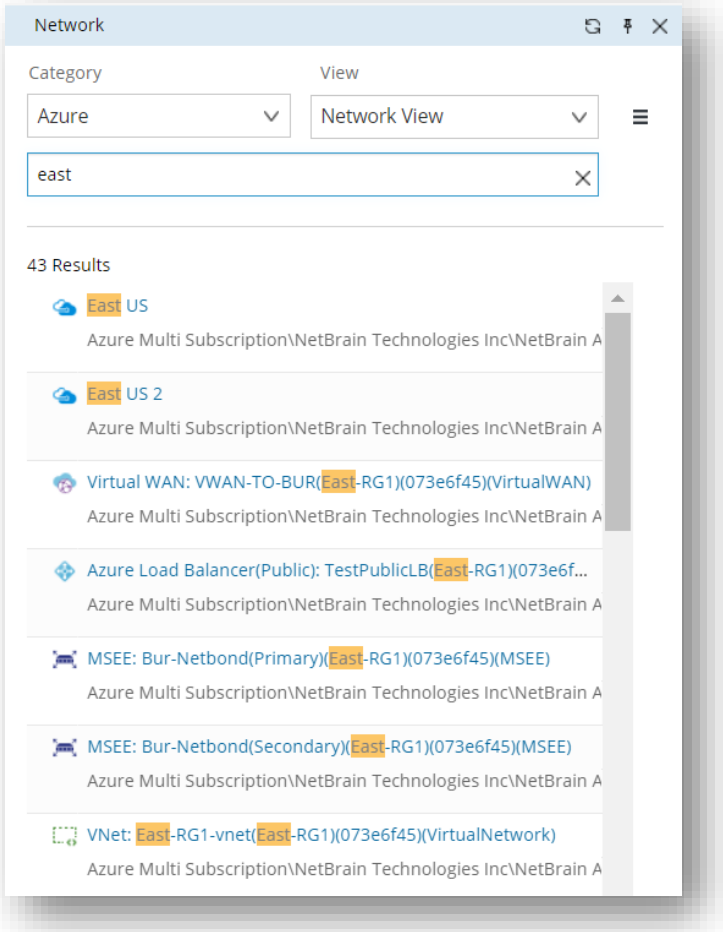
    - The virtual machine is listed under subnet that belong to this virtual network.
- The VPN gateway, ExpressRoute gateway, application gateway, Azure load balancer (internal), NAT gateway, Azure firewall are listed under virtual network which they belong to.
- The MSEE is simulated as a network object to connect with virtual network and on premise network, so it is listed under region.
- The Azure load balancer (public) might not belong to a certain virtual network, so it is listed under region.
- If the NAT gateway does not belong to any virtual network, it will be listed under region as an unassigned NAT gateway.
- The Virtual WAN is used to connect networks within different region, so it is listed under subscription. The virtual WAN hub is listed under virtual WAN, and the VPN gateway for vhub, ExpressRoute gateway for vhub and Azure firewall are listed under virtual WAN hub



From the details pane you can view the details for each object and the hyperlink will take you to the Azure console directly.

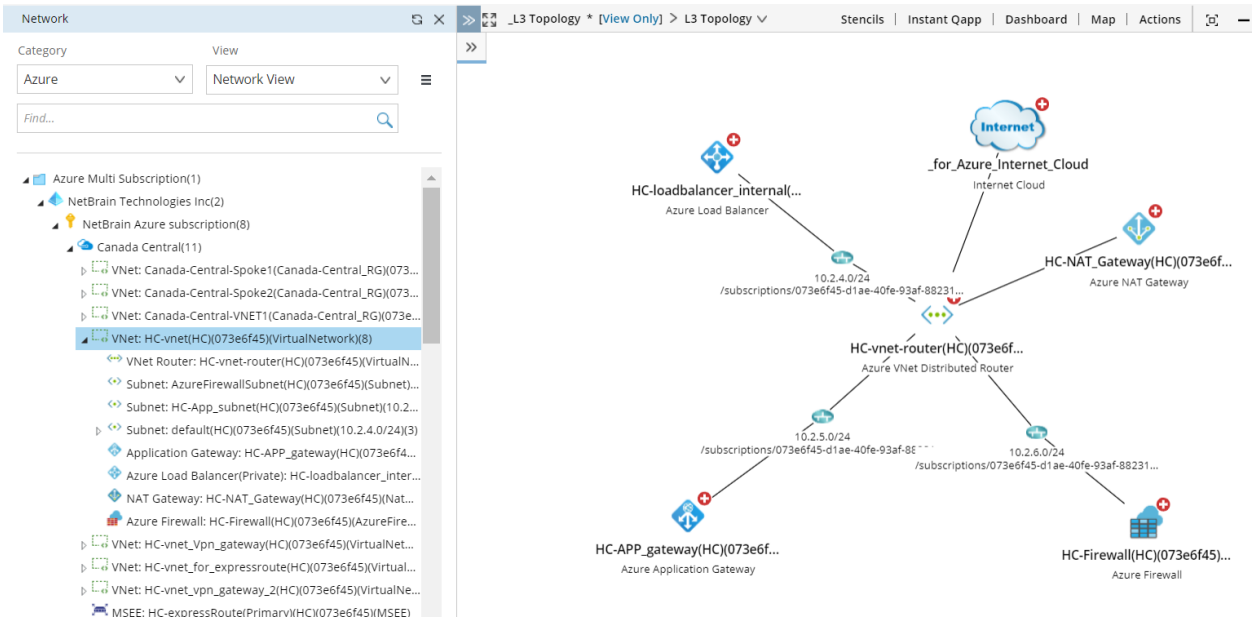


You can use the search function to view all matched results.



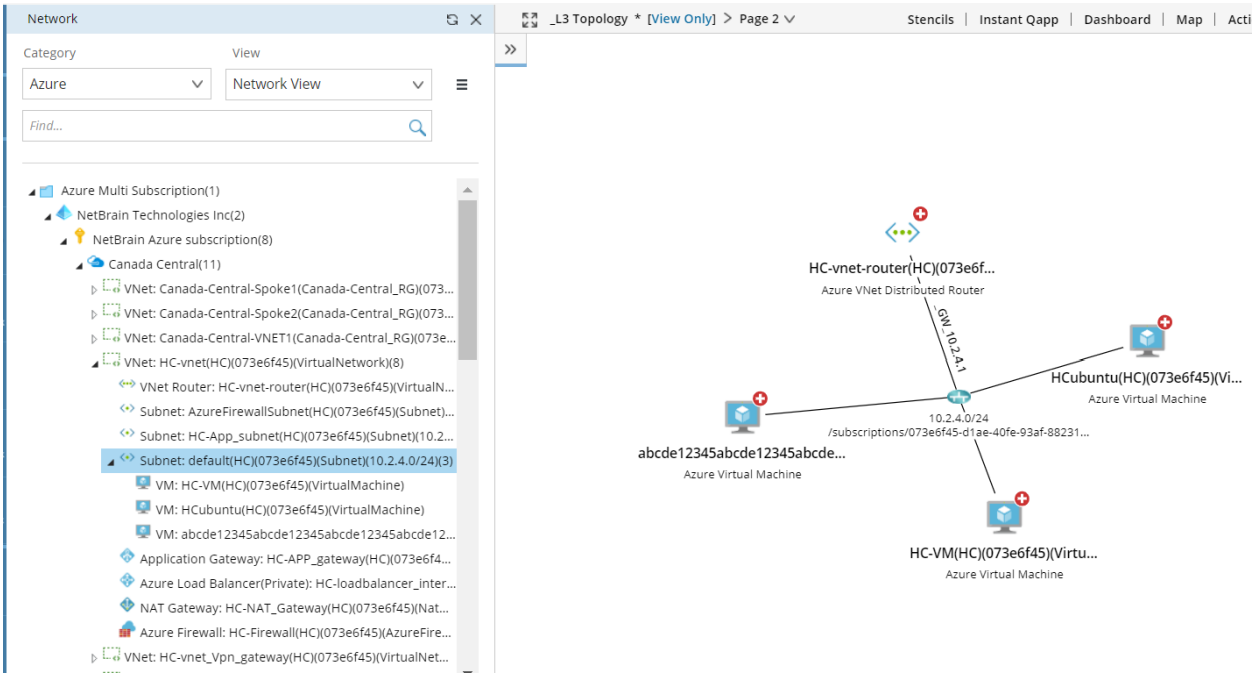
1.2.2.1. Virtual Network Context Map

The following context map is to help you understand the relationship of resources within the same virtual network. The virtual machine will not be mapped by default due to its massive number.



1.2.2.2. Subnet Context Map

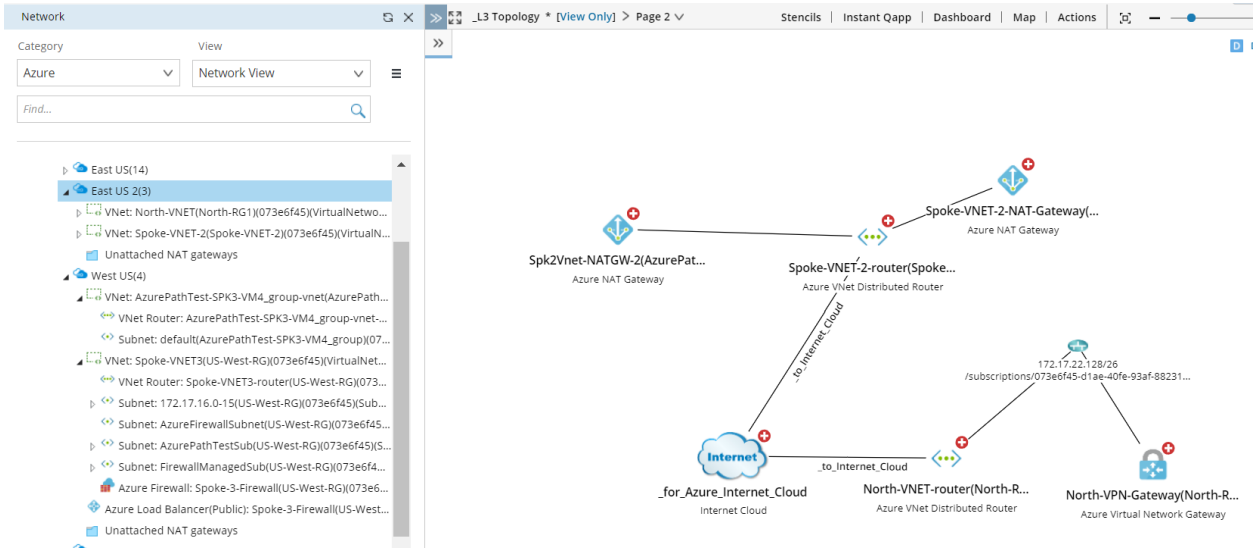
The following context map is to help you understand the virtual machine connecting to the same subnet within the virtual network.



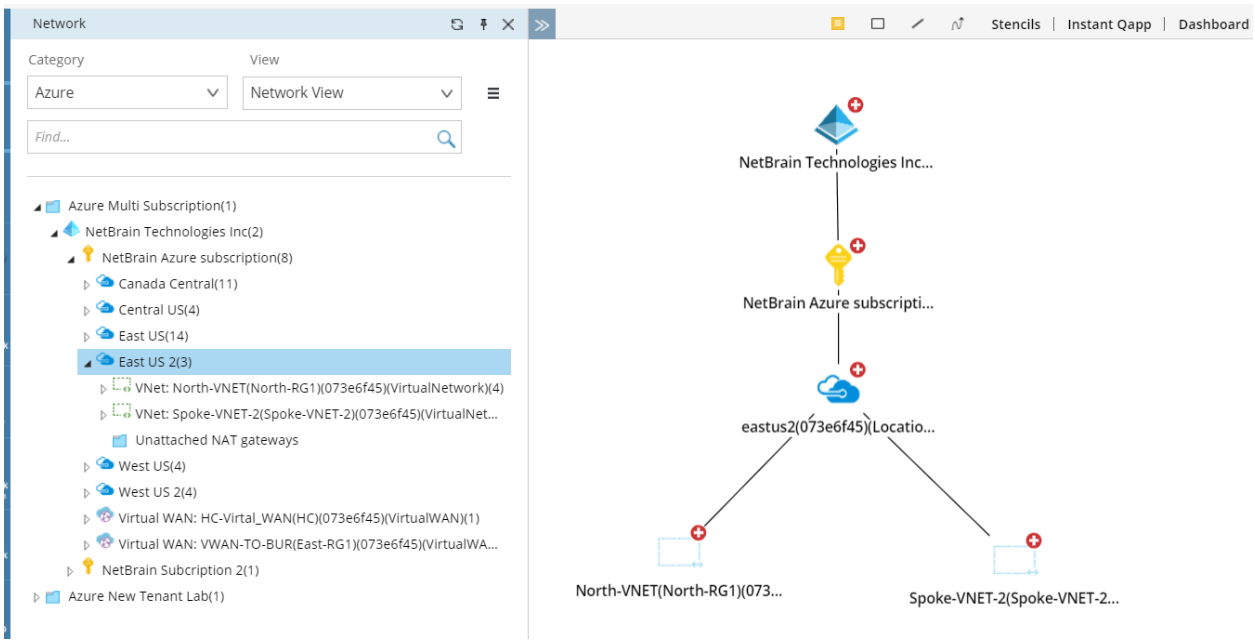
1.2.2.3. Region Context Map

The region context map provides the following information:

- Displaying all virtual network and its resources relationship within the same region.



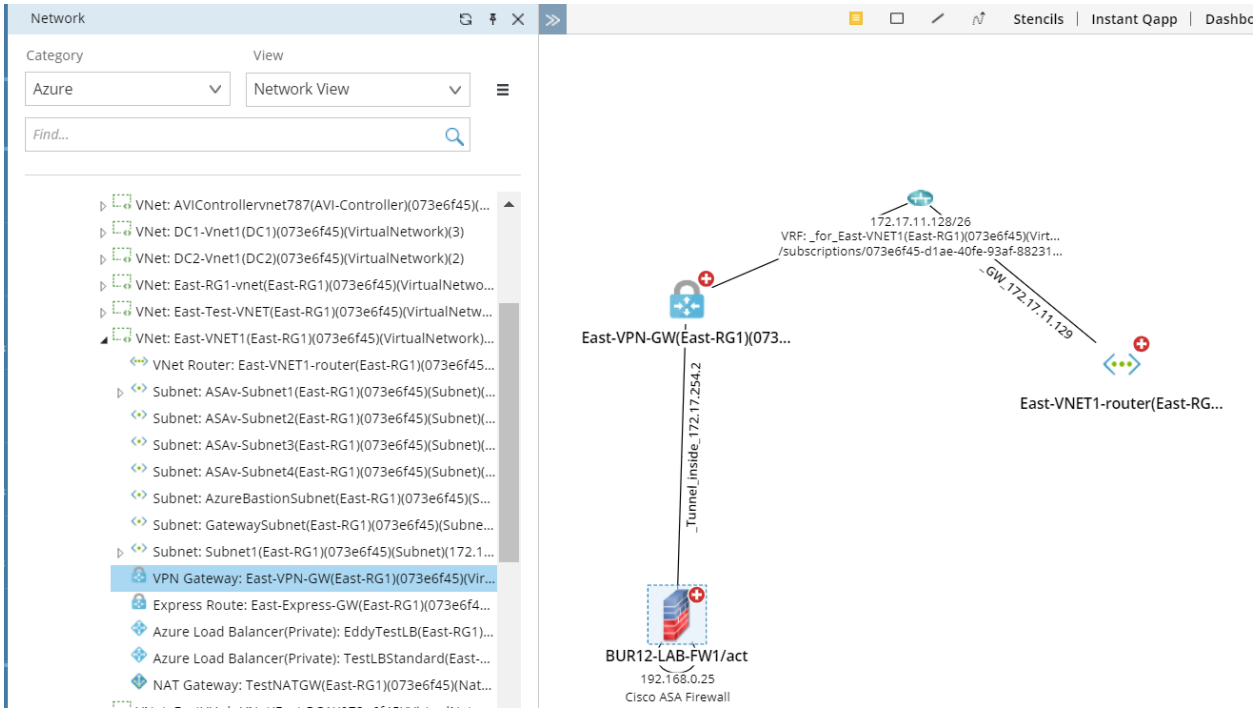
- Displaying the management view for the selected region.



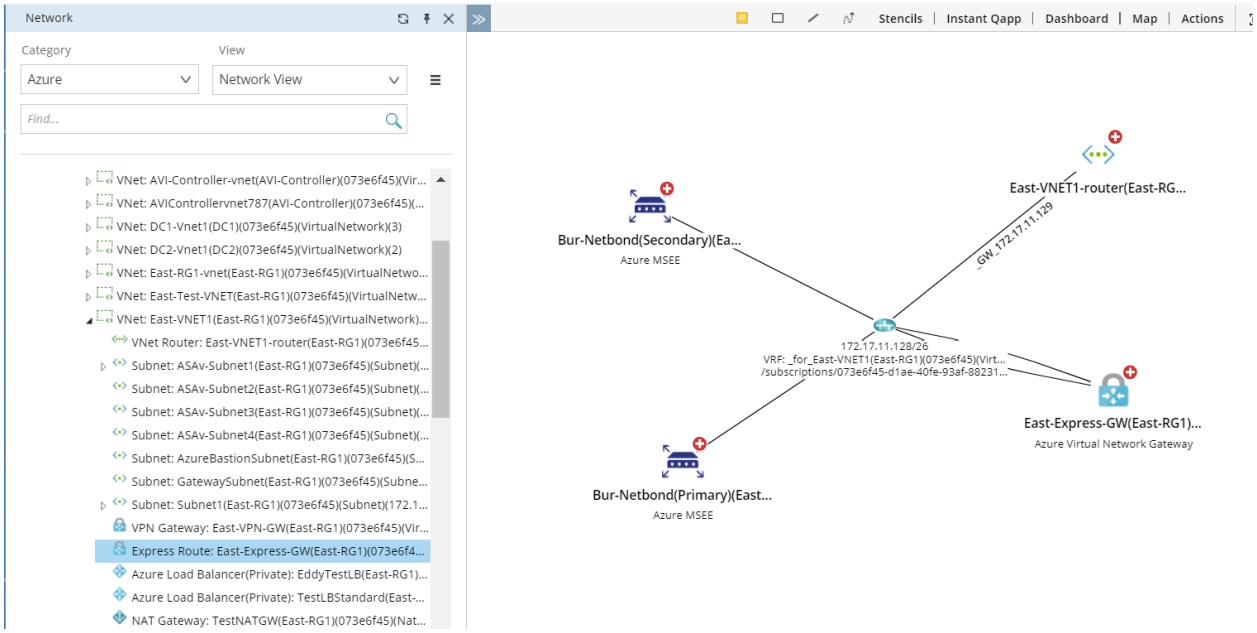
1.2.2.4. Azure to On-premise Network Context Map

The following context maps demonstrate the relationship between Azure and on-promise network.

- VPN gateway context map demonstrate the IPsec VPN connection between VPN gateway and on-premise edge device.

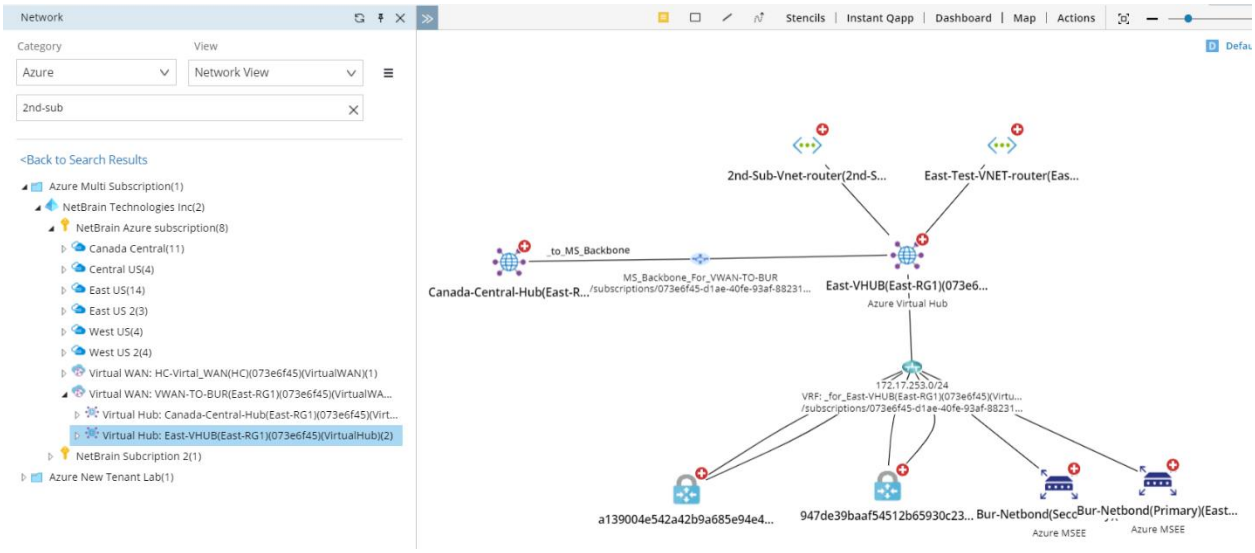


- ExpressRoute gateway context map demonstrate the connection between ExpressRoute gateway and on-promise network via MSEE.



1.2.2.5. Virtual Hub Context Map

In this context map will demonstrate the resources used to connect to on-promise network, the connected virtual network within different region(s), and other connected virtual hub(s) via MS backbone.



1.3. Application Path for Hybrid and Multi-cloud

NetBrain's path function has been extended to the public cloud in v10. The system supports end-to-end path calculation in hybrid/multi-cloud environment, and you can analyze the traffic flow between two endpoints. To start a path calculation:

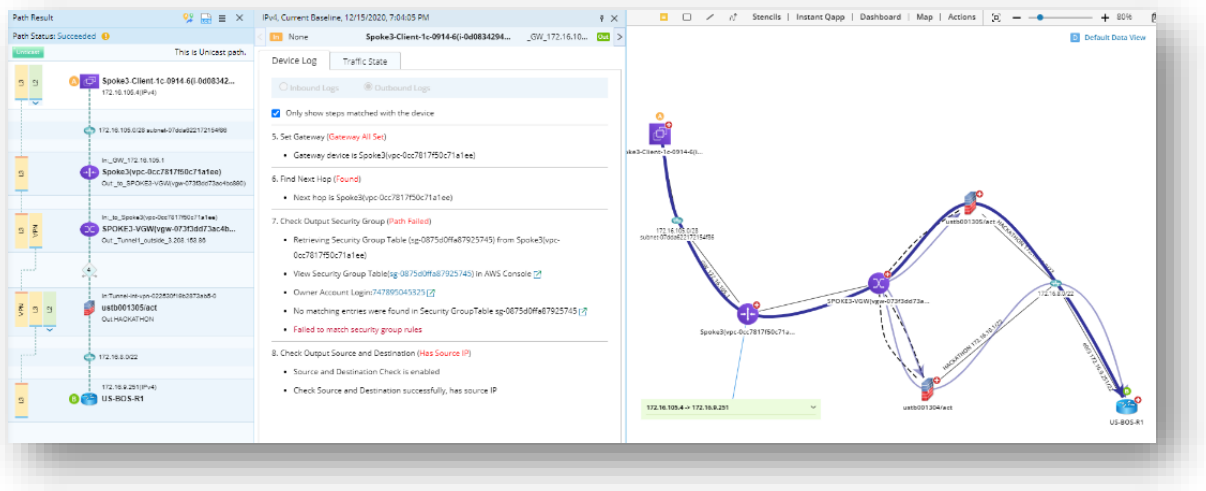
1. Click **Path** on the search bar.

2. Enter the IP address of endpoint A in the **Source** field and the IP address of endpoint B in the **Destination** field.

3. By default, the system calculates two-way paths. To change the path direction, select the icon or the icon.

4. The related gateways will be auto identified. If a device has multiple gateways, you can select the desired one from the **Gateway** list.

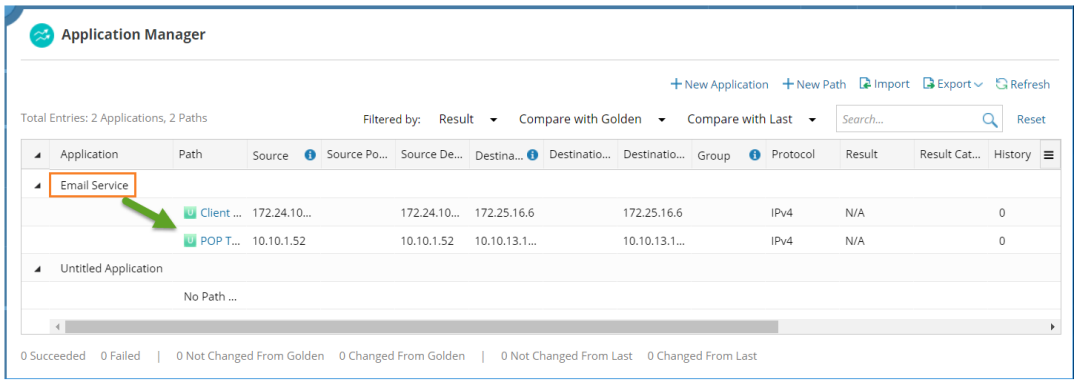
Click **Path** to view the diagrammed path on the map with a detailed summary log (in the left pane).



Create Application Path

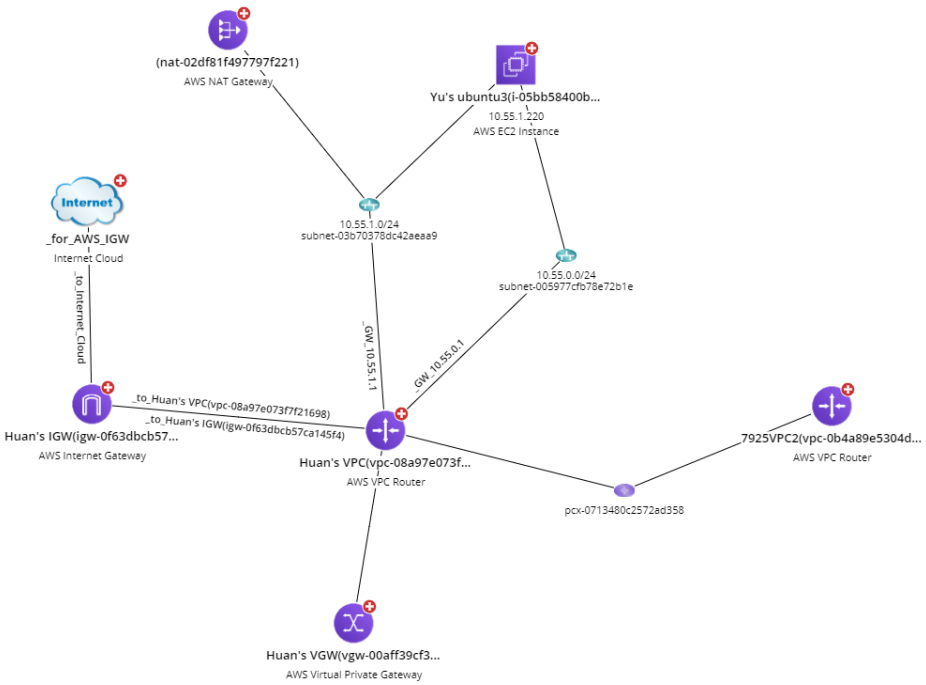
Your application may consist of web tier/application tier/database tier, so you probably want to create a application to include multiple paths for different paths. In this case, you can use NetBrain's path browser function to create applications and include the corresponding paths.

For more information about how to use the application manager to create and manage paths, please refer to the online help: Organizing and Verifying Paths in Application Manager

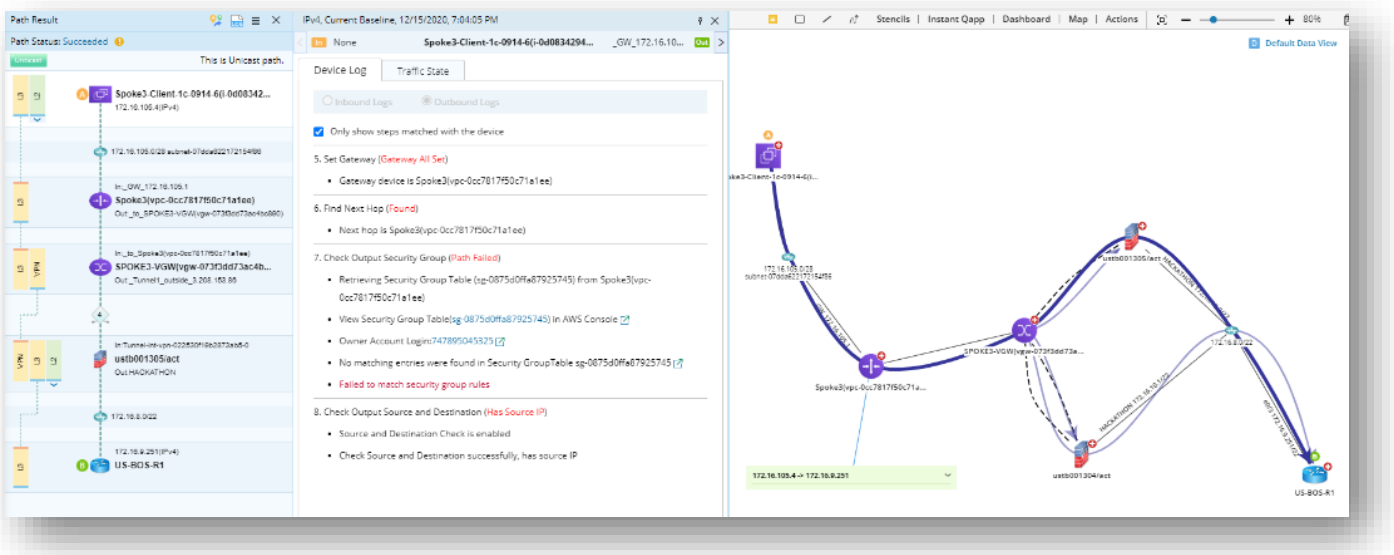


1.3.1.AWS Application Path Deep Dive

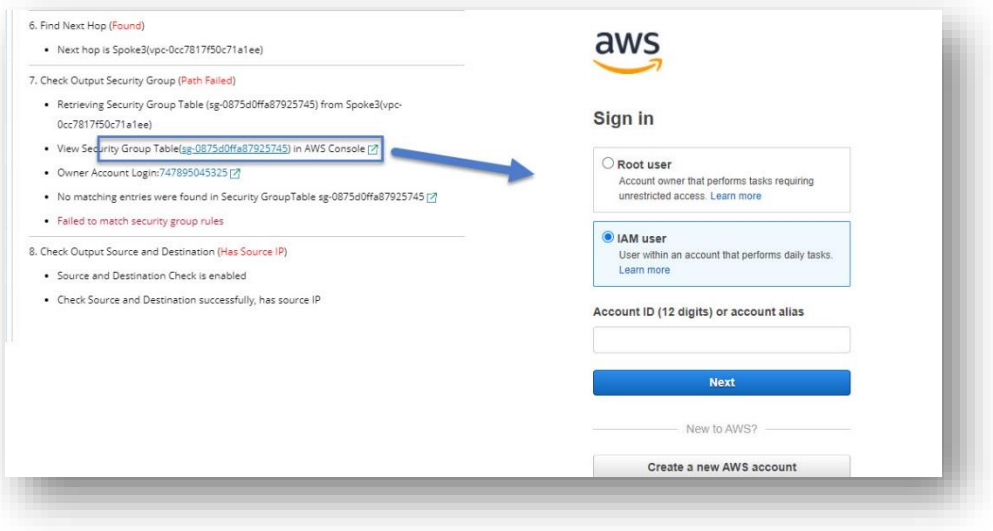
A VPC consists IP range, subnets, and it may also contain cloud-native networking services as NAT gateway, IGW, VGW etc., NetBrain will create a AWS VPC router for each VPC to simulate the routing/security check function for this VPC. Subnet is visualized in NetBrain's dynamic map via the concept called LAN media. From the dynamic map, you can view different networking objects and how they are connected. VPC peering is also supported- the corresponding peering ID will be visualized in the dynamic map.



Path calculation will render the path log containing the related routing and security check details.

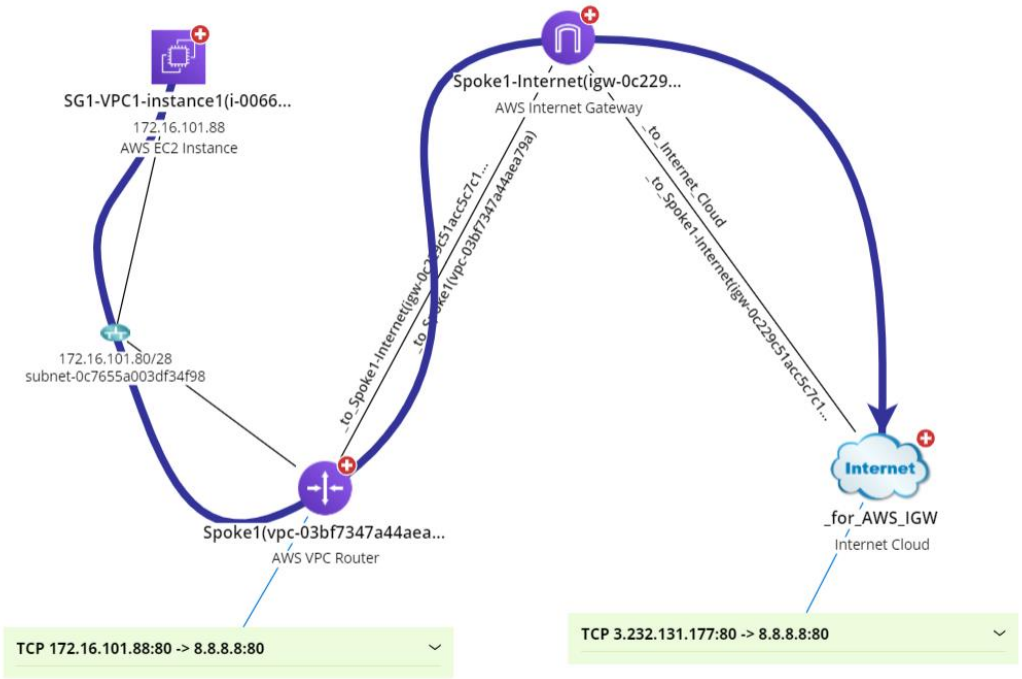


The link of each object will direct you to the AWS console, where you can view more information about the object or make desired changes.



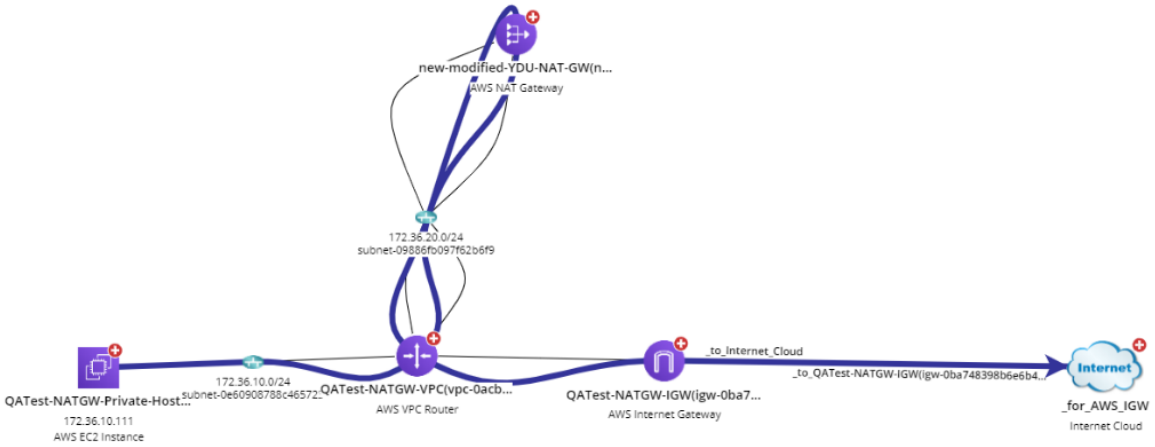
Path Example 1 - EC2 to Internet

The following path diagram demonstrates how a EC2 instance in a public subnet accesses the internet directly.



Path Example 2 - NAT Gateway

The following path diagram demonstrates how NetBrain can help you identify the traffic flow when a EC2 instance tries to access the internet via NAT gateway. From the path log, you will be able to better understand how the NAT works.



1.3.1.1. AWS On-Prem Connection via Direct Connect

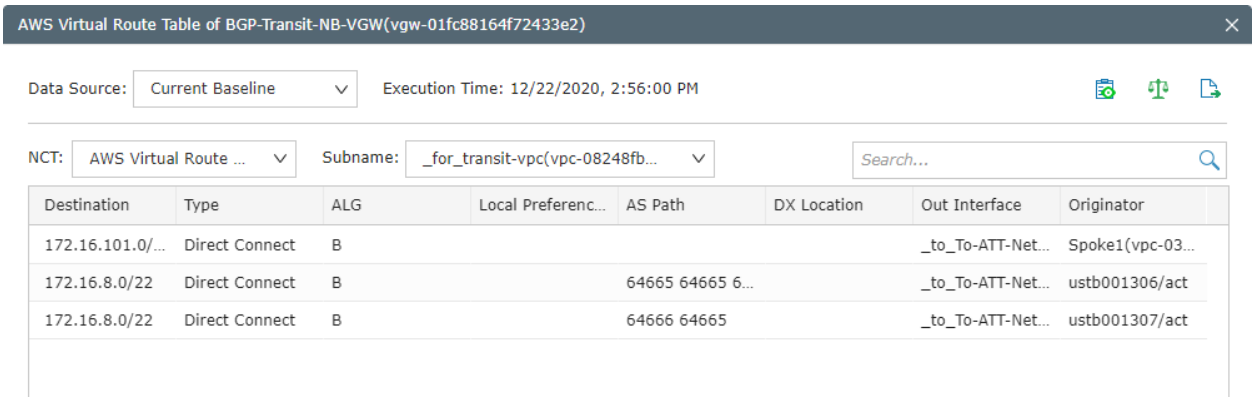
There are a lot of different architectures for connections between your on-prem network to the public cloud resources. NetBrain supports all of these popular deployment types as previously illustrated.

The key of supporting end-to-end path for public cloud environment is really to understand all the routing & security checks across the entire network. You may know AWS natively doesn't provide the routing tables for the following networking objects:

- Virtual private gateway
- Direct connect gateway
- Direct connect router

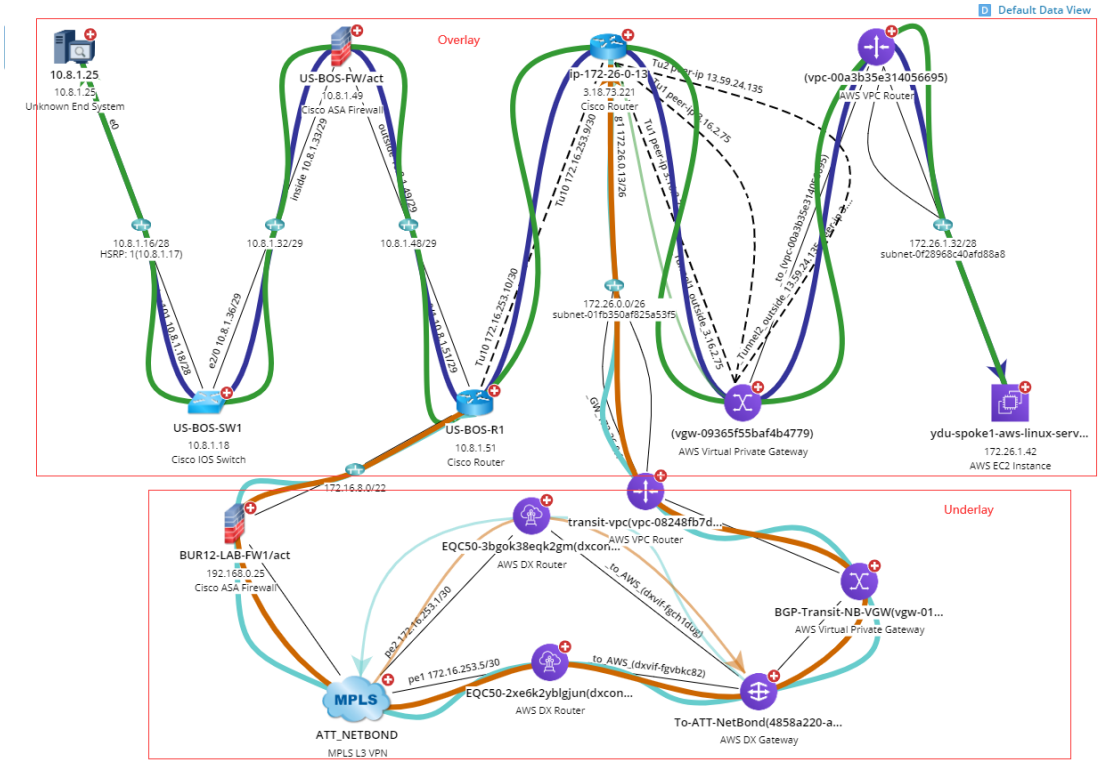
NetBrain has invented a unique algorithm to build the virtual routing table based on the topology info and route advertisement it captures for the surrounding devices. These information are also very useful for you to understand the potential routing problems:

- Neighbor relationship table: this table includes neighbors device information which are recognized as directly connected neighbors.
- Route dependency table: this table includes devices with routes advertised to the current device.
- AWS virtual routing table: this is the virtual route table NetBrain calculate to be used in path calculation. We also strictly follow AWS's route selection priority rules to choose the best path available if there's multiple paths to the destination.



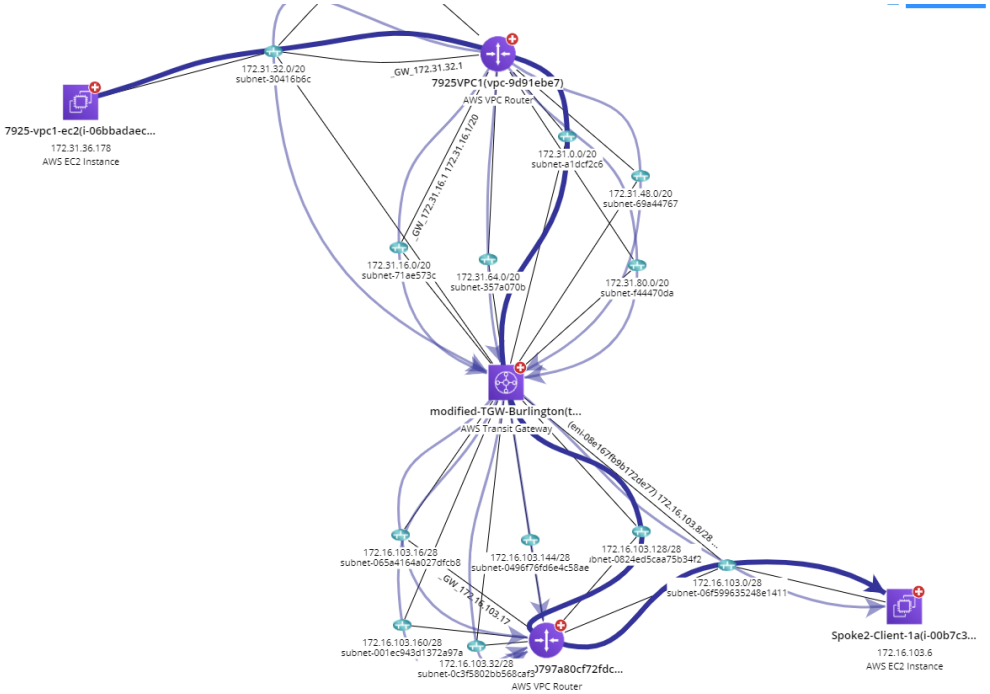
Below is an example demonstrating path from an EC2 instance to an end system in the on-prem network. This is a transit VPC architecture where we build the IPSEC tunnel between the customer gateway with the CSR1000v sitting in the transit VPC. The underlay communication is achieved via the direct connections via ATT Netbound.

You will be able to understand the overlay path for the IPSec tunnels as well as the underlay path going through the direct connect router and direct connect gateway to the virtual private gateway of the transit VPC.



1.3.1.2. Transit Gateway Reference Architecture

Transit Gateway is used to enable VPC-to-VPC communication or/and on-prem to cloud communication. The above scenarios are fully supported by NetBrain.

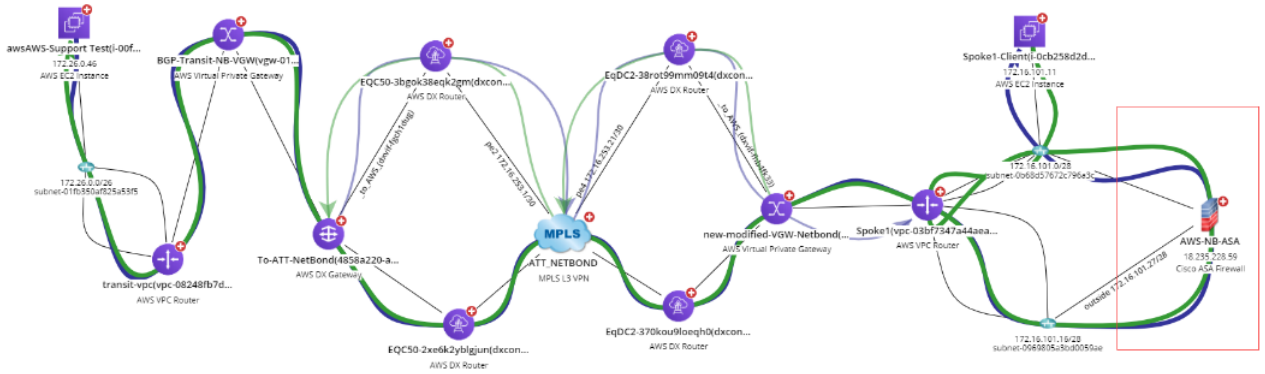


1.3.1.3. Virtual Appliance

Virtual appliance can be used in the public cloud environment (CSR1000v, ASAv, vedge etc.). The relevant deployment scenarios (including the application path across these virtual appliances) are fully supported by NetBrain.

In order to successfully establish a path going through the virtual appliances, CLI access to the virtual appliances is required in addition to accessing the AWS API (to retrieve the EC2 instance information).

The example below demonstrates how the ingress routing works with the ASAv configured within VPC to inspect the incoming traffic.

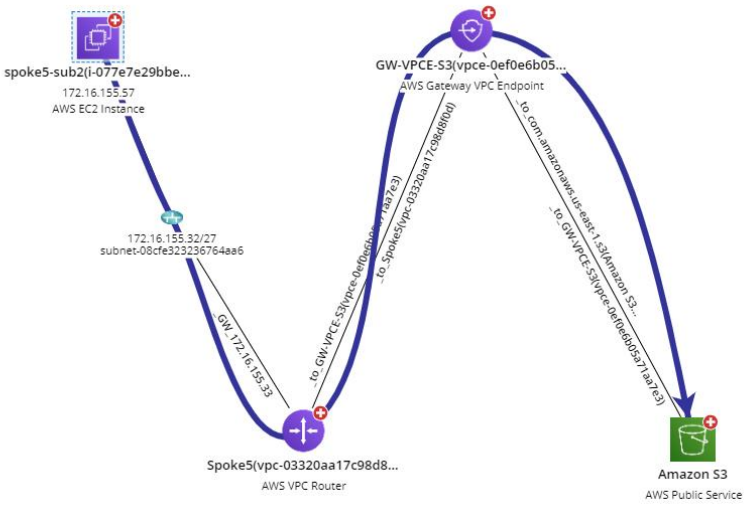


1.3.1.4. VPC Endpoint and Private Link

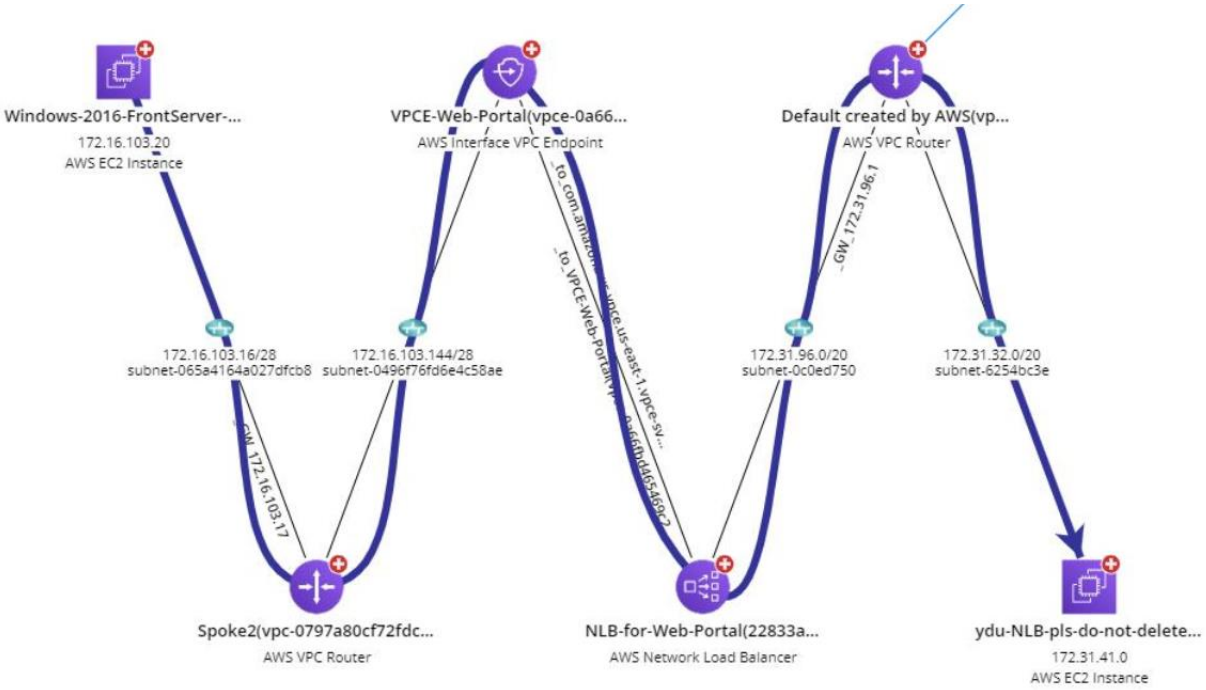
AWS Public Services are fully supported in current release, including the gateway endpoints and the interface endpoints.

Amazon Dynamo DB	AWS	Amazon Dyna...
Amazon EC2	AWS	Amazon EC2
Amazon S3	AWS	Amazon S3
Amazon SageMaker Notebook	AWS	Amazon SageM...

The following path shows how an EC2 instance communicates with the Amazon S3 service via the gateway endpoints. You can verify the traffic flow from NetBrain by entering the source IP, destination URL and NetBrain can confirm that the traffic goes through the Gateway endpoints instead of using the internet gateway.



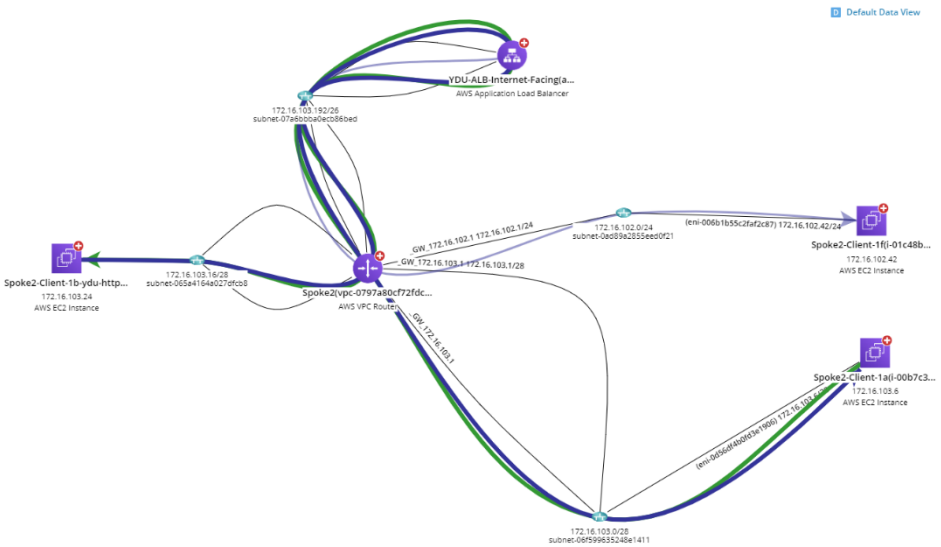
The following diagram demonstrates the private-link support. From the right hand side, the application owner shares the application with others via the private link service. NetBrain can map the private link services accordingly. When you calculate the path from the EC2 instance to the private link service, NetBrain can further visualize the entire path as well as the EC2 instances sitting behind the NLB.



1.3.1.5. Application View (NLB/ELB)

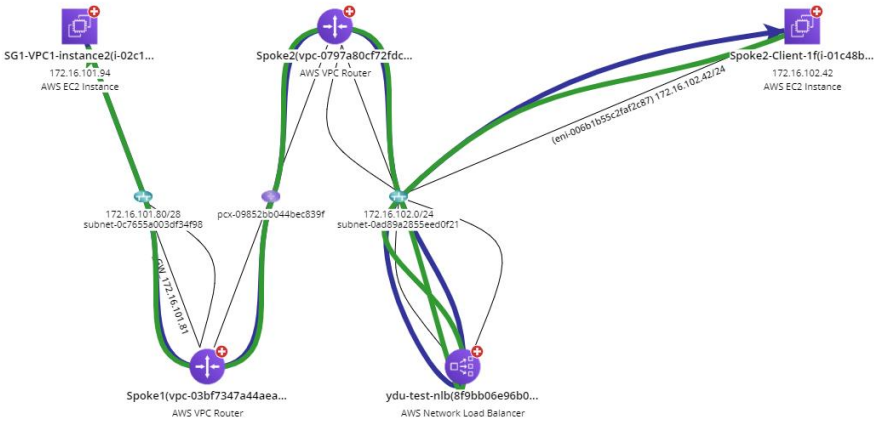
Path Example- Application Load Balancer

Note: *At the current stage we don't support layer 7 inspection details. Only layer 4 inspection is performed.*



Path Example- Network Load Balancer

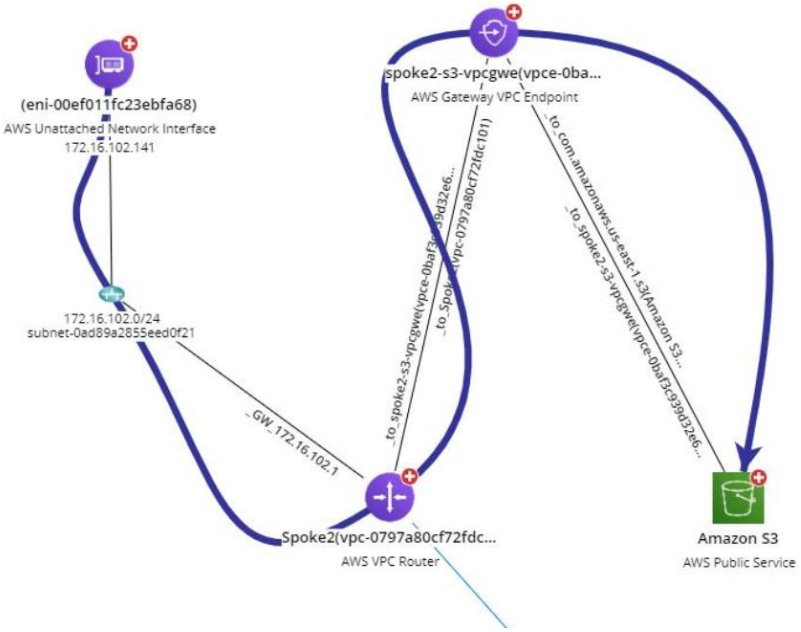
The following one shows the path goes through a network load balancer. You will find the EC2 instances behind the load balancer has been mapped out as expected.



1.3.1.6. AWS Lambda Support / Serverless Support

The current release only provides limited support for serverless application dues to NetBrain's current focus on Networking Objects. When launching a serverless application, AWS will automatically generate ENI interfaces to communicate with other VPC resources. You will need to configure the correct security group and ensure it can work properly. You can leverage NetBrain's path function to check the application flow from ENI interfaces to destinations.

The following path demonstrates the path from an ENI interface provisioned by AWS for serverless application to the AWS S3.



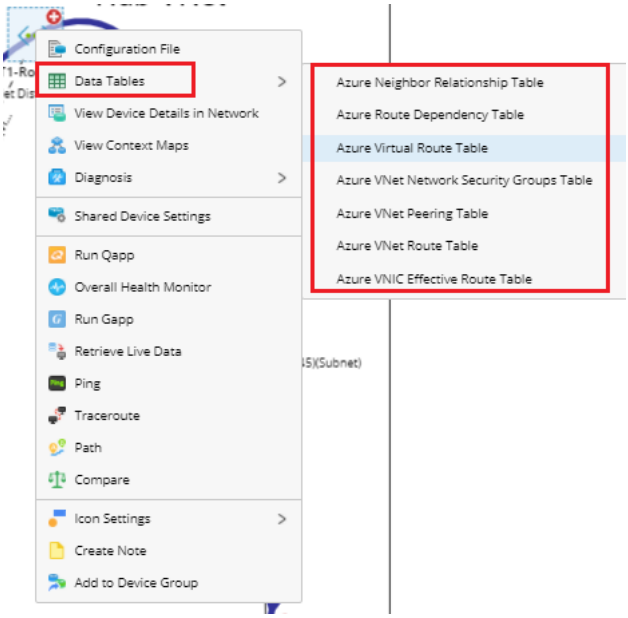
1.3.2.Azure Application Path Deep Dive

For a detailed list of Azure Networking Supported Functions, please refer to:

Azure Networking Supported Function List

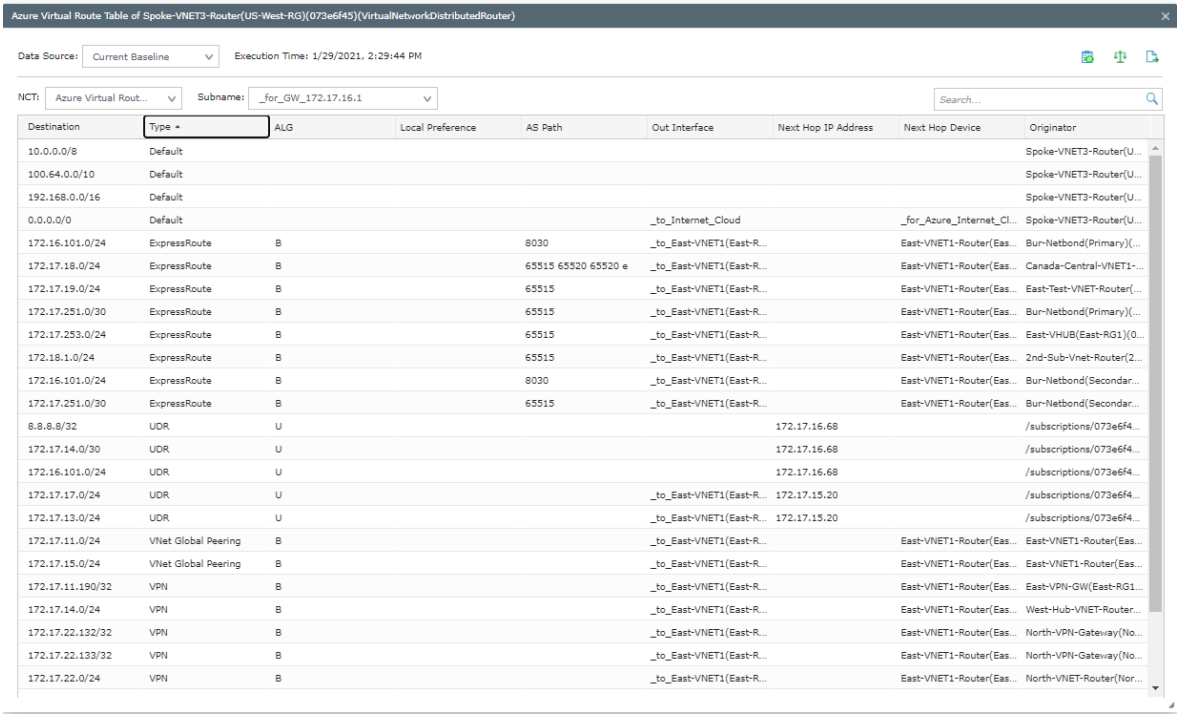
NetBrain has invented the concept of Virtual Network Distributed Router (VNet Router) with various resources and features to simplify the Azure Cloud network connections inside and outside the Virtual Network. The resources/features include:

- Routing information such as User Defined Route and Virtual Route Table for Virtual Network.
- Security rule information such as Network/Application Security Group rule in subnet/interface level.
- Peering information for various VNet peering details.
- Network Interface (NIC) Effective Route Table information



NetBrain has invented the unique algorithm to build the virtual routing table based on the topology info and route advertisement it captures for the surrounding devices. This information is very useful in the context of reviewing the potential routing problems:

- Neighbor Relationship Table: This table includes the neighbor device information which are recognized as directly connected neighbors.
- Route Dependency Table: This table includes the devices with routes advertised to the current device.
- Virtual Routing Table: This is the virtual route table to be used in path calculation. We strictly follow Azure's route selection priority rules to choose the best path available if there's multiple paths to the destination.



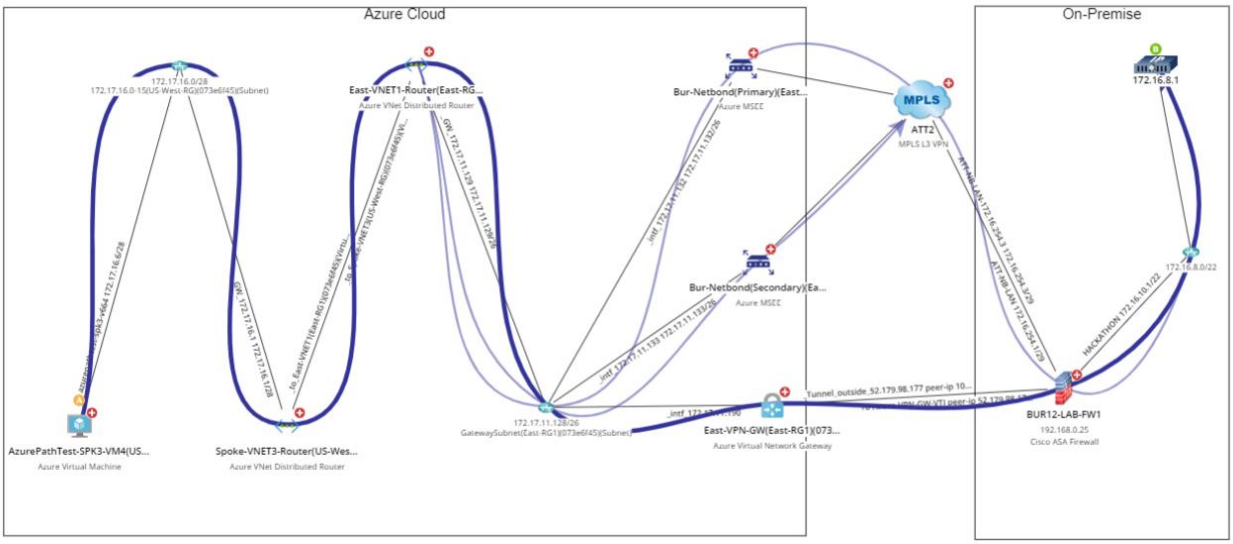
1.3.2.1. Traffic Cross Azure Cloud and On-Premises Scenario

There are several ways to connect an on-premises network to an Azure Virtual Network (VNet).

- **VPN connection**

A VPN gateway is a type of virtual network gateway that sends encrypted traffic between an Azure virtual network and an on-premises location. The encrypted traffic goes over the public Internet.

NetBrain VPN connection path sample:

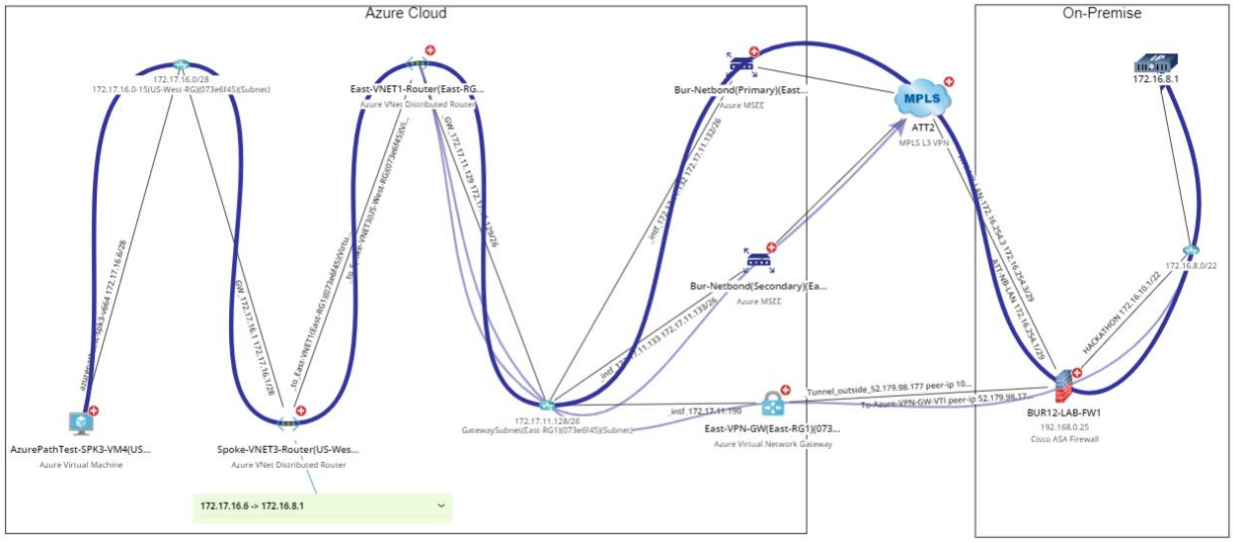


- **ExpressRoute connection**

ExpressRoute connections use a private, dedicated connection through a third-party connectivity provider. The private connection extends your on-premises network into Azure.

The figure below shows the traffic path between Azure Cloud and On-Premise via two ExpressRoute Circuits connections provisioned by ATT Netbound. Microsoft Enterprise edge (MSEE) devices are sitting at the edge of Azure Cloud.

NetBrain ExpressRoute connection path sample:

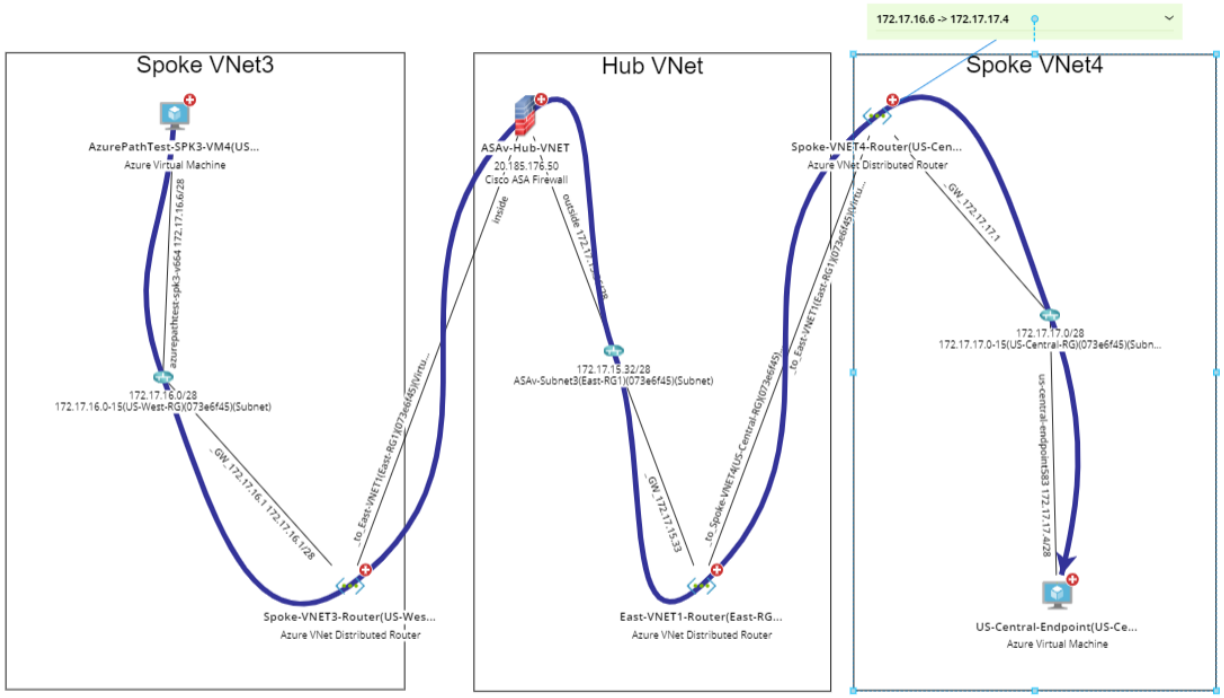


1.3.2.2. Hub-Spoke Typical Network Scenarios

A hub-spoke network topology is a way to isolate workloads while sharing services such as identity and security. The hub is a virtual network (VNet) in Azure that acts as a central point of connectivity to your on-premises network. The spokes are VNets that peer with the hub. Shared services are deployed in the hub, while individual workloads are deployed as spokes.

NetBrain can visualize the abstract cloud traffic path between different Azure nodes and enhance your efficiency of troubleshooting cloud network issues. The figure below shows the Hub provides a secure network boundary using Network Virtual Appliance (NVA) such as Cisco ASA by checking all inbound and outbound network traffic and passing only the traffic that meets network security rules.

NetBrain Hub-Spoke Network path sample:



1.3.2.3. Virtual Network (VNet) Connection Scenarios

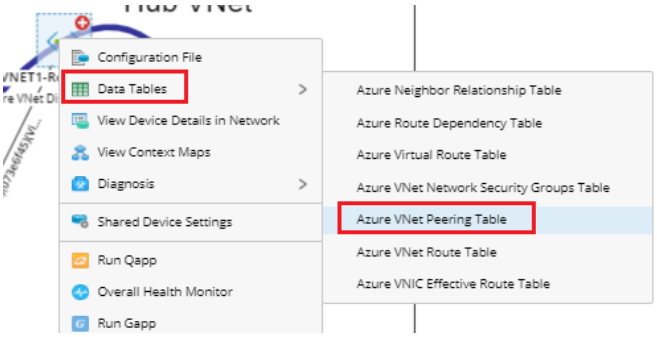
There are several options to connect Virtual Networks (VNet). You can connect virtual networks to each other with virtual network peering or using the VNet-to-VNet connection type.

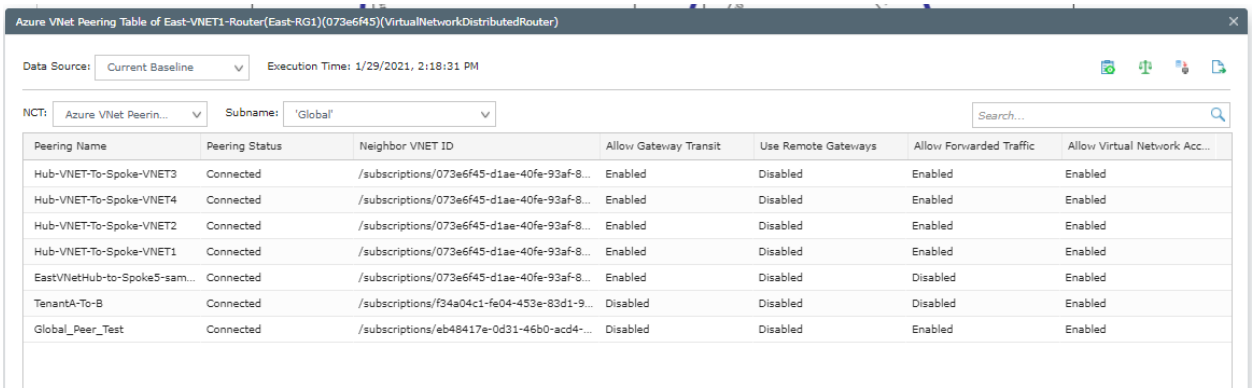
- **VNet Peering**

These virtual networks can be in the same region or different regions (also known as Global VNet peering). Once virtual networks are peered, resources in both virtual networks are able to communicate with each other, with the same latency and bandwidth as if the resources were in the same virtual network.

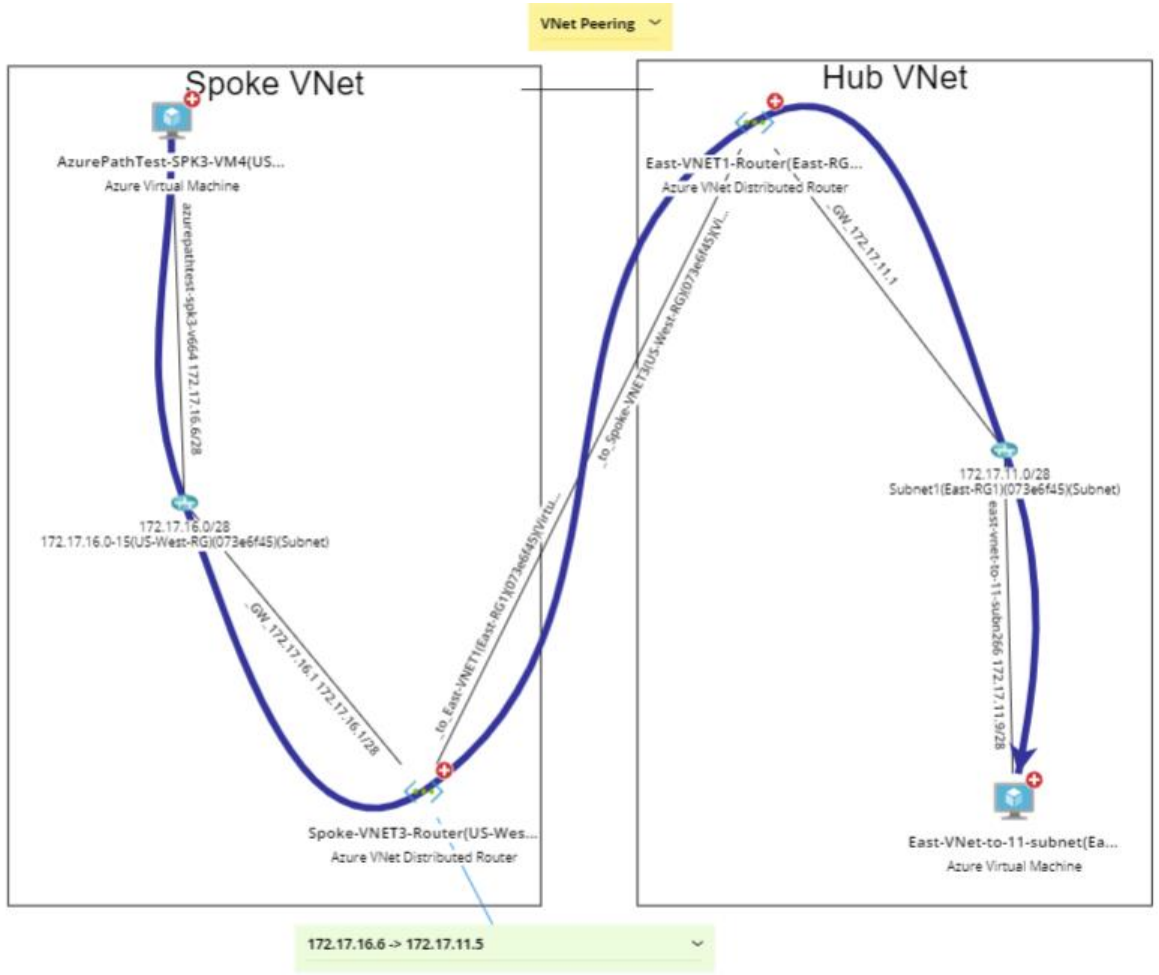
NetBrain provides various Virtual Network information on the MAP such as VNet Peering Table, from which you can view the peering details for current Virtual Network.

Virtual Network Available data table:





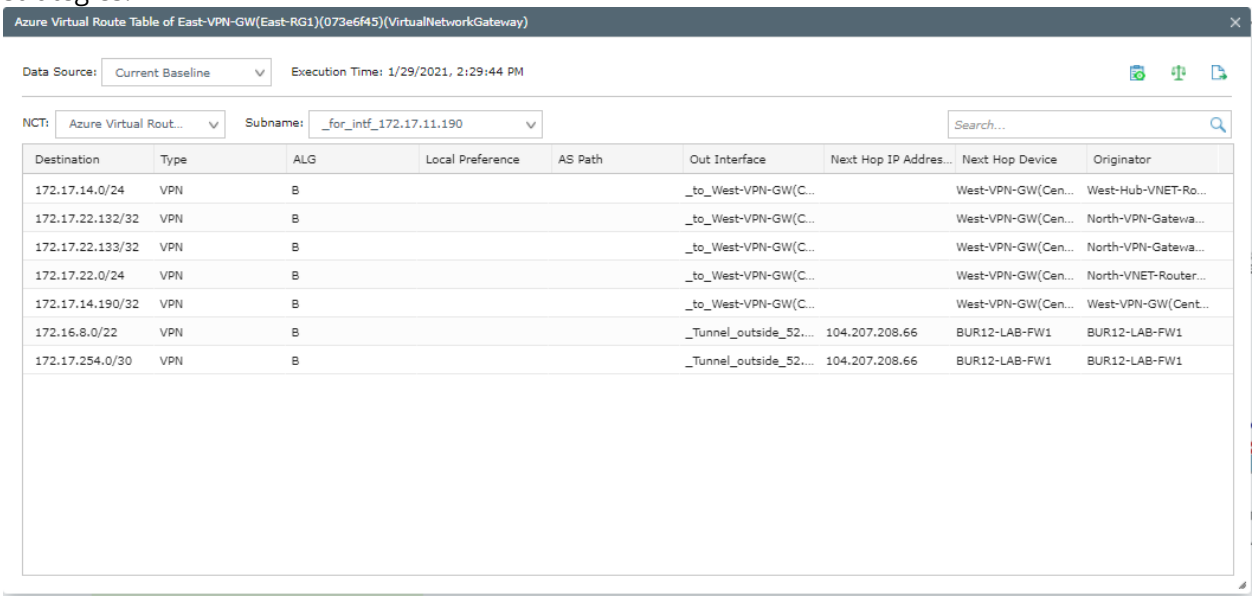
The VNet peering path sample:



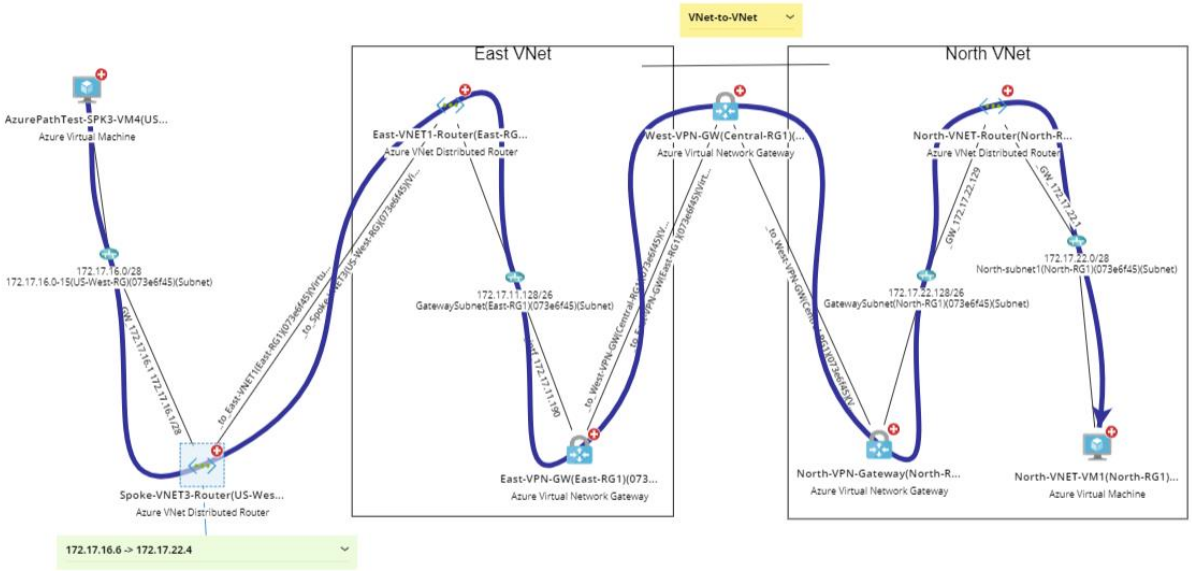
- **VNet-to-VNet Connection**

You can connect virtual networks by using the VNet-to-VNet connection type. The virtual networks can be in the same or different regions, and from the same or different subscriptions. When connecting VNets from different subscriptions, the subscriptions do not need to be associated with the same Active Directory tenant.

NetBrain has invented the proprieties Virtual Route Table based on Azure routing policies and rules, which can provide you an easy way to understand cloud routing details instead of struggling with abstract cloud routing strategies.



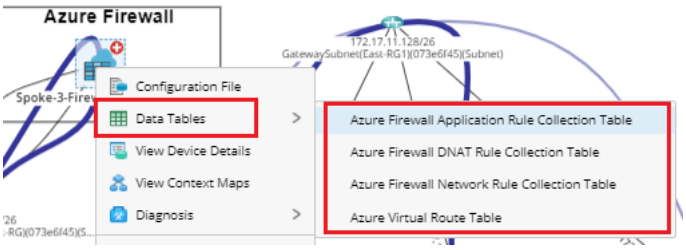
The VNet-to-VNet connection path sample is shown as below:

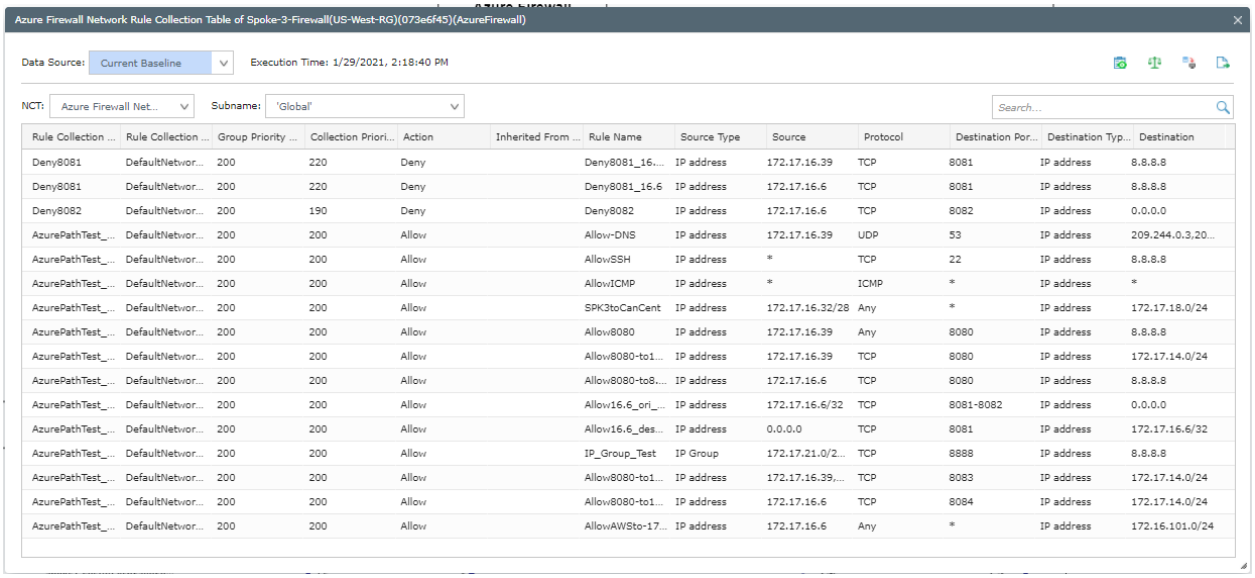


1.3.2.4. Azure Firewall Scenarios

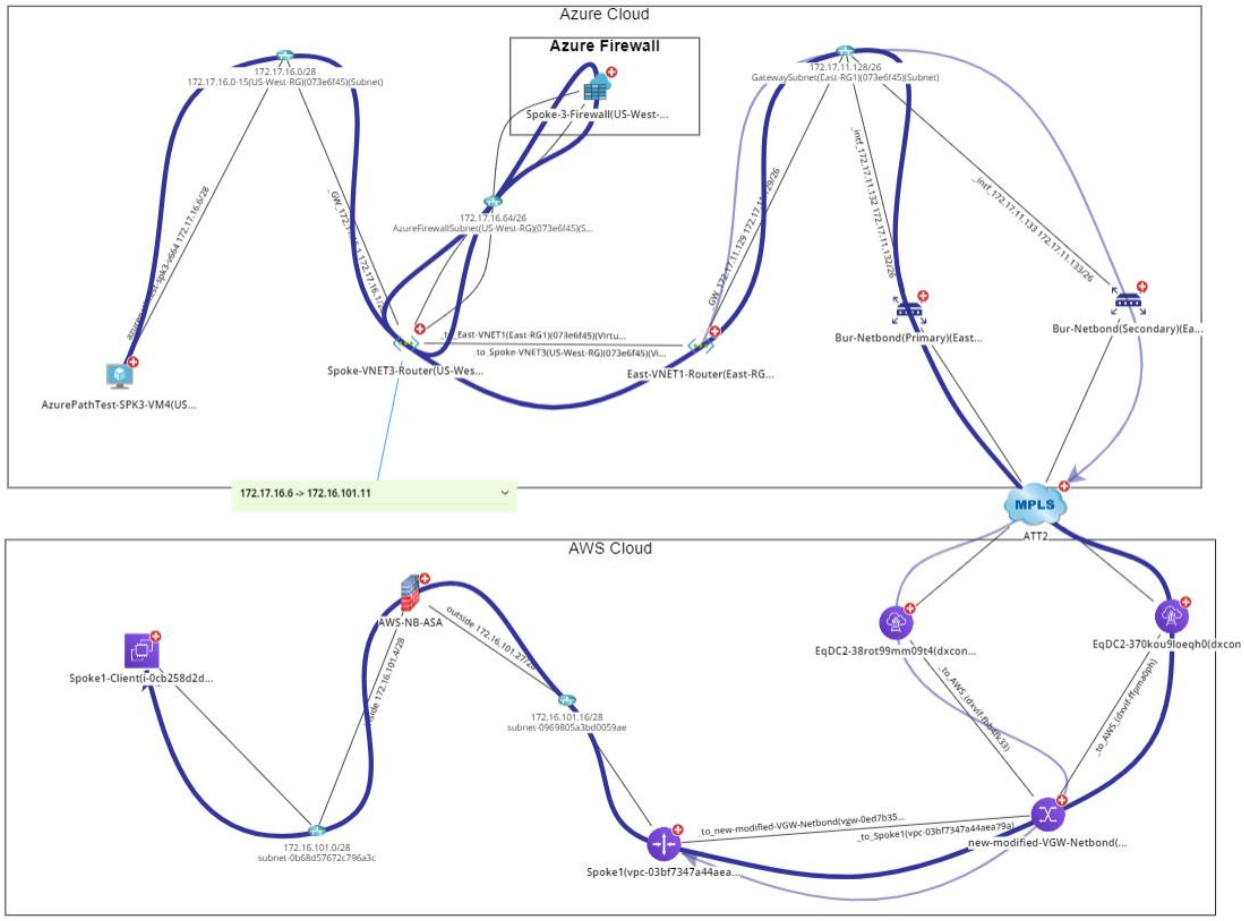
Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

NetBrain uses various tables to visualize different Azure Firewall Rule information, and performs lookup across all rules to calculate the path following Azure rule check policy.





The Azure Firewall path sample:



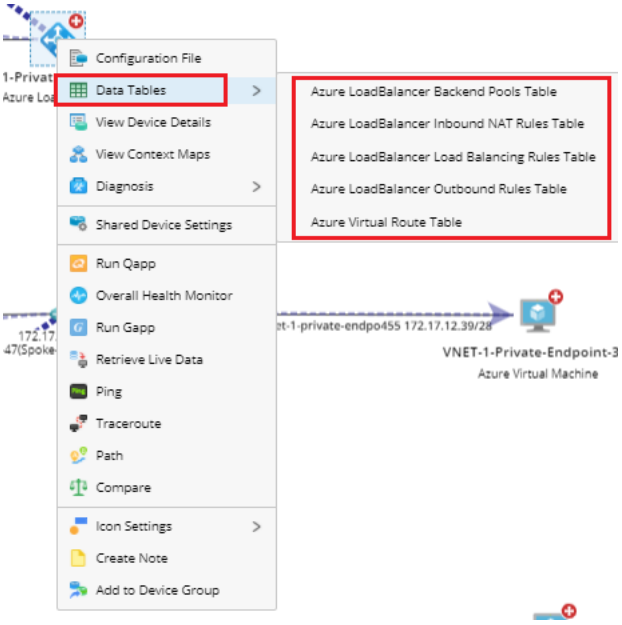
1.3.2.5. Azure Load Balancer Scenarios

Azure Load Balancer operates at layer four of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. Load Balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load balancing rules. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.

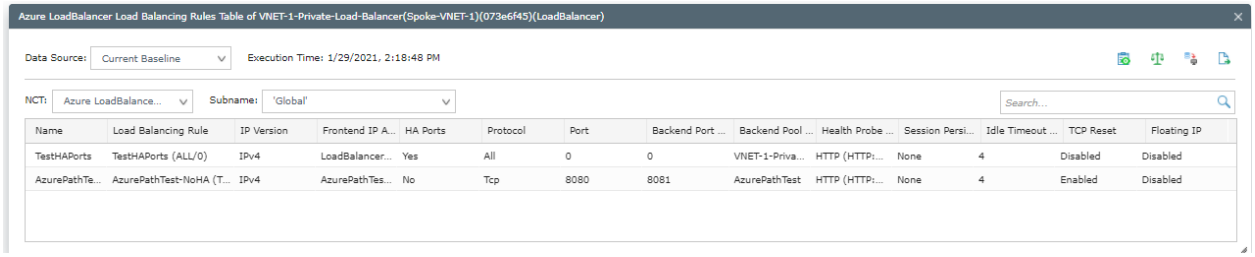
NetBrain supports both Public/Internal Load Balancer path and various Load Balancer features, including:

- Azure LoadBalancer Backend Pools Table
- Azure LoadBalancer Inbound NAT Rules Table
- Azure LoadBalancer Load Balancing Rules Table
- Azure LoadBalancer Outbound Rules Table
- Azure LoadBalancer Virtual Route Table

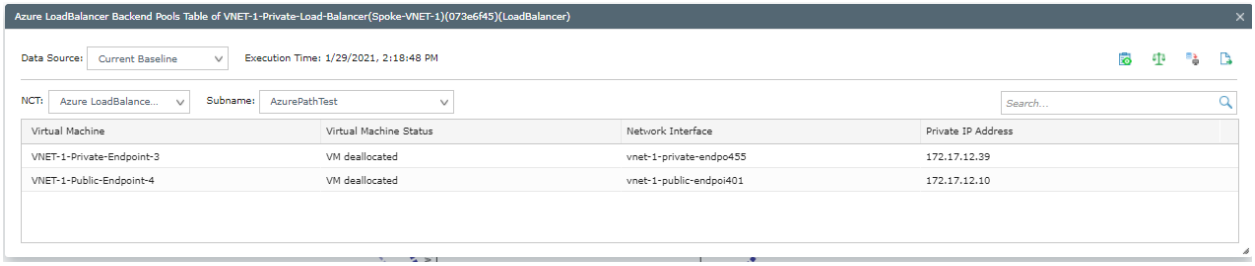
Azure Load Balancer available data table:



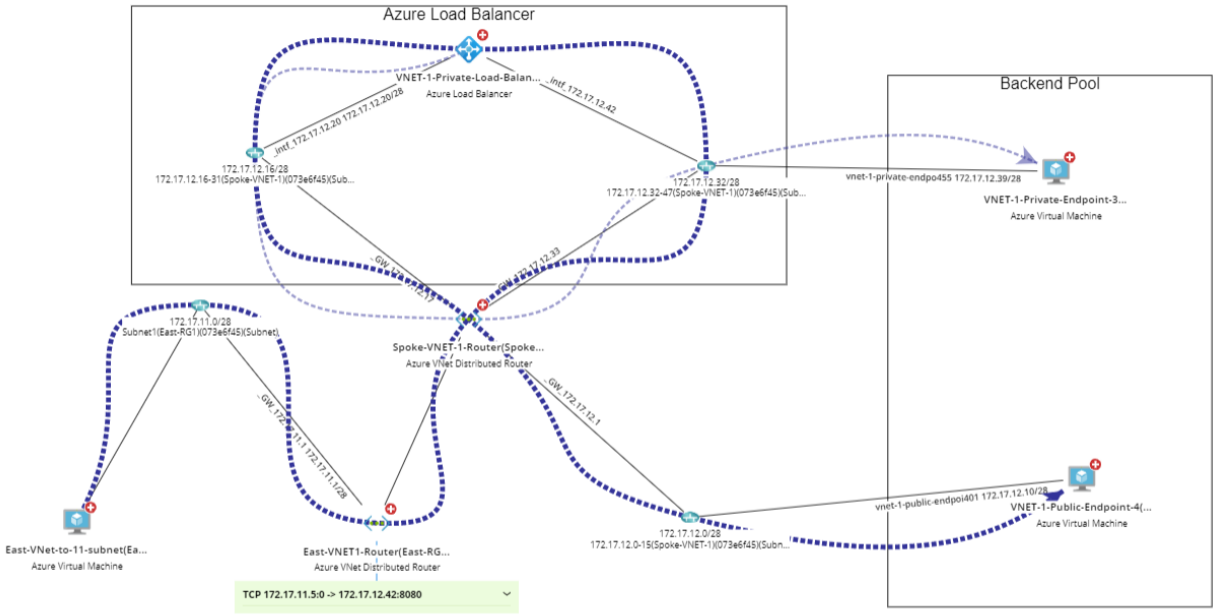
Azure Load Balancer Load Balancing Rules Table:



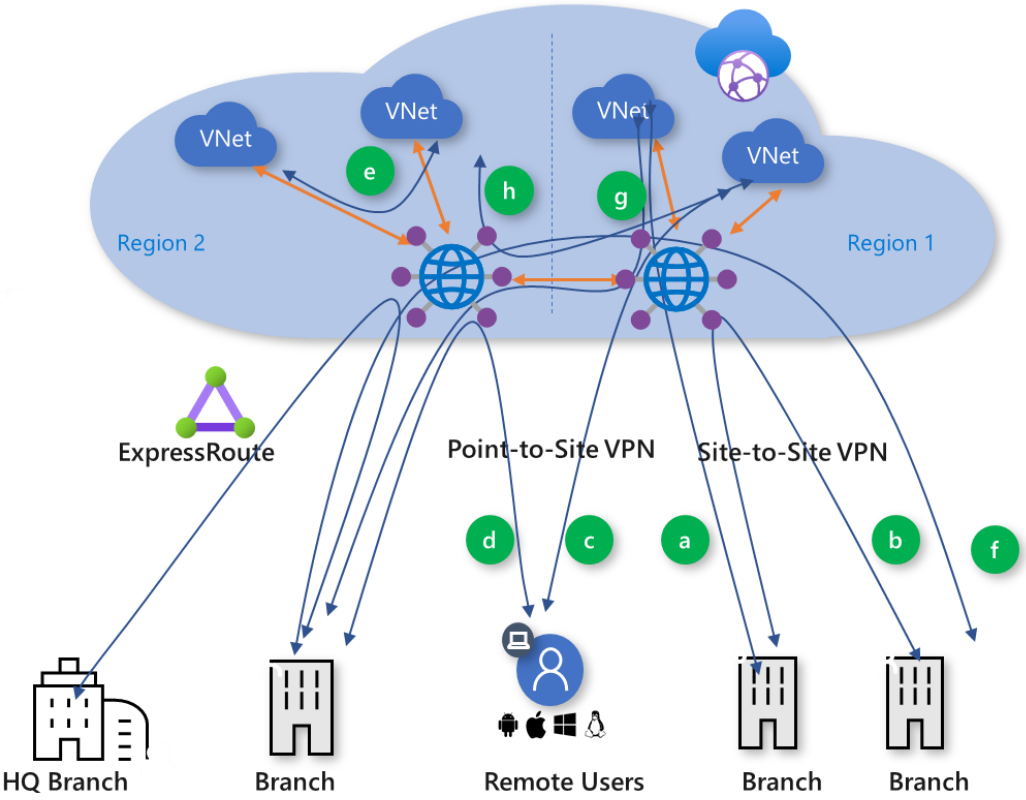
Azure Load Balancer Backend Pools Table:



The Azure Load Balancer path sample:



1.3.2.6. Azure Virtual WAN Network Scenarios

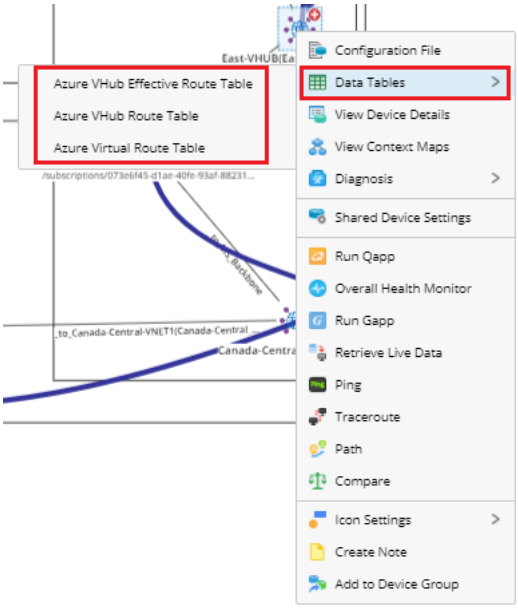


NetBrain supports the following global transit connectivity paths of Azure Virtual WAN. The letters in parentheses corresponds to the letters in the diagram above.

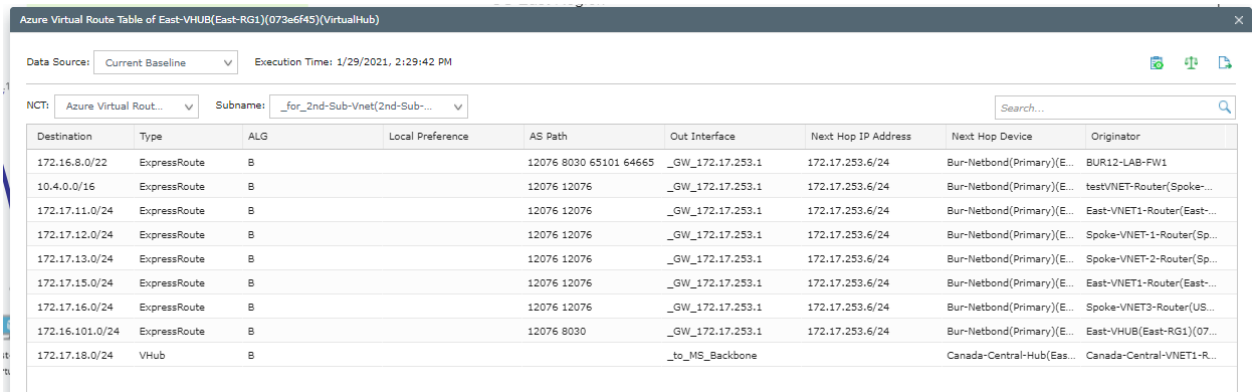
- Branch-to-VNet (a)
- Branch-to-branch (b)
  - ExpressRoute Global Reach and Virtual WAN
- Remote User-to-VNet (c)
- Remote User-to-branch (d)
- VNet-to-VNet (e)
- Branch-to-hub-hub-to-Branch (f)
- Branch-to-hub-hub-to-VNet (g)
- VNet-to-hub-hub-to-VNet (h)

NetBrain can provide key information including Virtual Hub Effective Route Table and Virtual Route Table.

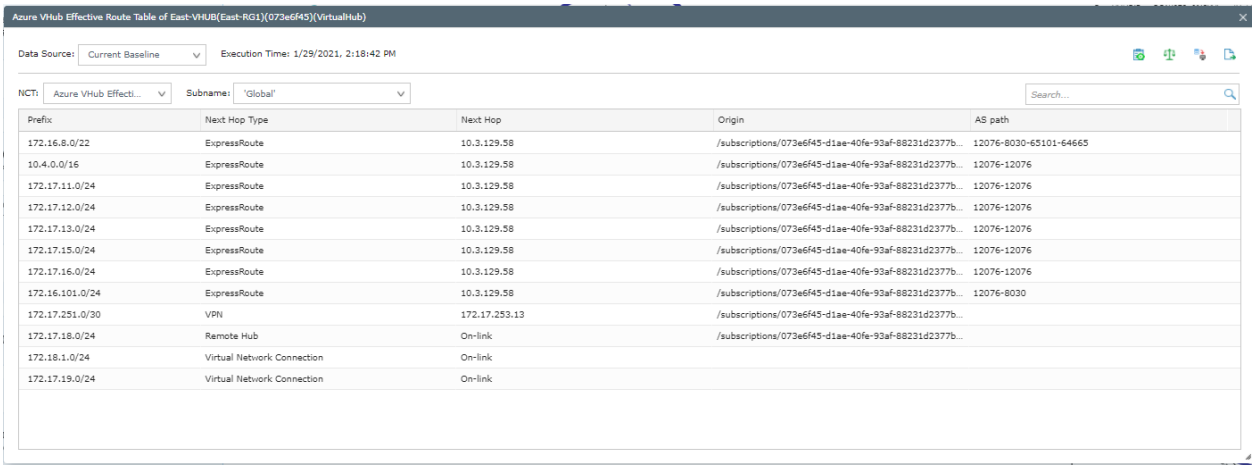
Virtual Hub Available Data Table:



Virtual Hub Virtual Route Table:

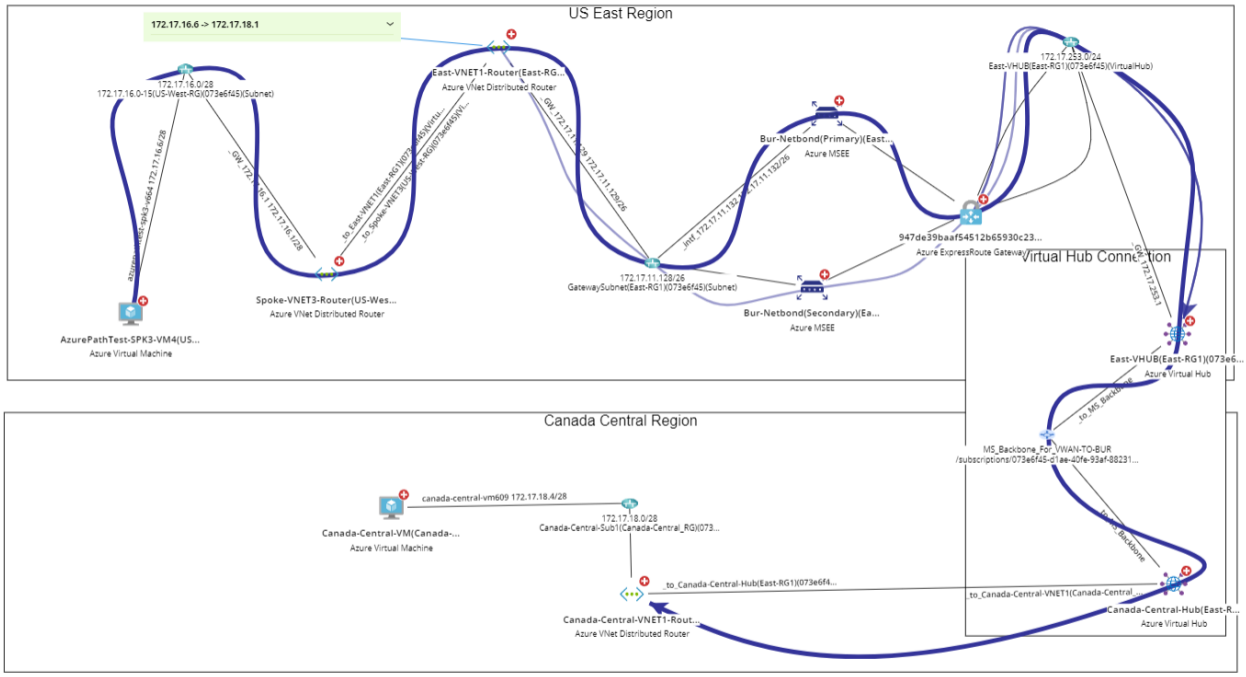


Virtual Hub Effective Route Table:



Prefix	Next Hop Type	Next Hop	Origin	AS path
172.16.8.0/22	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	12076-8030-65101-64665
10.4.0.0/16	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	12076-12076
172.17.11.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	12076-12076
172.17.12.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	12076-12076
172.17.13.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	12076-12076
172.17.15.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	12076-12076
172.17.16.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	12076-12076
172.16.101.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	12076-8030
172.17.251.0/30	VPN	172.17.253.13	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	
172.17.18.0/24	Remote Hub	On-link	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b...	
172.18.1.0/24	Virtual Network Connection	On-link		
172.17.19.0/24	Virtual Network Connection	On-link		

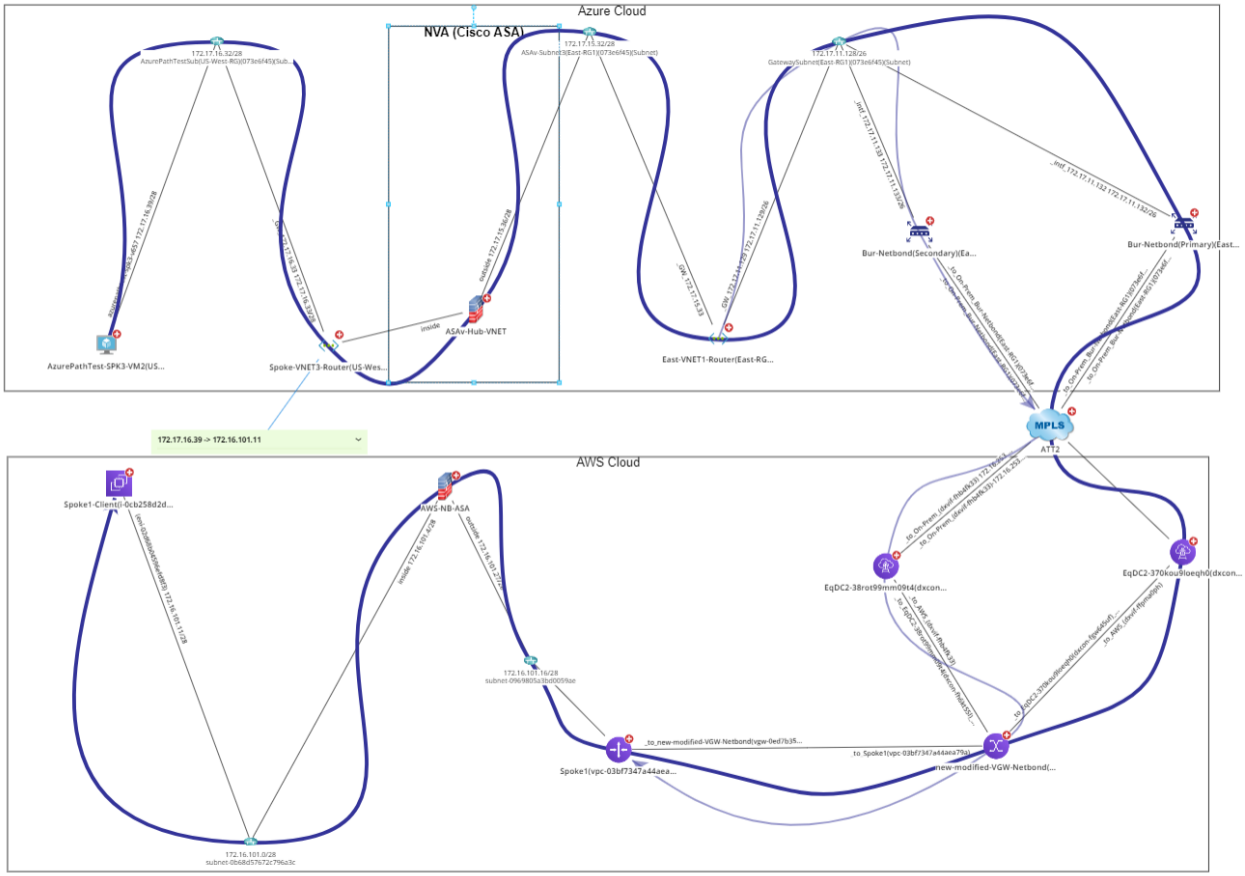
The Azure Virtual WAN path sample is shown as below:



1.3.2.7. Virtual Appliance Scenarios

A Network Virtual Appliance (NVA) is typically used to control the flow of network traffic from a perimeter network, also known as a DMZ, to other networks or subnets.

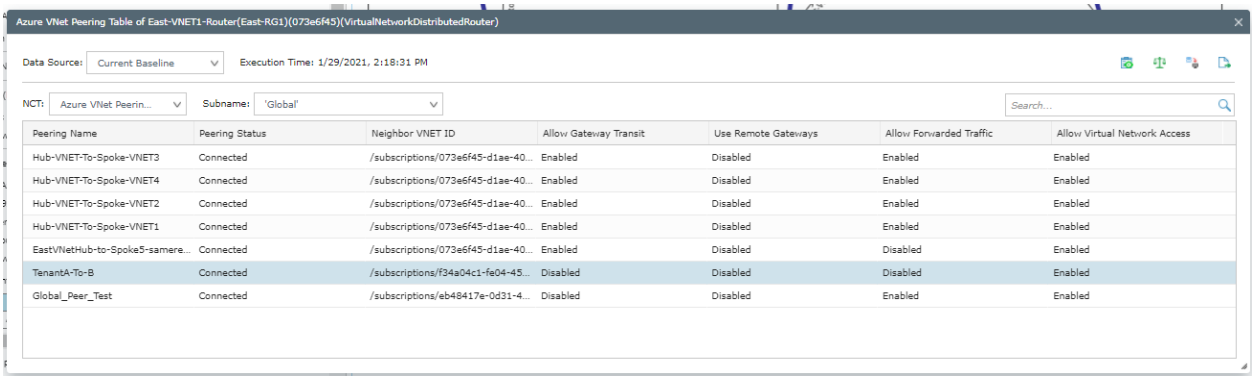
The diagram below shows the NVA provides a secure network boundary by checking all inbound and outbound network traffic and passing only the traffic that meets network security rules.



1.3.3.Path across Accounts (AWS) and across Tenants/Subscriptions (Azure)

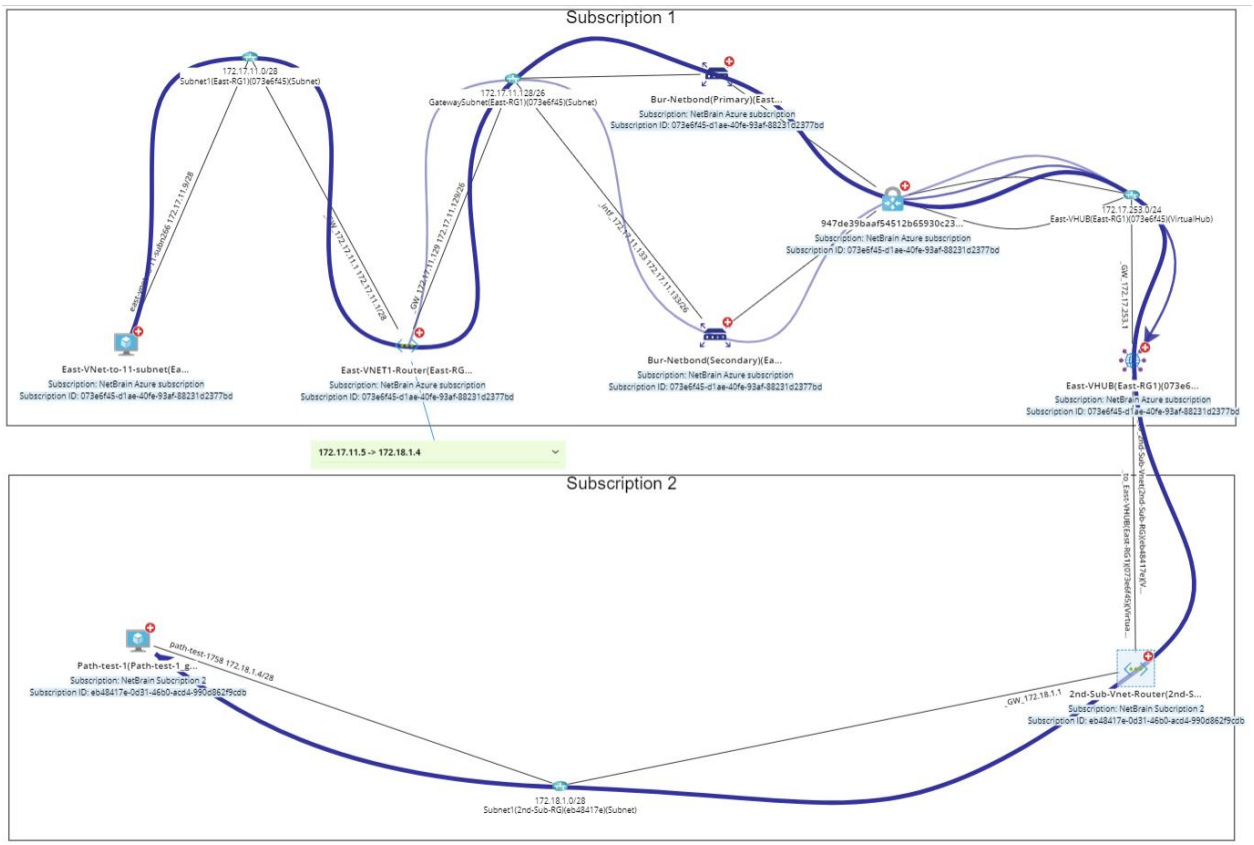
Enterprise customers may have a lot of AWS accounts and Azure subscriptions for data isolation. The application path may traverse multiple accounts/subscriptions. By setting API access to multiple accounts and subscriptions, NetBrain will be able to visualize the traffic path across multiple accounts as well as multiple subscriptions.

NetBrain can visualize the peering details if the crossing subscription/tenant is using VNet Peering.

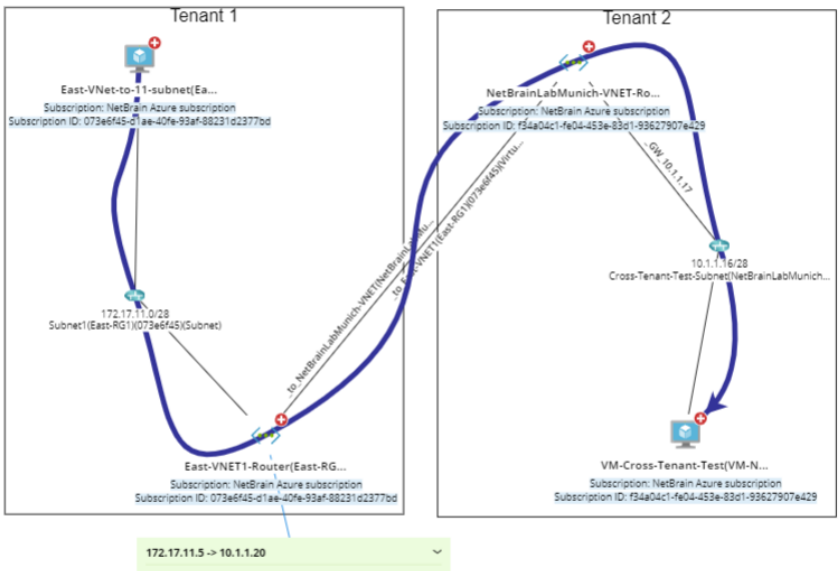


Peering Name	Peering Status	Neighbor VNET ID	Allow Gateway Transit	Use Remote Gateways	Allow Forwarded Traffic	Allow Virtual Network Access
Hub-VNET-To-Spoke-VNET3	Connected	/subscriptions/073e6f45-d1ae-40...	Enabled	Disabled	Enabled	Enabled
Hub-VNET-To-Spoke-VNET4	Connected	/subscriptions/073e6f45-d1ae-40...	Enabled	Disabled	Enabled	Enabled
Hub-VNET-To-Spoke-VNET2	Connected	/subscriptions/073e6f45-d1ae-40...	Enabled	Disabled	Enabled	Enabled
Hub-VNET-To-Spoke-VNET1	Connected	/subscriptions/073e6f45-d1ae-40...	Enabled	Disabled	Enabled	Enabled
EastVNetHub-to-Spoke5-samere...	Connected	/subscriptions/073e6f45-d1ae-40...	Enabled	Disabled	Disabled	Enabled
TenantA-To-B	Connected	/subscriptions/f34a04c1-fe04-45...	Disabled	Disabled	Disabled	Enabled
Global_Peer_Test	Connected	/subscriptions/eb48417e-0d31-4...	Disabled	Disabled	Enabled	Enabled

Azure crossing subscription path sample:



Azure crossing Tenant sample:



1.3.4.Multi-Cloud Support

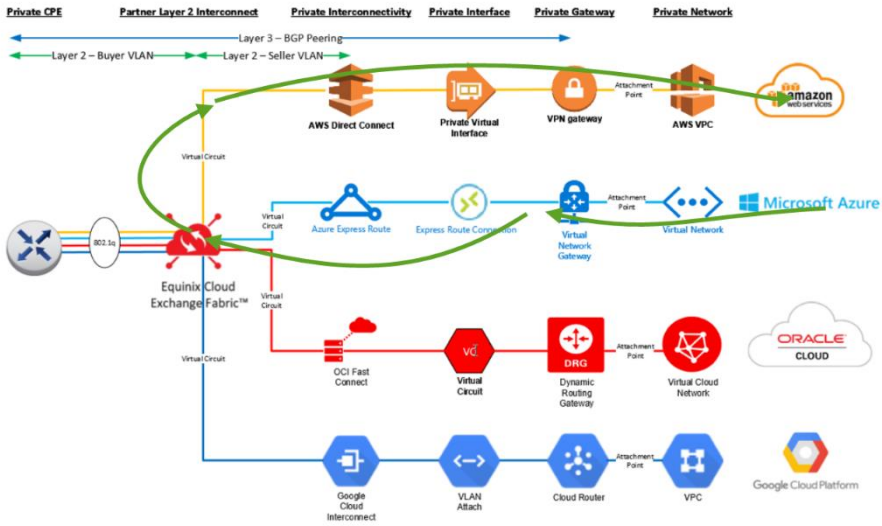
You may have one or more public cloud providers, with NetBrain's support for multiple cloud providers, you will be able to get a complete view of your public cloud infrastructure as well as the traffic flow going through multiple public cloud providers.

Following is the typical multi-cloud application design patterns:

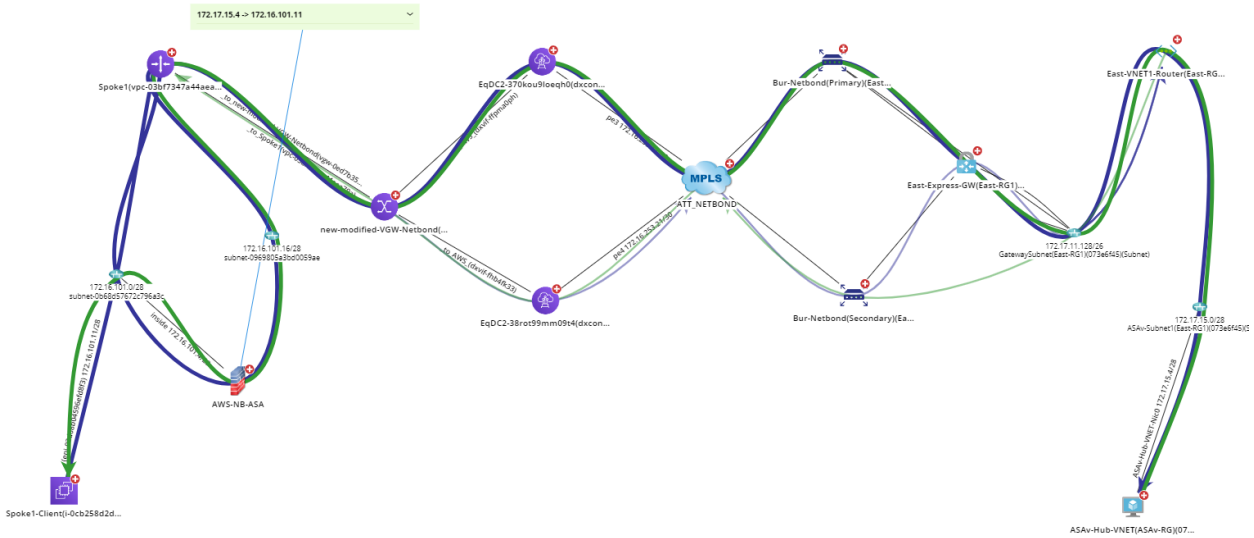
- Public Cloud Exchange via Cloud Exchange Provider Cloud
- Public Cloud communicate via IPSec Tunnels provided by cloud Virtual Appliances

1.3.4.1. Public Cloud Exchange via Cloud Exchange Provider Cloud

The following diagram depicts the typical dedicated cloud interconnect solution provided by different cloud providers. NetBrain is able to map the entire topology as well as the path going through multiple cloud providers.

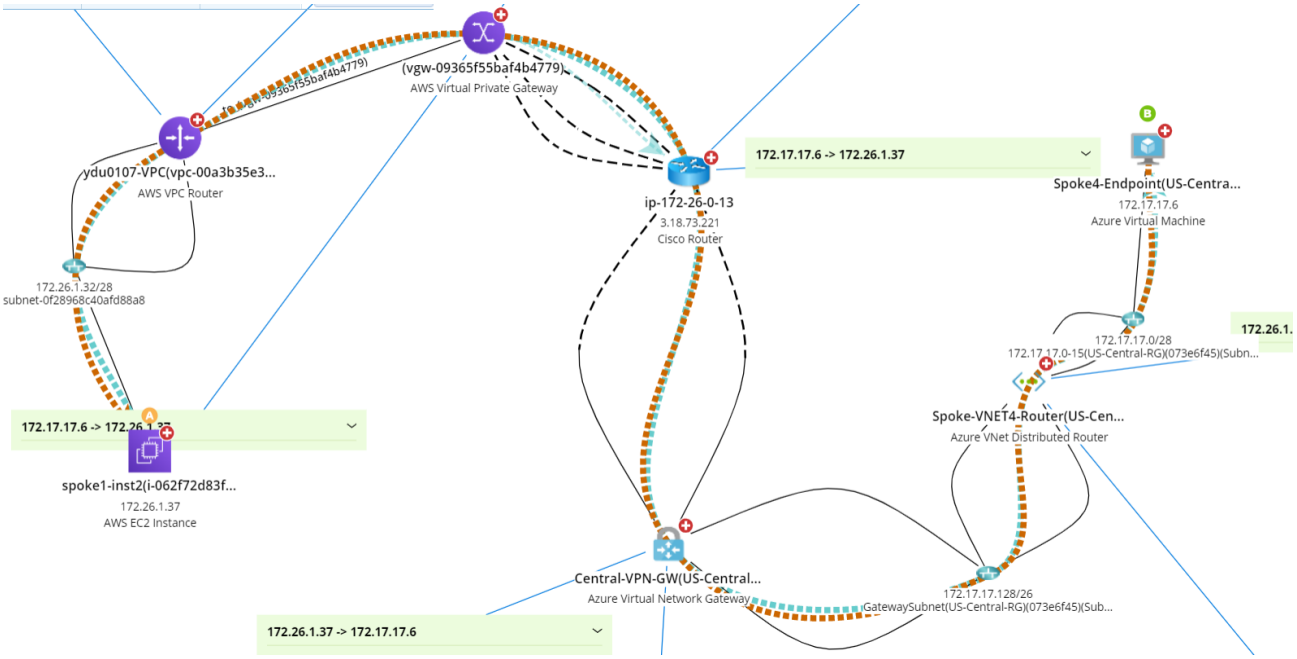


After setting up the benchmark to retrieve the data successfully, NetBrain will be able to calculate the path across public clouds. The following diagram shows how an EC2 instance can communicate with the virtual machines sitting on Azure via AT&T Netbound.



1.3.4.2. Public Cloud communicate via IPSec Tunnels provided by cloud Virtual Appliances

You can also use the transit VPC architecture to build the IPSec VPN tunnel between different cloud providers so the traffic flow can go through transit VPCs.



1.4. SPOG with Cloud Native Management Tools

NetBrain's data view function gives you the ability to monitor various public data in NetBrain environment. This chapter will focus on explaining how NetBrain system manages to visualize the data from public cloud providers in its dynamic map. There are basically two kinds of data that can visualized by NetBrain:

- **Public Cloud Infrastructure Data**: this involves the basic information of cloud operational status, routing/security, tag information etc.
- **Cloud Monitoring Metrics**: this involves the monitoring metrics from the cloud native monitoring tools, such as AWS CloudWatch and Azure Monitoring. These metrics are usually data plane status that can be visualized in NetBrain maps.

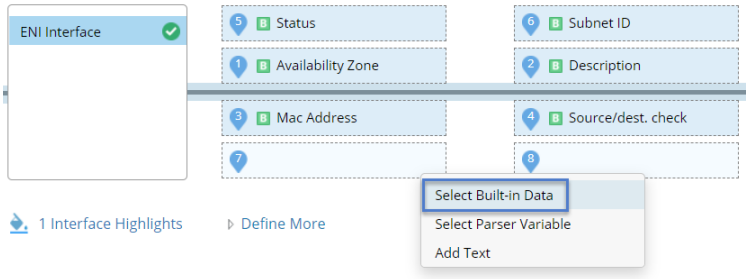
In order to visualize the relevant data using DVT, you can leverage the following two types of data:

- **GDR Data:** GDR data is already available for use since this type of data is retrieved during the discovery/benchmark process.
- **API Parser Data:** By using the API parser, you can retrieve any data from public cloud provider.

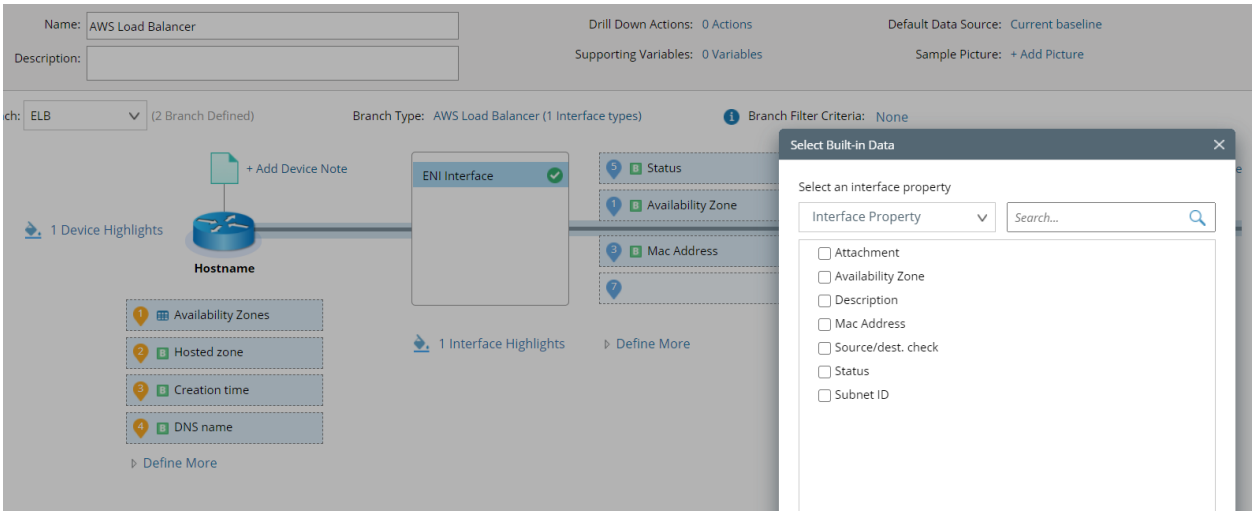
Building Data View Template with Public Cloud GDR Data

Since NetBrain uses API to retrieve the data from AWS for the related networking objects, the system makes some of these data available for you to select when using the data view template. You can re-organize and select the data you want to use in data view template based on your specific needs.

In order to select these data, you need to select the branch type first and then click the **Select Built-in Data** option.



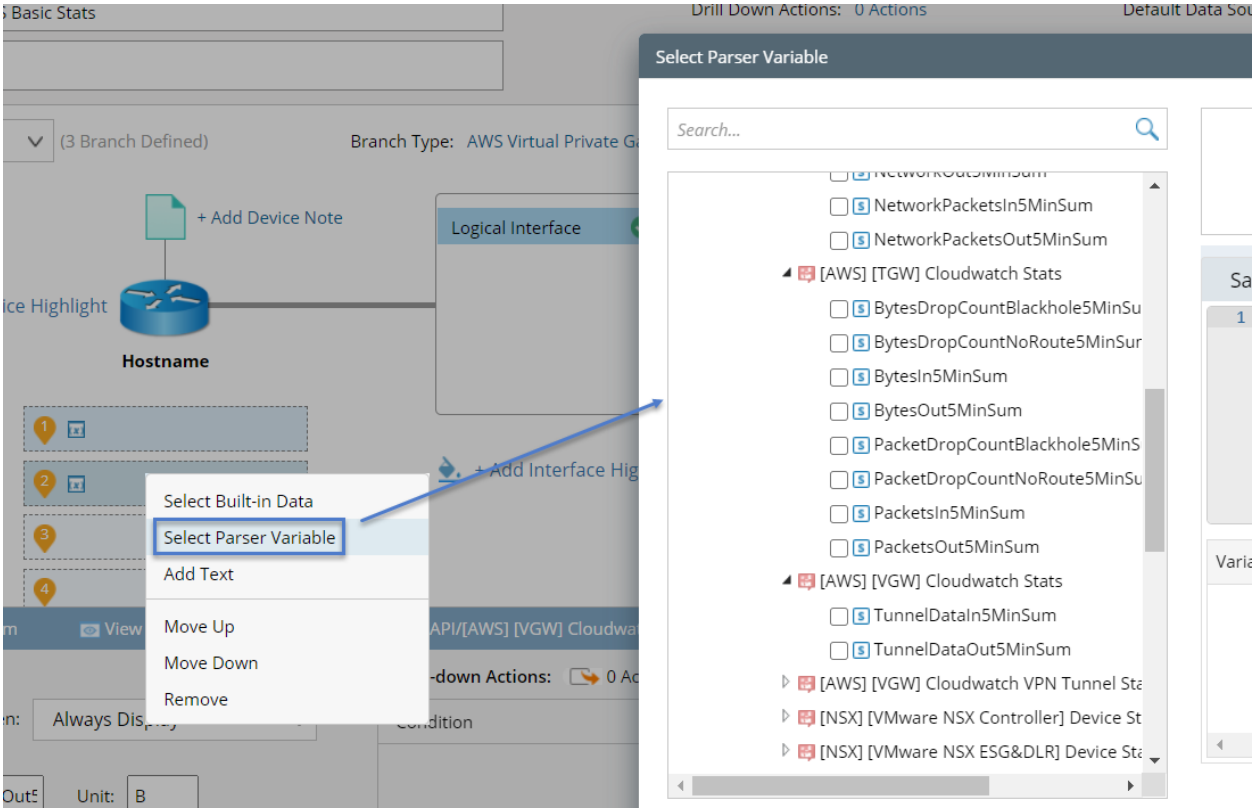
The following screenshot demonstrates the data you can select for the elastic load balancer. The selectable data will vary according to the type of network object.



Note: *Since the selected data is retrieved from the GDR stored in MongoDB, when you apply the Data View including the AWS GDR data, these data is cached from the system and will be retrieved during the latest discover/benchmark process. The data presented is infrastructure data and rarely changes.*

Building Data View Template with API Parser Data

To retrieve more types of data from AWS (e.g., live CloudWatch data), you will need to use the API parser to retrieve the data from AWS and then select respective Parser Variables. As the API parser data can be retrieved from live network with desired frequency, you can use this method to build your Data View Template if you need to pull the data from live.



Sample Data View Templates provided by NetBrain

NetBrain has built a lot of useful data view templates based on different use cases. We will go through some of these data view templates with the design intent. Please be aware that these data view templates are for reference purpose only. Thanks to the scalability of NetBrain platform, the function can be extended to any interested data.

1.4.1.SPOG with AWS Cloud Infrastructure Data

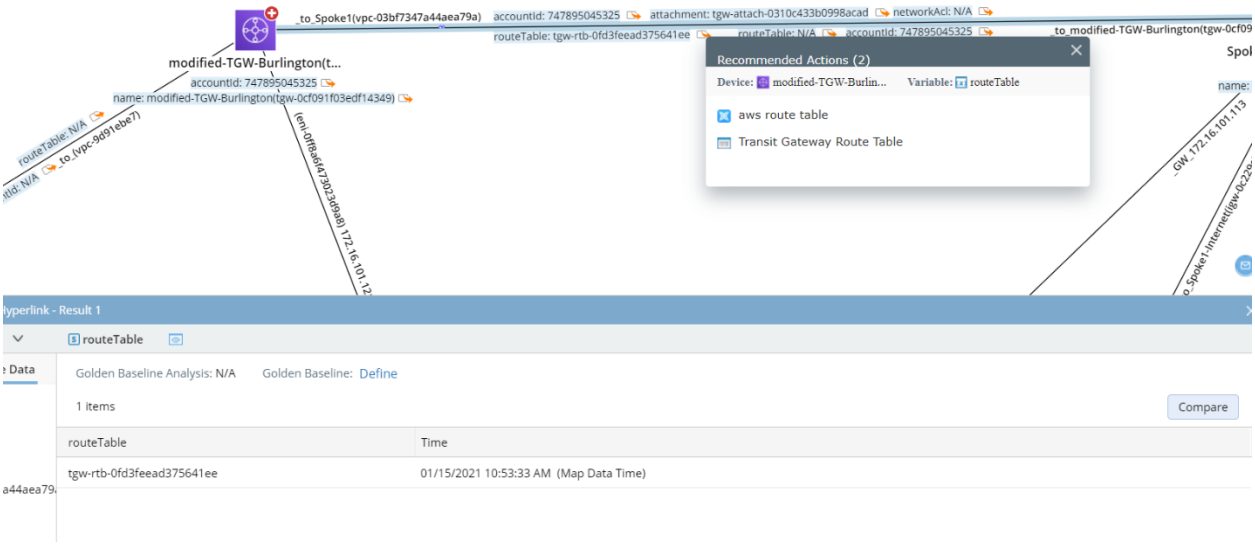
The following Data View Templates make it possible to visualize different types of AWS cloud infrastructure data in NetBrain dynamic map:

- Resource Links and Account Info
- Infrastructure View for Resources
- Cloud Interconnect BGP Design

1.4.1.1. Resource Links and Account Info

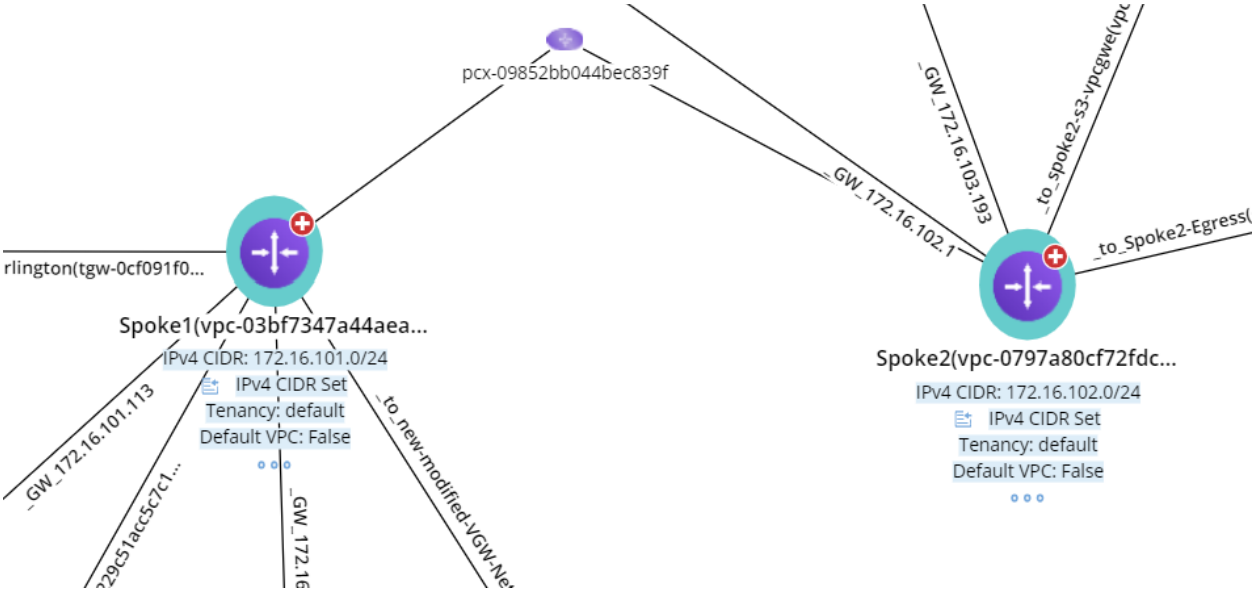
This data view template can visualize the account information for different networking objects and it provides the link to AWS management console.

Links are also available for resources such as ENI interfaces, security groups and network ACLs.



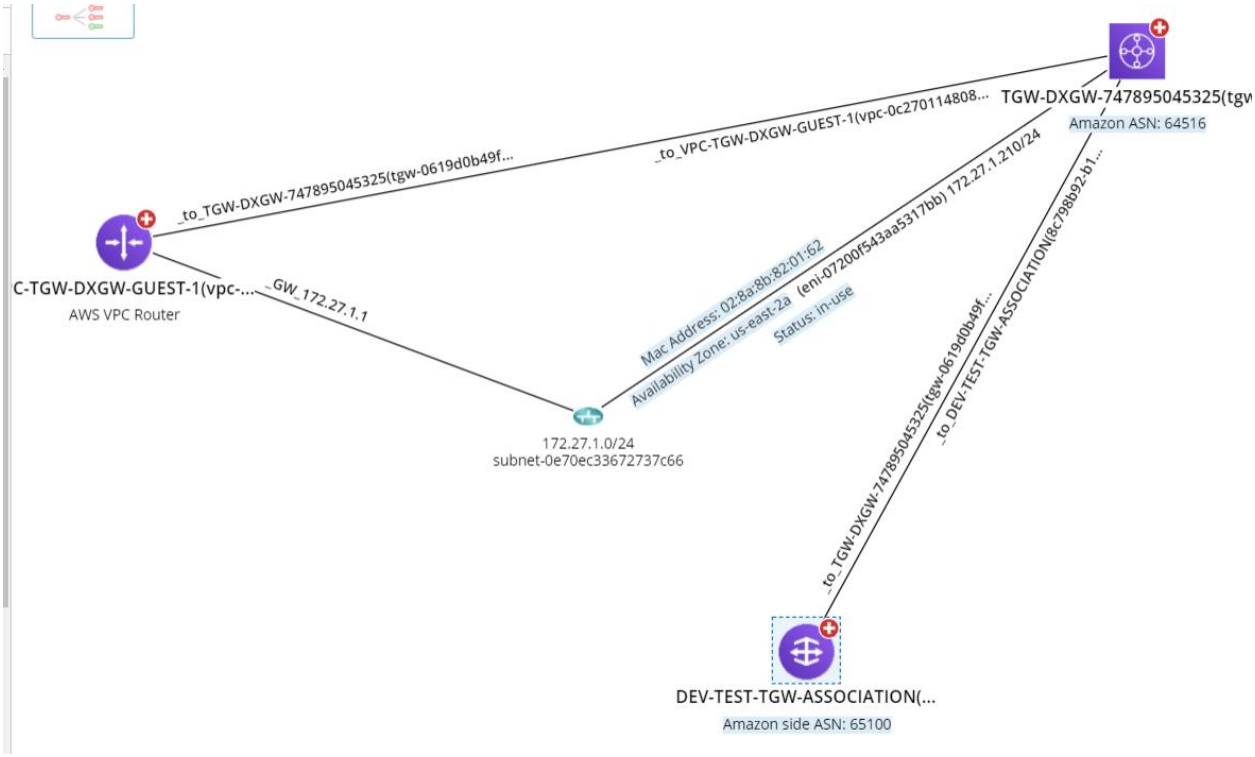
1.4.1.2. Infrastructure View for Resources

This data view template can visualize the infrastructure information for different networking objects.



1.4.1.3. Cloud Interconnect BGP Design

This data view template can demonstrate the detailed information about your Cloud Interconnect design. It visualizes all AS number from AWS and the advertised route details of the customer's gateway devices.

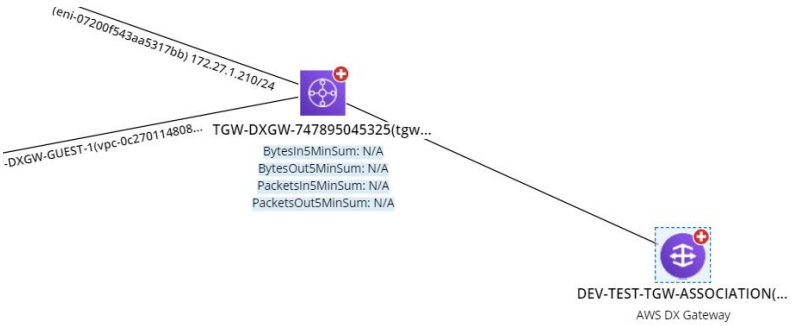


1.4.2.SPOG with AWS CloudWatch

1.4.2.1. CloudWatch Basic Statistics

This data view template demonstrates the metrics retrieved from AWS CloudWatch. It currently includes the following information:

- EC2 status
- VGW Tunnel status
- Direct Connect Status per Physical Connection
- Direct Connect Status per Virtual Interface
- TGW entire status
- TGW status per Attachment
- ELB Status



1.5. SPOG with 3rd Party Cloud Management Tools

The ability to visualize data from 3rd Party cloud management tools enables NetBrain dynamic map to render a complete view of your cloud infrastructures. The integration with 3rd Party cloud management tools is highly customizable meaning NetBrain can be integrated with any cloud management tools to suit your specific needs. The following integrations are the SPOG solutions currently supported by NetBrain:

- Datadog - AWS/Azure Monitoring Metrics
- Splunk – VPC Security Group Check Log

1.5.1.Datadog - AWS/Azure Monitoring Metrics

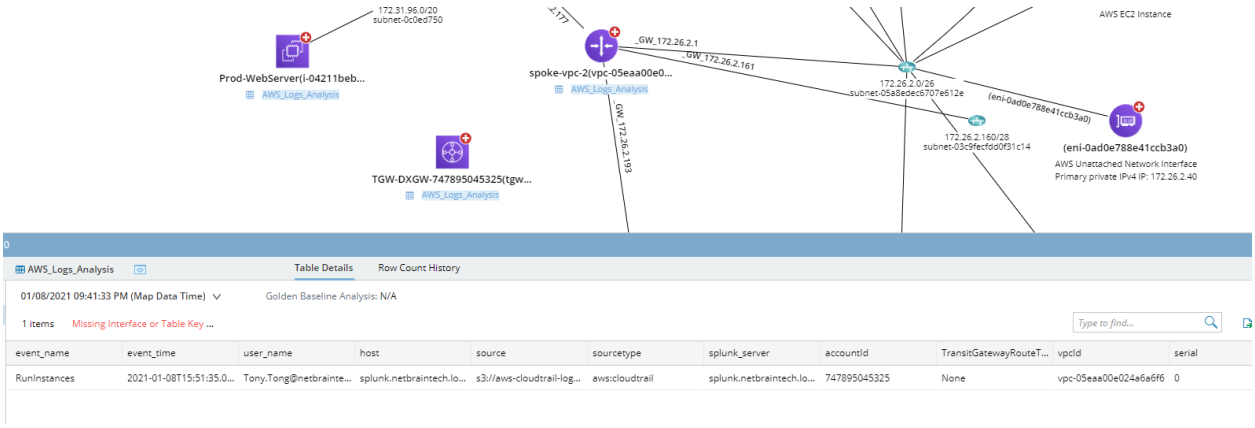
The following data view demonstrates the integration with Datadog- the metrics are retrieved from the Datadog agents installed on EC2 instances. NetBrain can retrieve and demonstrate the following types of metrics through the data view template:

- system.cpu.user (5 min aveg - double)
- system.mem.pct_usable (5 min aveg - double)
- system.uptime (The last non-empty value of the 5 min - int)
- system.net.packets_out.error (5 min aveg - int)
- system.disk.free (5 min aveg - int)
- system.io.r_s (5 min aveg - int)
- system.net.packets_in.error (5 min aveg - int)

NetBrain also provides a link to Datadog so you can easily switch to Datadog to explore more details.

1.5.2.Splunk – VPC Security Group Check Log

AWS CloudTrail is a service that allows you to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. The integration with Spunk allows you to view change log of security groups/network ACL and much for VPCs during a specific period of time.



1.6. Runbook Automation for Public Cloud

Runbook Template can be used to help you understand the network design and also troubleshoot network problems based on certain scenarios. A lot of useful functions such as DVT, Qapp, Gapp and Compare can be wrapped into Runbook to accomplish your tasks.

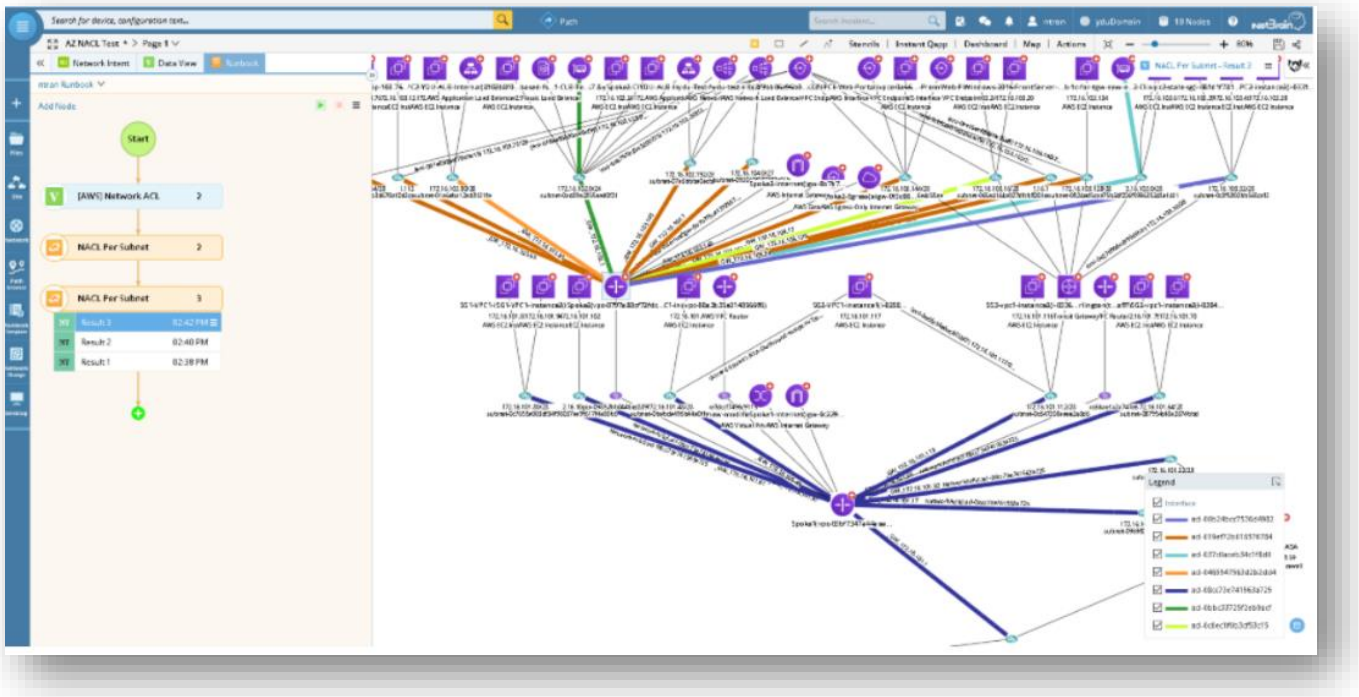
The following are some of the sample Runbooks we have provided based on some Troubleshooting scenarios:

- AWS - Troubleshoot General VPC Info
- AWS - Troubleshoot Transit Gateway Connectivity Issue

1.6.1.AWS - Troubleshoot General VPC Info

This runbook can help you quickly identify important resource information for the devices on map, which includes:

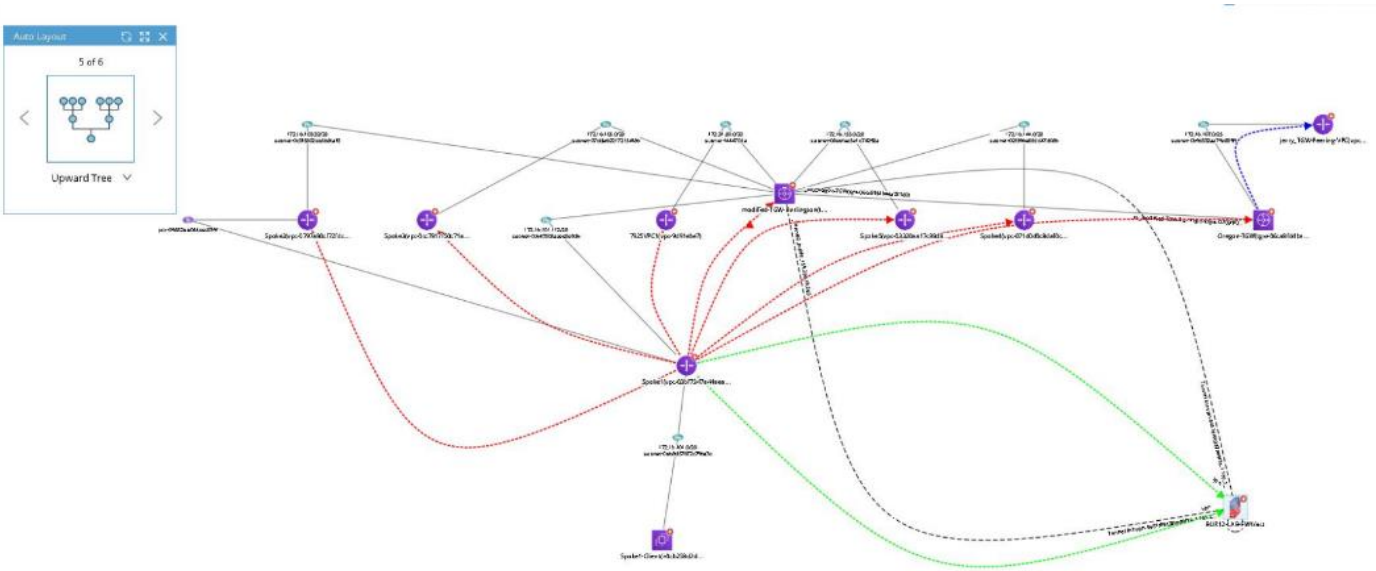
- Path - Application Path
- DVT - [AWS] Resource Links and Account Info
- DVT - [AWS] Infrastructure View for Resources
- DVT - [AWS CloudWatch] Basic Stats
- Qapp - Security Group
- Qapp - Network ACL



1.6.2.AWS - Troubleshoot Transit Gateway Connectivity Issue

This runbook can help customers troubleshoot the transit gateway routing issue and understand the current deployment. This Runbook includes:

- Path - Application Path
- DVT - AWS basic stats DVT
- Qapp - Map reachability from specific VPC
- Qapp - Map reachability from specific TGW Route Table
- Compare - Compare TGW NCT Tables (Attachment table/Route Table)


Auto Layout
5 of 6
Upward Tree