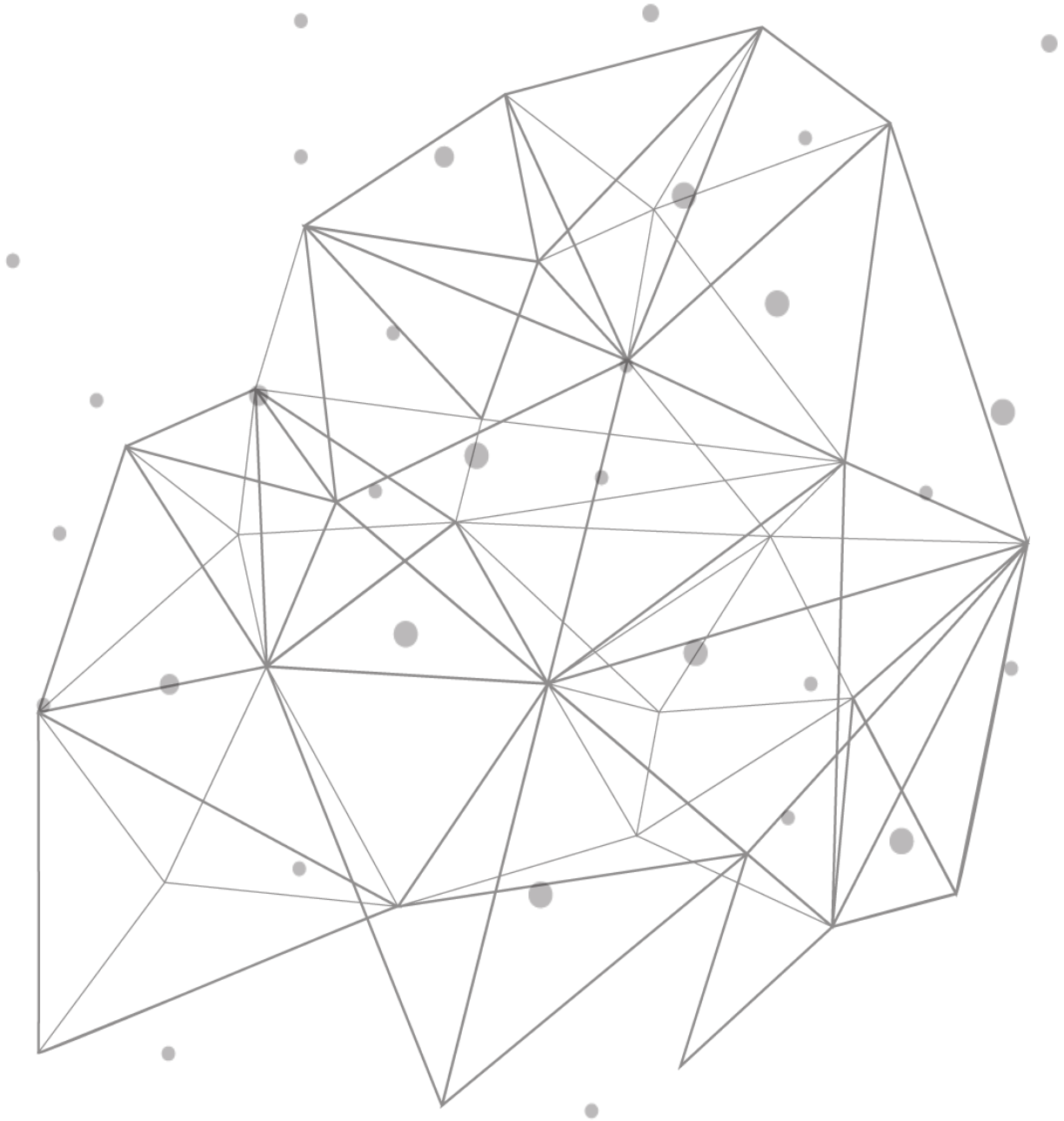
Split-Brain DNS Approach



Introduction

Nowadays, enterprises find themselves between a rock and a hard place in implementing DNS that prevents external clients from knowing the layout of the internal network. Some enterprises need internal and external domains to use the same domain name instead of separate namespaces. To hit the nail on the head for such a scenario, enterprises need to implement the Split-Brain DNS approach.

Split-Brain DNS

Split-Brain DNS is a DNS configuration method that enables proper name resolution of local resources inside and outside your local network. It provides different data regarding the contents of a DNS zone based on the location that the DNS query originates. Separate DNS namespaces are administered for external computers and internal ones.

Example: The DNS query for the host www.test.com may return a public IP address and a private IP address on the organization's internal network.

The goal of a Split-Brain DNS is to provide abstraction and enhance security by not divulging the correct internal IP address of the requested resource. You can implement Split-Brain DNS on Microsoft appliance using DNS Resolution Policies and DNS Zone Scopes.

DNS Resolution Policy & DNS Zone Scope

DNS Resolution Policies allow you to modify DNS server responses centered on the properties. DNS Zone Scopes allow you to create distinct DNS zone records, with each zone supporting multiple Zone Scopes, and DNS records can be members of various Zone Scopes.

With Split-Brain DNS, one can split the DNS records into different Zone Scopes on the same DNS server, and DNS clients receive a response based on whether the clients are internal or external.

Split-Brain DNS Configuration

You must implement the following on Microsoft appliance to configure Split-Brain DNS:

1. Add Zone Scopes
2. Add Resolution Policy
3. Add Resource Records

Note: You are required to execute PowerShell commands to add Zone Scopes and Resolution Policies

Adding Zone Scopes

Execute the following command to add a zone scope:
ADD-DNSSERVERZONESCOPE

Example: ADD-DNSSERVERZONESCOPE -name testScope -zoneName <zonename>

Adding Resolution Policy

- When creating a DNS policy, you must configure DNS zone scopes with one zone scope containing the host records that return to an external user and another DNS zone scope containing host records that return to internal users.
- Once the configuration of the two-zone scope is done, you must configure DNS policies.

- One policy configuration to return records from DNS zone scope to be used by external users, the other policy configuration to return records from the DNS zone scope to be used by internal consumers.
- The usual practice is to place all records that need to be available to users on the internet into the default zone scope.
    - All records must be available to internal users in the internal scope.
    - Once this is done, create a policy that allows access to the internal scope only for queries originating on the client subnets.

You create query resolution policies with the Add-DNSServerQueryResolutionPolicy cmdlet as shown in the example below:

Example: Add-DnsServerQueryResolutionPolicy -Name "1NorthAmericaPolicyFinal" -Action ALLOW -ClientSubnet "eq,NorthAmericaSubnet" -ZoneScope "internal,1"-ZoneName <zonename>

Client Subnet is one of the DNS parameters used to manage the DNS Resolution Policy. It represents either IPv4 or IPv6 subnet where the query originates from. Execute the following command to add a client subnet: Add-DnsServerClientSubnet.

Example:
Add-DnsServerClientSubnet -Name "NorthAmericaSubnet" -IPv4Subnet 172.21.33.0/16

Adding Resource Records

Execute the following command to add a zone scope:
Add-DnsServerResourceRecordA

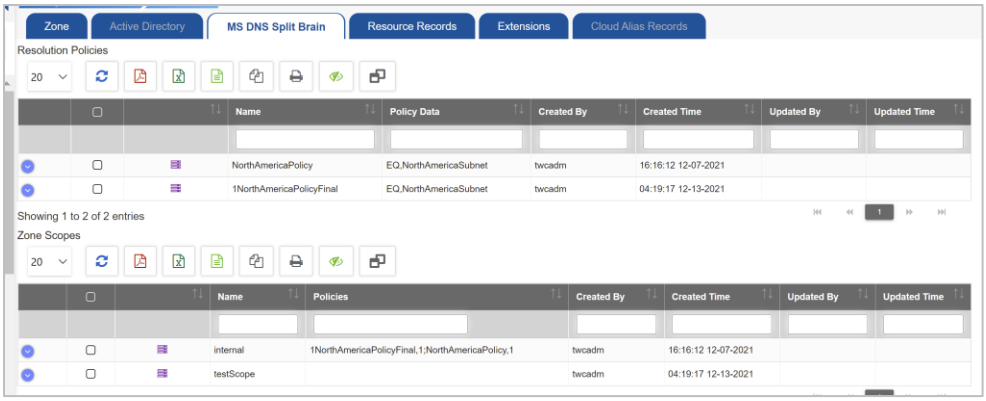
Example: Add-DnsServerResourceRecordA -Name "newrecord" -ZoneName <zonename> -IPv4Address "67.7.7.164" -TimeToLive 01:00:00 -ZoneScope internal

Note:

- You can update and delete the Resolution Policies on the Microsoft DNS appliance using the following commands:
- Set-DnsServerQueryResolutionPolicy
- Remove-DnsServerQueryResolutionPolicy
- You can delete the Zone Scopes on the Microsoft DNS appliance using the following command:
- Remove-DnsServerZoneScope

Viewing Data in TCPWave IPAM

When the zone is associated with the DNS zone template for which the Microsoft DNS appliance is master, the system imports the Zone Scopes and Resolution Policies from the Microsoft DNS appliance for the specified zone upon performing full sync or zone's force sync or auto sync operation. The Zone Scopes and Resolution Policies are displayed in the respective tabs as shown:



Conclusion

TCPWave delivers superior standards by offering scalable, integrated approaches like the Split-Brain DNS approach, etc. For more information on how TCPWave and its extensive features can meet your requirements, contact the TCPWave Sales Team.