Azure VWAN

Proposal for a Network Segmentation User Interface

# Introduction

A VWAN hub & spoke topology is not segmented by default, permitting communication between all spokes and branches. There are two basic strategies to segment and control flows between spokes:

1. Filtering: all spokes can route to each other via a firewall placed in the hub, with firewall policy controlling flows. All traffic flows through the central firewall and is visible in firewall logs.
2. Routing: spokes are segmented into domains and can route without restriction within the same domain. Spokes are not aware of routes for anything outside of their domain. Domains may be connected, so that routing between spokes in those domains is possible.

The filtering approach is enabled through Azure Firewall or a firewall NVA in the VWAN hub. This is built and operated through graphical user interfaces in Firewall Manager, and Azure Firewall Policies or the firewall product’s policy management engine such as Checkpoint Provider1 or Palo Alto Panorama. These interfaces are well understood by users with a general understanding of networking.

The Routing approach to segmentation in VWAN works through the custom routing capability (<https://learn.microsoft.com/en-us/azure/virtual-wan/scenario-isolate-vnets-custom>). This involves direct manipulation of routing tables and association and propagation, which requires expert knowledge of the VWAN technology. Customers and partners generally understand routing, but the specific implementation details in VWAN present a learning curve and can be a hurdle.

This document proposes a user interface overlay on the existing VWAN custom routing capability. It presents network segmentation functionally, abstracting the implementation detail of VWAN custom routing.

## Segmentation Domains

Spokes are grouped into Segmentation Domains. Routing within a Domain is unrestricted: all Spokes within a Domain learn each other’s routes. Routing across Domains is blocked by default: Spokes in one Domain do not learn routes to other Domains.

Branches (ExpressRoute- and VPN-connected sites) remain in a Default Domain, along with any Spokes that are not explicitly placed in any other Domain.

The scope of each Segmentation Domain is the entire Virtual WAN, meaning Domains span Hubs and there is no concept of a “local” or “per Hub” Domain. It is obviously possible to add only Spokes connected to a single Hub to a Domain, and no other Spokes. However, the Domain itself exists in the entire Virtual WAN, and Spokes connected to other Hubs could be added to it.



## Linked Groups

Cross Domain routing is enabled explicitly by grouping Domains into Linked Groups. Spokes then learn all routes for all Domains in the Group. Branch to Spoke routing is controlled by adding the Default Domain to one or multiple Linked Groups.

The connectivity matrix for example in the diagram below is as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | S1 | S2 | S3 | S4 | S5 | S6 | S7 | S8 | S9 | S10 | S11 | B1 | B2 | B3 | B4 |
| S1 | √ |  | √ | √ |  |  | √ |  | √ |  | √ | √ | √ | √ | √ |
| S2 |  |  |  |  |  |  |  | √ |  | √ |  |  |  |  |  |
| S3 | √ |  | √ |  |  |  |  |  | √ |  | √ | √ | √ | √ | √ |
| S4 | √ |  | √ |  |  |  |  |  | √ |  | √ | √ | √ | √ | √ |
| S5 |  |  |  |  | √ | √ |  | √ |  | √ |  |  |  |  |  |
| S6 |  |  |  |  | √ | √ |  | √ |  | √ |  |  |  |  |  |
| S7 | √ |  | √ |  | √ | √ |  |  |  |  | √ | √ | √ | √ | √ |
| S8 |  | √ |  |  | √ | √ |  | √ |  |  |  |  |  |  |  |
| S9 | √ |  | √ |  |  |  |  |  | √ |  |  |  |  |  |  |
| S10 |  |  |  |  | √ | √ | √ | √ |  | √ | √ | √ | √ | √ | √ |
| S11 | √ |  | √ | √ | √ | √ |  |  |  | √ | √ | √ | √ | √ | √ |
| B1 | √ |  | √ | √ | √ | √ |  |  |  | √ | √ | √ | √ | √ | √ |
| B2 | √ |  | √ | √ | √ | √ |  |  |  | √ | √ | √ | √ | √ | √ |
| B3 | √ |  | √ | √ | √ | √ |  |  |  | √ | √ | √ | √ | √ | √ |
| B4 | √ |  | √ | √ | √ | √ |  |  |  | √ | √ | √ | √ | √ | √ |



## User Interface

A Windows application demonstrates an implementation of the VWAN Segmentation User Interface:

Graphical user interface

Description automatically generated

## Subscription, Resource Group and Virtual WAN

After login to Azure, the user selects the subscription and resource group containing the target Virtual WAN from drop down boxes.

The Hubs in the VWAN instance selected are listed.

Graphical user interface, text, application

Description automatically generated

## Select Hubs

User selects a Hub, and connected Spokes are listed:

Graphical user interface, application

Description automatically generated

## Create Segmentation Domains

User enters name of Segmentation Domain to be created in text box and clicks Add Domain:

Graphical user interface, text, application

Description automatically generated

## Add Spokes to Domains

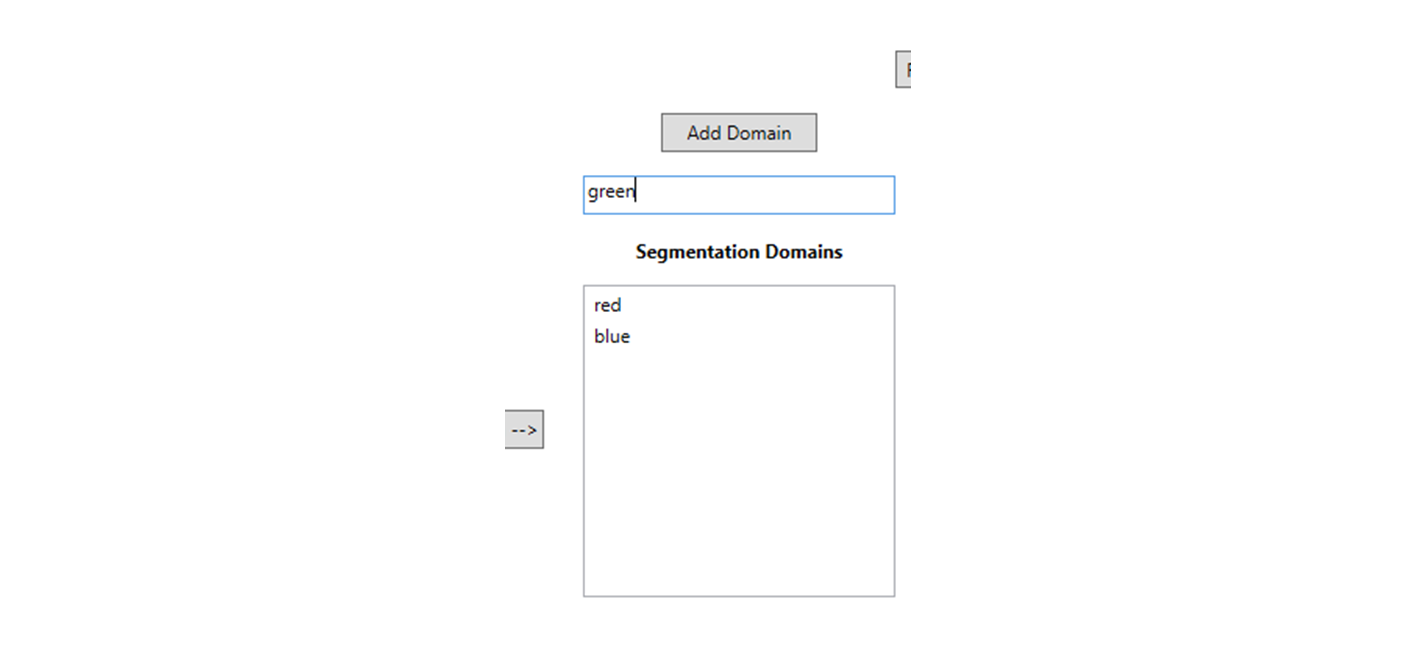
User now adds Spokes to Domains by selecting multiple Spokes under Spoke Connections, and one Domain under Segmentation Domains, and clicking Add Spokes to Domain:

## Graphical user interface, application, Word Description automatically generated

The process is repeated for Spokes connected to other Hubs.

## Create Linked Groups

User can now create Linked Groups and add Domains to Groups, to enable Domain interconnectivity:



Graphical user interface, application

Description automatically generated

## Commit

When configuration is complete, user commits to Azure by clicking Program Segmentation Domains.



This starts the configuration of Custom Routing Tables on the VWAN Hubs.

## Inspect

Lower part of the application window contains elements to inspect the configuration.

Graphical user interface, application

Description automatically generated

## Implementation