FORTINET

DEPLOYMENT GUIDE

Securing Azure Windows Virtual Desktop Guidebook

Securing Azure Windows Virtual Desktop Guidebook

Introduction

Fortinet is a leading provider of information and cybersecurity solutions through an integrated portfolio protecting against a broad range of threats leveraging cloud-aware automated workflows that are deeply integrated into Microsoft Azure. This guidebook will explain how Fortinet and Microsoft capabilities come together to provide a more secure and useful Windows Virtual Desktop (WVD) experience.

Windows Virtual Desktop is a comprehensive desktop and app virtualization service running in the cloud, providing simplified management, multi-session Windows 10, optimizations for Office 365 ProPlus, and support for Remote Desktop Services (RDS) environments. Windows Virtual Desktop is a powerful tool to support remote work, especially in situations where employees, partners, customers, or students are using their personal devices.

Azure customers can deploy WVD within Azure virtual networks (VNets). Typically, these deployments require advanced routing and security for connecting to data centers, branches, and for client-to-site access to Azure resources. The Fortinet FortiGate next-generation firewall (NGFW) adds to Azure's core capabilities by providing network inspection across all of these footprints with virtual private network (VPN) interconnections from the endpoint, through the premise, and into the cloud.

Teleworking and distance learning rely on Azure's WVD to provide scalable environments for desktop productivity services. Users connect to the Azure environment via client-to-site secure sockets layer (SSL) VPNs and log into the remote desktop provisioned for their user credentials. Users will then access internet, Microsoft services such as Office 365, and the corporate data center. This guide will address the following common needs to optimize the user experience and data security for WVD environments:

- Remote client-to-site access
- Optimized routing of Microsoft Office traffic
- Configuring FortiGate deep packet inspection and WVD policies
- Scalable site-to-site IPsec VPN for data-center connectivity

The figure below depicts the overall network layout of a VNet supporting WVD connected to a remote enterprise location. Remote users connect directly to local region Azure resources. Traffic from WVD sessions is default routed to the FortiGate for inspection and filtering. Microsoft control-plane and Office data remains on-net while data center-bound traffic is directed to the Express Route or VPN. While not covered in this guide, FortiGate Secure SD-WAN features can be configured to shape traffic across different links to the data center.

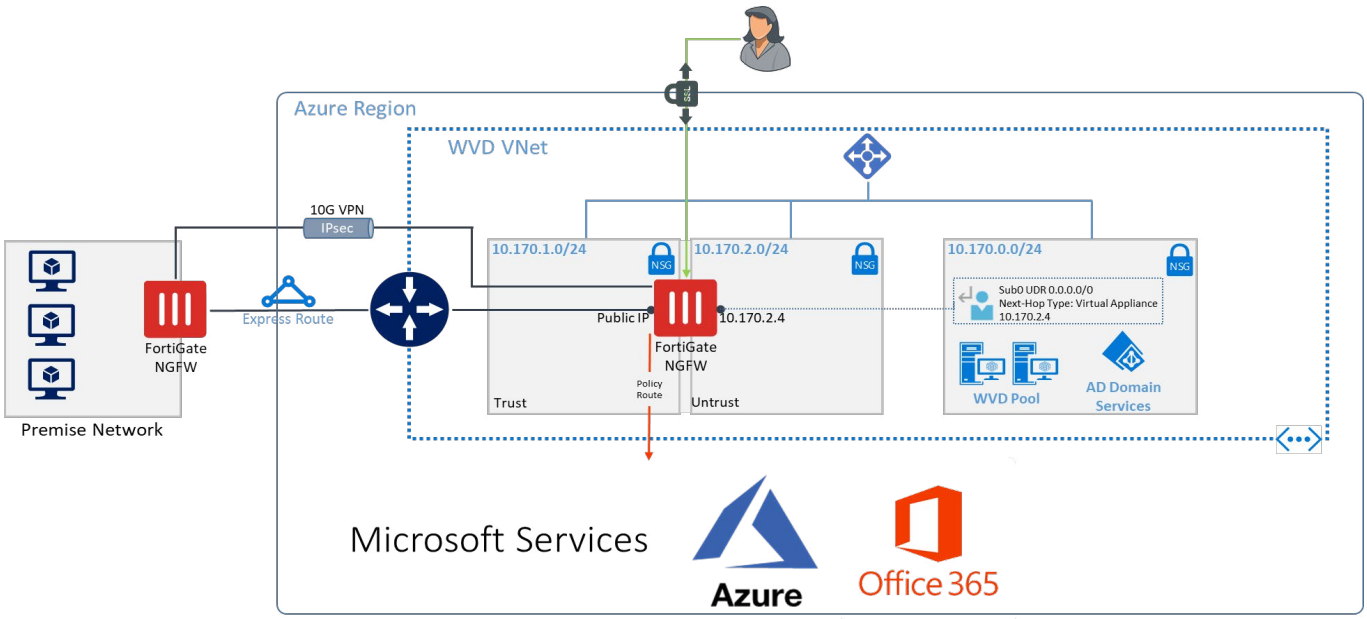


Figure 1: Remote user access to Azure.

NOTE: While not depicted, FortiGates are typically deployed in highly available pairs.
Documentation for this can be found at https://docs.fortinet.com/vm/azure/fortigate/6.2/azure-cookbook/6.2.0/983245/ha-for-fortigate-vm-on-azure

Remote Client-to-Site Access

Users connecting to their WVD services will need a secure away to reach those services. SSL VPNs are the most scalable and common way to do this. Managing user groups and permissions, routing, address space, and security profiles must be considered for the types of user roles to be provisioned. The figure below isolates the remote access SSL VPN use case.

While not required, the SSL VPN service could be set up with a dedicated SSL VPN front-end IP address. An FQDN can be registered to the IP address to simplify connectivity for the remote users.

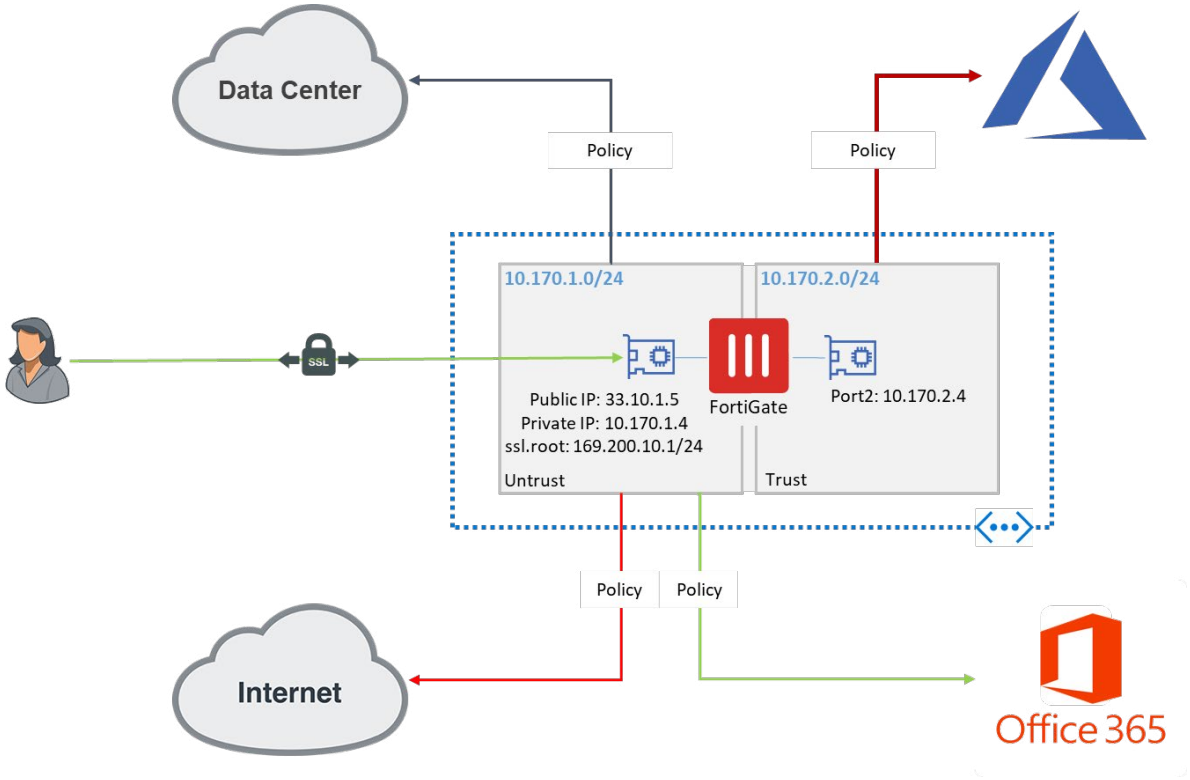


Figure 2: Remote SSL VPN user service access.

Configuring SSL VPN user access for such a scenario can be summarized with the following steps:

1. Configure the Azure NSG to allow the SSL VPN port
2. Configure SSL VPN user group
3. Configure the SSL VPN tunnel mode interface and IP address range
4. Configure policies for each user service
5. Configure default and policy routes for data center, internet, and on-net Microsoft services

Step 1: Configuring the Azure NSG to allow SSL VPN Port

Step 2: Configuring SSL VPN Services

In this step it is assumed that users would be imported from an Active Directory source such as LDAP. Other user types, such as RADIUS, local users, and SAML users, can be supported.

Create the LDAP Server to import user groups

a. In the FortiGate GUI, navigate to **User & Devices → LDAP Servers → Create New**

b. Enter the following information:

- Name – Unique name for the LDAP server on the FGT
- Server IP/Name – the IP or FQDN of the LDAP source

- Server port – Default is 389
- Distinguished name
- Select the Bind type
- Provide a Username and Password for the LDAP admin account
- Selecting “Secure Connection” will enable LDAPS
- Test the connection. Connection status should return “Successful”

Additional configuration details can be found at https://kb.fortinet.com/kb/documentLink.do?externalID=FD46240

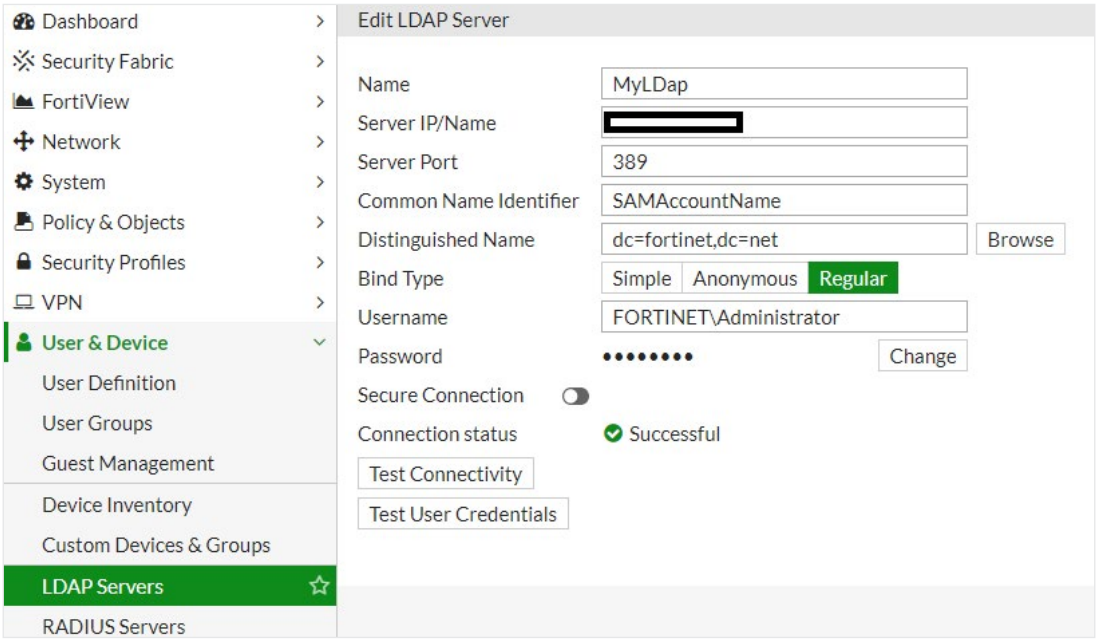


Figure 3: Configuring LDAP Server on FortiGate access.

Import LDAP Users

c. Next, import users from LDAP by navigating to **User & Devices → User Definition → Create New**

d. Choose ‘Remote LDAP Server’ and click ‘Next’

e. Select the LDAP Server name created in Step 2a. and click ‘Next’

Configure Tunnel Mode SSL portal

f. In the FortiGate menu, select VPN → SSL-VPN

g. Edit the “tunnel access”

- Disable “Enable Split Tunneling”

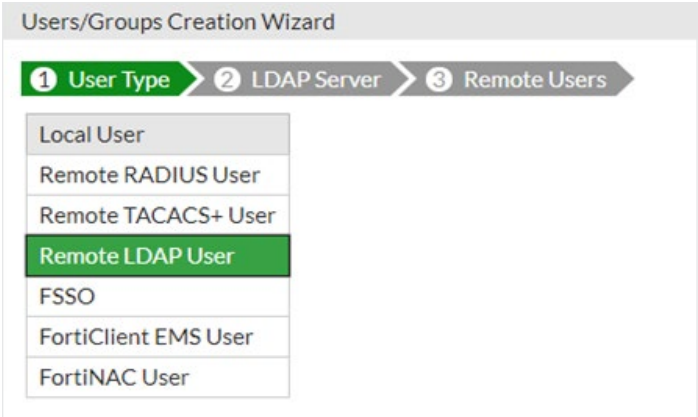


Figure 4: Import LDAP users.

Configure SSL VPN Settings

These next steps will configure the actual SSL VPN interface. This will map the ssl.root interface to the correct public-facing port. Additionally, it is a best practice to configure the listener to a port other than 443 as a best practice. A certificate should be imported to the FortiGate; else the default FortiGate Factory certificate will be used. Using the FortiGate Factory certificate will prompt a warning and is not a best practice.

h. From the menu, select **VPN → SSL-VPN Settings**

- Set the "Listen on Interface(s)" to the public-facing port, typical port1 for Azure's public interface
- Set "Listen on Port" to a port other than 443
- Select an imported server certificate that is trusted by client connections.

NOTE: The following link provides guidance on importing a certificate into FortiOS. Documentation for this can be found at https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/825073/purchase-and-import-a-signed-ssl-certificate

- Under "Tunnel Mode Client Settings," select an IP address range. The default value is 10.212.134.200-10.212.134.210. Change this by selecting "Specify custom IP ranges" in the "Address Range" setting. Take care to ensure this range does not overlap with another Virtual Network range should users be routed from the FortiGate without SNAT.
- In "Authentication/Portal Mapping," set "All Other Users/Groups" to the "tunnel-access" portal configured in Step 2g.

Configure SSL VPN Ingress Access Firewall Policy

The last step in configuring the SSL service is to set a firewall policy as all connections will be blocked by default. The following steps will configure a basic firewall policy. Additional configurations for threat protections are optional. See https://docs.fortinet.com for additional details.

i. Navigate to **Policy & Objects → IPv4 Policy** in the FortiGate menu. This will display the IP policy table for forward traffic (Local-in policies are maintained in a separate table).

j. Select "Create New" and enter the following policy details:

- Name – Enter name for the policy
- Incoming Port – This is the public interface to which SSL VPN users will connect, in this case the *ssl.root* interface.
- Outgoing Interface – If protecting services in the private VNet, ensure that the internally facing port connected to protected subnets is selected. For users egressing for data-center connections or for public access to Microsoft services, ensure those IPsec and public interfaces are included. These use cases will likely involve hairpinning traffic out of the public interface.
- Destination – Select "all"
- Schedule
- Service
- Action
- NAT – Typically this will be enabled to source NAT traffic from the FGT. By default the Outgoing Interface IP address will be used
- Configure additional inspection profiles as needed
- Select "OK" to save the configuration

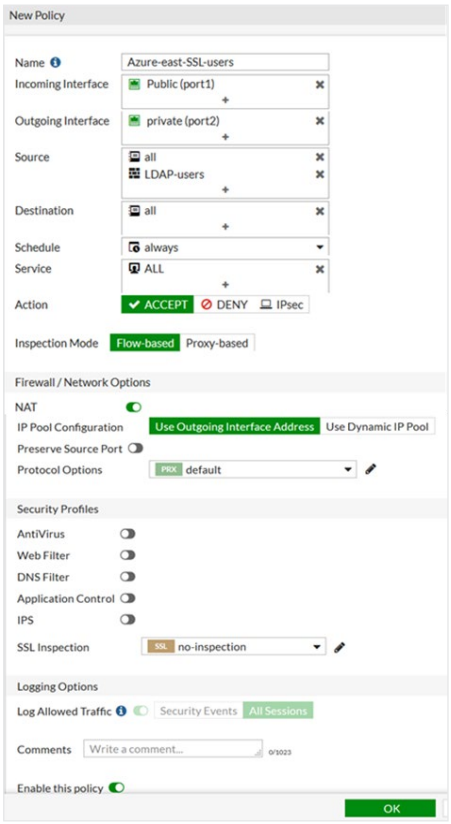


Figure 5: New IPv4 policy configuration.

This completes the basic SSL VPN user connectivity allowing access for SSL users to the internet. The next sections will discuss policy-based routing for data center, Microsoft control plane, and Microsoft Office 365 services.

Configuring Static Routing for Microsoft and Data Center

Routing on the FortiGate must be specified to ensure that the appropriate interfaces are used to route specific networks. The networks of concern for this deployment are the following:

- Internet (default route 0.0.0.0/0)
- Local WVD subnets
- Data center (IPsec)
- Microsoft local control plane (local Microsoft URL endpoints)
- Microsoft Office 365

The internet default route was defined with the deployment of the FortiGates and should already be in place. Review the section Deploying FortiGates and Azure Resources for more information. In summary, the default route should have a network of 0.0.0.0/0 and point to the next-hop gateway (or next hop) of the local vswitch address on the same subnet as port1. Later in this guide, instructions are given for implementing a required policy-based route for Microsoft Service Endpoints.

Local WVD Subnet Routes

By default there is a connected route for each interface. Additional routes to get to the WVD pool subnet are required as they do not or may not be connected directly. In our example case, the WVD pools resides in subnets that are not directly connected and use UDRs to default route back to the FortiGate's private interface. The following steps configure the local WVD routes.

Step 1: Create static route to the destination WVD Pool network

a. From the Menu, select **Network** → **Static Routes** → "Create New"

b. Enter the following:

- Destination – Select "Subnet" and enter the subnet range
- Gateway Address – Enter the next-hop default gateway for the interface
- Select "OK"
- Repeat for each back-end subnet that is not directly connected

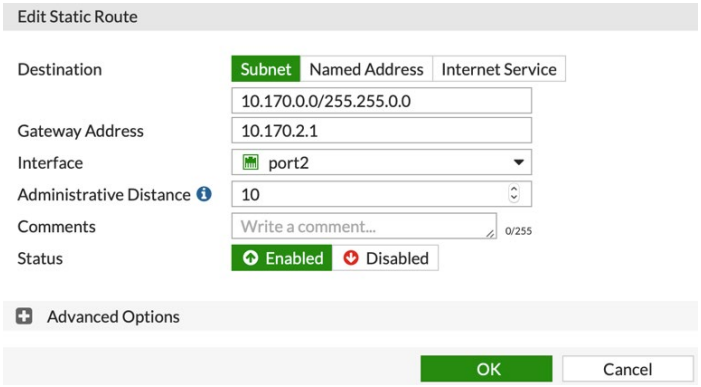


Figure 6: New WVD IPv4 route.

Step 2: Create static route for Microsoft Office 365 services

In the example scenario, VPN connectivity is provided to route traffic through the data center. However, Microsoft Office 365 traffic should be exempt from this routing and use local breakout to stay "on-net" and performance optimized. To do this, an Internet Services route is created for Azure services and Office 365 services, respectively. Here, the FortiGate is using its predefined, dynamic Internet Services Database to target these services.

a. As in Step 1, navigate to **Network** → **Static Routes** → "Create New" in the menu

b. Enter the following:

- Destination – Select *Internet Services* and "Microsoft-Azure" from the drop-down list
- Gateway Address – Enter the next-hop default gateway for the interface
- Select "OK"
- Repeat for a destination of "Microsoft-Office365"

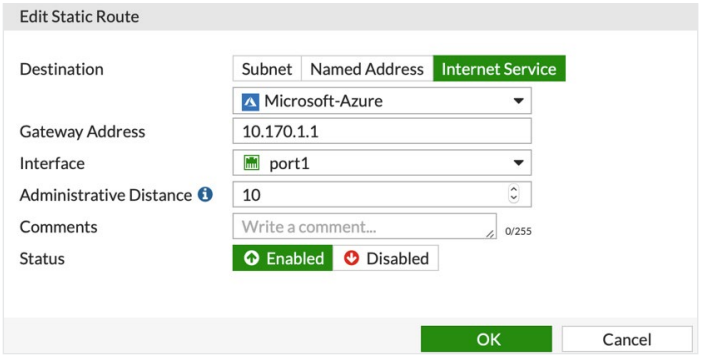


Figure 7.a: Microsoft Azure route.

NOTE: The FortiGate's Internet Services Database is updated regularly with FortiGuard Service Subscriptions. The default list is extensive and can be used in a variety of configurations. Customization of ISDB objects is also supported.
See more details at https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/825073/purchase-and-import-a-signed-ssl-certificate

The routes created to this point are redundant to the default route. However, once a new default (0.0.0.0/0) route through the VPN is added, these will take over as more specific routes for Azure and Office 365 destinations.

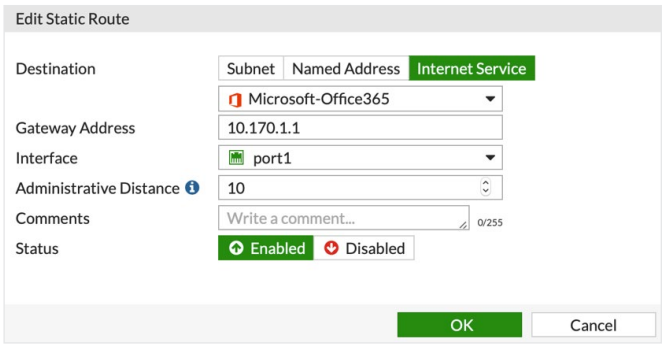


Figure 7.b: Microsoft Azure route.

Creating Address Objects

Before configuring firewall policies, it is necessary to define important Microsoft service endpoints to the FortiGate to allow for ease of administration with the narrowest security scope.

Configure Address Group for WVD Subnet

Address ranges within configurations and policies should be scoped as narrowly as possible as a best practice to ensure least access. Before creating a firewall policy, create a WVD address pool that matches the address range from the WVD VNet.

Step 1: Configuring WVD Address Object

a. Select **Policy & Objects** → **Addresses** → Create New → *New Address*

b. Enter the following information to define the subnet range as an address object:
- Name
- Type – As "Subnet"
- IP/Network – Matching the protected VNet
- Interface – Private interface
- Click "OK"

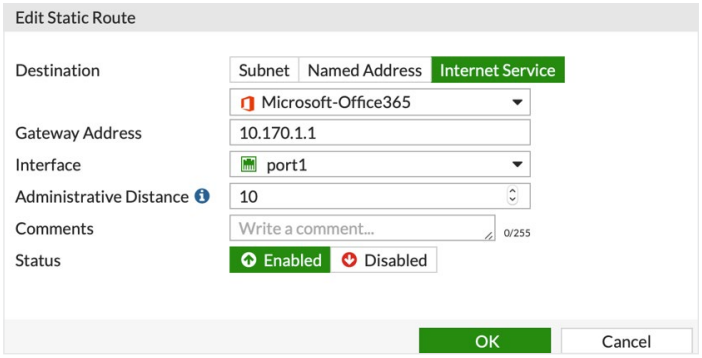


Figure 8: VNet Address Object.

Microsoft Service Tag Endpoints

Many Service Tags map to specific IP addresses and others to well-known URL endpoints defined by Microsoft. At a minimum, address objects (and group) must be defined, which will vary by Azure region. The example network deployed here is in WestUS2 and has the following IPs that must be reachable for WVD to function.

```
{
      "name": "WindowsVirtualDesktop.WestUS2",
      "id": "WindowsVirtualDesktop.WestUS2",
      "properties": {
        "changeNumber": 1,
        "region": "westus2",
        "platform": "Azure",
        "systemService": "WindowsVirtualDesktop",
        "addressPrefixes": [
          "13.66.251.49/32",
          "13.77.140.58/32",
          "20.190.43.99/32",
          "40.65.122.222/32",
          "51.141.173.236/32",
          "51.143.39.79/32",
          "52.143.96.87/32",
          "52.151.53.196/32",
          "52.175.253.156/32"
        ]
      }
    },
```

Figure 9: IP addresses required mapped to WVD Service Tags.

There are some URLs that don't all map directly to the WVD Service Tags, which must be allowed.
They can be found here: https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

Microsoft Service Endpoint	Port	Service	Type
*.wvd.microsoft.com	443	Service traffic	WindowsVirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	Agent and SXS track	AzureCloud
*core.windows.net	443	Agent traffic	AzureCloud
*.servicebus.windows.net	443	Agent traffic	AzureCloud
prod.warmpath.msftcloudes.com	443	Agent traffic	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows activation	Internet

Figure 10: Azure Service Tag Endpoints.

These IP addresses and URLs will be used as address objects in both IPv4 firewall policies and policy-based routing (PBR).

Configure Address Object and Group for WVD Service Tags

Step 1: Create address objects and group for minimum set of IPs as shown in Figure 11

a. Select **Policy & Objects** → **Addresses** → *Create New* → *Address Group*

b. Enter the following information:

- Group Name
- Members – A collection of defined addresses. These can be created directly from the Address Group page by selecting the **+**. In the pop-up list, select *Create* → *+Address*. Create an address object for each WVD Service Tag IP address and include in this group
- After adding all applicable addresses, click "OK" to create the address group

Step 2: Create address objects and group URL-based service endpoints

a. Select **Policy & Objects** → **Addresses** → *Create New* → *Address*

b. Enter the following information to define the FQDN-based address object:

- Name
- Type – As "FQDN"
- FQDN – enter the wildcard FQDN address for the service endpoint
- Interface – any
- Click "OK"

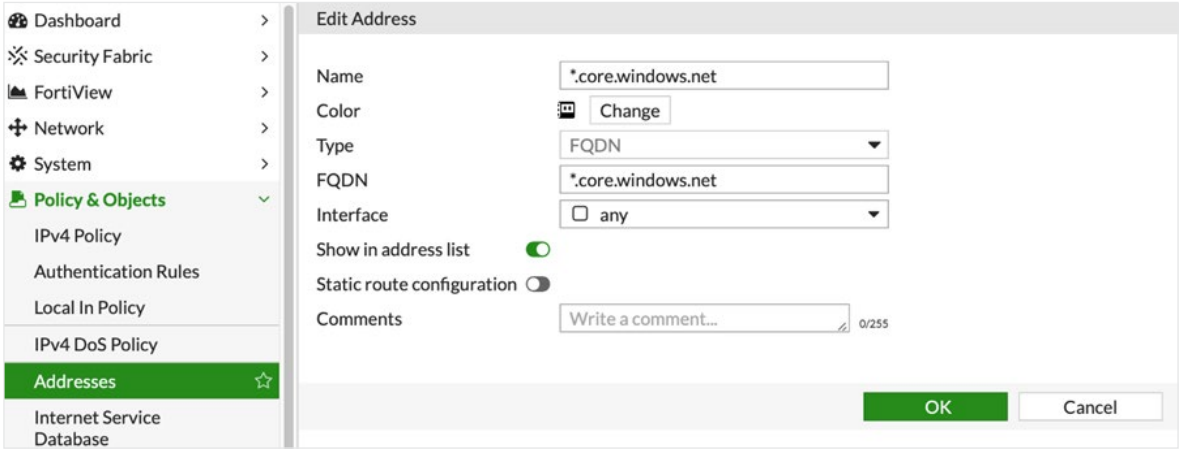


Figure 11: FQDN address object for URL Service Endpoints.

Step 3: Consolidate the FQDN address objects into a group

a. Navigate **Policy & Objects** → **Addresses** → *Create New* → *Address Object*

b. Enter the following information:

- Group name
- Members – add the FQDN members created in Step 2.
- Click "OK"

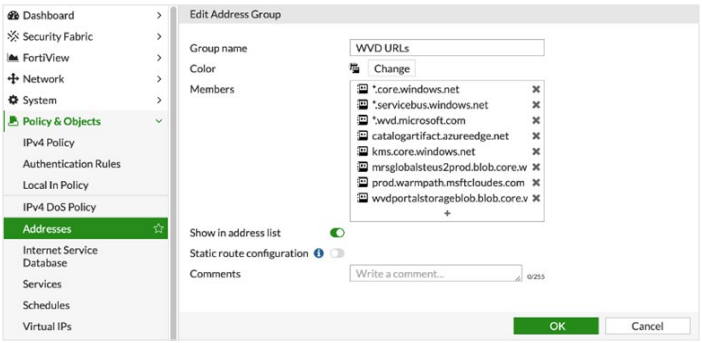


Figure 12: IP addresses required mapped to WVD Service Tags.

Creating Firewall Policies

Firewall policies must be configured between interfaces, zones, or services as all traffic through the FortiGate is denied by default. To ensure that hosts are accessible from the WVD pool, the next step is to create an allow IPv4 policy from the WVD subnet to the Azure control functions with the previously created address objects.

Configuring Azure IPv4 Policy for Azure Service Endpoints

Step 1: Configuring IPv4 Policy for Microsoft-Azure and Microsoft-Office365

a. Navigate to **Policy & Objects** → **IPv4 Policy** → *Create New*

b. Enter the following information as shown in Figure 13

- Name – Enter name for the policy
- Incoming Port – This is the private port originating WVD egress traffic
- Outgoing Interface – This is the internet-facing port1
- Source – Use the previously configured "VNet Address Space" object
- Destination – Select the Internet Services "Microsoft-Azure" and "Microsoft-Office365"
- Schedule
- Service
- Action
- NAT – SNAT must be enabled as this traffic is destined for the internet
- Application Control – Must be enabled to identify Microsoft traffic
- Configure additional inspection profiles as needed
- Select "OK" to save the configuration

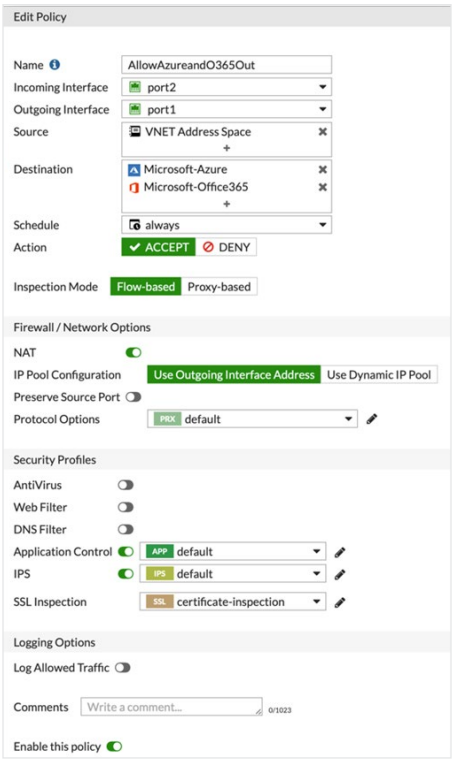


Figure 13: WVD egress policy.

Step 2: Configuring IPv4 firewall policy for Microsoft Service Endpoints

a. Enter the following information:

- Name
- Incoming Interface – protected
- Outgoing interface – public
- Source – Use the previously created object for the VNet address range
- Destination – This is the WVD URLs group and Service Endpoint IP group
- Service – All
- NAT – Enable for SNAT
- Application Control – To identify various Microsoft Services
- Click "OK"

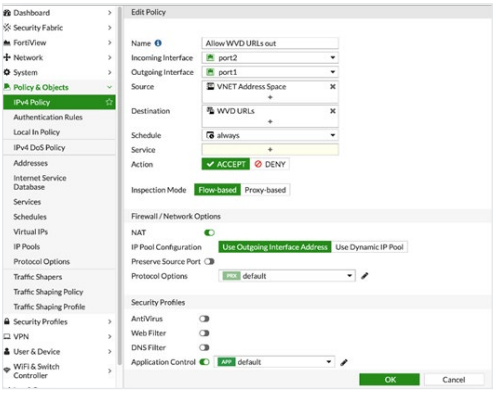


Figure 14: IP addresses required mapped to WVD Service Tags.

Policy-based Routing

With the firewall policies in place, a policy route is added to allow Microsoft Service Endpoints to egress through the internet interface and not the default VPN route that will be set up.

Policy routing allows you to redirect traffic away from a static route. This can be useful if you want to route certain types of network traffic differently. You can use incoming traffic's protocol, source address or interface, destination address, or port number to determine where to send the traffic. For example, generally network traffic will go to the router of a subnet, but you might want to direct SMTP or POP3 traffic directly to the mail server on that subnet.

Policy routes allow the FortiGate to override the routing table based on policy matches. Traffic entering the FortiGate will be evaluated against the match conditions set in the route. Note that the FortiGate must have an existing route to the destination network for the policy route to be invoked. Revisit section **Configuring Static Routing for Microsoft and Data Center** for instructions to configure the static route for Microsoft services. This section details how to configure the policy route.

Configure Policy Route for Microsoft Service Endpoint

Step 1: Configure Policy Route for URL-based endpoints

a. Navigate to **Network** → **Policy Routes** → *Create New*

b. Provide the following configurations:

- Incoming Interface – This is the private interface sourcing the WVD pool
- Addresses – This is the tunneled data center or premise address object created in the IPsec configuration
- Destination Address: Address – WVD URL address group
- Protocol – Any
- Outgoing interface – Interface-facing port1
- Gateway Address – Next-hop gateway for the port1 subnet
- Click "OK"

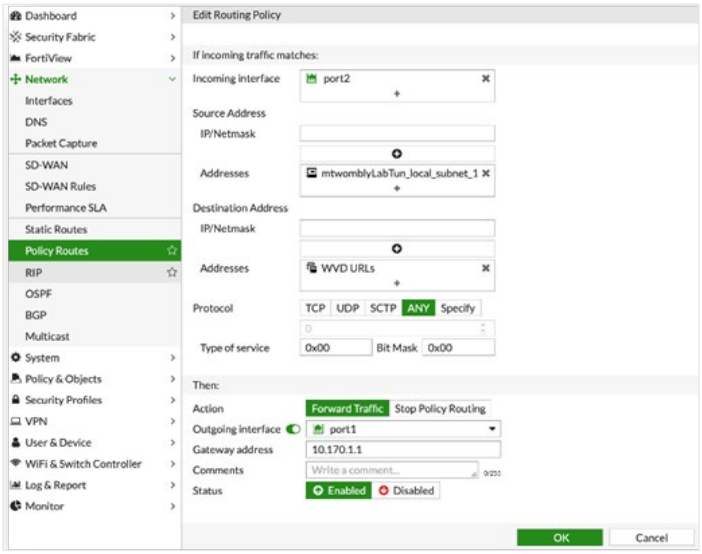


Figure 15: Policy-based route.

Creating Scalable IPsec Connectivity

The next step is to set up the site-to-site tunnel. This setup will be contingent on the remote endpoint. Several tunnel templates are available in the IPsec VPN Wizard that covers a variety of different types of IPsec VPN. A list of these templates appears on the first page of the wizard, located at **VPN** → **IPsec Wizard**. The tunnel template list follows. The sample setup described here connects to a physical FortiGate appliance.

Configuring IPsec Service

Step 1: Create Tunnel

a. Navigate to **VPN** → **IPSec Tunnels** → *Create New* → *IPsec Tunnel*

b. The default selection in the tunnel wizard is to connect a site-to-site VPN between FortiGates. Use this option and complete the guided configuration.

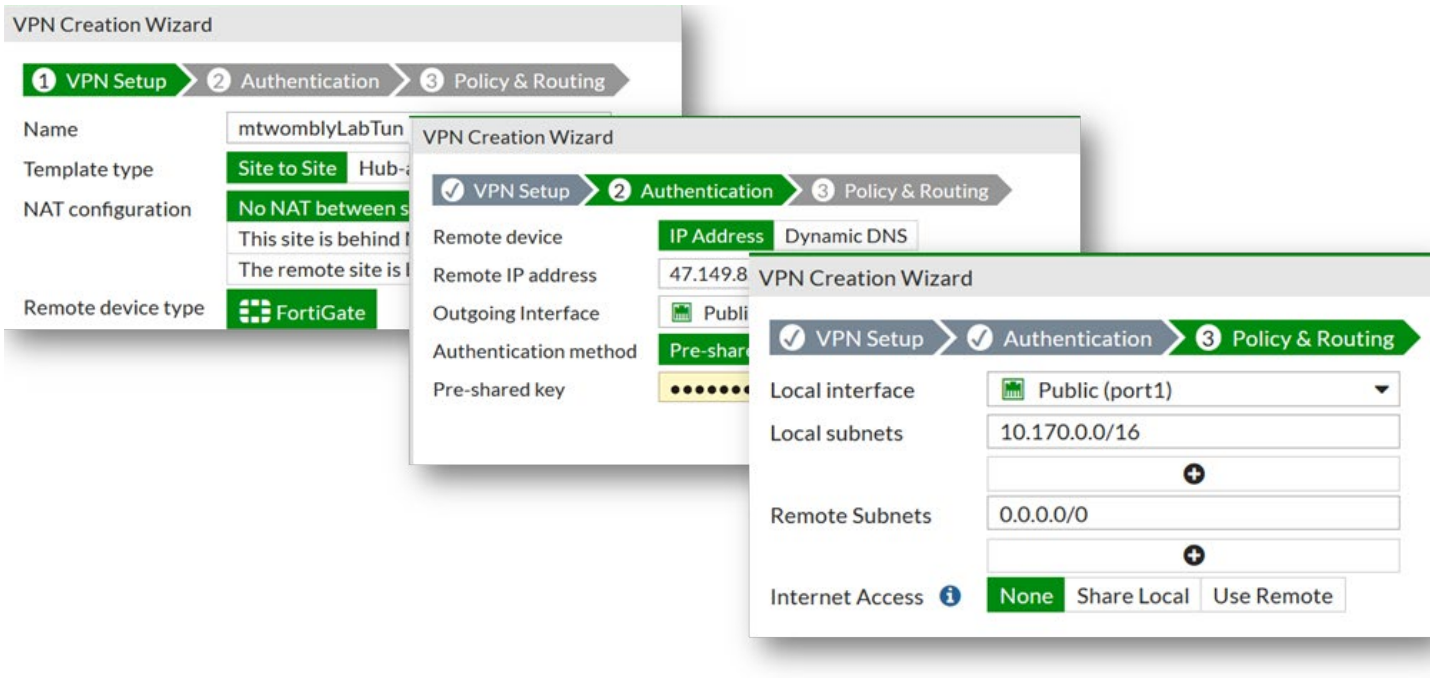
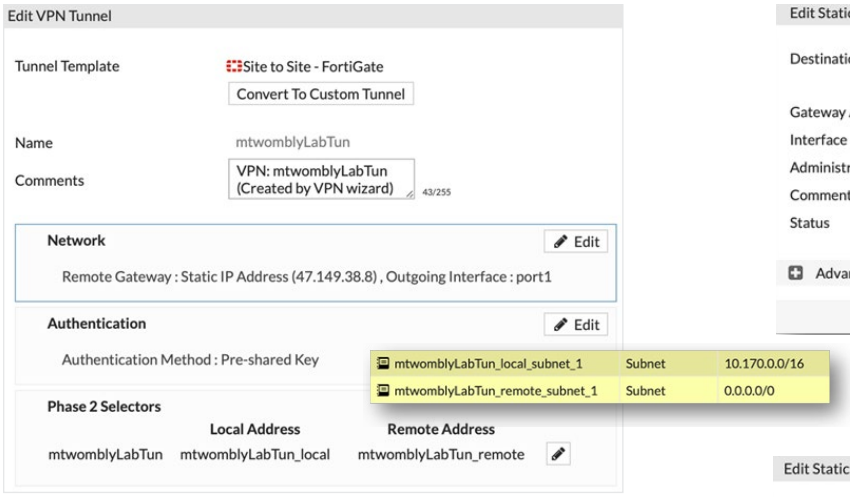


Figure 16: IPsec guided configuration.

When using a wizard, the local and remote address objects are created automatically. In this example all traffic is sent (except Azure and O365) over the tunnel with the remote address set to 0.0.0.0/0.

Next, the existing default route is modified to have a higher administrative distance. This route will be used as the backup in the event that the IPsec tunnel goes offline. Keep in mind that this is a policy decision. Another option could be to set up a black hole route to ensure that no traffic goes out if the tunnel is offline.



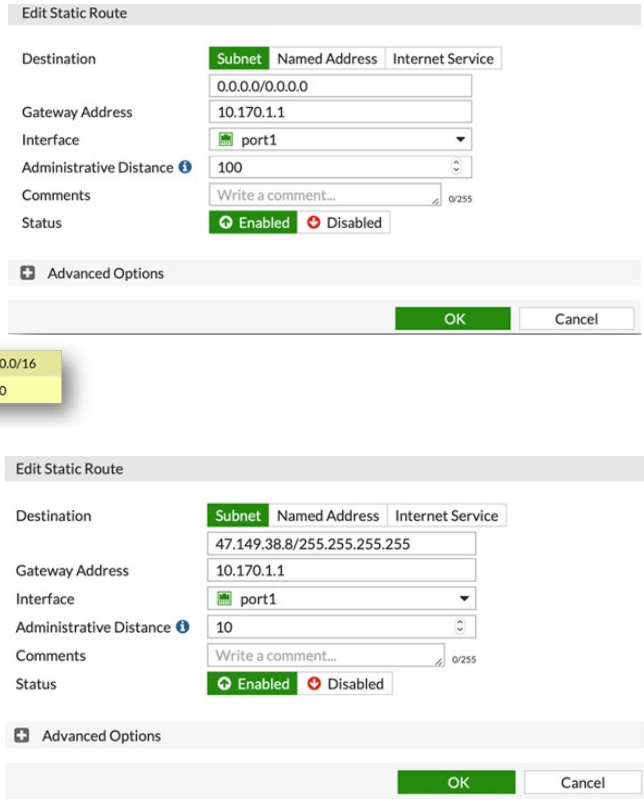


Figure 17: Site-to-site output.

To ensure that when setting up the new default static route through the tunnel, a static route is created for the remote tunnel endpoint, specifically.

Figure 18: Route to remote tunnel endpoint.

Once the tunnel endpoint route is in place, a new preferred default route is established through the tunnel.

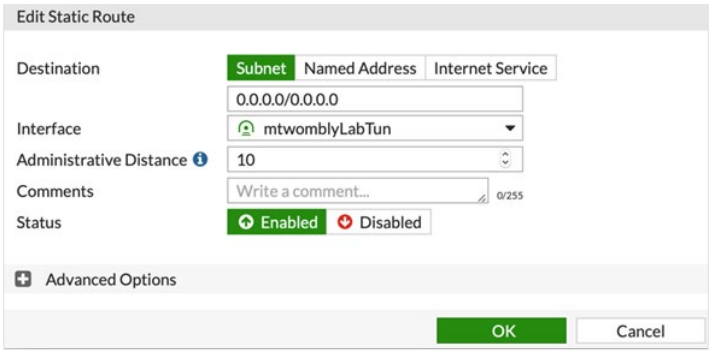


Figure 19: New default route through the IPsec tunnel.

The final step in the IPsec configuration on the FortiGate is to configure or modify the IPv4 tunnel policies to allow and inspect traffic across the tunnel based on policy. When creating a tunnel with a wizard, these policies are enabled, but are not restricted in any way. If creating a tunnel manually, the policies are not created and the tunnel won't come up until an allow policy is enabled for the tunnel interface.

These policies are stateful. The example in Figure 20 will allow the WVD virtual servers and VDI sessions running on them to initiate communication across the tunnel to any address, and the reply traffic will be allowed. However, this policy doesn't allow remote servers or workstations to initiate communication inbound to a WVD server. A separate policy would be required to enable that. Creating or modifying the policy is similar to steps described in earlier sections.

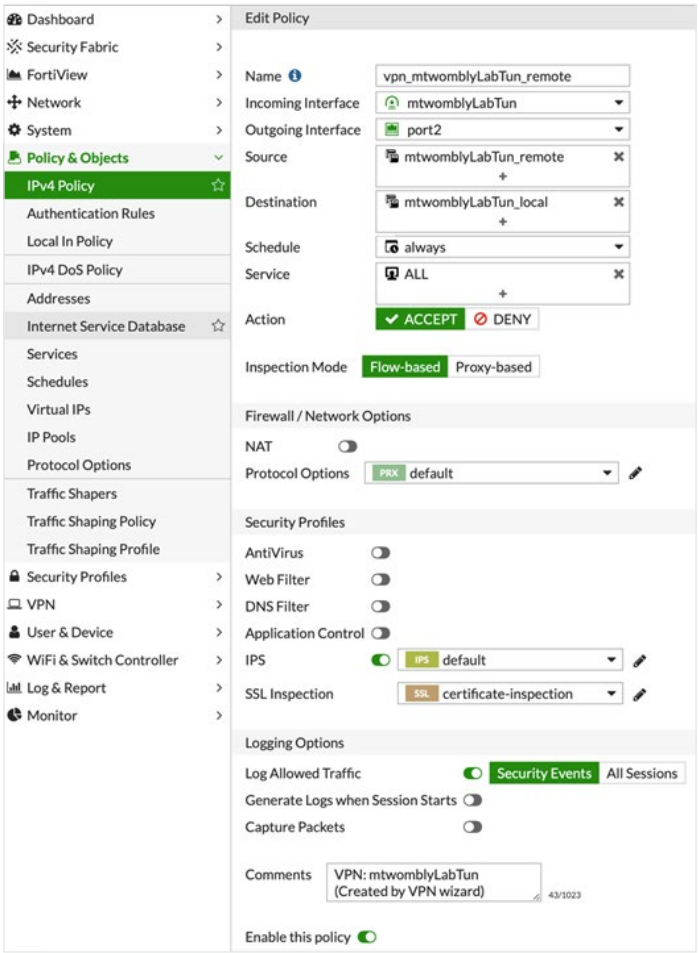


Figure 20: Policy allowing traffic through the IPsec tunnel.

Scaling IPsec with IPsec Aggregation

As of FortiOS 6.2, the FortiGate supports the ability to efficiently scale up VPN performance. It does this by allowing multiple phase 1 tunnels with the same origin and destination endpoints to be aggregated under a single routable interface. The VPN tunnels are then spread over multiple CPUs providing cost optimization of the Azure VM option used while providing high-bandwidth VPN services. This feature has become part of teleworking, hybrid cloud, and transitive use cases.

Detailed configuration information is located at:
https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/803478/represent-multiple-ipsec-tunnels-as-a-single-interface

Deploying FortiGates and Azure Resources

Once all the policies and routes have been created within the FortiGate, the final step is to configure and apply an Azure User Defined Route (UDR) table. If the FortiGate was deployed from the marketplace or a provided ARM template, a UDR table was created with a default route configured to the IP address assigned to the port2 interface of the FortiGate. The next section will review Azure configurations for UDRs.

User Defined Route Table Configuration

Step 1: WVD subnet UDR

a. Select the VNet in the Azure portal by going to **Settings** → **Subnets** → *WVD subnet*.

b. From the route table dropdown, select the route table (e.g., FortiGateTrustedSubnet-routes with a selected prefix and a unique suffix).

If you want or need to create your own route table, it should look similar to Figure 22.

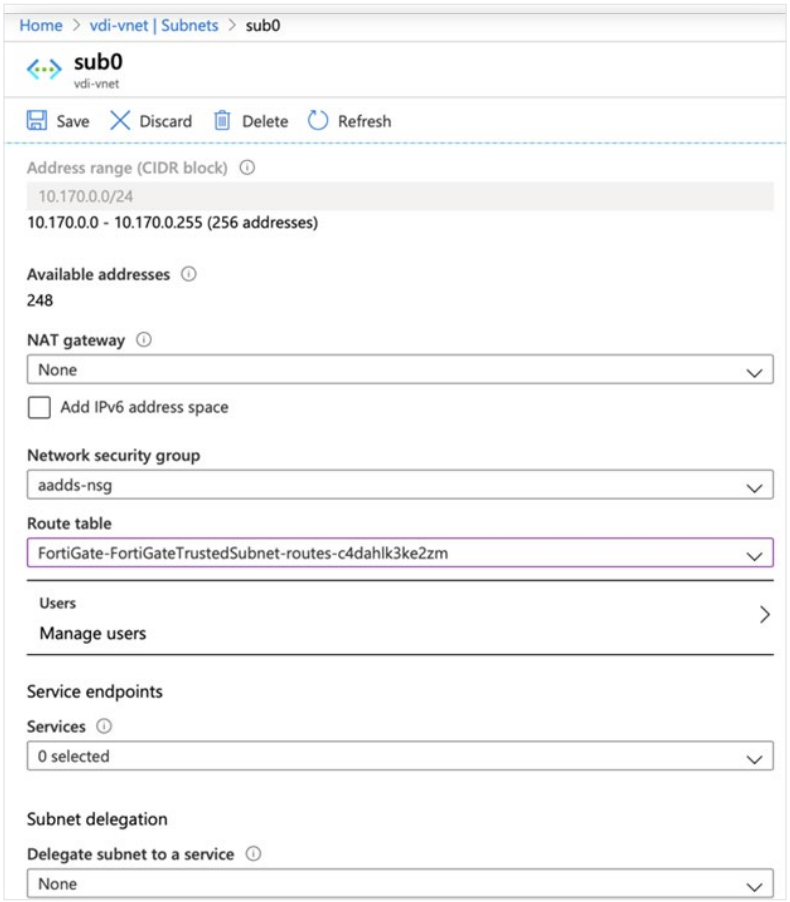


Figure 21: WVD route table.

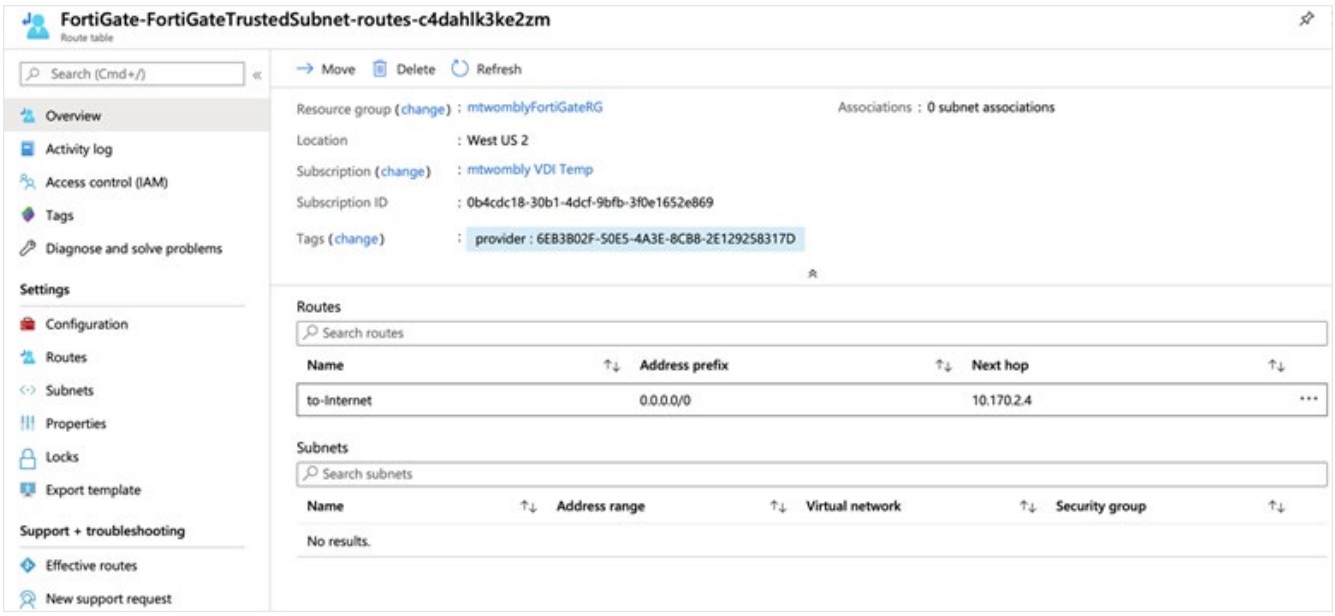


Figure 22: Route table example.

To validate that the routing is applied, select a vNIC of one of the WVD pool VMs in the Azure portal.
Under **Support + Troubleshooting → Effective routes**.

A default route from the "Default" source with a state of "Invalid" should be present. Another default route (0.0.0.0/0) should also exist from the "User" source with a state of "Active" and a next-hop IP that matches the internal interface IP of the FortiGate.

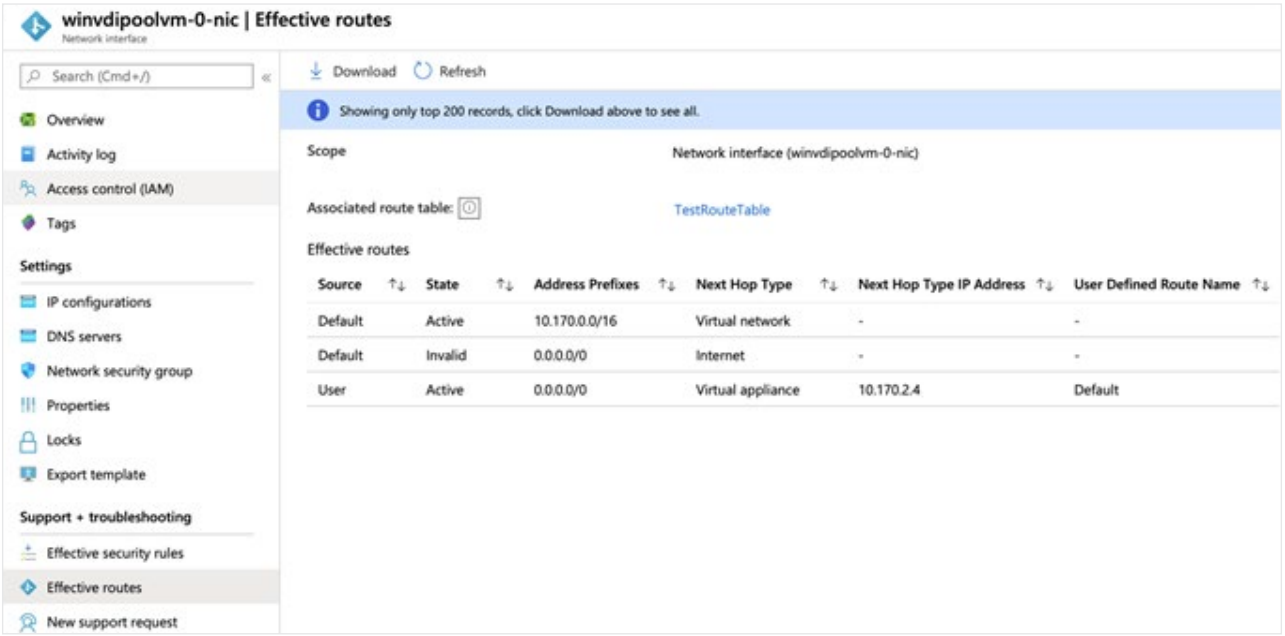


Figure 23: Effective routes.

Performance Options

Performance and capacity of WVD will scale by the size of the pool. However, this won't increase the bandwidth or inspection performance of the FortiGate. While the VM04 and VM08 FortiGates will offer more bandwidth than the standard Azure VPN service, it still may not be adequate depending on the number of WVD users and their traffic patterns.

A solution to this is to deploy the FortiGates, as an active/active HA cluster can use the same subnets as the first, but the WVD pool must be deployed on a unique subnet. Then a UDR similar to the first can be deployed with a next-hop configured for the second FortiGate. Once this setup is complete, you can load balance your users by having half of them connect to the first pool, and the other half to the second pool. The figure below adds this to our original design.

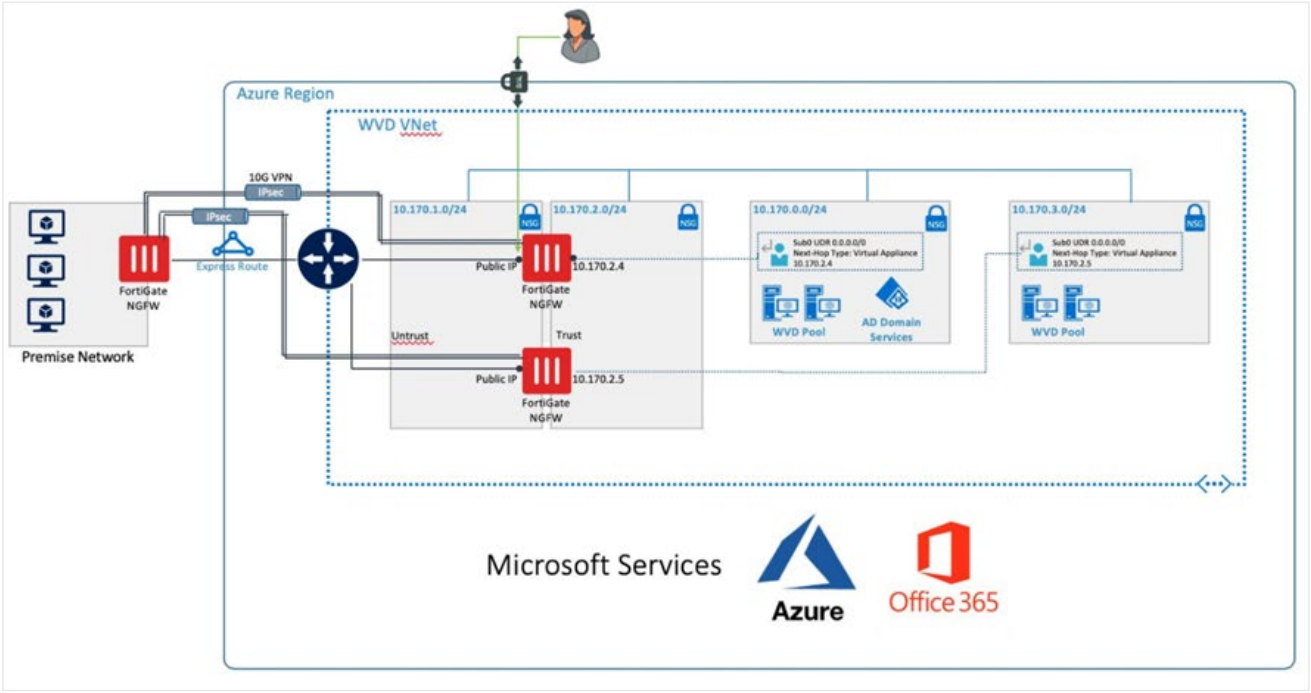


Figure 24: Effective routes.

May 13, 2020 12:55 AM

668114-0-0-EN

D:\Fortinet\Deployment Guides\BLUE DEPLOYMENT GUIDES\Azure Connect and Protect\dg-FA-secure-azure-windows-virtual-desktop-guidebook-5132020