**Azure Firewall for On-prem access to Service Endpoints: Step-by-Step Lab Guide**

Virtual Network (VNet) Service Endpoints extends your virtual network private address space, and

the identity of your VNet, to multi-tenant Azure PaaS services over a special NAT tunnel in the

Azure fabric.  Service Endpoints allow you to secure your critical Azure service resources to only

your virtual networks. Traffic from your VNet to the Azure PaaS service always remains on the

Microsoft Azure backbone network.

The key here is the ability to deploy Azure Storage with Service Endpoints, while *also* making these

private PaaS endpoints available over an IPSEC VPN or the ExpressRoute private peering. The current limitation of Service Endpoints is that it is not accessible to on-premise resources.  Using service endpoints with Azure Firewall gives on-premise devices a private endpoint to hit coupled with a stateful security device providing centralized logging.

The following diagram illustrates on-premise to cloud communication architecture secured via the

Azure Firewall hosted in Microsoft Azure.



Download the Configuration Details spreadsheet to record the appropriate lab details. This spreadsheet can be found at:

1. Create the following resource groups to hold all lab environments
   1. RG\_PAAS\_GTWY
   2. RG\_DEPT1
   3. RG\_CONTOSO\_BLOB
2. Create the following VNETs with the following details
   1. VNET\_PAAS\_GTWY
      1. Address space: 10.10.0.0/16
      2. Resource Group: RG\_PAAS\_GTWY
      3. Subnet: MGMT
      4. Subnet address space: 10.10.2.0/24
      5. Firewall: Enabled
      6. Firewall name: AzFW1
      7. Firewall subnet: 10.10.1.0/24
   2. VNET\_DEPT1
      1. Address space: 10.20.0.0/16
      2. Resource Group: EG\_DEPT1
      3. Subnet: server
      4. Subnet address space: 10.20.1.0/24
3. Edit the VNET\_PAAS\_GTWY VNET and enable service endpoints
   1. Service: Microsoft.Storage
   2. Subnets: AzureFirewallSubnet
4. Add a gateway subnet to the VNET\_PAAS\_GTWY VNET
   1. Address range: 10.10.0.0/24
5. Deploy a Virtual Network Gateway
   1. Name: VPN\_GTWY
   2. Type: VPN
   3. VPN Type: Route-based
   4. Virtual Network: VNET\_PAAS\_GTWY
   5. Public IP address: Create new (name vpn\_gtwy\_ip)
   6. Select Configure BGP ASN
   7. Autonomous System Number: 65440
6. Record ASN Number in Configuration Details Worksheet under Azure VNG BGP ASN

NOTE: The Virtual Network Gateway can take up to 30 minutes to deploy. You can continue with this lab as the gateway is being deployed.

1. Deploy a Virtual Machine
   1. Resource Group: RG\_DEPT1
   2. Name: VMDEPT1
   3. Image: Windows Server 2016 Datacenter
   4. Create credentials for administrator account
   5. Public Inbound Ports: Allow Selected ports
   6. Select Inbound Ports: RDP
2. Create the following storage accounts
   1. Department1
      1. Resource Group: RG\_CONTOSO\_BLOB
      2. Account Name: department1
      3. Account kind: BlobStorage
   2. Onprem1
      1. Resource Group: RG\_CONTOSO\_BLOB
      2. Account Name: Onprem1
      3. Account kind: BlobStorage
   3. Azfwlogs
      1. Resource Group: RG\_PAAS\_GTWY
      2. Account name: azfwlogs
      3. Account kind: BlobStorage
3. Edit the storage accounts and create the following containers
   1. Department1
      1. Name: dept1-stuff
   2. Onprem1
      1. Name: on-prem-stuff

NOTE: Check to see if the Virtual Network Gateway has been successfully deployed. If not wait to continue until this has completed.

1. Edit the VNET\_PAAS\_GTWY VNET and create a peering
   1. Name: Peer\_to\_DEPT1
   2. Virtual Network: VNET\_DEPT1
   3. Allow forwarded traffic: Enabled
   4. Select Allow Gateway Transit
2. Edit the VNET\_DEPT1 VNET and create a peering
   1. Name: Peer\_to\_PAAS\_GTWY
   2. Virtual Network: VNET\_PAAS\_GTWY
   3. Allow forwarded traffic: Enabled
   4. Select Use remote gateways
3. Edit the virtual network gateway to record information in the configuration details worksheet
   1. In Overview blade, record Public IP address under Azure VNG Public IP
   2. In Configuration blade, record BGP peer IP address under Azure VNG BGP Peer
4. Deploy a Local Network Gateway
   1. Name: OnPrem-GTWY
   2. IP address: Enter IP Address of the on-site IPSEC FW or Router
   3. Select Configure BGP settings
   4. ASN: enter BGP ASN for on-site device
   5. BGP peer IP address: enter IP address of on-site BGP peer
   6. Resource Group: RG\_PAAS\_GTWY
5. Create a connection for the IPSEC VPN
   1. Connection Type: Site-to-Site
   2. Resource Group: RG\_PAAS\_GTWY
   3. Virtual Network Gateway: VPN\_GTWY
   4. Local Network Gateway: OnPrem-GTWY
   5. Shared Key: enter your preshared key
   6. Select Enable BGP
6. Create the custom IPSEC policy based on the configuration details worksheet and configure the connection to use this custom policy
   1. Open the cloud shell from the portal
   2. Copy and paste the below into the portal

**$connection = Get-AzureRmVirtualNetworkGatewayConnection -Name VPN\_GTWY-OnPrem-GTWY -ResourceGroupName RG\_PAAS\_GTWY**

**$newpolicy = New-AzureRmIpsecPolicy -IkeEncryption AES256 -IkeIntegrity SHA256 -DhGroup DHGroup14 -IpsecEncryption AES128 -IpsecIntegrity SHA1 -PfsGroup PFS2048 -SALifeTimeSeconds 14400 -SADataSizeKilobytes 102400000**

**Set-AzureRmVirtualNetworkGatewayConnection -VirtualNetworkGatewayConnection $connection -IpsecPolicies $newpolicy**

* 1. Select Yes when prompted to make changes

1. Configure your on-prem device for the VPN tunnel and BGP settings
2. Deploy a Log Analytics Workspace
   1. Workspace Name: FW-Logs
   2. Resource Group: PG\_PAAS\_GTWY
3. Edit the Azure Firewall and under the Diagnostics settings select turn on diagnostics
   1. Name: Firewall\_Logs
   2. Select Archive to storage account: azfwlogs
   3. Select Send to Log Analytics
   4. Select Log AzureFirewallApplicationRule
   5. Select Log AzureFirewallNetworkRule
4. Edit the Department1 and Onprem1 storage accounts and record the Primary Blob Service Endpoint FQDN from the properties blade in the Configuration Details Worksheet
5. Edit the Department1 and Onprem1 storage accounts and under the Firewalls and virtual networks blade lock the account down to the AzureFirewall subnet
   1. Allow Access from: Selected Networks
   2. Add existing virtual network
   3. Virtual Networks: VNET\_PAAS\_GTWY
   4. Subnets: AzureFirewallSubnet
6. Edit the VMDEPT1 virtual machine and record the public and private IP addresses in the Configuration Details Worksheet
7. Edit the Azure Firewall and record the private IP address in the Configuration Details Worksheet under Azure Firewall IP
8. Under the Rules blade configure the Application Rule Collection Rules
   1. Name: BLOB-Access
   2. Priority: 200
   3. Target FQDNs Name: Department1
      1. Source address is Dept 1 Private IP
      2. Protocol: HTTPS
      3. Target FQDNS: FQDN for Department 1 storage account
   4. Target FQDNs Name: OnPrem
      1. Source address is on-prem network range
      2. Protocol: HTTPS
      3. Target FQDNS: FQDN for On-Prem storage account
9. RDP to the public address of VMDEPT1 and update the hosts file on the machine with the URL of the storage account to point to the Azure Firewall IP.
10. Download Azure Storage Explorer on VMDEPT1 (<https://azure.microsoft.com/en-us/features/storage-explorer/>)
11. Create a DNS entry on-prem for the FQDN of the on-prem storage account and point to Azure Firewall IP.
12. Download Azure Storage Explorer on an on-prem device (<https://azure.microsoft.com/en-us/features/storage-explorer/>)
13. Attempt connections from both on-prem and VMDEPT1 machines to the storage accounts using Azure Storage explorer. You should be able to hit the storage account assigned to that device but receive an error when trying to access another storage account.
14. Edit Log Analytics Workspace and open the View Designer blade.
15. Select Import from the toolbar and import a view. The file can be generated by following this doc (<https://docs.microsoft.com/en-us/azure/firewall/log-analytics-samples>)
16. Once imported a dashboard will be displayed with your Azure Firewall. Select View Dashboard at the top to see the attempts made through the Azure Firewall.

NOTE: There can be some delay in log data reaching Log Analytics so allow enough time for this data to be collected.