Azure VPN Gateway Dual-Stack Analysis

Cross-Premises IPv6 Connectivity Assessment

January 2026

Contents

1 Executive Summary

This report documents the analysis of Azure VPN Gateway's dual-stack (IPv4 + IPv6) capabilities for cross-premises connectivity. Testing was conducted using a GCP-hosted on-premises simulation connecting to Azure VPN Gateway in Active-Active mode.

Key Finding: Azure VPN Gateway dual-stack IPv6 is available in **PREVIEW** status, requiring explicit opt-in by emailing your subscription ID to Microsoft. Without preview enrollment, IPv6 is blocked at multiple levels.

Preview Availability: Microsoft documents dual-stack Site-to-Site VPN support with:

- Manual opt-in required (email subscription ID to Microsoft)
- Supported SKUs: VpnGw1-5, VpnGw1AZ-5AZ
- IKEv2 required (IKEv1 does not support IPv6)
- New gateway deployments only

Test Results Summary:

Component	IPv4	IPv6
IPsec Tunnels (IKEv2)	Pass	N/A
BGP Sessions	Pass	Fail
Route Learning	Pass	Fail
Cross-VPN Ping	69ms	Blocked
Static Routes (UDR)	Pass	Rejected

2 Test Environment

2.1 Architecture

The test environment consisted of:

- **Azure VPN Gateway**: VpnGw1 SKU, Active-Active mode, BGP enabled (ASN 65515)
- **On-Prem Simulation**: Two router VMs on GCP running LibreSwan + FRR
- **Test VMs**: One in Azure, one in GCP on-prem simulation

```
┌─────────────────────────────────────────────────────────────┐
│                    GCP On-Prem Simulation                   │
│                        (us-west1)                           │
│                                                             │
│  ┌─────────────────┐            ┌─────────────────┐        │
│  │   Router 1      │            │   Router 2      │        │
│  │  34.82.67.66    │            │  34.169.9.91    │        │
│  │  ASN: 65001     │            │  ASN: 65001     │        │
│  │  BGP: 169.254.  │            │  BGP: 169.254.  │        │
│  │       21.5      │            │       21.6      │        │
│  └────────┬────────┘            └────────┬────────┘        │
│           │                              │                  │
│           │   VPC: 192.168.0.0/16        │                  │
│           │         fd20:e:1::/48        │                  │
│           └──────────────┬───────────────┘                  │
│                          │                                  │
│               ┌──────────┴──────────┐                       │
│               │   Test VM           │                       │
│               │   192.168.1.100     │                       │
│               └─────────────────────┘                       │
└─────────────────────────────────────────────────────────────┘
              │                              │
              │ IPsec IKEv2                  │ IPsec IKEv2
              │ vti10                        │ vti10
              ▼                              ▼
┌─────────────────────────────────────────────────────────────┐
│                    Azure (eastus2)                          │
│                                                             │
│  ┌─────────────────────────────────────────────────────┐   │
│  │              Azure VPN Gateway                       │   │
│  │              (Active-Active, VpnGw1)                 │   │
│  │                                                      │   │
│  │  Instance 0: 20.110.156.183  │  Instance 1: 172.177. │   │
│  │  BGP: 169.254.21.1           │  98.104               │   │
│  │  ASN: 65515                  │  BGP: 169.254.21.2    │   │
│  └──────────────────────────────────────────────────────┘   │
│                          │                                  │
│           VNet: 10.1.0.0/16 + fd20:d:1::/48                │
│                          │                                  │
│               ┌──────────┴──────────┐                       │
│               │   Test VM           │                       │
│               │   10.1.1.100        │                       │
│               │   fd20:d:1:1::4     │                       │
│               └─────────────────────┘                       │
└─────────────────────────────────────────────────────────────┘
```

Listing 1: Test Environment Architecture

2.2 IP Addressing

Component	IPv4	IPv6
Azure VNet	`10.1.0.0/16`	`fd20:d:1::/48`

Azure GatewaySubnet	`10.1.0.0/27`	N/A (not supported)
Azure Workload Subnet	`10.1.1.0/24`	`fd20:d:1:1::/64`
Azure Test VM	`10.1.1.100`	`fd20:d:1:1::4`
On-Prem VPC	`192.168.0.0/16`	`fd20:e:1::/48`
On-Prem Router 1	`192.168.0.10`	auto-assigned
On-Prem Router 2	`192.168.0.11`	auto-assigned
On-Prem Test VM	`192.168.1.100`	auto-assigned

2.3 BGP Configuration

Side	**ASN**	**BGP Peering IPs (APIPA)**
Azure VPN Gateway Instance 0	65515	`169.254.21.1`
Azure VPN Gateway Instance 1	65515	`169.254.21.2`
On-Prem Router 1	65001	`169.254.21.5`
On-Prem Router 2	65001	`169.254.21.6`

3 IPv4 VPN Results

IPv4 connectivity was successfully established through the Azure VPN Gateway.

3.1 IPsec Tunnel Status

Both IPsec tunnels established successfully using IKEv2:

```
#1: "azure-vpngw-tun1":4500 STATE_PARENT_I3 (PARENT SA established)
#2: "azure-vpngw-tun1":4500 STATE_V2_IPSEC_I (IPsec SA established)
```

IPsec Parameters:

- IKE: AES256-SHA256-MODP2048
- ESP: AES256-SHA256
- IKE Lifetime: 28800s
- SA Lifetime: 3600s

3.2 BGP Session Status

Both BGP sessions established and exchanging routes:

```
Neighbor        V    AS   MsgRcvd MsgSent  Up/Down  State/PfxRcd
169.254.21.1    4 65515        3       5 00:00:41            1
169.254.21.2    4 65515        3       5 00:00:16            1
```

3.3 Connectivity Test Results

Test	Result	Latency
On-Prem → Azure (ping 10.1.1.100)	0% loss	69ms
Azure → On-Prem (ping 192.168.1.100)	0% loss	69ms
BGP Route Learning (10.1.0.0/16)	Learned	–

4 IPv6 VPN Results

Critical Finding: Azure VPN Gateway does not support cross-premises IPv6 connectivity at any level.

4.1 Blocking Issue 1: Local Network Gateway Rejects IPv6

When attempting to add IPv6 prefixes to the Local Network Gateway:

```
az network local-gateway update \
  --name lng-onprem-router-1-prod-eastus2 \
  --local-address-prefixes 192.168.0.0/16 fd20:e:1::/48
```

Error Response:

```
LocalNetworkGatewayIpv6NotSupported: Local Network Gateway
cannot contain IPv6 address prefix.
```

This is a fundamental limitation. The Local Network Gateway, which defines on-premises address spaces, explicitly rejects IPv6 prefixes.

4.2 Blocking Issue 2: BGP Does Not Learn IPv6 Routes

Although the BGP neighbor capability shows IPv6 Unicast support:

```
Address Family IPv6 Unicast: received
```

Azure VPN Gateway does **not** install IPv6 routes in its routing table. When on-prem routers advertise `fd20:e:1::/48`:

```
az network vnet-gateway list-learned-routes \
  --name vpngw-azure-prod-eastus2 \
  --resource-group rg-azure-vpngw-prod-eastus2
```

Result: Only IPv4 routes appear. No IPv6 routes are learned.

4.3 Blocking Issue 3: UDR Cannot Route IPv6 to VPN Gateway

Attempting to create a static route for IPv6 to the VPN Gateway:

```
az network route-table route create \
  --address-prefix fd20:e:1::/48 \
  --next-hop-type VirtualNetworkGateway
```

Error Response:

```
InvalidNextHopType: The next hop type for IPv6 address prefix
fd20:e:1::/48 cannot be 'VirtualNetworkGateway',
'HyperNetGateway' or 'VirtualNetworkServiceEndpoint'.
```

Azure explicitly blocks IPv6 routes from using VPN Gateway as a next hop.

4.4 Blocking Issue 4: Overlay Tunnels Blocked

As a workaround, we attempted to create a GRE tunnel (IPv6-in-IPv4) over the working VPN:

Azure VM Side	On-Prem Router Side
GRE tunnel to 192.168.0.10	GRE tunnel to 10.1.1.100
IPv6 address: fd20:ff::1/126	IPv6 address: fd20:ff::2/126

Result: GRE packets (IP protocol 47) are filtered by Azure networking. tcpdump on the on-prem router shows zero GRE packets arriving, despite Azure VM sending them.

```
# Azure VM tcpdump shows outgoing GRE:
IP 10.1.1.100 > 192.168.0.10: GREv0, length 108: IP6 ...

# On-prem router tcpdump shows nothing:
0 packets captured
```

ICMP and TCP to the same destination work fine, confirming the VPN tunnel is functional but GRE is specifically filtered.

5 Comparison with Other Cloud Providers

Capability	Azure VWAN	Azure VPN GW	GCP HA VPN	AWS TGW VPN
IPv4 VPN	GA	GA	GA	GA
IPv6 VPN Config	No	Preview†	GA	GA
IPv6 in LNG/ Site	Rejected	Preview†	N/A	N/A
IPv6 BGP Sessions	No	Preview†	GA	GA
IPv6 Route	No	Preview†	GA‡	GA

Learning				
IPv6 UDR to Gateway	Blocked	Preview†	N/A	N/A
Cross-VPN IPv4	69ms	69ms	32ms	63ms
Cross-VPN IPv6	Blocked	Untested	33ms	63ms
Deployment Time	30-45 min	30-45 min	~3 min	~5 min
Feature Status	GA	GA + Preview	GA	GA

† Azure VPN Gateway IPv6 requires manual preview enrollment (email subscription ID to Microsoft)

‡ GCP requires dedicated IPv6 BGP sessions rather than MP-BGP on IPv4 sessions

5.1 AWS Approach (Works)

AWS supports dual-stack by creating **separate VPN connections**:

- One VPN connection with `tunnel_inside_ip_version = "ipv4"` (traffic selector: `0.0.0.0/0`)
- One VPN connection with `tunnel_inside_ip_version = "ipv6"` (traffic selector: `::/0`)

This approach is **not possible with Azure** because the Local Network Gateway rejects IPv6 entirely.

5.2 GCP Approach (Works)

GCP supports dual-stack with:

- HA VPN Gateway with `stack_type = "IPV4_IPV6"`
- Dedicated IPv6 BGP sessions using `fdff:1::/64` peering addresses
- IPv6 routes properly installed in VPC routing table

6 Technical Details

6.1 IPsec Configuration (LibreSwan)

The following LibreSwan configuration successfully establishes IPv4 tunnels:

```
conn azure-vpngw-tun1
    authby=secret
    auto=start
    left=%defaultroute
    leftid=34.82.67.66
    right=20.110.156.183
    type=tunnel
    ikev2=yes
    ikelifetime=28800s
    salifetime=3600s
    ike=aes256-sha256-modp2048
    esp=aes256-sha256
    keyingtries=%forever
    leftsubnet=0.0.0.0/0
    rightsubnet=0.0.0.0/0
    mark=300/0xffffffff
    vti-interface=vti10
    vti-routing=no
    dpddelay=10
    dpdtimeout=30
    dpdaction=restart_by_peer
```

Important LibreSwan Syntax Notes:

- Use `ikev2=yes` (not `keyexchange=ikev2`)
- Use `ikelifetime=` (not `ikesalifetime=`)
- Use `salifetime=` (not `lifetime=`)

6.2 VTI Route Requirement

Azure BGP uses APIPA addresses (169.254.x.x). A static route must be added to ensure BGP traffic traverses the VTI interface:

```
ip route add 169.254.21.1/32 dev vti10
```

Without this route, BGP traffic exits the wrong interface and sessions fail to establish.

7 Enterprise Architecture: ExpressRoute + VPN Dual-Stack

For production environments, Microsoft recommends ExpressRoute as primary with S2S VPN as backup, both configured for dual-stack.

7.1 Target Architecture

```
┌────────────────────────────────────────────────────────────┐
│                   On-Premises (Dual-Stack)                 │
│                                                            │
│  ┌─────────────────┐            ┌─────────────────┐        │
│  │  ER Edge Router │            │  VPN Edge Router│        │
│  │  (BGP IPv4+v6)  │            │  (IKEv2, BGP)   │        │
│  └────────┬────────┘            └────────┬────────┘        │
└───────────┼──────────────────────────────┼─────────────────┘
            │                              │
            │ ExpressRoute                 │ S2S VPN
            │ (PRIMARY)                    │ (BACKUP)
            │ Private Peering              │ Over Internet
            │ IPv4 + IPv6                  │ IPv4 outer, dual-stack inner
            ▼                              ▼
┌────────────────────────────────────────────────────────────┐
│                   Azure Hub VNet (Dual-Stack)              │
│                                                            │
│  ┌─────────────────────────────────────────────────────┐   │
│  │              GatewaySubnet (/27 or larger)          │   │
│  │                                                     │   │
│  │  ┌─────────────────┐    ┌─────────────────┐         │   │
│  │  │  ExpressRoute   │    │  VPN Gateway    │         │   │
│  │  │  Gateway        │    │  (Dual-Stack)   │         │   │
│  │  │                 │    │  VpnGw1-5/AZ    │         │   │
│  │  └─────────────────┘    └─────────────────┘         │   │
│  └─────────────────────────────────────────────────────┘   │
│                          │                                 │
│          VNet: IPv4 + IPv6 (Global Unicast)                │
│                          │                                 │
│               ┌──────────┴──────────┐                      │
│               │   Spoke VNets       │                      │
│               │   (Peered)          │                      │
│               └─────────────────────┘                      │
└────────────────────────────────────────────────────────────┘
```

Listing 2: Enterprise Dual-Stack Architecture: ExpressRoute Primary + VPN Backup

7.2 ExpressRoute Dual-Stack (Primary Path)

Configuration Requirements:

Component	Requirement
Private Peering IPv6	Add /126 IPv6 subnets (primary + secondary)
Prefix Limits	4000 IPv4 prefixes, 100 IPv6 prefixes to Microsoft
Circuit Support	Must enable dual-stack on circuit before gateway attachment
Gateway	ER gateway in dual-stack VNet

Design Tip: Summarize IPv6 aggressively to stay under the 100-prefix ceiling.

7.3 S2S VPN Dual-Stack (Backup Path)

Preview Constraints:

- Preview enrollment required (new deployments only)
- Cannot convert existing IPv4-only gateway to dual-stack
- Supported SKUs: VpnGw1-5 / VpnGw1AZ-5AZ
- IKEv2 required (IKEv1 does not support IPv6)
- Dual-stack gateways cannot be reverted to IPv4-only

7.4 Routing & Failover Behavior

Azure Side:

- If same prefixes advertised over both ER and VPN, Azure prefers ExpressRoute
- Longest prefix match still applies first
- Advertise identical summarized prefixes over both paths

On-Prem Side:

- Set BGP Local Preference to favor ER-learned routes
- Optionally AS-path prepend on VPN BGP advertisements
- Prevents asymmetric routing during partial failures

Failover Behavior: When ER fails, traffic automatically shifts to VPN. When ER recovers, traffic returns to ER (preferred path).

7.5 Critical Limitations

Azure Route Server: Does NOT support IPv6. Placing Route Server in a VNet with IPv6 can break IPv6 connectivity. Keep Route Server hub IPv4-only if needed for NVA BGP.

Azure Firewall: Does NOT support IPv6 filtering. Can exist in dual-stack VNet but firewall subnet must be IPv4-only.

7.6 Implementation Checklist

Step	Task	Status
1	Define IPv4 + IPv6 address plan (summarize!)	□
2	Create Hub VNet dual-stack + GatewaySubnet /27+	□
3	Deploy ExpressRoute gateway (hub)	□
4	Configure ER private peering IPv4 + IPv6 (/126 pairs)	□

5	Deploy VPN gateway dual-stack (new deployment, right SKU, IKEv2)	□
6	Establish on-prem routing policy: prefer ER, VPN backup	□
7	Validate: simulate ER failure → traffic flips to VPN	□
8	Validate: restore ER → traffic returns to ER	□

8 Conclusions

8.1 Primary Finding

Azure VPN Gateway dual-stack IPv6 requires explicit preview enrollment. Without opt-in, IPv6 is blocked at multiple levels:

1. **Local Network Gateway**: Explicitly rejects IPv6 address prefixes
2. **BGP**: Does not learn or install IPv6 routes
3. **User Defined Routes**: Cannot specify VPN Gateway as next-hop for IPv6
4. **Network Filtering**: Blocks overlay protocols (GRE) that could tunnel IPv6

8.2 Azure Dual-Stack VPN Preview

Microsoft documents Site-to-Site VPN dual-stack support in **PREVIEW** status:

How to Enable Preview:

1. Email your Azure subscription ID to Microsoft (per documentation)
2. Deploy a **new** VPN Gateway (cannot upgrade existing)
3. Use supported SKU: VpnGw1-5 or VpnGw1AZ-5AZ
4. Configure IKEv2 (IKEv1 does not support IPv6)

Preview Constraints:

- Manual enrollment process (not self-service)
- New gateway deployments only
- Preview features may change or have limitations
- Production workloads should evaluate risk

8.3 Decision Guide

Scenario	**Recommended Solution**	**Notes**
Enterprise datacenter extension	ExpressRoute dual-stack	Primary path, VPN as backup
Dynamic routing to NVAs	Plan carefully	Azure Route Server lacks IPv6 support
Need dual-stack now, no ExpressRoute	VPN dual-stack preview	Accept preview constraints

Production with GA features only	GCP or AWS	Both have GA dual-stack VPN

8.4 Recommendations

For organizations requiring cross-premises IPv6 connectivity:

1. **Azure with Preview Enrollment**: Request dual-stack preview access
   - Email subscription ID to Microsoft
   - Plan for new gateway deployment
   - Use IKEv2 with supported SKU
2. **Use GCP or AWS**: Both have GA (non-preview) dual-stack VPN
   - GCP: Use dedicated IPv6 BGP sessions
   - AWS: Use separate IPv4 and IPv6 VPN connections
3. **Azure ExpressRoute**: Supports dual-stack (separate consideration)
   - Higher bandwidth than VPN
   - Different deployment model
4. **Avoid Workarounds**: Without preview enrollment:
   - Overlay tunnels (GRE) are filtered
   - UDRs cannot route IPv6 to VPN Gateway
   - BGP will not learn IPv6 routes

8.5 Infrastructure Resources

The following Terraform resources were created for this test:

```
terraform-azure-vpngw/
├── main.tf                     # VNet, subnets, NSG
├── vpn-gateway.tf              # VPN Gateway (Active-Active)
├── local-network-gateways.tf   # On-prem router definitions
├── connections.tf              # IPsec connections
├── test-vm.tf                  # Test VM
├── variables.tf
└── outputs.tf

terraform-onprem-sim/scripts/
└── configure-azure-vpn.sh      # Azure VPN tunnel config script
```

8.6 Useful Commands

Azure Status Checks:

```
# Connection status
az network vpn-connection show \
  --name conn-to-onprem-router-1-prod-eastus2 \
  --resource-group rg-azure-vpngw-prod-eastus2 \
  --query connectionStatus

# Learned routes
az network vnet-gateway list-learned-routes \
  --name vpngw-azure-prod-eastus2 \
  --resource-group rg-azure-vpngw-prod-eastus2
```

On-Prem Router Checks:

```
# IPsec status
sudo ipsec status

# BGP status
sudo vtysh -c "show bgp summary"
sudo vtysh -c "show bgp ipv4 unicast"
```

9 Appendix: Error Messages

9.1 LocalNetworkGatewayIpv6NotSupported

```
{
  "code": "LocalNetworkGatewayIpv6NotSupported",
  "message": "Local Network Gateway cannot contain IPv6 address prefix."
}
```

9.2 InvalidNextHopType for IPv6

```
{
  "code": "InvalidNextHopType",
  "message": "The next hop type for IPv6 address prefix fd20:e:1::/48
              cannot be 'VirtualNetworkGateway', 'HyperNetGateway'
              or 'VirtualNetworkServiceEndpoint'."
}
```

9.3 VpnSiteIpv6NotSupported (VWAN)

```
{
  "code": "VpnSiteIpv6NotSupported",
  "message": "Vpn Site cannot contain IPv6 address prefix."
}
```