Standard Operating Procedure: Azure Site-to-Site VPN with SonicWall

Document ID:	SOP-AZ-002
Title:	Azure Site-to-Site VPN with SonicWall
Category:	Azure / Network
Version:	1.0
Status:	Draft
Author:	OberaConnect
Creation Date:	2026-01-09
Approval Date:	Pending

1.0 Purpose

To establish a standardized process for creating a site-to-site IPsec VPN connection between an Azure Virtual Network Gateway and a SonicWall firewall, enabling secure communication between on-premises networks and Azure resources.

2.0 Scope

This SOP applies to Network Engineers and Cloud Administrators responsible for: - Adding new spoke sites to an existing Azure hub VPN gateway - Connecting SonicWall firewalls (Gen 6 or Gen 7) to Azure - Configuring IPsec/IKEv2 tunnels between Azure and on-premises networks

3.0 Definitions

Term	Definition
S2S VPN	Site-to-Site Virtual Private Network
VNet	Azure Virtual Network
VPN Gateway	Azure managed gateway service for VPN connections
Local Network Gateway	Azure resource representing the on-premises VPN device
PSK	Pre-Shared Key for IPsec authentication
IKE	Internet Key Exchange protocol
IPsec	Internet Protocol Security
PFS	Perfect Forward Secrecy
DH Group	Diffie-Hellman key exchange group
SA	Security Association

4.0 Roles & Responsibilities

Role	Responsibility
Network Engineer	Configure SonicWall VPN policy and verify tunnel connectivity
Cloud Administrator	Create Azure VPN resources and configure IPsec policies
Security Team	Approve network address ranges and PSK complexity requirements

5.0 Prerequisites

Azure Side

- Existing Azure VPN Gateway (Route-based, Generation2 recommended)
- Virtual Network with GatewaySubnet configured
- Appropriate Azure subscription permissions (Network Contributor or higher)
- Azure CLI authenticated (`az login`)

On-Premises Side

- SonicWall firewall (Gen 6 SonicOS 6.5.x or Gen 7 SonicOS 7.x)
- Static public IP address on WAN interface
- Defined LAN subnet(s) to route through VPN
- Administrative access to SonicWall

Information Required

Item	Example
SonicWall WAN IP	170.249.184.236
On-premises LAN subnet	192.168.10.0/24
Azure VNet subnet to access	10.20.1.0/24
Connection name	Obera_Lab

6.0 Procedure

6.1 Gather On-Premises Network Information

1. **Get SonicWall Public IP:**
   - From a device on the LAN, browse to https://ipchicken.com or https://ifconfig.me
   - Or use PowerShell: `(Invoke-WebRequest -Uri "https://ifconfig.me" -UseBasicParsing).Content`
   - Record the public IP address
2. **Document LAN Subnets:**
   - Identify all subnets that need VPN access to Azure
   - Example: `192.168.10.0/24`

6.2 Create Local Network Gateway in Azure The Local Network Gateway represents the on-premises SonicWall in Azure.

Azure Portal: 1. Search "Local network gateways" → **Create** 2. Configure: - **Resource Group:** Use existing networking RG - **Name:** `lgw-{site-name}` (e.g., `Obera_Lab`) - **Region:** Same as VPN Gateway - **IP address:** SonicWall WAN public IP - **Address space:** On-premises LAN subnets 3. Click **Create**

Azure CLI:

```
az network local-gateway create \
  -g DataCenter \
  -n Obera_Lab \
  --gateway-ip-address 170.249.184.236 \
  --local-address-prefixes 192.168.10.0/24 \
  --location eastus
```

6.3 Create VPN Connection **Azure Portal:** 1. Navigate to **Virtual Network Gateway** → **Connections** → **+ Add** 2. Configure: - **Name:** `conn-{site-name}` (e.g., `Obera_Lab`) - **Connection type:** Site-to-site (IPsec) - **Local network gateway:** Select created gateway - **Shared key (PSK):** Generate strong 20+ character key - **IKE Protocol:** IKEv2 3. Click **Create**

Azure CLI:

```
az network vpn-connection create \
  -g DataCenter \
  -n Obera_Lab \
  --vnet-gateway1 DataCenter_Gateway \
  --local-gateway2 Obera_Lab \
  --shared-key "YourSecurePSK123!" \
  --location eastus
```

6.4 Configure Custom IPsec/IKE Policy Configure matching IPsec parameters for SonicWall compatibility.

Recommended Settings:

Phase	Setting	Value
IKE Phase 1	Encryption	AES256
IKE Phase 1	Integrity	SHA256
IKE Phase 1	DH Group	DHGroup14 (2048-bit)
IKE Phase 1	SA Lifetime	28800 seconds
IPsec Phase 2	Encryption	AES256
IPsec Phase 2	Integrity	SHA256
IPsec Phase 2	PFS	None (disabled)
IPsec Phase 2	SA Lifetime	28800 seconds

Azure CLI:

```
az network vpn-connection ipsec-policy add \
  -g DataCenter \
  --connection-name Obera_Lab \
  --ike-encryption AES256 \
  --ike-integrity SHA256 \
  --dh-group DHGroup14 \
  --ipsec-encryption AES256 \
  --ipsec-integrity SHA256 \
  --pfs-group None \
  --sa-lifetime 28800 \
  --sa-max-size 0
```

6.5 Configure Traffic Selectors (Optional) To restrict which Azure subnets are accessible through the tunnel:

```
# Enable policy-based traffic selectors
az network vpn-connection update \
  -g DataCenter \
  -n Obera_Lab \
  --use-policy-based-traffic-selectors true

# Add traffic selector
az network vpn-connection update \
  -g DataCenter \
  -n Obera_Lab \
  --set trafficSelectorPolicies='[{"localAddressRanges":["10.20.1.0/24"],"remoteAddressRanges":["192.168
```

6.6 Configure SonicWall VPN Policy

Gen 7 SonicWall (SonicOS 7.x)

1. Navigate to **Network** → **IPSec VPN** → **Rules and Settings**
2. Click **+ Add** to create new policy

Gen 6 SonicWall (SonicOS 6.5.x)

1. Navigate to **VPN** → **Settings**
2. Click **Add** under VPN Policies

General Tab Configuration

Setting	Value
Policy Type	Site to Site
Authentication Method	IKE using Preshared Secret
Name	Azure-{VNet-Name}
IPSec Primary Gateway	Azure VPN Gateway Public IP
Shared Secret	Same PSK as Azure connection

Network Tab Configuration

Setting	Value
Local Networks	On-premises LAN subnet(s)
Remote Networks	Azure VNet subnet(s)

Create Address Objects if needed: - Local: `Local_LAN` → `192.168.10.0/24` - Remote: `Azure_VNet` → `10.20.1.0/24`

Proposals Tab Configuration IKE (Phase 1) Proposal: | Setting | Value | |———|——-| | Exchange | IKEv2 Mode | | DH Group | Group 14 | | Encryption | AES-256 | | Authentication | SHA256 | | Life Time (seconds) | 28800 |

IPsec (Phase 2) Proposal: | Setting | Value | |———|——-| | Protocol | ESP | | Encryption | AES-256 | | Authentication | SHA256 | | Enable Perfect Forward Secrecy | **Unchecked** | | Life Time (seconds) | 28800 |

Advanced Tab Configuration

Setting	Value
Local IKE ID	IP Address → SonicWall WAN IP
Peer IKE ID	IPv4 Address → Azure Gateway IP
Enable Keep Alive	Checked

4. Click **OK** to save
5. Ensure policy is **Enabled**

7.0 Verification & Quality Checks

Azure Side Verification Check Connection Status:

```
az network vpn-connection show \
  -g DataCenter \
  -n Obera_Lab \
  --query "{Name:name, Status:connectionStatus, Ingress:ingressBytesTransferred, Egress:egressBytesTrans
  -o table
```

Expected output when connected:

```
Name       Status     Ingress    Egress
---------  ---------  ---------  ---------
Obera_Lab  Connected  12345      67890
```

SonicWall Side Verification Gen 7: Navigate to **Monitor** → **VPN** → **IPSec Gen 6:** Navigate to **VPN** → **Settings** and check status indicator

Green indicator = Tunnel established

Connectivity Test From on-premises device (192.168.10.x):

```
ping 10.20.1.8    # Azure VM or resource
```

From Azure VM (10.20.1.x):

```
ping 192.168.10.1    # On-premises gateway or device
```

8.0 Troubleshooting

Issue	Possible Cause	Resolution
Status: NotConnected, 0 bytes transferred	SonicWall not initiating	Enable VPN policy; check "Keep Alive" is enabled
IKE Phase 1 failure	DH Group mismatch	Verify both sides use Group 14 (2048-bit)
IKE Phase 1 failure	Encryption mismatch	Ensure both use AES-256 and SHA256
IKE Phase 1 failure	IKE ID mismatch	Set Local IKE ID to IP Address (not Firewall Identifier)
Phase 2 failure	PFS mismatch	Disable PFS on SonicWall if Azure has PFS=None
Phase 2 failure	Lifetime mismatch	Set both Phase 1 and Phase 2 to 28800 seconds
Tunnel up but no traffic	Traffic selector mismatch	Verify Local/Remote networks match on both sides
Tunnel up but no traffic	Firewall rules	Check SonicWall access rules allow VPN zone traffic
Intermittent connectivity	NAT-T issues	Ensure UDP 500 and 4500 are open

SonicWall VPN Logs

- **Gen 7:** Monitor → Logs → Filter: VPN

- **Gen 6:** Log → View → Category: VPN

Look for IKE negotiation messages to identify which phase is failing.

Azure Diagnostics

```
# View activity logs for VPN connection
az monitor activity-log list \
  --resource-group DataCenter \
  --offset 1h \
  --query "[?contains(resourceId, 'Obera_Lab')]"
```

9.0 Related Documents

Document	Description
SOP-NET-001	Initial SonicWall Firewall Setup
SOP-NET-006	SonicWall Backup Configuration
SOP-AZ-001	Azure VM Infrastructure Administration

10.0 Revision History

Version	Date	Author	Change Description
1.0	2026-01-09	OberaConnect	Initial document creation

11.0 Approval

Name	Role	Signature	Date
	Network Manager Cloud Administrator		

Appendix A: Azure CLI Quick Reference

```
# List all VPN connections
az network vpn-connection list -g DataCenter -o table

# Check specific connection status
az network vpn-connection show -g DataCenter -n Obera_Lab \
  --query "{Status:connectionStatus}" -o table

# Update shared key
az network vpn-connection shared-key update \
  -g DataCenter --connection-name Obera_Lab \
  --value "NewSecurePSK123!"

# View IPsec policy
az network vpn-connection ipsec-policy list \
  -g DataCenter --connection-name Obera_Lab
```

```
# Delete connection (if needed)
az network vpn-connection delete -g DataCenter -n Obera_Lab
az network local-gateway delete -g DataCenter -n Obera_Lab
```

Appendix B: Setco Azure Hub Reference

Resource	Value
VPN Gateway	DataCenter_Gateway
Gateway Public IP	4.157.5.219
VNet	DataCenter_vNet
Primary Subnet	10.20.1.0/24
Resource Group	DataCenter
Region	East US