SME Reference: Hub-and-Spoke Packet Walk

Subject: Verified Data Plane Path (On-Prem to Spoke via NVA)

Current Logic: Symmetric Inspection with ILB Ingress and Subnet Gateway Egress.

1. The Ingress Path (On-Prem ➔ Spoke)

This path ensures that every packet entering your environment is inspected by the Palo Alto.

1. **On-Prem Source (10.0.11.21)**: Sends an ICMP Request to the Spoke VM.
2. **VPN Gateway**: Receives the packet via the VPN Tunnel.
3. **GatewaySubnet UDR**: Azure checks the Gateway Subnet Route Table.
   - *Route Match:* 172.17.0.0/16 ➔ **Next Hop: 172.18.2.6 (ILB)**.
4. **Internal Load Balancer**: Receives the packet and distributes it to a healthy NVA.
5. **NVA Ingress (ethernet1/2)**: Palo Alto receives the packet, inspects it against security policies, and creates a session entry in its state table.
6. **NVA Egress**: The NVA forwards the packet to the Spoke.
7. **VNet Peering**: The packet crosses the Hub-to-Spoke peering (**Allow Forwarded Traffic** must be enabled).
8. **Spoke VM (172.17.0.4)**: Receives the Request.

2. The Egress Path (Spoke ➔ On-Prem)

This is the "Return Path" where we fixed the loop by avoiding the ILB on the way out.

1. **Spoke VM (172.17.0.4)**: Generates an ICMP Reply for 10.0.11.21.
2. **Spoke Subnet UDR**: Azure checks the Spoke's Route Table.
   - *Route Match:* 10.0.0.0/8 ➔ **Next Hop: 172.18.2.6 (ILB)**.
3. **Internal Load Balancer**: Hands the packet back to the **same NVA** (due to session persistence).
4. **NVA Ingress (ethernet1/2)**: Palo Alto matches the packet to the existing "Active" session.
5. **NVA Trust-VR (The Loop Breaker)**: The Palo Alto checks its internal routing table (trust-vr).
   - *Route Match:* 10.0.11.0/24 ➔ **Next Hop: 172.18.2.1 (Subnet Gateway)**.
6. **Azure Fabric**: The packet is handed to the Azure SDN fabric at the .1 address.
7. **VPN Gateway**: The fabric delivers the packet to the Gateway, which puts it into the tunnel.
8. **On-Prem Destination**: Receives the 100% successful ping reply.

3. Visual Traffic Diagram

```
graph TD
    subgraph "On-Premises"
        OP[Client: 10.0.11.21]
    end

    subgraph "Azure Hub VNet"
        GW[VPN Gateway]
        GWS[GatewaySubnet UDR: 172.17/16 -> .6]
        ILB[Internal Load Balancer: 172.18.2.6]
        NVA[Palo Alto NVA: 172.18.2.x]
        VR[NVA VR: 10.0.11/24 -> 172.18.2.1]
    end

    subgraph "Azure Spoke VNet"
        S_UDR[Spoke Subnet UDR: 10.0.0.0/8 -> .6]
        VM[Spoke VM: 172.17.0.4]
    end

    %% Ingress Flow
    OP -->|1. VPN Tunnel| GW
    GW -->|2. UDR Trigger| GWS
    GWS -->|3. Route to VIP| ILB
    ILB -->|4. Inspect| NVA
    NVA -->|5. Forward| VM

    %% Egress Flow
    VM -->|6. Reply| S_UDR
    S_UDR -->|7. Route to VIP| ILB
    ILB -->|8. Match Session| NVA
    NVA -->|9. Route to .1| VR
    VR -->|10. Fabric Hand-off| GW
    GW -->|11. Return Tunnel| OP

    style NVA fill:#f9f,stroke:#333,stroke-width:4px
    style VR fill:#bbf,stroke:#333,stroke-width:2px
```

4. Why this Architecture is SME Standard

1. **Symmetry**: By using the ILB for both Ingress and Egress, the Palo Alto stays "Stateful." It sees the start and end of every conversation.
2. **Linearity**: By pointing the NVA return route to .1 (The Fabric) instead of .6 (The LB), you prevent the "Hairpin Loop" that breaks traceroutes and causes TCP instability.

3. **Determinism**: If a ping fails, you now know exactly which hop to check: the Gateway UDR, the NVA Policy, or the Spoke UDR.