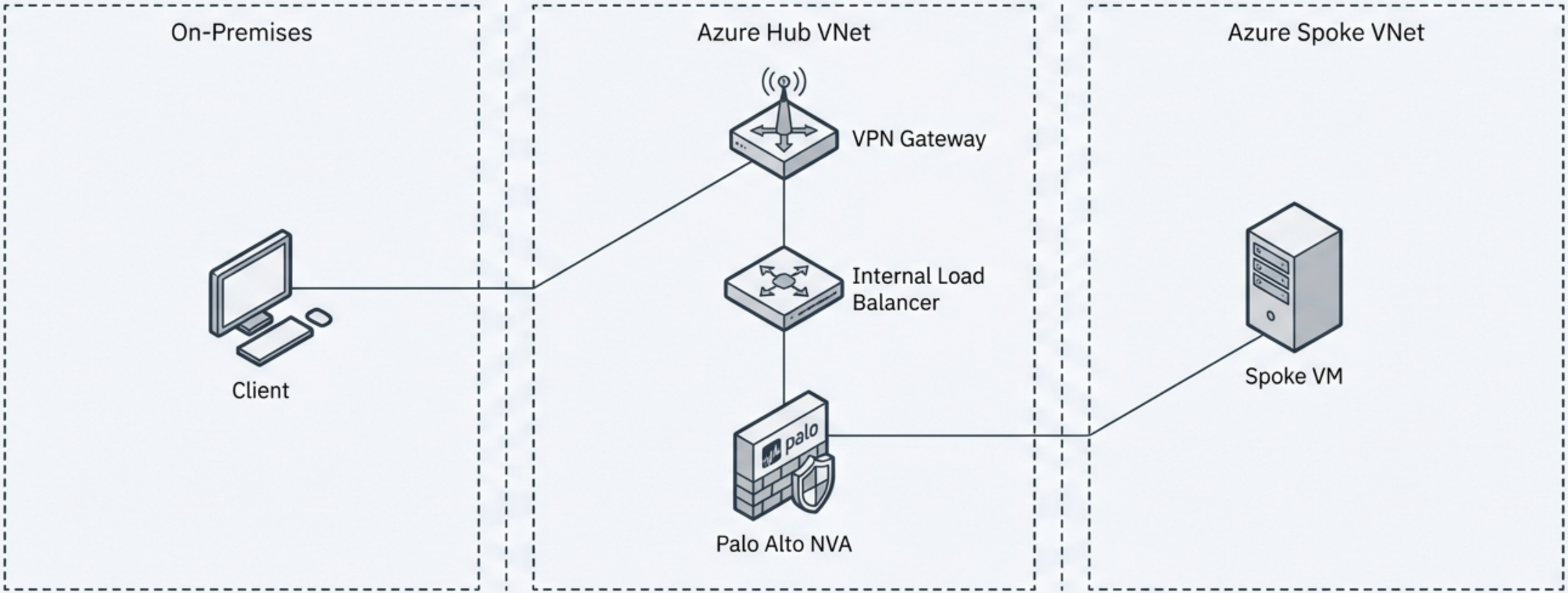
Symmetric Routing Logic for NVA Hub-and-Spoke Traffic

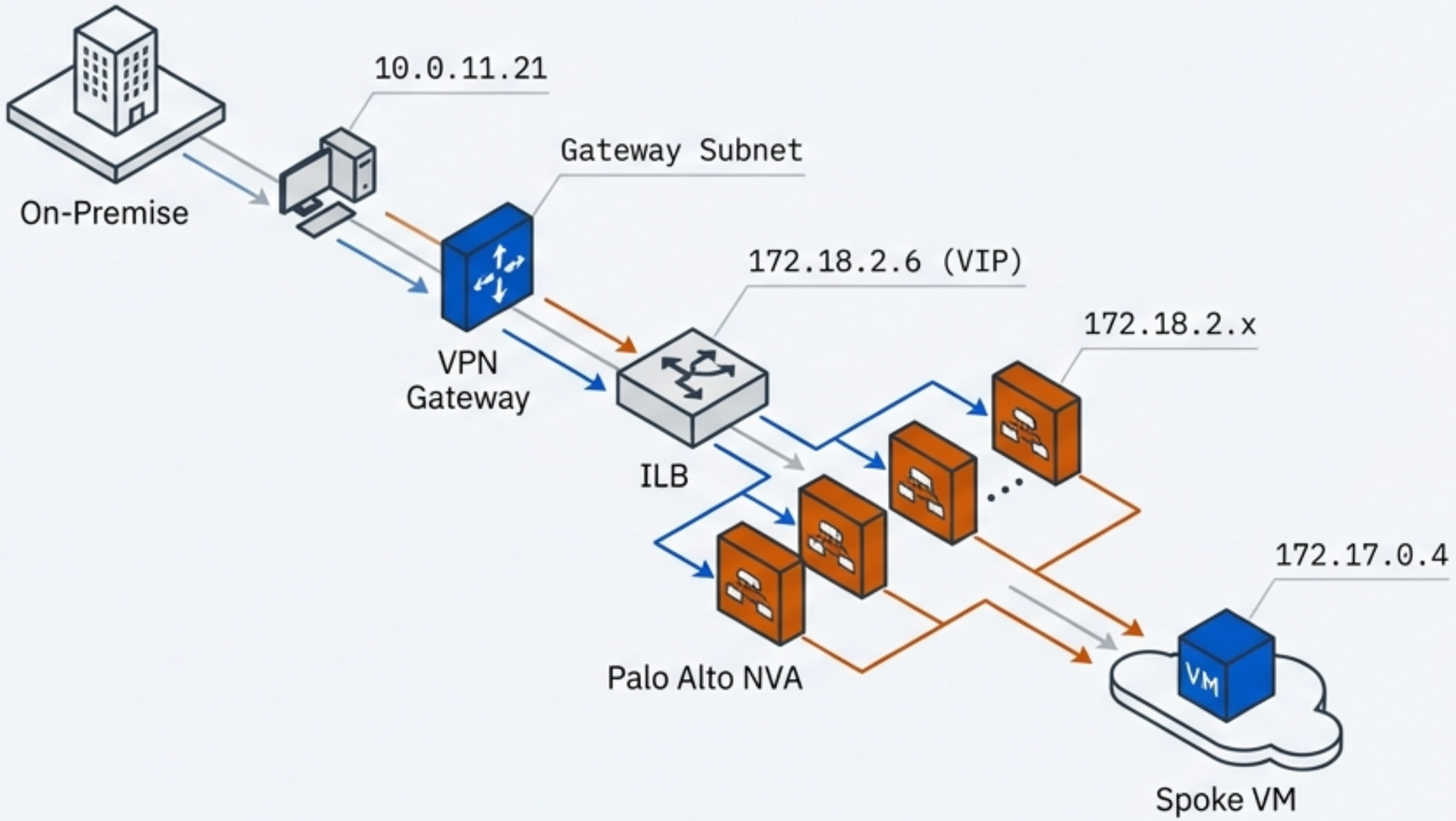
Verified Data Plane Path: On-Prem to Spoke Inspection



Packet Walk Visualization: Ingress & Egress Flows

The Objective: Ensuring Symmetric Inspection

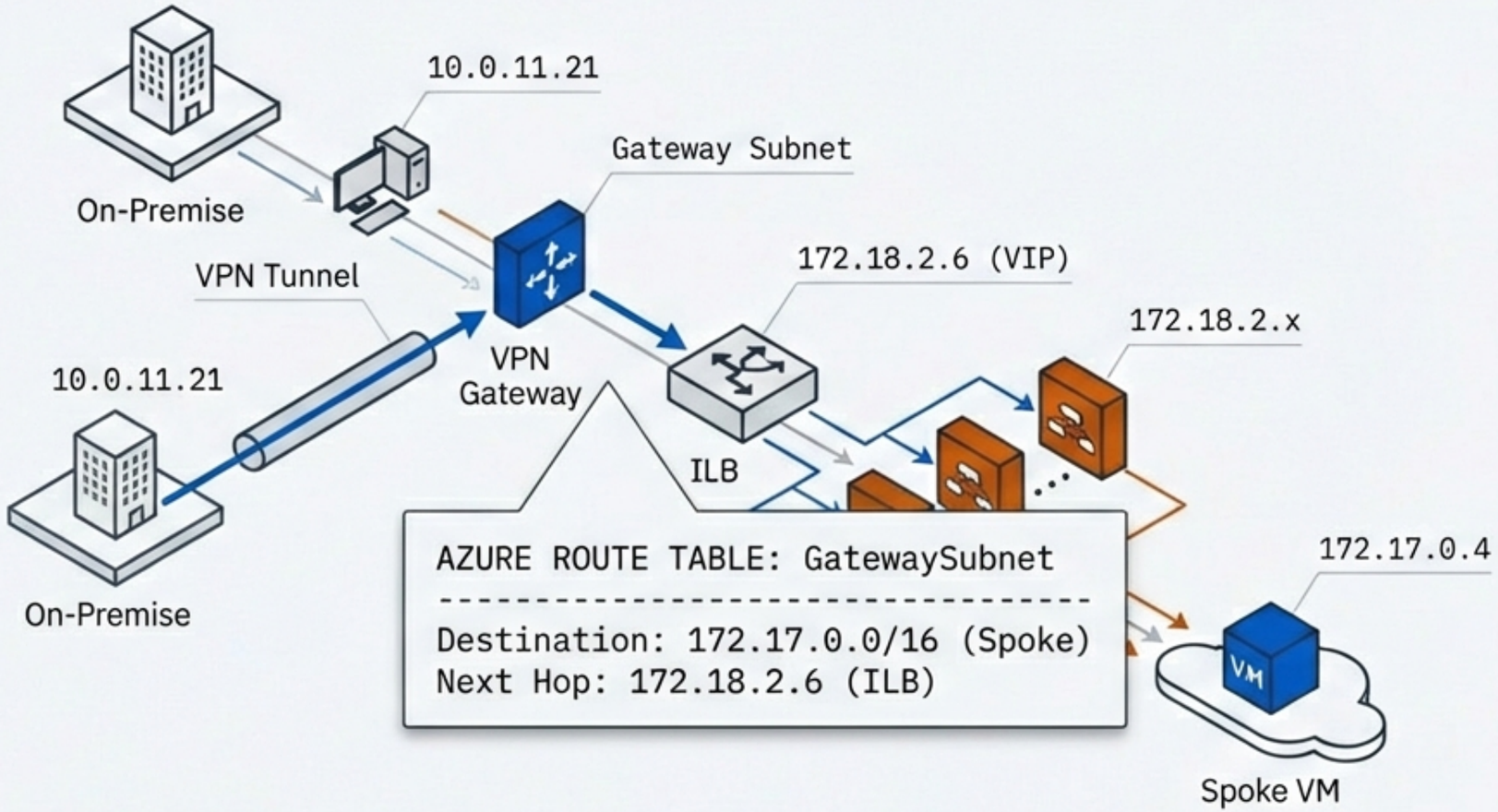
The goal is to ensure the firewall creates and maintains a stateful session by seeing traffic in *both* directions. We must avoid asynchronous routing routing where return traffic bypasses the firewall.



Source → Gateway → ILB → NVA → Spoke

Ingress Step 1: Entry & The UDR Trigger

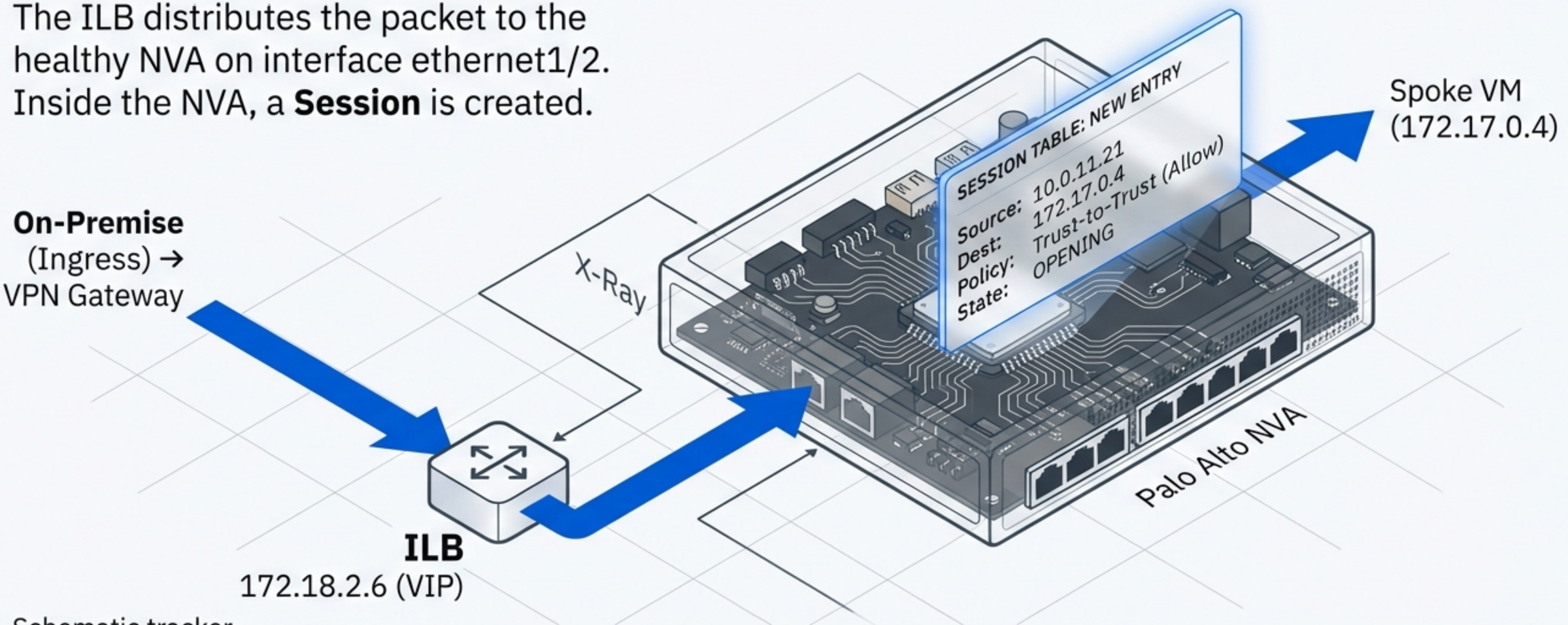
The On-Prem Client (10.0.11.21) sends an ICMP Request. The VPN Gateway receives the packet via the tunnel. Azure immediately checks the **GatewaySubnet UDR**.



Source → Gateway → ILB → NVA → Spoke

Ingress Step 2: Load Balancing & Session Creation

The ILB distributes the packet to the healthy NVA on interface ethernet1/2. Inside the NVA, a **Session** is created.

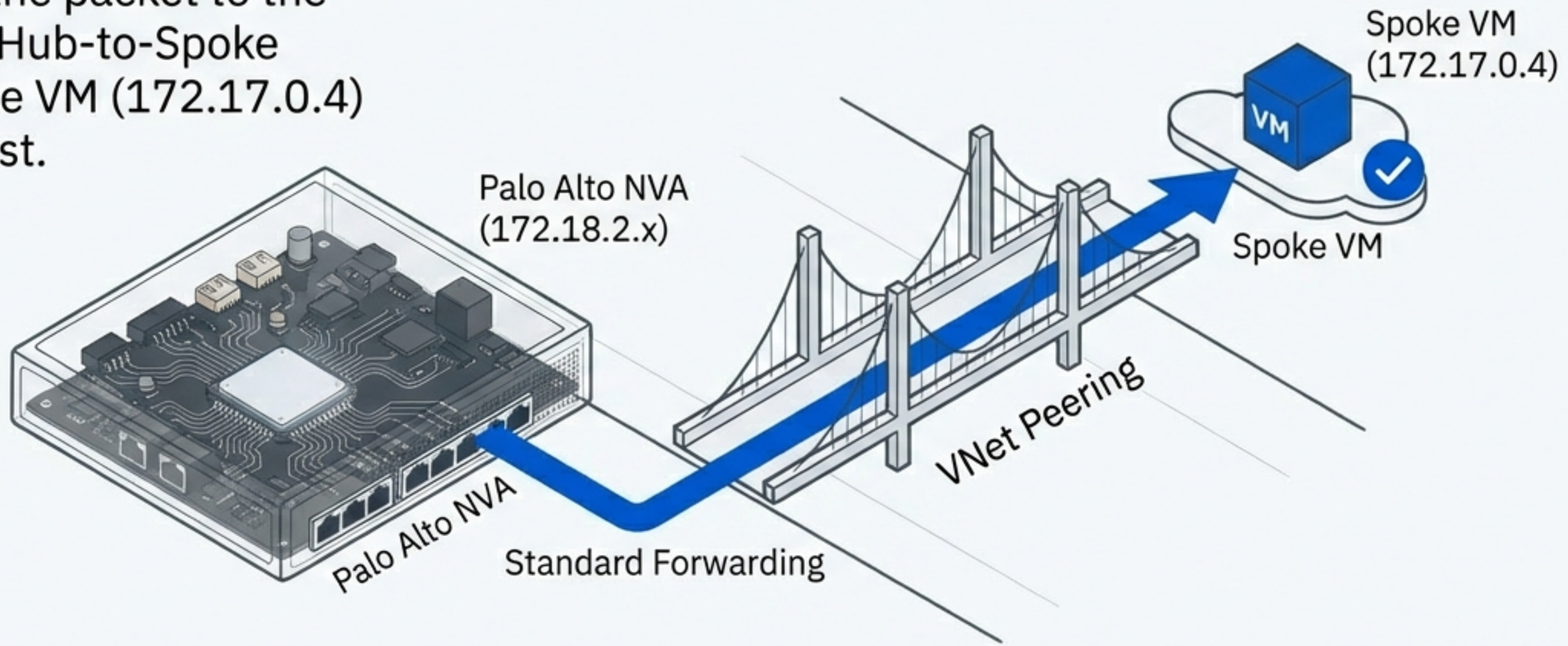


Schematic tracker

Source → Gateway → ILB → **ILB → NVA** → Spoke

Ingress Step 3: Delivery to Spoke

The NVA forwards the packet to the destination via the Hub-to-Spoke VNet peering. Spoke VM (172.17.0.4) receives the Request.



Ingress Complete. State Established.

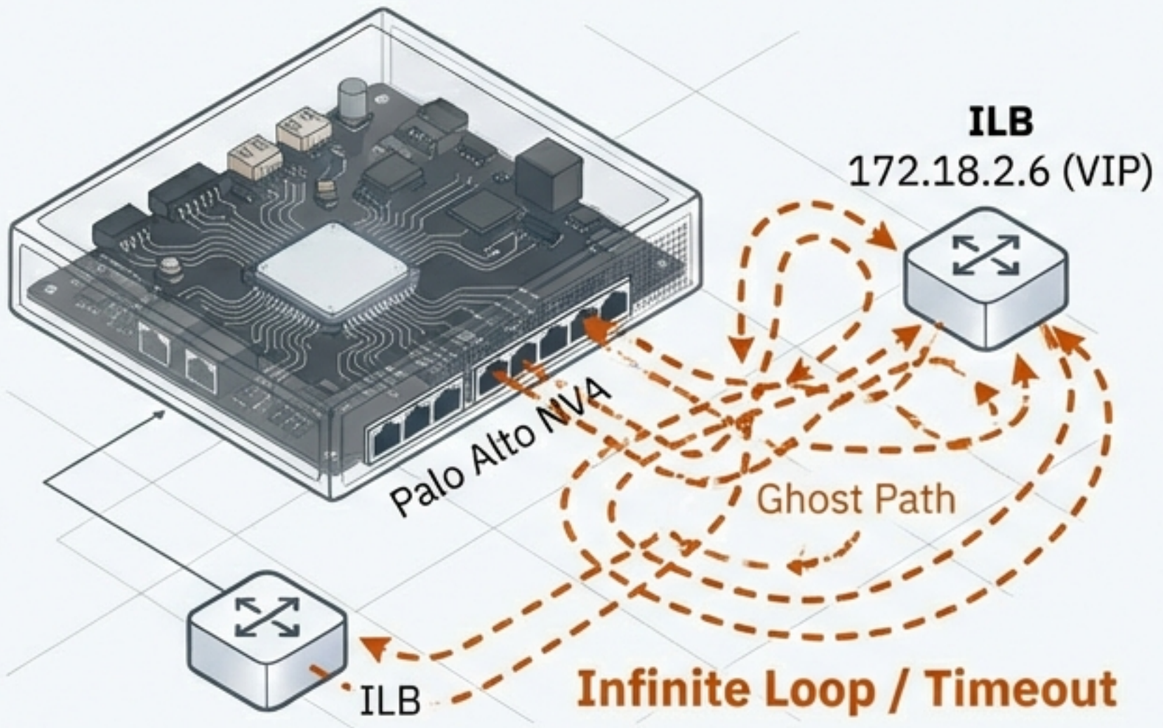
Schematic tracker

Source → Gateway → ILB → **ILB → NVA** → **Spoke**

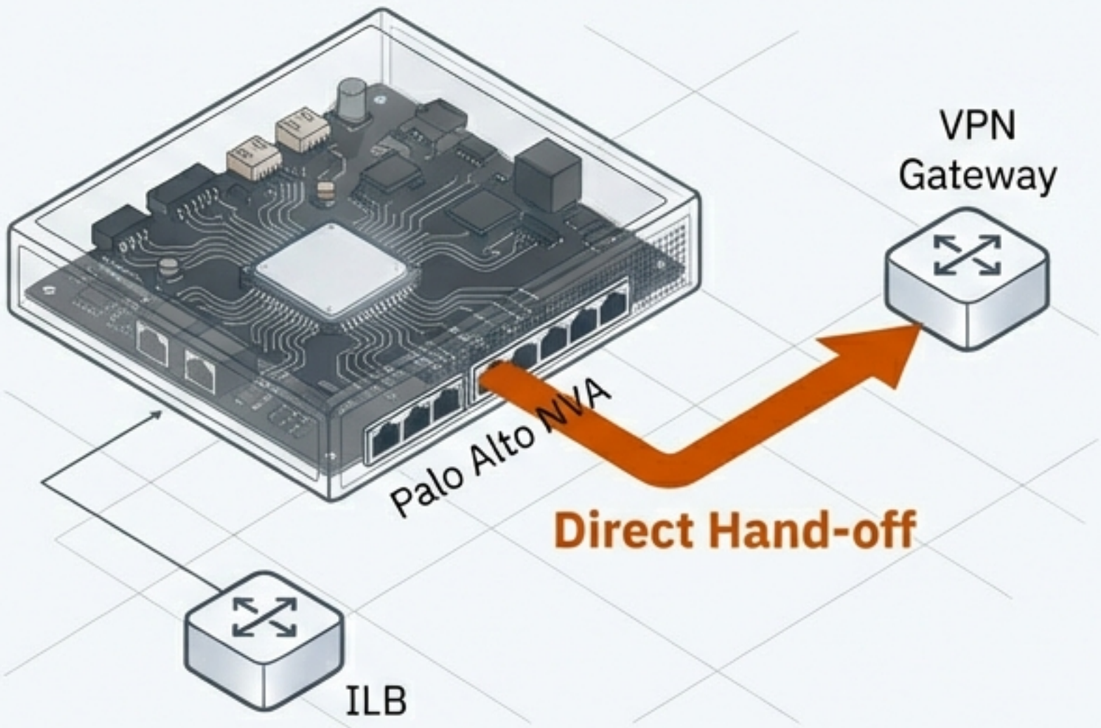
The Egress Challenge: Avoiding the Loop

"A packet should never visit the same Load Balancer VIP twice in a single direction. The .1 hand-off is the exit strategy that makes this design production-ready."

THE RISK: ASYMMETRIC LOOP

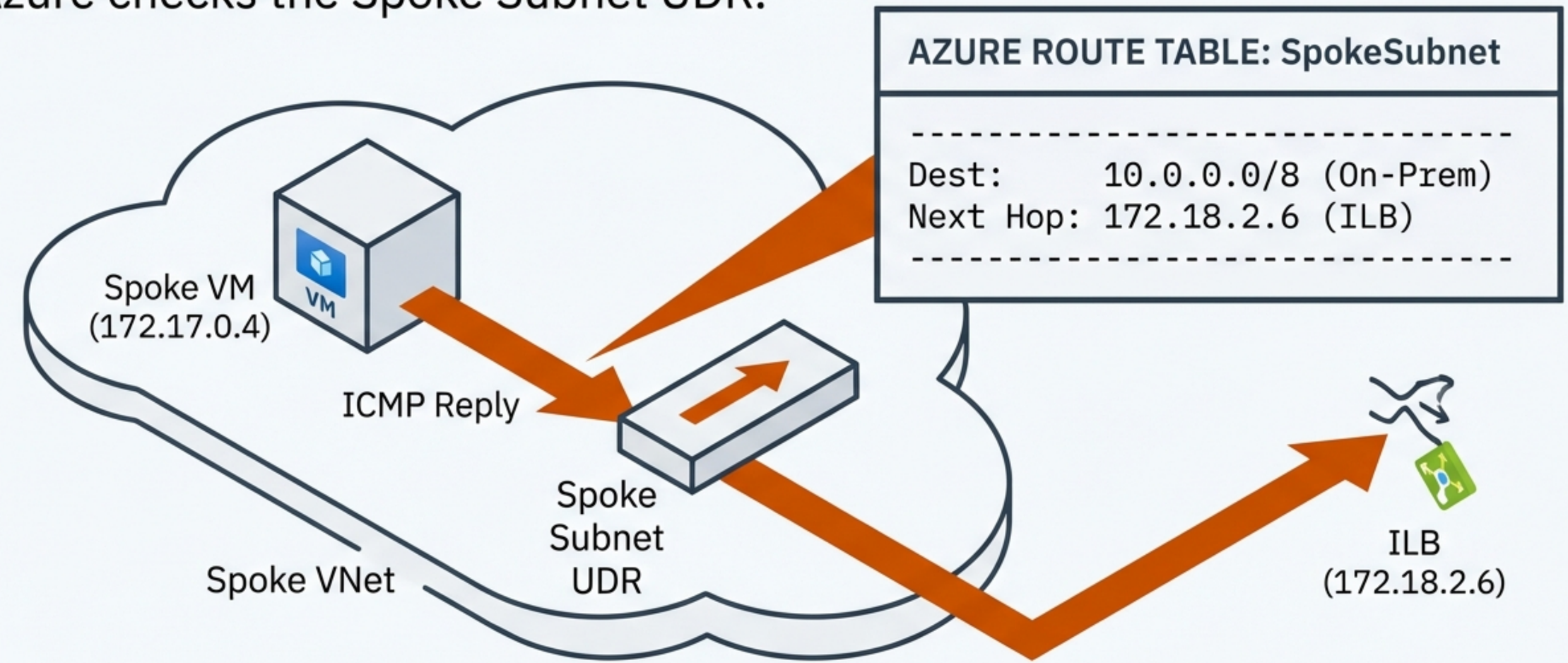


THE FIX: SYMMETRIC EXIT



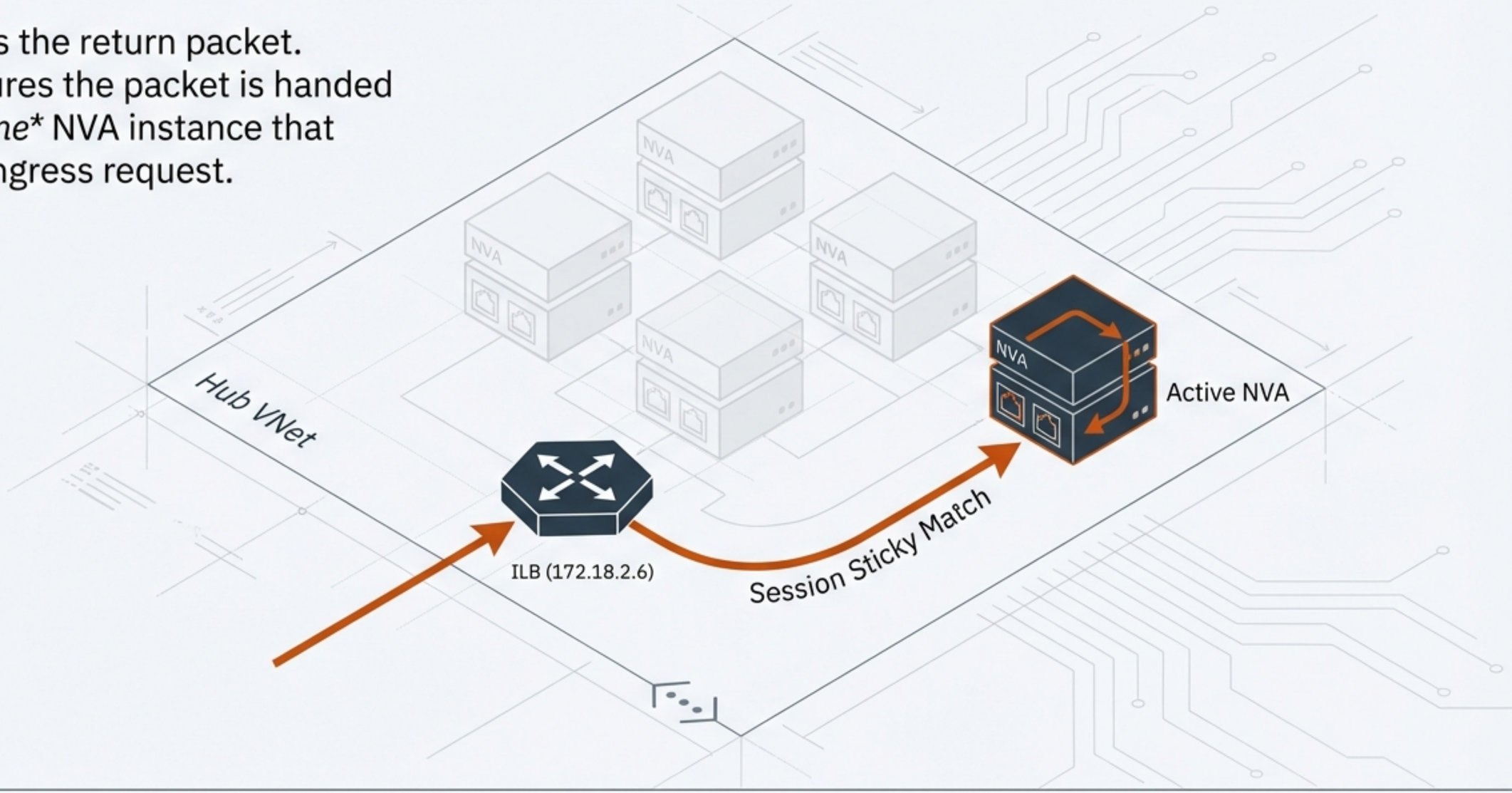
Egress Step 1: The Reply & Spoke UDR

The Spoke VM generates an ICMP Reply destined for the On-Prem Client. Azure checks the Spoke Subnet UDR.



Egress Step 2: Session Persistence

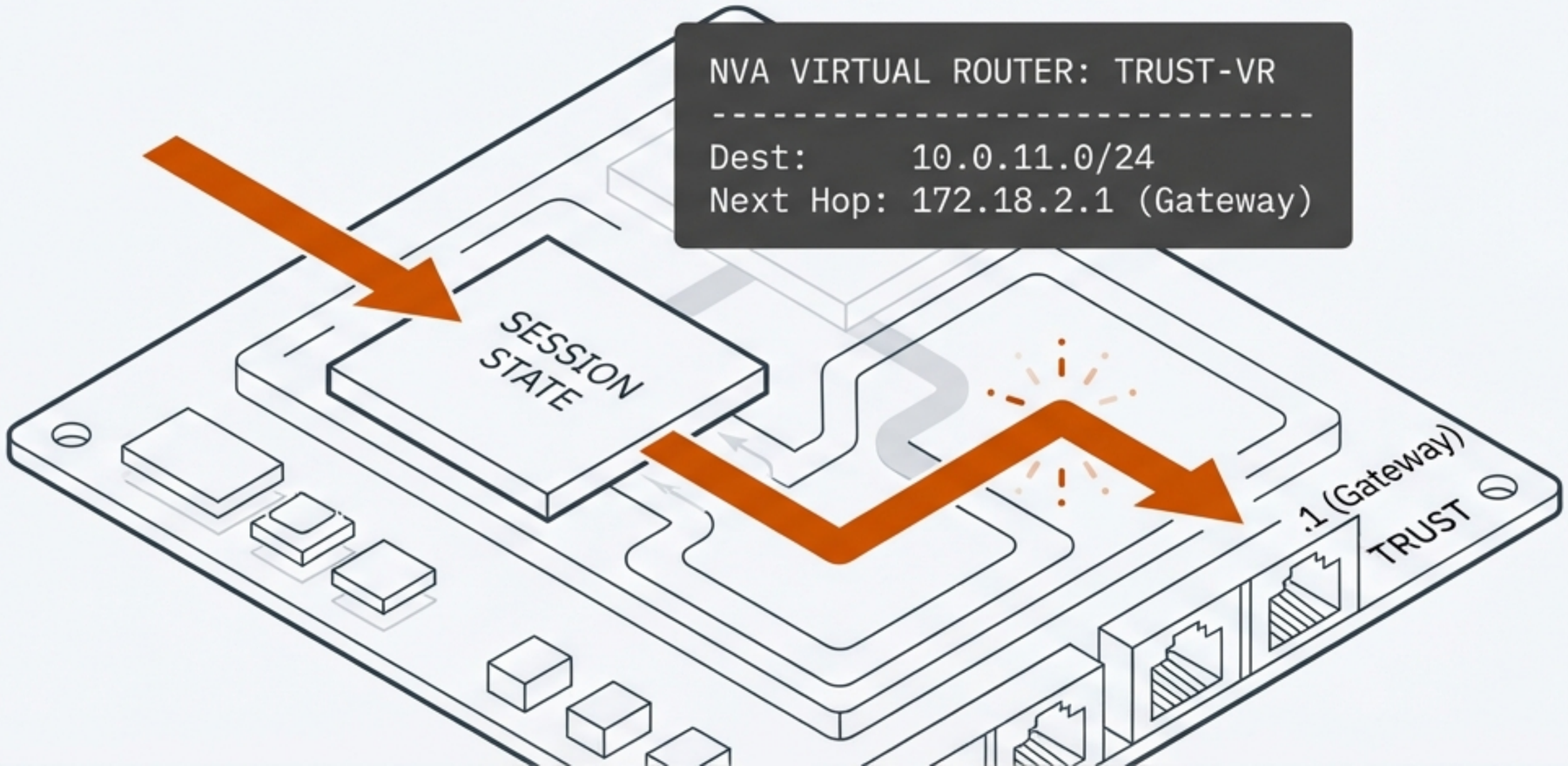
The ILB receives the return packet. **Stickiness** ensures the packet is handed back to the **same** NVA instance that processed the ingress request.



Spoke → **ILB ➔ NVA** → Gateway → Source

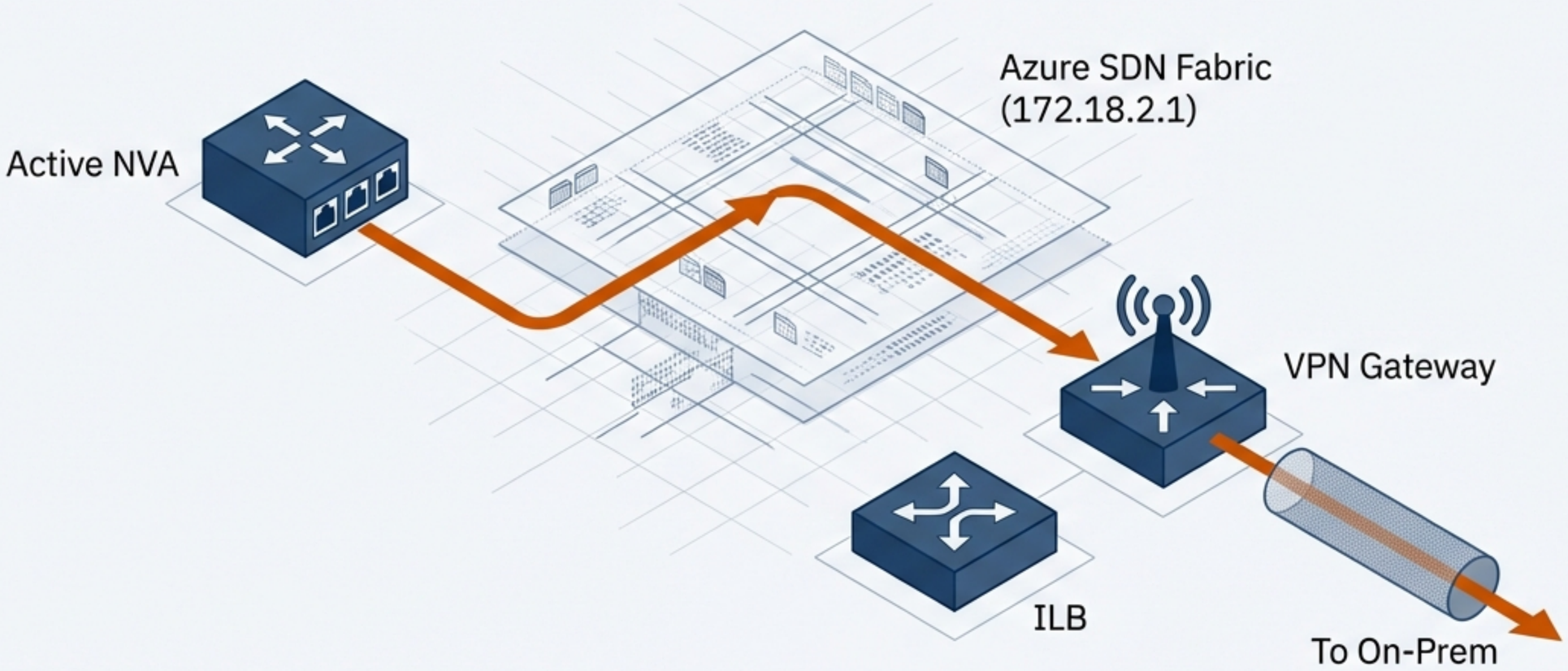
Egress Step 3: The Fix (NVA Internal Routing)

The Palo Alto matches the packet to the existing ‘Active’ session. Crucially, the NVA checks its **Trust-VR** (Virtual Router) to decide where to send it next.



Egress Step 4: The Fabric Hand-off

The NVA sends the packet to the Azure SDN fabric at the .1 address.
The Fabric delivers it to the VPN Gateway, bypassing the ILB.



Spoke → ILB → NVA → Gateway → Source

The Logic Map: End-to-End Verification

Step	Device	Action	Routing Logic
1 |	VPN Gateway	Receive	`GatewaySubnet UDR: Dest Spoke -> .6`
2 |	ILB	Load Balance	`Sends to NVA`
3 |	NVA (Ingress)	Security Check	`Policy: Trust-to-Trust`
4 |	NVA (Egress)	Forward	`Peering to Spoke`
5 |	Spoke VM	Respond	`Spoke Subnet UDR: Dest On-Prem -> .6`
6 |	ILB	Persistence	`Stickiness to same NVA`
7 |	**NVA (Return)**	**Routing Match**	**`NVA Trust-VR: Dest On-Prem -> .1`**
8 |	Azure Fabric	Hand-off	`Delivers to VPN Gateway`

Evidence of Success: Log Verification

Logs confirm the symmetric path and successful handshake.

Palo Alto Traffic Log						
TIME:	SOURCE:	DEST:	INGRESS INT:	EGRESS INT:	ACTION:	STATUS:
2023-10-27 14:23:01	10.0.11.21	172.17.0.4	ethernet1/2	tunnel.200	allow	**ACTIVE** ✅

Status ‘Active’ confirms the firewall saw both the Request and the Reply.

Production-Ready **Symmetric** Routing

By pointing the NVA's internal route to the .1 Gateway instead of back to the .6 Load Balancer, we successfully break the loop and ensure symmetric inspection for all traffic.