**1. Route Table Updates**

**NEW Route Table (zanrgfwrtp01) - Currently configured:**

* **Out-to-Firewall**: 0.0.0.0/0 → 10.20.40.4 (Correct - points to new firewall)

**OLD Route Tables that need updating:**

**zanrgfwrtp01** (OLD):

* Currently: 0.0.0.0/0 → 181.0.1.4 (old firewall)
* **Update to**: 0.0.0.0/0 → 10.20.40.4 (new firewall)

**zanrgfwrtdev01**:

* Currently: 0.0.0.0/0 → 181.0.1.4 (old firewall)
* **Update to**: 0.0.0.0/0 → 10.20.40.4 (new firewall)

**2. VNet Peerings Required**

Create these three peerings from the new VNet (10.20.40.0/24):

1. **To Dev VNet (182.0.0.0/16)**
   * Name: zanrgvnetldzp-10.20.40.0-24-to-zanrgvnetdevd01-182.0.0.16
   * Allow forwarded traffic: Yes
   * Allow gateway transit: Yes (from new VNet)
   * Use remote gateways: No
2. **To New Prod VNet (183.0.0.0/16)**
   * Name: zanrgvnetldzp-10.20.40.0-24-to-zanrgvnetldzp01-183.0.0.0-16
   * Allow forwarded traffic: Yes
   * Allow gateway transit: Yes (from new VNet)
   * Use remote gateways: No
3. **To Dev VNet 2 (184.0.0.0/16)**
   * Name: zanrgvnetldzp-10.20.40.0-24-to-zanrgvnetdevd01-184.0.0.0-16
   * Allow forwarded traffic: Yes
   * Allow gateway transit: Yes (from new VNet)
   * Use remote gateways: No

**3. Firewall Rule Updates**

**Network Rules to Update:**

Since the firewall is moving from 181.0.1.4 to 10.20.40.4, no existing rules need IP updates as they use source/destination addresses that remain valid.

**New Network Rule Required:**

Add a rule to allow the new VNet to communicate with the old networks:

**Collection**: Net-Allow-Peering (Priority 100) **New Rule**:

* Name: NewLandingZone-to-AllNetworks
* Source: 10.20.40.0/24
* Destination: 181.0.0.0/16, 182.0.0.0/16, 183.0.0.0/16, 184.0.0.0/16
* Ports: \*
* Protocol: Any
* Action: Allow

**DNS Rules Update:**

The existing DNS rules don't include the new network. Add:

**Collection**: Net-Allow-DNS (Priority 200) **New Rule**:

* Name: Allow-DNS-NewLandingZone
* Source: 10.20.40.0/24
* Destination: 169.63.129.16, 209.244.0.3, 209.244.0.4
* Port: 53
* Protocol: UDP

**4. NSG Review**

The NSG (zanrgnsgssp001) doesn't need updates as:

* It's not attached to any resources currently
* The rules are based on IP ranges that remain valid
* It can be attached to new subnets as needed without modification

**5. Additional Considerations**

1. **Update DNS servers** on the new VNet if needed (currently showing 183.0.11.36 which should be decommissioned later)
2. **Verify ExpressRoute connection** is properly configured with the new gateway (zanrgergwp01)
3. **Test connectivity** after making these changes, especially:
   * On-premises to new VNet (10.20.40.0/24)
   * New VNet to existing peered networks
   * DNS resolution from new VNet
4. **Monitor firewall logs** after cutover to ensure traffic is flowing correctly through the new firewall at 10.20.40.4

**Rules to ADD for On-Premises Communication:**

**1. Allow On-Premises to reach new Landing Zone**

There's already a rule **Net-Allow-10.20-OnPrem** that allows 181.0.3.4 → 10.20.0.0/24. We need to:

**UPDATE existing rule Net-Allow-10.20-OnPrem**:

* Source: 181.0.3.4
* Destination: 10.20.0.0/24, **10.20.40.0/24** (add the new network)
* Ports: \*
* Protocol: Any, ICMP, UDP, TCP

**2. Allow new Landing Zone to reach On-Premises**

Looking at the pattern, we need a rule for the new VNet to reach on-premises (10.20.x.x networks):

**ADD to Net-Allow-10.20-OnPrem collection**: **Rule Name: NewLandingZone-to-OnPrem**

* Source: 10.20.40.0/24
* Destination: 10.20.0.0/16 (this covers all on-premises 10.20.x.x ranges)
* Ports: \*
* Protocol: Any, ICMP, UDP, TCP

**3. For full bidirectional communication through peerings**

The existing **Net-Allow-Peering** rules handle inter-Azure network communication. To ensure traffic can flow from on-premises through the new ExpressRoute gateway to peered networks and back, we need:

**Already covered by existing rules**:

* The six existing Net-Allow-Peering rules (NewProd>OldDev, etc.) handle Azure-to-Azure traffic
* These will work once peerings are established

**ADD these two rules to Net-Allow-Peering**:

1. **AllNetworks>NewLandingZone**
   * Source: 181.0.0.0/16, 182.0.0.0/16, 183.0.0.0/16, 184.0.0.0/16
   * Destination: 10.20.40.0/24
   * Ports: \*
   * Protocol: Any
2. **NewLandingZone>AllNetworks**
   * Source: 10.20.40.0/24
   * Destination: 181.0.0.0/16, 182.0.0.0/16, 183.0.0.0/16, 184.0.0.0/16
   * Ports: \*
   * Protocol: Any

**4. DNS Resolution**

**ADD to Net-Allow-DNS**: **Rule Name: Allow-DNS-NewLandingZone**

* Source: 10.20.40.0/24
* Destination: 169.63.129.16, 209.244.0.3, 209.244.0.4
* Port: 53
* Protocol: UDP

**Summary of communication flow:**

1. **On-premises → New Landing Zone**: Via ExpressRoute, allowed by updated Net-Allow-10.20-OnPrem
2. **New Landing Zone → On-premises**: Via ExpressRoute, allowed by new NewLandingZone-to-OnPrem rule
3. **On-premises → Peered VNets**: Traffic flows through new ExpressRoute gateway in Landing Zone, then to peered VNets (enabled by gateway transit)
4. **Peered VNets → On-premises**: Return traffic flows back through Landing Zone gateway

**Total changes needed:**

* **UPDATE**: 1 existing rule (Net-Allow-10.20-OnPrem)
* **ADD**: 4 new rules (NewLandingZone-to-OnPrem, AllNetworks>NewLandingZone, NewLandingZone>AllNetworks, Allow-DNS-NewLandingZone)

This ensures complete bidirectional communication between on-premises, the new Landing Zone, and all peered Azure networks.