TEMPLATE

Azure Virtual Network Peering Production Readiness Template

A practical worksheet for evaluating Azure VNet peering designs before rollout, with routing, segmentation, DNS, and validation checks.

Azure Virtual Network Peering Production Readiness Template

Use this template to assess whether an Azure virtual network peering design is ready for production. Complete each section before enabling or expanding peering.

---

1) Scope

Project / Environment: _____

Owner: _____

Date: _____

Peer VNets:

- VNet A: _____
- VNet B: _____

Region(s): _____

Purpose of peering:

- [ ] App tier connectivity
- [ ] Shared services access

- [ ] Cross-environment connectivity
- [ ] Hub-and-spoke integration
- [ ] Other: _____

---

2) Business and architecture intent

Why peering is needed:

_____

_____

What traffic must be allowed:

- Source subnet(s): _____
- Destination subnet(s): _____
- Required ports/protocols: _____
- Required directionality: _____

What traffic must be blocked:

_____

_____

---

3) Address space review

- [ ] VNet address spaces do not overlap
- [ ] Subnet ranges are documented
- [ ] Future growth has been considered
- [ ] No temporary or test ranges conflict with production

VNet A address space: _____

VNet B address space: _____

Notes:

_____

---

4) Connectivity model

Peering type

- [ ] Regional VNet peering
- [ ] Global VNet peering

Topology

- [ ] Direct VNet-to-VNet
- [ ] Hub-and-spoke
- [ ] Multi-spoke with central inspection
- [ ] Other: _____

Transit requirements

- [ ] No transit required
- [ ] Gateway transit required
- [ ] Forwarded traffic required
- [ ] Custom routing required
- [ ] Firewall/inspection path required

If transit is required, describe the intended path:

_____

_____

---

5) Routing validation

- [ ] Effective routes reviewed on source and destination subnets
- [ ] User-defined routes documented
- [ ] Return path confirmed symmetrical
- [ ] No unintended default route breaks connectivity
- [ ] No asymmetric routing through inspection points
- [ ] Route table changes are tracked

Expected route behavior:

_____

Inspection or firewall hop, if any:

_____

---

6) Security controls

- [ ] NSG rules reviewed for both directions
- [ ] Firewall policy reviewed, if used
- [ ] Only intended sources can reach intended destinations
- [ ] Administrative ports are restricted
- [ ] Deny rules are documented and tested
- [ ] No broad allow rules were added for convenience

Required allow rules:

Source	Destination	Port/Protocol	Reason

Required deny rules:

Source	Destination	Port/Protocol	Reason

---

7) DNS and name resolution

- [ ] Private DNS zones reviewed
- [ ] Hostnames resolve to the intended private IPs
- [ ] Resolver path is documented
- [ ] No reliance on public endpoints for private traffic
- [ ] Split-horizon DNS behavior confirmed, if applicable

DNS dependencies:

_____

Known names or records that must work:

_____

---

8) Shared services and dependency checks

- [ ] Identity services reachable as expected
- [ ] Logging/monitoring endpoints reachable
- [ ] Certificates or key services accessible, if needed
- [ ] Storage, database, or API dependencies validated
- [ ] Service dependencies documented by subnet and port

Critical dependencies:

_____

_____

---

9) Operational risk review

- [ ] No overlap with incident-response isolation requirements
- [ ] Peering changes are part of change control
- [ ] Rollback steps are documented
- [ ] Monitoring/alerts exist for failed connectivity
- [ ] Ownership of both VNets is clear
- [ ] Peering sprawl is controlled and documented

Potential failure modes identified:

_____

_____

---

10) Validation plan

Validate from the actual source subnet to the actual destination subnet.

Test checklist

- [ ] Ping/ICMP test, if permitted by policy
- [ ] TCP connection test to required ports
- [ ] Application-level test completed
- [ ] Reverse path tested
- [ ] DNS resolution verified from both sides
- [ ] Logs confirm traffic followed the expected route

Test matrix

Test	Source	Destination	Expected result	Actual result

Validation completed by: _____

Date: _____

---

11) Go-live decision

Ready for production if all are true:

- [ ] Address spaces do not overlap

- [ ] Routing is symmetric and intentional
- [ ] Security rules are least-privilege
- [ ] DNS resolves correctly
- [ ] Transit requirements are understood and implemented
- [ ] Validation tests passed
- [ ] Rollback plan is approved

Decision

- [ ] Approved for production
- [ ] Approved with conditions
- [ ] Not approved

Conditions / follow-up items:

_____

_____

Approver: _____

Signature or confirmation: _____

---

12) Rollback plan

Rollback trigger:

_____

Rollback steps:

- _____
- _____
- _____

- _____

Backout owner: _____

Communication plan:

_____

Quick reference: common peering mistakes

- Treating peering as transitive when it is not
- Assuming peering replaces routing design
- Forgetting NSG or firewall return-path behavior
- Using public DNS names for traffic meant to stay private
- Allowing broad east-west access without subnet-level controls
- Skipping validation from the real source and destination subnets
- Expanding peering without documenting ownership and intent

Final sign-off

This design has been reviewed for connectivity, routing, segmentation, DNS, and operational readiness.

Reviewer: _____

Date: _____

Comments:

_____

_____