200 XP

What is an NVA?

7 minutes

A network virtual appliance (NVA) is a virtual appliance that consists of various layers like:

- a firewall
- a WAN optimizer
- application-delivery controllers
- routers
- load balancers
- IDS/IPS
- proxies

You can deploy NVAs chosen from providers in Azure Marketplace. Such providers include Check Point, Barracuda, Sophos, WatchGuard, and SonicWall. You can use an NVA to filter traffic inbound to a virtual network, to block malicious requests, and to block requests made from unexpected resources.

In the retail-organization example scenario, you must work with the security and network teams. You want to implement a secure environment that scrutinizes all incoming traffic and blocks unauthorized traffic from passing on to the internal network. You also want to secure both virtual-machine networking and Azure-services networking as part of your company's network-security strategy.

Your goal is to prevent unwanted or unsecured network traffic from reaching key systems.

As part of the network-security strategy, you must control the flow of traffic within your virtual network. You also must learn the role of an NVA and the benefit of using an NVA to control traffic flow through an Azure network.

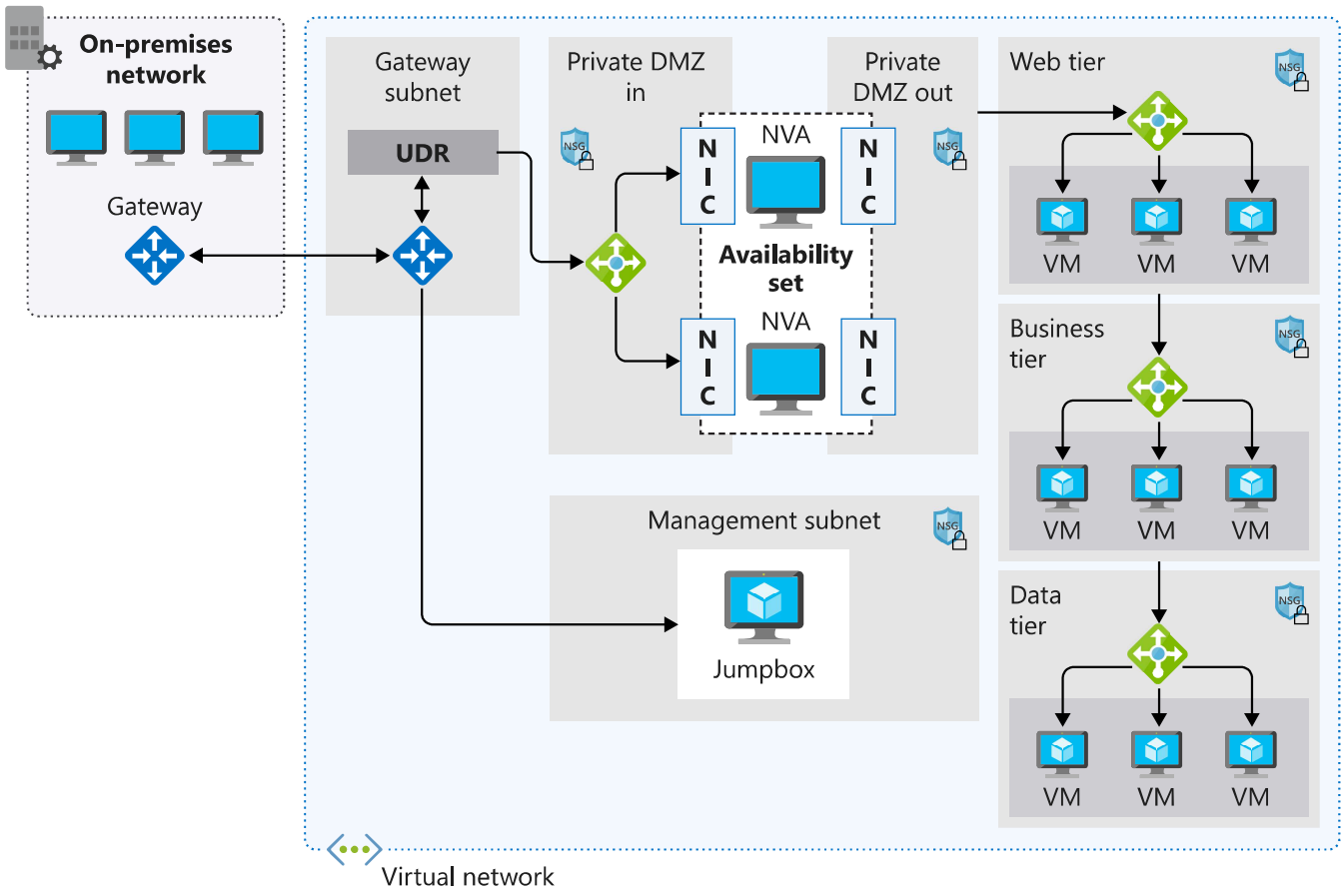
Network virtual appliance

Network virtual appliances or NVAs are virtual machines that control the flow of network traffic by controlling routing. You typically use them to manage traffic flowing from a perimeter-network environment to other networks or subnets.

An NVA often includes various protection layers like:

- a firewall
- a WAN optimizer

- application-delivery controllers
- routers
- load balancers
- proxies
- an SD-WAN edge



You can deploy firewall appliances into a virtual network in different configurations. You can put a firewall appliance in a perimeter-network subnet in the virtual network. Or if you want more control of security, implement a microsegmentation approach.

With the microsegmentation approach, you can create dedicated subnets for the firewall and then deploy web applications and other services in other subnets. All traffic is routed through the firewall and inspected by the NVAs. You enable forwarding on the virtual-appliance network interfaces to pass traffic that is accepted by the appropriate subnet.

Microsegmentation lets the firewall inspect all packets at OSI Layer 4 and, for application-aware appliances, Layer 7. When you deploy an NVA to Azure, it acts as a router that forwards requests between subnets on the virtual network.

Some NVAs require multiple network interfaces. One network interface is usually dedicated to the management network for the appliance. Additional network interfaces manage and control the traffic processing. After you've deployed the NVA, you can then configure the appliance to route the traffic through the proper interface.

User-defined routes

For most environments, the default system routes already defined by Azure are enough to get the environments up and running. But in certain cases you should create a routing table and add custom routes. Examples include:

- Access to the internet via on-premises network using forced tunneling.
- Using virtual appliances to control traffic flow.

You can define multiple routing tables in Azure. Each routing table is associated with one or more subnets. But each subnet is associated with only one routing table.

Network virtual appliances in a highly available architecture

If traffic is routed through an NVA, the NVA becomes a critical piece of your infrastructure. Any NVA failures will directly affect the ability of your services to communicate. It's important to include a highly available architecture in your NVA deployment.

There are several methods of achieving high availability when using NVAs. At the end of this module, you can find more information about using NVAs in highly available scenarios.

Check your knowledge

1. What is the main benefit of using a network virtual appliance?

- ○ To control outbound access to the internet.
- ○ To load balance incoming traffic from the internet across multiple Azure virtual machines and across two regions for DR purposes.
- ○ To control incoming traffic from the perimeter network and allow only traffic that meets security requirements to pass through.
- ○ To control who can access Azure resources from the perimeter network.

2. How might you deploy a network virtual appliance?

- ○ You can configure a Windows virtual machine and enable IP forwarding after routing tables, user-defined routes, and subnets have been updated. Or you can use a partner image from Azure Marketplace.

  Using Azure CLI, deploy a Linux virtual machine in Azure, connect

- ○ this virtual machine to your production virtual network, and assign a public IP address.
- ○ Using the Azure portal, deploy a Windows 2016 Server instance. Next, using Azure Application Gateway, add the Windows 2016 Server instance as a target endpoint.
- ○ Download a virtual appliance from Azure Marketplace and configure the appliance to connect to the production and perimeter networks.

Check your answers