AZURE NETWORK SECURITY

AUGUST 2018

Disclaimer

This document is for informational purposes only. MICROSOFT MAKE NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided “as-is.” Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this white paper may result in increased data, network, or compute resource usage, and may increase your license or subscription costs.

Executive summary

Azure network services maximize flexibility, availability, resiliency, security, and integrity by design. This white paper provides details on the networking functions of Azure. It also describes how customers can use the native security features in Azure to help protect their information assets.

The intended audiences for this white paper include:

- Technical managers, network administrators, and developers who are looking for security solutions that are available and supported in Azure.
- SMEs or business process executives who want a high-level overview of the Azure technologies and services that relate to network security in the Azure public cloud.

Contents

Executive summary 2

Overview 4

Azure network infrastructure 4

Enterprise view of Azure network components and their security issues 5

- Basic network connectivity 5
- Connectivity between virtual networks 5
- Azure DNS 7
- Application Gateway 10
- Traffic Manager 12
- Load Balancer 13

Azure network security capabilities 14

- Isolation 15
- Internet connectivity 15
- Resource connectivity 16
- Cross-premises connectivity and hybrid connectivity 16
- Traffic filtering 20
- Routing 21
- Azure DDoS Protection 21

Security controls to consider through Azure network services 22

- Network access controls 22
- Network security appliances 24
- Virtual network service endpoints 26

Network security validation through logging and auditing 26

Microsoft cloud services and network security 26

Best practices 27

Next steps 29

Resources 29

- GitHub repositories 29
- Samples 29

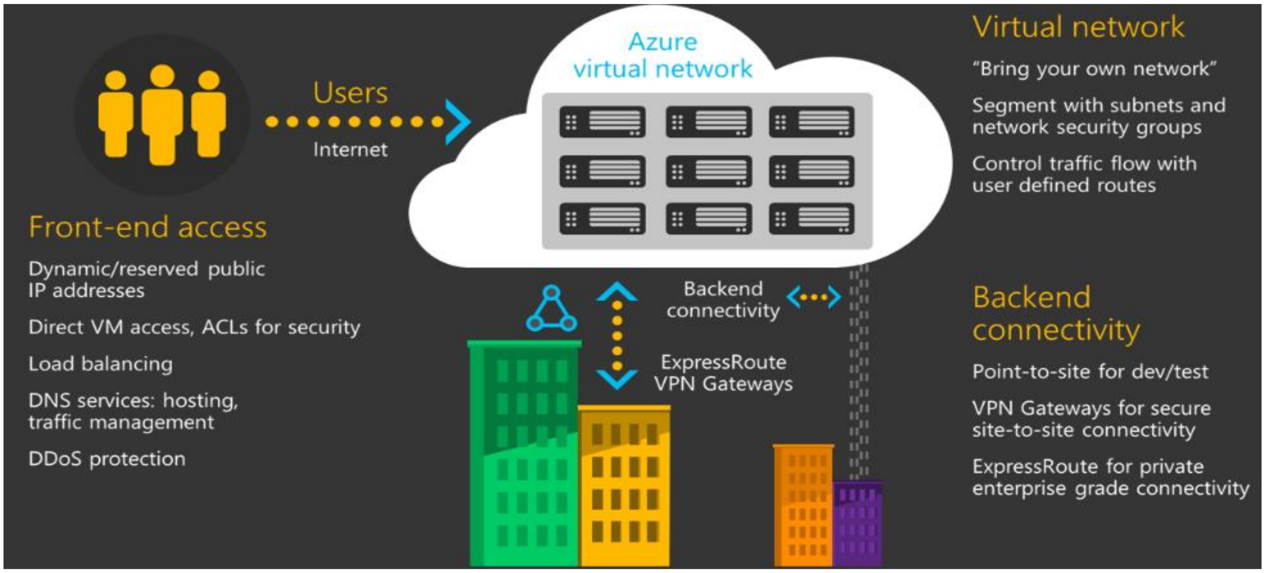
Overview

Security is paramount in the cloud. One of the best reasons to use Microsoft Azure for your applications and services is to take advantage of the security tools and capabilities in Azure. These tools and capabilities can help you create secure solutions on the Azure platform.

Azure provides confidentiality, integrity, and availability of customer data, while also enabling transparent accountability. This paper describes the network controls that you can configure to enhance the security of the solutions that you deploy in Azure. If you're interested in what Microsoft does to secure the network fabric of the Azure platform itself, see the section about Azure security in the Microsoft Trust Center.

Azure network infrastructure

Microsoft Azure includes a robust network infrastructure to support your application and service connectivity requirements. Network connectivity is possible between resources located in Azure, between on-premises and Azure-hosted resources, and to and from the internet and Azure. The following diagram illustrates this infrastructure:


Users
Internet
Azure virtual network
Front-end access
Dynamic/reserved public IP addresses
Direct VM access, ACLs for security
Load balancing
DNS services: hosting, traffic management
DDoS protection
Backend connectivity
ExpressRoute VPN Gateways
Virtual network
"Bring your own network"
Segment with subnets and network security groups
Control traffic flow with user defined routes
Backend connectivity
Point-to-site for dev/test
VPN Gateways for secure site-to-site connectivity
ExpressRoute for private enterprise grade connectivity

The Azure network infrastructure enables you to securely connect Azure resources to each other by using *virtual networks*. A virtual network is a representation of your own network in the cloud. A virtual network is a logical isolation of the Azure cloud network that's dedicated to your subscription.

Security aspects of Azure network components for the enterprise

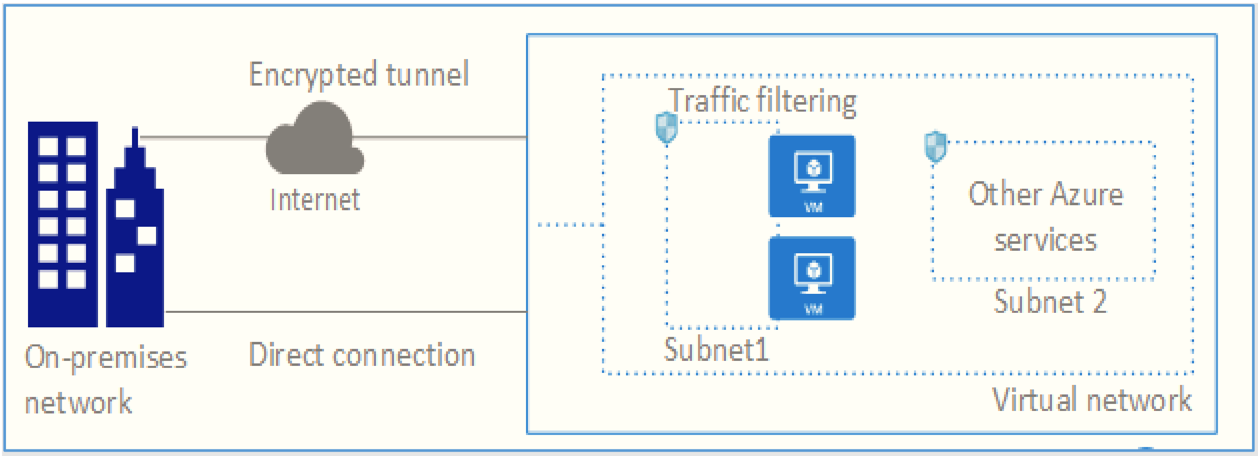
An enterprise view requires capturing and specifying organizational requirements. Azure has many components that can help enterprises meet network security requirements. The following sections describe these network components and the security issues related to them.

Note:
This paper doesn't cover all aspects of Azure network services. It discusses only the services and features that are pivotal in planning and designing a secure network infrastructure for services and applications that you deploy in Azure.

Basic network connectivity

The Azure Virtual Network service enables you to securely connect Azure resources to each other by using virtual networks. You can also connect virtual networks to each other and to your on-premises networks by using site-to-site virtual private networks (VPNs) and dedicated WAN links. Virtual network isolation helps enterprise customers protect their environments from unauthorized or unwanted access.

The following figure shows how the Virtual Network service works:



You use virtual machines (VMs) to host servers in Azure. Those VMs connect to an Azure virtual network. Azure virtual networks are like the virtual networks that you use on-premises with your own virtualization platform solutions, such as Microsoft Hyper-V or VMware.

Connectivity between virtual networks

If connect virtual networks to each other resources that are connected to either network can communicate with each other.

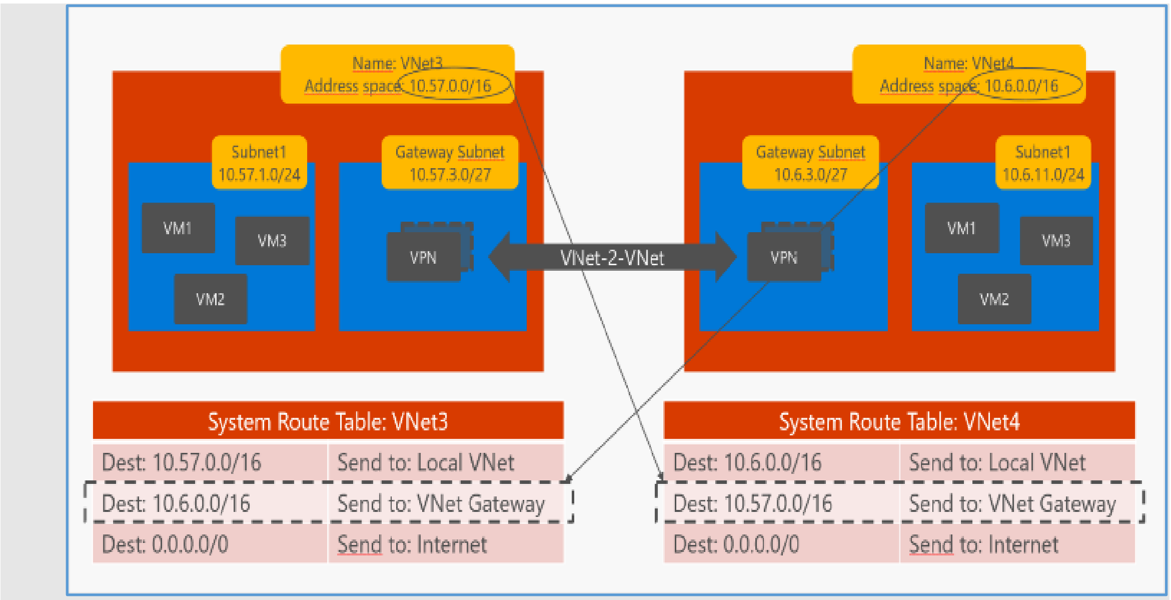
For example, after you create your virtual networks, your lines of business might need to exchange data, or you might need to enable IP connectivity between the virtual networks. There are three options for communication within the Azure cloud platform:

- Network to network via VPN
- Network to network via Azure ExpressRoute
- Network to network via (virtual network peering) and virtual network transit

Network-to-network connection via VPN

A network-to-network connection enables resources to connect to a different Azure virtual network within the same region or from other regions. Unlike peering, bandwidth is limited between virtual networks because traffic must flow through an Azure VPN gateway. These cross-region virtual networks use a site-to-site VPN link for the connection.

The following figure illustrates this connection:



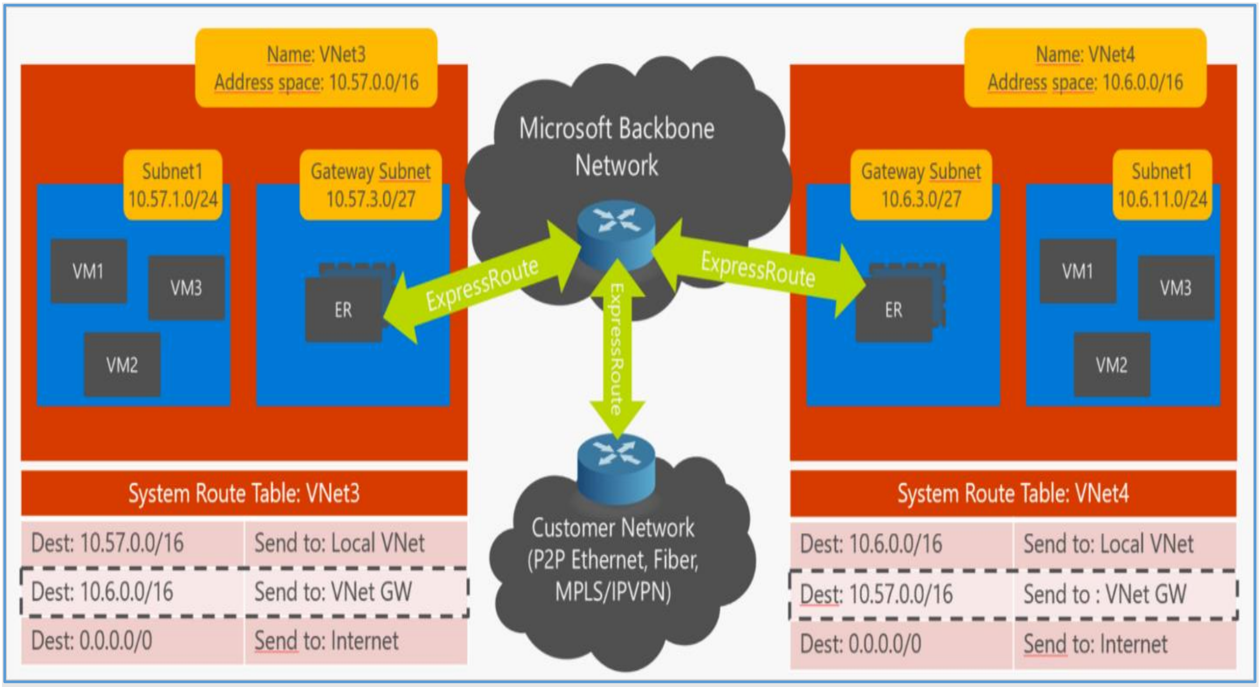
System Route Table: VNet3	
Dest: 10.57.0.0/16	Send to: Local VNet
Dest: 10.6.0.0/16	Send to: VNet Gateway
Dest: 0.0.0.0/0	Send to: Internet

System Route Table: VNet4	
Dest: 10.6.0.0/16	Send to: Local VNet
Dest: 10.57.0.0/16	Send to: VNet Gateway
Dest: 0.0.0.0/0	Send to: Internet

To learn more about network-to-network connections, read Configure a VNet-to-VNet connection.

Network-to-network connection via ExpressRoute

If you link two virtual networks to the same ExpressRoute circuit, this is what the route table looks like:



System Route Table: VNet3

Dest: 10.57.0.0/16	Send to: Local VNet
Dest: 10.6.0.0/16	Send to: VNet GW
Dest: 0.0.0.0/0	Send to: Internet

System Route Table: VNet4

Dest: 10.6.0.0/16	Send to: Local VNet
Dest: 10.57.0.0/16	Send to : VNet GW
Dest: 0.0.0.0/0	Send to: Internet

The virtual networks can communicate with each other without going outside the Microsoft Enterprise Edge (MSEE) router. This means you can use the worldwide Microsoft backbone to connect multiple virtual networks together. That network-to-network traffic is *free of charge*, as long as you can connect these virtual networks to the same ExpressRoute circuit.

Network-to-network connection via virtual network peering

Virtual network peering enables resources connected to different Azure virtual networks within the same Azure region to communicate directly with each other without needing to loop back through the internet. Avoiding the internet represents a security advantage. There are also performance advantages in that the bandwidth and latency across the virtual networks is the same as if the resources were connected to the same virtual network.

You can peer your virtual networks from across the world. Global virtual network peering seamlessly connects your virtual networks across Azure regions. It can be configured in less than a minute. After the virtual networks are peered, they appear as one global virtual network from a connectivity perspective. Resources within the peered virtual networks can directly communicate with each other via the Microsoft global network. Global virtual network peering enables data replication across your virtual networks so that you can copy data from one location to another for better disaster recovery.

To learn more about peering, read Virtual network peering.

Azure DNS

The Domain Name System, or DNS, is responsible for translating (or resolving) a service name to its IP address. Azure DNS is a hosting service for DNS domains. It provides name resolution by using the Microsoft Azure infrastructure. In addition to internet-facing DNS domains, Azure DNS supports private DNS domains as a preview feature.

DNS domains in Azure DNS are hosted on the Azure global network of DNS name servers. Azure DNS uses Anycast networking so that each DNS query is answered by the closest available DNS server. This provides both fast performance and high availability for your domain.

You can use the Azure DNS service to manage DNS records for your Azure services and to provide DNS for your external resources. Azure DNS is integrated in the Azure portal and uses the same credentials, billing, and support contract as your other Azure services.

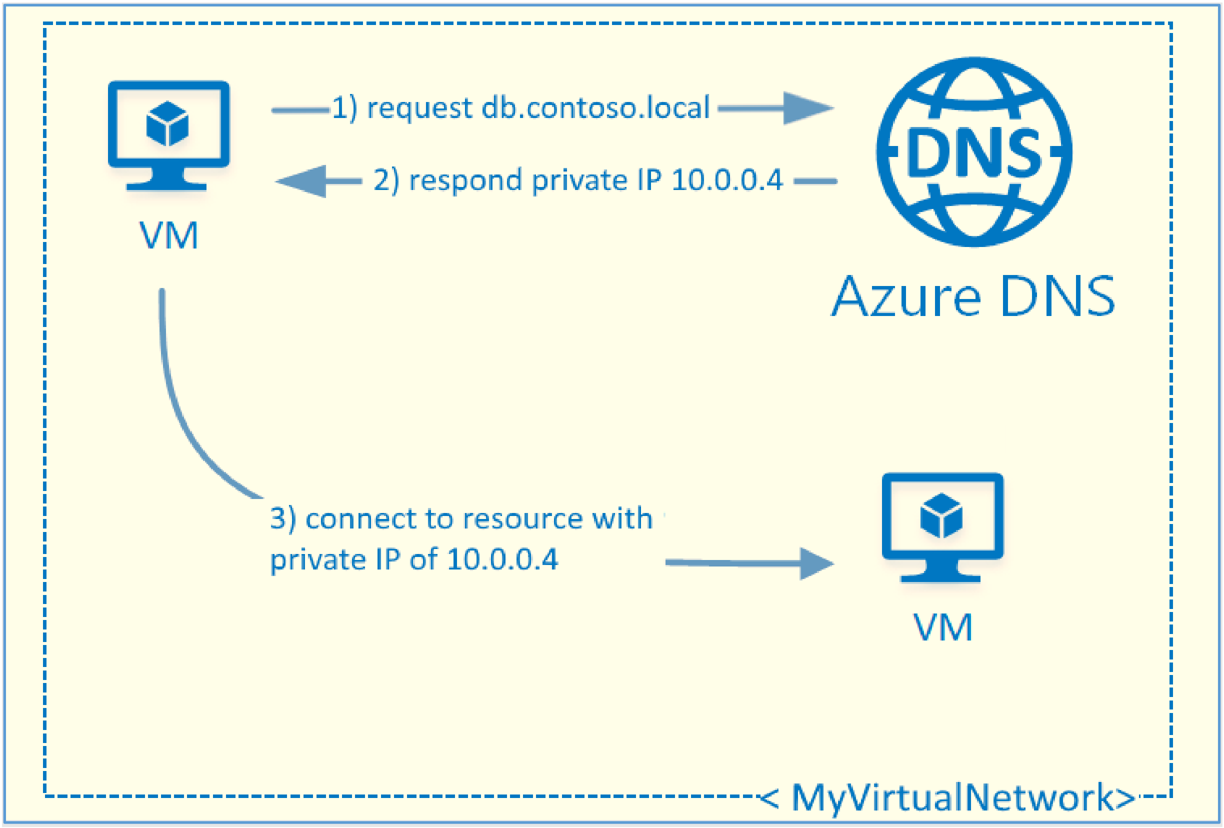
You can specify DNS server IP addresses in the virtual network settings. The setting is applied as the default DNS server or servers for all VMs in the virtual network. You can change the DNS server list for your virtual network at any time. If you change your DNS server list, you'll need to restart each VM in your virtual network so it can pick up the new DNS server. You can set DNS servers per VM or cloud service to override the default network settings.

However, we recommend that you:

- Use network-wide DNS as much as possible.
- Make sure that all VMs and Azure Cloud Services role instances deployed within a virtual network can connect to the internet.

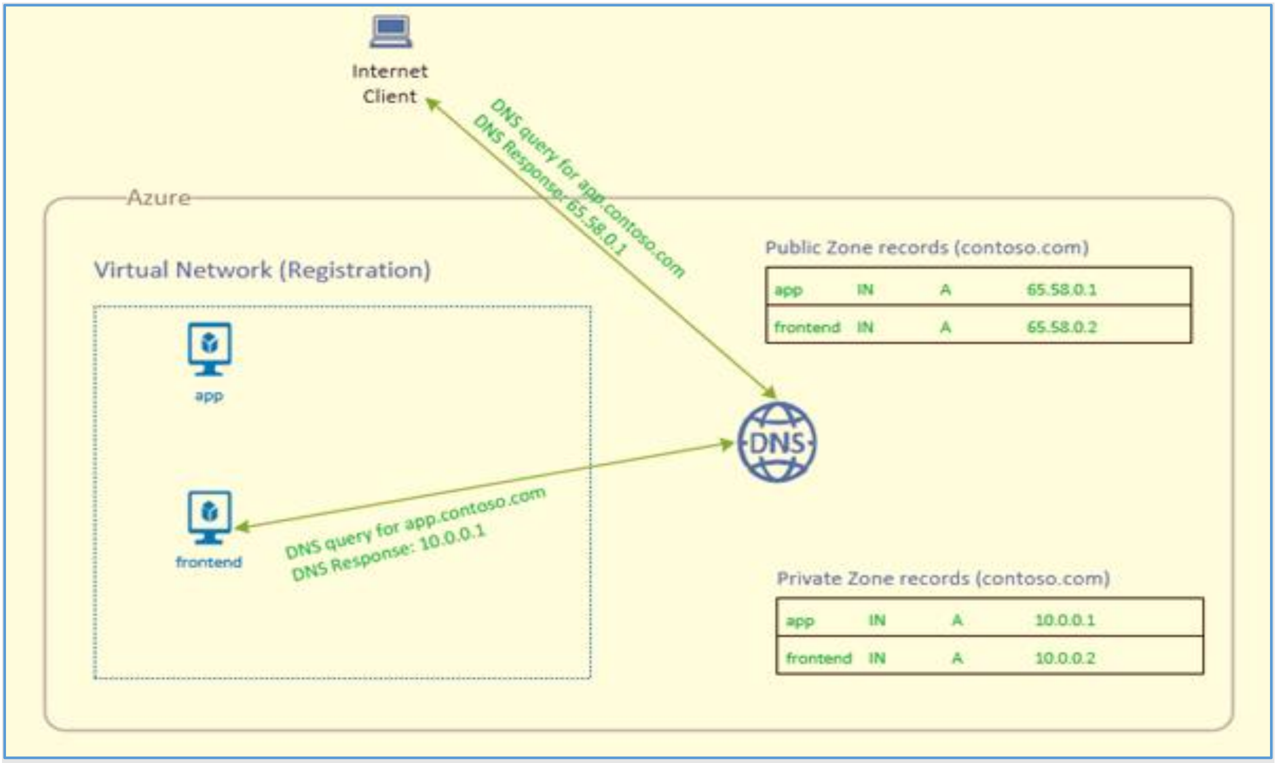
The Azure DNS service is based on Azure Resource Manager. As such, it benefits from Resource Manager features such as role-based access control, audit logs, and resource locking. You can manage your domains and records via the Azure portal, Azure PowerShell cmdlets, and the cross-platform Azure CLI. Applications that require automatic DNS management can integrate with the service via the REST API and SDKs.

The following image shows how Azure DNS works with VMs in a virtual network:


VM
1) request db.contoso.local
2) respond private IP 10.0.0.4
DNS
Azure DNS
3) connect to resource with private IP of 10.0.0.4
VM
< MyVirtualNetwork>

Azure DNS provides a reliable, secure DNS service to manage and resolve domain names in a virtual network without the need to add a custom DNS solution. Private DNS zones enable you to use your own custom domain names rather than the Azure-provided names. Using custom domain names helps you tailor your virtual network architecture to best suit your organization's needs. It provides name resolution for VMs within a virtual network and between virtual networks.

Additionally, you can configure split DNS infrastructures, as shown in the following figure. A private and a public DNS zone can then share the same name. You can use a split DNS infrastructure to validate your workloads in a local test environment, before you put them in production. Because name resolution is confined to configured virtual networks, you can prevent DNS exfiltration.


Internet Client
DNS query for app.contoso.com
DNS Response: 65.58.0.1
Azure
Virtual Network (Registration)
app
frontend
DNS
DNS query for app.contoso.com
DNS Response: 10.0.0.1
Public Zone records (contoso.com)
Private Zone records (contoso.com)

app	IN	A	65.58.0.1
frontend	IN	A	65.58.0.2

app	IN	A	10.0.0.1
frontend	IN	A	10.0.0.2

When you designate a virtual network as a Registration virtual network, Azure dynamically registers DNS and records in the private zone for the all VMs in the virtual network.

Azure DNS now provides metrics via Azure Monitor so you can configure and receive alerts. For details, see Azure DNS metrics and alerts.

Application Gateway

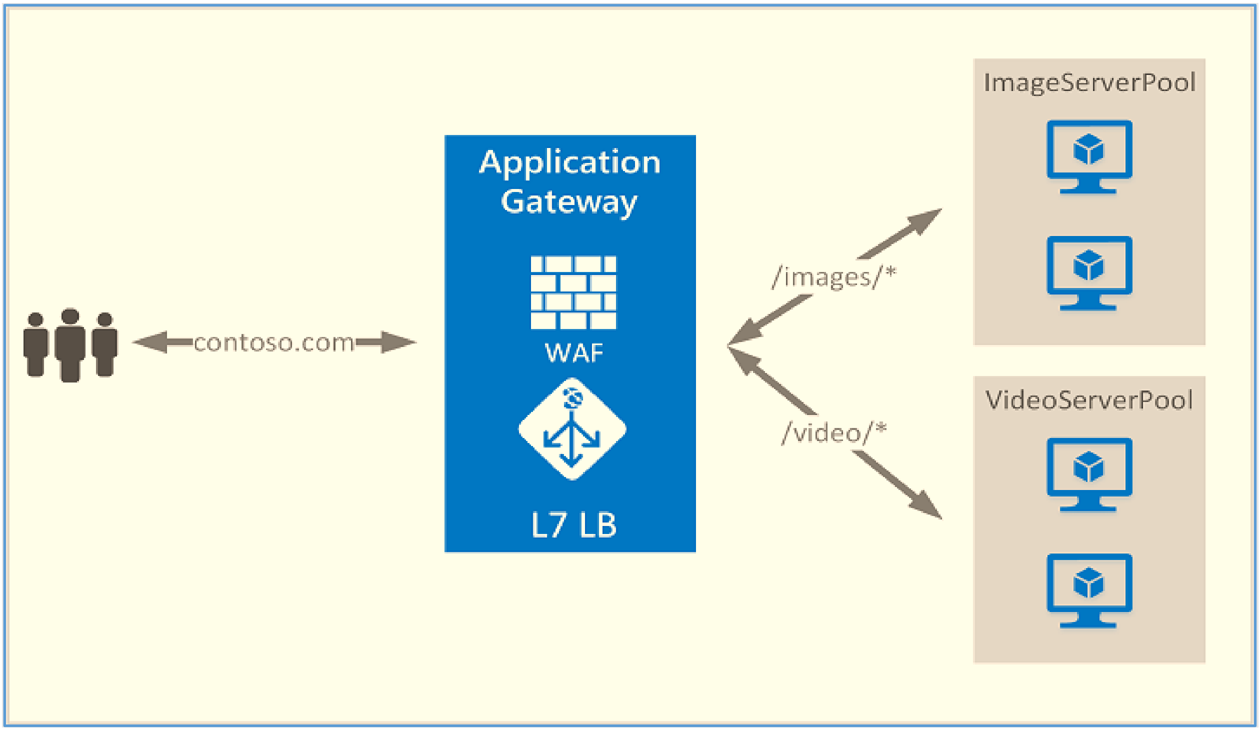
Microsoft Azure Application Gateway is a dedicated virtual appliance that provides an application delivery controller (ADC) as a service. Application Gateway enables you to optimize web farm performance and availability by offloading CPU-intensive SSL termination to the application gateway (SSL offloading). It also provides other Layer 7 routing capabilities, including:

- Round-robin distribution of incoming traffic.
- Cookie-based session affinity.
- URL path-based routing.
- The ability to host multiple websites behind a single application gateway.

In Application Gateway, enhanced SSL policy support for cipher suite selection and priority ordering increases security and simplifies your compliance. The ability to redirect incoming requests from HTTP to HTTPS ensures that all website traffic is encrypted.

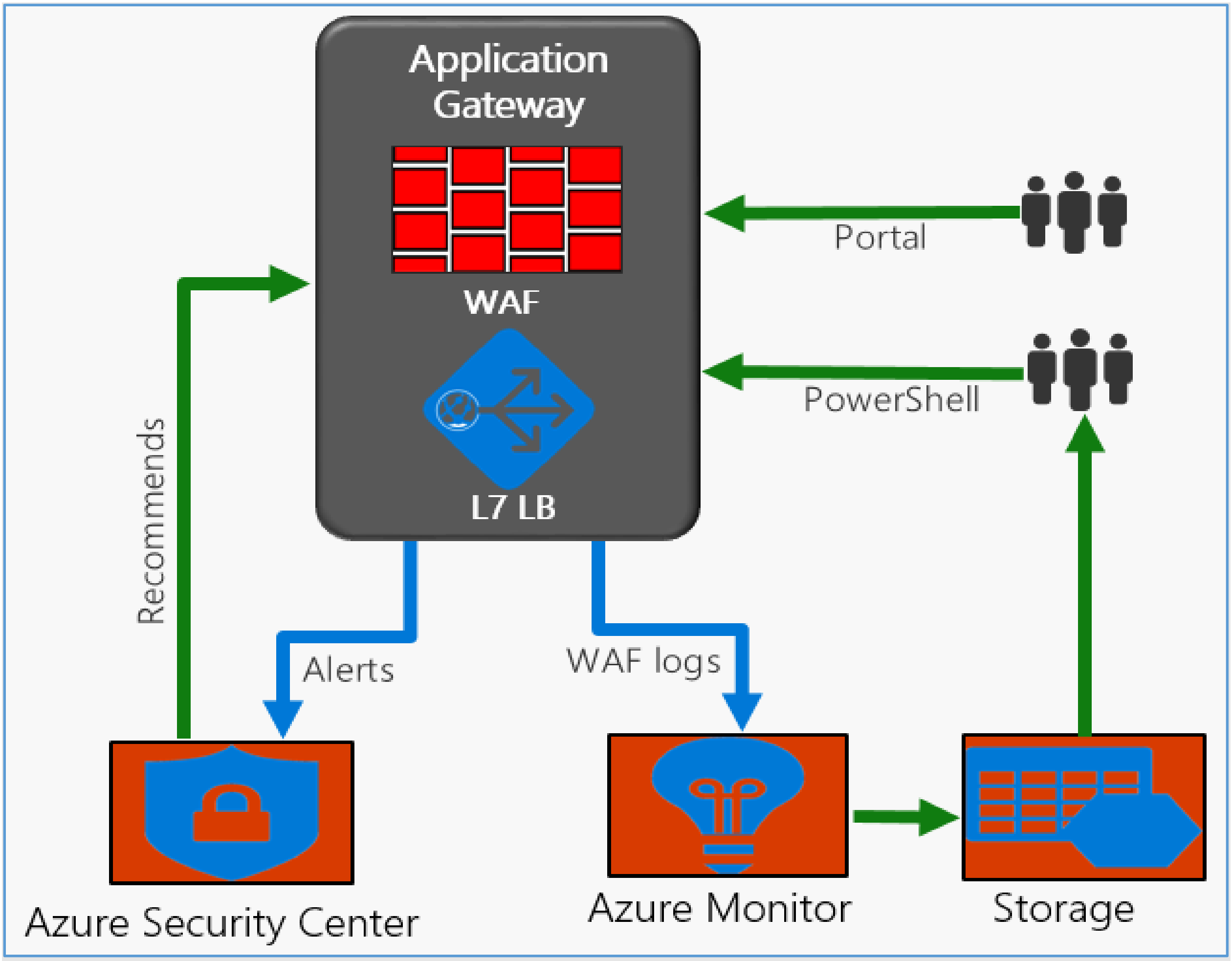
Application Gateway includes a web application firewall (WAF). It provides protection to web applications from common web vulnerabilities and exploits. You can configure Application Gateway as an internet-facing gateway, an internal-only gateway, or a combination of both.

The following figure shows how Application Gateway works:



You can run the Application Gateway WAF in detection or prevention mode. A common use case is for administrators to run WAF in detection mode to observe traffic for malicious patterns. If potential exploits are detected, turning to prevention mode blocks suspicious incoming traffic.

In addition, the Application Gateway WAF helps you monitor web applications for attacks by using a real-time WAF log. As shown in the following diagram, the log is integrated with Azure Monitor and Azure Security Center, so you can track WAF alerts and easily monitor trends.



The JSON-formatted log goes directly to your storage account. You have full control over these logs and can apply your own retention policies.

Traffic Manager

You can use Azure Traffic Manager to control the distribution of user traffic for service endpoints in different datacenters. An endpoint is any internet-facing service that's hosted inside or outside Azure. Service endpoints that Traffic Manager supports include Azure Virtual Machines, the Web Apps feature of Azure App Service, and Cloud Services. You can also use Traffic Manager with external, non-Azure endpoints.

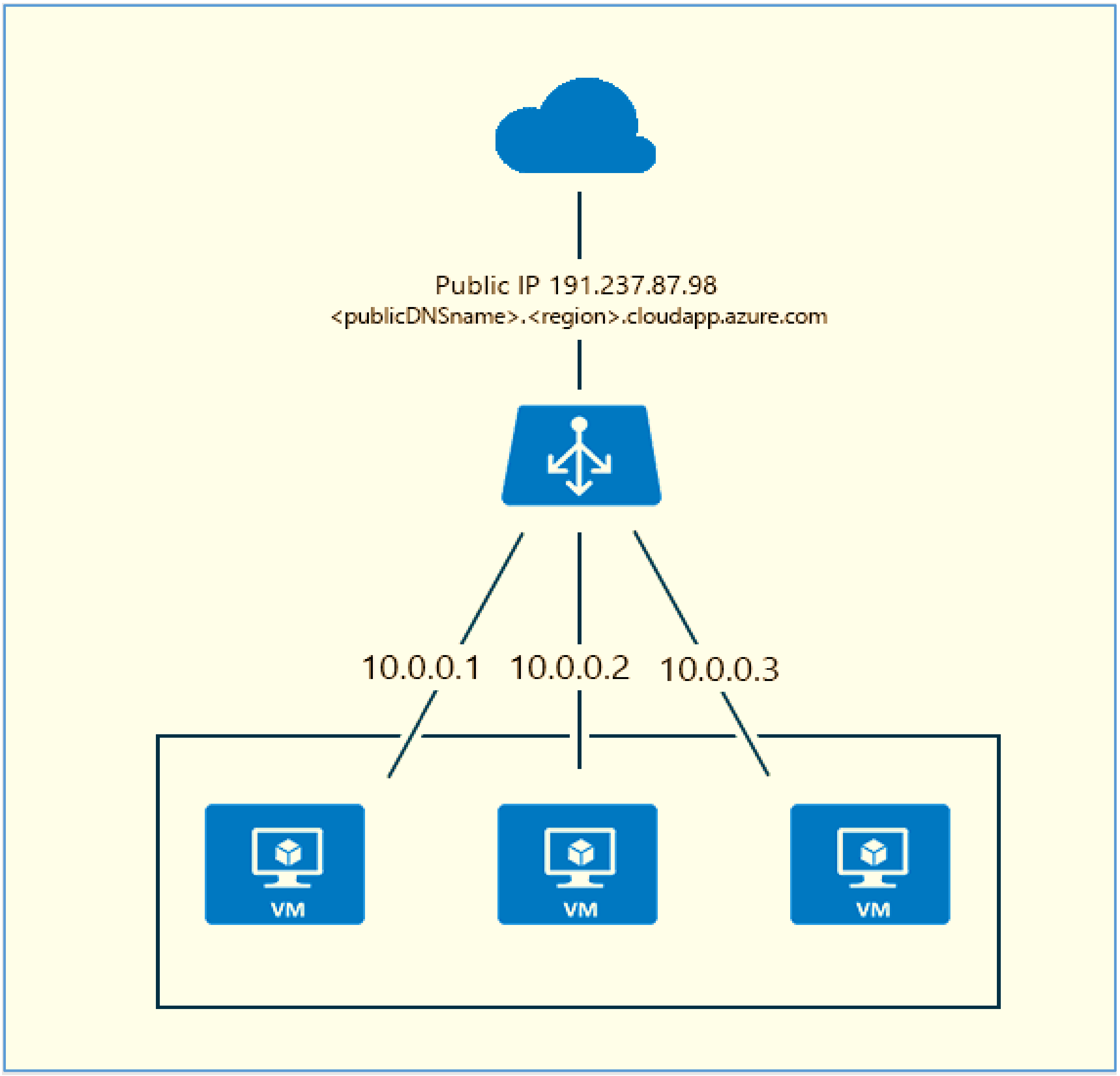
Traffic Manager uses DNS to direct client requests to the most appropriate endpoint based on a traffic-routing method and the health of the endpoints. Traffic Manager provides a range of traffic-routing methods to suit different application needs, continuous monitoring of endpoint health, and automatic failover. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

When a client tries to connect to a service, it must first resolve the DNS name of the service to an IP address. The client then connects to that IP address to access the service. The client directly connects to the endpoint that Traffic Manager selects. Traffic Manager is not a proxy or a gateway. It doesn't see the traffic passing between the client and the service.

The Real User Measurements and Traffic Manager Traffic View features in Traffic Manager help you understand where your users are located, the traffic volume from these regions, the representative user latency, and specific traffic patterns. With this information, you can better manage your capacity and global expansion so your users get a great network experience.

Load Balancer

Azure Load Balancer delivers high availability and network performance to your applications. It's a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic among healthy instances of services defined in a load-balanced set. The following diagram shows how Load Balancer works with virtual machines:



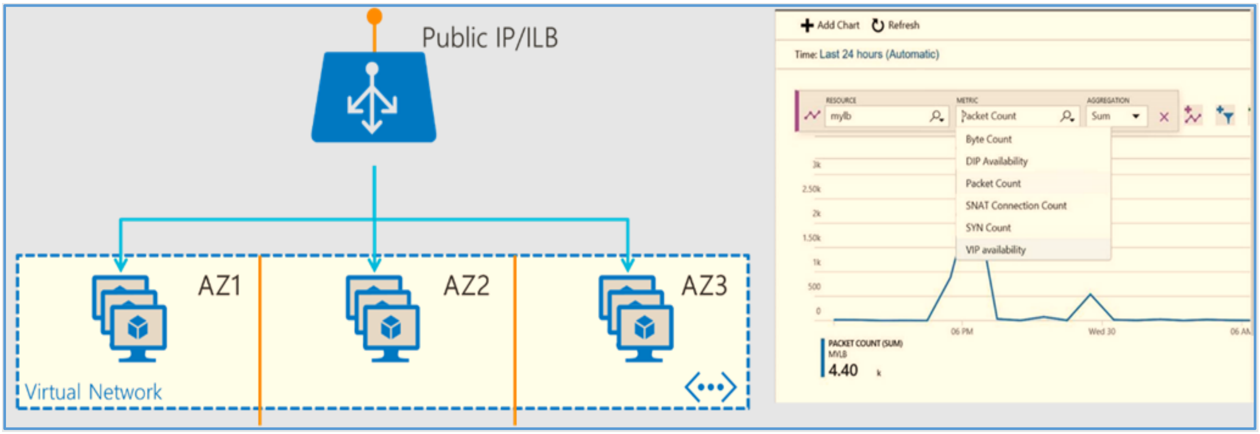
Azure Load Balancer can be configured to:

- Load balance incoming internet traffic to virtual machines. This configuration is known as internet-facing load balancing.
- Load balance traffic between virtual machines in a virtual network, between virtual machines in cloud services, or between on-premises computers and virtual machines in a cross-premises virtual network. This configuration is known as internal load balancing.
- Forward external traffic to a specific virtual machine.

All resources in the cloud need a public IP address to be reachable from the internet. The cloud infrastructure in Azure uses private IP addresses (RFC 1918) for its resources. Azure uses network address translation (NAT) with public IP addresses to communicate to the internet.

Azure Load Balancer enables you to load balance 1,000 VMs. Load Balancer takes advantage of regional Anycast IP addresses to quickly load balance external or internal traffic to help ensure availability in the presence of failures. You can load balance across all your VMs deployed in Availability Zones—enabling scenarios with zonal front ends and cross-zone load balancing for the back end.

You also get extensive health and diagnostic metrics. These metrics include continuous in-band measurements for data plane health, per-endpoint health probe status, and counters for packets, bytes, connection attempts, and outbound connections. The following example shows how Load Balancer supports Availability Zones and provides diagnostics:



Time: Last 24 hours (Automatic)

RESOURCE: mylb
METRIC: Packet Count
AGGREGATION: Sum

Azure network security capabilities

Protecting the security and confidentiality of network traffic, whether in the cloud or on-premises, is a critical part of any data protection strategy. Securing the network infrastructure helps prevent attacks, block malware, and protect your data from unauthorized access, interrupted access, or loss.

The following sections describe Azure network capabilities from a security perspective.

Isolation

Virtual networks are isolated from one another through Network Virtualization using Generic Routing Encapsulation (NVGRE). NVGRE enables encapsulation of virtual networks from each other, adding a layer of isolation on its security fabric. You can create separate virtual networks for development, testing, and production that use the same CIDR address blocks. Conversely, you can create multiple virtual networks that use different CIDR address blocks and connect networks together. You can segment a virtual network into multiple subnets.

You can implement multiple virtual networks within each Azure subscription and Azure region. For each virtual network, you can:

- Specify a custom private IP address space by using public and private (RFC 1918) addresses. Azure assigns this IP address to resources that are connected to the virtual network.
- Segment the virtual network into one or more subnets, and allocate a portion of the virtual network address space to each subnet. Consider creating a virtual network for each type of workload or security zone you're hosting.
- Use Azure-provided name resolution, or specify your own DNS server for use by resources connected to a virtual network. To learn more, read Name resolution for resource in Azure virtual networks.

Internet connectivity

For Azure Virtual Machines and Cloud Services, all role instances connected to a virtual network have outbound access to the internet, by default. You can also enable inbound access to specific resources, as needed.

The Azure infrastructure translates the private IP address of the resource to a public IP address by using source network address translation (SNAT). You can change the default connectivity by implementing custom routing and traffic filtering. To learn more, read Understanding outbound connections in Azure.

To communicate inbound to Azure resources from the internet, or to communicate outbound to the internet without SNAT, a resource must be assigned a public IP address.

What about outbound connectivity to the internet through a predictable IP address? For example, a virtual machine can communicate outbound to the internet without a public IP address assigned to it, but Azure translates its address to an unpredictable public address. Assigning a public IP address to a resource enables you to know which IP address is used for the outbound connection.

To learn more about public IP addresses, read Create, change, or delete a public IP address.

Deploy perimeter networks for security zoning and attack prevention

A perimeter network (also known as DMZ, demilitarized zone, and screened subnet) is a physical or logical network segment that provides an additional layer of security between your assets and the internet. You place specialized network access control devices on the edge of the perimeter network so that only desired traffic is allowed past the network security device and into your Azure virtual network.

Perimeter networks are useful because you can focus your network access control management, monitoring, logging, and reporting on the devices at the edge of your Azure virtual network. Here you would typically enable DDoS prevention, an intrusion detection system (IDS) or intrusion prevention system (IPS), firewall rules and policies, web filtering, network antimalware, and more. The network security devices sit between the internet and your Azure virtual network and have an interface on both networks.

Resource connectivity

You can connect Azure resources—such as cloud services, VMs, the App Service Environment for PowerApps, and virtual machine scale sets—to the same virtual network. The resources can connect to each other by using their private IP addresses, even if they're in different subnets. Azure provides default routing between subnets, virtual networks, and on-premises networks, so you don't have to configure and manage routes.

VMs connect to a subnet within a virtual network through a network interface card (NIC). To learn more about NICs, read Create, change, or delete a network interface.

You can use virtual network service endpoints to create network rules that allow traffic only from selected virtual networks and subnets. This technique creates a secure network boundary for your data. You can also grant access to on-premises networks and other trusted internet traffic by using network rules based in IP address ranges.

You manage network rules by using the Azure portal, PowerShell, Azure CLI 2.0, and Azure Resource Manager templates. Connecting resources via service endpoints is a security advantage, because these resources connect with other Azure resources over the Azure network fabric instead of looping back into Azure through the internet.

Cross-premises and hybrid connectivity

You can connect virtual networks to on-premises networks through private network connections between your network and Azure, or through a site-to-site VPN connection over the internet.

Azure supports dedicated WAN link connectivity to your on-premises network and an Azure virtual network with ExpressRoute. The link between Azure and your site uses a dedicated connection that does not go over the public internet.

Security recommendations for cross-premises connectivity include:

- **Enable forced tunneling to avoid security breaches and attacks**: Connections destined for the internet and connections destined for corporate resources should go through a VPN tunnel. Connections to the internet are then forced through the corporate network security devices. That wouldn't be the case if the VPN client connected to the internet outside the VPN tunnel.

  The default routes for an Azure virtual network allow virtual machines to initiate traffic to the internet. This too can represent a security risk, because these outbound connections might increase the attack surface of a virtual machine and be used by attackers. For this reason, we recommend that you enable forced tunneling on your virtual machines when you have cross-premises connectivity between your Azure virtual network and your on-premises network.

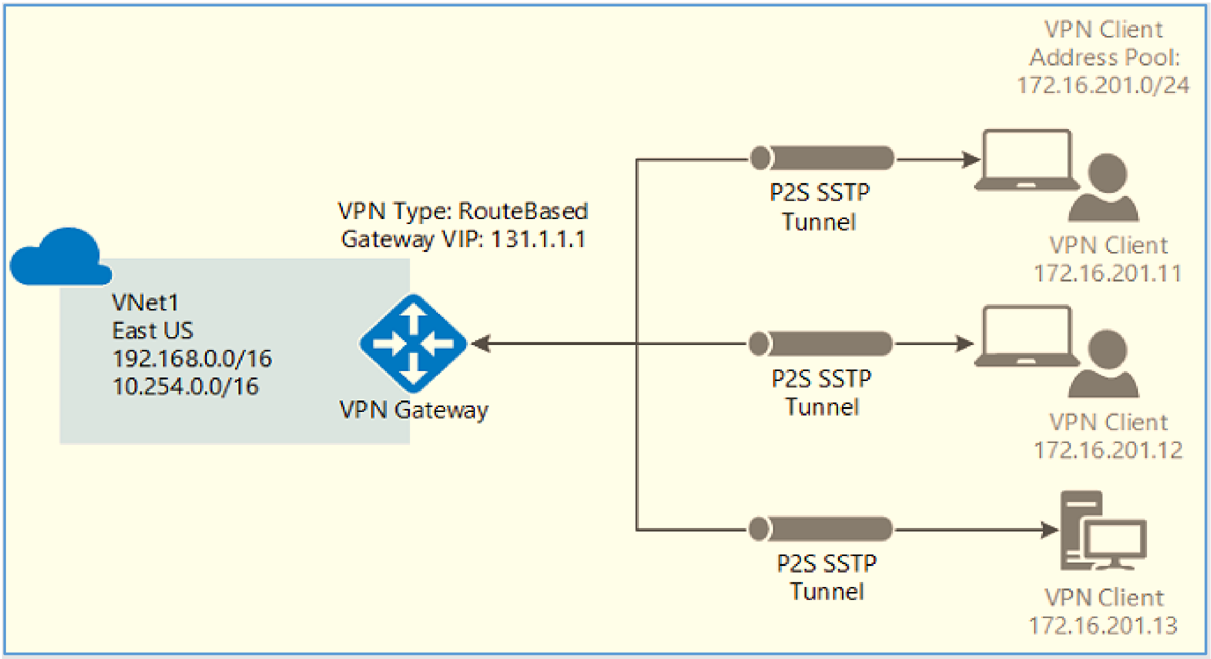
- **Disable RDP/SSH access to Azure virtual machines to avoid brute-force attacks**: It's possible to reach Azure virtual machines by using the Remote Desktop Protocol (RDP) and Secure Shell (SSH) protocols. These protocols make it possible to manage virtual machines from remote locations and are standard in datacenter computing.

  The potential security problem with using these protocols over the internet is that attackers can use brute-force techniques to gain access to an Azure virtual machine. After the attackers gain access, they can use your virtual machine as a launch point for compromising other machines on your Azure virtual network or even attack networked devices outside Azure. Because of this, we recommend that you disable direct RDP and SSH access to your Azure virtual machines from the internet.

You can connect your on-premises network to a virtual network by using any combination of the following options. To learn more about these options, see the Connection topology diagrams.

Point-to-site VPN

A point-to-site (P2S) configuration lets you create a secure connection from an individual client computer to a virtual network. P2S is a VPN connection over Secure Socket Tunneling Protocol (SSTP), as shown in the following diagram:



Point-to-site connections are useful when you want to connect to your virtual network from a remote location, such as from home or a conference center. They're also useful when you have only a few clients that need to connect to a virtual network.

P2S connections don't require a local VPN device or a public-facing IP address (local to the VPN client). You establish the VPN connection from the client computer. We don't recommend P2S VPN as a way to connect to Azure if you need a persistent connection from many on-premises devices and computers to your Azure network.

For more information about point-to-site connections, see the point-to-site FAQ.

Site-to-site VPN

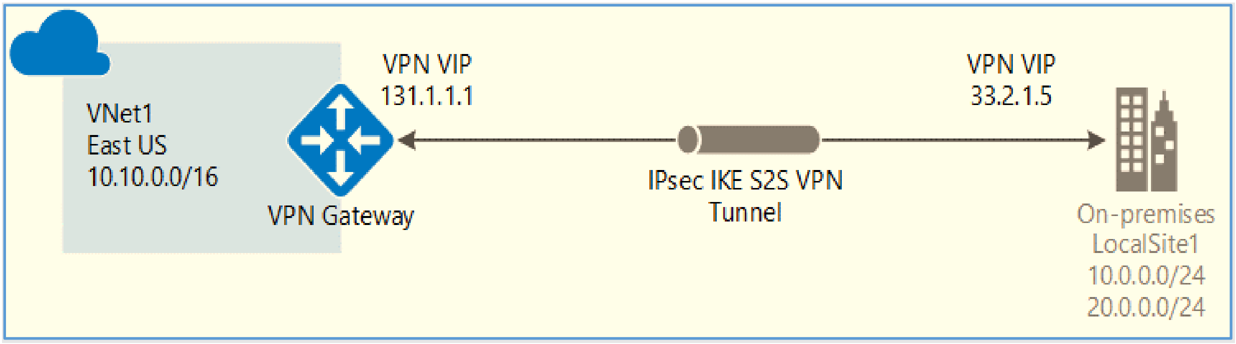
You use a site-to-site VPN to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.

Site-to-site VPN is a trusted, reliable, and established technology. Traffic within the tunnel does traverse the internet. Site-to-site VPN bandwidth tops out at about 1.25 Gbps.

IPsec VPN site-to-site tunnels offer the following security advantages :

- The internal IP addresses of both local and remote networks and nodes remain hidden from each other and from external users.
- The entire communication between the source and destination sites remains encrypted, so chances of information theft are extremely low.
- You no longer need to buy dedicated, expensive lease lines from one site to another because the public internet is used to transmit data.

Here's an example of how an IPsec VPN site-to-site tunnel works:



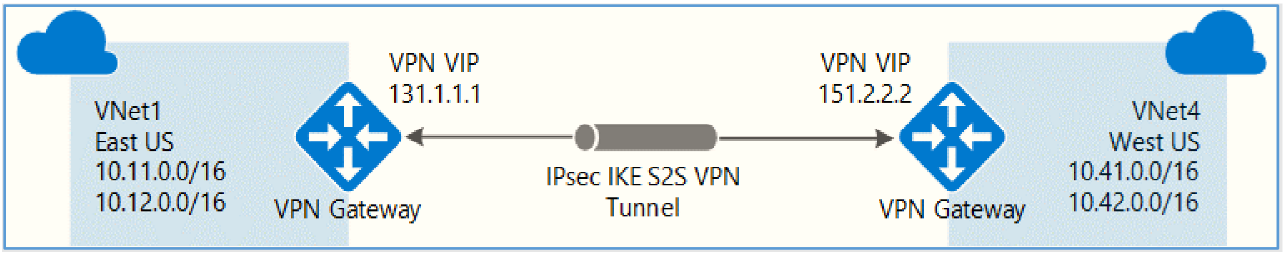
Network-to-network connections (IPsec/IKE VPN tunnel)

Connecting a virtual network to another virtual network is similar to connecting a virtual network to an on-premises site location. Both connectivity types use a VPN gateway to provide a secure tunnel through IPsec/IKE. You can even combine network-to-network communication with multiple-site connection configurations. This lets you establish network topologies that combine cross-premises connectivity with connectivity between virtual networks.

The virtual networks that you connect can be:

- In the same or different regions.
- In the same or different subscriptions.
- In the same or different deployment models.

Here's an example of how a network-to-network connection through an IPsec/IKE VPN site-to-site tunnel works:

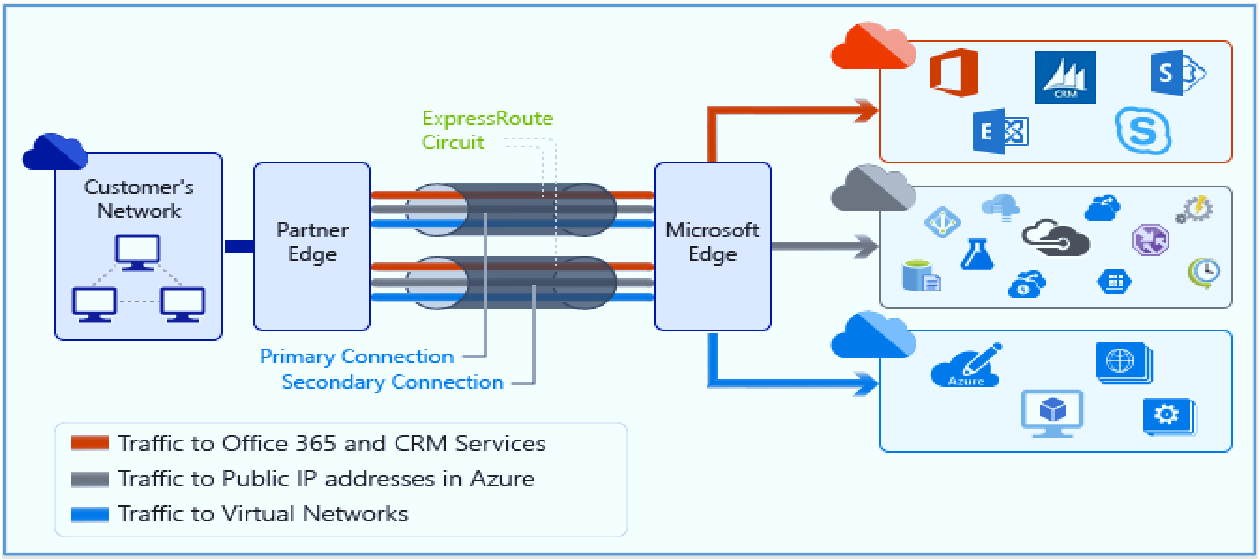


Azure ExpressRoute

You can use Azure ExpressRoute to extend your on-premises networks into Azure virtual networks over a dedicated WAN link that's facilitated by a connectivity provider.

ExpressRoute connections don't go over the public internet. ExpressRoute connections offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the internet.

The following diagram shows how ExpressRoute connects an on-premises network to virtual networks:



Traffic filtering

Network traffic from VM and Cloud Services role instances can be filtered inbound and outbound by source IP address and port, destination IP address and port, and protocol.

You can filter network traffic between subnets by using either or both of the following options:

- **Network security groups (NSGs)**: Each NSG can contain multiple inbound and outbound security rules that you can use to filter traffic by source and destination IP address, port, and protocol. You can apply an NSG to each NIC in a VM. You can also apply an NSG to the subnet that a NIC, or another Azure resource, is connected to.

  Previously, you could assign an NSG to a subnet or to a standalone virtual machine NIC, but not directly to a scale set. NSGs can now be applied directly to scale sets. You can enforce and control network traffic rules through NSGs to help secure your scale sets in Azure. This capability allows finer control over your infrastructure.

  To learn more about NSGs, read Network security.

- **Virtual network appliances**: A virtual network appliance is a VM running software that performs a network function, such as a firewall, on a virtual network. View a list of available virtual network appliances in the Azure Marketplace. Some virtual network appliances provide WAN optimization and other network traffic functions and are typically used with user-defined or BGP routes. You can also use a virtual network appliance to filter traffic between virtual networks.

Routing

The ability to control routing behavior on your Azure virtual networks is a critical network security and access control capability. If routing is configured incorrectly, applications and services hosted on your virtual machine might connect to unauthorized devices, including systems owned and operated by potential attackers.

Azure network services support the ability to customize the routing behavior for network traffic on your Azure virtual networks. You can then alter the default routing table entries in your Azure virtual network. Control of routing behavior helps you make sure that all traffic from a certain device or group of devices enters or leaves your virtual network through a specific location.

Azure creates route tables that enable resources connected to any subnet in any virtual network to communicate with each other, by default. You can implement user-defined routes or BGP routes to override the default routes that Azure creates.

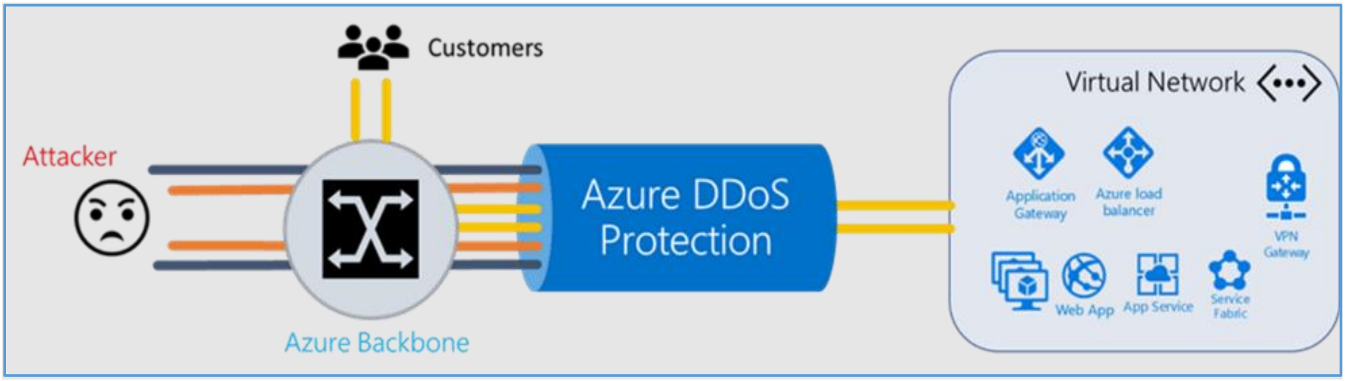
For example, you might have a virtual network security appliance on your Azure virtual network. You want to make sure that all traffic to and from your Azure virtual network goes through that virtual network security appliance. You can do this by configuring user-defined routes in Azure. You can create custom route tables with routes that control where traffic is routed to for each subnet.

You can override the Azure default routing by configuring your own routes or using BGP routes through a network gateway. If you connect your virtual network to your on-premises network by using an Azure VPN Gateway or ExpressRoute connection, you can propagate BGP routes to your virtual networks.

Azure DDoS Protection

Azure DDoS Protection is a Standard service that provides enhanced DDoS mitigation capabilities for your application and resources deployed in virtual networks. You can enable DDoS Protection with no application or resource changes so that your services benefit from the same DDoS technologies that Microsoft uses to protect itself. Dedicated monitoring, along with machine learning that automatically configures DDoS protection policies that are continuously tuned to your application’s traffic profiles, helps protect your services.

The following diagram shows how Azure DDoS Protection works:



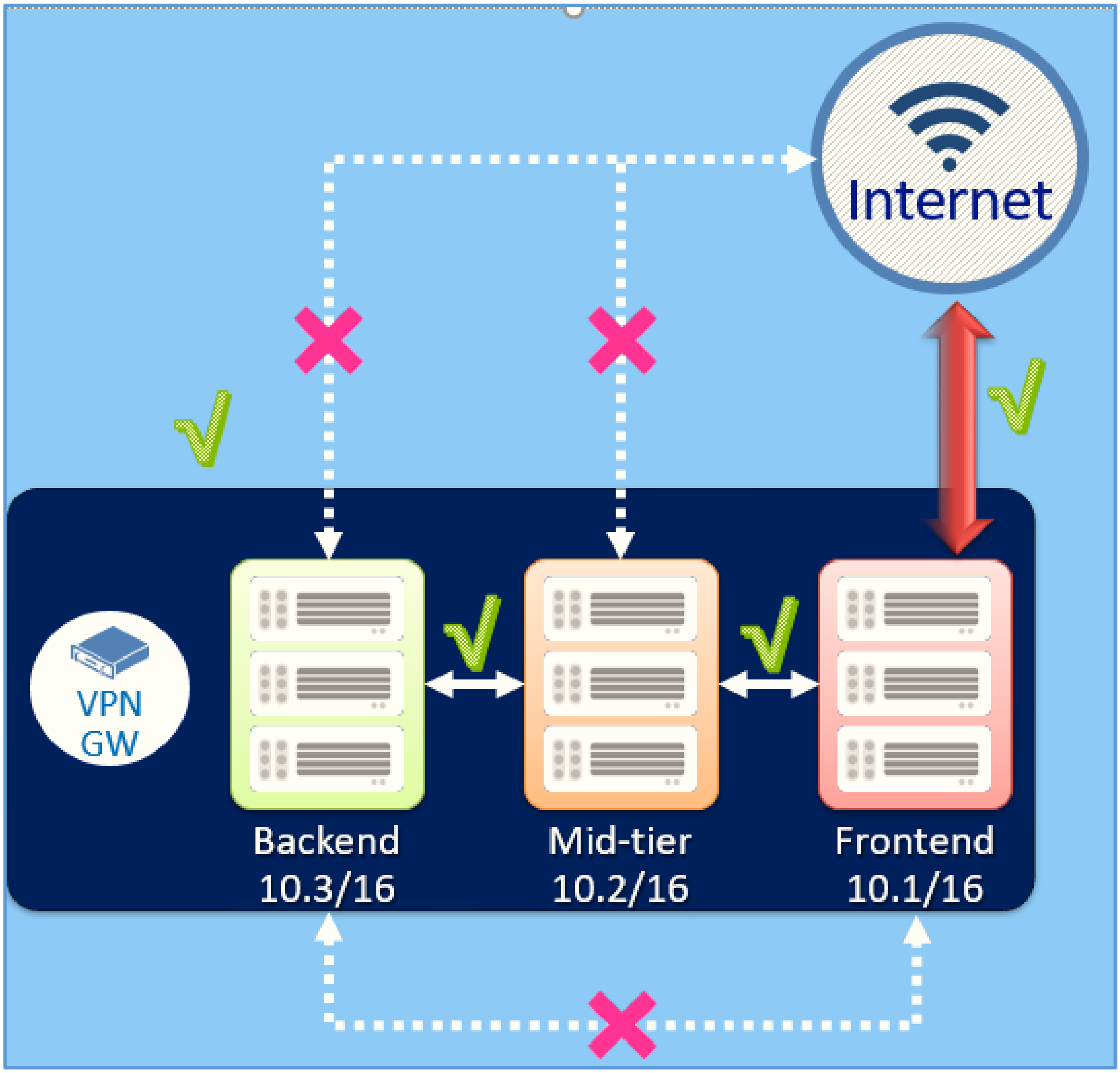
Security controls to consider through Azure network services

An Azure virtual network provides a secure, logical network that's isolated from other virtual networks and supports many security controls that you use on your on-premises networks.

The following security controls are available on Azure virtual networks.

Network access controls

Although the Azure virtual network is the cornerstone of the Azure networking model and provides isolation and protection, network security groups are the main tool that you use to enforce and control network traffic rules at the network level. The following diagram illustrates these network traffic rules:



You can control access by permitting or denying communication between the workloads within a virtual network, communication from systems on customers' networks via cross-premises connectivity, or direct internet communication.

In the diagram, both virtual networks and NSGs reside in a specific layer in the Azure overall security stack. You can use NSGs, UDR, and virtual network appliances to create security boundaries to protect the application deployments in the protected network.

NSGs use a 5-tuple to evaluate traffic. You use these items in the rules that you configure for the NSG.

- Source and destination IP address
- Source and destination port
- Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)

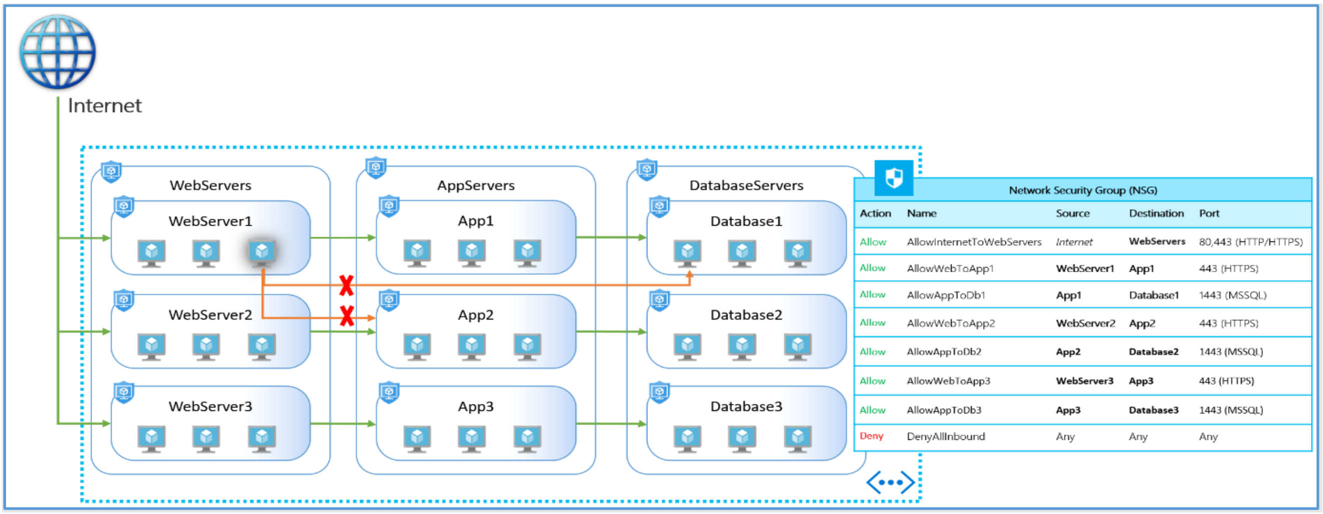
This means you can control access between a single VM and a group of VMs, between a single VM and another single VM, or between entire subnets. Keep in mind that this is simple stateful packet filtering, not full packet inspection. There is no protocol validation or network-level IDS or IPS capability in a network security group.

You should be aware of built-in rules that all network security groups use, because they can affect your overall network security posture.

Application security groups

You can use application security groups (ASGs) to centralize policy configuration and simplify your security management. With application security groups, you can define detailed network security policies based on workloads, applications, or environments by using monikers assigned to virtual machines. This enables you to implement a zero-trust model, limiting access to the application flows that are explicitly permitted.

The following diagram shows an example of an application security group:

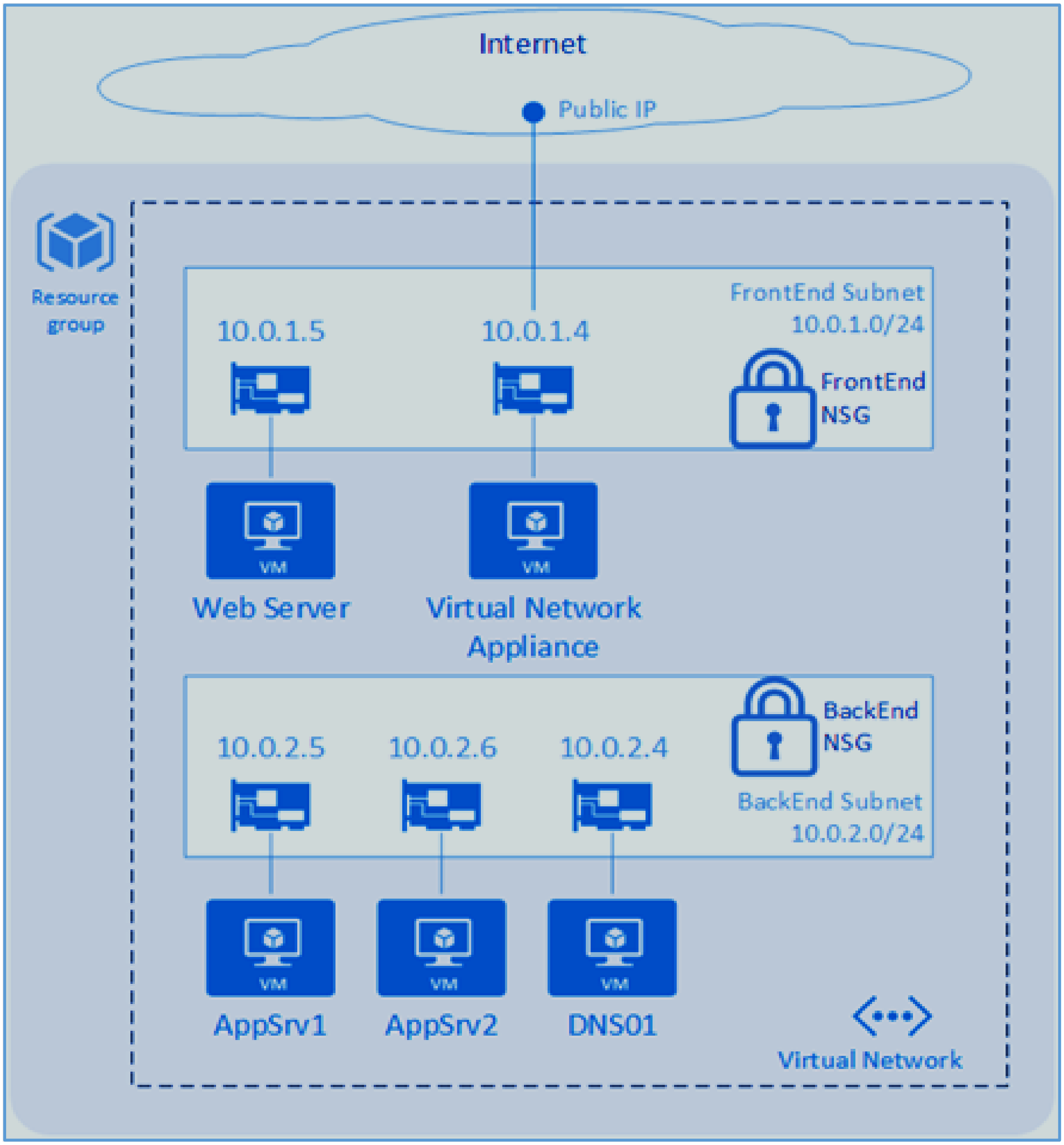


Network Security Group (NSG)

Action	Name	Source	Destination	Port
Allow	AllowInternetToWebServers	*Internet*	**WebServers**	80,443 (HTTP/HTTPS)
Allow	AllowWebToApp1	**WebServer1**	**App1**	443 (HTTPS)
Allow	AllowAppToDb1	**App1**	Database1	1443 (MSSQL)
Allow	AllowWebToApp2	**WebServer2**	**App2**	443 (HTTPS)
Allow	AllowAppToDb2	**App2**	**Database2**	1443 (MSSQL)
Allow	AllowWebToApp3	**WebServer3**	**App3**	443 (HTTPS)
Allow	AllowAppToDb3	**App3**	**Database3**	1443 (MSSQL)
Deny	DenyAllInbound	Any	Any	Any

Network security appliances

Although network security groups and user-defined routes can provide some network security at the network and transport layers of the OSI model, in certain situations, you need to enable security at higher levels of the networking stack. In such situations, we recommend that you deploy virtual network security appliances (illustrated in the following figure) from Azure partners.



Azure network security appliances improve virtual network security and network functions, and they're available from numerous vendors via the Azure Marketplace. Deploying virtual security appliances can provide:

- Intrusion detection
- Web application firewalls
- Routing
- Certificate management

- Active Directory
- Multi-factor authentication

Virtual network service endpoints

Virtual network service endpoints extend your virtual network private address space to Azure services. This enables you to limit access to business-critical Azure resources to only your virtual networks, fully removing internet access. All traffic through a service endpoint stays in Azure.

This feature is available for the following Azure services and regions:

- **Azure Storage**: Generally available in all Azure regions.
- **Azure SQL Database**: Generally available in all Azure regions.
- **Azure Cosmos DB**: Generally available in all Azure public cloud regions.
- **Azure SQL Data Warehouse**: Preview in all Azure public cloud regions.

Network security validation through logging and auditing

Azure network validation helps ensure that the Azure network is operating as it's configured. You can do this validation by using the services and features available to monitor the network.

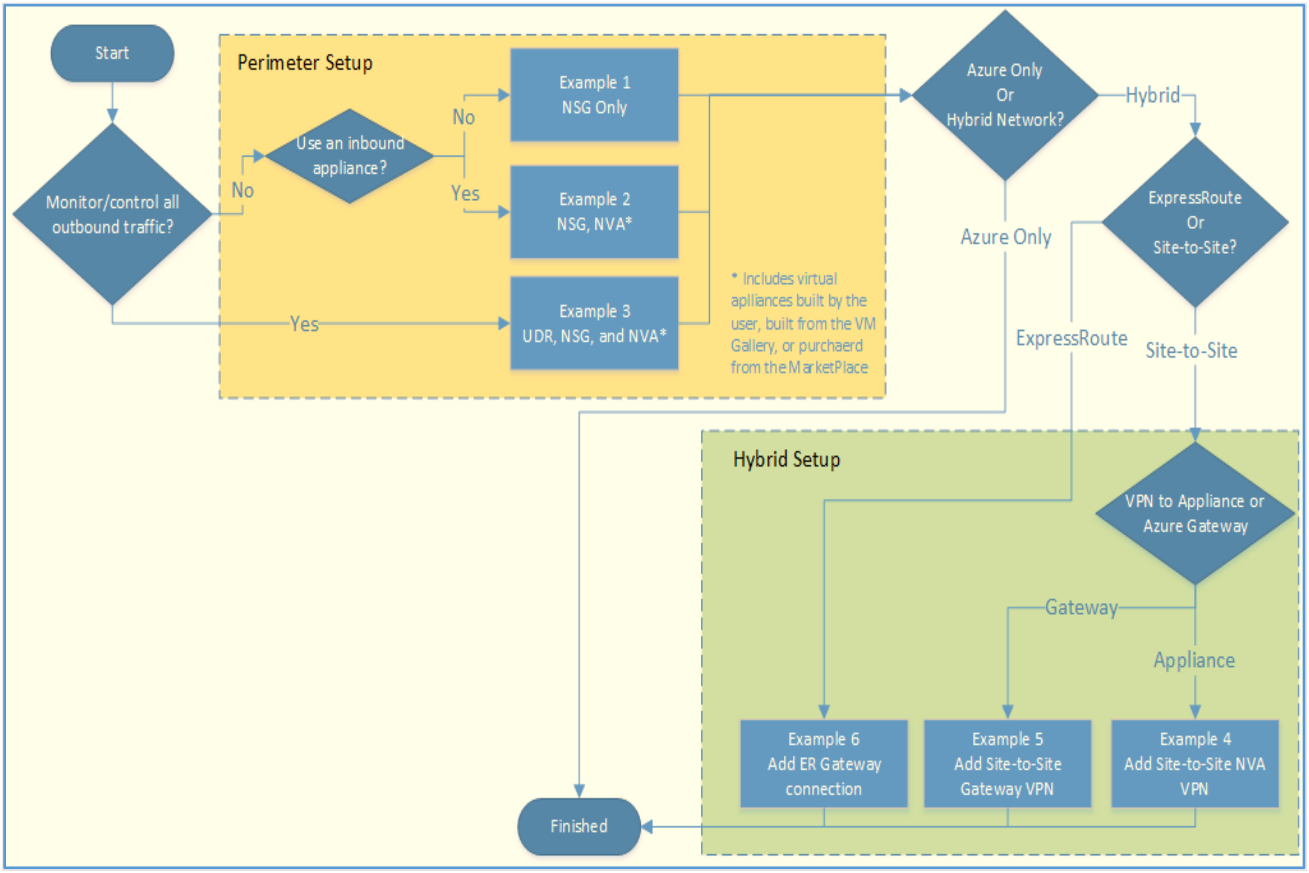
With Azure Network Watcher, you can access logging and diagnostic capabilities that empower you with insights to understand your network performance and health. These capabilities are accessible via the portal, PowerShell, Azure CLI, REST API, and SDKs.

Other tools that you can use to monitor, prevent, detect, and respond to network security events include network-resource-level monitoring and Azure Log Analytics.

Microsoft cloud services and network security

Microsoft cloud services deliver hyperscale services and infrastructure, enterprise-grade capabilities, and many choices for hybrid connectivity. Customers can choose to access these services either via the internet or via Azure ExpressRoute, which provides private network connectivity. The Azure platform enables customers to extend their infrastructure into the cloud and build multitier architectures. Additionally, third parties can enable enhanced capabilities by offering security services and virtual appliances.

The following logic chart can direct you to a specific example of the many security techniques available with the Azure platform:


Start
Perimeter Setup
Monitor/control all outbound traffic?
No
Use an inbound appliance?
No
Yes
Example 1
NSG Only
Example 2
NSG, NVA*
Yes
Example 3
UDR, NSG, and NVA*
* Includes virtual appliances built by the user, built from the VM Gallery, or purchaerd from the MarketPlace
Azure Only Or Hybrid Network?
Hybrid
ExpressRoute Or Site-to-Site?
Azure Only
ExpressRoute
Site-to-Site
Hybrid Setup
VPN to Appliance or Azure Gateway
Gateway
Appliance
Example 6
Add ER Gateway connection
Example 5
Add Site-to-Site Gateway VPN
Example 4
Add Site-to-Site NVA VPN
Finished

Example 1: Build a perimeter network to help protect applications with NSGs.

Example 2: Build a perimeter network to help protect applications with a firewall and NSGs.

Example 3: Build a perimeter network to help protect networks with a firewall, user-defined route, and NSGs.

Example 4: Add a hybrid connection with a site-to-site virtual appliance VPN.

Example 5: Add a hybrid connection with a site-to-site Azure VPN gateway.

Example 6: Add a hybrid connection with ExpressRoute.

Best practices

The following best practices summarize the information in this article. They're derived from our experience with Azure networking and the experiences of customers. For more information, see Azure network security best practices.

- **Control routing behavior**: The default system routes are useful for many deployment scenarios, but there are times when you want to customize the routing configuration for your deployments. These customizations will enable you to configure the next hop address to reach specific destinations. You can learn more about user-defined routes and how to configure them by reading the article Virtual network traffic routing.

- **Enable forced tunneling**: We recommend that you enable forced tunneling on your virtual machines when you have cross-premises connectivity between your Azure virtual network and your on-premises network.

- **Use virtual network appliances**: Although network security groups and user-defined routing can provide some network security at the network and transport layers of the OSI model, sometimes you might need to enable security at high levels of the stack. In such situations, we recommend that you deploy virtual network security appliances from Azure partners.

- **Deploy perimeter networks for security zoning**: DMZs are useful because you can focus your network access control management, monitoring, logging, and reporting on the devices at the edge of your Azure virtual network. Here you typically enable DDoS prevention, intrusion detection and prevention systems, firewall rules and policies, web filtering, network antimalware, and more. The network security devices sit between the internet and your Azure virtual network and have an interface on both networks.

- **Avoid exposure to the internet with dedicated WAN links**: If you need an exceptional level of security or performance for your cross-premises connections, we recommend that you use Azure ExpressRoute for your cross-premises connectivity. ExpressRoute is a dedicated WAN link between your on-premises location and an Exchange hosting provider. Because this is a telco connection, your data doesn't travel over the internet and therefore is not exposed to the potential risks inherent in internet communications.

- **Optimize uptime and performance**: Confidentiality, integrity, and availability (CIA) compose the triad of today's most influential security model. Confidentiality is about encryption and privacy, integrity is about making sure that data is not changed by unauthorized personnel, and availability is about making sure that authorized individuals can access the information they're authorized to access. Failure in any one of these areas represents a potential breach in security.

- **Use global load balancing**: You can get global load balancing in Azure by taking advantage of Azure Traffic Manager. Traffic Manager makes it possible to load balance connections to your services based on the location of the user. For example, if the user is making a request to your service from the EU, the connection is directed to your services located in an EU datacenter. This part of Traffic Manager global load balancing helps improve performance because connecting to the nearest datacenter is faster than connecting to datacenters that are far away.

- **Disable RDP access to Azure virtual machines**: We recommend that you disable direct RDP and SSH access to your Azure virtual machines from the internet. After you disable direct RDP and SSH, access from the internet is disabled.
- **Enable Azure Security Center**: Azure Security Center helps you prevent, detect, and respond to threats. It gives you increased visibility into, and control over, the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.
- **Extend your datacenter into Azure**: Microsoft has created the datacenter extension reference architecture diagram and supporting collateral to help you understand the key components of such a datacenter extension. You can use this example reference implementation to plan and design a secure enterprise datacenter extension to the cloud.

Next steps

Learn more about security by reading in-depth security topics:

- Diagnostic logging for a network security groups
- Networking innovations that drive the cloud disruption
- SONiC: The networking switch software that powers the Microsoft Global Cloud
- How Microsoft builds its fast and reliable global network
- Lighting up network innovation

Resources

GitHub repositories

- Azure Virtual Network libraries for .NET
- ExpressRoute connectivity models
- Configure a point-to-site connection to a virtual network using native Azure certificate authentication

Samples

- Azure DNS sample for managing DNS zones
- Application security group sample
- Azure Traffic Manager sample for managing profiles