MICROLAND®

Extraordinary. Everyday.

BUILDING GOVERNMENT-GRADE-SECURE INFRASTRUCTURE ON MICROSOFT AZURE – 101

SOLUTION PAPER

Building Government-Grade-Secure Infrastructure on Microsoft Azure – 101

Introduction

This is a primer on building secure infrastructure for organizations/industries that are sensitive to data security and have stringent security regulations and controls. Usage of components, rationale and optimizing for compliance requirements for Azure Government and Azure Government for DoD is discussed in the final section of the document. This paper is primarily relevant for Azure, Azure Government and Azure Government for DoD.

This document focusses on a few broad properties listed below which are critical to building a secure core infrastructure for applications and workloads.

- Network security
- Administrative/operational security
- Securing data at rest
- Securing data in transit
- Security logging & auditing

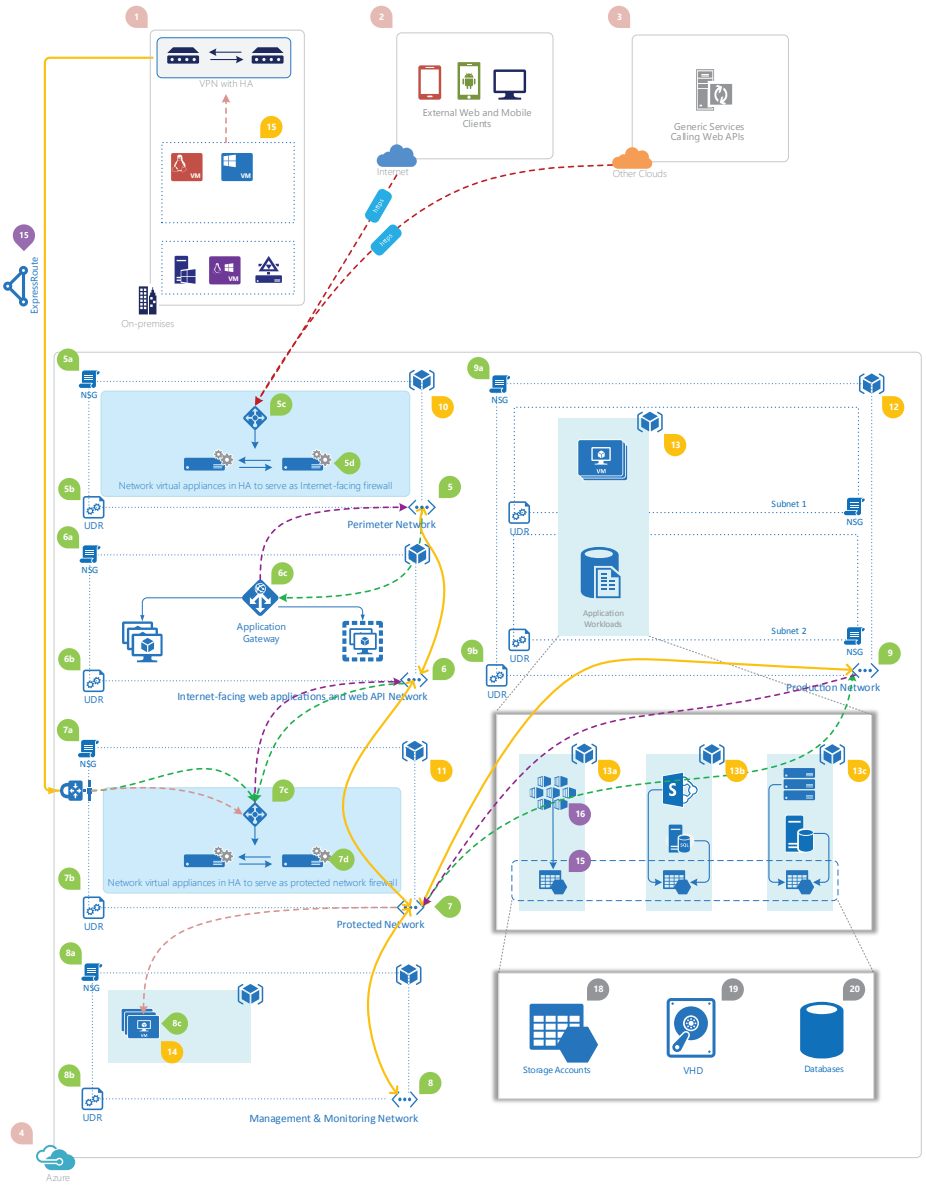
Overview

The illustration below indicates an Azure layout that depicts the fundamentals of building a secure infrastructure. The infrastructure outlined here comprises of some of the common scenarios/patterns found in most settings. As in the case of most infrastructure setups, this scenario indicates an on-premise infrastructure or a traditional datacenter. The design factors the need of users/external systems who have to access public-facing web applications or APIs hosted on Azure, and also the possibility of generic services hosted in other public clouds that access the public internet-facing applications. The theme of this document is securing the core infrastructure that is hosted on Azure, patterns and practices of designing, architecting and building a secure application is not in the scope of this document.

The high-level design is architected such that the on-premise environment is connected to the Azure environment via ExpressRoute. The design accommodates users and devices accessing the Azure environment from the internet for scenarios in which applications are hosted publicly. The rationale behind the choice of technology, components & placement/architecture is detailed in the subsequent sections.

With this introduction, one may choose to use the reference architecture below and associate the components used with the legend distributed across the broad categories mentioned above.

Reference architecture



1. On-premises environment/traditional datacenter
2. Devices and users on the internet consuming public APIs/Web
3. Other cloud services accessing public APIs/Web
4. Azure infrastructure

- ExpressRoute/Peered Virtual Networks
- Trusted traffic
- Untrusted traffic originating from the internet
- Management traffic
- Outbound traffic

Design — Components & rationale

Network security

The network design in this reference architecture comprises a perimeter virtual network, a virtual network for internet-facing applications, a protected network and further down is a production network. The architecture aims at adopting a defense-in-depth strategy. There are platform components used like network security groups and user-defined routes along with network virtual appliances used at various junctures to offer security.

Perimeter network

5 Perimeter network – Implemented to form the first line of defense for internet-facing public applications and APIs. Only network virtual appliances (NVA) contributing to forming proxies, and firewalls are placed in this virtual network (VNet). This network appears with the internet-facing web apps network.

5a Network Security Group (NSG) – NSG provides network ACLs like in a firewall. This configuration allows https traffic to pass and blocks any other protocol.

5b User Defined Routes (UDR) – Allows for customized routing of data packets. This configuration implies that any traffic intended for a public web application or APIs will be directed to *internet-facing web applications* & APIs VNet. Traffic directed to any other destination will be dropped.

5c Azure Load Balancer – An external load balancer to direct traffic from the internet to the NVAs.

5d Network Virtual Appliances (NVA) – While the NSG and UDR could be used for network security; it might be a compliance requirement or specific security needs that call for an NVA to act as a firewall or proxy. In the perimeter network, NVAs are used in high availability mode with an Azure external (L4) load balancer distributing traffic. It works in conjunction with the NSG to log, monitor and filter traffic. In this configuration, it allows to pass through https traffic directed to the front-end applications in the *internet-facing web applications & APIs* VNet and blocks traffic to any other destination.

Internet-facing web applications and web API network

6 Internet-facing web apps and APIs network – Designed to host web apps and APIs for access via the internet. This network should contain hardened, low surface area web servers. This could be traditional web server farms or VM ScaleSets in Azure. This network peer with the protected network for web apps to access the backend servers and perimeter network for traffic from the internet.

6a Network Security Group (NSG) – NSG provides network ACLs much like in a firewall. This configuration, allows https traffic originated at perimeter network to pass to the web servers hosted in this VNet directed via the application gateway (explained below).

6b User Defined Routes (UDR) – Allows for customized routing of data packets. In this configuration, any traffic originating in this VNet directed to backend *servers in the production network* will be directed through the NVAs for logging, monitoring, and filtering in the protected network. Traffic directed to any other destination will be dropped.

6c Application Gateway – Provides Layer 7 load balancing capabilities, web application firewall, URL-based routing, SSL termination, etc. In this configuration, the application gateway forms a layer of protection from web-based attacks like XSS and SQL injection; and does multi-site routing for various web applications/APIs.

Protected network

7 Protected network – Designed to form the second line of defense for the infrastructure. This network hosts NVAs that acts as firewalls protecting application and database servers. This network also hosts the ExpressRoute Gateway for connectivity with the on-premise environment. Any traffic originating on-premises traverses through the protected network to the production network. This network is peered with the *internet-facing web apps/APIs network* to allow traffic from web servers directed to the production network and on-premises to production network and on-premises to the management network.

7a Network Security Group (NSG) – NSG provides network ACLs much like in a firewall. This configuration allows traffic originated at *internet-facing web apps/APIs network* or on-premises via the ExpressRoute gateway to pass to the *production network/ management network*.

7b User Defined Routes (UDR) – Allows for customized routing of data packets. In this configuration, any traffic originating on-premises via ExpressRoute directed to servers in the *production network/management network* will be directed through the NVAs for logging, monitoring, and filtering in the protected network. Traffic originating elsewhere or directed to any other destination will be dropped.

7c Azure Load Balancer – An internal load balancer to direct traffic from the Internet-facing web applications and web API network & on-premises to the NVAs.

7d Network Virtual Appliances (NVA) – Employs NVAs to act as a firewall or proxy in the protected network. In this network, NVAs are used in high availability mode with an Azure external (L4) load balancer distributing traffic. It works in conjunction with the NSG to log, monitor and filter traffic. In this configuration, it allows to pass through traffic from on-premises and *Internet-facing web applications & web API network* directed to the management and production network and blocks traffic to any other destination

Management network

8 Management network – Designed as the network that allows for management and monitoring activities within the Azure infrastructure, this network is peered with the protected network and has transitive connectivity to all networks through management ports and protocols within the environment.

8a Network Security Group (NSG) – NSG provides network ACLs much like in a firewall. This configuration, allows passing traffic originated on-premises via the ExpressRoute gateway from the POW network (detailed under security-least privilege).

8b User Defined Routes (UDR) – Allows for customized routing of data packets. In this configuration, any management/monitoring traffic passing through the protected network directed to resources in the environment will be directed to the appropriate VNet.

8c Management/monitoring hosts – These are servers that have access to the environment for management activities (only the incoming management traffic from on-premise to the management hosts via the protected network is shown in the diagram.)

Production network

9 Production network – Designated VNet for all applications and workloads. This network peer with the Protected network. Any traffic designated to this network would have traversed through the NVAs in the protected network. This VNet has multiple subnets depending on the tiers of various applications hosted here. Each subnet will have it's own NSGs and UDRs based on specific routing/security needs.

9a Network Security Group (NSG) – NSG provides network ACLs much like in a firewall. This configuration allows traffic directed via the protected network to pass through and drops all other traffic.

9b User Defined Routes (UDR) – Allows for customized routing of data packets. In this configuration, any outbound traffic is directed via the NVAs in the protected network.

Administrative/operational security

Administrative/operational security is enforced by using RBAC controls that represents the administrative, operational or responsibility model that exists and shared among various parties. Defining the right amount and degree of access is critical for these parties. Enforcing just-in-time access is also detailed in this section. RBAC focusses on defining permissions at a management plane and not at a data plane.

Role-based access control

10 The perimeter VNet, NVAs and associated components that make up this boundary are grouped into a single resource group. The RBAC controls on resources and resource groups are selected such that there is no over-provisioning of rights. The built-in roles are classified into Owner, Contributor, and Reader. Multiple security groups are created to map to appropriate roles, the membership to those groups are guided based on the administrative and responsibility model. In this model, the perimeter security resource group should be maintained and operated by a party (accounts/credentials) that is separate from the one that manages any other aspects of the environment (specifically the protected network).

11 Much like in case of the perimeter network, the components that make up the protected network is to be wrapped into a single resource group with permissions isolated across various built-in roles. Separation of responsibilities should be accomplished with the permissions matrix that gets built. In other words, the reason for there being a perimeter network and the protected network is to ensure that an attacker has to successfully penetrate through two sets of NVAs to compromise the production environment, the operational/administrative model you have should reflect this purpose and in turn, the permissions matrix has to represent this goal.

12 The production should wrap the core network infrastructure components into a single resource group. The permissions to be set such that there are minimum accounts with Network Owner or Contribute level privileges. The applications' owners/administrators should have enough privileges to join this VNet.

13 The applications are to be wrapped in their respective resource groups based on the administrative model following the principle of least privilege. If there is shared responsibility amongst various parties to different parts of the applications, permissions are to be set accordingly. 13a 13b 13c

Just-in-time access

14 Management ports are vulnerable and prone to brute force attacks. Just-in-time can be enabled to block inbound traffic towards VMs and providing access only during times when it is needed. Just-in-time access policy can be used throughout the environment, the policy allows to define the ports, protocol, and source as parameters. This allows access to be provided on a need-to-know basis. The owners of applications, admins of NVA in perimeter/protected network should be brought to the scope of just-in-time access policy. In this configuration, the administrators of NVAs have reader-level permissions for both perimeter and protected network; however, the access to those server for management is given just in time.

Privileged access workstations

15 In a secure environment, it is common practice to classify the risk of administrative activities. All high risk/high privileged access are prone to attacks like pass-the-hash, keystroke-logging, pass-the-ticket, etc. Having a dedicated workstation and dedicated credentials or accounts greatly reduces the exposure of a large category of threat vectors. In this configuration, all of the management is directed from PAWs from on-premise directed to the management network via ExpressRoute after inspection by the NVAs in the protected network.

Security for data in transit

It is obvious that there is much effort put in to securing the environment, be it on-premises or on Azure. Ultimately, all this exercise narrows down to safeguarding the data these environments house. One of the important tenets to consider is securing this data while being passed around within an environment and across environments or the internet.

ExpressRoute

15 ExpressRoute (ER) offers direct connectivity from an on-premise environment to the Azure Environment. ER provides direct connectivity from an Azure datacenter to an on-premise datacenter (Azure Government's ER provides connectivity from an AzureGov location to an on-premise location owned by a govt. agency via teleco providers authorized for this category of services. This partnership with teleco and Azure is already in place). The environment also provides isolation for DoD customers. The connections are TLS encryption enabled by default. Customer may choose to use NVAs to run a VPN tunnel over ExpressRoute for additional security.

Transport-level encryption – Using https

16 Any traffic between client and Azure storage should be protected with https. REST API calls to Azure storage should be enforced to use https.

Client-side encryption

17 Applications handling data may choose to encrypt data prior to sending it over to the storage or through API calls. Decryption should happen programmatically upon retrieval. Combining this with the https will offer additional data security during transit and at rest.

Security for data at rest

This is the crux of data security, integrity, and privacy. This section details ways in which data at rest can be secured and protected.

Storage service encryption (SSE)

18 Storage service encryption applies at the scope of a storage account. Any data written to the storage account is encrypted by default and decrypted automatically upon retrieval. Customers may choose to apply client (application) side encryption to further security.

Disk encryption

19 Linux uses DMCrypt and Windows uses Bitlocker. In Azure, these encryption keys can be stored in Azure Key Vault. This ensures the data disks and OS disks are encrypted at the file system level. Customers may chose to perform disk encryption in combination with SSE.

Transparent data encryption

20 It has been a requirement in many industries that databases are protected at a file level while at rest. TDE/equivalent is supported by most database vendors like Microsoft, Oracle, etc. This ensures that data is encrypted at a page level while at rest.

Security logging & auditing

All the above sections discuss methods to devise a strategy against potential vulnerabilities & threats. Security logging and auditing is about measuring the effectiveness of security measures employed. Logging activities in the environment throws light into usage, patterns and potential pitfalls in design and deployment.

The reference architecture above does not explicitly call out logging auditing mechanisms put in place. It is advisable to consider logging activities across the management plane via the Azure activity logs. Activities within the data plane could be observed from logs generated by individual services engaged. All of the components used in this architecture has the capability of generating data plane logs.

Management Plane (RBAC) – Azure Activity Monitor, AAD reporting
Data Plane (Virtual Machines, Storage, Network, Other Azure services) - Storage Analytics, Network Watcher, Azure Monitor, Linux Syslog.

Azure Government

Azure Government has two categories of offerings available; and the compliances regulations are also categorized accordingly. Azure Government is for usage by state and federal agencies; and Azure Government for DoD is for exclusive usage by the DoD.

The compliance requirements from various state and Federal agencies are categorized into FedRAMP Moderate and FedRAMP High.

Azure has the following components included in the scope of FedRAMP Moderate - Application Gateway, Azure Active Directory (Free and Basic), Cloud Services, Key Vault, Load Balancer, Multi-Factor Authentication, SQL Database, Storage (Blobs, Disks, Files, Queues, Tables) including Cool and Premium Storage, Traffic Manager, Virtual Machines, Virtual Network, VPN Gateway, and supporting infrastructure and platform services.

Azure Government has the following components in the scope of FedRAMP High - App Service, Web Apps, Application Gateway, Automation, Azure Active Directory (Free and Basic), Azure Resource Manager, Backup, Batch, Cloud Services, Event Hubs, ExpressRoute, HDInsight, Import/Export, Key Vault, Load Balancer, Log Analytics, Media Services, Microsoft Azure Portal, Notification Hubs, Redis Cache, Scheduler, Service Bus, Site Recovery, SQL Data Warehouse, SQL Database, Storage (Blobs, Disks, Files, Queues, Tables) including Cool and Premium Storage, StorSimple, Traffic Manager, Virtual Machines, Virtual Network, VPN Gateway, and supporting infrastructure and platform services.

The DoD requires compliance in the order of DoD DISA SRG Level 4 and DoD DISA SRG Level 5.

DoD DISA SRG Level 4 goes with the same components in the scope of FedRAMP High and following components are in scope for Azure Government for DoD - Azure Active Directory (Free and Basic), ExpressRoute, Load Balancer, SQL Database, Storage (Blobs, Disks, Files, Queues, Tables) including Cool and Premium Storage, Traffic Manager, Virtual Machines, Virtual Network, VPN Gateway, and supporting infrastructure and platform services.

FedRAMP High indicates that highest degree of compliance requirements from government agencies and DoD DISA SRG Level 5 is the highest for DoD.

The reference architecture above complies with FedRAMP High in terms of the components used and the compliance certifications of Azure Government.

Conclusion

This document outlines a few patterns and practices that may be used to design a secure core-infrastructure. For most part of this document, the properties to look for and principles to follow are applicable to Azure, not just Azure Government. Implementing a complete solution would require understanding of the fine details of the scenario and architecting for data security, privacy, integrity, security, security reporting, etc., at an application, storage, network and management layers.

One of the areas that is critical to maintaining a secure infrastructure is security analytics; this has been briefly touched upon in the document.

About the author

Vishnu Rajkumar
Principal Architect

Vishnu Rajkumar is a Sr. Principal Architect at Microland. He is a Microsoft certified Azure Solutions Architect and focuses on helping customers with the adoption and operationalization of Microsoft Azure cloud technologies and services for their business benefits. He works closely with the customer's architecture and operations teams to help architect, design and deploy a highly resilient, scalable, compliant and efficient Azure based application and infrastructure solutions. He is experienced in architecting and implementing enterprise class core infrastructure and application infrastructure on Microsoft Azure platform using, Virtual Machines, PaaS, Containers and Microservice based architectures.

For further information
Contact us at: +1 646-254-3598 or Email us at: cloud@microland.com

About Microland

Microland accelerates the digital transformation journey for global enterprises enabling them to deliver high-value business outcomes and superior customer experience. Headquartered in Bangalore, India, Microland has more than 3,800 professionals across its offices in Australia, Europe, India, Middle East and North America. Microland partners with global enterprises to help them become more agile and innovative by integrating emerging technologies and applying automation, analytics and predictive intelligence to business processes.

Learn more about us at:

www.microland.com