Azure-HBSS-Dev-Environment

The Azure-HBSS-Dev-Environment repository contains a number of ARM templates to deploy a basic development environment consisting of representative networking for a core site and two satellite sites within Azure. This enables air-gapped virtual environments to be rapidly deployed in support of development, test and integration activities. It is left to the user to deploy individual VMs within each site's subnet(s) or expand the subnets as required.

Architecture

The overarching architectural principle for the HBSS Dev environment is that individual virtual machines and subnets are isolated both from the wider internet and each other by default. This means individual virtual machines cannot communicate with each other outside of their own subnet.

Four virtual networks are deployed by default. The vNet-HBSS-DCC virtual network is designed to roughly replicate a main HQ network. The network is partitioned into five initial subnets to segregate resources as required.

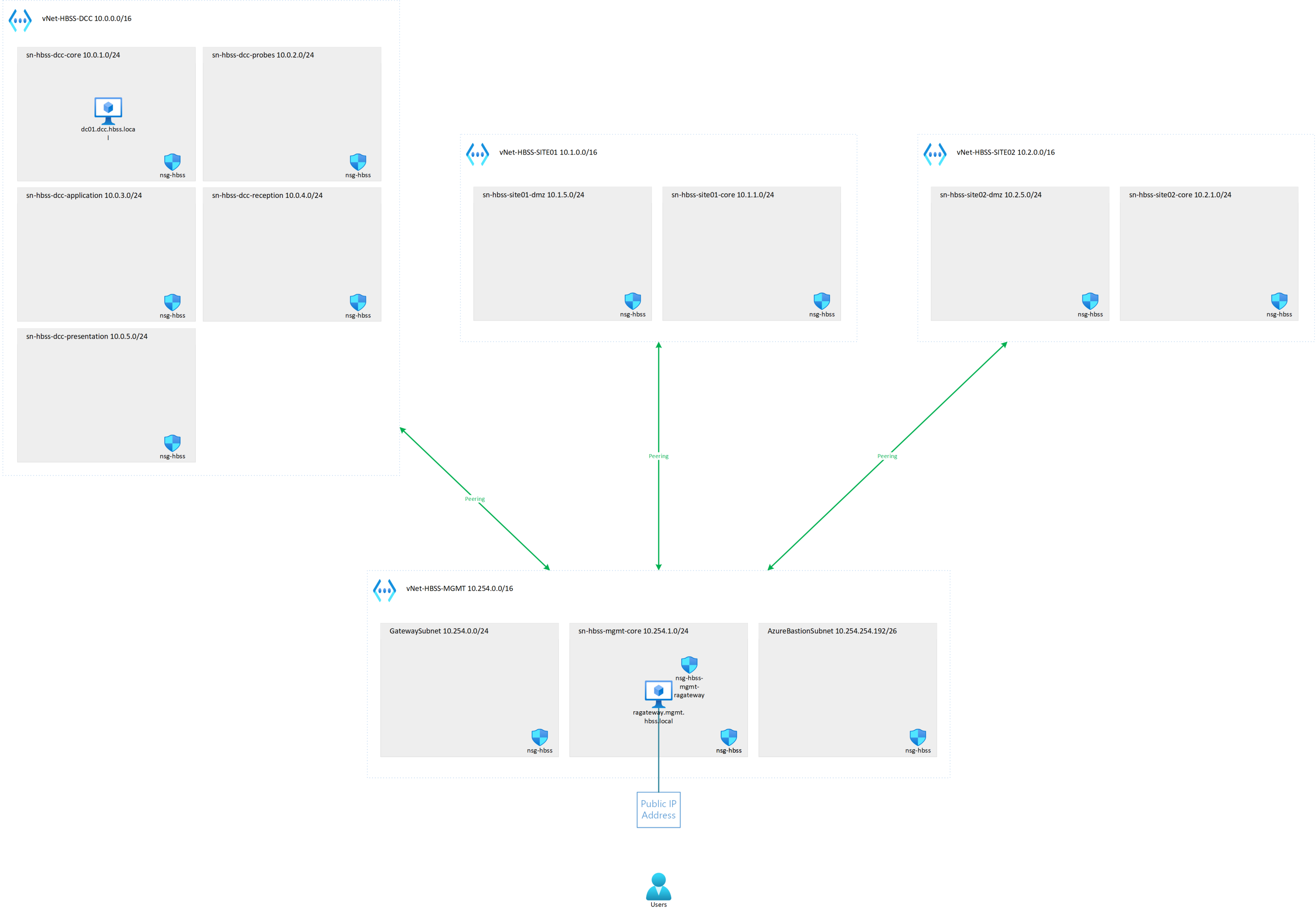
Two further vNets are deployed (vNet-HBSS-SITE01 and vNet-HBSS-SITE01) to represent more basic satellite sites/locations. These each initially contain two subnets, a core subnet for site services and a DMZ for WAN facing services.

Connectivity between sites is intially disabled and will need to be enabled using either peering between sites with additional limiting NSG rules, or using gateway devices. This is left to be implemented on a use case basis.

The management subnet (vNet-HBSS-MGMT) exists purely for management of the environment and the VMs within it. This management subnet is peered with each of the other site vNets and traffic to/from it is unrestricted allowing virtual machines on the management subnet to RDP/SSH to any other VM in the environment.

Individual virtual machines do not by default have any Network Security Groups (NSGs) associated with them. All subnets however are restricted by the same common NSG (nsg-hbss) which provides a single central location to control traffic flow across the environment.

Please see the overview diagram below.


vNet-HBSS-DCC 10.0.0.0/16
sn-hbss-dcc-core 10.0.1.0/24
dc01.dcc.hbss.local
nsg-hbss
sn-hbss-dcc-probes 10.0.2.0/24
nsg-hbss
sn-hbss-dcc-application 10.0.3.0/24
nsg-hbss
sn-hbss-dcc-reception 10.0.4.0/24
nsg-hbss
sn-hbss-dcc-presentation 10.0.5.0/24
nsg-hbss
vNet-HBSS-SITE01 10.1.0.0/16
sn-hbss-site01-dmz 10.1.5.0/24
nsg-hbss
sn-hbss-site01-core 10.1.1.0/24
nsg-hbss
vNet-HBSS-SITE02 10.2.0.0/16
sn-hbss-site02-dmz 10.2.5.0/24
nsg-hbss
sn-hbss-site02-core 10.2.1.0/24
nsg-hbss
Peering
Peering
Peering
vNet-HBSS-MGMT 10.254.0.0/16
GatewaySubnet 10.254.0.0/24
nsg-hbss
sn-hbss-mgmt-core 10.254.1.0/24
nsg-hbss-mgmt-ragateway
ragateway.mgmt.hbss.local
nsg-hbss
AzureBastionSubnet 10.254.254.192/26
nsg-hbss
Public IP Address
Users

Management of the environment is initially performed via a web portal running on the ragateway.mgmt.hbss.local virtual machine. This is the only virtual machine in the environment with wider internet access and consequently the only virtual machine with its own NSG limiting traffic from the wider internet to ssl web encrypted traffic on port 8443. If further lock down is required, access to the VM can be additionally restricted using Azure Just in Time (JIT) access meaning all traffic is blocked until specific ports are opened to individual IPs as required.

The ragateway VM runs Apache Guacamole enabling web based RDP or SSH sessions to be defined for each of the VMs on the internal environment. In addition, if configured, file transfer to the internal VMs can be performed from the same web portal. Apache Guacamole performs all of the functionality of Azure Bastion and more for out of band access to air gapped virtual machines. It is however significantly cheaper to run and can be shutdown when not in use unlike Bastion which needs to be deleted.

Finally, AzureBastionSubnet and GatewaySubnet subnets have been created on the managment vNet ready to deploy Azure Bastion or Gateway devices should they be required in the future.

Security Rules

As previsouly mentioned, all subnets in the HBSS-DEV environment are, in their initial state, isolated from one another with the exception of the management vNet and its subnets which can access all network locations across the environment. At present this is implemented via a single Network Security Group (nsg-hbss) which controls all access across the environment. The default rules for this NSG are shown below:

nsg-hbss Inbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action	Notes
100	Allow Bastion From Mgmt Network	22,3389	Any	10.254.0.0/16	Any	Allow	Priority rule to allow management traffic from management network
4096	Deny InBound	Any	Any	Any	Any	Deny	Overrides AlowVnetInBound below to block traffic across subnets
65000	Allow VnetIn Bound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	Default rule to allow traffic across subnets within the same vNet. This is overridden by DenyInBound rule above.
65001	Allow Azure Load Balancer InBound	Any	Any	AzureLoadBalancer	Any	Allow	Default rule to allow traffic from Azure Load Balancers. Not currently used.
65500	Deny All InBound	Any	Any	Any	Any	Deny	Default rule to block all other traffic.

nsg-hbss Outbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action	Notes

Priority	Name	Port	Protocol	Source	Destination	Action	Notes
100	Allow Outbound To PrivateIPs	Any	Any	Any	10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16	Allow outgoing traffic to any IP that is in a private IP range. This allows any newly defined vNets to be accessible if their inbound rules allow.	
4096	Deny Outbound	Any	Any	Any	Any	Deny	All other (non private IPs) will be blocked, effectively airgapping any vNets from the wider internet.
65000	Allow Vnet OutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	Default rule to allow traffic across subnets within the same vNet.
65001	Allow Internet OutBound	Any	Any	Any	Internet	Allow	Default rule to allow traffic to the internet. This is overriden by the DenyOutbound rule above meaning vNets are airgapped from the internet.

Priority	Name	Port	Protocol	Source	Destination	Action	Notes
65500	Deny All OutBound	Any	Any	Any	Any	Deny	Default rule to block all other traffic.

In addition to the nsg-hbss global NSG, there is a single additional NSG associated with the ragateway.mgmt.hbss.local virtual machine. This managment VM is the only virtual machine in the environment with direct internet access and so is further hardened with the following rules.

nsg-hbss-mgmt-ragateway Inbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action	Notes
100	SSH	22	TCP	Any	Any	Allow	Priority rule to allow SSH traffic to the remote access gateway VM for initial configuration. This should be disabled once configuration is complete or Just In Time (JIT) access rules should be implemented.

Priority	Name	Port	Protocol	Source	Destination	Action	Notes
200	HTTPS	8443	TCP	Any	Any	Allow	Priority rule to allow encrypted web traffic to the remote access gateway web interface. The device will initially be configured with a self signed certificate. To further secure the connection, please configure a trusted, signed certificate for your environment. Further restrictions can be enforced by enabling just in time (JIT) access on this port.
65000	Allow Vnet InBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	Default rule to allow traffic across subnets within the same vNet.

Priority	Name	Port	Protocol	Source	Destination	Action	Notes
65001	Allow Azure Load Balancer InBound	Any	Any	AzureLoadBalancer	Any	Allow	Default rule to allow traffic from Azure Load Balancers. Not currently used.
65500	Deny All InBound	Any	Any	Any	Any	Deny	Default rule to block all other traffic.

nsg-hbss-mgmt-ragateway Outbound Security Rules

Priority	Name	Port	Protocol	Source	Destination	Action	Notes
65000	Allow Vnet OutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	Default rule to allow traffic across subnets within the same vNet.
65001	Allow Internet OutBound	Any	Any	Any	Internet	Allow	Default rule to allow traffic to the internet.
65500	Deny All OutBound	Any	Any	Any	Any	Deny	Default rule to block all other traffic.