

Secure access to Azure VMs with Azure Bastion

by Gregor Reimling

Menti

Gregor Reimling

 Cloud Consultant @Sepago

 Cloud and Datacenter, Governance

 Azure Infrastructure (Governance, IaaS, Security)

 info@reimling.eu

 @GregorReimling | @AzureBonn

 www.reimling.eu | www.neutralien.com

Identity Summit 2020
follow @IdentitySummit
on Twitter

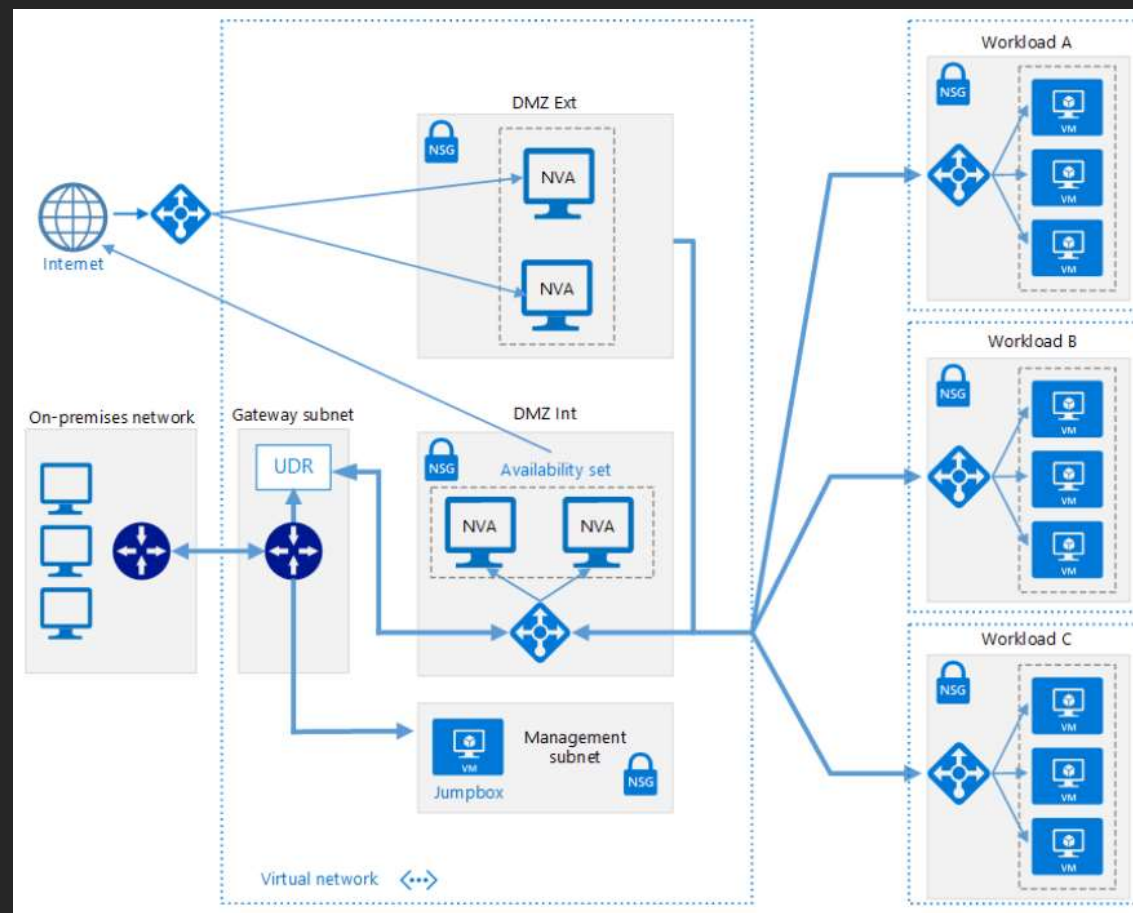


www.AzureBonn.de

Azure Bastion - Agenda

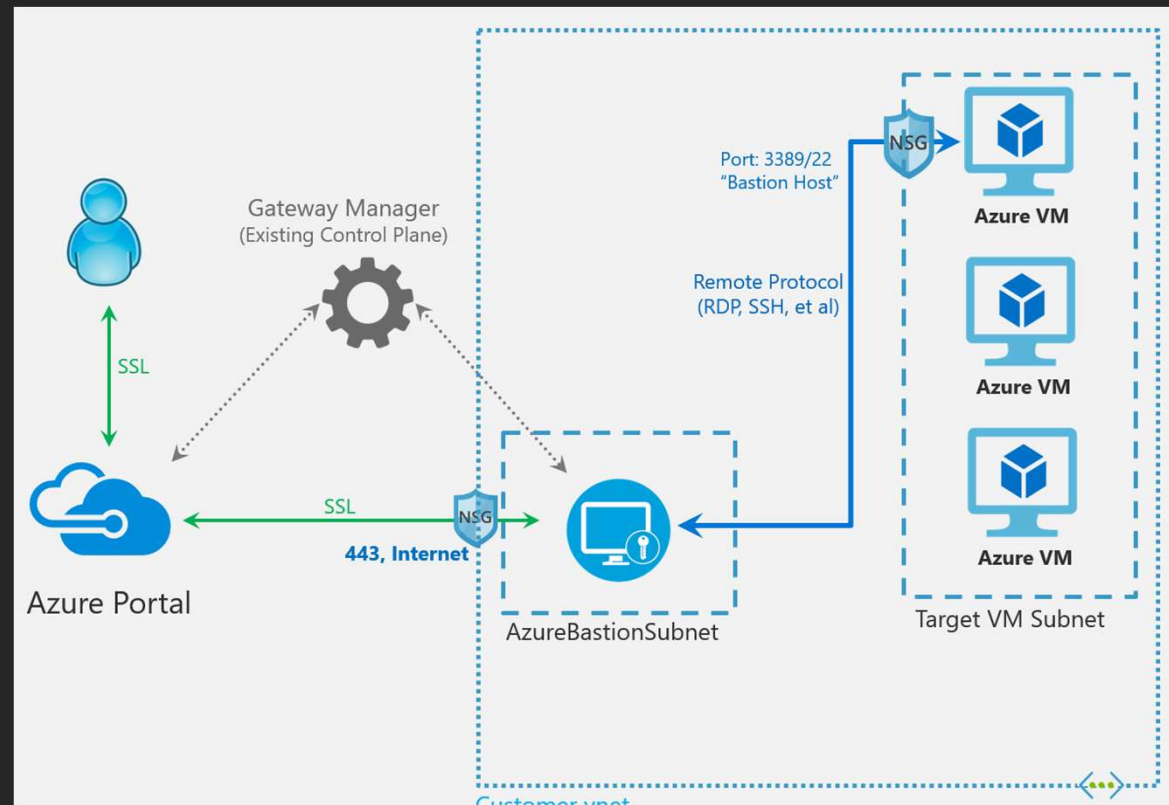
- Overview
- Requirements
- Demo
- Hardening
- Pricing & SLA
- Roadmap

Azure VNET Best Practices



Azure Bastion - Overview

- Fully-managed PaaS Service by Microsoft
- Replace Management of own Jumphosts
- Avoid bind Public IP on VM for Management purposes
- RDP and SSH directly inside the Azure Portal
- No need for an Agent inside VM
- Easy to deploy



Azure Bastion – General Notes



Region availability

West US, East US,
South Central US

West Europe

Australia East &
Japan East – take
a look at

<https://docs.microsoft.com/en-us/azure/bastion/bastion-overview#which-regions-are-available>



Browser

compatibility
Chromium based
(Edge Dev and
Chrome)

Firefox also works

| Instance details | |
|----------------------------|------------------|
| Name * | AzBastionVNETHub |
| Region * | West Europe |
| Configure virtual networks | |
| Virtual network * ⓘ | Australia East |
| | East US |
| | Japan East |
| | South Central US |
| | West Europe |
| | West US |
| Public IP address | |
| Public IP address * ⓘ | |

Azure Bastion – Requirements

- Minimum privileges
 - Reader role on the VM
 - Reader role on the assigned NIC
 - Reader Role on the Azure Bastion resource
- Need an own Subnet inside the Virtual Network
 - subnet need at least /27 or larger subnet

Azure Bastion – How it works

- Deploy a HTML 5 based Webclient
- RDP and SSH direct over the Portal
- Forward SSH/RDP over SSL
- Only accessible via the Portal
- Can't access the Public IP directly

Virtual machines

AzureMechanic

+ Add ▾ ⌚ Reservations ▾ ⋮

Try the new virtual machine resource browser! This experience is faster and has improved sorting and filtering capabilities. Please note that the new experience will not show classic virtual machines and does not include support for some columns such as maintenance status.

Filter by name...

☐ Name

- ☐ AzBstTEstVM1
- ☐ AzCMFS1
- ☐ AzCMWAC1
- ☐ AzCMWDC1
- ☐ AzVMAFSMS1



AzBstTEstVM1 | Bastion

Virtual machine

🔍 Search (Ctrl+ /)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks
- Size
- Security
- Advisor recommendations
- Extensions



Connect using Azure Bastion

Azure Bastion Service enables you to securely and seamlessly connect to your virtual machine over the network, without exposing a public IP on the VM, directly from the Azure portal, without the need for additional client/agent or any piece of software. [Learn more](#)

Using Bastion: **AzBstMVPPProdWESpoke**, Provisioning State: **Successful**

Please enter username and password to your virtual machine to connect.

☒ Open in new window

Username * ⓘ

Password * ⓘ

Connect

Azure Bastion - Demo

Azure Bastion – Hardening

- Harden Bastion Subnet with NSG
- Must define Inbound and Outbound Rules

The screenshot displays the Azure portal interface for the 'AzureBastionSubnet-NSG' network security group. The left-hand navigation pane includes sections for Overview, Settings, Monitoring, and Support. The main content area shows the NSG's properties, including its resource group, location, subscription, and tags. Below this, it lists the inbound and outbound security rules. The inbound rules table includes rules for allowing traffic from the GatewayManager, AzureCloud, and Internet, as well as rules for denying all inbound traffic. The outbound rules table includes rules for allowing traffic to the AzureCloud and Internet, as well as a rule for denying all outbound traffic.

AzureBastionSubnet-NSG
Network security group

Search (Ctrl+F)

Move Delete Refresh

Resource group (change) : azurebastion_rg
Location : West Europe
Subscription (change) : MVP Sponsorship
Subscription ID : 27a2c2c1-3244-4d2b-81fb-295710fdb66d
Tags (change) : Customer : GrR Environment : Eval Owner : Gregor

Custom security rules : 3 inbound, 2 outbound
Associated with : 1 subnets, 0 network interfaces

Inbound security rules

| Priority | Name | Port | Protocol | Source | Destination | Action |
|----------|-------------------------------|------|----------|-------------------|----------------|--------|
| 102 | Allow_Income_GatewayManager | Any | Any | GatewayManager | Any | Allow |
| 112 | Allow_Income_AzureCloud | Any | Any | AzureCloud | Any | Allow |
| 122 | Allow_Port_443_AzureBastion | 443 | TCP | Internet | Any | Allow |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowAzureLoadBalancerInBound | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | DenyAllInBound | Any | Any | Any | Any | Deny |

Outbound security rules

| Priority | Name | Port | Protocol | Source | Destination | Action |
|----------|---------------------------|---------|----------|----------------|----------------|--------|
| 100 | Allow_Outbound_22_3389 | 22,3389 | TCP | Any | Any | Allow |
| 110 | Allow_Outbound_AzureCloud | 443 | Any | Any | AzureCloud | Allow |
| 65000 | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowInternetOutBound | Any | Any | Any | Internet | Allow |
| 65500 | DenyAllOutBound | Any | Any | Any | Any | Deny |

<https://docs.microsoft.com/en-us/azure/bastion/bastion-nsg>

Azure Bastion – Pricing & SLA

- In all regions same pricing
- Euro: $0,081\text{€ per hour} \times 730 \text{ hours} = 116,97\text{€}$
- \$ $0,095\$ \text{ per hour} \times 730 \text{ hours} = 138,70\$$
- SLA: Azure Bastion will be available at least 99.95%

Azure Bastion - Summary

Pro

- Easy to deploy
- Secure your VNET
- Forget Jumpshosts
- Can see and manage connections

Contra

- Need an own subnet
- Region availability
- Doesn't support multi keystrings
- No file copy inside the remote session

Additional Details

- VNET Peering is coming (Planned availability end of 2020)
- More regions coming soon (Germany West Central end of 2020)
- Alternative to Azure Bastion?
 - Azure VPN Gateway with P2S Connection and Azure AD authentication
- Check Azure Private Link for secure connection to PaaS

Azure Bastion – Links

- Azure Bastion Documentation Microsoft Docs
 - <https://azure.microsoft.com/en-us/services/azure-bastion/>
- What is Azure Bastion
 - <https://docs.microsoft.com/en-us/azure/bastion/bastion-overview>
- Azure Bastion Feedback
 - <https://feedback.azure.com/forums/217313-networking?query=bastion>
- Secure Azure Bastion Subnet
 - <https://docs.microsoft.com/en-us/azure/bastion/bastion-nsg>
- Blog Article about Azure Bastion
 - <https://www.reimling.eu/2020/01/azure-bastion-how-to-secure-access-azure-vms-via-ssh-rdp-without-public-ip-or-jumphosts/>
- Azure VPN Gateway AAD authentication
 - <https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant-multi-app>
- Azure Private Link (Secure PaaS in Azure)
 - <https://www.reimling.eu/2020/06/connect-and-secure-azure-paas-services-to-virtual-networks-with-private-link/>

Q&A

Identity Summit 2020
follow @IdentitySummit
on Twitter



Thank you



@GregorReimling | @AzureBonn
www.reimling.eu | www.neutralien.com