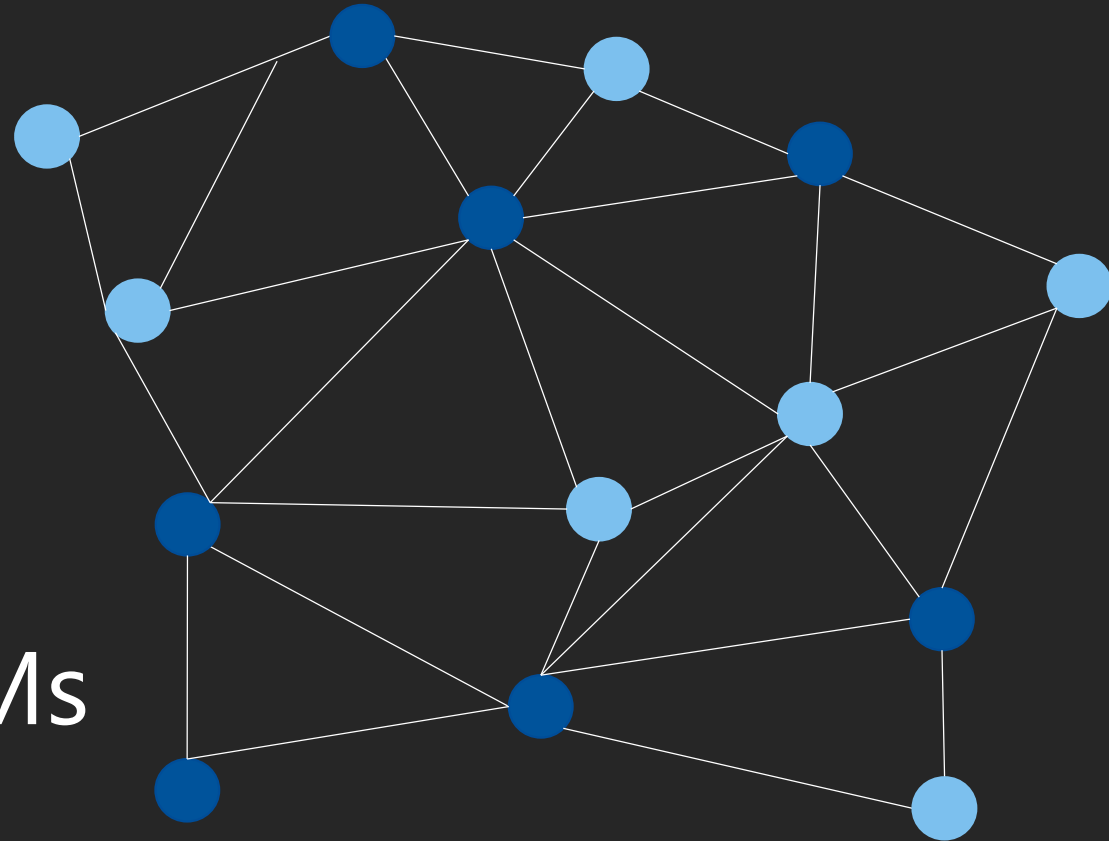


Azure Bastion – Secure access to your Azure VMs

without JumpHost or Public IP Address

by Gregor Reimling



Gregor Reimling



Cloud Consultant @Sepago



Cloud and Datacenter, Governance



Azure Infrastructure (Governance, IaaS, Security)



info@reimling.eu



@GregorReimling | @AzureBonn

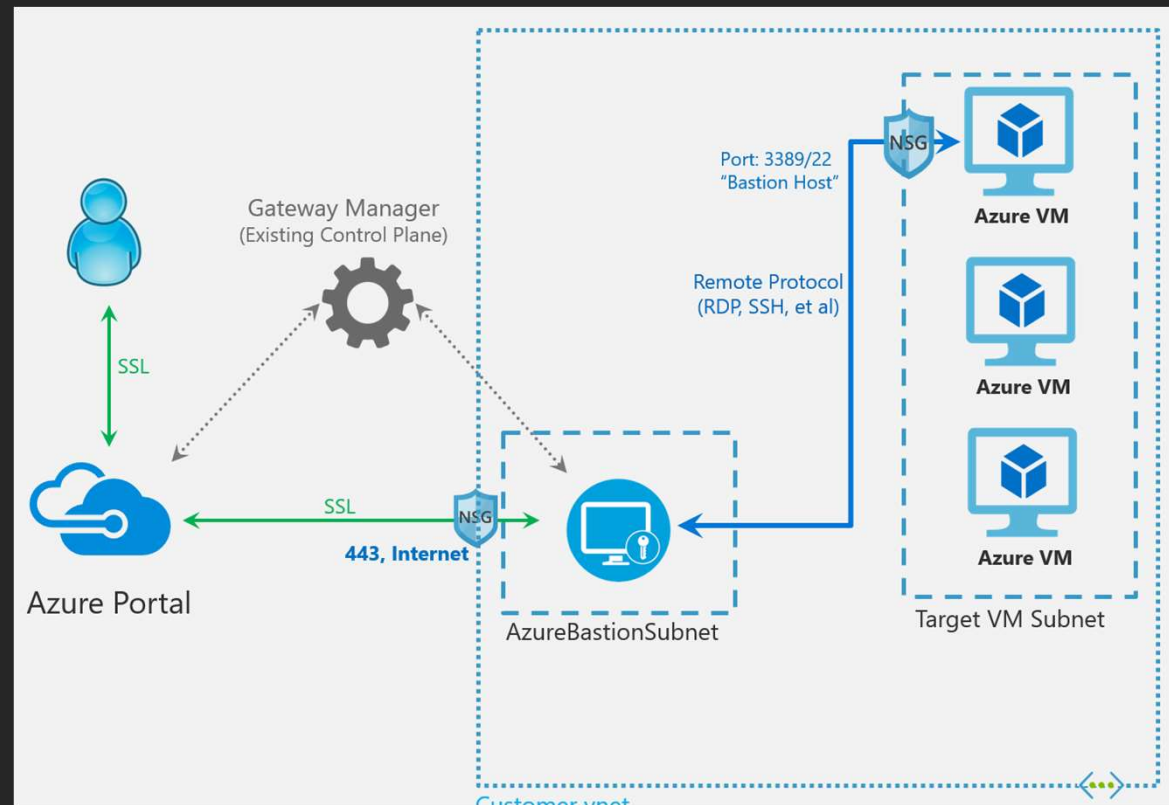


www.reimling.eu | www.neutralien.com



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



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

Azure Bastion - Demo

Dashboard > Virtual machines > AzAFSCB01

Virtual machines

AzureMechanic

+ Add

⌚ Reservations

⋮ More

Filter by name...

☐ Name ↑↓

AzAFSCB01

⋮

AzCMWDC1

⋮

AzAFSCB01

Virtual machine

Search (Ctrl+ /)

⌕

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Disks

Connect to virtual machine

AzAFSCB01

⚠ To improve security, enable just-in-time access on this VM. →

RDP

SSH

BASTION

To connect to your virtual machine over the web, enter login credentials and click connect (opens a new browser window).

☒ Open in new window

Username * ⓘ

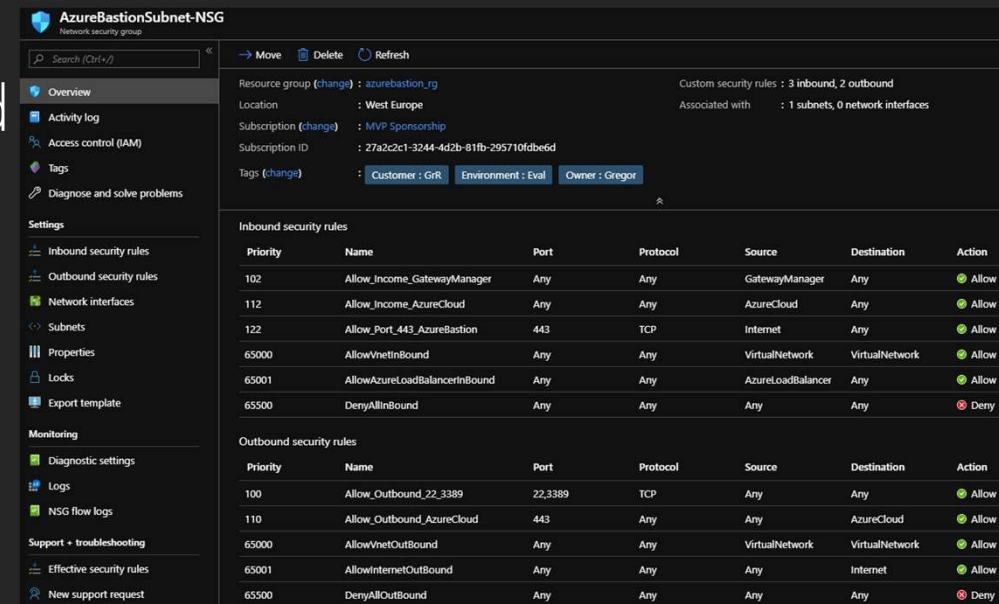
Password * ⓘ

Connect

7

Azure Bastion – Hardening

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



AzureBastionSubnet-NSG
Network security group

Resource group (change): azurebastion_rg
Location: West Europe
Subscription (change): MVP Sponsorship
Subscription ID: 27a2c2c1-3244-4d2b-81fb-295710fdb66d
Tags (change): Customer: GR, 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

Azure Bastion – Pricing & SLA

- In all regions same pricing
- Euro: $0,081\text{€ per hour} \times 730 \text{ hours} = 59,13\text{€}$
- \$ $0,095\$ \text{ per hour} \times 730 \text{ hours} = 69,35\$$
- SLA: Azure Bastion will be available at least 99.95%

Azure Bastion - Summary

Pro

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

Contra

- VNET Peering not supported
- Need an own subnet
- Doesn't support multi keystrings
- Region availability

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 (German)
 - <https://www.reimling.eu/2019/06/azure-bastion-sicherer-azure-vm-zugriff-via-ssh-rdp-ohne-public-ip/>

Thank you!



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

Feedback



Please use your form to
send us Feedback!

<http://feedback.azureaturdaycologne.de/>