



Bastion Host as a Service

Browser based RDP/SSH to your workloads anywhere

Ashish Jain

Principal Program Manager
ashish.jain@microsoft.com



Azure Bastion

Agenda

Security Aspects

Architecture

Demo

Roadmap

Security

Minimize threat surface

Role Based Access Control (RBAC)

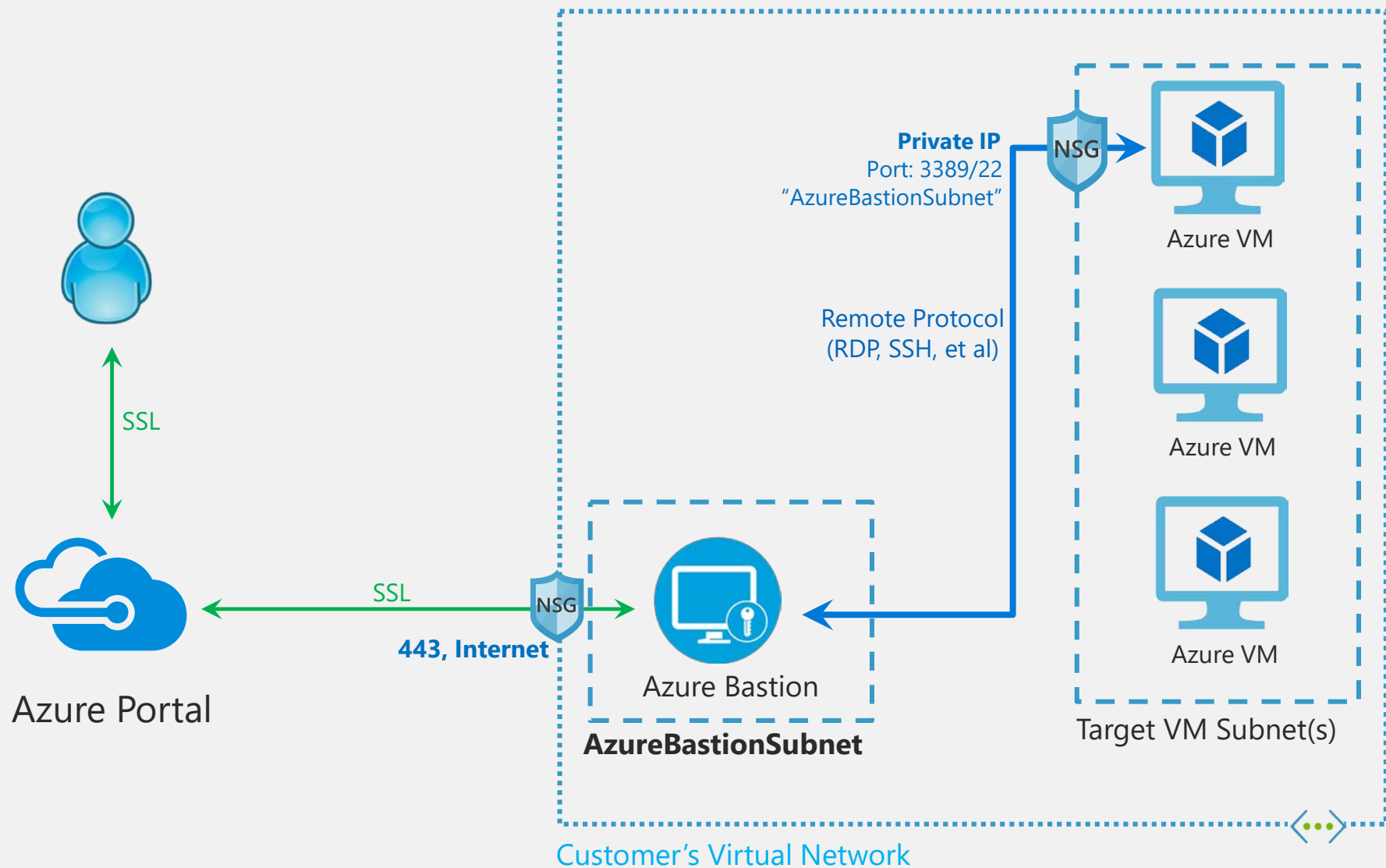
Monitoring & Auditing

- RDP/SSH traffic contained within vnet for Azure workload VMs
- Identity/Credential Management for seamless logon
 - Create and Manage ephemeral identity (identity not delivered outside Azure)
 - RBAC based portal auth required to initiate connection
 - Multi-factor/Extensible Auth
- No direct access to Workload VM for remote access (only through Bastion Host)
- Full RDP/SSH session audit

Architecture

Azure Bastion deployed in Customer's Virtual Network

- User connects to the Azure Portal using any HTML5 browser
- Select the workload to RDP/SSH
- Single-click RDP/SSH session inside the browser
- No Public IP required on the Azure VM



Demo

Preview:

#1: Access to IaaS Workloads in Virtual Networks

Future:

#2: Access to IaaS Workloads in Virtual Networks using MFA

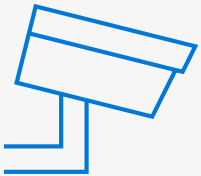
#3: Access to Workloads On-Premise/Beyond Azure

Bastion Roadmap



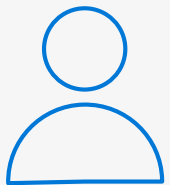
Security

- Integration with AAD with support for Multi-factor authentication
- Role Based Access Control Integration for authorizations
- SSH Key Management
- Ephemeral Identity (short-lived/temporary)
- Third Party Auth Integration through Azure Marketplace
- JIT-NSG



Monitoring

- Record RDP/SSH sessions for later viewing
- Audit – Playback recorded sessions for audit/compliance
- Live Audit – Play RDP/SSH sessions while they are in progress
- Service Logging & Diagnostics
- Session Management (force disconnect, etc.)



Experience

- Full screen Support
- Native Client Support
- Shareable URL (time bound, revoke)
- File Transfer
- Copy Paste + Richer experience
- Audio Support with RDP



Connectivity

- RDP+SSH Access over port 443 as PaaS
- Provisioned Virtual Network
- Peered Virtual Networks
- Bastion on private IP
- On-Premise workloads for RDP/SSH
- Beyond



Extensibility

- DTL Integration
- IoT, VMSS, AKS
- PowerShell
- Debugging Proxy
- Storage including SQL/DB access
- Third Party Protocol Integration through Azure Marketplace



Scalability, Performance & Availability

- On-Demand Virtual Network attach
- Auto-scale support
- Zone-Redundancy for extra resiliency

Azure Bastion is now available for preview

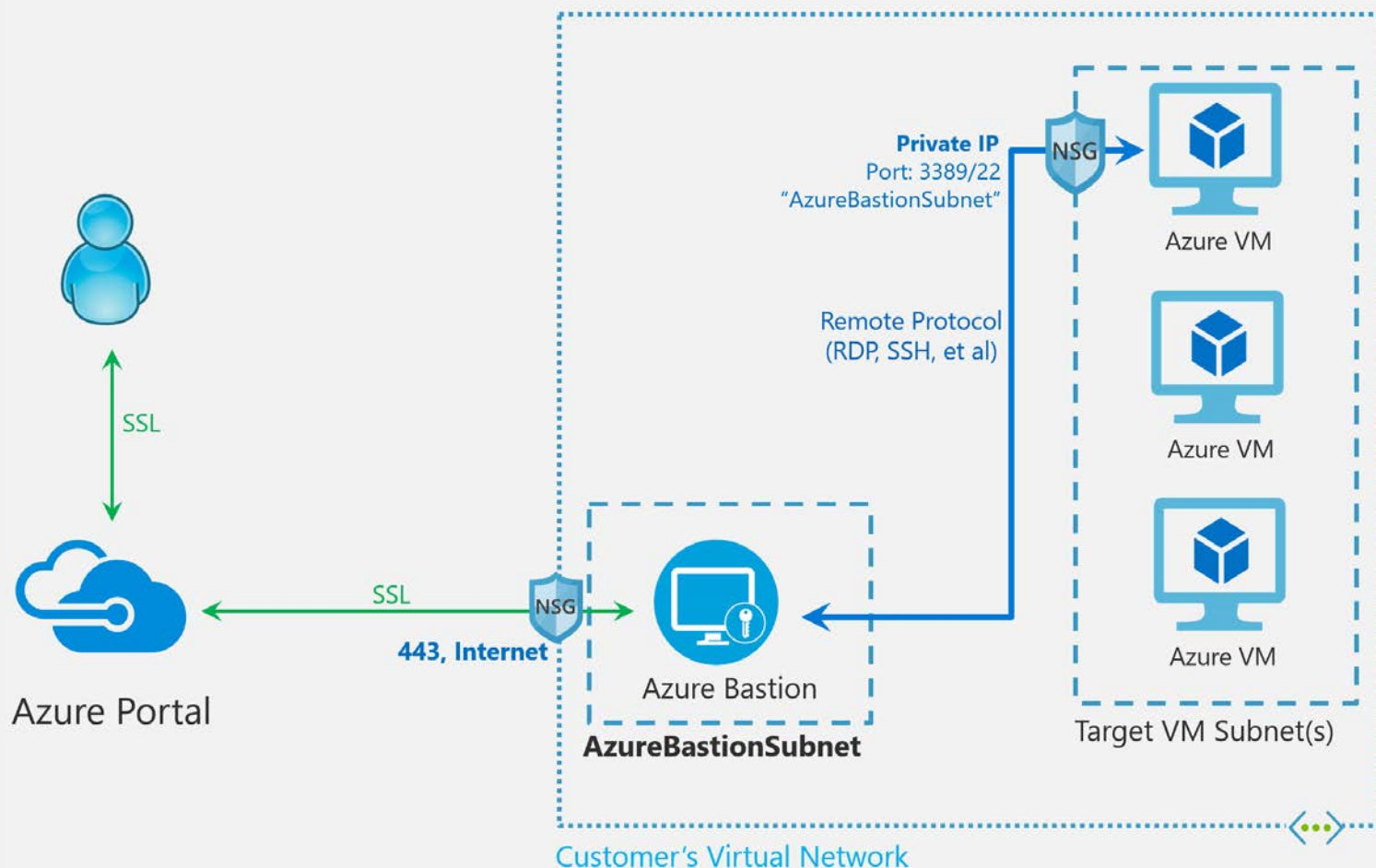
Product Page

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

Product Documentation

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

Looking forward to you trying out our preview soon and your precious feedback



Thank You