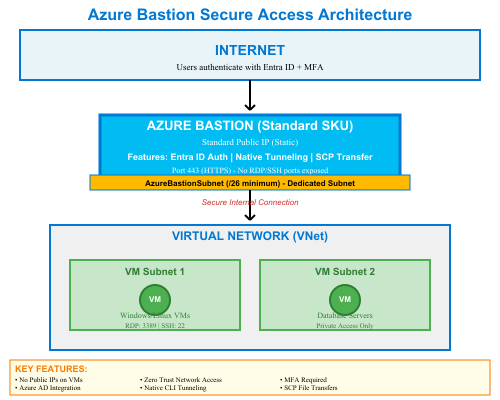
**Azure Bastion Secure Access Architecture**

*Production-Grade Remote Access with Entra ID, Native Tunneling & SCP*

# Architecture Diagram



# Executive Summary

This architecture implements Azure Bastion with Standard SKU to provide secure, seamless RDP and SSH connectivity to virtual machines without exposing them via public IP addresses. The solution integrates Entra ID (Azure AD) authentication, native client support for SSH/RDP tunneling, and secure file transfer via SCP.

# Component Overview

## Azure Bastion (Standard SKU)

Platform-as-a-Service (PaaS) that provides secure RDP/SSH connectivity

* Fully managed by Microsoft Azure
* Automatic security patches and updates
* No management overhead
* Standard SKU enables advanced features

## Standard Public IP

Static public IP address for Bastion service

* Static allocation (does not change)
* Single entry point for all connections
* Protected by Azure DDoS protection
* No direct access to VMs

## AzureBastionSubnet

Dedicated subnet required for Bastion deployment

* Minimum size: /26 (64 IP addresses)
* Must be named exactly "AzureBastionSubnet"
* Isolated from VM subnets
* Network Security Group (NSG) not required but can be configured

## Virtual Network (VNet)

Azure virtual network containing VMs and Bastion

* Contains all VM subnets
* Private IP addressing
* Network isolation and segmentation
* Can span multiple subnets

## Virtual Machines

Target Windows and Linux servers

* No public IPs required
* Private network access only
* Standard RDP (3389) and SSH (22) ports
* Protected by Network Security Groups

# Three Advanced Features (Standard SKU)

## 1. Entra ID (Azure AD) Authentication

Users authenticate using their corporate Azure AD credentials with Multi-Factor Authentication (MFA) enforcement.

* No local VM passwords to manage
* Centralized identity management
* Conditional Access policies apply
* MFA enforced for all connections
* Complete audit trail of access
* Just-in-Time (JIT) access integration

## 2. Native Client Support (SSH/RDP Tunneling)

Connect using your favorite SSH or RDP client applications instead of the browser.

* Use native Windows Remote Desktop Connection
* Use PuTTY, MobaXterm, or any SSH client
* Better performance than browser-based access
* Full client feature support (copy/paste, multiple monitors)
* CLI-based automation support
* Works with existing scripts and tools

### Example Commands:

* az network bastion ssh --name BastionHost --resource-group rg-prod \
* --target-resource-id /subscriptions/.../vm-name --auth-type AAD

## 3. SCP File Transfer Capability

Securely upload and download files to/from VMs using the SCP protocol over the Bastion tunnel.

* No need for separate file transfer solutions
* Encrypted file transfers through Bastion
* Standard SCP commands work seamlessly
* Supports large file transfers
* Bi-directional file copy
* Integrated with existing workflows

### Example Commands:

* # Create tunnel first
* az network bastion tunnel --name BastionHost --resource-group rg-prod \
* --target-resource-id /subscriptions/.../vm-name --resource-port 22 --port 50022
* # Then use SCP through the tunnel
* scp -P 50022 localfile.txt user@localhost:/remote/path/

# Why This Architecture is Excellent

## Security Excellence

**Zero Trust Network Access** - No public IPs on VMs eliminates attack surface

**Defense in Depth** - Multiple layers: Azure AD, MFA, Bastion, NSG, private networking

**Compliance Ready** - Meets SOC 2, ISO 27001, HIPAA, PCI DSS requirements

**Audit Trail** - Complete logging of all connection attempts and activities

**Encrypted Transit** - All traffic uses TLS 1.2+ encryption

**No Credential Exposure** - Passwords never transmitted; Azure AD tokens only

**Automatic Threat Protection** - Azure DDoS protection on public IP

**Session Recording** - Optional session recording for compliance

## Operational Excellence

**Zero Management Overhead** - Fully managed PaaS, no VM management

**Automatic Updates** - Microsoft handles all patches and updates

**High Availability** - Built-in redundancy with 99.95% SLA

**Scalability** - Handles thousands of concurrent connections

**Cost Effective** - Flat hourly rate, no per-user licensing

**Quick Deployment** - 10-15 minutes from script to production

**Disaster Recovery** - Multi-region deployment supported

**Monitoring** - Integrated with Azure Monitor and Log Analytics

## User Experience Excellence

**Single Sign-On** - Users authenticate once with corporate credentials

**Native Tools** - Use familiar RDP and SSH clients

**Performance** - Direct connection, minimal latency

**Reliability** - No VPN required, works from anywhere

**Simplicity** - One-click access from Azure Portal

**Mobile Support** - Access from tablets and mobile devices

**File Transfer** - SCP support eliminates need for separate tools

**Copy/Paste** - Full clipboard integration

## Business Excellence

**Reduced Attack Surface** - 70-80% reduction in potential entry points

**Compliance Acceleration** - Simplifies audits and certifications

**Cost Optimization** - Eliminates VPN infrastructure costs

**Productivity** - Faster access, fewer support tickets

**Risk Reduction** - Eliminates password-related breaches

**Scalability** - Supports growth without infrastructure changes

**Vendor Trust** - Microsoft-managed service with enterprise SLA

**Future-Proof** - Regular feature updates from Microsoft

## Technical Excellence

**Standard SKU** - Enterprise-grade features and performance

**Network Isolation** - Dedicated subnet with controlled access

**Protocol Support** - RDP, SSH, and SCP in single solution

**Azure AD Integration** - Leverage existing identity infrastructure

**Conditional Access** - Apply location, device, risk-based policies

**JIT Access** - Integrate with Privileged Identity Management

**Automation Ready** - Full Azure CLI and PowerShell support

**Multi-Region** - Deploy across regions for global access

# Deployment Checklist

## Prerequisites

* Azure subscription with Contributor or Owner role
* Az PowerShell modules installed
* Virtual Network already created
* Resource Group already created

## Network Planning

* Identify VNet for Bastion deployment
* Plan Bastion subnet (/26 or larger)
* Verify no subnet named "AzureBastionSubnet" exists
* Document VM subnets that need Bastion access

## Deployment Steps

* Run Deploy-Bastion-VM.ps1 script
* Select target subscription
* Provide Resource Group name
* Provide Virtual Network name
* Wait 10-15 minutes for deployment
* Verify Public IP assignment
* Test browser-based connection
* Test native client connection

## Post-Deployment

* Configure Network Security Group rules if needed
* Set up Azure Monitor alerts
* Enable diagnostic logging
* Configure Bastion resource logs
* Test SCP file transfers
* Document connection procedures
* Train users on access methods
* Update runbooks and documentation

# Connection Methods Reference

## Method 1: Azure Portal (Browser-Based)

1. 1. Navigate to Azure Portal
2. 2. Go to Virtual Machines
3. 3. Select target VM
4. 4. Click "Connect" button
5. 5. Select "Bastion"
6. 6. Enter credentials or use Azure AD
7. 7. Connect in new browser tab

## Method 2: Native SSH Client (Linux/Mac)

Using Azure CLI to create SSH tunnel:

* az network bastion ssh \
* --name BastionHost \
* --resource-group rg-production \
* --target-resource-id /subscriptions/xxx/resourceGroups/rg-production/providers/Microsoft.Compute/virtualMachines/vm-linux-01 \
* --auth-type AAD

## Method 3: Native RDP Client (Windows)

Create RDP tunnel then connect:

* az network bastion tunnel \
* --name BastionHost \
* --resource-group rg-production \
* --target-resource-id /subscriptions/xxx/resourceGroups/rg-production/providers/Microsoft.Compute/virtualMachines/vm-windows-01 \
* --resource-port 3389 \
* --port 3389

Then connect using Remote Desktop Connection to: localhost:3389

## Method 4: SCP File Transfer

Step 1: Create SSH tunnel (port 50022):

* az network bastion tunnel \
* --name BastionHost \
* --resource-group rg-production \
* --target-resource-id /subscriptions/xxx/.../vm-name \
* --resource-port 22 \
* --port 50022

Step 2: Use SCP through tunnel:

* # Upload file
* scp -P 50022 local-file.txt azureuser@localhost:/home/azureuser/
* # Download file
* scp -P 50022 azureuser@localhost:/home/azureuser/remote-file.txt .

# Troubleshooting Guide

## Bastion deployment fails

* Verify subnet is at least /26
* Ensure subnet name is exactly "AzureBastionSubnet"
* Check subscription has available quota
* Verify no conflicting NSG rules

## Cannot connect to VM

* Verify VM is running
* Check NSG allows RDP (3389) or SSH (22)
* Verify Bastion and VM are in same VNet
* Ensure user has appropriate RBAC permissions
* Check VM has network connectivity

## Native client connection fails

* Verify using Standard SKU (not Basic)
* Update Azure CLI to latest version
* Check firewall allows outbound 443
* Verify Azure AD authentication is configured
* Ensure user has "Virtual Machine Administrator Login" role

## SCP transfer fails

* Verify tunnel is still active
* Check SSH service running on VM
* Verify correct port (usually 50022)
* Ensure proper file permissions
* Check disk space on target VM

# Cost Analysis

Azure Bastion pricing is straightforward and cost-effective compared to alternative solutions.

## Pricing Model

|  |  |  |
| --- | --- | --- |
| **Component** | **Cost** | **Notes** |
| Azure Bastion Standard SKU | $0.19/hour | Flat rate, no per-user fees |
| Standard Public IP | $0.005/hour | Static IP included |
| Outbound Data Transfer | $0.087/GB | Standard Azure rates |
| Monthly Base Cost | ~$140/month | 730 hours × $0.19 |

## Cost Comparison

### Traditional VPN Gateway

* Base cost: $150-$500/month
* Additional per-user licenses
* VPN client software costs
* Management overhead
* Total: $300-$800/month

### Jump Box / Bastion Host VM

* VM cost: $50-$200/month
* Public IP: $3.65/month
* Management time: 10-20 hours/month
* Security patching overhead
* Total: $100-$500/month + labor

### Azure Bastion Standard

* Base cost: $140/month
* No per-user fees
* Zero management overhead
* Automatic updates
* Total: $140/month

## ROI Analysis

Azure Bastion typically provides positive ROI within 1-3 months through:  
  
• Eliminated VPN infrastructure costs  
• Reduced security incident costs  
• Decreased management overhead (20-40 hours/month saved)  
• Faster troubleshooting and support  
• Reduced compliance audit costs  
• Lower training costs (simpler than VPN)

# Security Best Practices

## Identity & Access

* Enforce MFA for all users
* Use Conditional Access policies
* Implement Just-in-Time (JIT) access
* Regular access reviews
* Use Azure AD groups for permissions
* Enable Privileged Identity Management (PIM)

## Network Security

* Keep Bastion subnet isolated
* Configure NSG rules appropriately
* Enable Azure DDoS Protection
* Use Azure Firewall for additional filtering
* Implement network monitoring
* Regular security assessments

## Monitoring & Logging

* Enable diagnostic logs
* Send logs to Log Analytics workspace
* Set up Azure Monitor alerts
* Monitor connection attempts
* Track authentication failures
* Regular log review and analysis

## Compliance & Governance

* Use Azure Policy for enforcement
* Regular compliance audits
* Document all configurations
* Maintain change logs
* Regular security training
* Incident response procedures

Azure Bastion Architecture Documentation  
*Generated by Deploy-Bastion-VM.ps1  
Professional Azure Automation Scripts*