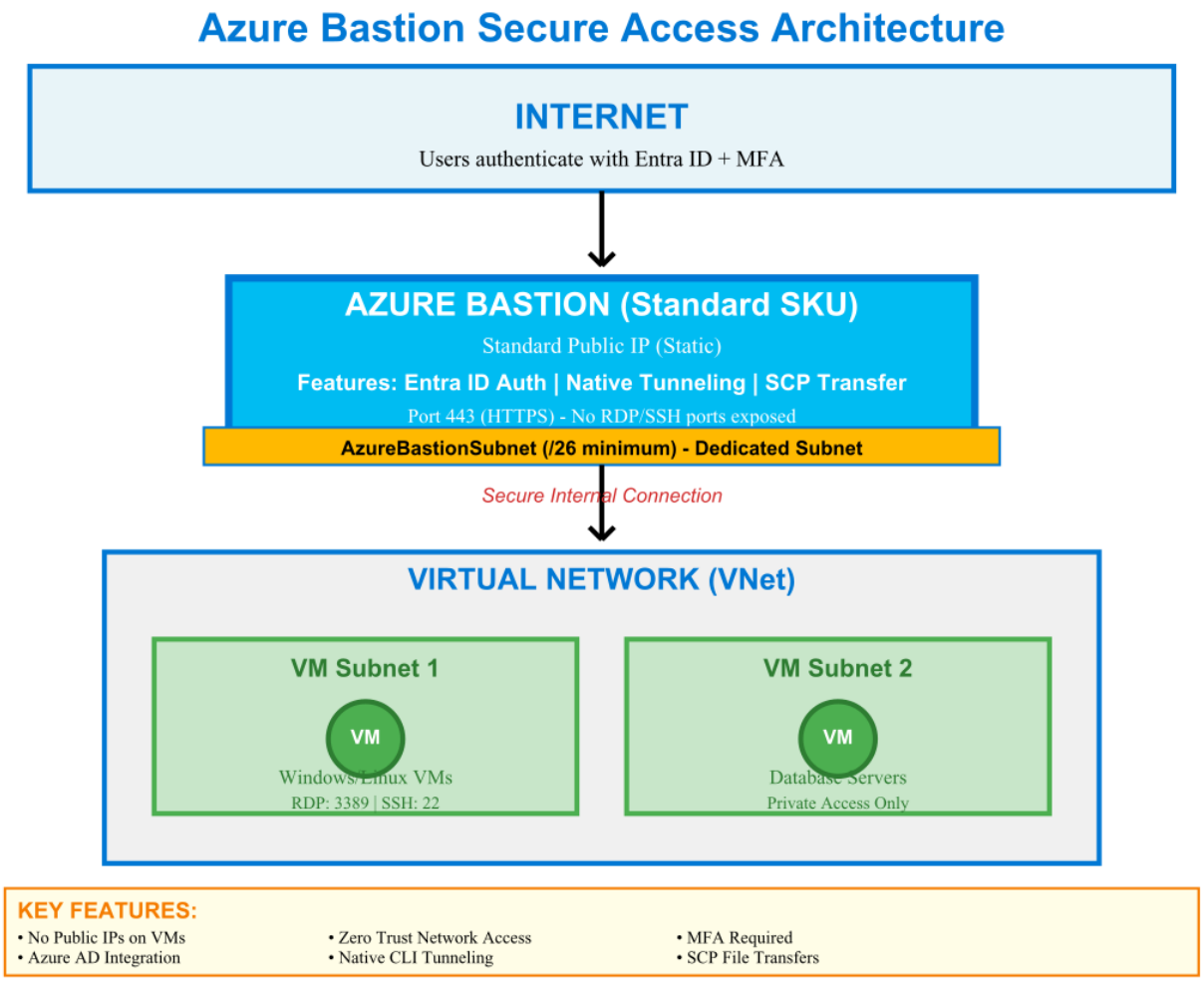
Azure Bastion Secure Access Architecture

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.

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

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

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

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

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

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

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

Cost Analysis

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

Component	Cost	Notes
Bastion Standard SKU	$0.19/hour	Flat rate, no per-user fees
Standard Public IP	$0.005/hour	Static IP included
Monthly Base Cost	~$140/month	730 hours × $0.19

Azure Bastion Architecture Documentation

Generated by Deploy-Bastion-VM.ps1

Professional Azure Automation Scripts