**Azure Bastion with Service Principal and Key Vault Integration**

**Business Case for Management**

Prepared: October 2025

Purpose: Secure Remote Access Architecture Recommendation

# Contents

[Contents 1](#_Toc212468376)

[Executive Summary 1](#_Toc212468377)

[Solution Components 1](#_Toc212468378)

[Azure Bastion 1](#_Toc212468379)

[Business Value 1](#_Toc212468380)

[Service Principal Authentication 1](#_Toc212468381)

[Business Value 1](#_Toc212468382)

[Azure Key Vault Integration 1](#_Toc212468383)

[Business Value 1](#_Toc212468384)

[Architecture Benefits 1](#_Toc212468385)

[Security Advantages 1](#_Toc212468386)

[Eliminated Attack Vectors: 1](#_Toc212468387)

[Defense in Depth: 1](#_Toc212468388)

[Compliance and Governance 1](#_Toc212468389)

[Audit and Compliance: 1](#_Toc212468390)

[Access Control: 1](#_Toc212468391)

[Operational Efficiency 1](#_Toc212468392)

[Reduced Complexity: 1](#_Toc212468393)

[Cost Optimization: 1](#_Toc212468394)

[Use Cases 1](#_Toc212468395)

[Automated Deployment Pipelines 1](#_Toc212468396)

[Maintenance and Administration 1](#_Toc212468397)

[Third-Party Vendor Access 1](#_Toc212468398)

[Disaster Recovery Operations 1](#_Toc212468399)

[Risk Mitigation 1](#_Toc212468400)

[Implementation Considerations 1](#_Toc212468401)

[Prerequisites 1](#_Toc212468402)

[Timeline 1](#_Toc212468403)

[Costs 1](#_Toc212468404)

[Compliance Benefits 1](#_Toc212468405)

[Recommendations 1](#_Toc212468406)

[Immediate Actions: 1](#_Toc212468407)

[Ongoing: 1](#_Toc212468408)

[Conclusion 1](#_Toc212468409)

[Questions & Contact 1](#_Toc212468410)

[References 1](#_Toc212468411)

[Azure Bastion Documentation 1](#_Toc212468412)

[Azure Key Vault Documentation 1](#_Toc212468413)

[Service Principal Security and Best Practices 1](#_Toc212468414)

[Compliance and Regulatory Frameworks 1](#_Toc212468415)

[Additional Industry Resources 1](#_Toc212468416)

# Executive Summary

This document outlines the business and security rationale for implementing Azure Bastion with service principal authentication, utilizing Azure Key Vault for credential management. This architecture provides secure, auditable remote access to Azure virtual machines while eliminating common security vulnerabilities and reducing operational overhead.

**Key Benefits:**

* Eliminates public IP exposure on virtual machines
* Removes direct SSH/RDP access vulnerabilities
* Centralizes credential management with enterprise-grade security
* Provides complete audit trails for compliance
* Reduces attack surface by 90%+

# Architecture Overview

The Azure Bastion architecture provides a secure pathway for administrative access without exposing virtual machines to the public internet. The following diagram illustrates the connection flow:

**Architecture Flow Diagram:**

## Key Architecture Points

Network Isolation: Virtual machines remain on private subnets with no public IP addresses. Azure Bastion acts as a secure gateway within the virtual network.

Dedicated Subnet: Bastion requires a dedicated subnet named 'AzureBastionSubnet' with a minimum size of /26. This subnet is used exclusively for the Bastion service.

Connection Methods: Users can connect via browser through Azure Portal or use native SSH/RDP clients with Azure CLI tunneling commands. All connections are authenticated through Entra ID.

Network Security Groups: NSG rules control traffic to and from the Bastion subnet. Only necessary ports are opened, and all traffic is logged for audit purposes.

## Ports and Protocols Summary

# Solution Components

## Azure Bastion

Azure Bastion is a fully managed PaaS service that provides secure RDP and SSH connectivity to virtual machines directly through the Azure portal over SSL, without exposing VMs to the public internet.

### Business Value

* No public IP addresses are required on VMs
* Protection against port scanning and brute force attacks
* Seamless integration with Azure security controls
* Zero infrastructure maintenance overhead

### Enhanced Features (Standard SKU)

#### Entra ID (Azure AD) Authentication

Azure Bastion integrates directly with Entra ID (formerly Azure AD) to provide enterprise-grade authentication. Users authenticate with their corporate credentials and multi-factor authentication (MFA) is enforced automatically. This eliminates the need to manage separate VM passwords and ensures all access attempts are validated against organizational identity policies.

#### Native Client Support (Tunneling)

The Standard SKU enables tunneling capabilities, allowing connections through native SSH and RDP clients instead of only browser-based access. This is accomplished using Azure CLI to create secure tunnels to target VMs. This feature is critical for automation scripts, DevOps workflows, and users who prefer traditional remote desktop tools over web-based connections.

#### SCP File Transfer Capability

Secure Copy Protocol (SCP) support enables file transfers to and from VMs through the Bastion tunnel. This is essential for deploying scripts, uploading configurations, and retrieving reports without requiring separate file transfer infrastructure. Files are transferred over the encrypted Bastion connection, maintaining security while enabling operational flexibility.

## Service Principal Authentication

A service principle is an identity created for use with applications, hosted services, and automated tools to access Azure resources. Unlike user accounts, service principals provide:

### Business Value

* Non-interactive authentication for automated processes
* Granular permission control at the resource level
* Eliminates shared credential usage
* Enables role-based access control (RBAC)
* Facilitates automation and DevOps workflows

## Azure Key Vault Integration

Azure Key Vault provides centralized, hardware-secured storage for secrets, keys, and certificates with comprehensive access policies and audit logging.

### Business Value

* Hardware Security Module (HSM) backed encryption
* Eliminates hardcoded credentials in code or configuration
* Automatic secret rotation capabilities
* Complete audit logging of all secret access
* Compliance with SOC, ISO, PCI-DSS standards

# Architecture Benefits

## Security Advantages

### Eliminated Attack Vectors:

* No public IP addresses exposed to internet
* No open RDP (3389) or SSH (22) ports
* No credential storage in plain text or configuration files
* Protection against credential theft from compromised systems

### Defense in Depth:

* Multiple layers of authentication and authorization
* Network segmentation without complexity
* Encrypted connections end-to-end
* Just-in-time access capabilities

## Compliance and Governance

### Audit and Compliance:

* Complete audit trail of all access attempts
* Centralized logging for SIEM integration
* Demonstrates due diligence for regulatory requirements
* Supports compliance frameworks: SOC 2, HIPAA, PCI-DSS, GDPR

### Access Control:

* Principle of least privilege enforcement
* Time-bound access permissions
* Automated access reviews through Azure AD
* Immediate credential revocation capabilities

## Operational Efficiency

### Reduced Complexity:

* No VPN infrastructure to maintain
* No jump box or bastion host servers to patch and manage
* Simplified network security group rules
* Reduced firewall management overhead

### Cost Optimization:

* Eliminates need for dedicated bastion host VMs
* Reduces public IP address costs
* Decrease in security incident response costs
* Lower administrative overhead

# Use Cases

## Automated Deployment Pipelines

Service principals authenticate deployment tools to execute remote commands on VMs through Bastion without exposing credentials in CI/CD pipelines.

## Maintenance and Administration

IT teams access production systems securely without VPN connections or public internet exposure, with all actions logged for audit.

## Third-Party Vendor Access

Temporary service principal credentials can be issued to vendors with automatic expiration, eliminating long-lived shared passwords.

## Disaster Recovery Operations

Automated DR scripts can authenticate securely to execute recovery procedures without hardcoded credentials.

# Risk Mitigation

| **Traditional Approach Risk** | **This Architecture Mitigation** |
| --- | --- |
| Public RDP/SSH exposure | Zero public exposure via Bastion |
| Credential theft from config files | Credentials never stored locally |
| Untracked admin access | Complete audit logs in Azure Monitor |
| Shared password usage | Individual service principles per use case |
| No credential rotation | Automated rotation via Key Vault |
| VPN infrastructure vulnerabilities | No VPN required |

# Implementation Considerations

## Prerequisites

* Azure subscription with appropriate permissions
* Virtual machines deployed in Azure Virtual Network
* Azure Key Vault instance
* Service principal creation rights

## Timeline

*An Example Scenario not based on actual Production*

* Initial setup: 2-4 hours
* Testing and validation: 4-8 hours
* Documentation and training: 4 hours
* Total implementation: 1-2 days

## Costs

*An Example Scenario not based on actual Production*

* Azure Bastion: ~$140/month per deployment
* Key Vault: $0.03 per 10,000 operations (minimal)
* ROI: Eliminates need for dedicated bastion VMs, VPN infrastructure, and reduces security incident costs

# Compliance Benefits

This architecture directly supports compliance requirements for:

* NIST Cybersecurity Framework: Secure credential management and access control
* CIS Controls: Controlled use of administrative privileges
* ISO 27001: Access control and cryptographic controls
* PCI-DSS: Requirement 8 (Identify and authenticate access)
* SOC 2 Type II: Security and availability controls

# Recommendations

## Immediate Actions:

* Approve implementation of Azure Bastion for production environments
* Establish service principal naming and governance standards
* Configure Key Vault with appropriate access policies
* Implement monitoring and alerting for access patterns

## Ongoing:

* Review service principal permissions quarterly
* Rotate service principal credentials every 90 days
* Conduct access reviews monthly
* Monitor Azure Monitor logs for anomalous access patterns

# Conclusion

Implementing Azure Bastion with service principal authentication and Key Vault credential management represents the best security practices for cloud infrastructure access. This architecture eliminates critical attack vectors, ensures compliance with regulatory requirements, and reduces operational overhead while providing complete visibility into system access.

The investment in this architecture pays immediate dividends through reduced security risk, simplified operations, and demonstrated compliance posture.

**Recommendation: Proceed with implementation for all production Azure environments.**

# Questions & Contact

For technical questions or implementation planning, please contact the Cloud Security and Infrastructure team.

# References

This document is based on official Microsoft Azure documentation, industry best practices, and compliance frameworks. The following sources were consulted in the preparation of this business case:

## Azure Bastion Documentation

* Microsoft Learn. "About Azure Bastion." Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/bastion/bastion-overview
* Microsoft Learn. "Azure Bastion Configuration Settings." Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/bastion/configuration-settings
* Microsoft Azure. "Azure Bastion Product Overview." https://azure.microsoft.com/en-us/products/azure-bastion
* Microsoft Learn. "Azure Bastion FAQ." Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/bastion/bastion-faq
* Microsoft Learn. "Connect to a Windows VM using RDP Azure Bastion." https://learn.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows

## Azure Key Vault Documentation

* Microsoft Learn. "Azure Key Vault Security Overview." Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/key-vault/general/security-features
* Microsoft Learn. "Azure Key Vault Overview." Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/key-vault/general/overview
* Microsoft Azure. "Key Vault Product Overview." https://azure.microsoft.com/en-us/products/key-vault/
* Microsoft Learn. "Best Practices for Using Azure Key Vault." Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/key-vault/general/best-practices
* Microsoft Learn. "What is Azure Key Vault?" Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/key-vault/general/basic-concepts
* Microsoft Learn. "Secure Your Azure Key Vault." Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/key-vault/general/secure-key-vault
* Microsoft Learn. "Azure Security Baseline for Key Vault." https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/key-vault-security-baseline

## Service Principal Security and Best Practices

* Microsoft Learn. "Securing Service Principals in Microsoft Entra ID." Microsoft Entra Documentation. https://learn.microsoft.com/en-us/entra/architecture/service-accounts-principal
* Microsoft Learn. "Security Best Practices for Application Properties." Microsoft Identity Platform. https://learn.microsoft.com/en-us/entra/identity-platform/security-best-practices-for-app-registration
* Microsoft Learn. "Best Practices for Azure RBAC." Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/role-based-access-control/best-practices
* Gerber, Marco. "Securing Service Principals in Azure." marcogerber.ch, January 2025. https://marcogerber.ch/securing-service-principals-in-azure/

## Compliance and Regulatory Frameworks

* Microsoft Learn. "Azure Compliance Documentation." Microsoft Azure. https://learn.microsoft.com/en-us/azure/compliance/
* Microsoft Learn. "PCI DSS Azure Compliance." Microsoft Azure Documentation. https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-pci-dss
* Microsoft Learn. "Azure Compliance Offerings." Microsoft Documentation. https://learn.microsoft.com/en-us/compliance/regulatory/offering-home
* Aqua Security. "Azure Compliance: Standards, Tools, and 6 Critical Best Practices." October 2024. https://www.aquasec.com/cloud-native-academy/cloud-compliance/azure-compliance/
* Tigeara. "Azure PCI Compliance: A Quick Guide for Cloud Users." May 2024. https://www.tigera.io/learn/guides/pci-compliance/azure-pci-compliance/
* Microsoft Learn. "Regulatory Compliance Details for HIPAA HITRUST Azure Policy." https://learn.microsoft.com/en-us/azure/governance/policy/samples/hipaa-hitrust

## Additional Industry Resources

* CrowdStrike. "5 Best Practices for Securing Azure Resources." April 2025. https://www.crowdstrike.com/en-us/blog/azure-security-best-practices/
* Varonis. "The Complete Azure Compliance Guide: HIPAA, PCI, GDPR, CCPA." June 2023. https://www.varonis.com/blog/azure-compliance

|  |
| --- |
| **User / Administrator** |
| ↓ HTTPS Port 443 |
| **Azure Portal / Azure CLI** |
| ↓ Secure TLS Connection |
| **Azure Bastion Service (AzureBastionSubnet)** |
| ↓ RDP Port 3389 / SSH Port 22 |
| **Virtual Machine (Private IP Only)** |

|  |  |  |
| --- | --- | --- |
| **Connection** | **Port** | **Protocol** |
| User to Portal | 443 | HTTPS |
| Bastion to Windows VM | 3389 | RDP |
| Bastion to Linux VM | 22 | SSH |