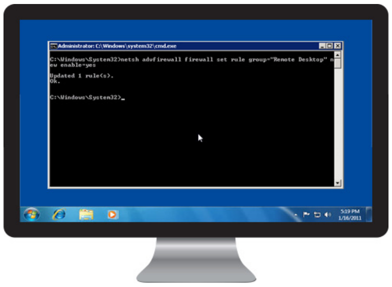
SSH Key Manager™

Secure, manage, monitor and control access to SSH keys in accordance with organizational policies.



```
C:\Windows\System32>netsh advfirewall firewall set rule group="Remote Desktop" n
ew enable=yes

Updated 1 rule(s).
Ok.


C:\Windows\System32>_
```

SSH Key Manager enables organizations to prevent unauthorized access to privileged accounts in Unix/ Linux environments and reduce the risk of a data breach.

Why CyberArk?

CyberArk is the trusted expert in helping organizations stop the most critical cyber-attacks before they stop the business.

The Challenge

SSH keys are commonly used as a means of authentication within enterprise IT environments, protecting user access to privileged accounts and verifying trust in automated application to application communications. Thanks to their ease of use and reliability, SSH keys have become an authentication method of choice for IT administrators, but when not managed properly, these keys can pose major security risks to the business.

The challenge with SSH is that there is no inherent oversight for key pairs, and once created, key pairs never expire. In effect, SSH keys, which provide privileged account access to users and applications, can be generated, distributed and never thought of again. As a result, many organizations tend to overlook these powerful credentials when building a privileged account security strategy. By leaving SSH keys unmanaged and unsecured, and failing to treat them as the privileged credentials they truly are, organizations will face a number of significant challenges, including:

- **Increased risk of data breach due to compromised keys.** Without centralized storage and access control policies, private SSH key files can be lost, stolen or shared with unauthorized users. As a result, malicious or curious users can easily gain possession of private SSH keys and use them to access critical systems and sensitive data, all while going unnoticed by the security team.
- **Failed audits resulting from unsecured, unmanaged privileged accounts.** Many IT organizations are required to protect, control and track access to privileged accounts. To maintain compliance with internal policies and industry regulations, organizations must secure, manage and monitor the use of SSH keys that protect privileged accounts.
- **High operational costs from manually rotating SSH keys.** Some organizations choose to manually rotate SSH keys for security or compliance purposes. However, due to the time and effort required to manually rotate and distribute key pairs across the network, these organizations can face high operational costs.

The Solution

CyberArk SSH Key Manager enables organizations to secure, rotate and control access to SSH keys in accordance with organizational policies. The solution also offers strong access controls to ensure that only authorized users are able to access private keys, as well as reporting capabilities to audit the use of keys. With CyberArk SSH Key Manager, organizations can:

Securely store private SSH keys. CyberArk SSH Key Manager enables organizations to securely store private SSH keys in the Digital Vault. Designed with security in mind, the CyberArk Digital Vault includes seven built-in layers of security, including the protection of data-at-rest and in-transit, granular access controls and segregation of duties.

Control access to private SSH keys. Granular access controls enable organizations to define which credentials each user or user group is permitted to view or access, protect access to these credentials, and hide all other unauthorized credentials from the user's view. Automated workflows can allow users to request one-time access to credentials with privileges as needed for business reasons.

Centralized policy creation and management, as well as integration with strong authentication solutions mean that organizations can go a step further to ensure that only authorized users are able to access and use these privileged credentials.

- **Automate key rotation.** By automating SSH key rotation, organizations can reduce the risk of unauthorized access to privileged accounts without burdening the IT team. CyberArk SSH Key Manager enables organizations to automatically rotate SSH key pairs in accordance with policy, as well as rotate key pairs on-demand as required. Automated distribution of public keys to target systems and storage of private keys in the Digital Vault helps organizations streamline security processes and gain operational efficiencies.
- **Report on the use of private SSH keys.** Built-in audit capabilities enable organizations to view and report on who accessed what keys, and when. By reviewing the check-out and check-in of private SSH keys, organizations can learn what systems were accessed, by whom they were accessed and how long each session lasted. Audit logs are stored in the tamper-proof Digital Vault, and reports can easily be generated and handed over to auditors to prove compliance with requirements.

Benefits

CyberArk SSH Key Manager can help organizations incorporate SSH key security and management into a broader privileged account security strategy. With CyberArk SSH Key Manager, organizations are able to:

- **Mitigate risks by strengthening privileged account security.** CyberArk SSH Key Manager enables organizations to securely store, manage and control access to private SSH keys. By better protecting these privileged credentials, organizations can prevent unauthorized access to privileged accounts and reduce the risk of a data breach.
- **Avoid penalties by meeting and proving compliance.** To comply with standards and regulations, organizations must protect all privileged accounts. By securely storing, managing and controlling access to SSH keys, organizations comply with privileged account security requirements, and built-in reporting tools help organizations expedite audit processes.
- **Improve operational efficiency by automating security processes.** The automated rotation of SSH key pairs, storage of private keys and distribution of public keys to target systems helps organizations strengthen security and meet compliance requirements without burdening the IT team. SSH Key Manager's integration into the CyberArk Shared Technology Platform enables organizations to manage a comprehensive Privileged Account Security Solution from a single platform, behind a single pane of glass.

A Comprehensive Solution

CyberArk SSH Key Manager is a component of the CyberArk Privileged Account Security Solution, a complete solution designed to secure, manage, monitor and control access to privileged account credentials, including both passwords and SSH keys. Products in the solution can be managed independently or combined for a complete privileged account security solution. CyberArk SSH Key Manager is based on the CyberArk Shared Technology Platform which delivers enterprise-class security and allows customers to deploy a single infrastructure and expand the solution to meet changing business requirements.

Specifications

Supported Platforms:

- **DNA Discovery:**
  RHEL 4-6; Solaris Intel and Solaris SPARC 9, 10, 11; SUSE 10; Fedora 18; Oracle Linux 5; CentOS 6; AIX 5.3, 6.1, 7.1; ESXi 5.0 and 5.1
- **SSH Key Security and Management:**
  RHEL 4-6; Solaris SPARC and Solaris Intel v9, v10, v11; CentOS 6; AIX 5.3, 6.1, 7.1; ESX, ESXi v5.1
- **Private Key Security:**
  Windows XP; Windows 7; Windows Vista; Windows 2008R2; Windows 2012R2

Target SSH Servers:

- OpenSSH

Private Key Formats:

- OpenSSH
- Putty
- Tectia

Encryption Algorithms:

- AES
- DSA

SSH Key Lengths:

- 1024
- 2048
- 4096
- 8192

Access and Workflow Management:

- LDAP directories
- Identity and Access Management
- Ticketing and workflow systems

Multi-lingual Portal:

- English
- French
- German
- Spanish
- Russian
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean
- Brazilian Portuguese

Authentication Methods:

- Username and Password
- RSA SecurID
- Web SSO
- RADIUS
- PKI and smartcards
- LDAP

Windows-based Authentication Monitoring:

- SIEM integration
- SNMP traps
- Email notifications