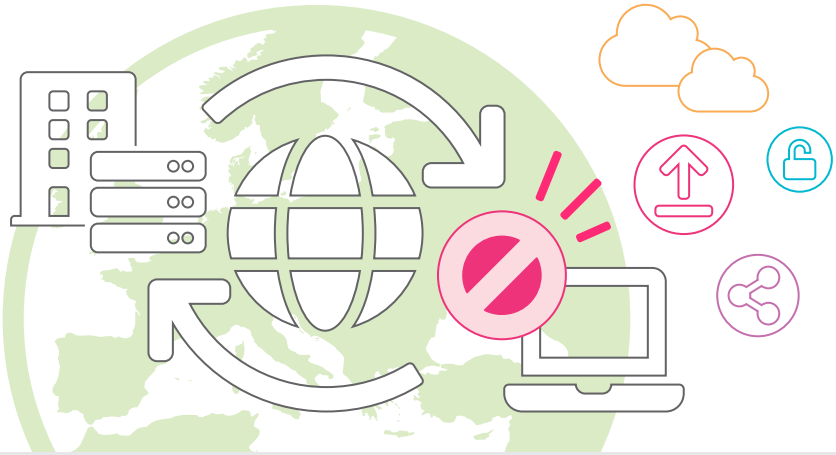
iC CONSULT



Lockdown Remote Server Access in the Enterprise

By Kevin Shannon kevin.shannon@ic-consult.com

In this case, the Customer had an existing PAM deployment, configured to manage their accounts (Windows, Linux, database… etc.). The Customer wanted to restrict all direct remote desktop protocol (RDP) & ssh access to Windows and Linux servers throughout their network, and force all employees to go through the Customer's PAM web portal for remote server access, allowing for optional session recording and auditing capabilities.

iC Consult professionals installed clustered & load-balanced bastion host/RDP gateway (session recorder) servers into the Customer's PAM deployment configuration. We locked-down Windows RDP access in the enterprise via Group Policy Object (GPO), only allowing RDP connections from the PAM bastion host servers. Linux ssh access was also restricted throughout the enterprise, only allowing ssh connections from PAM bastion host servers. All remote server RDP/ssh connections were published through the PAM solution using a delegated, role-based access model. The customer's employees were notified that all remote server access via RDP or ssh must go through the Customer's PAM web portal, and advised that they could optionally record individual RDP/ssh sessions, keystrokes, and running processes as needed. From that point forward, all remote RDP and ssh server access was effectively controlled and audited via the Customer's PAM solution.

High Level Steps:

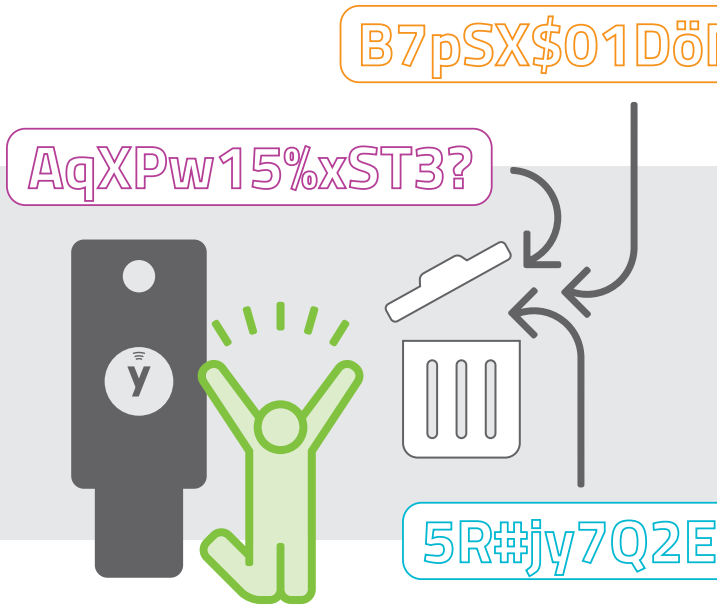
- Implement a PAM solution.
- Load balance several bastion (application session recorder) host servers, as needed for your organization.
- Shutdown Windows RDP access in the enterprise via Group Policy Object (GPO), allowing RDP connections only from PAM bastion host servers.
- Shutdown Linux ssh access throughout the enterprise, allowing ssh connections only from PAM bastion host servers.
- All remote server RDP/ssh connections are delegated through the PAM solution.
- Optionally record the sessions, keystrokes and running processes as needed.
- All Remote RDP and ssh server access effectively controlled via the PAM solution.

This is a real-world example of how iC Consult experts may enhance your PAM program.

iC CONSULT

Eliminate Passwords Using YubiKey

By Kevin Shannon kevin.shannon@ic-consult.com



In this case, the Customer used YubiKey for multi-factor authentication (MFA) enhanced logon security in their environment. The YubiKey is a hardware authentication device manufactured by Yubico to protect access to computers, networks, and online services that supports one-time passwords, public-key cryptography, and authentication, and the Universal 2nd Factor (U2F) and FIDO2 protocols developed by the FIDO Alliance.

Every employee had a YubiKey issued, and Active Directory schema was modified to accept YubiKey PIV authentication. Customer's PAM tool was installed and configured to manage the usual use case. Windows accounts, Linux accounts, AD service accounts, database accounts, and others etc. YubiKey PIV authentication was configured for access to Customer's PAM web portal. Clustered bastion host/RDP gateway (session recorder) servers were installed and added into the PAM deployment configuration.

All company applications, Windows remote desktop protocol (RDP) sessions, and ssh sessions, were configured in the PAM tool, and published based on a delegated role-based access model. When employees start their workday, they log on to their workstation using their YubiKey (no password required). The employee would subsequently log on to the Company's PAM web portal using their YubiKey (no password required). From the Company's PAM web portal, the employee could view and launch any application they need (no password required). Employees could launch any RDP or ssh server session, either auto-logged in as a designated account, or pre-authenticated using their YubiKey (no password required). Optionally, RDP and ssh sessions could be recorded, as needed.

The Customer effectively eliminated the need for employees to know, or use, passwords in the organization. If an employee lost their YubiKey, the Help Desk would be notified. The Help Desk would disable the missing YubiKey, and all Workstation access, Active Directory network access, and PAM web portal access would be disabled for that YubiKey token.

High Level Steps:

- Implement a PAM solution.
- Issue YubiKey (or other MFA/2FA) tokens to all employees.
- Enable workstation login via YubiKey (or other MFA/2FA).
- Enable MFA logon to PAM via YubiKey (or other MFA/2FA).
- Publish all applications, services, remote desktops, etc., via PAM role-based access configuration.
- Employees no longer need to know or remember passwords

This is a real-world example of how iC Consult experts may enhance your PAM program.