Next Generation Jump Servers for Industrial Control Systems

Isolation, Control and Monitoring - Learn how Next Generation Jump Servers go beyond network separation to protect your critical infrastructure and ICSs against today's advanced security threats

Table of Contents

ICS and Next Generation Jump Servers

Jump servers have emerged in recent years as a security best practice to create a separation between networks with different security requirements. Creating separation is strongly recommended to minimize the risk of a potential attacker accessing critical systems, but does the typical homegrown jump server really create a single, isolated control point? Does it really keep the attackers out? Learn how you can go the extra mile to enhance security with a next generation jump server, which closes the vulnerability holes that exist in the traditional jump server solution.

Introduction

Jump servers, also known as jump hosts, golden hosts, jump boxes or bastion hosts, emerged as a security solution to attain isolation between networks that have different security levels. The jump servers are sometimes used in addition to other security devices such as firewalls and Intrusion Detection Systems (IDS) in order to create a more secured environment which implements the Defense-In-Depth concept.

In recent years, automation networks and Industrial Control systems (ICS) are seeing an increase in the number of access points and connections to other networks, such as

- Remote maintenance and diagnostics connections from vendors
- Remote access from government entities, regulatory agencies and business partners
- Corporate users connecting for business information

The increase in the number of connections comes at a time of increased pressure in the opposite direction- to isolate the ICS and automation networks. Isolation is required due to the increased threat of a cyber attack against the ICS network. Many of the elements in the ICS networks have little to no security controls to protect them (e.g. PLC and RTUs) making them very vulnerable to cyber attacks.

In recent years we have seen the rise of sophisticated cyber attacks and as these targeted assaults continue to rise, privileged account exploitation have emerged as the primary attack vector. Privileged accounts exist everywhere – on desktops, servers, databases, SCADA devices, network devices, in the telephony system, embedded in applications – and are generally left unmanaged and unmonitored. The proliferation of privileges accounts make them a more compelling target.

Many Cyber-Security standards and regulations which were published (e.g. the NERC-CIP) in the last years have identified the need to secure privileged remote access into critical systems. In fact, the 2012 Verizon Data Breach Investigations Report ranked key logging, exploitation of default or guessable credentials and use of stolen credentials as the top threat action types identified in the breaches analyzed. All three action types are applicable in attacking a critical system by accessing it remotely after capturing credentials.

Isolation of sensitive assets is indeed a mandatory security step to control access to critical infrastructure and systems, but if your jump server solution does not create the only control point into the target server, what stops a malicious insider or external attacker from hijacking the privileged administrator password and bypassing the whole jump server solution? Should we even allow people to type in passwords that can be key-logged or hacked? And let's say they connect into the server via your existing jump server, do you have a clear view of the actions being performed or are you relying on reviewing and correlating logs to get that picture?

In this whitepaper, we review some common use cases of jump servers and reveal where vulnerabilities may still exist in the homegrown solutions e.g. customized Unix boxes or terminal servers. We go on to propose how a next generation jump server can eliminate these vulnerabilities with tighter security controls that adopt new security best practices and create a paradigm shift in the way we look at network security. The next generation jump server brings together complete isolation, control and monitoring into a single solution to truly protect the Industrial Control Systems (ICS) and other critical systems. It creates accountability as to who is accessing the critical systems without a tradeoff on security, compliance or productivity.

Jump Servers: A Secure Stepping Stone

Since the early 1990s homegrown jump servers emerged as a solution to control access between one security zone to the other. A jump server works similarly to an entrance to a highly secure building. You identify yourself and enter through one door. Only once that first door is shut, a second door opens to let you into the building.

Why Are Jump Servers Needed: Common Use Cases

Use Case 1: Separation of Networks

The most common use case for jump servers is to attain network separation (see figure 1). Network separation is necessary to create isolation between environments, monitor specific environments for regulatory needs or simply to better control who can and cannot come through the jump server to reach the target system. Jump servers will often be an additional security measure on top of implementing a firewall between environments. However, in many cases due to poor firewall management and maintenance, the multiple rules created over time in the firewall will eventually implement an "allow all" policy exposing the critical network, potentially allowing vulnerabilities to slip in and take advantage of the critical and sensitive systems.

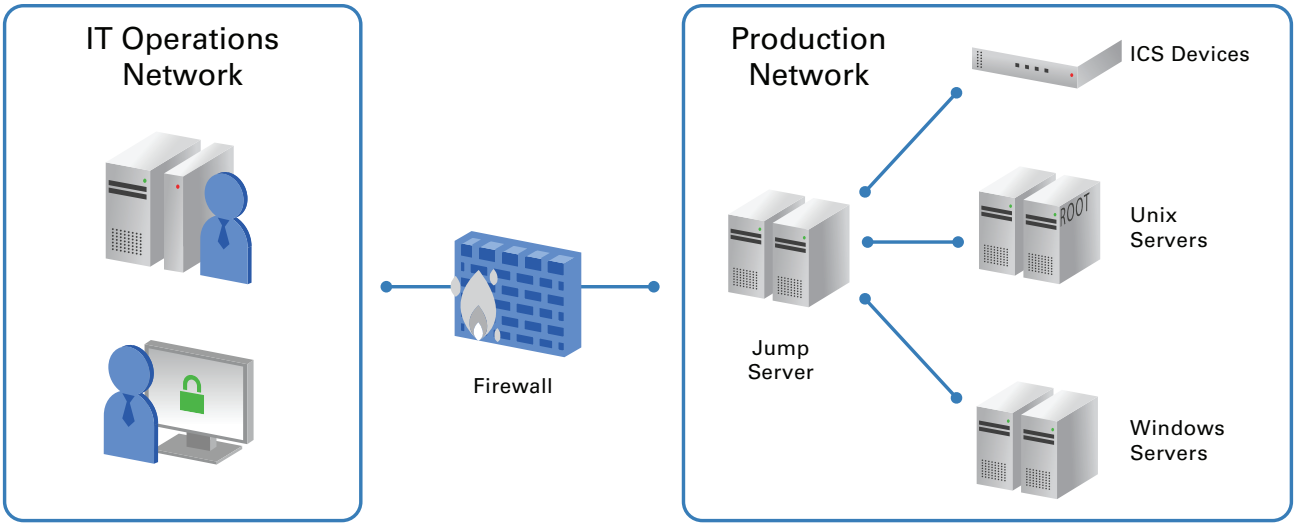

Figure 1: Use of Jump Server to Attain Network Separation

Use Case 2: A Safe Passage for Remote Vendors

Often vendors, such as system and software providers, need access to the critical internal elements for support, maintenance and remediation issues. So as not to create a direct connection into the critical network, organizations employ VPN connections to jump server environments (see figure 2). However, this raises a series of questions around whether this is really protecting the critical network as we know that the network is only as secure as the connected device. However, the organization has no control over what is installed on that device (PC) that could potentially harm the critical system. Once going through the jump server, which is connected by VPN, the remote vendor still needs to type in the privileged credential to logon to a server or a device. Do we know exactly who logged in using that credential in order to create accountability and a comprehensive audit trail? Is there an automatic or even manual process for changing that password as soon as the remote vendor completes the task at hand? Can we ensure that the external vendor can connect from the jump server only to the relevant devices or servers? Is there some kind of 'over the shoulder' monitoring capability to view what the remote vendor is doing in real-time and intervene or terminate their activity if necessary? Is the task related to a change management request or a ticket ID in the enterprise ticketing system for a full understanding and audit of what was done and why?

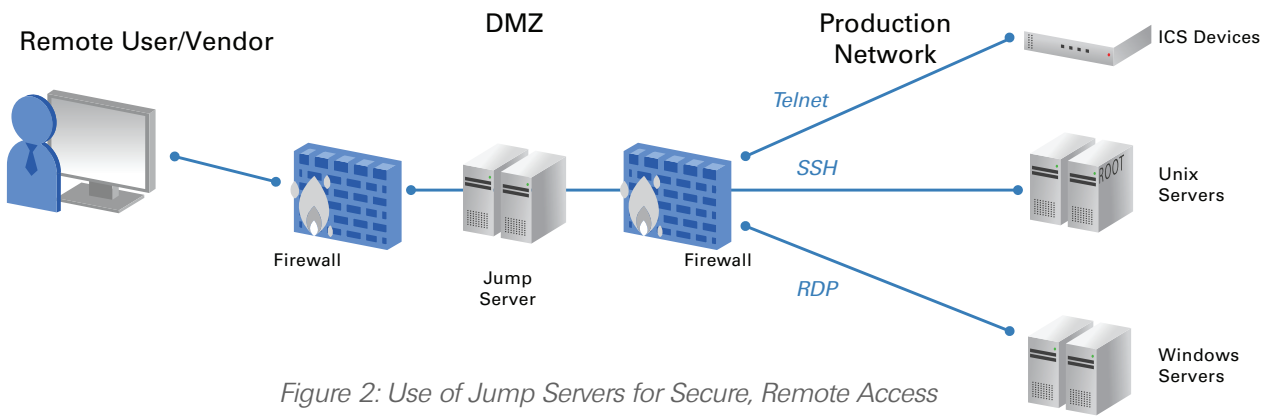

Figure 2: Use of Jump Servers for Secure, Remote Access

Use Case 3: A Central Place for Audit

By acting as the single stepping-stone into a controlled environment, jump servers also act as a central place for audit. The question of accountability, however, remains open. If people are logging in with a shared, administrator password, there is no true accountability for the actions they take, nor for the commands they run. Furthermore, there is no way to replay their full session, in video-like format for example, and only a partial list of audited events may exist for monitoring their actions.

Homegrown jump servers will not protect against a cyber attacker trying to key log or brute force an unprotected privileged server credential

10 Security 'Gotchas' With Homegrown Jump Servers

1. **True isolation is not fully achieved.** Regardless of whether a jump server exists or not, there is still a need to login to target systems using privileged credentials. If the privileged credential to the target system is known, which is the case when using a homegrown jump server, what's to stop an insider from bypassing the jump server? This makes the target system more susceptible to attack by use of key logging techniques used on the engineer/ administrator's desktop. If an attacker hijacks the password, s/he can impersonate the privileged user and connect to any critical system via the jump server. S/he can also erase logs to cover their tracks and move around the network undetected for years.

2. **No accountability of who is logging on.** If privileged accounts are not managed then it is likely that multiple users log on using a shared administrative credential when connecting through the jump server to the target system. As a result, there is no accountability as to who is using the password when it comes to forensic analysis.

3. **Access cannot be video recorded for playback.** To review what happened in a privileged session on a server that was routed through a jump server, there is a need to sift through an exhaustive list of logs (if available) which do not always correlate or give a full, in-context picture. What if you need real-time monitoring since a remote vendor needs access and you want to watch him as if it were 'over the shoulder'?

4. **Platform support is limited**. Traditional jump servers typically support only one or two platforms e.g. Windows / Unix. To create a truly secure solution, access to any critical device must be through a jump server like solution, preferably one that supports multiple platforms through a unified interface and control point.

5. **No access control to target systems**. Homegrown jump servers do not allow granular restriction of users to connect to specific target systems only.

6. **Remote vendors** – the "All or Nothing Challenge". Jump servers cannot restrict control over what a remote vendor can or cannot do. Examples include granting them access to a specific machine during a certain time period, linking their access to a valid ticket ID in your ticketing system, ensuring managerial approval as part of the access workflow and more.
7. **Lack of security best practices and high maintenance.** Homegrown and tailored solutions typically do not implement industry security best practices and require more resources for development and maintenance.
8. **Lack of granular SIEM insight.** Unmanaged privileged credentials on jump servers are not fed into the SIEM system for setting privileged activity alerts and gaining a granular view into who accessed the privileged account, when, why and what actions did they actually perform on the target system.
9. **No command level monitoring and keystroke logging.** Understanding the privileged commands that were run in a session eases the forensic analysis process and dramatically shortens the resolution time.
10. **No enforcement of enterprise workflow processes upon access.** Homegrown jump servers cannot enforce workflows out-of-the-box. Workflows such as, managerial approval prior to system access, integration with the helpdesk ticketing system for ticket ID validation, limitation of session duration, enforce insertion of reason for server access, limit server access to one person only in parallel (exclusivity), two-factor authentication enforcement and more, ensure better control, audit and tighter security over how sensitive systems are accessed.

Revisiting Security Best Practices With A New Paradigm: CyberArk's 3-In-1 Next Generation Jump Server

Given today's advanced threats and attack techniques for going after privileged accounts and the emphasis of many best practices and regulations (e.g. NERC-CIP) on including specific requirements on protecting against remote privileged access ("Interactive access"), critical infrastructure operators need to rethink their security architecture and consider using a next generation jump server. According to a Gartner Research report2 on advanced persistent threats, protecting against this type of threat requires **locking down privileged accounts**. The report concluded that "to reduce the impact of social engineering attacks, ensure that end users do not have administrative access; and when IT administrator access is required for system administration, perform these functions **on isolated systems** that are not used for email or Web browsing."

The crux of a next generation jump server encompasses three critical components for a stronger security posture against advanced threats:

1. Isolation that blocks the spread of desktop malware

Typically, attackers will exploit vulnerable desktops to directly access core assets with malware, key logging, memory mapping and other techniques. By connecting through CyberArk's Privileged Session Management (PSM) Suite, a zero-footprint solution that acts as a secure proxy, critical infrastructure operators can isolate, control and monitor all remote access to critical systems and servers.

Privileged sessions are initiated via the PSM server since only it knows the privileged credential to the target system. This means that remote users do not even need to type in the privileged credential and can connect directly through the PSM server – this results in no password disclosure due to privileged single sign on and the password does not even reach the admin's desktop, blocking any of the aforementioned attack techniques.

CyberArk's PSM creates strict isolation between a potentially infected desktop, which could have been infected because of social engineering techniques, and the target system. In this case, any malware that may exist on the desktop does not spread to the critical system since the session is running on an isolated secure proxy, not on the end-point and the malware "sees pixels" without being able to access the asset.

2. Control that protects the privileged account

CyberArk's PSM solution acts as a central control point so that any remote session has pre-defined workflows that are enforced for every remote session e.g. two factor authentication, session duration limitations, managerial approval prior to session initiation, integration with other systems e.g. ticketing system for ticket ID validation etc.

Part of controlling the privileged account is also to be able to manage it. Periodic or one-time password replacements protect against any attempt to reuse a password that may have been hacked. Enforcing complex passwords will minimize the risk of password cracking. Lastly, storing privileged credentials in a highly secure repository - CyberArk's Digital Vault - will reduce the risk of an attacker breaching the credential repository.

3. Monitoring for malicious actions

The first two components of a next generation jump server (isolation and control), cover the preventative approach necessary to improve an organization's security posture. The third component covers the detection approach. Once a remote connection is made through the PSM jump server, all sessions can be viewed in real-time or video recorded for forensic analysis playback. All privileged activity and recordings can be fed into the SIEM platform so that if there is an exploit of authentic sessions for malicious actions they will be alerted upon. Should any suspicious activity be detected, incident response or security operations teams can intervene in the session and terminate it if necessary. Being able to monitor the sessions provides audit-ready proof, change management review and faster resolution time where privileged activity can be searched and viewed in context rather than having to sift through and correlate a long list of logs.

Monitoring and forensic analysis is also an important part of being able to meet regulations common in many industries (such as, PCI-DSS, NERC-CIP, NIST 800-53 and more) where there is a common need for accountability, access control and monitoring of privileged account usage and activity. Some regulations even require 'four eyes principle' where live monitoring is necessary as if the person were sitting next to the user accessing the sensitive machine.

Lastly, the three-in-one capability of a next generation jump server is particularly important when working with external vendors. You can enable secure remote access on-demand yet not have to disclose the privileged credential to your critical core operational systems. At the same time, the session is continuously monitored and can be intervened with in real-time, as if you were looking 'over the shoulder' of your remote vendor.

CyberArk's Next Generation Jump Server In Action

Figure 4 below depicts how a remote vendor or employees on the corporate network would securely connect to a critical system using the CyberArk Privileged Session Management Suite.

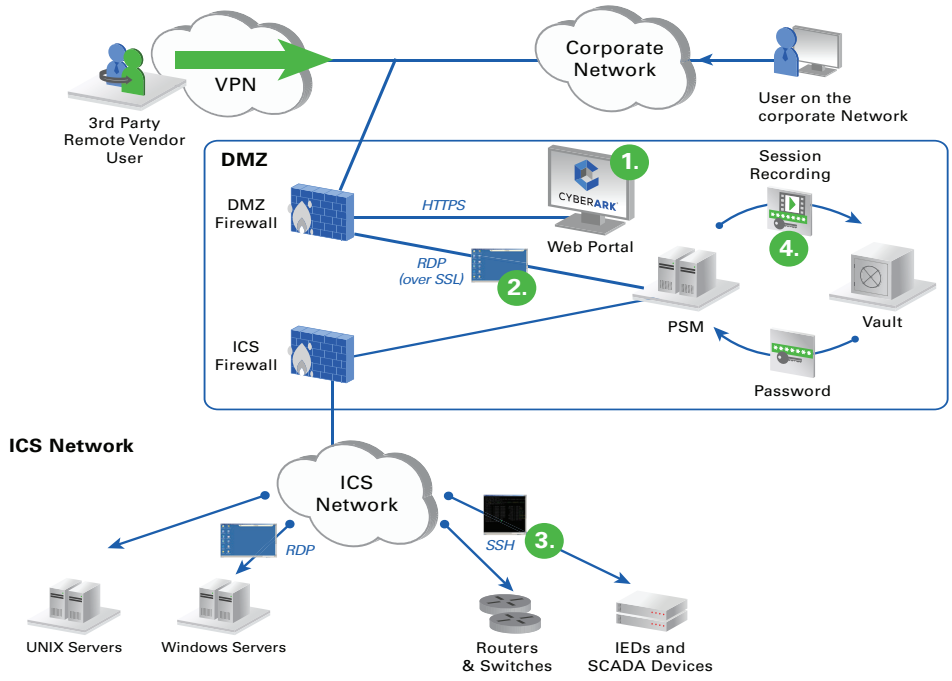

Figure 4: CyberArk's PSM as a Next Gen Jump Server for Isolation, Control & Monitoring

1. Initially they may connect over VPN when connecting into the network remotely and from there log in to the PSM server via a secure web portal. If an internal employee is connecting to sensitive systems from within the organizational network, they would connect directly to the PSM web portal (without a VPN).

2. Once logged into the PSM web portal, the privileged user selects the target machine or device to which they would like to log on to. At this point, PSM controls who can access which systems acting as the single control point into target machines (a logged user will only be able to choose and connect to systems and devices that he is authorized to access).

3. Once selecting the target machine to connect to, a direct connection is established over RDP, SSH or another supported protocol. By going through PSM, which acts as a jump server, there is complete isolation between the remote desktop and the target system. Since the session is running on an isolated secure proxy, a malware, if exists on the desktop, is blocked from spreading or accessing the target system. Furthermore, such malware will not be able to hijack the privileged credentials as they are not entered by the end-user nor are they stored in the desktops memory.

4. All privileged sessions that are established through the PSM can be monitored in real-time or video recorded for playback and then sent back to the Digital Vault for tamper-proof storage or sent to an organizational SIEM system for privileged intelligence insights and alerting.

Summary

Privileged and shared accounts are critical attack points in many ICSs and corporate networks and are what attackers go after to inflict maximum damage. Organizations must start to isolate their critical systems from standard enterprise resources and from remote access users in order to minimize the impact of a targeted attack once the attacker is within the network. This is commonly done today by creating a homegrown jump server solution yet security vulnerabilities still exist. A next generation jump server goes beyond isolation to offer strict access control and real-time monitoring of every privileged activity on critical assets. The three-in-one capabilities offered through a next generation jump server better protect against threats whether they are from inside personnel or targeted by external attackers. Next generation jump servers, such as CyberArk's Privileged Session Management Suite provides comprehensive protection, accountability and monitoring of these critical attack points across multiple systems.

The table below summarizes some of the common attack techniques used to hijack privileged credentials and may be causing you concern. When evaluating a homegrown jump server solution versus CyberArk's Privileged Session Management Suite (a next generation jump server) consider the following:

Attack Vector	CyberArk's Privileged Session Manager® (PSM)	Homegrown Jump Server
Key logging - take control of a workstation and steal passwords to critical ICS systems as they are being typed in	Privileged single sign on does not require typing in a password to connect to the target system	No solution
Exploitation/Use of stolen credentials of the target system	Access control into the target system is controlled by PSM which is the only control channel that knows the privileged credential protected by a secure Digital Vault	No protection – the homegrown jump server only acts as a stepping stone into the target system which then requires a separate login
Brute force – repeatedly try default and various password combinations to connect from the desktop to the target system.	This will only succeed if weak passwords are used. With CyberArk's solution, privileged credentials are managed, automatically changed with complex and frequently replaced passwords, enforced by pre-defined policies.	No solution
Backdoor/RAT – the attacker creates a backdoor on an administrator's desktop to maintain continuous access into the organizational network. This is often referred to as RAT – Remote Administration Tools – and it is a prevalent technique employed by attackers in targeted attacks. RATs can be used to take over end-user desktop and establish a new, or tamper with an existing privileged session.	CyberArk's PSM solution isolates the sensitive assets ensuring that all the privileged sessions are solely established through the PSM and that all the controls and policies are enforced. Thus, the attacker is channeled to act through PSM where his actions are controlled and monitored. All connections through PSM are "visual" – any action is performed either by keyboard or mouse and any response is presented on screen, thus the malware sees only pixels, and cannot intervene in the session or inject/modify the commands. Moreover, by monitoring privileged accounts and actions, irregular activity can be detected.	Partial solution - only with the right configuration will direct access to the target device be avoided. Moreover, even with proper network architecture, the privileged password is still entered on the administrator's machine and sessions are opened from it to the sensitive asset through the jump server. This means that the attacker can use the backdoor and create a new session or inject his commands into an authentic one, without the local user or network administrator's awareness and going undetected

About CyberArk

CyberArk is the only security company laser-focused on striking down targeted cyber threats; those that make their way inside to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world's leading companies – including 40 of the Fortune 100 – to protect their highest-value information assets, infrastructure, and applications.

For over a decade CyberArk has led the market in securing enterprises against cyber attacks that take cover behind insider privileges and attack critical enterprise assets. Today, only CyberArk is delivering a new category of targeted security solutions that help leaders stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable business harm is done. At a time when auditors and regulators are recognizing that privileged accounts are the fast track for cyber attacks and demanding stronger protection, CyberArk's security solutions master high-stakes compliance and audit requirements while arming businesses to protect what matters most.

With offices and authorized partners worldwide, CyberArk is a vital security partner to more than 1,400 global businesses, including:

- 40 of the Fortune 100
- 17 of the world's top 20 banks
- 8 of the world's top 12 pharmaceutical companies
- 75 of the leading energy companies
- Global brands in retail, manufacturing and telecommunications/cloud

For additional information, visit www.cyberark.com.