Virginia Information Technologies Agency

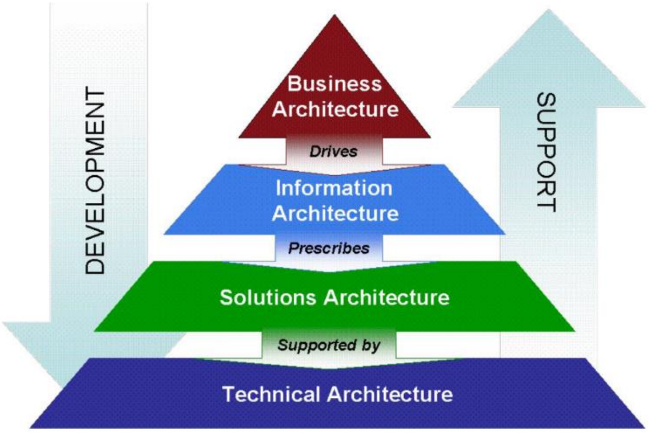
VITA

Enterprise Architecture
Technical Brief

Jump Servers

Robert Kowalke

July 2018



Contents

Jump Server Recommendation

VITA recommends leveraging "hardened" jump servers to improve security and help withstand attacks. VITA endorses use of jump servers where administrators first connect in to, before connecting to any other servers, or to untrusted environments. Hardened jump servers are highly secured computers that are not used for non-administrative tasks, which makes it easier for event monitors to see unauthorized activities. Jump servers are great for:

- Controlling remote access by outside suppliers/vendors quickly with minimal impact.
- Crossing security domains.
- Better control of remote access VPN's for vendors and other support personnel.
  - Forcing remote admins to VPN into a jump server before proceeding with other network connections.
- Placing application-specific admin tools on application-specific jump servers.
- Enabling remote monitoring by responsible parties (suppliers, etc.).
- Accommodating flexible mobile workforces with 24/7 access.
- Third party access to facilitate support and maintenance for emergency incident responses.
- Providing a means to monitor and enforce service level agreements with outside providers.

For any comments, questions, and/or concerns with this technical brief, please contact VITA EA: ea@vita.virginia.gov

General understanding of terms:

Jump Point [1] [2] [3]

- The central tenet behind jump boxes is they are highly-secured computers never used for non-administrative tasks.
- A hardened and monitored device that spans two dissimilar security zones, and provides a controlled means of access between them.
  - User access should be tightly controlled and monitored.
- Used to establish a persistent, one-to-one connection.
- Must be installed on each remote system to access.
- Deploy a jump point if you need:
  - Control of installing a persistent, secure, active or passive remote access client.
  - Access to SSH, Telnet, or systems on a network such as servers, routers, POS systems, or ATMs.
  - Unattended access to Windows, Mac, and Linux computers regardless of network location.
  - To run Microsoft Remote Desktop Protocol (RDP) sessions while maintaining a consistent audit trail.

Bastion Host [4]

- Allows complete control over how each service interacts with the network.
- Typically designed with one function in mind, that of allowing information to flow securely between the internet and the internal network without directly exchanging packets.
- Can be as simple as a router or as complex as a DNS server.
  - Most common roles include being a router, DNS server, FTP server, SMTP server, or web server.

[1] How Jump Technology Works: Unattended Access to Remote Systems – a Jump Technology Overview by Bomgar Corporation, January 11, 2018.

[2] Jump Server by Wikipedia, https://en.wikipedia.org/wiki/Jump_server June 25, 2018.

[3] Jump Boxes and SAWs Improve Security – If You Set Them-Up-Right, by CSO https://www.csoonline.com/article/2612700/data-protection/security-jump-boxes-improve-security-if-you-set-them-up-right.html - July 26, 2017.

[4] Hardening Bastion Hosts by the SANS Institute InfoSec Reading Room in 2001.

- As a part of an overall defense in depth strategy, they can slow an attacker's progress while protecting confidentiality, integrity, and availability of a private network.

Secure Administrative Workstation (SAW) [5]

- The concept of a traditional "jump box" has morphed into an even more comprehensive and locked-down "secure admin workstation" (SAW).
- A SAW is a computer the admin must originate from, before performing any administrative task, or connecting to any other administered server or network.
- A jump box and SAW are related, but they're used at different points.
  - The SAW is always the first computer.
- Both can be used to make your environment significantly more secure.
- You should be using one or both.
- The central tenet behind both jump boxes and SAWs is that they are highly-secured computers never used for non-administrative tasks.
- Jump boxes and SAWs:
  - Must be configured so that they are both less likely to be exploited.
  - Must be restricted in what they are allowed to visit.
  - Only by having both controls enforced can they provide much needed security.

[5] Jump Boxes and SAWs Improve Security – If You Set Them-Up-Right, by CSO https://www.csoonline.com/article/2612700/data-protection/security-jump-boxes-improve-security-if-you-set-them-up-right.html - July 26, 2017.

Background Information

Jump Boxes Improve Security [6]

- Organizations consistently and reliably using one or both of these approaches have far less risk than those that do not.
- A jump box is a secure computer that all admins first connect to before launching any administrative task or use as an origination point to connect to other servers or untrusted environments.
- The concept of a traditional "jump box" has morphed into an even more comprehensive and locked-down "secure admin workstation" (**SAW**).
  - A SAW is a computer the admin must originate from before performing any administrative task or connecting to any other administered server or network.
  - A jump box and SAW are related, but they're used at different points.
    - The SAW is always the first computer.
    - Both can be used to make your environment significantly more secure.
    - You should be using one or both, and if you're not, you need to get busy
- The central tenet behind both jump boxes and SAWs is that they are highly-secured computers never used for non-administrative tasks.
- Jump boxes and SAWs are both highly secure computers for completing admin tasks, or using as jumping off points to other computers and networks.
  - They differ in their location and physical implementation.
    - Jump boxes are normally centrally located "servers" to which remote admins connect to and begin their administrative duties.
    - SAWs are individual, dedicated computers used by each admin for only their admin duties.
- Jump boxes are not dead
- Jump boxes and SAWs must be configured so that they are both less likely to be exploited and also must be restricted in what they are allowed to visit. Only by having both controls enforced can they provide much needed security.
- SAWs are preferred over jump boxes, but jump boxes are great solutions for particular scenarios.

[6] Jump Boxes and SAWs Improve Security – If You Set Them-Up-Right, by CSO https://www.csoonline.com/article/2612700/data-protection/security-jump-boxes-improve-security-if-you-set-them-up-right.html - July 26, 2017.

   - For example, the highest security possible can be gained by having “SAW-using admins” connect to centralized jump servers for all admin tasks. That way all the admin connections can be constrained to fewer origination points, making it easier for event monitors to see unauthorized admin attempts.
   - Jump boxes are also great places for crossing security domains or forcing remote admins to VPN into before going on to further connect to a network.
- Protective measures you should take for jump boxes and SAWs.
   - Use the latest OS and application versions
   - Extremely important they’re not allowed to connect to just anyplace.
      - At the very least, they should not be allowed to connect to the internet and anything from the internet should not be allowed to connect to them.
      - Almost as important, is that they not be allowed to connect to regular end-user workstations.
   - SAWs should not have any inbound connections at all.
   - Jump boxes should have none, or be limited, or only allowed by exception, a connection from another trusted computer.
   - You can enforce connection-allows and -denies using firewalls, IPSEC, VPNs, or other connection limiting mechanisms, such as NetBIOS computer enforcement, VLANs, proxies, or 802.1x network enforcement.
   - The best shops prevent elevated admins, like domain admins or enterprise admins in Microsoft Active Directory environments, from connecting to anything other than domain controllers or the few servers to which they absolutely have to connect for install or configuration duties (i.e., Exchange servers, Active Directory Certificate Services installs, etc.).
   - No browsing the internet
   - Some allow a very limited number of connections to pre-approved internet sites – say fewer than 10 sites, and are mostly vendor software download locations.
   - Simply restricting port 80 or 443 traffic is not enough.
      - Blocking connections to and from the internet means blocking all port traffic and not just internet browsing.
   - Almost as critical as blocking internet access is blocking any non-pre-approved applications.
   - Something stronger than regular passwords (e.g., smartcards, key fobs, multi-factor authentication) should be required to log on.

  - Require smartcards or other two-factor authentication methods for all elevated users.
  - Test them, and if they don’t cause critical operational issue, implement them across your entire environment, if possible. If not, implement them on the jump boxes and SAWs.

Use Windows Server 2016 to Secure a Jump Server [7]

- A jump server typically does not store any sensitive data, but keep in mind it does have sensitive data in memory.
- Jump servers enable users to connect and manage servers/services in separate security zones.
  - When establishing the connections, user credentials are stored in memory, and these credentials are attractive targets for credential theft attacks.
  - Should a malicious actor take over your jump server, they can act on behalf of connected users to take control over the assets that are managed through that jump server.
- A jump server typically runs on dedicated hardware within a physically secure perimeter, running a specific workload.
  - Once deployed, the workload does not change very much, which makes jump servers a good candidate to lock down the software it trusts.
- If the jump server runs Windows Server Core edition, the FilePublisher policy is recommended.
  - FilePublisher white lists all the files allowed to run on the server.
- If the jump server runs Windows Server full desktop edition, the Publisher policy is recommended which uses only the signer certificates in the policy (i.e. the server will allow files to run as long as they are signed by the certificates in the CI policy).

[7] Use Windows Server 2016 to Secure a Jump Server, Microsoft TechNet, February 2, 2017. Downloaded from https://blogs.technet.microsoft.com/datacentersecurity/2017/02/02/use-windows-server-2016-to-secure-a-jump-server/ on June 25, 2018.

Interactive and Automated Access Management by NIST [8]

- 5.1.2 SSH Identity and Authorized Keys
  - Pivot Prevention: Accounts should not be configured with both incoming and outgoing identity key-based trust relationships unless expressly needed (for example, an approved jump server).
- NIST SP 800-53 Controls: AC-2, ACCOUNT MANAGEMENT, control #k
  - SSH Implications: Any private keys held by a group of individuals should be rotated whenever an individual is removed from the group (note: administrators may obtain copies of keys when using service accounts). Keys stored on shared accounts on jump servers should be rotated when someone's access to the jump server is terminated.
- NIST SP 800-53 Controls: IA-5, AUTHENTICATOR MANAGEMENT
  - SSH Implications: Shared accounts on jump servers are group/role accounts, and any private keys stored on such accounts (for access from the jump server to end hosts) should be changed when a user's access to the shared account is terminated (effectively, membership in the group of people with access to the account is terminated).

Amazon Web Services (AWS) Security by Solinor [9]

- Avoid too complex networks
  - Simple networks, simple services, simple AWS accounts.
- Network Security – Use jump/bastion hosts, NAT, VPNs.

Six Best Practices for Securing AWS Environments [10]

- Secure your operating systems and applications.
  - AWS Best Practice: Use bastion hosts to enforce control and visibility.

[8] Interactive and Automated Access Management Using Secure Shell (SSH) by NISTIR-7966, October 2015.
[9] Amazon Web Services (AWS) Security by Solinor.
[10] Six Best Practices for Securing AWS Environments Whitepaper by Centrify, July 1, 2017.

        - Centrify Recommendation: Although Centrify can provide one, our best practice is to enforce control with an agent and audit on every EC2 instance. This can't be bypassed whereas a central bastion host/proxy can.
- Manage security monitoring, alerting, audit trail, and incident response.
    - AWS Best Practice: Manage commands that can be used during sessions. For interactive sessions like SSH or appliance management, or AWS XLI, such solutions can enforce policies by limiting the range of available commands and actions.
        - Centrify Recommendation: Many solutions filter commands at a (bastion) host level. This is insufficient; it can be bypassed by directly compromising an instance and with malware on the instance. Centrify enforces access controls at the host level and so is not affected when the bastion is bypassed.
    - AWS Best Practice: We recommend configuring the following areas for logging and analysis: Actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of audit logs; creation and deletion of system level objects.
        - Centrify Recommendation: Centrify audits all user activities across the hybrid enterprise and ties all activity back to a unique individual user for 100% accountability. Privileged login sessions can be video recorded either at the bastion host/proxy level or at the host level to avoid being bypassed by a direct login to the instance. All attempts to login to Centrify UIs, AWS portals, and EC2 instances as well as all privilege elevation attempts can be audited and recorded.

CyberArk Privileged Account Security for AWS [11]

- Implement a Jump Server for Accessing the AWS environment
    - <snip>For security implications, to reduce the size of the attack vector and secure assets on AWS, a common security best practice is to limit RDP and/or SSH access to instances through a bastion host or a proxy (jump) server. The server can be located outside the organization's

[11] CyberArk Privileged Account Security for Amazon Web Services (AWS) downloaded from the web on June 22, 2018.

firewall or DMZ and used to establish a VPN connection to the AWS cloud, preventing a VPC connection directly into the organization network. Any allowed access to AWS instances are only permitted from that proxy server. Also, organizations may only allow outbound communication from the organizational environment to the AWS cloud.

How Jump Technology Works: Unattended Access to Remote Systems [12]

- Bomgar jump technology allows a user to access and control remote and/or unattended computers in any network.
- Jump technology is a cost-effective way to reach every device in your enterprise.

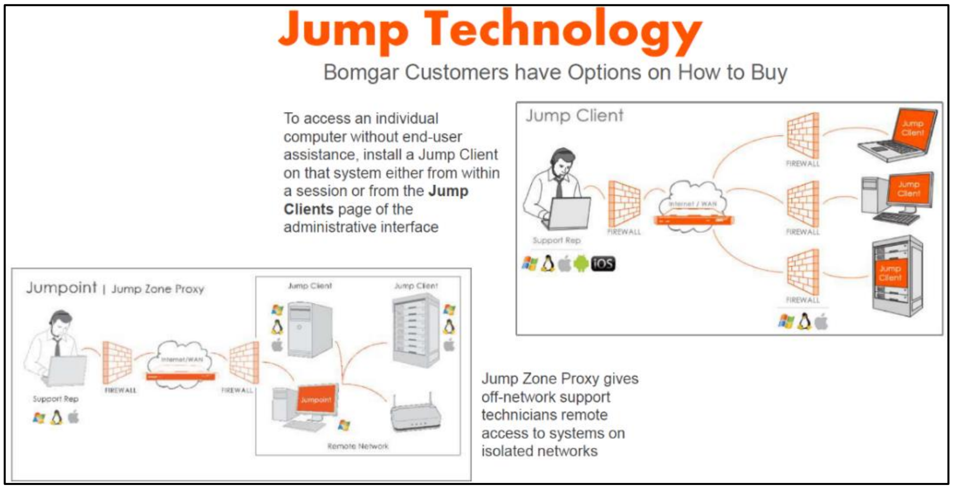
What is a Jump server/client/box?

  - Jump clients are used to establish a persistent, one-to-one connection.
    - Jump clients must be installed on each remote system to access.
  - Deploy a jump client if you need:
    - Unattended access to Windows, Mac, and Linux computers regardless of network location.
    - Control of installing a persistent, secure active or passive remote access client.

- Jump points extend the reach of jump functionality to Windows systems in a JumpZone enabling establishment of a session with any remote Windows system in the JumpZone.
- Deploy a jump point if you need:
  - Access to SSH, Telnet, or vPro systems on that network such as servers, routers, POS systems, or ATMs.
  - To run Microsoft Remote Desktop Protocol (RDP) sessions while maintaining a consistent audit trail.

[12] How Jump Technology Works: Unattended Access to Remote Systems – a Jump Technology Overview by Bomgar Corporation, January 11, 2018.

- A jump point acts as a conduit for unattended access to Windows computers on a known remote network.



Jump Technology

Bomgar Customers have Options on How to Buy

To access an individual computer without end-user assistance, install a Jump Client on that system either from within a session or from the **Jump Clients** page of the administrative interface

Jump Zone Proxy gives off-network support technicians remote access to systems on isolated networks

Use Case: Secure Remote Access for ICS/SCADA [13]

- Providing remote access and connectivity to ICS/SCADA systems opens them up to considerable risk.
- With the deployment of more advanced IP-enabled assets into the ICS, the need for remote access will continue to grow for both company employees and third-party support.

[13] Use Case: Secure Remote Access for ICS/SCADA by Palo Alto Networks, February 16, 2018.

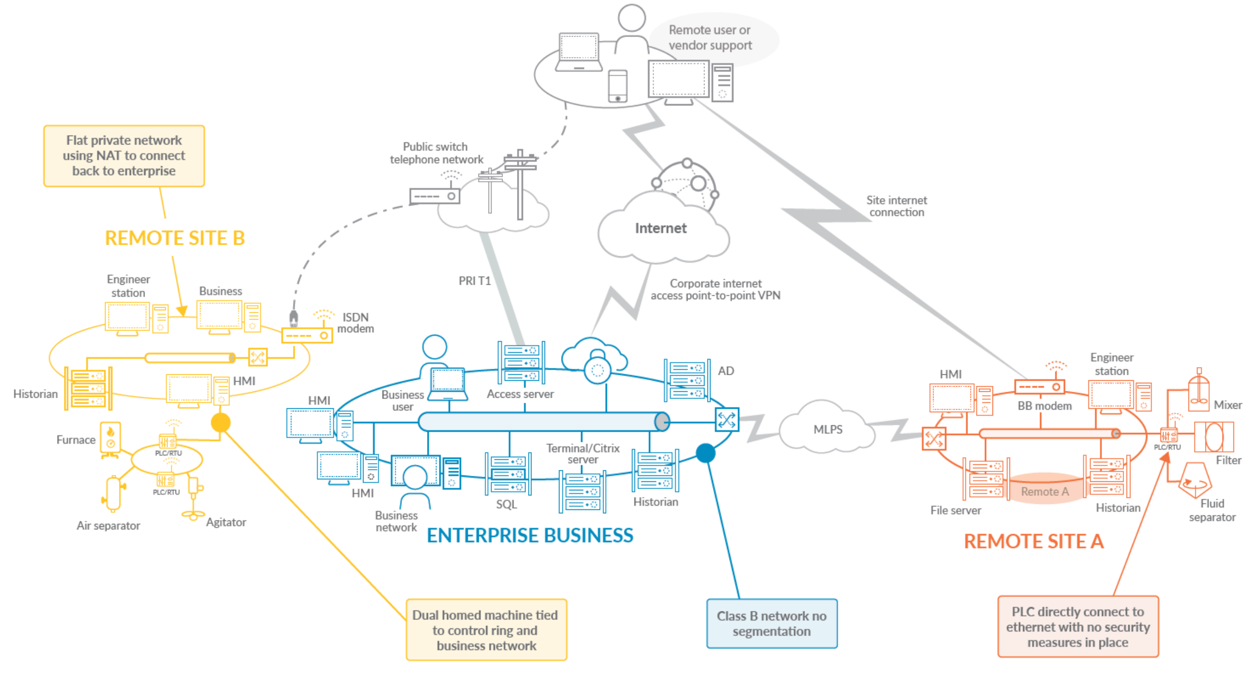
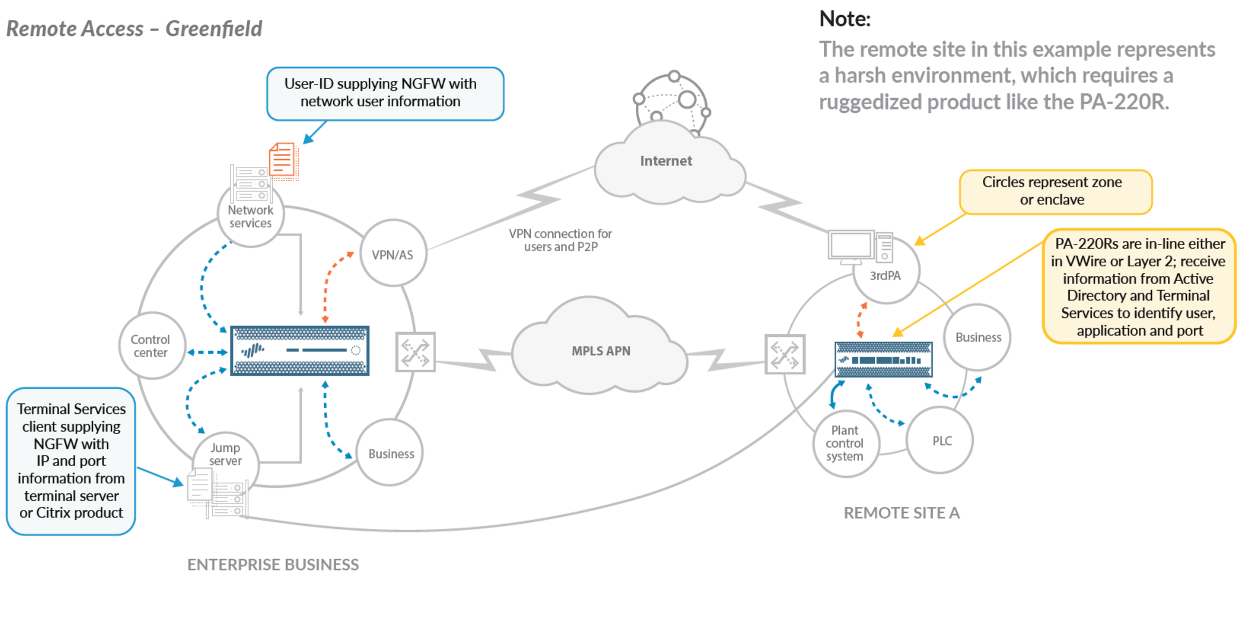


Figure 1: Typical remote access design in older systems

- Use Zero Trust architecture and design principles based on the "never trust, always verify" premise to address the deficiencies of a traditional remote access implementation.


Remote Access – Greenfield
User-ID supplying NGFW with network user information
Internet
Network services
VPN/AS
VPN connection for users and P2P
Control center
MPLS APN
Jump server
Business
Terminal Services client supplying NGFW with IP and port information from terminal server or Citrix product
ENTERPRISE BUSINESS
Circles represent zone or enclave
PA-220Rs are in-line either in VWire or Layer 2; receive information from Active Directory and Terminal Services to identify user, application and port
3rdPA
Business
Plant control system
PLC
REMOTE SITE A

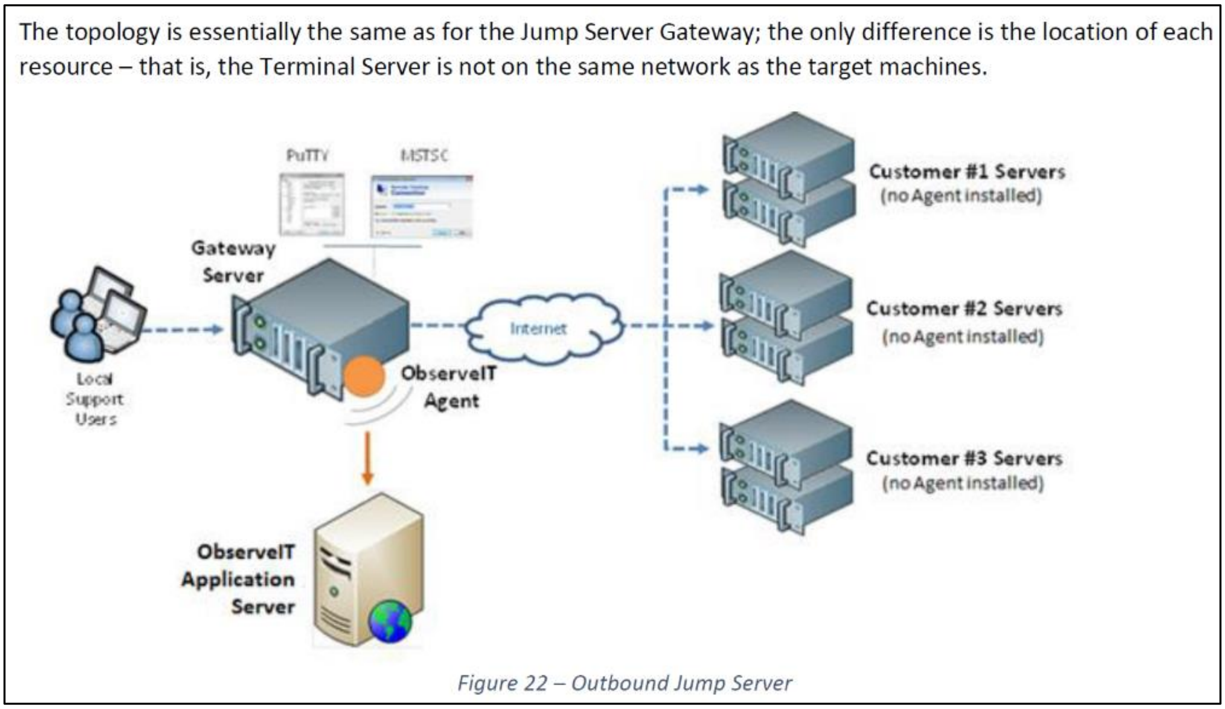
Note:
The remote site in this example represents a harsh environment, which requires a ruggedized product like the PA-220R.

Figure 2: Greenfield deployment – Zero Trust network with jump servers

- The recommended approach is to leverage the use of a jump server, which is a purpose-built server designed and configured to withstand attacks that runs Terminal Services.

ObservIT Enterprise Technical Solutions Overview [14]

- The Jump Server (Terminal Server) Gateway deployment is the ideal solution for logging all user configuration changes on remote network devices, servers, desktops, and DB servers.



The topology is essentially the same as for the Jump Server Gateway; the only difference is the location of each resource – that is, the Terminal Server is not on the same network as the target machines.

Figure 22 – Outbound Jump Server

[14] Use Case: Secure Remote Access for ICS/SCADA by Palo Alto Networks, February 16, 2018.

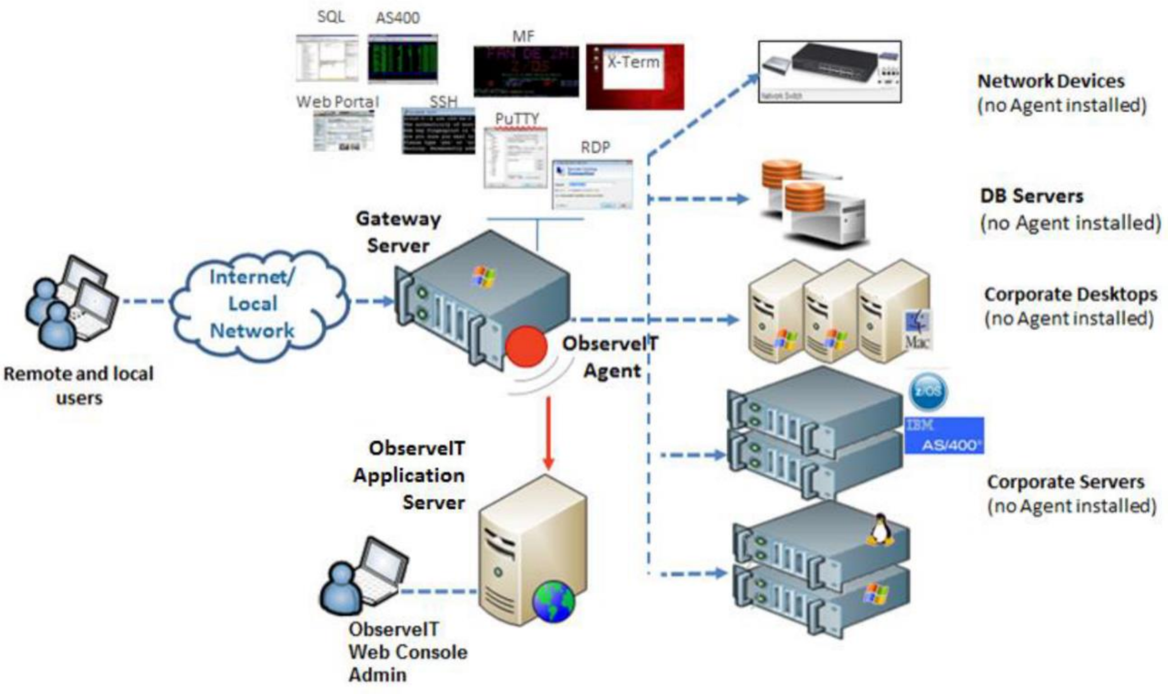


Figure 20 – Terminal Server Gateway (Jump Server) Deployment

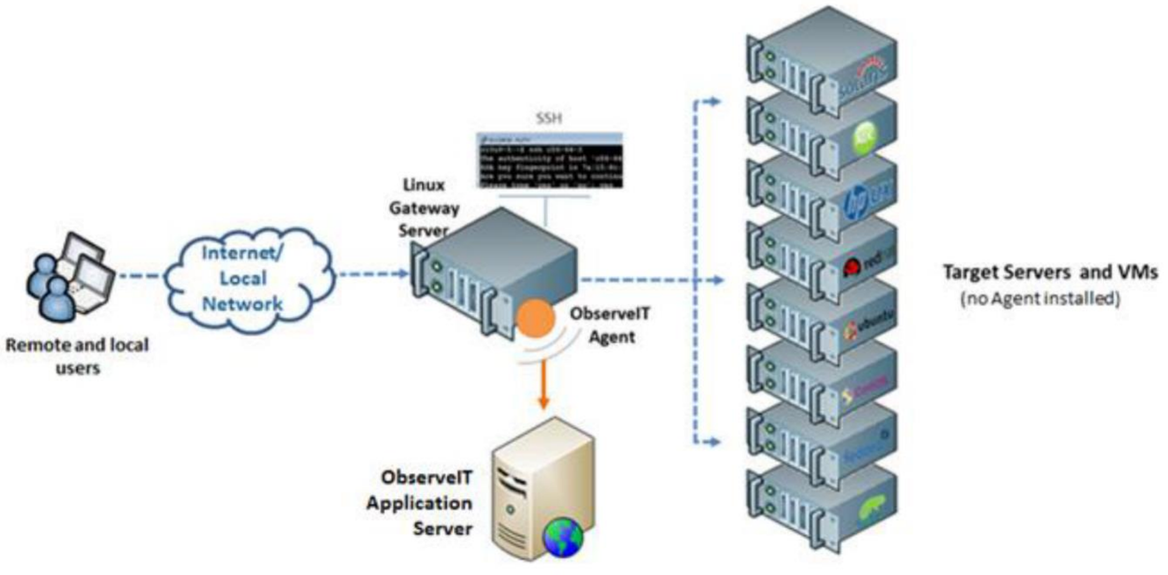
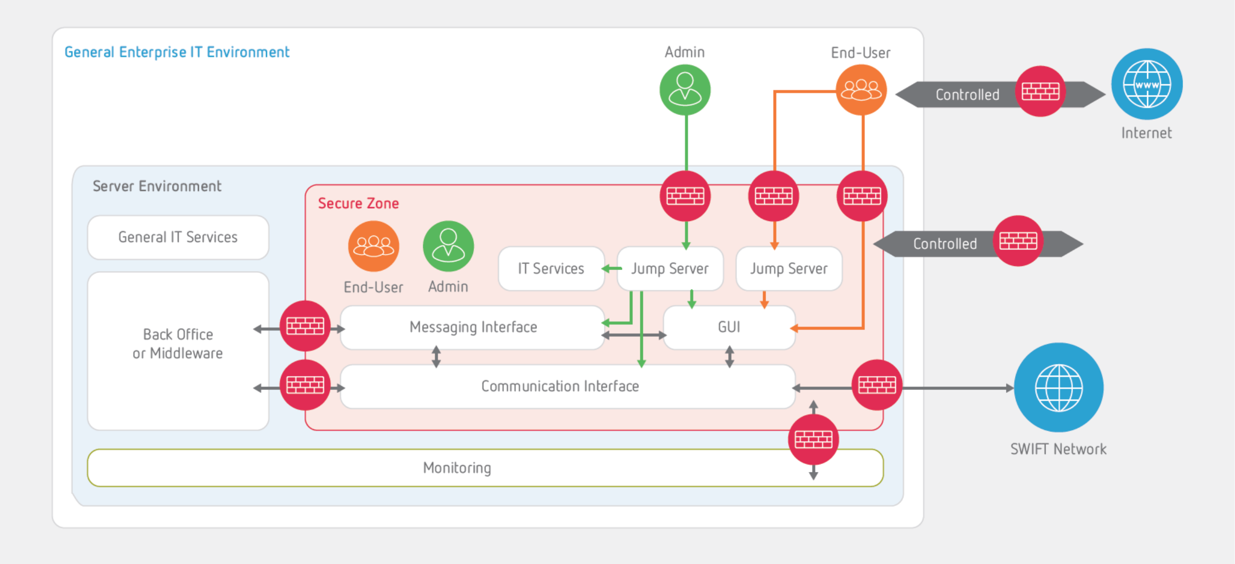


Figure 21 – Linux Gateway (Jump Server) Deployment

Maintain Compliance with SWIFT Security Standards by Citrix [15]

- Securing Your SWIFT systems
  - Whether deployed in a full stack, partial stack, or connector architecture, Citrix aids compliance with the new SWIFT CSP framework by providing direct controls to secure access to the SWIFT network. In the full stack architecture diagram below, a secure zone is established around the SWIFT systems. Operator access from within the general enterprise IT environment is controlled through multifactor authentication to a jump-server connecting to a server within the secure zone.

Figure 1 Secure zone example: full stack within the user location.

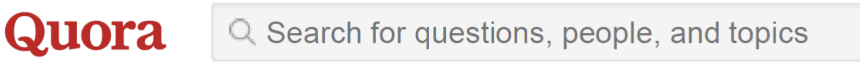


- SWIFT Control Categories: 1. Restrict Internet Access and Protect Critical Systems from General IT Environment.
- SWIFT Controls: 1.1 SWIFT environment protection.
- Citrix Solution Principles: 1.1 SWIFT environment protection. Segmentation between the user's local SWIFT infrastructure and its larger enterprise network reduces the attack surface. Citrix can decouple the web browser, email client and critical apps from the endpoint, and deliver hosted apps virtually from the datacenter or cloud. Operators connect from their general-purpose operator PC

[15] Maintain Compliance with SWIFT Security Standards by Citrix in 2017.

to the SWIFT secure zone via a jump server located within the secure zone, as can be enabled using Citrix.

Are Jump Servers the Same as Bastion Hosts? [16]



- No.
  - A jump server is not the same as a bastion host.
  - A Bastion host is a machine that is outside of your security zone. It is expected to be a weak point, and in need of additional security considerations. Because your security devices are technically outside of your security zone, firewalls and security appliances are also considered in most cases Bastion hosts.
  - Usually we're talking about:
    - DNS Servers
    - FTP Servers
    - VPN Servers
  - A Jump Server is intended to have a gateway to access something inside of the security zone, from the DMZ. The main reason I've seen this utilized is to make sure that the one known entrance to a specific server that has to be accessible from the outside is kept up to date and is known in its purpose as only having to connect to a specific host(s). Usually this is a hardened Linux box only used for SSH.

Information Supplement: Guidance for PCI DSS Scoping & Networking Segmentation [17]

- System Type: Connected to and/or Security Impacting Systems
  - Description: <snip> System component can connect to or access the Cardholder Data Environment (CDE) via another system—for example, via connection to a jump server that provides access to the CDE). OR <snip>.
- 4. Example Segmentation Implementations: Shared Services

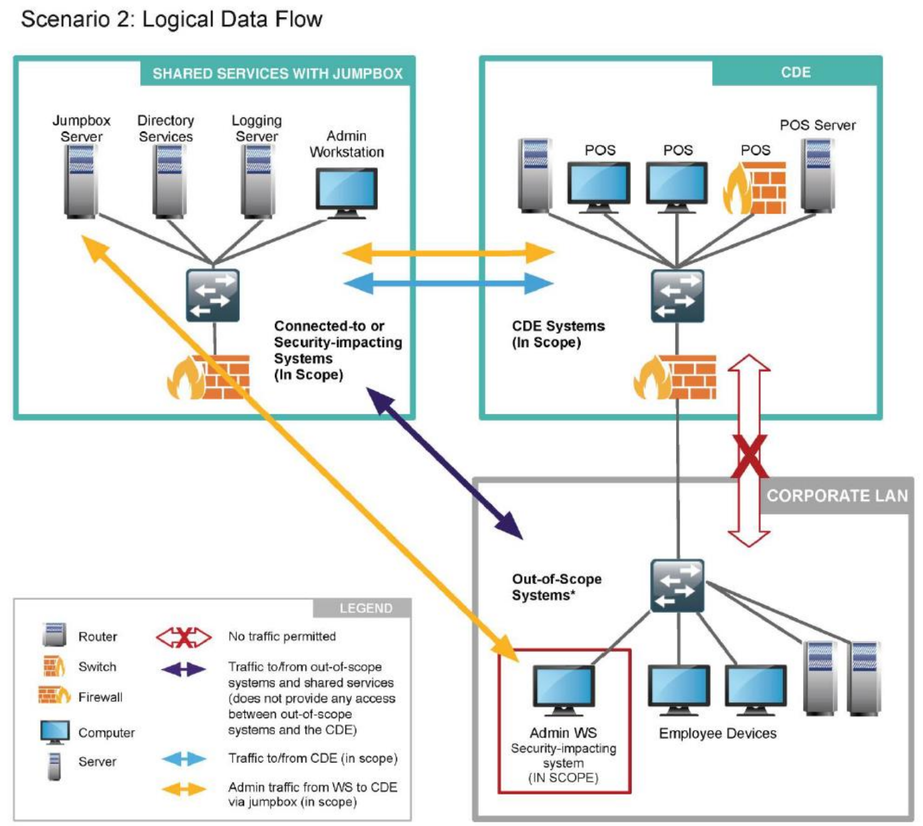
[16] Are Jump Servers the Same as Bastion Hosts? Quora. Pawan Shivarkar, Threat Analyst for Symantec and former ERS Consultant for Deloitte, January 9, 2016.

[17] Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation by PCI Security Standards Council, December 2016.

- 4.2 Example 2: CDE Administration Workstation outside of the CDE.
  - This example builds on the Shared Services network from the previous example, with the addition of:
    1) An administrator's workstation in the Corporate LAN and
    2) A jump box within the Shared Services network to manage and control administrative access into the CDE.

- A "jumpbox" (Bastion host) is installed in the Shared Services network.

FIGURE 5 – Logical Data Flow: Administration of CDE Systems from a Security-Impacting System in the Corporate LAN


Scenario 2: Logical Data Flow
SHARED SERVICES WITH JUMPBOX
Jumpbox Server
Directory Services
Logging Server
Admin Workstation
Connected-to or Security-impacting Systems (In Scope)
CDE
POS Server
POS
POS
POS
CDE Systems (In Scope)
CORPORATE LAN
Out-of-Scope Systems*
Admin WS Security-impacting system (IN SCOPE)
Employee Devices
LEGEND
Router
Switch
Firewall
Computer
Server
No traffic permitted
Traffic to/from out-of-scope systems and shared services (does not provide any access between out-of-scope systems and the CDE)
Traffic to/from CDE (in scope)
Admin traffic from WS to CDE via jumpbox (in scope)

- Bastion hose = a computer specifically designed and configured to withstand attacks. (Source: wikipedia.org)
- Firewall and router rules ensure that
  - Connections to the jump host from the Corporate LAN are restricted to only designated personnel from the Admin workstation, and all other connection attempts are blocked.
  - The Admin workstation is unable to access the CDE directly and must go through the jump box for all access to the CDE.
- Active monitoring and data loss prevention tools (DLP) are in place to ensure account data cannot be transferred from the CDE to the jump box.

- Administration of the jump box itself is via local console only, and there is no remote management of this device.
- Access to the jump box from the Admin workstation is via a different user account than that used to administer the CDE. The account used to access the jump box does not have elevated privileges on the jump box.
- Access to the jump box from the Admin workstation requires multi-factor authentication for individuals. At least one of the multi-factor authentication methods is independent of the Admin workstation and is "in hand" of the designated administrator personnel (e.g. a physical smart card or token is used as "something you have" authentication).
- All applicable PCI DSS requirements are in place to manage and secure connectivity between the Admin workstation and jump box, including firewalls, IDS/IPS, anti-malware and other threat defense tools and techniques.
- All applicable PCI DSS requirements are in place to manage and secure connectivity between the jump box and CDE, including firewalls, IDS/IPS, anti-malware and other threat defense tools and techniques.

You Need to Rethink that Jump Server [18]

- The idea is that admins are completely firewalled off from the datacenter, and instead have to log into a "jump server," which is itself in the datacenter, and is the portal by which admins access the rest of the datacenter.
- A jump server can be useful when it is a sort of privilege access proxy meaning I connect to it as a normal user and it does what is asked of it using elevated privileges that only last for the duration of one's login.
- The jump server should be rebuilt daily to make it harder for a hacker to take hold.
- Allow trusted outsiders test the server (pentest/hack it).
- Run it in read-only mode to prevent installing/copying anything on it, which prevents hackers copying their toolkits onto the machine.

[18] You Need to Rethink that Jump Server by Don Jones downloaded from https://donjones.com/2016/12/15/you-need-to-rethink-that-jump-server/ on June 25, 2018.

BeyondTrust Privilege Management [19]

- Like most PAM providers, BeyondTrust utilizes a bastion or jump-host architecture that can restrict what commands an admin is allowed to run, and what arguments can be supplied afterwards.
    - For example, admins may have access to certain Oracle commands, but not the ability to write to a table, dump a table or write a report. New features include a drag-and-drop UI that allows non-technical admins to use PowerBroker without knowing how to write command-line scripts, which the company hopes will help increase adoption by midsized firms with limited IT resources.

Remote Desktop Gateway on the AWS Cloud [20]

- This section describes general considerations for implementing and configuring RD Gateway in the cloud.
    - Initial Remote Administration Architecture
        - <snip>Using this architecture, an administrator can use a traditional RDP connection to an RD gateway to configure the local server.
        - The RD gateway can also be used as a jump box; that is, when an RDP connection is established to the desktop of the RD gateway, an administrator can start a new RDP client session to initiate a connection to an instance in a private subnet, as illustrated in the following Figure 1.

[19] BeyondTrust Platform Plan Privileged Management Assets by 451 Research, June 18, 2015.
[20] Remote Desktop Gateway on the AWS Cloud by Amazon Web Services, June 2017.

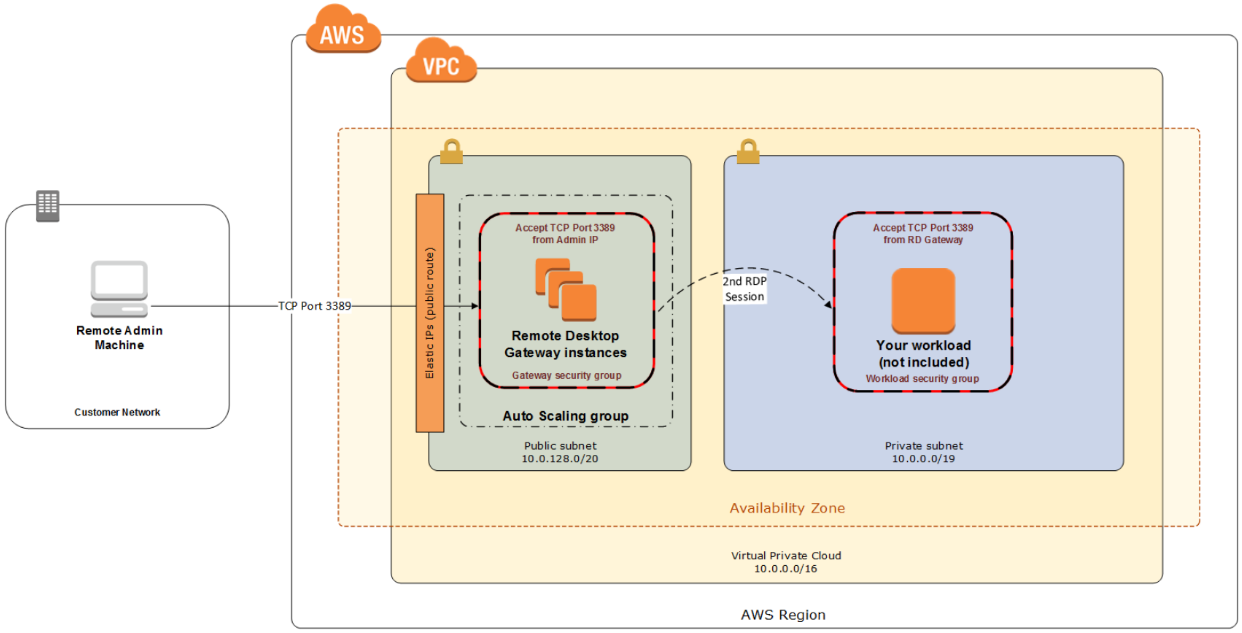

AWS
VPC
Remote Admin Machine
Customer Network
TCP Port 3389
Elastic IPs (public route)
Accept TCP Port 3389 from Admin IP
Remote Desktop Gateway instances
Gateway security group
Auto Scaling group
Public subnet 10.0.128.0/20
2nd RDP Session
Accept TCP Port 3389 from RD Gateway
Your workload (not included)
Workload security group
Private subnet 10.0.0.0/19
Availability Zone
Virtual Private Cloud 10.0.0.0/16
AWS Region

Figure 1: Initial architecture for remote administration

HubSpot Security and Risk Management Program Overview [21]

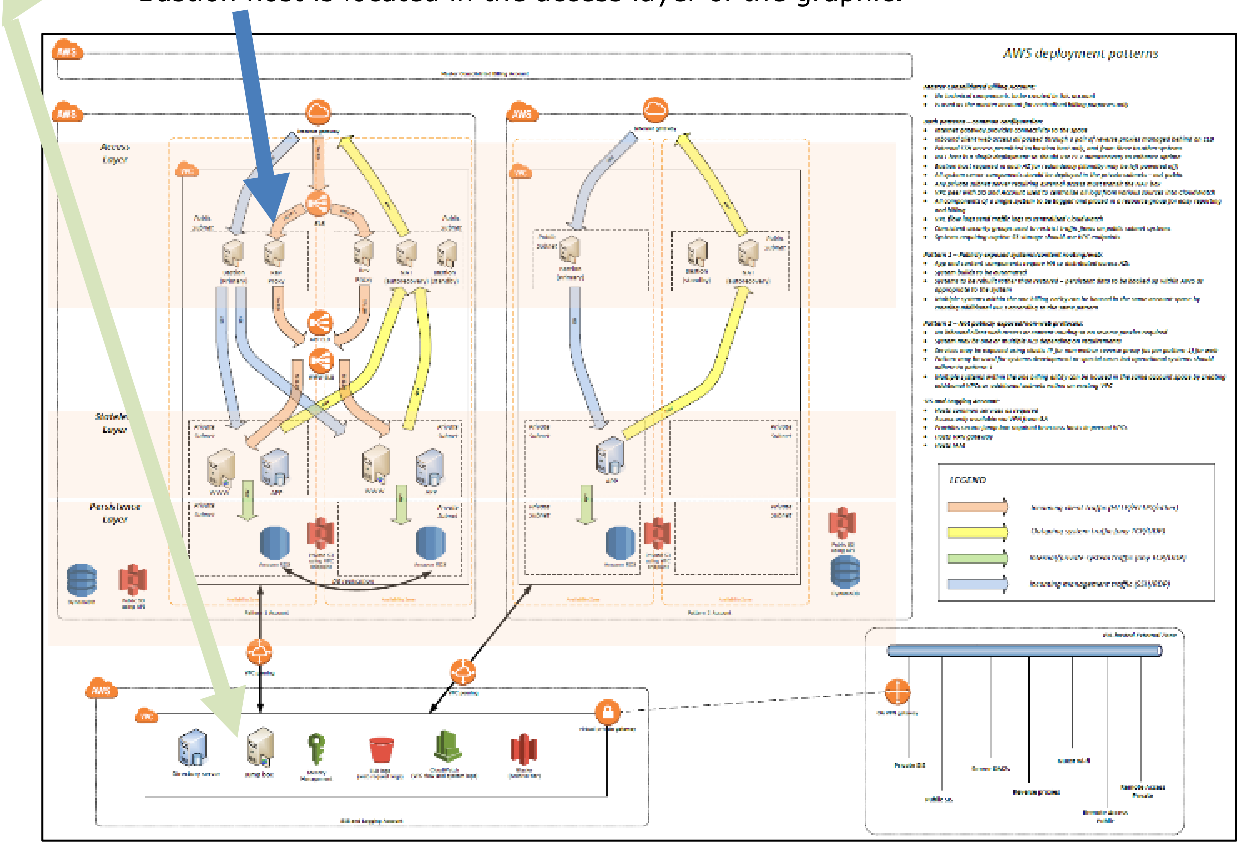
- Infrastructure Access:
  - <snip> Additionally, direct network connections to product infrastructure devices over SSH or similar protocols is prohibited, and engineers are required to authenticate first through a bastion host or "jump box" before accessing QA or production environments. Server-level authentication uses user-unique SSH keys and token-based two factor authentication.

HubSpot
Security & Risk Management

[21] HubSpot Security and Risk Management Program Overview, June 2018.

AWS Deployment Architecture [22]

- Jump box is located in the VPC Section of the graphic.
    - SIS and Logging Account:
        - Hosts common services as required
        - Access only available via VPN from GA
        - Provides secure jump box required to access hosts in peered VPCs
        - Hosts VPN gateway
        - Hosts IAM
- Bastion host is located in the access layer of the graphic.



Hardening Bastion Hosts by SANS Institute InfoSec [23]

What is a bastion host?

- Bastions are the highly fortified parts of a medieval castle; points that overlook critical areas of defense, usually having stronger walls, room for

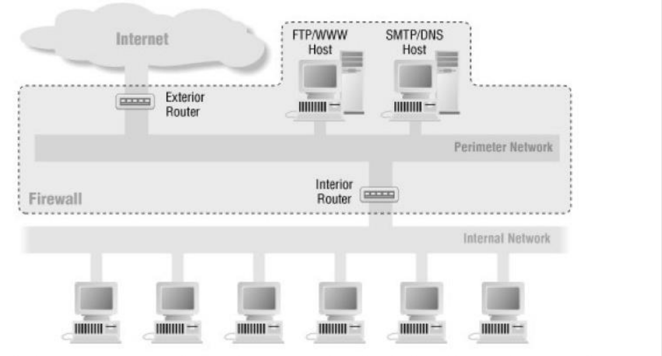
[22] Are Jump Servers the Same as Bastion Hosts? Quora. Pawan Shivarkar, Threat Analyst for Symantec and former ERS Consultant for Deloitte, January 9, 2016.
[23] Hardening Bastion Hosts by the SANS Institute InfoSec Reading Room in 2001.

extra troops, and the occasional useful tub of boiling hot oil for discouraging attackers.

  - A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Generally, bastion hosts will have some degree of extra attention paid to their security, may undergo regular audits, and may have modified software." (Steves, Kevin).

    Bastion hosts are typically a gateway, on the perimeter network, between the Internet and the internal network.

  - A bastion host's main function is to protect the network behind it.



Architecture using two bastion hosts (Zwicky, Elizabeth D., Simon Cooper and Brent D. Chapman. Page 138.)

- Bastion hosts are typically designed with one function in mind: To allow information to flow securely between the Internet and the internal network without directly exchanging packets.
  - The most common roles of bastion hosts to be used as: Router; DNS; FTP; SMTP; News; Web servers