DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

NOV 2 0 2017

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Approval of Identity Federation Service Providers –Remote Desktop Services Jumpbox Solution for the United States Coast Guard

Reference: (a) National Institute of Standards and Technology Special Publication 800-63C

Identity Federation Services (IFS) serve as trusted intermediaries between users seeking to obtain data from a system, application, or device, and the system, application, or device on which the data is stored. IFS capabilities facilitate strong authentication to systems, applications, and devices which are unable to process strong authentication technology directly. Reference (a) focuses on the different ways IFS capabilities can be configured and implemented, and the impact this has on the reliability and trustworthiness of an identity authentication.

This memorandum certifies the United States Coast Guard's (USCG) Remote Desktop Service (RDS) Jumpbox solution as a DoD-approved IFS. The USCG RDS Jumpboxes utilize a number of applications (e.g. Secure Shell) to facilitate secure privileged user Public Key Infrastructure based user-authentication to Unix and Linux systems.

The USCG RDS Jumpbox implementation was briefed to the Privileged User Working Group, which found its security and access controls sufficient to mitigate against privilege escalation and insider threats. For example, only PUs can access the jumpboxes, and they're blocked from accessing the Unix/Linux servers without going through the jumpboxes. Also, the PUs can only access the systems behind the jumpbox that they administer, and cannot authenticate from one server or system behind the jumpbox to another.

The attachment to this memorandum provides more details on the USCG RDS Jumpbox solution. This memorandum shall not be construed to indicate approval of other jumpbox solutions, which may be addressed in future memos.

The point of contact is Mr. Andy Seymour, charles.a.seymour.civ@mail.mil, (571) 372-6990.

Essye B. Miller
Deputy Chief Information Officer
for Cybersecurity and DoD Senior
Information Security Officer

Attachment:
As stated

Distribution:
Secretaries of the Military Departments
Chairman of the Joint Chief of Staff
Under Secretaries of Defense
Deputy Chief Management Officer
Chief, National Guard Bureau
General Counsel of the Department of Defense
Director of Cost Assessment and Program Evaluation
Inspector General of the Department of Defense
Director of Operational Test and Evaluation
Assistant Secretary of Defense for Legislative Affairs
Assistant to the Secretary of Defense for Public Affairs
Director of Net Assessment
Director, Strategic Capabilities Office
Directors of the Defense Agencies
Directors of the DoD Field Activities

cc.
Chief Information Officer, United States Coast Guard

ATTACHMENT

Homeland Security

U.S. COAST GUARD

United States Coast Guard

C4IT Service Center
Operations Systems Center (OSC)

Remote Desktop Services
Jumpbox

Contents

Figures

1 Remote Desktop Services Jumpbox

The Remote Desktop Services (RDS) Jumpbox was developed for privileged user PKI enforcement. It provides a secure and consolidated access point for OSC privileged users to connect to their authorized Linux and Unix servers.

1.1 Account Set Up

CG Cyber Command has directed that all privileged users employ a separate physical token from the member's DoD CAC. Candidates must follow the Privileged User Management Process (PUMP) to seek approval for access and Alternate Token (Alt-Token) issuance.

Privileged users on the Sensitive but Unclassified (SBU) Coast Guard Network (CGOne) must complete and digitally sign a DD-2842, DOD PKI Certificate of Acceptance and Acknowledgement of responsibilities. The DD-2842 is submitted to their local Trusted Agent. The Trusted Agent initiates a request through CGFixit, a Remedy Request Management tool. After the approval process is completed, the local Trusted Agent issues the Alt-Token to the privileged user.

A separate Active Directory user account is created for each privileged user. For this separate user account, the sAMAccountName attribute is appended with '-admin' and the userPrincipalName (UPN) attribute is set to match the Subject Alternative Name (SAN) on the Alt-Token certificate. This separate user account also has the "Smart card is required for interactive logon" setting enabled, which prevents the usage of a username\password login.

An instance for the privileged user is also created in the BMC BladeLogic Server Automation (BSA) property dictionary. BSA is used as the central data store for privileged user account information. It contains the privileged user's name, e-mail address, username, Active Directory domain security group membership, SSH public key, and unique identifier. Additional data that is used for reporting is also stored in the BSA property dictionary. Using BSA as a central data store allows us to ensure that the unique identifiers are not reused. It also enables us to synchronize Active Directory domain security group membership across disparate Active Directory domains. When a change in user access is requested (e.g. grant\revoke access to target servers or disable the user account on all target servers), the automated scripts in BSA use the property dictionary to implement the change.

Privileged users submit their Alt-Token certificate to the Platform as a Service (PaaS) Operations team via a website. An automated process obtains their SSH public keys from their Alt-Token certificates and adds them to their user instance in the BSA property dictionary. BSA is also used to populate their ~/.ssh/authorized_keys files on each of the target servers that they have been approved to access.

1.2 RDS Jumpbox Overview

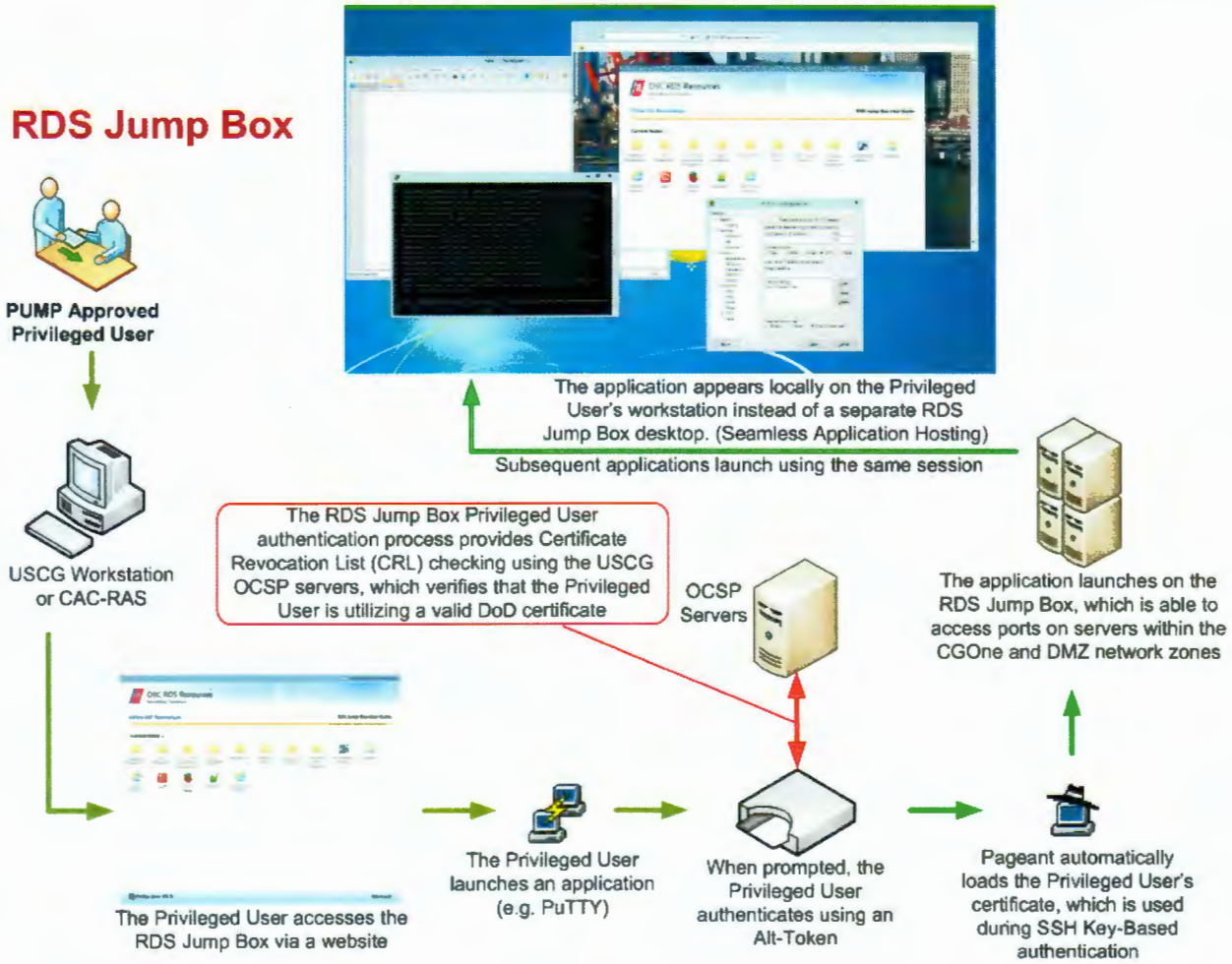

Figure 1

- The privileged user logs into their local workstation using their CAC card.
- The user navigates to the RDS Jumpbox website via a client browser. There are two RDS Jumpbox sites (OSC and FINCEN). The sites are secured with an SSL certificate. The user is prompted for their Alt-Token and PIN.
- After logging into the website, the available applications are displayed. There are over 30 different applications. The most commonly used are PuTTY, WinSCP, SQL Developer and Remote Desktop Connection Manager.
- The privileged user selects an application to launch. Figure 1 illustrates the use of PuTTY. The privileged user is prompted again for their Alt-Token and PIN. Password authentication has been disabled on the Linux and Unix servers.

- The USCG Enterprise OSCP servers verify that the certificates are not expired or revoked.
- The Active Directory account's userPrincipalName attribute is configured to be the same as the Subject Alternative Name on the Alt-Token certificate. Pageant reads the Windows user certificate store (from the user's profile on the RDS Jumpbox server). It loads a Microsoft CryptoAPI entry (CAPI) into Pageant and acts as the communication broker between the Alt-Token and the Microsoft CryptoAPI.
- PuTTY presents the username and uses Pageant to present Alt-Token certificate's private key to the target server. The authentication process ensures that the SSH public key that is stored on the target server (e.g. ~/.ssh/authorized_keys) matches with the private key that was presented. A SSH session is established.
- Microsoft App-V streams the application to the Remote Desktop Session Host. The application window is displayed on the user's workstation.

1.3 Hosted Applications

- Windows Server Management:
  - Active Directory Users and Computers (ADUC)
  - Main Domain RDP
  - Non-Main Domain RDP
  - Remote Desktop Connection (RDC) Manager
  - Windows PowerShell
  - Windows PowerShell ISE

- Linux, HP-UX, Solaris Server Management:
  - Putty
  - Super Putty
  - WinSCP

- Database Management:
  - Oracle SQL Developer
  - SQL Server Management Studio
  - Toad for Oracle (License is needed)
  - Toad for SQL (License is needed)

- ASG Remote Desktop
- Notepad++
- Internet Explorer (with Flash)
- File Explorer

- User Troubleshooting:
  - Restart Processes (Fix Pageant or Xming)
  - Show Processes (Shows the current user processes for the session)
  - Wireshark
  - ActivClient User Console
  - Set Logon Options

- Logoff (Used to logoff current session; useful during jump box maintenance or troubleshooting)

1.4 Jumpbox Configuration

- Workstation:
  - ActivClient
  - Axway Desktop Validator
  - Cisco AnyConnect
  - Virtual Desktop Infrastructure (VDI)
  - Remote Desktop Connection (RDP Client -- mstsc.exe)

- Enterprise Services:
  - Active Directory
  - Online Certificate Status Protocol (OCSP)
  - F5 (used for load balancing)
  - Infrastructure as a Service (IaaS) VMware Virtual Machines
  - IaaS IBM Blade Servers
  - PaaS Common Operating System (Using DISA's Server Image)

- RDS Jumpbox:
  - ActivClient
  - Axway Desktop Validator
  - Remote Desktop Web Access
  - Remote Desktop Connection Broker
  - Remote Desktop Session Host
  - Microsoft Application Virtualization (App-V) Server, Client, and Sequencer
  - Microsoft SQL Server 2014
  - Always On Availability Groups (SQL Server)
  - Remote Desktop Licensing Server
  - Failover Clustering (File Server)
  - User Profile Disk

1.5 Security Controls

The RDS Jumpbox runs a Windows 2012R2 Defense Information Systems Agency (DISA) image which is hardened to over 95% Security Technical Implementation Guide (STIG) compliance. Security patching is performed monthly as part of the enterprise patching process. Additional settings are applied, as needed, when new STIG settings are released and\or when a new finding occurs during a vulnerability scan.

Network firewalls exist at each network zone boundary to restrict communications. Here are some examples of the network zone boundaries:

CGOne	DMZ
Office Space	OSC Enterprise Services
Development	Zone 2 Restricted
Test	Zone 2 Unrestricted
Production	Zone 3 Restricted
OSC Enterprise Services	Zone 3 Unrestricted

Certain communications are not allowed by policy. For example, servers in DMZ Zone 2 Restricted are not allowed to initiate communication to servers in CGOne Stage. A firewall rule request for this would not be approved. In order for traffic to cross into a different network zone, there must be a completed, approved network firewall rule request to allow the communication.

The RDS Jumpbox servers reside in the CGOne OSC Enterprise Services network zone and may communicate with servers in any zone on specific ports. These ports include, but are not limited to, 22, 80, 443, 445, 1433, 1521, and 3389.

The network firewall prevents workstations, which reside in the Office Space network zone, from communicating with servers on port 22 (i.e. SSH). The RDS Jumpbox must be used in order for privileged users to login to target servers via SSH.

From the RDS Jumpbox, privileged users may login to their Linux and Unix servers via SSH using PuTTY. Pageant is used for the SSH key-based authentication. The authentication process will ensure that the SSH public key that is stored on the target server (e.g. ~/.ssh/authorized_keys) matches with the private key that is stored on their Alt-Token certificates. In order to access the private key on the Alt-Token certificates, the privileged users will be prompted for their Alt-Token smart card PIN. Provided the correct PIN is entered, the privileged users are successfully authenticated to their server. In order to login to subsequent servers, the process is repeated from the RDS Jumpbox. Authentication forwarding is not enabled to allow privileged users to establish a SSH connection to another Linux\Unix server from the first Linux\Unix server.

The DISA STIG settings have been implemented on both the RDS Jumpbox servers and the target servers. This includes the auditing\logging settings. Both the RDS Jumpbox server and the target servers also forward audit\log data to the Host Based Security System (HBSS) Security Information & Event Management (SIEM). The PaaS Operations team performs log reviews on both the RDS Jumpbox and the target servers.

Unified Infrastructure Management (UIM) is our enterprise monitoring tool. Warning and alarm thresholds are configured for various aspects of the server (e.g. specified service stops, low available disk space, server reboot, unreachable website, user added to local

group, local user created, etc.). When warning thresholds are reached, we receive an e-mail and take appropriate action. When alarm thresholds are reached, in addition to the e-mail, our 24x7 Data Center Support watch standers will begin contacting the on-call duty analyst to ensure the issue is addressed. UIM also offers reports on server metrics (e.g. CPU, memory, and disk).

RDPSoft, a Commercial off-the-shelf (COTS) product, has also been implemented on the RDS Jumpbox servers. This product gives us a central location to view the user activity on the RDS Jumpbox servers. Reports may be generated for various aspects of the user sessions (e.g. users per session host, process with highest process load, user login times, etc.).

The RDS Jumpbox servers reside in the CGOne network, which is an internal network.

Active Directory security groups are used to grant access to the RDS Jumpbox. Only privileged users that have completed, approved (PUMP) requests are granted access.

Privileged users login to the RDS Jumpbox using their Alt-Token smart card. This login process utilizes Active Directory (Kerberos) to use their domain accounts and OSCP servers to ensure their Alt-Token certificates are valid. They do not have administrative access on the RDS Jumpbox; they are standard users.

After successfully logging into the RDS Jumpbox, Pageant automatically starts and loads a reference to the users' Alt-Token certificates from their Windows user certificate store. PuTTY, WinSCP, and Pscp use Pageant for authentication. From the RDS Jumpbox, privileged users may login to their Linux and Unix servers via SSH using PuTTY. Pageant is used for the SSH key-based authentication. The authentication process will ensure that the SSH public key that is stored on the target server (e.g. ~/.ssh/authorized_keys) matches with the private key that is stored on their Alt-Token certificates. In order to access the private key on the Alt-Token certificates, the privileged users will be prompted for their Alt-Token smart card PIN. Provided the correct PIN is entered, the privileged users are successfully authenticated to their server. The ActivClient smart card software provides PIN caching, which times out after 15 minutes. While the PIN cache is valid, subsequent authentication attempts will be allowed to access the Alt-Token certificates' private key without prompting the privileged users. After the ActivClient PIN cache times out, the privileged users will be prompted for their Alt-Token smart card PIN on the next authentication attempt.

The privileged users' local accounts on each Linux and Unix server have their password disabled (i.e. password based authentication is not allowed).

The DISA STIG settings have been implemented on both the RDS Jumpbox servers and the target servers. This includes the following SSH configuration setting target servers:

Configuration File: /etc/ssh/sshd_config
Ciphers aes256-ctr,aes192-ctr,aes128-ctr

A local firewall (e.g. iptables) is implemented on each target Linux and Unix server. Connections to port 22 (i.e. SSH) on each target server are only allowed from the RDS Jumpbox IP Addresses.