Secure Access to Infrastructure Devices

June 2016

Privileged access to infrastructure devices allows access to resources that are normally unavailable to most users and permits the execution of actions that would otherwise be restricted. When privileged access on infrastructure devices are administered improperly, granted widely, or not closely audited, intruders are able to exploit them. Intruders can then move laterally through a network, gaining access and potentially full control of the infrastructure backbone. Secure access enables an administrator to maintain positive control of users accessing network infrastructure.

Standard fixed passwords are not enough to control device access, as effective access control calls for use of multi-factor authentication mechanisms. The recommended multi-factor solutions use hardware tokens (what the user has) that use a PIN or passphrase (what the user knows). Some also include options for biometric activation (what the user is). These tokens allow access and execution of actions on infrastructure devices. Security risks associated with default or weak passwords can be mitigated by properly implementing secure access methodologies and disabling password-based access. There are multiple secure access devices and techniques that are scalable and can be used to keep your networks secure depending on which method fits the requirement.



Implement Multi-Factor Authentication

Authentication is the process of confirming a user's identity. Weak authentication processes are commonly exploited by attackers. Multi-factor authentication uses more than one type of identity information including something the user knows, something the user has, or something the user is to verify a user's identity. Common multi-factor solutions include a combination of the following:

One-Time Password (OTP) Hard Token Authentication

OTP token authentication is a method that leverages the user's possession of a token and knowledge of a PIN to verify a user's identity. OTP tokens are compact and portable devices that allow the user to enter a PIN and then display a time-sensitive password. OTP token authentication is designed to protect credentials from reuse. Users enter this password into the Web or network application to authenticate their identity using an Authentication, Authorization, and Accounting (AAA) server. The AAA needs to be synchronized with the OTP tokens. The authenticator gives online service providers a highly secure means of offering their customers a protected online environment for carrying out network management, network maintenance, and access to trusted information online. One-time passwords and token authentication prevent malicious attacks that capture and reuse passwords.

Certificate-Based Authentication

Certificate-based authentication uses public and private encryption keys that are unique to the device and the user. Certificate-based authentication can be used to authenticate devices that support public key authentication, or to AAA or privileged access management servers. They can also digitally sign transactions, and individually issued credentials can support non-repudiation. Certificates can be issued to hardware devices such as USB tokens or smart cards and promote a high level of assurance.

Secure Access to Infrastructure Devices

Context-Based Authentication

Context-based authentication uses information such as location, time, device, and/or network to determine a user's identity. This method of authentication requires knowledge of who the user is, what the user is requesting, how the user is connected, and where the user is located. An example is requiring certain users to only access a particular network during specific times at particular locations. This authentication method is recommended as a complement to other strong authentication technologies.

Biometric Authentication

Biometric authentication is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, facial recognition, retina and iris patterns, and voice recognition. Biometric authentication has advanced considerably with the improvements to sensors.

Manage Privileged Access

One of the best practices to manage network access devices is to use a centralized Authentication, Authorization, and Accounting (AAA) server or a Remote Authentication Dial-In User Service (RADIUS) server. AAA servers store authentication (username and password) information for authorization. The AAA server enables network managers to assign different privilege levels to users based on permitted access and need-to-know. If a user tries to execute a command that is not authorized, it will be rejected. Use a certificate/token manager in addition to the AAA server for strong authentication when using hard tokens. This type of control makes it more difficult for intruders to steal and re-use credentials to gain access to network devices. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and returning configuration information to the client according to the user. RADIUS servers allow for user profiles to be kept in a central database. Communications between the client and RADIUS server are authenticated through the use of a shared key. Any user passwords that are sent between the client and the RADIUS server are also encrypted.

Manage Administrative Credentials

Multi-factor authentication, which includes a hard token and a PIN or passphrase is the best practice for securing privileged credentials. Additionally, the DoD requires the use of hard tokens (DoDI 8520). Systems that cannot meet these practices can at least improve their security level by enforcing strong password policies. Network accounts should contain complex passwords of at least 14 characters using letters, numbers, and symbols. Simple passwords can be guessed. Regularly change passwords for all network accounts and ensure the passwords are different from other accounts. Do not keep passwords in on-line directories. If passwords are stored, keep these in a protected, off-network location, such as a safe. Training and consistent communication with all employees about protecting credentials is essential. In order to develop a robust authentication solution, organizations should consider their business, risk, and select a solution that provides them with flexibility to adapt as needed to different risk environments.

Contact Information

Industry Inquiries:

Business Affairs Office
410-854-6091
email: bao@nsa.gov

Client Requirements and General Information Assurance Inquiries:

IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov

Disclaimer: The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.