Sistema de Doble Factor de Autenticación para VPN de Acceso Remoto

Especificaciones Técnicas

[Enero 2025]

Indice

Propósito

Las siguientes especificaciones técnicas tiene por objeto la provisión de un sistema que brinde el servicio de autenticación de doble factor (2AF) para integrar al servicio de VPN existente y brindar mayor seguridad al acceso remoto.

Además de la provisión de los componentes que se requieran para este sistema , el oferente deberá cotizar los servicios de instalación , configuración y capacitación en el uso de la herramienta.

Alcance

La solución propuesta deberá tener compatibilidad completa con el fabricante Fortinet ya que deberá integrarse al servicio de VPN actual para brindar la seguridad de doble factor al acceso remoto en modo túnel y web-ssl .

Tiene que dar soporte a doscientos (200) usuarios y de acuerdo a lo anterior, deberá tener full compatibilidad con los dos (2) appliance Firewall FortiGate que brindan el servicio de VPN SSL e IPSec para el Poder Judicial. Deberá ser posible escalar el servicio a mayor cantidad de usuarios a futuro.

Los usuarios referidos son aquellos que utilizan el servicio de VPN de acceso remoto provisto por el Poder Judicial.

Todas las tareas deberán ser coordinadas previamente con el personal de la SIJ involucrado en este proyecto y quienes supervisarán todo el proceso.

Requerimientos

El sistema tendrá que ser del tipo centralizado que provea el servicio de autenticación multifactor . En este sentido tiene que permitir la generación del token desde dispositivos móviles ,computadoras y/o mediante dispositivos físicos dedicados (llaveros). Para el caso de los dispositivos el sistema deberá ser compatible con los sistemas operativos Windows, Android e IOS.

Los componentes necesarios del sistema deberán ser dimensionados para la cantidad de usuarios establecido considerando además un crecimiento del doble de usuarios.

La implementación de la infraestructura requerida deberá llevarse a cabo sobre la plataforma de nube Huawei en el espacio perteneciente al Poder Judicial. Por esta razón la infraestructura ofertada deberá ser en formato de máquina/s virtual/es y compatible para su instalación y funcionamiento en dicho entorno de nube.

El sistema deberá dar servicio de autenticación de doble factor para el servicio VPN de acceso remoto que funciona en la infraestructura que se decribe a continuación.

Los appliances existentes que controlan el servicio de VPN son del fabricante Fortinet y son firewalls modelos :

- Fortigate 300E v7.2.8 , appliance físico ubicado on premise, en el centro de cómputos del Superior Tribunal de Justicia.
- Fortigate VM64-KVM v7.2.10, appliance virtual ubicado en la plataforma de nube Huawei dentro del espacio del Poder Judicial.

Funcionalidades del sistema

El sistema en general deberá cumplir como mínimo con las siguientes características

- Permitir políticas de seguridad basadas en identidad y en roles sin necesidad de autenticación adicional a través de la integración con Active Directory.
- Gestión de la información de indentidad del usuario de manera centralizada.
- Soporte para la autenticación multifactor (SMS, aplicaciones móviles , dispositivos token) y OTP

- Soporte para integrar la autenticación RADIUS , LDAP y Active Directory.
- Gestión de certificados para la implementación de VPNs
- Soporte para 802.1x para seguridad de redes inalámbricas y cableadas
- Soporte de SAML SP / IdP Web SSO
- Soporte OpenID Connect SSO
- Soporte para funcionalidad FIDO2

Instalación y Puesta en servicio

El servicio deberá incluir el proceso de instalación y configuración de la solución de acuerdo a lo descrito en la sección Alcance y sección Requerimiento. Este proceso deberá incluir las pruebas necesarias para dejar el servicio completamente operativo. Para esto y en conjunto con el personal de la Secretaría de Informática Jurídica, el oferente realizará el diseño de los casos de pruebas para la verificación de la funcionalidad requerida de la solución propuesta.

El oferente deberá capacitar a dos personas del Poder Judicial en los aspectos de la configuración y gestión de la solución incluyendo tareas de mantenimiento. Dicho personal posee lo conocimientos necesarios para la administración de los appliances referidos en la sección Requerimientos

El oferente deberá presentar un plan de trabajo que será evaluado por la SIJ donde detalle la secuencia de tareas a realizar y tiempos de ejecución, incluyendo la capacitación , la provisión e instalación del appliance, el proceso de implementación de la configuración y las pruebas para verificar la conectividad y funcionalidad del servicios . El plan podrá ser modificado de acuerdo al criterio de la SIJ en caso de ser necesario.

En caso de ser necesario se podrá consultar a la SIJ cualquier duda o consulta respecto a la plataforma ya instalada.

Confidencialidad de Datos e Información

El adjudicatario queda sujeto al deber de confidencialidad respecto de datos y/o programas de propiedad o custodia del Poder Judicial. Las actividades desarrolladas por el adjudicatario no habilitarán a la copia, de datos, programas y configuraciones pertenecientes o en custodia del Poder Judicial para su posesión y posterior uso en otros ámbitos.

Tiempo de ejecución

Se prevee un máximo de treinta (30) días para las tareas de implementación a la puesta en servicio de la solución.

Licencia de uso

La licencia de uso para la infraestructura y servicios de la solución ofertada deberá ser por treinta y seis (36) meses. Esta incluirá la licencia por los usuarios requeridos , las actualizaciones del sistema y la de sus funcionalidades de seguridad.

Antecedentes del Oferente

En este sentido el oferente deberá contar con las certificaciones y homologaciones correspondientes del fabricante Fortinet para integrar la solución ofertada . En igual sentido, para las tareas referidas de instalación, configuración , puesta en servicio y capacitación de la solución.

Garantía y Soporte

El proveedor deberá considerar un (1) año de garantía para la solución implementada incluyendo en este período el soporte por consultas técnicas. Deberá contar con un servicio de atención de consultas o reclamos con un plazo máximo de 24 hs. para los días hábiles (Lunes a Viernes).