Funcionalidades Generales

Se puede entregar en una única solución o conjunto de soluciones, siempre que cumpla con todos los requisitos

Licenciamiento deberá ser basadas en hardware, no en recursos

Admite la opción de implementar en entornos virtualizados en los siguientes proveedores de nube pública: Microsoft Azure y Amazon AWS

La solución debe soportar implementación en hardware o en ambientes virtualizados, en nubes privadas o nubes públicas

La solución debe soportar crecimiento adaptativo de usuarios a traves de licenciamiento (en caso de opción virtualizada)

La solución debe soportar implementación en las plataformas de virtualizacióno VMware ESXi 6.0/6.5, Microsoft Hyper-V 2012 R2 / 2016 y Xen

La solución debe soportar número ilimitado de vCPUs en implementación en ambientes virtualizados

La solución debe soportar administración vía interface gráfica (GUI) por HTTP / HTTPS

La solución debe soportar administración por línea de comandos (CLI) utilizando Telnet / SSH

Permite definir perfiles de administradores para una solución, de modo que puede segmentar la responsabilidad de los administradores por tareas operativas

Incluya un indicador visual centralizado de información crítica (estado de la licencia, versión de firmware, consumo de CPU / memoria / disco, número de usuarios creados y con licencia)

La solución debe soportar actualización de firmware a través de la interfaz gráfica, mediante un proceso simplificado e intuitivo

La solución debe soportar la personalización de mensajes de solución estándar como páginas de error, portales de autenticación, autorregistro, restablecimiento de contraseña y otros. También

La solución debe soportar la inclusión, alteración y eliminación de imágenes en mensajes / páginas sin la necesidad de recursos o conectividad externa

La solución debe soportar la configuración de alta disponibilidad (HA), minimizando el tiempo de inactividad

La solución debe soportar implementaciones de HA como "Active-Passive" o configuraciones de sincronización entre dos unidades activas

La solución permite la sincronización automática de configuraciones entre todos los equipos que componen la solución HA

La solución debe soportar la implementación de HA sincronizando configuraciones con dispositivos en ubicaciones geográficamente separadas

La solución debe soportar la opción de copia de seguridad cifrada

La solución debe soportar copias de seguridad automatizadas (programadas por criterios predefinidos), no solo bajo demanda

La solución debe soportar copia de seguridad completa de la configuración, incluida la base de usuarios, grupos, tokens, certificados, configuraciones de inicio de sesión único, etc. La solución también Permite la restauración de toda la configuración directamente desde la interfaz gráfica

La solución debe soportar NTP (Protocolo de tiempo de red), con el objetivo de sincronización de hora / fecha

La solución debe soportar ruteo estático

La solución debe soportar SNMP v1, v2 e v3 permitiendo consultar MIBs propias y envío de SMNP Traps
La solución debe soportar nativo SNMP Trap que indica un cambio de estado en el HA
La solución debe soportar la captura de paquetes a través de la interfaz gráfica para solucionar problemas avanzados en herramientas de análisis de paquetes (por ejemplo, Wireshark)
La solución debe soportar el envío de correos electrónicos actuando como su propio servidor (localhost) o integración con servidores externos para enviar mensajes a usuarios o administradores
El equipo permite el envío de correos electrónicos relacionados con el restablecimiento de la contraseña, la aprobación de nuevos usuarios, el auto registro del usuario y la autenticación de segundo factor (vía token).
Permita el envío de mensajes SMS a los usuarios a través de gateway SMS de terceros
La solución debe soportar el registro de todos los eventos que los usuarios de su base de datos local realizan con sus cuentas, como crear un usuario, cambiar la contraseña de un usuario y cambiar la información general

Funcionalidades de la autenticación
La solución debe realizar la autenticación para la gestión de identidad de los usuarios de la red, siendo un punto central de control de autenticación, donde se pueden consolidar múltiples métodos de autenticación
La solución debe soportar autenticación de dos factores (two-factor authentication)
La solución debe soportar autenticación de dos factores en al menos dos tipos diferentes de tokens, el primero es físico (token) y el segundo lógico como software para dispositivos móviles
La solución debe permitir la definición de un nivel de complejidad mínima para las contraseñas de todos los usuarios registrados en la base de datos local, permitiendo la definición de un número mínimo de letras minúsculas, mayúsculas, caracteres numéricos, caracteres especiales, etc.
La solución debe permitir la creación de una política de bloqueo automático de usuarios después de una serie de fallas de autenticación, evitando así los ataques de fuerza bruta
La solución debe soportar la creación de usuarios a nivel local, que se puede utilizar para autenticar dispositivos según sea necesario.
La solución debe permitir la creación masiva de usuarios en la base de datos local mediante la importación de una lista de usuarios que se creará en archivos externos.
La solución debe permitir la creación de nuevos usuarios en la base de datos local y que el administrador pueda definir una contraseña al momento de crearlos.
La solución debe permitir la creación de nuevos usuarios en la base de datos local y que el equipo genere una contraseña aleatoria y la envíe automáticamente al usuario.
La solución debe permitir la creación de nuevos usuarios en la base de datos local sin la definición de una contraseña, requiriendo que use el token como el único factor de autenticación
Permite asociar tokens a usuarios creados localmente en la base de datos
Permite a los propios usuarios registrar sus tokens e informar la pérdida de un token automáticamente, sin la necesidad de involucrar a un administrado
Eliminación automática masiva de usuarios inactivos, según criterios definidos

La solución permite a los usuarios locales restablecer sus contraseñas de manera segura, sin la intervención de los administradores, por correo electrónico o preguntas de seguridad en portal de autoservicio.
La solución debe soportar la creación de grupos de usuarios, que pueden usarse para autenticar uno o varios dispositivos.
Los tokens deben generar códigos con un mínimo de 6 dígitos e intervalos que no excedan los 60 segundos
La solución debe soportar autenticación de dos factores por hardware dedicado (token)
La solución debe soportar autenticación de dos factores por aplicación móvil (iPhone y Android)
La solución debe soportar autenticación de dos factores enviando un mensaje SMS
La solución debe soportar autenticación de dos factores mediante el envío de correo electrónico.
La solución debe soportar sincronización de dispositivos en hardware de generación OTP (one time password)
Permite sincronizar los tokens con el equipo para su correcto funcionamiento.
Permite desactivar un token cuando es robado o perdido, permitiendo su reactivación posterior cuando / si se recupera
Permite la disociación de un token a un usuario y asociarlo con otro usuario cuando sea necesario, permitiendo así su reutilización
Permite la autenticación de doble factor en clientes Windows, incluso con la máquina fuera de línea
Debe proporcionar un portal web para que los usuarios se registren automáticamente, de modo que puedan acceder, completar sus datos y enviar el registro. Después de que el usuario inicia sesión, el administrador debe ser notificado automáticamente para aprobar o denegar el registro del usuario antes de que el usuario sea activado.
La solución debe funcionar como un servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticación a dispositivos compatibles con dicho protocolo
La solución La solución debe soportarr la integración con el servidor RADIUS remoto
La solución puede funcionar como un servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticación a dispositivos compatibles con ese protocolo
La solución debe tener un servidor LDAP interno que permita su configuración jerárquica, para la correcta administración por grupos o unidades organizativas de usuarios locales.
La solución debe soportar la integración con un servidor LDAP remoto (como Microsoft Active Directory)
La solución debe soportar la autenticación de usuarios con credenciales de redes sociales como Facebook, Twitter y LinkedIn
La solución debe permitir a los usuarios que no tienen una cuenta local o de redes sociales autenticarse a través de un registro rápido, que garantice una trazabilidad mínima, a través de la validación de direcciones de correo electrónico o números de teléfono.
La solución debe permitir el inicio de sesión automático de los usuarios visitantes después de que se hayan registrado con éxito
La solución debe permitirle configurar los parámetros de red (como la configuración de WiFi) en un dispositivo de usuario (laptop, móvil) mediante la descarga de un script o un archivo ejecutable a través del portal de visitantes.

La solución debe soportar el lenguaje de marcado de aserción de seguridad (SAML), que actúa como un proveedor de identidad (IDP), estableciendo una relación de confianza para la autenticación segura de los usuarios que intentan acceder a un Proveedor de Servicios (SP)

Funcionalidades de Single Sign-On

La solución debe proporcionar la capacidad de servicio SSO (Single Sign-On), con autenticación transparente de usuarios (pasiva) en sistemas compatibles

Debe poder integrarse con un directorio activo (Windows AD) y poder ofrecer la funcionalidad SSO, donde la autenticación automática / transparente a través de SSO para los servicios necesarios se basa en la autenticación previa del usuario en el dominio

Permite definir una lista de usuarios de SSO que serán ignorados, evitando así la interferencia de cuentas de servicio como antivirus o scripts a través de GPO

La solución debe soportar el análisis de archivos syslog enviados desde una fuente remota, para uso del servicio SSO

La solución debe soportar el Security Assertion Markup Language (SAML), para solicitar información de identidad del usuario a Proveedores de identidad (IDP) de terceros.

La solución debe soportar SSO basado en radio (RSSO - RADIUS Single Sign-On)

La solución debe soportar el RSSO RADIUS Accounting Proxy, que permite la recepción de paquetes de radio de búsqueda, la modificación de estos paquetes y el reenvío de ellos a varios otros puntos

Requerimientos técnicos de implementación

1- Empresa con técnico certificado en: solución ofertados y CEH, ITIL Foundation y 10 años de experiencia en implementaciones de la solución, Unico ingeniero. (No se permiten certificaciones individuales)

2- Certificación del fabricante de distribución autorizado

3- Servicios técnicos basados en la migración de los equipos actuales y nuevos requerimientos

4- Logística de distribución de equipos en todo el país

5- Precio final debe de incluir viáticos de implementación.