Arabako Kalkulu Gunea, A.B.
Centro de Cálculo de Álava, S.A.

SUMINISTRO, INSTALACIÓN Y CONFIGURACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A LA RED (NAC)

PLIEGO DE PRESCRIPCIONES TÉCNICAS. EXP 2021020

OBJETO:

El objeto de este pliego consiste en el suministro, la instalación y la configuración de un sistema de control de acceso a la red (NAC) de la DFA.

1. Antecedentes y situación actual

La DFA dispone de un sistema que controla el acceso a la red (RADIUS) de todos los usuarios tanto por cable como por wifi, así como el acceso a la configuración de la electrónica de red (TACACS+).

Este sistema se encuentra fuera de mantenimiento y es necesaria su renovación.

En el documento de “Situación actual” se describe el detalle de la actual solución de control de acceso a la red de la DFA, sus funciones y los componentes de red con los que se integra.

Por motivos de seguridad de DFA, en el presente pliego no se publica el documento de “Situación actual”. Los interesados en el proceso de licitación deberán solicitarlo de las fuentes en la dirección de correo electrónico licitacion_CCASA@araba.eus indicando:

- Nº de expediente
- Empresa solicitante
- Nombre del contacto
- Correo electrónico
- Número de teléfono del contacto

La información contenida en el Documento de Situación Actual no será facilitada a empresas que por su tipología y en opinión de DFA no tengan interés legítimo en participar en el proceso.

2. Características de la solución

El sistema de control de acceso a la red propuesto debe soportar las siguientes características:

- Alta disponibilidad: El sistema debe permitir configuraciones en alta disponibilidad con dos appliances que permitan seguir prestando el servicio en caso de caída de uno de ellos. Los appliances funcionarán en modo activo-activo. El sistema admitirá configuraciones de appliances tanto físicos como virtuales. Se soportará la creación de Virtual-IP Address (VIP) entre dos nodos de la solución de NAC sin requerir elementos externos.

- Validación RADIUS de usuarios y dispositivos integrándose con el protocolo 802.1x con autenticación:
    - RADIUS, RADIUS CoA, TACACS+, Web authentication, and SAML v2.0
    - EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
    - PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public)
    - TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
    - EAP-TLS
    - EAP-TEAP (Tunneled EAP)
    - PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5
    - Wireless and wired 802.1X and VPN
    - OAuth2
    - Microsoft NAP and NAC
    - Windows machine authentication
    - Online Certificate Status Protocol (OCSP)
    - SNMP generic MIB, SNMP private MIB
    - Common Event Format (CEF), Log Event Extended Format (LEEF)

Se deberá soportar el envío de CoA (Change of Authentication) mediante atributos RADIUS estándar a equipos Wired y Wireless. No será necesario proporcionar credenciales de administración para ejecutar el CoA.

- Validación de dispositivos por MAC. La gestión de las MAC´s podrá ser centralizada.

- Validación TACACS. Debe permitir la validación TACACS para el acceso a la configuración de los dispositivos de red definidos en el documento de situación actual. Dicha validación admitirá la definición de "comand sets" que pueden ejecutar los diferentes administradores para permitir diferentes niveles en la administración.

- Perfilado: Debe permitir identificar de forma automática, en base al tráfico cursado y sin necesidad de instalación de agentes en el dispositivo de usuario, las siguientes características del mismo:

    - Si el dispositivo que se conecta es una impresora, un terminal de fichajes, una cámara de vigilancia, un PC, un portátil, un smartphone, una tablet, …

    - El fabricante

    - El tipo de Sistema Operativo: si el PC es Windows, MAC, Linux… si el smartphone es Android, iOS, …

  Para el perfilado se admitirán los siguientes mecanismos:

    - Activos: NMAP, WMI, SSH, SNMP

    - Pasivos: MAC-OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFlow, Span Port, HTTP User-Agent, IF-MAP

  El sistema deberá disponer de firmas de perfilado incorporadas, pudiéndose realizar actualizaciones de las mismas.

  El sistema detectará automáticamente posibles conflictos en el perfilado y marcará los endpoints si detecta incongruencias.

  El sistema deberá realizar descubrimiento y perfilado de dispositivos sin necesidad de equipos adicionales en sedes remotas.

  Este perfilado se podrá utilizar para determinar la red a la que se asigna al dispositivo o el tráfico que se le permite.

- Bring Your Own Device (BYOD). Debe permitir:

- Facilitar la descarga de certificados a los dispositivos móviles corporativos minimizando la carga de trabajo en el departamento de TI.
- Comprobar los certificados en los dispositivos móviles corporativos para facilitarles el acceso a la red corporativa.
- Los usuarios dispondrán de un acceso seguro para conocer los dispositivos que tienen asociados un certificado y revocar/eliminarlos de forma personalizada. Este acceso será configurable y opcional para los usuarios.
- Se podrá limitar el número de dispositivos que pueden disponer de certificado para cada usuario corporativo.
- Para los dispositivos móviles personales redirigirlos a una red con acceso exclusivo a internet y portal cautivo.

- Comprobación de salud del endpoint (Posture). debe permitir la comprobación de características del puesto para su admisión a la red:
  - La distribución de Windows 10: (si es la 20H2, …)
  - Si tiene instalados los últimos parches de Sistema Operativo
  - Si tiene antivirus instalado
  - Si el antivirus está actualizado
  - Bloqueo de los puertos USB
  - Detección de programas P2P

  Para entornos Windows, se soportará la comprobación se salud del dispositivo mediante WMI sin necesidad de agente.

- NAC. Una vez identificado el usuario/dispositivo, debe permitir:
  - Realizar simulaciones de políticas de seguridad antes de su implantación
  - Autorizar el acceso en función de características como pertenencia a un grupo de usuarios, tipo de dispositivo móvil, aplicación utilizada, localización del dispositivo, estado de salud del dispositivo, etc.
  - Asignarle a una VLAN concreta o aplicarle ACL´s

- Aplicar políticas en base a calendarios/horarios

- Portal cautivo. Permitirá:
  - Definir portales diferentes, con diferentes métodos de autenticación, en función del SSID y de la red.
  - Limitar la duración de la conexión.
  - Autorregistro de usuarios (con mensaje al correo electrónico, SMS al móvil o integración con redes sociales) sin necesidad de partición de personal de TI. Soportará la posibilidad de definir un periodo de cortesía con acceso libre a la red wifi para poder consultar el correo.
  - Integración con la plataforma de envío de mensajes SMS de la DFA definida en el documento de situación actual.
  - Registro basado en sponsor: se define una persona a la que llegan las solicitudes de acceso y que puede aprobarlas o denegarlas, sin necesidad de participación de personal de TI. Para ello el portal permitirá menús desplegables que permitan registrar información relativa al invitado (motivo de la visita, duración de la misma, persona a la que visita, y cualquier opción adicional).
  - Los portales cautivos permitirán personalizar el look&feel de forma completa, con posibilidad de adaptación del código HTML completo y de las hojas de estilo CSS.
  - Interface web responsive.
  - Presentación del portal en hasta 3 idiomas según el idioma definido en el navegador del usuario.
  - Posibilidad de incluir todo de tipo de contenido multimedia en el portal: imágenes, audio, video, etc… que varíe de forma dinámica según patrones establecidos.
  - Borrado automático de usuarios autorregistrados al cabo de un tiempo establecido.
  - El sistema debe proporcionar un interfaz web para que un operador pueda registrar a los usuarios manualmente mediante impresión de tickets para aquellos casos en los que no sea posible el autorregistro (p.e. para usuarios extranjeros para los cuales el sistema de envío de mensajes SMS de la DFA no permite el envío de SMS´s a móviles internacionales).

- Informes. Facilitará los siguientes informes:

- Se podrá emitir tanto informes de alto nivel en formato PDF como con los datos en bruto en formato CSV.
- Se deberán poder hacer informes bajo demanda de autenticaciones satisfactorias y fallidas en periodos de tiempo limitado.
- Dispositivos conectados a la red en cada momento (número y tipo).
- Detalles de cada conexión: usuario, dispositivo de usuario, en qué dispositivo de red y puerto se han conectado, cuándo.
- Alertas.
- El portal cautivo proporcionará informes de actividad relativa al tráfico de invitados: número de visitas, numero de SMS enviados con credenciales, etc.

- Integraciones con los siguientes sistemas detallados en el documento de situación actual:
  - Active Directory de Microsoft: debe permitir la validación en el acceso a la red de los usuarios y equipos definidos en el AD de la DFA. Debe permitir integración con múltiples AD´s (al menos 5)
  - Gestor de logs: debe permitir el envío de syslog a la herramienta de gestión de logs. Los mensajes de Syslog podrán filtrarse en función de diferentes tipos de eventos y a servidores diferentes. El sistema soportará mensajes de Syslog en los siguientes formatos: Standard, LEEF, CEF y RFC5424.
  - SIEM: debe permitir el envío de equipos a una red de remediación ante la recepción de alertas de seguridad procedentes del SIEM.
  - Antivirus: debe permitir el envío de equipos a una red de remediación ante la recepción de alertas de seguridad procedentes del sistema de antivirus corporativo.
  - Firewall: Debe permitir que los firewalls deleguen la autenticación de usuarios en el sistema de control de acceso a la red.
  - Balanceador: Debe permitir que el balanceador delegue la autenticación de usuarios en el sistema de control de acceso a la red.

  El sistema soportará la recepción de eventos vía Syslog para ejecutar acciones sobre la infraestructura de acceso, desconectando usuarios o cambiándoles de VLANs.

El sistema deberá poder exportar a sistemas de terceros información contextual de los usuarios autenticados: username, dispositivo usado, estado de salud, punto de conexión, etc.

3. Productos y/o servicios a entregar

Se deberá suministrar los siguientes productos y servicios:

3.1 Productos

En concreto, deberá suministrarse la siguiente solución de acceso a la red:

- Compuesta por dos appliances constituidos en alta disponibilidad, de modo que, ante la caída de uno de ellos, el servicio se siga prestando por el otro. Los appliances pueden ser físicos o virtuales. En este último caso tendrán que ser compatibles con la plataforma de virtualización de la DFA detallada en el documento de situación actual.

- Cada uno de los appliances debe estar dimensionado para soportar, al menos, hasta 5.000 usuarios simultáneos.

- Licenciada para, al menos, el siguiente número de dispositivos:

    - 2.500 dispositivos de usuario para validación RADIUS, todos ellos con funcionalidades de perfilado.

      De ellos, 700 requieren, además, funcionalidades BYOD.

      De ellos, 300 pueden ser usuarios invitados en el portal cautivo

    - 600 dispositivos de red para validación TACACS.

3.2 Servicios

- **Instalación**

El proveedor deberá realizar, conjuntamente con los técnicos de CCASA, la instalación y configuración de la solución de acceso a la red descrita anteriormente hasta que esté plenamente operativa e integrada con el resto de instalación de la DFA.

A modo orientativo y no excluyente:

- Instalación de los appliances
- Configuración en alta disponibilidad
- Traspaso de las reglas y políticas del sistema de control de acceso a la red actual al nuevo
- Configuración de la validación RADIUS de los usuarios y dispositivos definidos en los directorios activos de la DFA (Hasta 5 Directorios Activos). Esta validación deberá integrarse con el protocolo 802.1x con autenticación MSCHAPv2, EAP-TLS y PEAP.
- Configuración de la validación por MAC con gestión centralizada.
- Configuración de la validación por TACACS para acceso a la administración de los dispositivos de red. Se deberán definir dos distintos perfiles de administración.
- Configuración del perfilado que permita identificar el tipo de dispositivo, el fabricante, el tipo de Sistema Operativo. Definición de reglas de validación específicas para determinados grupos de dispositivos como, por ejemplo, impresoras.
- Configuración del sistema BYOD que permita:
    - Facilitar la descarga de certificados a los dispositivos móviles corporativos.
    - Comprobar los certificados en los dispositivos móviles corporativos para facilitarles el acceso a la red corporativa.
    - Para los dispositivos móviles personales redirigirlos a una red con acceso exclusivo a internet y portal cautivo.

- Configuración del sistema NAC: diseño, definición e implementación de las políticas de acceso. Una vez identificado el dispositivo/usuario, se aplicarán políticas diferentes, asignándole a una VLAN concreta o aplicándole ACL´s, todo ello en función del dispositivo, la pertenencia del usuario a grupos del AD y/o un calendario/horario.

- Configuración de dos portales cautivos:

    - Ambos se configurarán web responsive y se presentarán en hasta 3 idiomas en función del idioma definido en el navegador del usuario. Se personalizará el interfaz web.

    - Uno de ellos para empleados con dispositivos personales que se integrará con el AD de la DFA, de modo que puedan identificarse con su usuario/contraseña de AD.

    - Otro para público en general con autorregistro mediante envío de mensaje SMS. Para ello, deberá hacer uso de la plataforma de envío de mensajes a móviles de la DFA. Los usuarios autorregistrados se deberán dar de baja de forma automática, transcurrido un determinado periodo de tiempo. Este portal se configurará, además de para usuarios Wireless, para PC´s cableados de uso público disponibles en una de las bibliotecas de la DFA.

- Configuración de las siguientes vistas e informes:

    - Dispositivos conectados a la red en cada momento (número y tipo).

    - Gráficas horarias de conexiones.

    - Detalles de la conexión: usuario, dispositivo de usuario, en que dispositivo de red y puerto se han conectado y cuándo.

    - Alertas.

- Configuración de las siguientes integraciones:

    - Integración con los directorios activos de la DFA y entes afines (hasta 5) para permitir el acceso a la red a aquellos usuarios y equipos definidos en el directorio Activo.

    - Integración con los firewalls definidos en el documento de situación actual para redirigir las peticiones http/https de la red de invitados al portal cautivo que suministra la herramienta.

- Se configurará el sistema de acceso a red de modo que, ante la recepción de alertas provenientes del SIEM de la DFA, se envíen los equipos afectados a una red de remediación.

- Se configurará el sistema de acceso a red de modo que, ante la recepción de alertas provenientes de la plataforma corporativa de antivirus de la DFA, se envíen los equipos afectados a una red de remediación.

- Se configurará el sistema de control de acceso a la red para el envío de syslog a la herramienta de gestión de logs de la DFA.

- **Documentación de la instalación**

El adjudicatario deberá entregar la documentación técnica de proyecto con la configuración y arquitecturas resultantes del sistema de acceso a la red implantado.

- **Formación**

La instalación de la solución de acceso a la red se realizará de forma conjunta con los técnicos de CCASA, de modo que se produzca una transferencia de conocimientos para que estos sean capaces de administrar el sistema.

Además, se deberá incluir un curso de formación con las siguientes características:

- On line
- Preferentemente en castellano
- Oficial del fabricante de la solución de acceso a la red para la administración de su herramienta
- Con una duración mínima de 5 días
- Para dos asistentes.

- **Otros**

Además de los trabajos descritos anteriormente, deberán entregarse todos aquellos productos/trabajos necesarios para dejar la nueva infraestructura plenamente operativa e integrada con la instalación informática de la DFA, aunque no se hayan detallado en la relación anterior.

3.3 No es objeto del presente pliego

No es objeto del presente pliego los siguientes suministros o trabajos:

- Configuración de los switches y Access Points de la red de la DFA: CCASA configurará estos dispositivos para que consulten al servicio RADIUS y TACACS del nuevo sistema de control de acceso a la red con las pautas que marque el adjudicatario.
- Control del despliegue de certificados a los dispositivos móviles corporativos.
- Licencias o configuraciones para la comprobación del estado de salud del puesto (posture)