**Introducción.**

En este documento se trata de explicar el funcionamiento del servidor radius así como las implicaciones y requerimientos necesarias para el mismo

**Detalle.**

DCS dispone de un sistema de conexión VPN con doble factor de autenticación sobre Radius (implementado en un servidor Windows con rol NPS).

Cliente “X” inicia app de VPN (Checkpoint) y autentica con username, password + segundo factor de autenticación; en caso de que las respuesta sea positiva, el cliente de VPN permite al cliente “X” conectar contra el entorno de trabajo; por ejemplo: IBM database

Se dispone de un servidor Radius, el cual recibe peticiones de acceso desde el firewall del cliente VPN administrado por deloitte (autenticaciones de usuarios o cliente X), estas peticiones son consultadas por radius apuntando al controlador de dominio (Windows server 2019) donde está ubicado un grupo de seguridad: basic access. Este grupo basic access contiene los miembros dados de alta en el Active Directory de este “Domain Controller”. De modo que los usuarios que forman parte de este grupo de seguridad tienen permitida la conexión a la VPN. Toda esta consulta se encuentra en un entorno “premise” alojado en servicios web: AWS

Por otro lado, DCS tiene una hibridación de sus Domain Controllers con Azure a través del servicio/programa “Azure AD connect”. Por seguridad, los usuarios (en Azure) disponen de doble factor de autenticación (MFA) a nivel global. En otras palabras, si un usuario trata de autenticar en su servicio de office365 en un equipo, dispondremos de una petición de usuario, contraseña + doble factor (app authenticator, sms, llamada…)

Retomando el asunto del servidor radius; radius contacta con el DC (premise) para comprobar que el usuario pertenece al grupo correspondiente (basic Access) y lanza una petición de acceso a Azure (hay un servicio en radius que ataca a Azure previamente instalada). Si azure recibe autenticación correcta (MFA incluido) contestan al radius para que este indique al firewall checkpoint que la conexión está permitida o denegada

**Diagrama orientativo.**

Diagrama, Esquemático

Descripción generada automáticamente

**Implicados.**

* **Cliente:** Checkpoint VPN
* **Firewall VPN checkpoint:** 10.160.130.10
* **VPC AWS:** Entorno de seguridad
* **Servidores Microsoft:**
  + **Domain controller:** 10.160.108.54
    - Usuario Checkpoint AWS Tier 0
  + **Radius:** 10.160.132.37. RADW00SEGAWS01.dcs.es
    - Usuario administrador global de Azure Tier 1 (script contra Azure)
    - Usuario administrador dominio Tier 0 (conexión contra DC)
* **Azure:** dinersclub.es
* **IBM i database:** 192.168.47.1

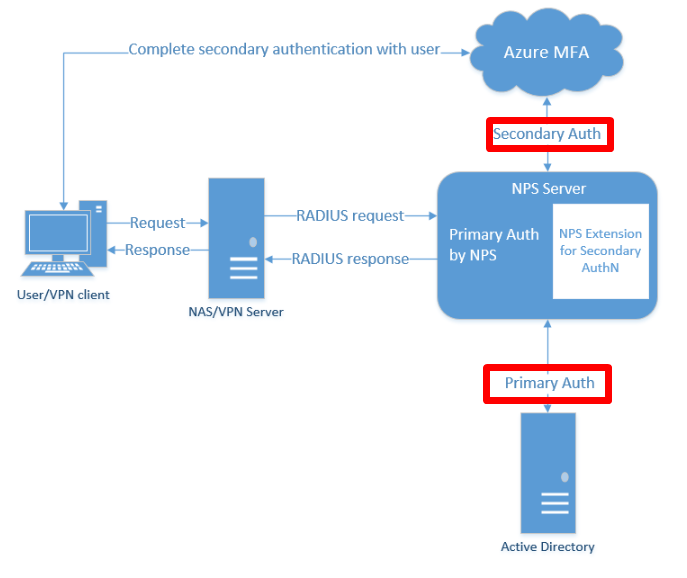
**Requerimientos.**

* Servidor Microsoft Windows unido a dominio con rol NPS; 2 CPU y 8GB RAM
  + .NET Framework 4.7.2 o superior
  + PowerShell versión 5.1 o superior
  + Librería VS 2017 C++
  + Microsoft Graph powershell
  + Software de extensión NPS
* Información tenant ID de la organización
* Usuario de Azure registrados en MFA. https://aka.ms/mfasetup
* Pruebas de red:
  + Puertos TCP-80 y TCP-443 permitidos de salida hacia Azure
  + Puertos UDP-1812, UDP-1813 e ICMP destino servidor Windows server Radius origen firewall checkpoint VPN
  + Conectividad entre radius y domain controller por el puerto 3268
  + Usuario administrador global Azure
  + Usuario administrador de dominio
  + Pruebas DNS por puerto 443:
    - https://login.microsoftonline.com
    - https://login.microsoftonline.us (Azure Government)
    - https://login.chinacloudapi.cn (Microsoft Azure operated by 21Vianet)
    - https://credentials.azure.com
    - https://strongauthenticationservice.auth.microsoft.com
    - https://strongauthenticationservice.auth.microsoft.us (Azure Government)
    - https://strongauthenticationservice.auth.microsoft.cn (Microsoft Azure operated by 21Vianet)
    - https://adnotifications.windowsazure.com
    - https://adnotifications.windowsazure.us (Azure Government)
    - https://adnotifications.windowsazure.cn (Microsoft Azure operated by 21Vianet)

**Fuente instalación office.com**

Una vez cumplidos todos los requerimientos anteriores, se procede a la instalación siguiendo la documentación oficial de Microsoft

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-nps-extension>



**Información del servidor y mantenimiento**

* Update habitual de Microsoft y posterior reinicio. Dicho reinicio NO implica pérdida de servicio salvo que el usuario desconecte el cliente durante el proceso. En ese caso y tras inicio del servidor radius el usuario podrá volver a autenticar
* Usuario de conexión remota: Tier 0
* Servicio NPS arrancado en el servidor

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* Propiedades del cliente radius. Shared secret Vpn123 o consultar con Deloitte

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* Network policies

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Fundamental apuntar al grupo de VPN del DC

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

El resto de las configuraciones son predeterminadas. Estos datos los facilita el proveedor de comunicaciones

* Visor de eventos. Se habilitan eventos de Azure para visualizar los intentos de conexión. Se dividen fundamentalmente en los eventos del rol NPS contra el DC y los eventos de conexión por Azure MFA

Interfaz de usuario gráfica

Descripción generada automáticamente

Ejemplo de rechazos por usuarios sin MFA

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Conexiones permitidas:

Una captura de pantalla de una computadora

Descripción generada automáticamente

**Contingencia VPN.**

Ante una hipotética incidencia del servidor “físico”, contactar urgentemente con el proveedor de comunicaciones:

* Configuración método principal en su firewall por usuario y contraseña. Actual Radius