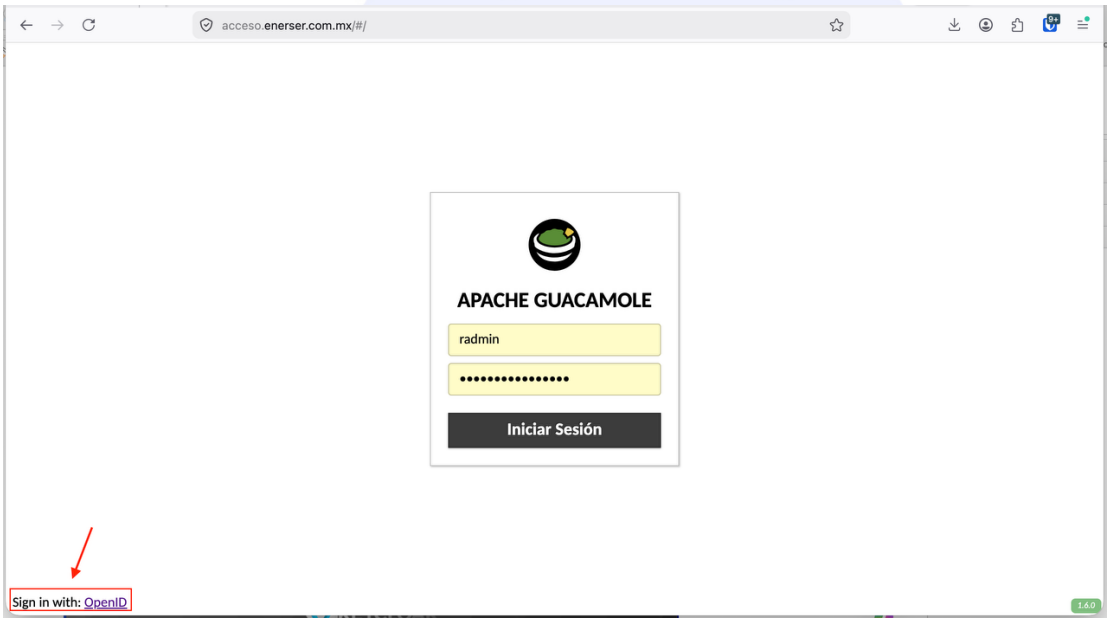
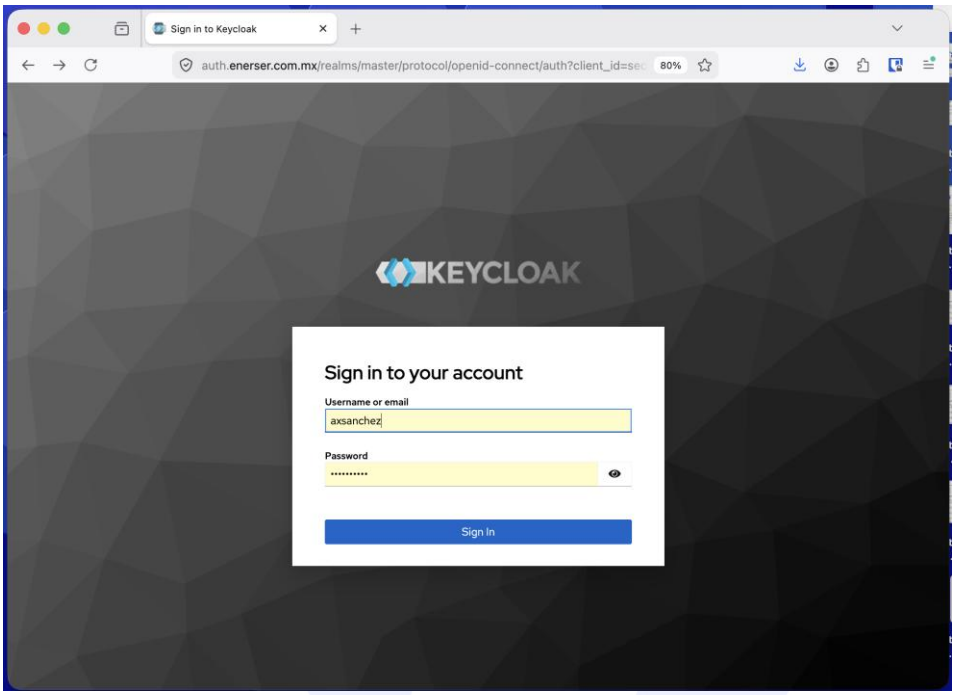
28. Evidencia de uso de contraseñas en la plataforma de servidores y equipos de red

Para el acceso remoto a los servidores vía SSH y RDP utilizamos Apache Guacamole, que es una solucion PAM (Gestión de acceso privilejiado), la cual gestiona la conexión de los administradores a travez de un proxy reverso que autentica a los usuarios contra Keycloack (un gestor de Identidades) una vez que los usuarios son autenticados co 2FA en keycloak guacamole inyecta una credencial desconocida paralos administradores en la sesión RDP o SSH. Todas las conexiones se realizan a través de un navegador web. Adicional a esto se almacena un log de conexiones por usuario y grabación de video de las actividades que realizaron.

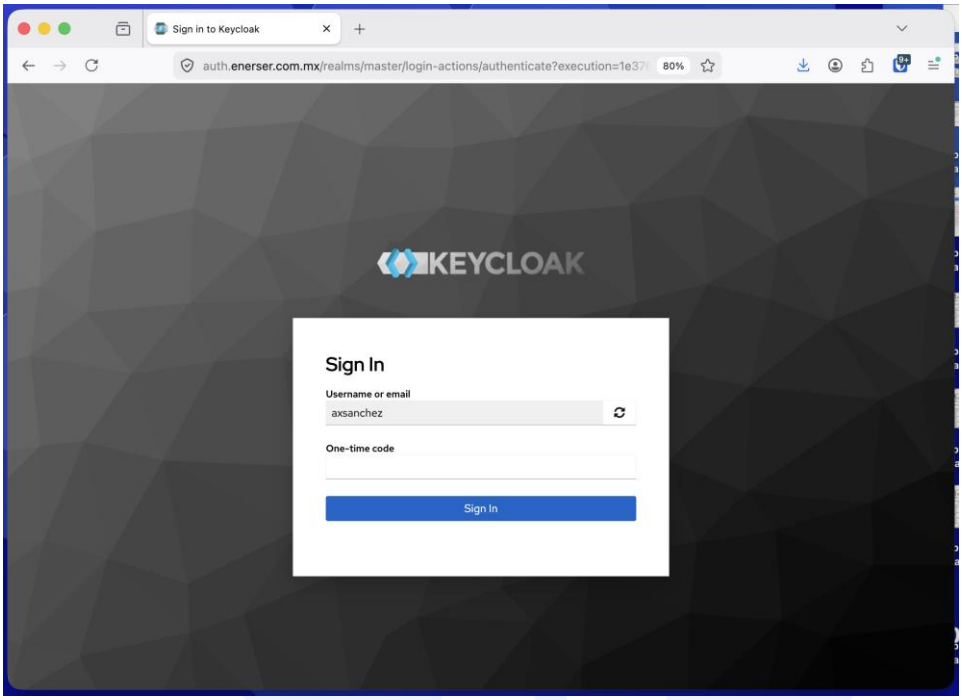
La imagen inferior muestra captura de pantalla de Apache Guacamole, donde se observa que esta habilitada la autenticación OpenID, al firmarse con este protocolo los usuarios son redirigidos a keycloack



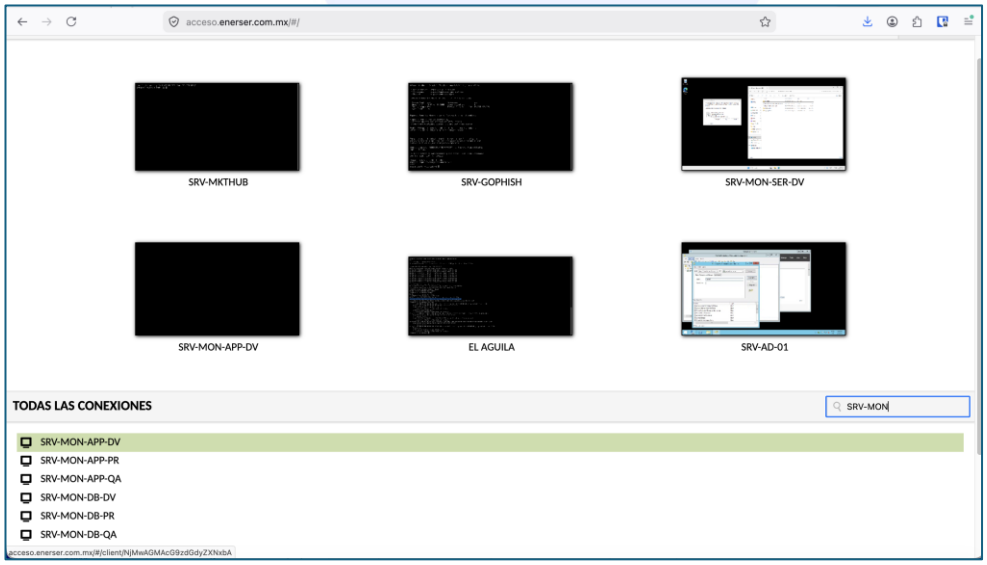
La imagen inferior muestra captura de pantalla de Keycloack, gestor de identidad, solicitando usuario y contraseña



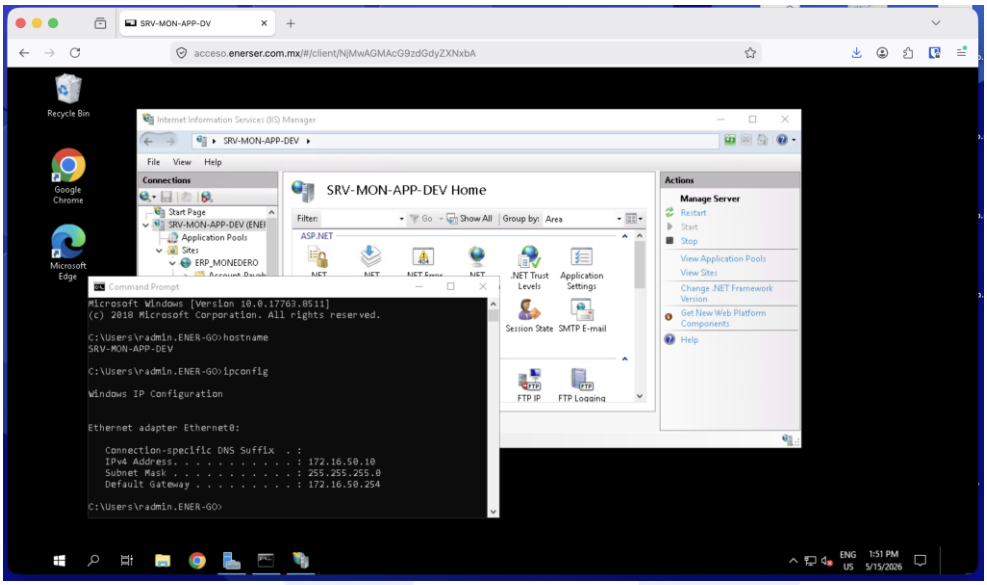
La imagen inferior muestra captura de pantalla de keycloack solicitando el doble factor de autenticación, una vez que keycloack identifica sin duda al usuario lo redirige a Apache Guacamole



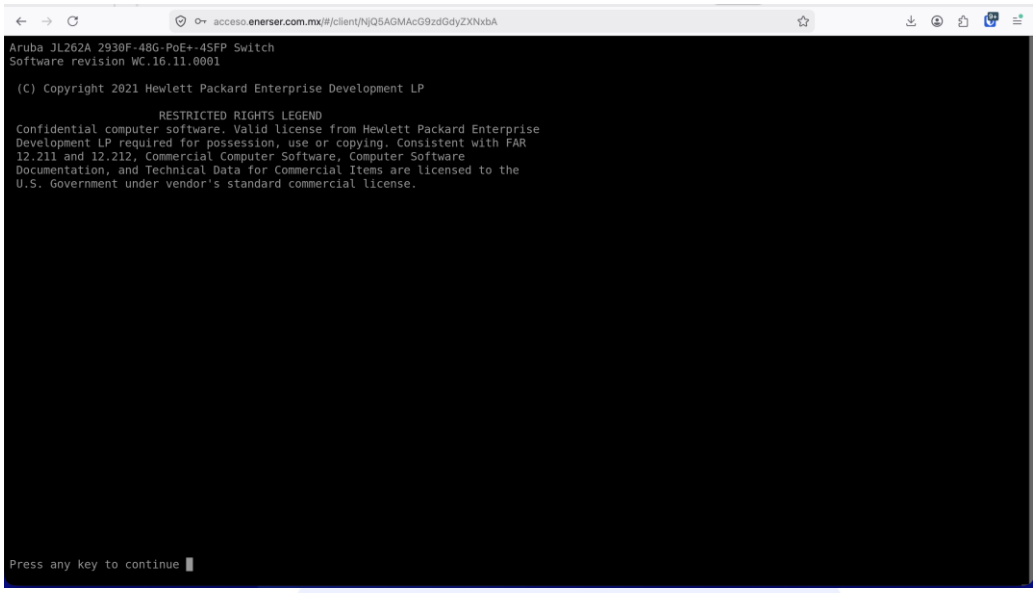
La imagen inferior muestra captura de pantalla de Apache Guacamole donde se observa, historial de sesiones previas y en la parte inferior área de busqueda para conexión a servidores.



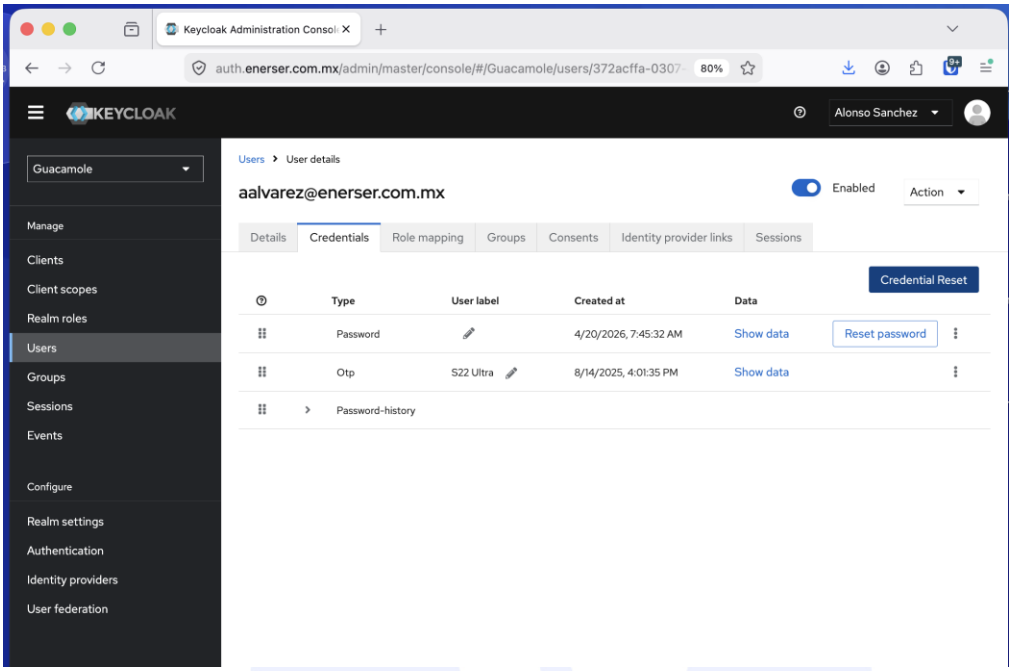
La imagen inferior muestra captura de pantalla de Apache Guacamole una vez realizada la conexión, se aprecia el escritorio del servidor SRV-MON-APP-DV, con dirección IP 172.16.50.10 done se ejecuta la instancia de desarrollo del servidor de aplicación del monedero electronico.



La imagen muestra catura de pantalla de una conexión ssh a traves de Apache Guacamole al Switch de red SW-ARUBA-2930F, con dirección IP 10.100.0.14, instalado de las oficinas del Monedero Energo.

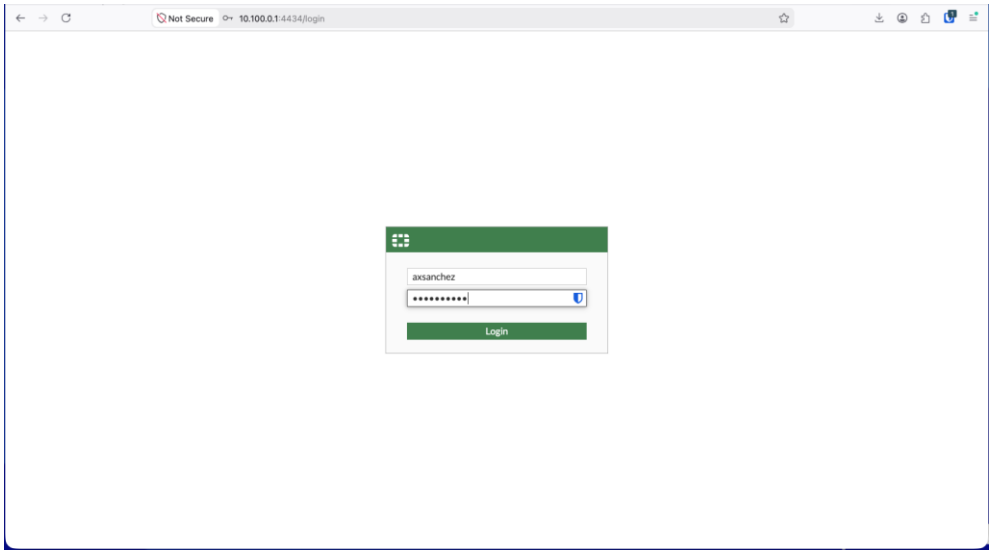


La imagen inferior muestra captura de pantalla de keycloak, el sistema utilizado como gestor de identidad, con el cual intergra con Apache Guacamole, en la imagen se observa el perfil de un usuario, al cual necesita de un pasword y un doble factor de autenticación. Esto complica en gran medida la suplantacion de una sesión y los accesos no autorizados aun que sus credenciales fueran expuestas.

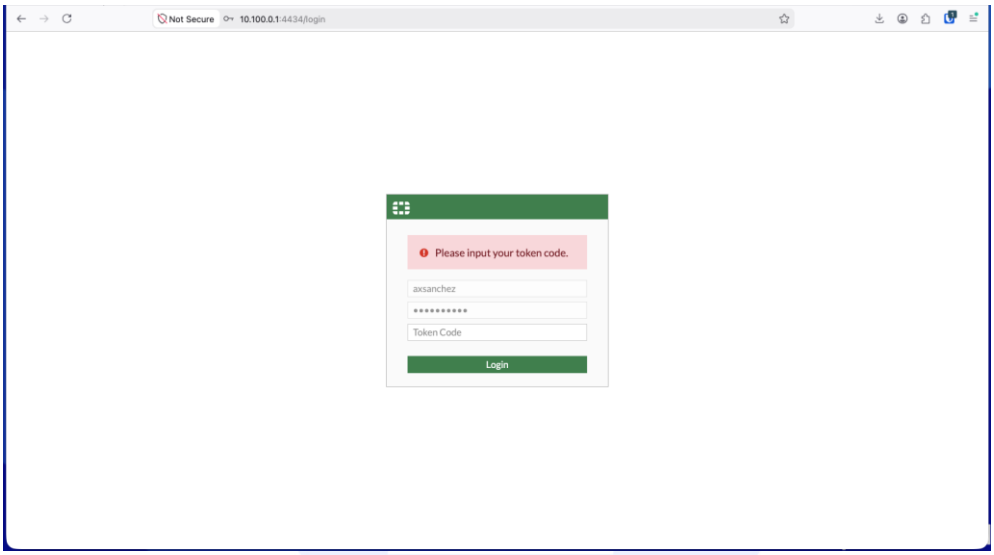


El único dispositivo que no se accesa a traves de apache Guacamole para tareas administrativas es el firewall Fortigate 200F, este se gestiona a través de su propia interfaz web, pero habilita doble factor de Autenticación con FortiToken

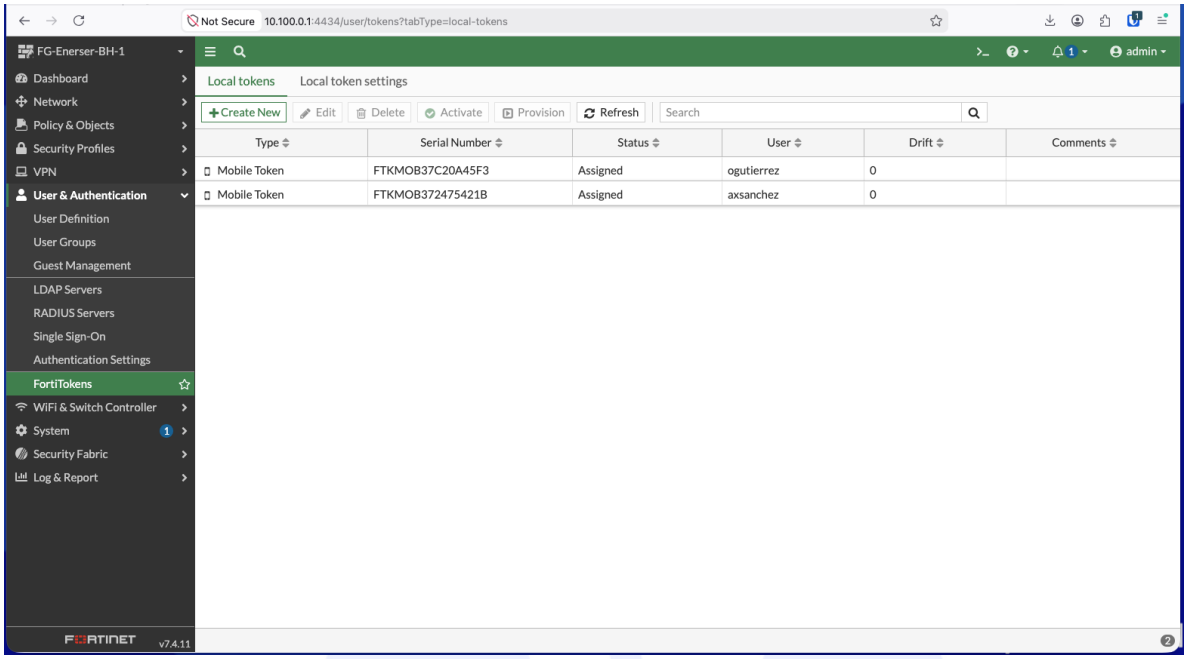
La imagen muestra captura de pantalla de inicio de sesión del firewall Fortigate FW-FG200F-03, con dirección IP 10.100.0.1 donde se observa inicio de sesión con usuario u contraseña



La imagen muestra captura de pantalla de inicio de sesión del firewall Fortigate FW-FG200F-03, con dirección IP 10.100.0.1 donde se observa la solicitud del doble factor de autenticación para continuar con el inicio de sesión.



La imagen muestra captura de pantalla de inicio de sesión del firewall Fortigate FW-FG200F-03, con dirección IP 10.100.0.1 donde se observa configuracion del doble factor de identidad para los usuarios administradores


Not Secure 10.100.0.1:4434/user/tokens?tabType=local-tokens
FG-Enerser-BH-1
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
User Definition
User Groups
Guest Management
LDAP Servers
RADIUS Servers
Single Sign-On
Authentication Settings
FortiTokens
WiFi & Switch Controller
System
Security Fabric
Log & Report
Local tokens
Local token settings
Create New
Edit
Delete
Activate
Provision
Refresh
Search
Type
Serial Number
Status
User
Drift
Comments
Mobile Token
FTKMOB37C20A45F3
Assigned
ogutierrez
0
Mobile Token
FTKMOB372475421B
Assigned
axsanchez
0
FORTINET
v7.4.11