UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
T U N J A

TÍTULO PASANTÍA

Herramienta de sustitución de cortafuegos para las operaciones del centro de datos de de Arvato Systems

PROPONENTE(S)
Alix Ivonne Chaparro Vasquez
1020805932
2259476

DIRECTOR
Martha Susana Contreras Ortiz

Tunja
20 de mayo de 2023

CONTENIDO

1. FICHA TÉCNICA DE LA PASANTÍA

Título	Herramienta de sustitución de cortafuegos para las operaciones del centro de datos de Arvato Systems
Nombre Estudiante	Alix Ivonne Chaparro Vasquez
Documento estudiante	1020805932
Correo electrónico	alix.chaparro@usantoto.edu.co
Director	Martha Susana Contreras Ortiz
Entidad o sector de la empresa	Arvato Systems GmbH.
Lugar de ejecución de la pasantía	Gütersloh, Nordrhein-Westfalen.
Duración	5 meses

Los abajo firmantes confirman que todos los datos incluidos en la presente propuesta son correctos y verídicos, que no incumplen ninguna ley o norma vigente. (Incluir nombres y firmas de estudiantes, director y tutor).

Firma del autor
Alix Ivonne Chaparro Vasquez

Firma del director
Nombre director de la pasantía

2. PLANTEAMIENTO DEL PROBLEMA

Un cortafuegos es el que permite bloquear el acceso a una red privada conectada a internet, a usuarios no autorizados. En Arvato Systems se cuenta con una aplicación de cortafuegos, sin embargo, no brinda el apoyo necesario debido a que no posee todas sus funcionalidades. Por tal motivo se tiene previsto la adquisición de una licencia completa que requiere ser adaptada a las necesidades de la empresa.

Entre los requisitos necesarios desde el punto de vista organizativo, se tiene principalmente el garantizar la seguridad de la información a la hora de autenticarse, la cual puede ser cubierta por medio de la autorización a través de LDAPS [1], la funcionalidad de lo que actualmente está habilitado, así como también de las funciones que estaban anterior a la compra de este aplicativo y la puesta en funcionamiento mejorando la opción de búsqueda. De esta forma se logra que la búsqueda se pueda filtrar y obtener resultados más personalizados al usuario, sin dejar atrás la usabilidad.

En cuanto a la seguridad, se requiere realizar el logueo al cortafuegos y es necesario implementar la autenticación a través de LDAPS (Protocolo ligero de acceso a directorios). Este protocolo permite cifrar los datos (que incluyen credenciales de usuario) en tránsito durante cualquier comunicación con el servidor LDAP[2] (como un enlace de directorio), protegiendo contra el robo de credenciales.

El propósito del presente proyecto consiste en la implantación de la autenticación por medio de LDAPS, revisando la seguridad y la funcionalidad de búsqueda, para poder utilizar la herramienta de cortafuegos de forma productiva. Además, se propone la puesta en marcha del cortafuegos con funciones de exportación y la exclusión de la interpretación errónea de los resultados de búsqueda, en caso de elección equivocada de los parámetros.

---

[1] Ciberseg. (2021). LDAP: qué es, cómo funciona, usos y riesgos de seguridad. Ciberseguridad. https://ciberseguridad.com/guias/prevencion-proteccion/ldap/

[2] Castillo, J. A. (2019). LDAP: Qué es y para qué se utiliza este protocolo. Profesional Review. https://www.profesionalreview.com/2019/01/05/ldap/

Por otra parte, con el desarrollo de este trabajo se busca mejorar la curva de aprendizaje para los nuevos empleados de Arvato Systems, teniendo en cuenta el proceso de adecuación, la operabilidad, la protección contra errores de usuario, la estética de la interfaz de usuario y la accesibilidad.

Como se puede observar, y teniendo en cuenta el gran incremento que ha venido sucediendo, no solo de ataques cibernéticos a las empresas sino además el robo de información con fines económicos, los aspectos aquí implementados buscan proteger, tanto a la empresa como a los usuarios, de accesos indebidos al sistema. De esta forma, lo anterior se constituye como un paso primordial, sobre el cual se implementarán opciones de búsqueda con posibilidad de filtración, la facilidad de uso y se abrirá el camino para la adecuación de nuevas aplicaciones, que vayan mejorando la seguridad general de las empresas.

3. OBJETIVOS

1.1. Objetivo General

Adaptar una herramienta de cortafuegos para las operaciones de los centros de datos de Arvato Systems, con el fin de garantizar la seguridad y mejorar la usabilidad mediante el desarrollo de nuevas funcionalidades de búsqueda empleando buenas prácticas de desarrollo y herramientas de código abierto como soporte para la solución.

1.2. Objetivos específicos

Tabla 1.Objetivos específicos

1	Identificar los requerimientos por medio de entrevistas con el cliente, a fin de poder garantizar la seguridad, la funcionalidad y la usabilidad de una herramienta de cortafuegos para el centro de datos.
2	Definir las opciones de adaptación en cuanto a la seguridad y la funcionalidad, por medio de diagramas de clase, casos de uso, de despliegue y mockups.
3	Implementación de la seguridad en el cortafuegos utilizando lenguajes de código abierto.
4	Ejecutar plan de pruebas de error y criterios de adaptación en la seguridad del aplicativo, teniendo en cuenta la guía de recomendaciones de OWASP - Open Web Application Security Project.

Fuente 1 :Autor

4. DESCRIPCIÓN DE LAS ACTIVIDADES REALIZADAS

4.1. Actividades realizadas en el proyecto

En la Tabla 2 se presenta una descripción detallada con las actividades realizadas en el marco de un proyecto llevado a cabo para Arvato Systems con el fin de implementar una herramienta de sustitución de cortafuegos para sus operaciones del centro de datos. Las actividades se dividieron en diferentes fases y se llevaron a cabo en un periodo de tiempo determinado, siguiendo un plan de proyecto previamente establecido. La tabla presenta información sobre la sección, la descripción de la actividad, la fecha de inicio y entrega y en que parte se define el entregable. El objetivo principal del proyecto fue adaptar una herramienta de cortafuegos para las operaciones de los centros de datos de Arvato Systems, con el fin de garantizar la seguridad y mejorar la usabilidad mediante el desarrollo de nuevas funcionalidades de búsqueda empleando buenas prácticas de desarrollo y herramientas de código abierto como soporte para la solución.

Tabla 2. Actividades realizadas en el proyecto

Sección	Descripción de la actividad	Fecha inicio	Fecha entrega	Producto entregado
Identificación de los requerimientos	Análisis del problema a tratar y definición del alcance.	2.1.2023	2.1.2023	Documento
	Entrevista a usuarios.	2.1.2023	2.1.2023	Documento
	Especificación de requerimientos.	3.1.2023	4.1.2023	Documento
Definir opciones de adaptación para seguridad y funcionalidad	Diseño de mockups.	5.1.2023	6.1.2023	Documento
	Construcción de diagramas de casos de uso.	9.1.2023	10.1.2023	Documento
	Construcción de diagramas de clase.	11.1.2023	13.1.2023	Documento
	Construcción de diagramas de despliegue.	16.1.2023	18.1.2023	Documento
Implementación de seguridad y nuevas	Estudio y análisis del código fuente del cortafuegos entregado	19.1.2023	2.2.2023	Documento

Sección	Descripción de la actividad	Fecha inicio	Fecha entrega	Producto entregado
funcionalidades en el cortafuegos	Implementación de nuevas funcionalidades.	3.2.2023	15.3.2023	Documento
	Implementación del frontend.	16.3.2023	30.3.2023	Documento
Implementación del plan de pruebas	Diseño del plan de pruebas teniendo en cuenta las recomendaciones del OWASP (Open Web Application Security Project).	3.4.2023	7.4.2023	Documento
	Ejecución del plan de pruebas teniendo en cuenta las recomendaciones del OWASP (Open Web Application Security Project).	10.4.2023	14.4.2023	Documento
	Realización de ajustes necesarios a partir del plan de pruebas.	17.4.2023	17.4.2023	Documento
	Construcción del manual de usuario.	18.4.2023	28.4.2023	Documento

Fuente 2: Autor

4.2. Herramientas utilizadas en el desarrollo del proyecto

Durante el desarrollo del proyecto, se utilizan diversas herramientas registradas en la Tabla 3, que son clave que permiten la implementación y funcionamiento efectivo del sistema. Estas herramientas incluyen:

Tabla 3. Herramientas utilizadas en el desarrollo del proyecto

Herramienta utilizada	Para qué la utilizó
Base de datos MySQL	Almacenar y gestionar cierta cantidad de datos
Lenguaje de etiquetas HTML5	Diseñar el fronend del cortafuegos
Lenguaje de programación PHP/8.2.0	Programar las funcionalidades del cortafuegos

Herramienta utilizada	Para qué la utilizó
Entorno de desarrollo Visual Studio Code	Escribir el código fuente
Servidor Apache/ 2.4.55 (Win64)	Lugar donde está alojado el aplicativo.
Active Directory	Para recurrir al grupo de personas en la empresa que pueden tener acceso al aplicativo.
OpenSSL/1.1.1h	Para poder implementar el LDAPS
Balsamiq	Diseño de mockups
Genially	Diseño del árbol de problemas
Draw.io	Diseño de diagramas.
Confluence	Donde se aloja la documentación del cortafuegos

Fuente 3. Autor

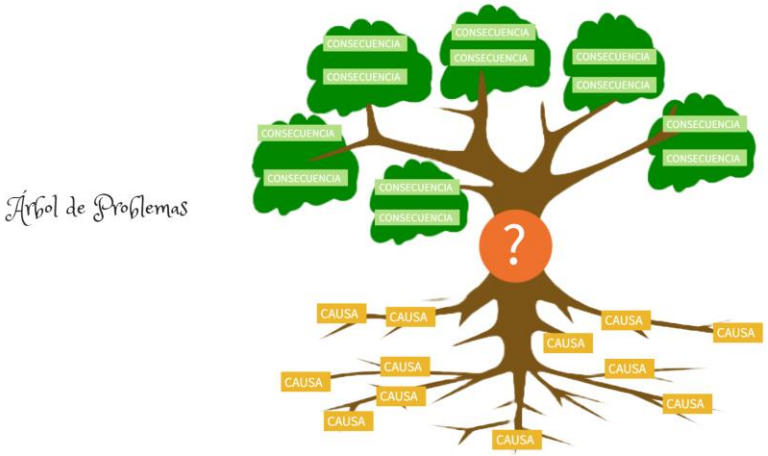
4.3. Descripción profunda de las actividades

4.3.1. Identificación de los requerimientos

4.3.1.1. Análisis del problema a tratar y definición del alcance.

Esta explicación se hizo a partir de un diagrama de árbol de problemas, ver en Figura 1, con 12 causas y consecuencias. En el enlace a continuación podra visualizar el diagrama interactivo: https://view.genial.ly/6454dc333fabe9001d3f931d/interactive-image-basic-interactive-image

Figura 1. Árbol de Problemas



Fuente 4:Autor

4.3.1.2. Entrevista a los usuarios.

Con el fin de identificar los requerimientos, se realizó una entrevista por teleconferencia, con los directores de aplicaciones de Arvato Systems, de la sede de Letonia, en la Tabla 4 se puede ver información adicional. En donde él mostró el estado del aplicativo, los errores que presentaba y los deseos para éste.

Tabla 4. Ficha Técnica

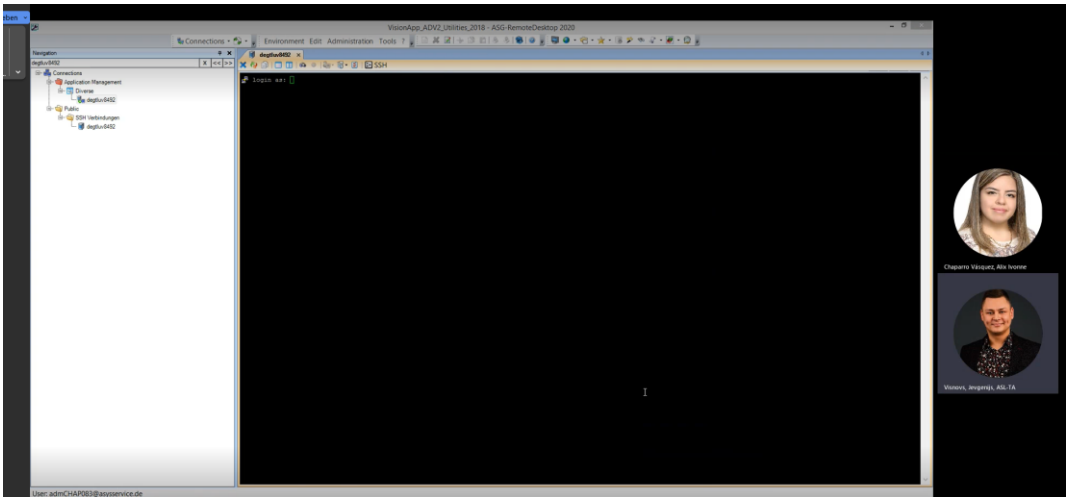
Ficha Técnica	
Fecha	02.01.2023
Duración	21 minutos
Participantes	Jevgenijs Visnovs (Application Manager) y Alix Ivonne Chaparro Vásquez
Metodología	Se realizó por medio de Microsoft Teams, en donde se explicó el estado actual de la herramienta y los problemas que ésta presentaba, así como también lo que se deseaba obtener.
Conclusiones	Estas se encuentran en el apartado de especificación de requerimientos

Fuente 5:Autor

Evidencia de la entrevista:

En la Figura 2 se muestra la captura de pantalla de la reunión remota realizada a Jevgenijs Visnovs por parte de Alix Ivonne Chaparro Vásquez:

Figura 2. Entrevista a Jevgenijs Visnovs



Fuente 6:Autor

4.3.1.3. Especificación de requerimientos.

Un cortafuegos es una herramienta de seguridad fundamental para proteger una red contra amenazas externas e internas. Para implementar un cortafuegos de manera efectiva, es importante tener en cuenta una serie de requisitos que garanticen su eficacia y eficiencia en la protección de la red. En este apartado se incluyen los requerimientos identificados a partir de la entrevista con uno de los directores de la aplicación.

Número	001
Tipo	☒ Requisito ☐ Restricción
Prioridad	☒ Alta/Esencial ☐ Media/Deseada ☐ Baja/Opcional
Descripción	Implementación de LDAPS (Protocolo ligero de acceso a directorios) para la autentificación en el cortafuegos.

Número	002
Tipo	☐ Requisito ☒ Restricción
Prioridad	☒ Alta/Esencial ☐ Media/Deseada ☐ Baja/Opcional
Descripción	Esta implementación debe hacerse en un entorno de UNIX.

Número	003
Tipo	☒ Requisito ☐ Restricción
Prioridad	☐ Alta/Esencial ☒ Media/Deseada ☐ Baja/Opcional
Descripción	La búsqueda se puede filtrar y se pueden obtener resultados personalizados para el usuario.

Número	004
Tipo	☒ Requisito ☐ Restricción
Prioridad	☐ Alta/Esencial ☒ Media/Deseada ☐ Baja/Opcional
Descripción	Optimizar el Frontend, teniendo en cuenta la importancia de la usabilidad, los colores y fuentes distintivas de la empresa.

Número	005
Tipo	☒ Requisito ☐ Restricción
Prioridad	☒ Alta/Esencial ☐ Media/Deseada ☐ Baja/Opcional
Descripción	Diseño y desarrollo del inicio de sesión en el aplicativo de cortafuegos

Número	006
Tipo	☒ Requisito ☐ Restricción
Prioridad	☐ Alta/Esencial ☒ Media/Deseada ☐ Baja/Opcional
Descripción	Implementación de la función de exportación y la exclusión de la interpretación errónea de los resultados de búsqueda, en caso de elección equivocada de los parámetros.

Número	007
Tipo	☒ Requisito ☐ Restricción
Prioridad	☐ Alta/Esencial ☒ Media/Deseada ☐ Baja/Opcional
Descripción	Mejorar la curva de aprendizaje para los nuevos empleados de Arvato Systems, teniendo en cuenta el proceso de adecuación, la operabilidad, la protección contra errores de usuario, la estética de la interfaz de usuario y la accesibilidad.

Durante la reunión con el director, se aprobaron los requisitos necesarios para avanzar en el proyecto en cuestión. La aprobación se llevó a cabo directamente en la reunión, lo que permitió una discusión más detallada y la posibilidad de rectificar cualquier requisito que fuera necesario. Antes de finalizar la reunión, se revisaron cuidadosamente todos los requerimientos para asegurarse de que estaban claros y que se habían entendido correctamente. De esta manera, se garantizó que todos los requisitos necesarios para el proyecto se habían aprobado y se había hecho una revisión exhaustiva de los mismos antes de continuar.

4.3.2. Definir opciones de adaptación para seguridad y funcionalidad

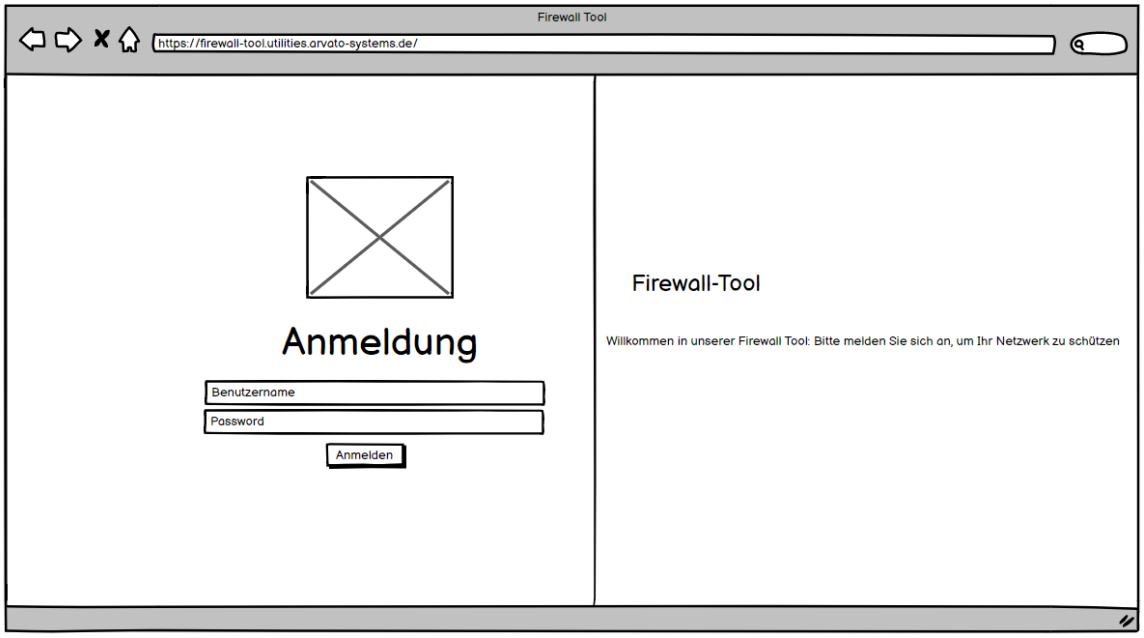
4.3.2.1. Diseño de Mockups

La creación de un cortafuegos efectivo es esencial para garantizar la seguridad de los sistemas informáticos y proteger la información crítica de una organización. Antes de comenzar el desarrollo de un cortafuegos, es importante tener una clara comprensión de cómo se verá y funcionará el producto final. Es aquí donde entran en juego los mockups, que son una representación visual de cómo se verá el producto y cómo funcionará su interfaz. En este caso, se utiliza inicialmente papel y lápiz para realizar bosquejos y luego se procede a usar la herramienta Balsamiq para crear los mockups del cortafuegos, lo que permite tener una idea clara de cómo debe ser el producto final y cómo debe interactuar con el usuario.

4.3.2.1.1. Página login.php

Como se evidencia en la Figura 3, el formulario de inicio de sesión se divide en dos secciones. La sección izquierda se centra en la información de inicio de sesión y contiene una imagen, un título, campos para ingresar el nombre de usuario y la contraseña, y un botón para iniciar sesión. Por otro lado, la sección derecha muestra el nombre de la página y un mensaje de bienvenida, ubicados en el centro de la sección.

Figura 3. Mockup Página login.php



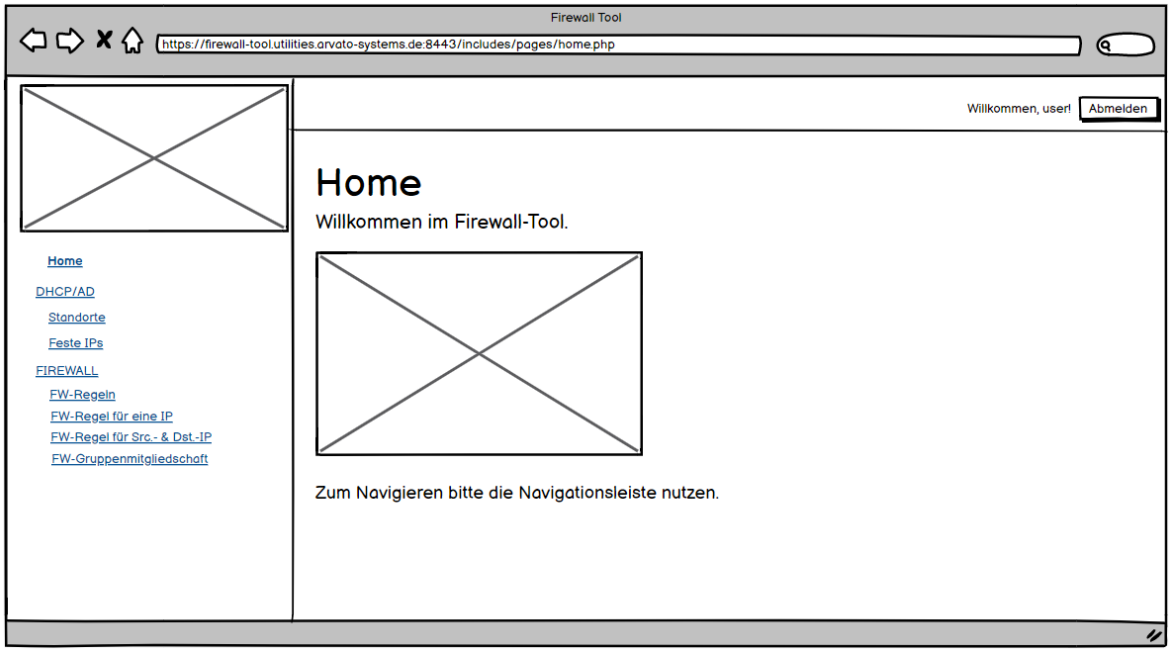
Fuente 7. Autor

4.3.2.1.2. Página home.php

Como se muestra en la Figura 4, en la página principal, a la izquierda se encuentra un menú con el logo de la empresa y una lista de secciones, cada una de las cuales incluye subsecciones adicionales y se muestra en qué sección uno se encuentra, resaltando el nombre de esta. A la derecha, se encuentra una cabecera que da la bienvenida al usuario y muestra su nombre, así como un botón para cerrar sesión.

En el cuerpo de la página, se presenta el título de la sección actual, un mensaje de bienvenida y una imagen correspondiente. Además, se proporciona una guía para navegar por la página y utilizar sus características.

Figura 4. Mockup Página home.php



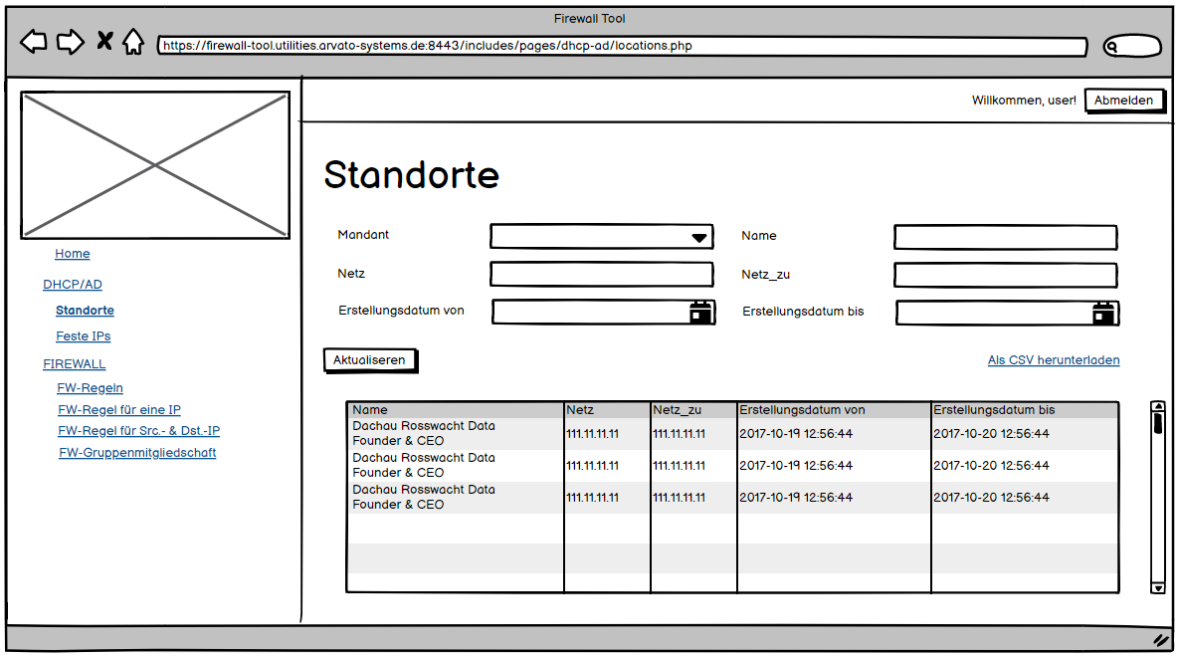
Fuente 8:Autor

4.3.2.1.3. Página locations.php

Como se observa en la Figura 5, en la página de ubicaciones, a la izquierda se encuentra un menú con el logo de la empresa y una lista de secciones, cada una de las cuales incluye subsecciones adicionales. La sección actual en la que se encuentra el usuario se resalta en el menú. A la derecha se encuentra una cabecera que da la bienvenida al usuario, muestra su nombre y proporciona un botón para cerrar sesión.

En el cuerpo de la página, se encuentra un formulario de búsqueda que incluye varios campos de búsqueda. También hay un botón para actualizar la búsqueda y un enlace para descargar los resultados de la búsqueda. Los resultados de la búsqueda se muestran en una tabla que contiene información detallada de cada ubicación encontrada.

Figura 5. Mockup Página locations.php



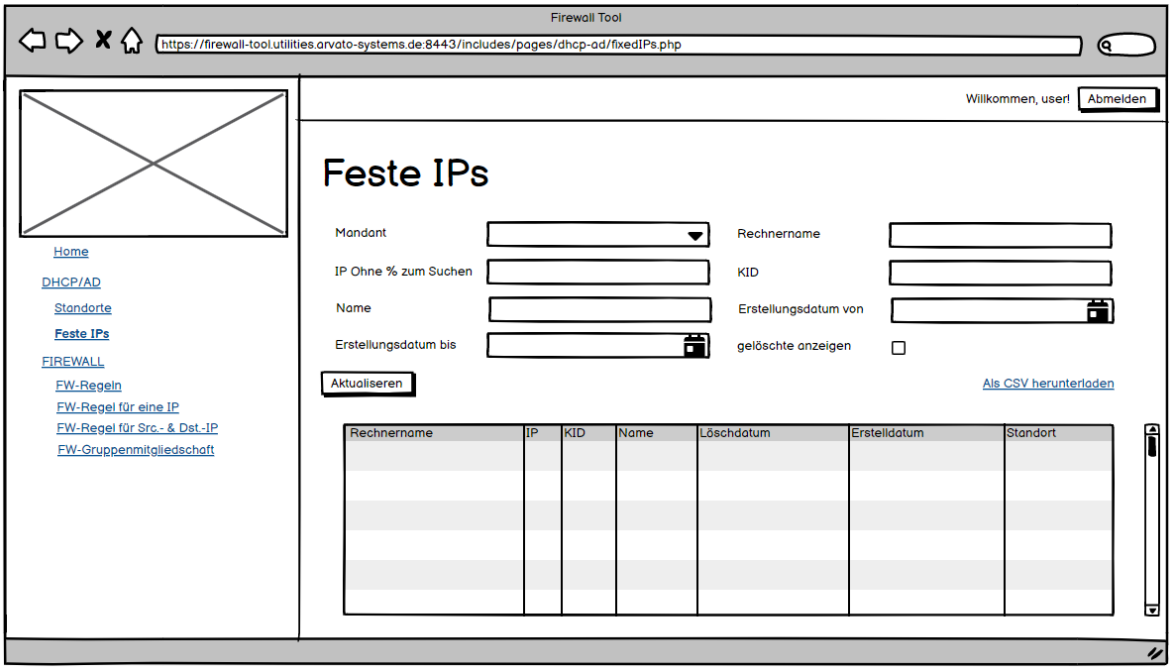
Fuente 9. Autor

4.3.2.1.4. Página fixedIPs.php

Cómo se percibe en la Figura 6, en la página de IP fijas, a la izquierda se encuentra un menú con el logo de la empresa y una lista de secciones, incluyendo subsecciones adicionales. El menú resalta la sección actual en la que se encuentra el usuario. A la derecha, en la cabecera, se le da la bienvenida al usuario mostrando su nombre y ofreciendo un botón para cerrar sesión.

En el cuerpo de la página, se encuentra un formulario de búsqueda que permite ingresar varios criterios de búsqueda. Además, se encuentra un botón para actualizar la búsqueda y un enlace para descargar los resultados obtenidos. Estos resultados se presentan en una tabla que proporciona información detallada de cada IP fija encontrada.

Figura 6. Mockup Página fixedIps.php



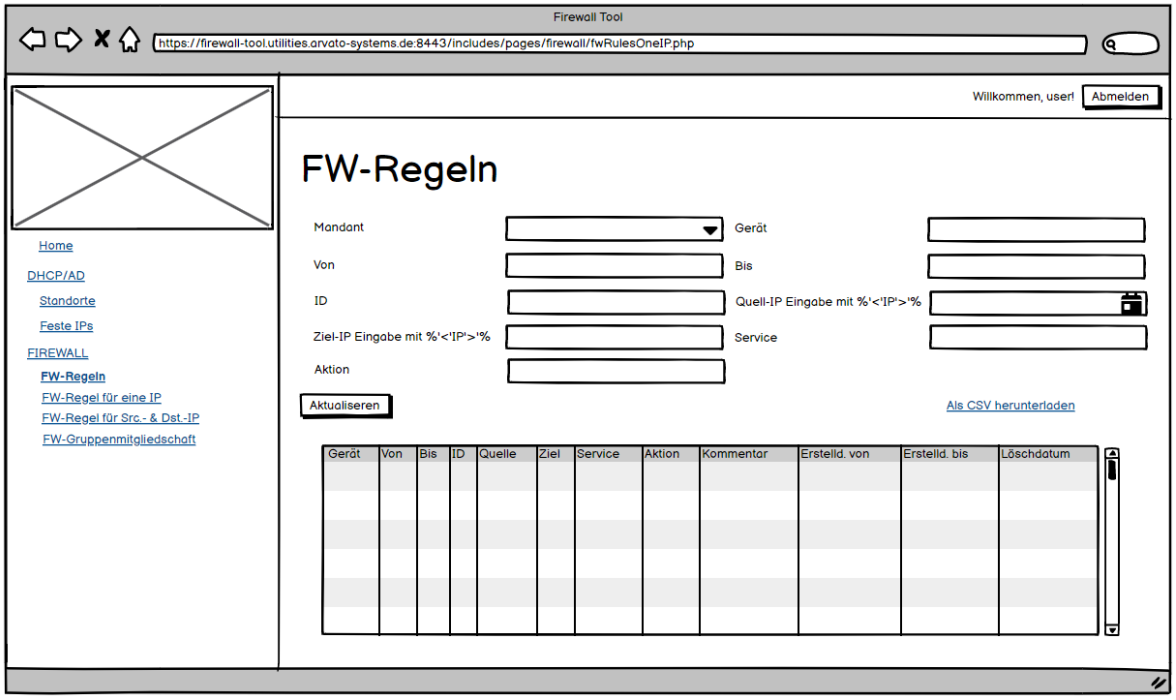
Fuente 10. Autor

4.3.2.1.5. Página fwRules.php

Cómo se muestra en Figura 7, en la página de reglas del cortafuegos, se encuentra a la izquierda un menú con el logo de la empresa y una lista de secciones, que incluyen subsecciones adicionales. El menú resalta la sección actual en la que se encuentra el usuario. A la derecha, en la cabecera, se da la bienvenida al usuario mostrando su nombre y se ofrece un botón para cerrar sesión.

En el cuerpo de la página, se encuentra un formulario de búsqueda que permite ingresar diversos criterios. Además, hay un botón para actualizar la búsqueda y un enlace para descargar los resultados obtenidos. Dichos resultados se presentan en una tabla que brinda información detallada de cada dato encontrado.

Figura 7. Mockup Página fwRules.php



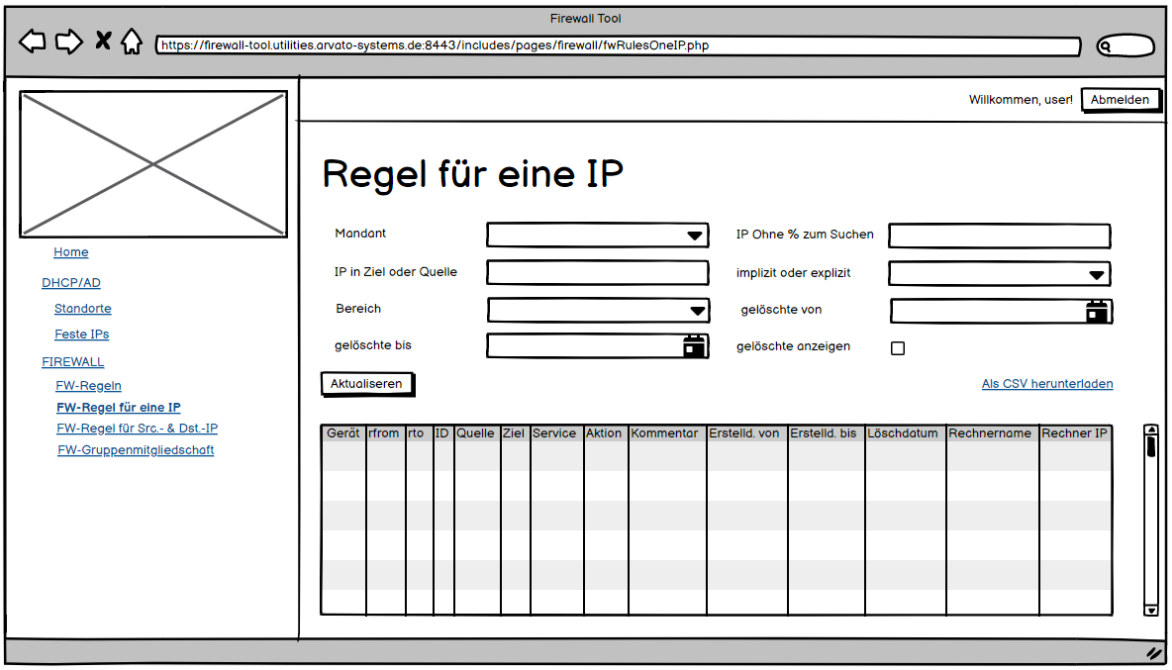
Fuente 11. Autor

4.3.2.1.6. Página fwRulesOneIP.php

En la página de reglas del cortafuegos para una sola IP, se muestra en la Figura 8. A la izquierda se encuentra un menú con el logo de la empresa y una lista de secciones, incluyendo subsecciones adicionales. El menú destaca la sección actual en la que se encuentra el usuario. En la cabecera, ubicada a la derecha, se da la bienvenida al usuario mostrando su nombre y se proporciona un botón para cerrar sesión.

En el cuerpo de la página, se encuentra un formulario de búsqueda que permite ingresar diferentes criterios. Asimismo, se incluye un botón para actualizar la búsqueda y un enlace para descargar los resultados obtenidos. Estos resultados se presentan de manera detallada en una tabla que muestra información específica de cada dato encontrado.

Figura 8. Mockup Página fwRulesOneIP.php



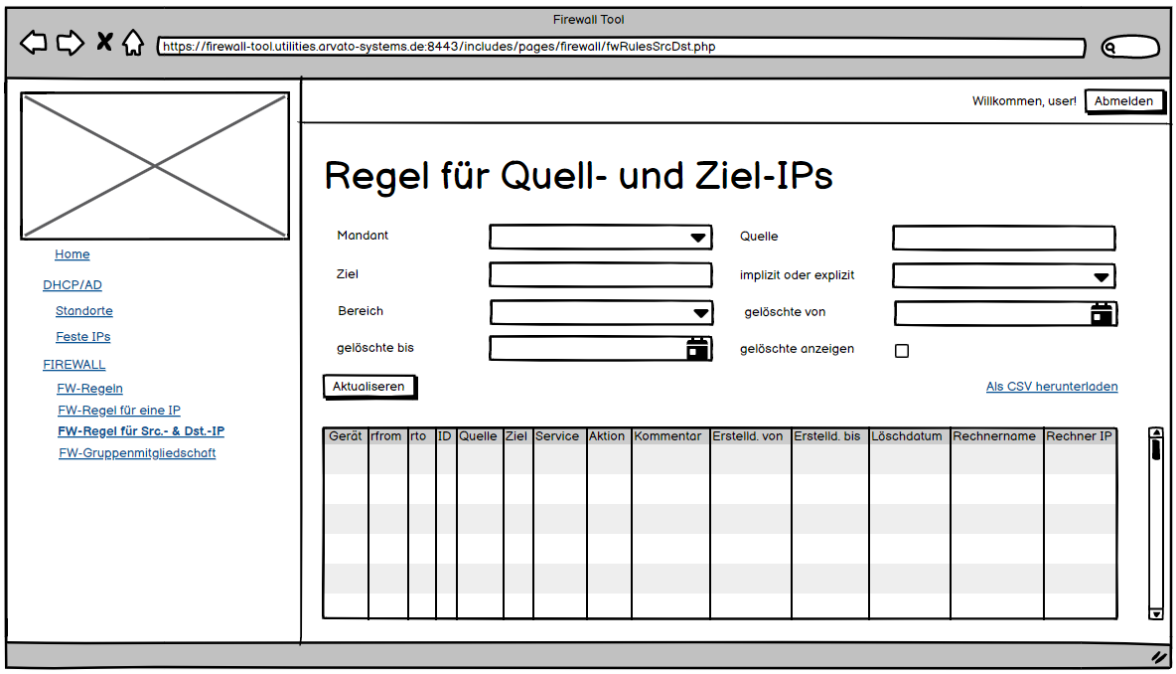
Fuente 12. Autor

4.3.2.1.7. Página fwRulesSrcDst.php

En la página de reglas del cortafuegos para Ips con una fuente y un destino, se muestra en la Figura 9. A la izquierda, se encuentra un menú con el logo de la empresa y una lista de secciones, que incluyen subsecciones adicionales. El menú resalta la sección actual en la que se encuentra el usuario. En la cabecera, ubicada a la derecha, se da la bienvenida al usuario mostrando su nombre y se proporciona un botón para cerrar sesión.

En el cuerpo de la página, se encuentra un formulario de búsqueda que permite ingresar diferentes criterios. Además, se incluye un botón para actualizar la búsqueda y un enlace para descargar los resultados obtenidos. Estos resultados se presentan detalladamente en una tabla que muestra información específica de cada dato encontrado.

Figura 9. Mockup Página fwRulesSrcDst.php



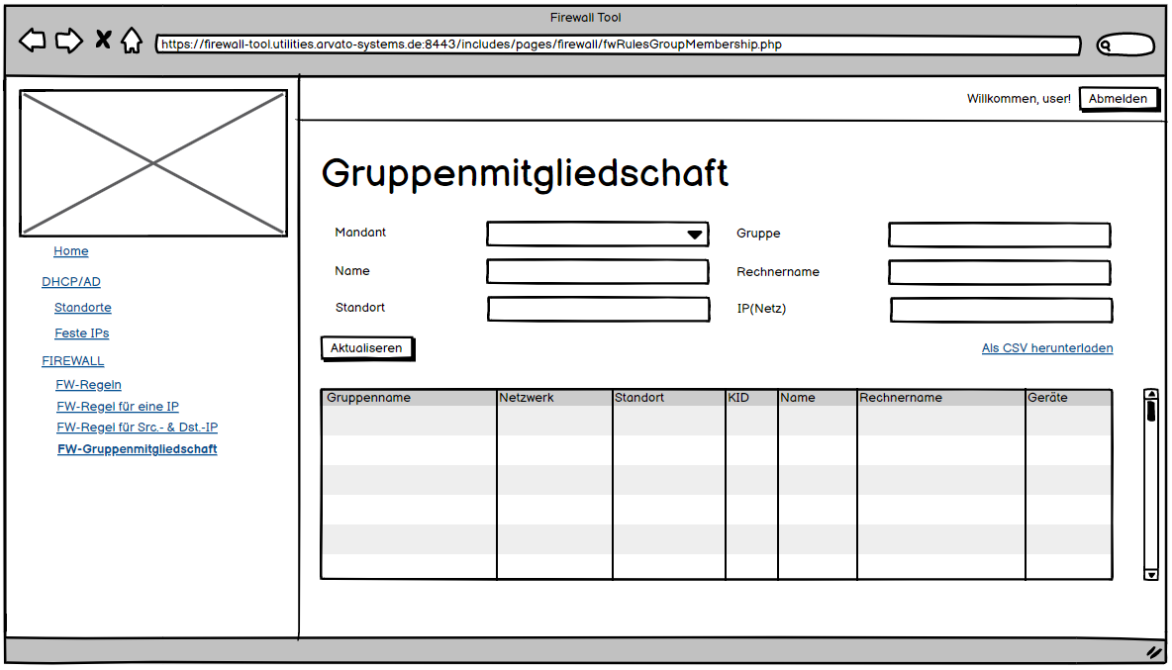
Fuente 13. Autor

4.3.2.1.8. Página fwRulesGroupMembership.php

En la página de reglas del cortafuegos para los miembros de un grupo, se puede visualizar la información en la Figura 10. A la izquierda, se despliega un menú que contiene el logotipo de la empresa y una lista de secciones, que a su vez incluyen subsecciones adicionales. El menú destaca la sección actual en la que se encuentra el usuario. En la parte superior derecha, se muestra una cabecera que da la bienvenida al usuario y muestra su nombre, junto con un botón para cerrar sesión.

En el cuerpo de la página, se encuentra un formulario de búsqueda que permite ingresar diversos criterios. Además, se incluye un botón para actualizar la búsqueda y un enlace para descargar los resultados obtenidos. Estos resultados se presentan en una tabla detallada, donde se muestra información específica de cada dato encontrado.

Figura 10. Mockup Página fwRulesGroupMembership.php



Fuente 14. Autor

4.3.2.2. Diseño de diagrama de secuencia (Para la autenticación con LDAPS)

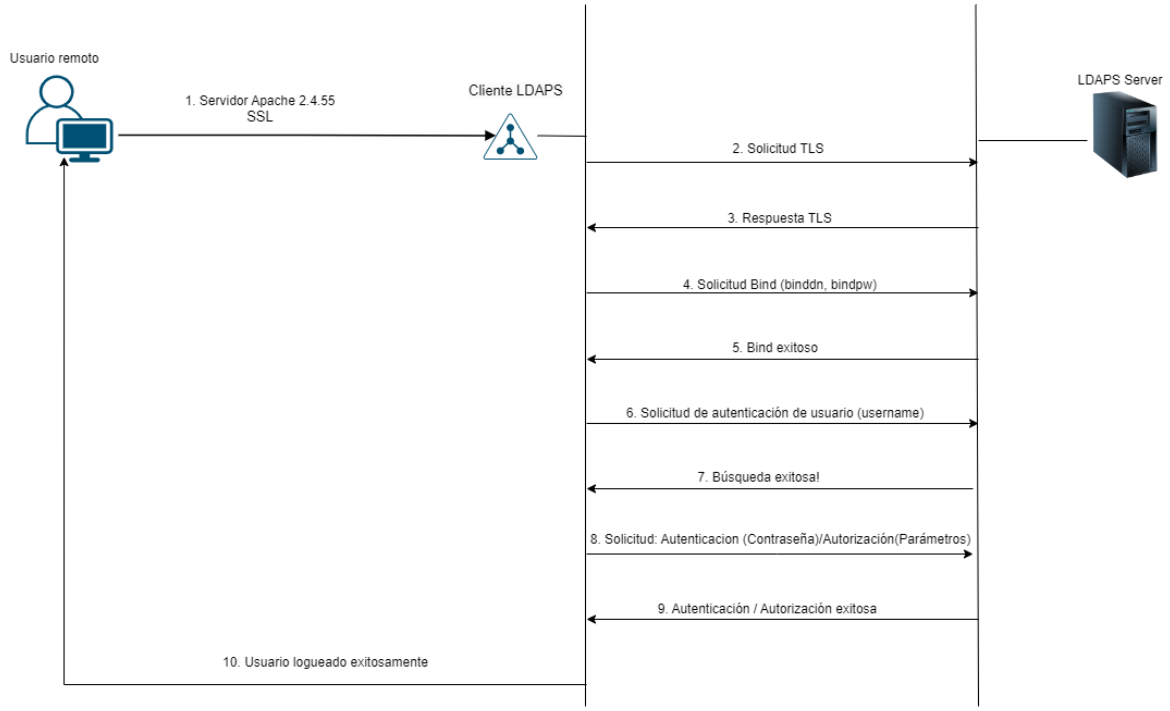
El diseño de un diagrama de secuencia es una herramienta útil para visualizar y comprender el flujo de interacciones entre los diferentes componentes involucrados en un proceso, como la autenticación utilizando LDAPS en un cortafuegos. Un diagrama de secuencia muestra la secuencia temporal de los mensajes y las acciones entre los objetos participantes, brindando una representación clara y detallada del proceso de autenticación. Al diseñar un diagrama de secuencia para la autenticación con LDAPS en un cortafuegos, se pueden identificar los pasos clave. Esto permite una comprensión más profunda del proceso y facilita la detección de posibles problemas o mejoras en la implementación de la autenticación en el cortafuegos.

Descripción de la Figura 11:

- Un usuario remoto inicia sesión en la herramienta de cortafuegos alojada en el servidor de apache que ejecuta SSL.

- El cliente LDAPS establece una conexión TCP con el servidor de autorización LDAPS mediante una solicitud de protocolo TLS.
- Después de que el cliente recibe la respuesta TLS, el cliente y el servidor autentican sus identidades.
- El cliente LDAPS se autentica a sí mismo mediante la cuenta de proxy que está preconfigurada en el servidor LDAPS mediante la solicitud de enlace (binddn y bindpw).
- Si la operación de enlace es correcta, el servidor LDAPS envía un reconocimiento al cliente LDAPS.
- A continuación, el cliente LDAPS envía una solicitud de autenticación al servidor LDAPS con las credenciales de inicio de sesión del usuario que intenta iniciar sesión.
- Después de la autorización correcta, el cliente LDAPS notifica al usuario el inicio de sesión correcto.
- El cliente cierra la conexión con el servidor LDAPS.

Figura 11. Diagrama de Secuencia Autenticación LDAPS



Fuente 15: Autor

4.3.2.3. Diseño de diagrama de casos de uso (Para la autenticación con LDAPS)

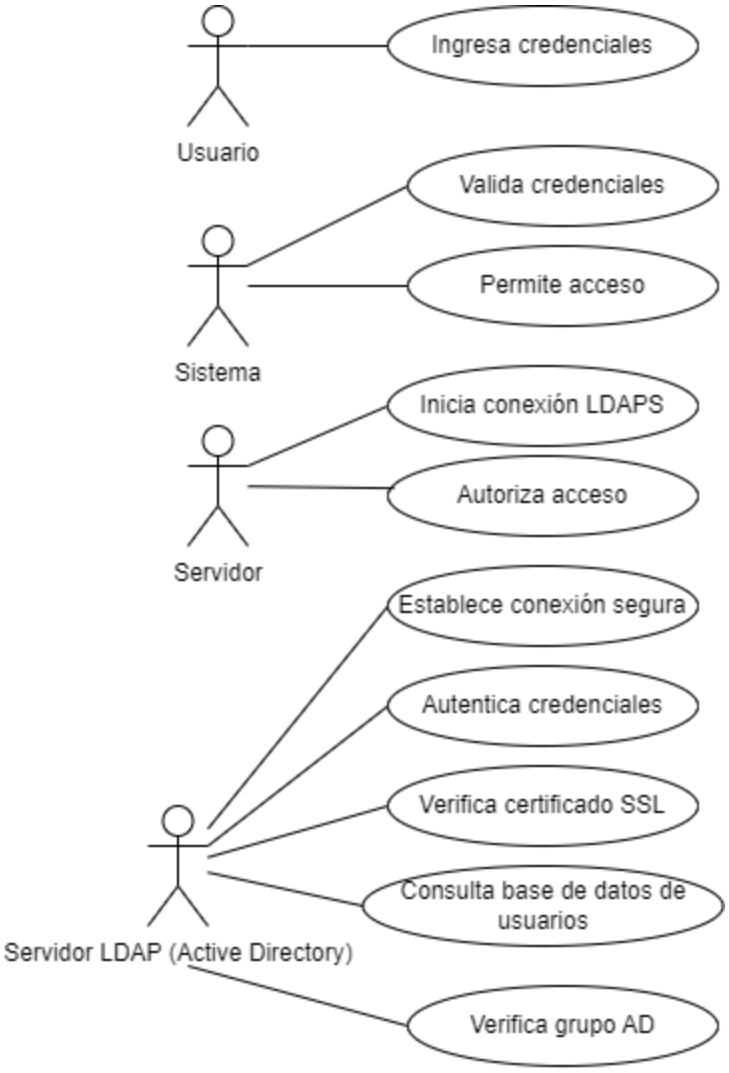
El diseño de un diagrama de casos de uso es una herramienta fundamental para comprender y representar las interacciones entre los actores y el sistema en un proceso determinado, como la autenticación utilizando LDAPS en un cortafuegos. Un diagrama de casos de uso proporciona una visión general de las funcionalidades y los roles involucrados en el proceso de autenticación, identificando las acciones que cada actor realiza y cómo interactúa con el sistema. Al diseñar un diagrama de casos de uso para la autenticación con LDAPS en un cortafuegos, se pueden identificar los pasos clave, como el ingreso de credenciales por parte del usuario, la validación de las mismas por el sistema, la comunicación con el servidor LDAP y la autorización de acceso al cortafuegos. Esto permite comprender de manera clara y concisa cómo se lleva a cabo el proceso de autenticación y ayuda a identificar los requisitos funcionales y no funcionales necesarios para su implementación efectiva en el cortafuegos.

Descripción de la Figura 12:

- Ingresa credenciales: El usuario ingresa sus credenciales (nombre de usuario y contraseña) en el formulario de autenticación.
- Valida credenciales: El sistema valida y verifica las credenciales ingresadas por el usuario.
- Inicia conexión LDAPS: El servidor establece una conexión segura utilizando LDAPS (LDAP sobre SSL/TLS).
- Establece conexión segura: El servidor LDAP establece una conexión segura utilizando el certificado SSL.
- Autentica credenciales: El servidor LDAP autentica las credenciales del usuario verificando si son válidas.
- Verifica certificado SSL: El servidor LDAP verifica el certificado SSL proporcionado por el servidor para garantizar la autenticidad.
- Consulta base de datos de usuarios: El servidor LDAP consulta la base de datos de usuarios para obtener información adicional del usuario.
- Verifica grupo AD: El servidor LDAP verifica si el usuario pertenece al grupo autorizado en Active Directory.

- Autoriza acceso: El servidor autoriza el acceso del usuario al sistema si las credenciales y verificaciones son exitosas.
- Permite acceso: El sistema permite al usuario acceder a la herramienta de cortafuegos.

Figura 12. Diagrama de Casos de Uso para la Autenticación LDAPS



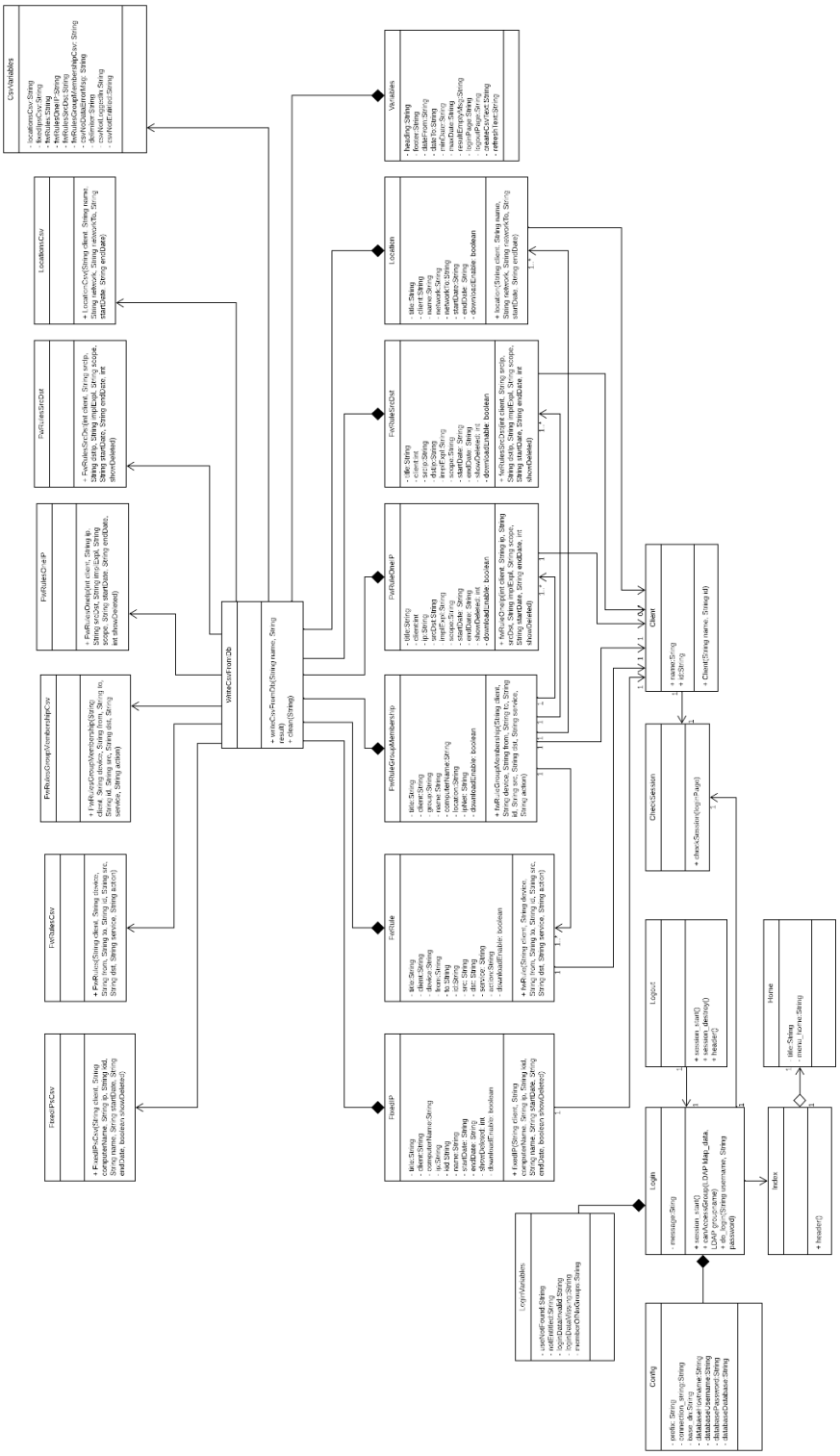
Fuente 16 . Autor

4.3.2.4. Construcción de diagramas de clase.

El diseño de un diagrama de clase Figura 13 es una herramienta esencial para comprender y representar la estructura y las relaciones entre las clases y objetos en un sistema, como

la autenticación utilizando LDAPS en un cortafuegos. Un diagrama de clase proporciona una representación visual de las clases involucradas en el proceso de autenticación, sus atributos, métodos y las relaciones entre ellas. Este diagrama facilita una comprensión clara y estructurada de las interacciones entre las clases y objetos involucrados en el proceso de autenticación con LDAPS, lo que permite una implementación eficiente y un mejor entendimiento del sistema de cortafuegos

Figura 13. Diagrama de clase



Fuente 17. Autor

4.3.2.5. Construcción de diagramas de despliegue.

- Se toma el módulo SSL, junto con la dirección IP y el puerto del cliente que está haciendo la solicitud en el servidor y se indica que la conexión con el cliente se ha establecido correctamente en firewall-tool.utilities.arvato-systems.de:443
- Se encuentra un host virtual SSL para el nombre del servidor firewall-tool.utilities.arvato-systems.de, lo cual significa que el servidor ha encontrado un certificado válido para el nombre del servidor especificado y que la comunicación con el cliente se realizará a través de una conexión SSL segura.
- Se selecciona un protocolo para comunicarse con el cliente que se conecta al servidor firewall-tool.utilities.arvato-systems.de.
- La conexión con el cliente se establece exitosamente.
- Se detecta un host virtual SSL para el servidor. Cuando se utiliza SSL es común que se utilice un host virtual para proporcionar una capa adicional de seguridad, para múltiples sitios web en el mismo servidor.
- El servidor recibe una solicitud del cliente indicando los protocolos que admite para la conexión con el cliente.
- Se utiliza el protocolo TLSv1.3 para la comunicación SSL/TLS y para el cifrado se usa TLS_AES_256_GCM_SHA384, que utiliza una clave de cifrado de 256 bits.
- Se usa un módulo de caché compartido de Apache, donde se almacena la información de la memoria intermedia. Esto puede mejorar el rendimiento del servidor web donde se accede a los mismos recursos con frecuencia por múltiples clientes.
- El módulo SSL recibe una solicitud HTTPS inicial sin cifrado previo para el servidor firewall-tool.utilities.arvato-systems.de en el puerto 443 y la IP del cliente.
- El módulo mod_authz_core evalúa una directiva con la IP del cliente y concede el acceso al recurso solicitado por el cliente, porque éste ha cumplido con los requisitos de autorización definidos, en el caso contrario se le niega el acceso.
- Cuando se concede el acceso se verifica que esté usando el protocolo TLSv1.3 para la conexión y que el cifrado utilizado ha sido TLS_AES_256_GCM_SHA384, con una longitud de clave de 256 bits y una función hash SHA-384.
- El servidor recibe una solicitud HTTPS segura de un cliente. Lo anterior significa que éste ya ha iniciado sesión en el cortafuegos.

- Se llama a la función ldap_sasl_bind_s. Esta es una función de la biblioteca de protocolo de directorio LDAP (Lightweight Directory Access Protocol) que se utiliza para autenticar un usuario en un servidor LDAP mediante el mecanismo de enlace SASL (Simple Authentication and Security Layer). SASL es un marco de autenticación estándar que permite que aplicaciones entre cliente-servidor se autentiquen entre sí mediante diferentes mecanismos de autenticación.
- Luego se ejecuta la función ldap_sasl_bind que es asíncrona de ldap_sasl_bind_s, lo que significa que retorna inmediatamente, sin bloquear el hilo de ejecución y el resultado de la operación se maneja en un momento posterior a través de una función de callback.
- Después de que se ha establecido una conexión con el servidor de LDAP, con la función ldap_send_initial_request envía una solicitud inicial al servidor LDAP que generalmente incluye información como la operación LDAP especifica que se va a realizar, los parámetros de búsqueda y cualquier filtro o criterio de búsqueda aplicable. Una vez enviada la solicitud, se espera una respuesta del servidor. Es una función muy importante en las aplicaciones que interactúan con servidores de LDAP, ya que es necesaria para iniciar una transacción con el servidor y enviar las solicitudes necesarias como la búsqueda de objetos en el directorio o la modificación de los atributos de los objetos existentes.
- Se inicia una conexión TCP con el servidor LDAP que se encuentra en la dirección IP y el puerto 636, que es el puerto estándar para las operaciones LDAP seguras utilizando SSL/tls.
- Cuando la conexión con LDAP es exitosa, el cliente y el servidor acuerdan los parámetros de cifrado y autenticación para la conexión segura.
- Como forma de prueba el cliente le envía un saludo y el servidor TLS/SSL debe responder a éste.
- Se verifica que se tenga el certificado TLS sin errores. En este caso el emisor del certificado es Bertelsmann CA - G2 y el sujeto de éste es Bertelsmann SE & Co. KgaA.
- Se valida que el paso anterior esté sin errores, concluyendo que el certificado ha sido emitido por la "Bertelsmann CA - G2" y se ha utilizado para asegurar la conexión con el servidor "gtltntads0011.de.alfa.local.

- El cliente recibe el certificado del servidor, así como también recibe el intercambio de claves del servidor y se puede ahora iniciar una conexión segura. Todo está listo para poder intercambiar información cifrada y segura.
- Se establece una conexión exitosa con un servidor LDAP.

4.3.3. Implementación de seguridad y nuevas funcionalidades en el cortafuegos

No se puede compartir el código fuente del cortafuegos debido a dos razones fundamentales: la seguridad de la empresa y los derechos de autor.

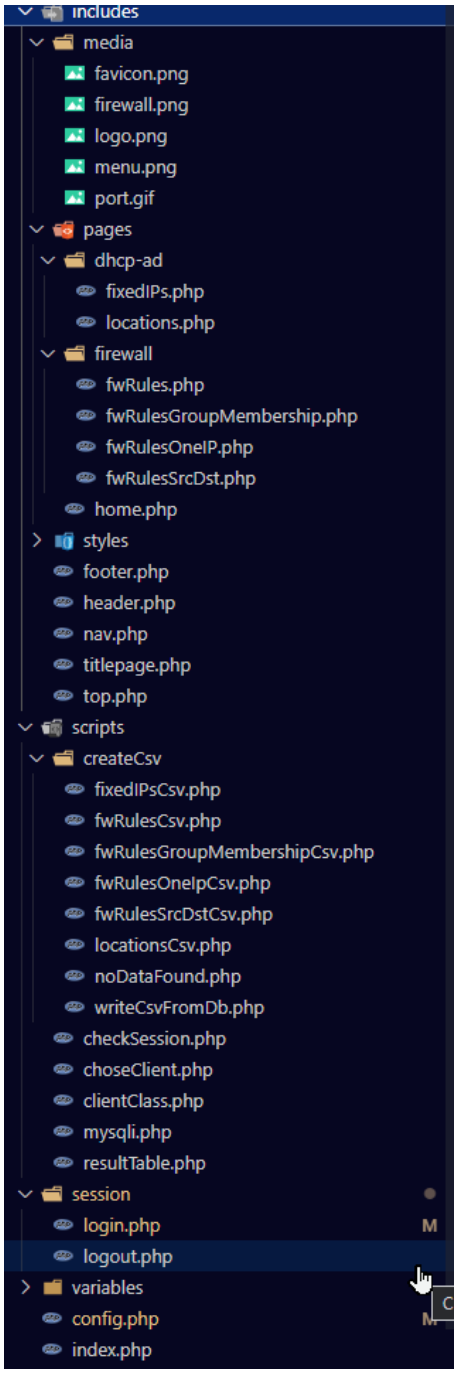
En primer lugar, la seguridad de la empresa es de vital importancia. El código fuente del cortafuegos contiene información sensible y detalles técnicos sobre cómo se implementan las funciones de seguridad. Compartirlo públicamente podría exponer debilidades y vulnerabilidades, lo que podría ser aprovechado por actores maliciosos para comprometer la seguridad de la red. Mantener el código fuente restringido dentro de la empresa ayuda a proteger los sistemas y mantener la integridad de la infraestructura de seguridad.

En segundo lugar, los derechos de autor protegen la propiedad intelectual del código fuente del cortafuegos. La empresa o los desarrolladores que crearon el cortafuegos tienen derechos exclusivos sobre el código y pueden controlar su distribución y uso. Compartir el código fuente sin el consentimiento apropiado violaría los derechos de autor y podría dar lugar a consecuencias legales.

Por lo tanto, la no divulgación del código fuente del cortafuegos es esencial para salvaguardar la seguridad de la empresa y proteger los derechos de autor. Sin embargo, es posible compartir información sobre las funcionalidades generales y las mejores prácticas de configuración del cortafuegos sin revelar detalles específicos del código fuente.

A continuación, en la Figura 14 se presenta una estructura del código fuente, una explicación más detallada se puede encontrar en la Figura 13:

Figura 14. Estructura de código fuente



Fuente 18. Autor

Datos importantes al realizar la conexión con LDAPS:

LDAPS (LDAP Secure) es una variante del Protocolo Ligero de Acceso a Directorios (LDAP) que utiliza una capa de transporte segura para la comunicación entre el cliente y el servidor

LDAP. La capa de transporte segura se establece mediante el protocolo SSL/TLS (Secure Sockets Layer/Transport Layer Security), lo que garantiza la confidencialidad y la integridad de los datos transmitidos.

Al utilizar LDAPS, se establece una conexión cifrada entre el cliente y el servidor LDAP, lo que protege la información sensible, como nombres de usuario, contraseñas y otros datos confidenciales, frente a posibles interceptaciones o manipulaciones por parte de atacantes.

La seguridad proporcionada por LDAPS se basa en la utilización de certificados digitales para autenticar tanto al cliente como al servidor. El cliente verifica la autenticidad del certificado del servidor y, si es válido, establece una conexión segura. Esto permite proteger la comunicación frente a posibles ataques de intermediarios o suplantación de identidad.

LDAPS se utiliza comúnmente en entornos empresariales donde se requiere una mayor seguridad en la comunicación con los servicios LDAP. Es especialmente útil en casos donde se transmiten datos sensibles, como contraseñas, y se necesita garantizar la privacidad de la información.

Es importante tener en cuenta que LDAPS requiere la configuración adecuada tanto en el cliente como en el servidor para habilitar la capa de seguridad SSL/TLS. Además, se deben gestionar y renovar los certificados digitales para mantener la integridad de la comunicación.[3]

Certificado SSL/TLS:

Un certificado SSL/TLS utilizado para la conexión con LDAPS es un componente esencial para establecer una comunicación segura y confiable entre el cliente y el servidor LDAP. Aquí hay más información relevante sobre los certificados SSL para la conexión LDAPS:

Autoridades de certificación (CA): Los certificados SSL/TLS son emitidos por una Autoridad de Certificación (CA) confiable. Una CA es una entidad de confianza que verifica la identidad

[3] Carter, G. (2003). LDAP System Administration: Putting Directories to Work. " O'Reilly Media, Inc.".

del titular del certificado y firma digitalmente el certificado para confirmar su autenticidad. Las CAs populares incluyen Let's Encrypt, Symantec, Comodo, entre otras.

Contenido del certificado: Un certificado SSL/TLS contiene información importante, como el nombre del dominio o la dirección IP del servidor LDAP, el nombre de la organización o empresa propietaria del certificado y la clave pública del servidor. Además, el certificado también incluye la firma digital de la CA que emitió el certificado.

Validación del certificado: Antes de establecer una conexión LDAPS, el cliente debe validar el certificado del servidor para garantizar su autenticidad. Esto implica verificar que el certificado esté emitido por una CA confiable y que no haya sido revocado. El cliente también puede verificar si el nombre del dominio o la dirección IP en el certificado coincide con el servidor LDAP al que se está intentando conectar.

Administración del certificado: Los certificados SSL/TLS tienen una fecha de vencimiento y deben renovarse periódicamente. Es importante administrar y renovar los certificados para evitar interrupciones en la comunicación segura. Las organizaciones también pueden utilizar certificados autofirmados si no desean depender de una CA externa, aunque estos certificados pueden requerir configuraciones adicionales en los clientes para aceptarlos como confiables.

Configuración del servidor: Para habilitar LDAPS en el servidor LDAP, se debe configurar adecuadamente para utilizar el certificado SSL/TLS. Esto incluye instalar y configurar el certificado en el servidor, así como configurar el servidor para utilizar el puerto apropiado (por defecto, el puerto 636 para LDAPS).

La utilización de certificados SSL/TLS en la conexión con LDAPS proporciona seguridad y privacidad a la comunicación entre el cliente y el servidor, evitando la interceptación y manipulación de datos sensibles. Es una práctica recomendada para proteger las

operaciones LDAP en entornos empresariales y garantizar la integridad de la información transmitida.[4]

ldap_connect():

La función ldap_connect() es una función en PHP que se utiliza para establecer una conexión con un servidor LDAP.

Cuando se llama a ldap_connect(), se intenta establecer una conexión con el servidor LDAP especificado, utilizando los parámetros proporcionados. Estos parámetros pueden incluir la dirección IP o el nombre de host del servidor LDAP, así como el puerto en el que se encuentra el servicio LDAP.

La función ldap_connect() devuelve un recurso de conexión LDAP si se establece la conexión correctamente, o devuelve false en caso de que no se pueda establecer la conexión.

Es importante destacar que ldap_connect() solo establece la conexión con el servidor LDAP, pero no realiza ninguna operación de autenticación o búsqueda en la base de datos LDAP. Una vez establecida la conexión, se pueden realizar otras operaciones, como autenticación de usuarios, búsqueda de entradas en el directorio o modificaciones de datos, utilizando las funciones y métodos proporcionados por la extensión LDAP de PHP.

ldap_set_option($connect, LDAP_OPT_PROTOCOL_VERSION, 3):

La función ldap_set_option($connect, LDAP_OPT_PROTOCOL_VERSION, 3); establece la opción LDAP_OPT_PROTOCOL_VERSION en el valor 3 para la conexión LDAP especificada por la variable $connect.

---

[4] Chen, Y., & Su, Z. (2015, August). Guided differential testing of certificate validation in SSL/TLS implementations. In Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering (pp. 793-804).

La opción LDAP_OPT_PROTOCOL_VERSION se utiliza para especificar la versión del protocolo LDAP que se utilizará en la comunicación entre el cliente y el servidor LDAP. Al establecerla en 3, se selecciona la versión 3 del protocolo LDAP.

La versión 3 del protocolo LDAP (LDAPv3) es una versión más reciente y mejorada en comparación con las versiones anteriores (LDAPv2 y LDAPv1). LDAPv3 incluye mejoras de seguridad, mayor flexibilidad y características adicionales en comparación con las versiones anteriores.

Al establecer LDAP_OPT_PROTOCOL_VERSION en 3, le estás indicando a la conexión LDAP que utilice LDAPv3 para las operaciones que realices. Esto permite aprovechar las ventajas y características proporcionadas por LDAPv3, como la capacidad de realizar búsquedas más avanzadas, trabajar con atributos binarios y soporte para controles de extensión.

Es importante tener en cuenta que no todos los servidores LDAP admiten LDAPv3, y algunos pueden requerir configuraciones adicionales para habilitar y admitir esta versión. Por lo tanto, es recomendable verificar la compatibilidad del servidor LDAP antes de establecer LDAP_OPT_PROTOCOL_VERSION en 3.

En general, utilizar LDAPv3 es una buena práctica, ya que proporciona mejor seguridad y funcionalidad en comparación con las versiones anteriores del protocolo.

ldap_bind():
La función ldap_bind() se utiliza en PHP para autenticarse en un servidor LDAP después de haber establecido una conexión exitosa con el mismo mediante la función ldap_connect().

La autenticación es un paso necesario para acceder y realizar operaciones en un directorio LDAP, como buscar, modificar o agregar entradas.

Existen dos formas de utilizar la función ldap_bind():

1. Autenticación anónima: Si el servidor LDAP permite conexiones anónimas, se puede utilizar ldap_bind() sin proporcionar ningún nombre de usuario o contraseña. Esto se hace pasando null o una cadena vacía ("") como argumento para los parámetros $bindRDN y $bindPassword. Por ejemplo:

   ```
   $ldapConnection = ldap_connect("ldap://ldap.example.com");
   ldap_bind($ldapConnection); // Autenticación anónima
   ```

2. Autenticación con credenciales: Si se requiere autenticación con un nombre de usuario y una contraseña válidos, se deben proporcionar como argumentos los valores correspondientes para $bindRDN y $bindPassword. Por ejemplo:

   ```
   $ldapConnection = ldap_connect("ldap://ldap.example.com");
   ldap_bind($ldapConnection,"cn=usuario,ou=usuarios,dc=example,dc=com",
   "contraseña");
   ```

   La función ldap_bind() intentará autenticar al cliente en el servidor LDAP utilizando las credenciales proporcionadas. Si la autenticación tiene éxito, la función devolverá true. En caso contrario, devolverá false.

   Es importante tener en cuenta que la autenticación exitosa no garantiza que el usuario tenga permisos suficientes para realizar las operaciones deseadas en el directorio. Los permisos y los niveles de acceso están determinados por la configuración del servidor LDAP y las políticas de seguridad establecidas.

ldap_search():

La función ldap_search() se utiliza en PHP para realizar una búsqueda en un servidor LDAP después de haber establecido una conexión y autenticación exitosas mediante las funciones ldap_connect() y ldap_bind() respectivamente.

La búsqueda en un servidor LDAP permite encontrar y recuperar entradas que coincidan con ciertos criterios de búsqueda dentro del árbol de directorio. La función ldap_search() acepta varios parámetros que definen los detalles de la búsqueda, incluyendo el objeto de conexión LDAP, la base de búsqueda, el filtro de búsqueda y los atributos a recuperar.

A continuación, se muestra la estructura básica de la función ldap_search() en PHP:

ldap_search($ldapConnection, $baseDN, $filter, $attributes);

$ldapConnection: El recurso de conexión LDAP devuelto por ldap_connect().
$baseDN: El DN (Distinguished Name) de la base de búsqueda, especificando el punto de partida dentro del árbol de directorio desde donde se realizará la búsqueda.
$filter: El filtro de búsqueda LDAP que define los criterios para encontrar las entradas deseadas.
$attributes (opcional): Un array o una cadena que especifica los atributos que se desean recuperar de las entradas encontradas. Si se omite, se devolverán todos los atributos de las entradas.

Después de realizar la búsqueda con ldap_search(), los resultados pueden ser procesados utilizando la función ldap_get_entries() para obtener un array de las entradas encontradas y sus atributos correspondientes.

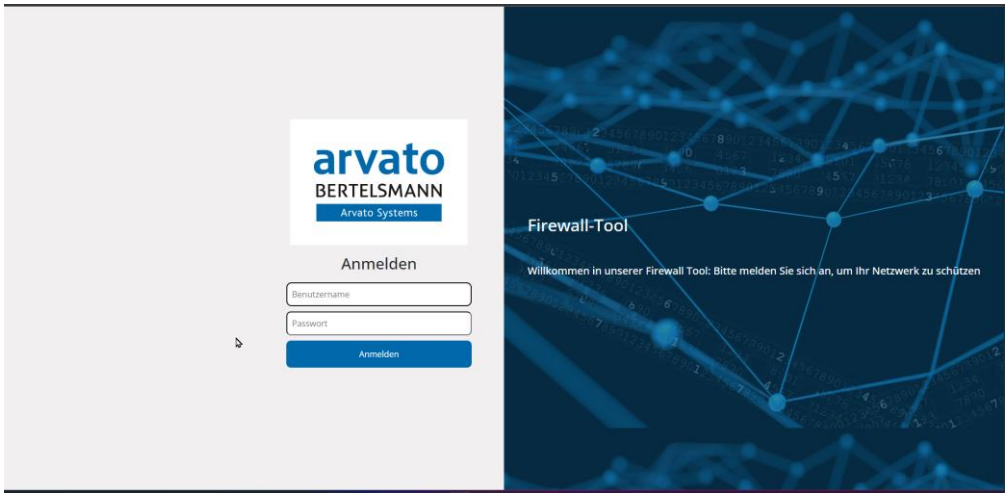
Atributos de LDAP:

- cn (Common Name): Este atributo se utiliza para representar el nombre común de una entrada en el directorio LDAP. Generalmente, se refiere al nombre completo o identificador único de un objeto dentro del árbol de directorio.
- ou (Organizational Unit): Este atributo se utiliza para representar una unidad organizativa dentro de una estructura jerárquica. Se utiliza para organizar y agrupar objetos relacionados en el directorio.

- dc (Domain Component): Este atributo se utiliza para representar los componentes de un nombre de dominio en el contexto de un servidor LDAP. El nombre de dominio se descompone en partes más pequeñas utilizando dc como separador. [5]

Vista final de la herramienta de Cortafuegos:

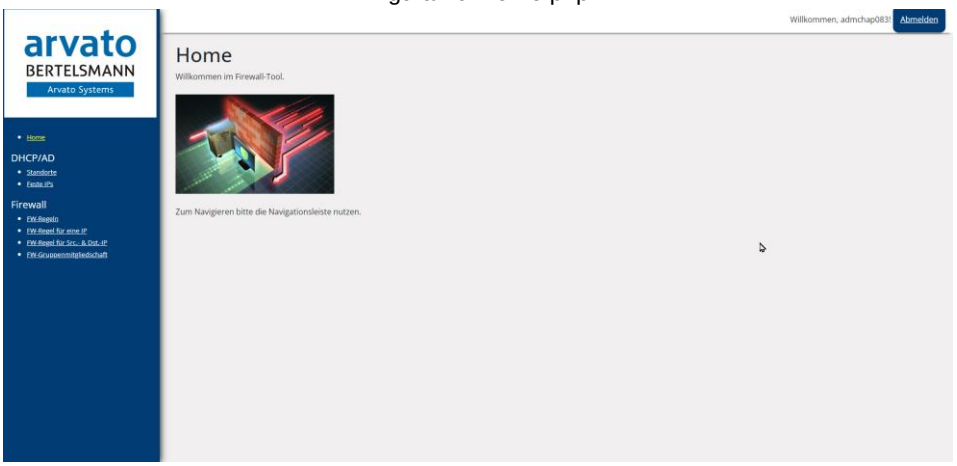
Figura 15. login.php



Fuente 19. Autor

La Figura 15, representa una página con una sección de inicio de sesión y otra sección que proporciona información sobre el cortafuegos "Firewall-Tool" y un mensaje de bienvenida.

Figura 16. home.php

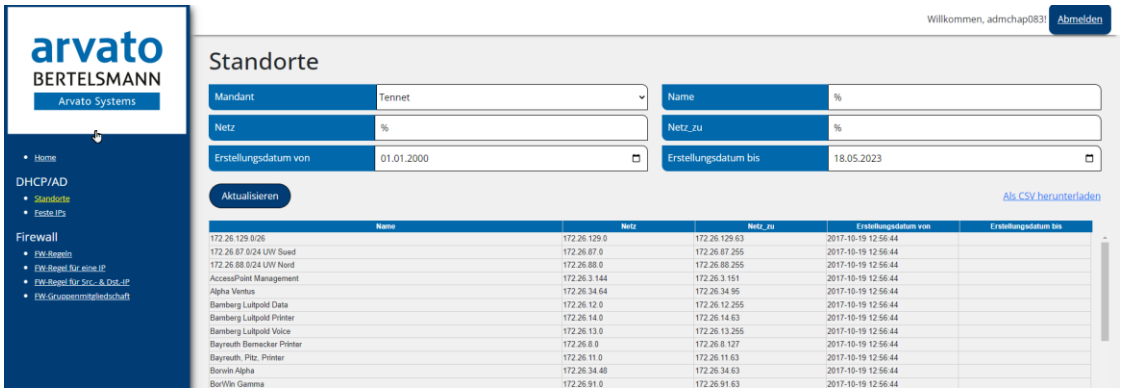


Fuente 20. Autor

[5] Gilmore, W. J. (2006). PHP and LDAP. Beginning PHP and MySQL 5: From Novice to Professional, 399-423.

La Figura 16, representa una página con una estructura de diseño de columnas, donde se incluye contenido dinámico a través de archivos PHP para el menú de navegación, la sección superior, el título de la página y el pie de página. El contenido está en alemán y se presenta una imagen de un firewall con un mensaje para navegar en la página. El contenido de la izquierda es el menú, la cabecera contiene la bienvenida, el nombre del usuario con la sesión activa y al lado un botón para cerrar sesión.

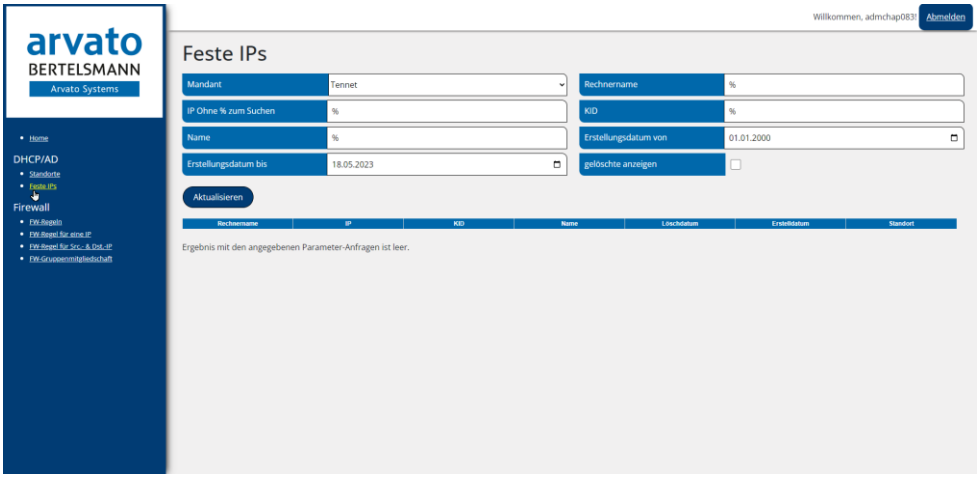
Figura 17. locations.php



Fuente 21. Autor

La Figura 17 muestra un formulario de búsqueda de ubicaciones con opciones para ingresar criterios de búsqueda y filtrar los resultados. Los resultados se muestran en una tabla y también se proporciona la opción de descargar los resultados en formato CSV.

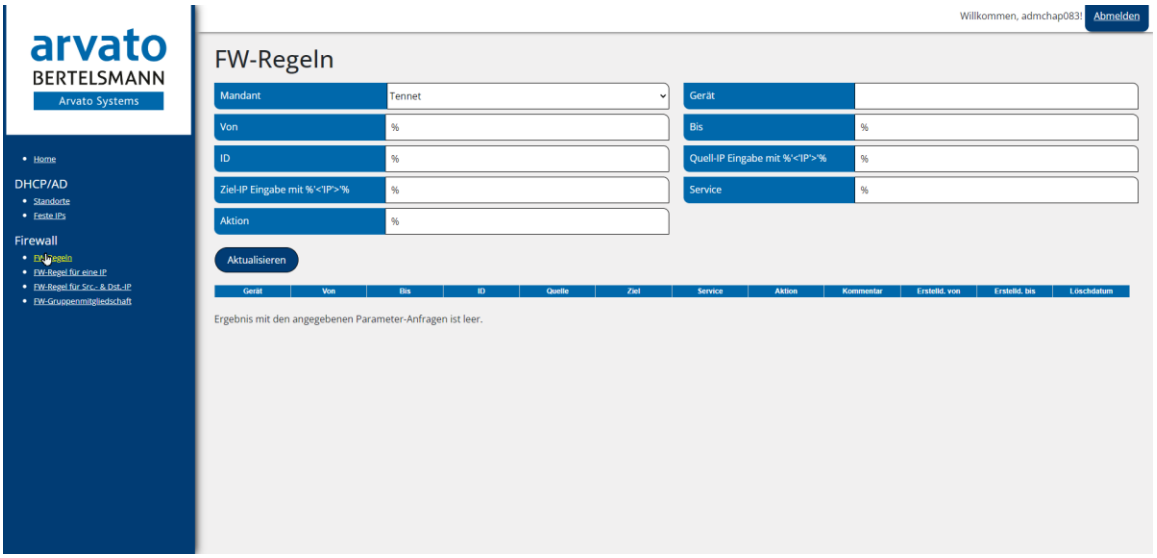
Figura 18. fixedIPs.php



Fuente 22. Autor

La Figura 18 muestra un formulario de búsqueda de reglas de firewall con opciones para ingresar criterios de búsqueda y filtrar los resultados. Los resultados se muestran en una tabla y también se proporciona la opción de descargar los resultados en formato CSV

Figura 19. fwRules.php



Fuente 23. Autor

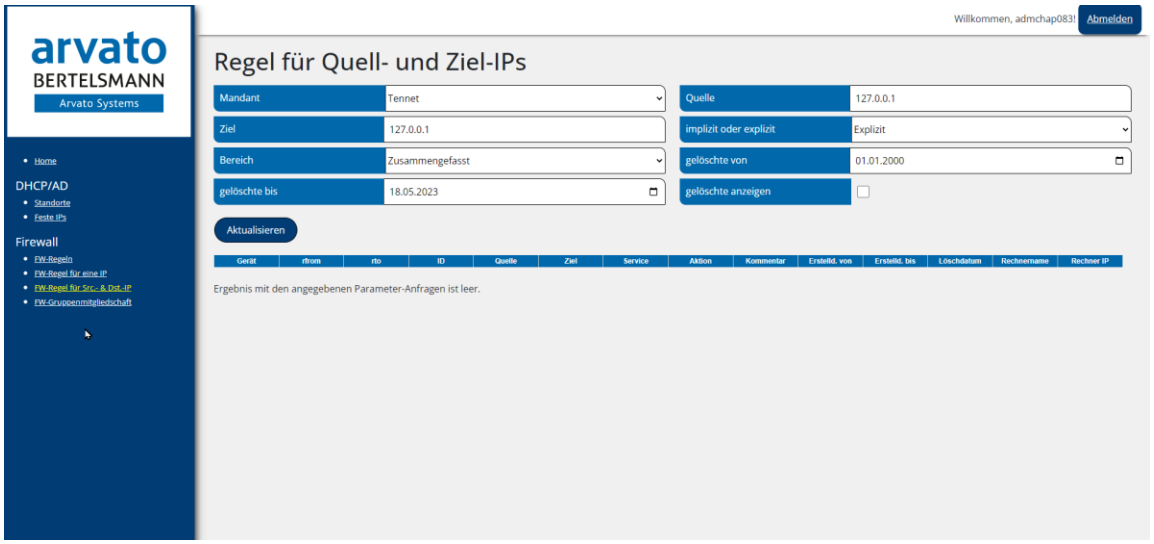
La Figura 19 muestra un formulario para buscar reglas de firewall relacionadas con una dirección IP específica y muestra los resultados en una tabla, brindando opciones para filtrar y descargar los datos.

Figura 20. fwRulesOneIP.php

Fuente 24. Autor

La Figura 20 muestra un formulario para buscar reglas de firewall relacionadas con una dirección IP específica y muestra los resultados en una tabla, brindando opciones para filtrar y descargar los datos.

Figura 21. fwRulesSrcDst.php

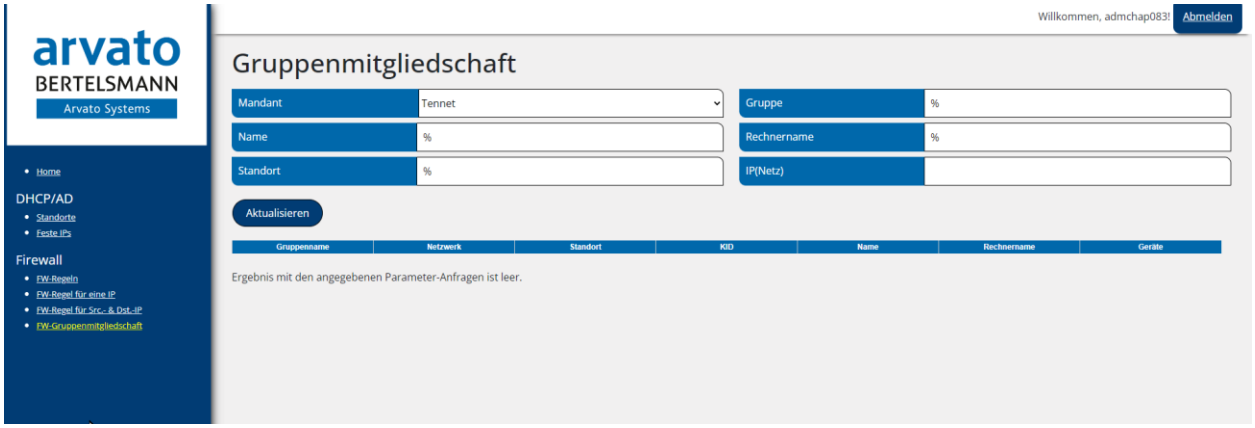


Fuente 25. Autor

La Figura 21 muestra que esta página permite a los usuarios buscar y mostrar reglas de firewall basadas en diferentes criterios, como la dirección IP de origen, la dirección IP de destino, reglas explícitas/implícitas, rango de fechas, etc. Los resultados se presentan en

un formato de tabla. También hay una opción para descargar los resultados como un archivo CSV.

Figura 22.fwRulesGroupMembership.php



Fuente 26. Autor

La Figura 22 muestra una interfaz de búsqueda y visualización de resultados de pertenencia a grupos relacionados al cortafuegos. Permite al usuario introducir varios criterios de búsqueda y muestra los resultados en una tabla. También ofrece la opción de descargar los resultados en formato CSV.

Figura 23. Vista desde un celular o tablet

Fuente 27. Autor

La Figura 23 nos muestra la página de ubicaciones, pero esta vez adaptada en una versión para celular o tablet. El menú lateral izquierdo se acopla y desacopla adaptándose a el tamaño de la pantalla, para lograr que el usuario tenga mayor visibilidad.

4.3.4. Implementación del plan de pruebas

4.3.4.1. Diseño del plan de pruebas teniendo en cuenta las recomendaciones del OWASP (Open Web Application Security Project)

- Requisitos de prueba:
  - Documentar los requisitos funcionales y no funcionales de autenticación con LDAPS.
  - Identificar los sistemas y componentes involucrados en la autenticación con LDAPS.
- Análisis de riesgos:
  - Identificar los posibles riesgos y vulnerabilidades asociados con la autenticación con LDAPS.
  - Priorizar los riesgos según su impacto y probabilidad.
- Diseño de casos de prueba:
  - Crear casos de prueba que validen diferentes aspectos de la autenticación con LDAPS, incluyendo casos para la autenticación exitosa y fallida.
- Ejecución de pruebas:
  - Ejecutar los casos de prueba diseñados previamente, registrando los resultados y cualquier problema encontrado.
  - Verificar que la autenticación con LDAPS se realice correctamente, validando el proceso de inicio de sesión y la comunicación segura.
- Informe final:
  - Preparar un informe final que resuma los hallazgos, recomendaciones y mejoras propuestas.

4.3.4.2. Ejecución del plan de pruebas teniendo en cuenta las recomendaciones del OWASP (Open Web Application Security Project)

- Requisitos de prueba:
    - Documentar los requisitos funcionales y no funcionales de autenticación con LDAPS.
        - Requisitos funcionales:
            - Inicio de sesión: Proporcionar un mecanismo para que los usuarios inicien sesión utilizando sus credenciales de autenticación con LDAPS.
            - Permisos de autenticación: Solo se pueden autenticar los usuarios pertenecientes al grupo “Tennet-NMD-G Firewall-Tool Reader GG” en Active Directory.
        - Requisitos no funcionales:
            - Seguridad: Garantizar la seguridad de las comunicaciones mediante el uso de cifrado SSL/TLS a través de LDAPS.
            - Rendimiento: Proporcionar un rendimiento adecuado durante el proceso de autenticación, minimizando el tiempo de respuesta.
            - Disponibilidad: Mantener la disponibilidad del sistema de autenticación, asegurando que los usuarios puedan iniciar sesión cuando lo necesiten.
            - Escalabilidad: Permitir que el sistema de autenticación con LDAPS se expanda y maneje un número creciente de usuarios sin degradar el rendimiento.
    - Identificar los sistemas y componentes involucrados en la autenticación con LDAPS.
        - El servidor LDAP
        - Active Directory
        - Certificado SSL/TLS
        - Cliente LDAP
- Análisis de riesgos:

- Identificar los posibles riesgos y vulnerabilidades asociados con la autenticación con LDAPS.
    - Fallos en el cifrado: Si el cifrado SSL/TLS utilizado en LDAPS no está configurado correctamente o es débil, puede haber riesgos de interceptación de datos o ataques de descifrado. Esto podría exponer las credenciales de autenticación y comprometer la seguridad de la autenticación.
    - Certificados no confiables: Si los certificados utilizados en LDAPS no son confiables o no se valida su autenticidad, existe el riesgo de que los usuarios sean víctimas de ataques de suplantación de identidad (phishing) o que se establezcan conexiones inseguras con servidores LDAP maliciosos.
    - Exposición de credenciales: Si las credenciales de autenticación se almacenan o transmiten de manera insegura en el cliente o el servidor LDAP, pueden ser interceptadas y utilizadas por atacantes para acceder de manera no autorizada al sistema.
    - Ataques de fuerza bruta: Si no se implementan medidas adecuadas para mitigar los ataques de fuerza bruta, los atacantes podrían intentar adivinar las contraseñas de los usuarios mediante la repetición masiva de intentos de inicio de sesión, lo que podría conducir al acceso no autorizado.
    - Robo de sesiones: Si no se implementan mecanismos de protección adecuados, las sesiones de autenticación con LDAPS podrían estar expuestas al robo o secuestro de sesiones, lo que permitiría a los atacantes hacerse pasar por usuarios legítimos.
    - Acceso no autorizado a los datos del directorio: Si se configuran incorrectamente los permisos y controles de acceso en el servidor LDAP, podría permitirse el acceso no autorizado a los datos almacenados en el directorio, lo que podría exponer información sensible.

- Desbordamiento de búfer y vulnerabilidades de software: Si el servidor o cliente LDAP tiene vulnerabilidades conocidas, como desbordamiento de búfer u otras debilidades en el software, los atacantes podrían explotar estas vulnerabilidades para comprometer la autenticación y acceder a los sistemas.

- Priorizar los riesgos según su impacto y probabilidad.

  Para priorizar los riesgos asociados con LDAPS según su impacto y probabilidad, se pueden utilizar escalas numéricas del 1 al 5, donde 1 representa un impacto/probabilidad bajo y 5 representa un impacto/probabilidad alto. A continuación, en la Tabla 5, se muestra una posible priorización para los riesgos mencionados

Tabla 5. Riesgos según su impacto y probabilidad

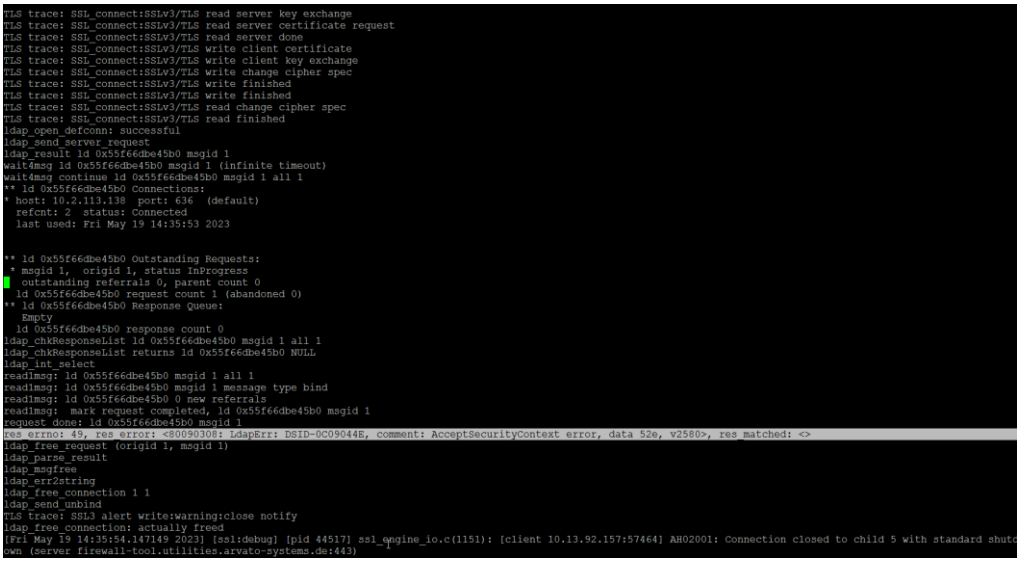
	Impacto	Probabilidad	Puntuación de riesgo
Fallos en el cifrado	4	4	16
Certificados no confiables	3	3	9
Exposición de credenciales	4	3	12
Ataques de fuerza bruta	3	2	6
Robo de sesiones	4	2	8
Acceso no autorizado a los datos del directorio	4	3	12
Desbordamiento de búfer y vulnerabilidades de software	3	2	6

Fuente 28. Autor

- Diseño de casos de prueba:
    - Crear casos de prueba que validen diferentes aspectos de la autenticación con LDAPS, incluyendo casos para la autenticación exitosa y fallida.
        - Un usuario perteneciente al grupo de Active Directory inicie sesión, este debe ser un caso de éxito.
        - Un usuario no perteneciente a el grupo de Active Directory inicie sesión, este debe ser un caso de fallo.
- Ejecución de pruebas:
    - Ejecutar los casos de prueba diseñados previamente, registrando los resultados y cualquier problema encontrado.

      En el primer caso se intentó ingresar con un usuario no existente y se obtuvo el resultado mostrado en la Figura 24

Figura 24. Caso de prueba fallido

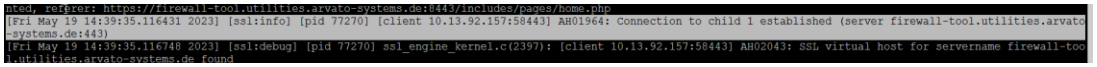


Fuente 29. Autor

    - Verificar que la autenticación con LDAPS se realice correctamente, validando el proceso de inicio de sesión y la comunicación segura.

En el segundo caso se intentó ingresar con un usuario existente en el grupo y se obtuvo un resultado exitoso como se muestra en la Figura 25.

Figura 25. Caso de prueba exitoso



Fuente 30. Autor

- Informe final:
  Luego de hacer la prueba se detectó que había un problema con los datos del usuario, sus credenciales podian ser vistas en los archivos de log cuando se estaban analizando los errores. Por tal motivo se decidió agregarle una función en la contraseña del login de esta manera:

  $password_hashed = password_hash($password, PASSWORD_DEFAULT);

4.3.4.3. Realización de ajustes necesarios a partir del plan de pruebas

Al agregar la función del hash a la contraseña se logró cifrarla y esto se puede ver evidenciado en el archivo de log en la Figura 26.

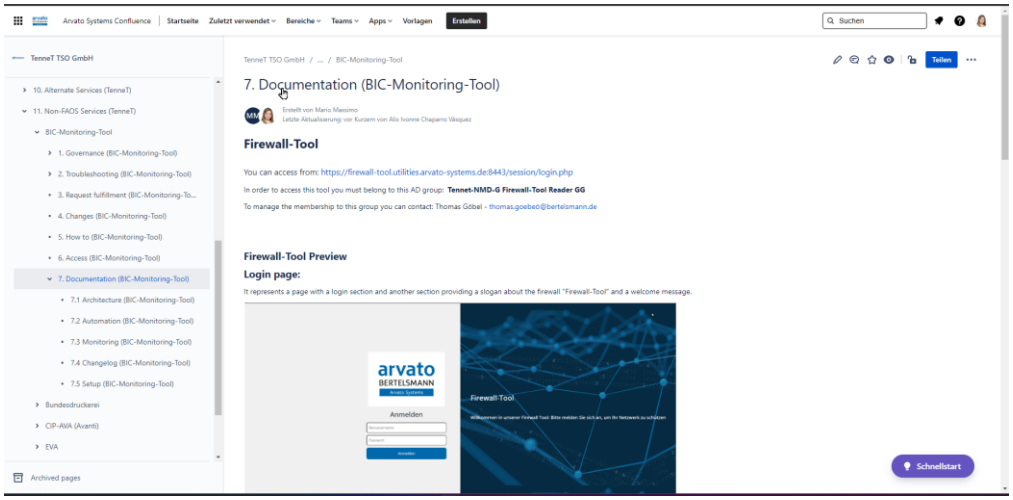
Figura 26. Contraseña cifrada

Fuente 31. Autor

4.3.4.4. Construcción del manual de usuario

Se llevó a cabo la documentación del manual de usuario y se publicó en Confluence, que es donde la empresa aloja toda su documentación. En la Figura 27 puede evidenciar su publicación.

Figura 27. Manual de usuario en Confluence



Fuente 32. Autor

5. CONCLUSIONES

1. Las entrevistas con el cliente desempeñan un papel fundamental para obtener una comprensión clara de los requerimientos de seguridad, funcionalidad y usabilidad de la herramienta de cortafuegos. Estos hallazgos nos permitirán desarrollar una solución personalizada que satisfaga las necesidades del cliente, garantizando la protección efectiva del centro de datos contra amenazas y asegurando un entorno seguro y confiable.
2. La definición de las opciones de adaptación en cuanto a la seguridad y la funcionalidad a través de diagramas de clase, casos de uso, de despliegue y mockups nos permite tener una visión clara y detallada de nuestra solución. Estas representaciones gráficas nos ayudan a tomar decisiones informadas, comunicar de manera efectiva y garantizar que nuestra solución cumpla con los requisitos y expectativas del proyecto.
3. La implementación de la seguridad en el cortafuegos mediante lenguajes de código abierto y la autenticación de LDAPS utilizando Active Directory nos brinda una solución robusta y confiable para proteger el sistema. Al aprovechar estas tecnologías, podemos garantizar la autenticación segura de los usuarios y proteger la integridad de los datos, fortaleciendo así la seguridad del entorno.
4. La ejecución de un plan de pruebas de errores y criterios de adaptación en la seguridad del aplicativo, siguiendo la guía de recomendaciones de OWASP, nos ayuda a fortalecer la seguridad de nuestra aplicación web. Al identificar y corregir posibles fallas y vulnerabilidades, podemos garantizar la protección de los datos y la confidencialidad de los usuarios, brindando una experiencia segura y confiable en nuestra aplicación.
5. La autenticación con LDAPS para un cortafuegos en un servidor de Linux que utiliza Active Directory fortalece la seguridad del entorno al establecer una autenticación cifrada y centralizada. Esta implementación proporciona un control de acceso más riguroso y facilita la administración de usuarios y permisos. Al combinar estas tecnologías, se establece un marco sólido para proteger los recursos y asegurar un entorno seguro en el cortafuegos.

6. REFERENCIAS

- Ciberseg. (2021). LDAP: qué es, cómo funciona, usos y riesgos de seguridad. Ciberseguridad. https://ciberseguridad.com/guias/prevencion-proteccion/ldap/
- Castillo, J. A. (2019). LDAP: Qué es y para qué se utiliza este protocolo. Profesional Review. https://www.profesionalreview.com/2019/01/05/ldap/
- Carter, G. (2003). LDAP System Administration: Putting Directories to Work. " O'Reilly Media, Inc.".
- Chen, Y., & Su, Z. (2015, August). Guided differential testing of certificate validation in SSL/TLS implementations. In Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering (pp. 793-804).
- Gilmore, W. J. (2006). PHP and LDAP. Beginning PHP and MySQL 5: From Novice to Professional, 399-423.