Tarea #982 Instalar un UTM y configurar el firewall creando una regla por cada servicio en el MS2

Israel Alejandro Cel Alcocer

Seguridad de Datos

Docente: Ismael Jimenez

Descripción de Endian Community

Endian Community es una versión de código abierto y gratuita de la suite de firewall Endian, que es una solución de seguridad de red. Está diseñada principalmente para pequeñas y medianas empresas (PYMEs), y ofrece funcionalidades como un firewall, un router, un filtro de contenido web, un servidor VPN, y un servidor de correo electrónico, entre otros.

Pasos a desarrollar

En este documento podremos aprender a como configurar un firewall utilizando Endian Community en VirtualBox. Iniciamos a través del proceso de instalación y configuración de Endian Community en una máquina virtual. Se enfoca en configurar dos máquinas virtuales: una para el firewall Endian y otra como cliente Windows 7.

Preparación de la máquina virtual:

Comenzamos creando una máquina virtual específicamente para Endian Community. Asigna 1GB de memoria RAM y configura dos interfaces de red: una para conectar la máquina virtual a una red interna y otra para proporcionar acceso a Internet.

1.- Instalación de Endian Community:

Se descarga la imagen de Endian Community de la página oficial y se procede a la instalación en la máquina virtual. Durante la instalación, se selecciona el inglés como idioma y establece la dirección IP estática para Endian en 192.168.0.20.

2.- Configuración del cliente Windows 7:

Se prepara otra máquina virtual que actúa como cliente, corriendo Windows 7. Se configura su tarjeta de red para operar en la misma red interna que el firewall Endian, asignándole una dirección IP estática dentro del rango de la red interna.

3.- Verificación de conectividad:

Utilizando la línea de comandos, se verifica la conectividad entre el cliente Windows y el firewall, asegurándose de que pueden comunicarse correctamente.

4.- Configuración a través de la interfaz web de Endian:

Accediendo a la interfaz web del Endian por medio del navegador en el cliente Windows, se inicia la configuración detallada del firewall. Esto incluye ajustes de idioma y región, así como la configuración inicial de la contraseña de administrador.

5.- Servicios y políticas de firewall:

Se habilita y configura servicios esenciales como el servidor DHCP y el proxy HTTP. Establece políticas de acceso y reglas específicas para gestionar el tráfico de la red.

6.- Filtrado de contenido:

Se crea un perfil de filtrado web para bloquear contenido no deseado como sitios de adultos, juegos, hacking, y tiendas. Se configura el perfil para actualizar diariamente sus filtros de URL.

7.- Habilitación del proxy HTTPS:

Debido a que muchas páginas modernas usan HTTPS, Antonio configura el proxy HTTPS para manejar y filtrar este tráfico cifrado. Esto incluye la creación y distribución de un certificado a la máquina cliente para permitir la inspección del tráfico.

8.- Pruebas y ajustes finales:

Finalmente, se realizan pruebas para asegurar que los sitios web especificados están siendo bloqueados conforme a las políticas establecidas. Realiza ajustes en la configuración del proxy y las políticas de firewall según sea necesario para asegurar el funcionamiento adecuado.

Proceso de configuración de varios servicios y las reglas específicas del firewall que se aplican en cada caso.

Se describe el proceso de configuración de varios servicios y las reglas específicas del firewall que se aplican en cada caso.

1.- Servidor DHCP:

Regla: Permitir tráfico en el puerto 67 (UDP) y 68 (UDP) internamente para facilitar la distribución de direcciones IP en la red local.

Configuración: Se habilita un servidor DHCP que asigna automáticamente direcciones IP a los dispositivos de la red.

2.- Proxy HTTP y HTTPS:

Regla para HTTP: Redireccionar todo el tráfico HTTP del puerto 80 al puerto 8080 donde está configurado el proxy.

Regla para HTTPS: Todo el tráfico HTTPS es redirigido para inspección a través del proxy, que utiliza un puerto específico (usualmente 3128 o 8080) y requiere la instalación de un certificado en los clientes.

Configuración: Habilitar el modo transparente para el proxy HTTP, mientras que para HTTPS se configura desencriptación para permitir la inspección de tráfico cifrado.

3.- Filtrado de Contenido Web:

Regla: Aplicar políticas de filtrado basadas en categorías de sitios web (como sitios para adultos, juegos, hacking) y listas negras o blancas específicas.

Configuración: Se crea un perfil de filtrado web que se aplica a todos los usuarios o a grupos específicos dentro de la red, gestionando el acceso a contenido en línea.

4.- Registros de Conexión:

Regla: Habilitar el registro detallado de todas las conexiones a través del firewall para monitorizar y auditar el tráfico de red.

Configuración: Se configuran los registros para que capturen datos sobre el tráfico permitido, bloqueado y las alertas generadas por el sistema.

Estas reglas y configuraciones forman la base de un sistema de firewall robusto que no solo protege la red de accesos no autorizados y tráfico malicioso, sino que también ofrece un control detallado sobre el tipo de contenido al que pueden acceder los usuarios. La implementación de estas reglas debe considerar tanto la seguridad de la red como las necesidades específicas de acceso y comunicación de la organización.

Presencia del Metasploitable 2.

Dentro de un entorno que utiliza un firewall como Endian Community, Metasploitable 2 podría usarse de las siguientes maneras:

Segmentación de Red: Idealmente, Metasploitable 2 debería estar en una segmentación de red separada que pueda ser estrictamente controlada por el firewall. Esto evita que cualquier ataque exitoso sobre Metasploitable 2 se propague al resto de la red.

Reglas de Firewall: Deberías configurar reglas específicas en el firewall para controlar qué tráfico puede entrar y salir de la red donde se aloja Metasploitable 2. Esto incluiría:

Permitir tráfico específico necesario para realizar pruebas de penetración, como tráfico HTTP, SSH, FTP, entre otros, pero solo desde y hacia direcciones IP específicas.

Bloquear todo el acceso no autorizado desde Internet a Metasploitable 2 para evitar exposiciones accidentales.

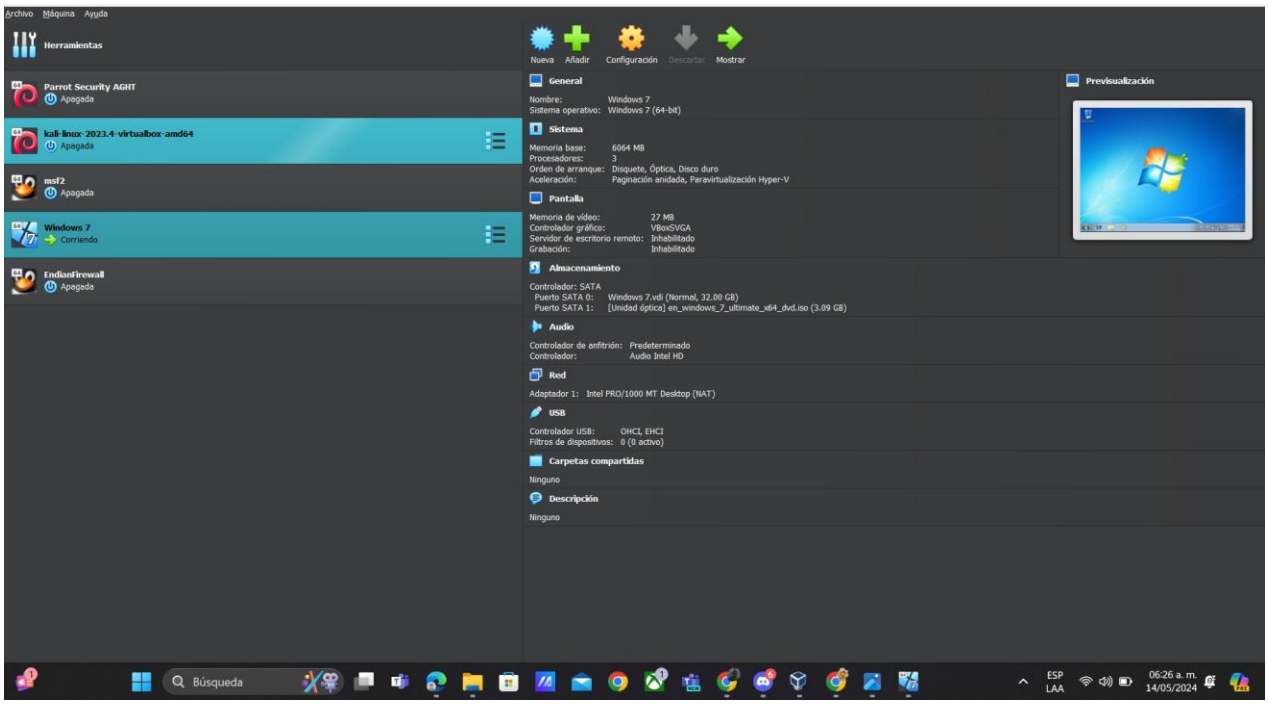
Monitoreo y logística: Dado que Metasploitable 2 contiene múltiples vulnerabilidades, es crucial monitorear cualquier tráfico sospechoso. Configurar el firewall para registrar detalladamente las actividades de red asociadas con Metasploitable 2 ayudará a identificar intentos de explotación y otras actividades maliciosas.

Aislamiento y Control: Utilizar VLANs o redes virtuales dedicadas para aislar Metasploitable 2 del resto de la red empresarial. El firewall puede ser configurado para asegurar que solo los usuarios autorizados dentro de la red puedan interactuar con Metasploitable 2.

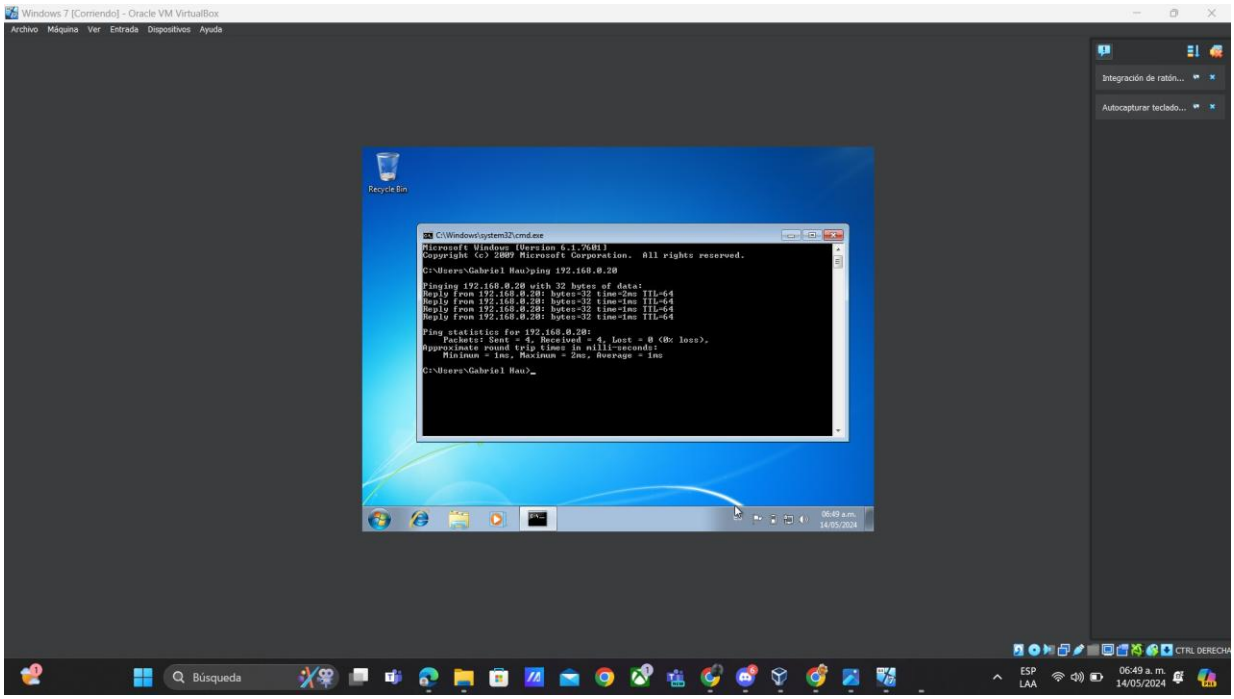
Estas medidas aseguran que puedas usar Metasploitable 2 como una herramienta de entrenamiento sin comprometer la seguridad de tu infraestructura de TI principal. Asegurarse de que el firewall está correctamente configurado para gestionar el tráfico hacia y desde Metasploitable 2 es esencial para mantener un entorno de red seguro y controlado.

Capturas de Pantalla

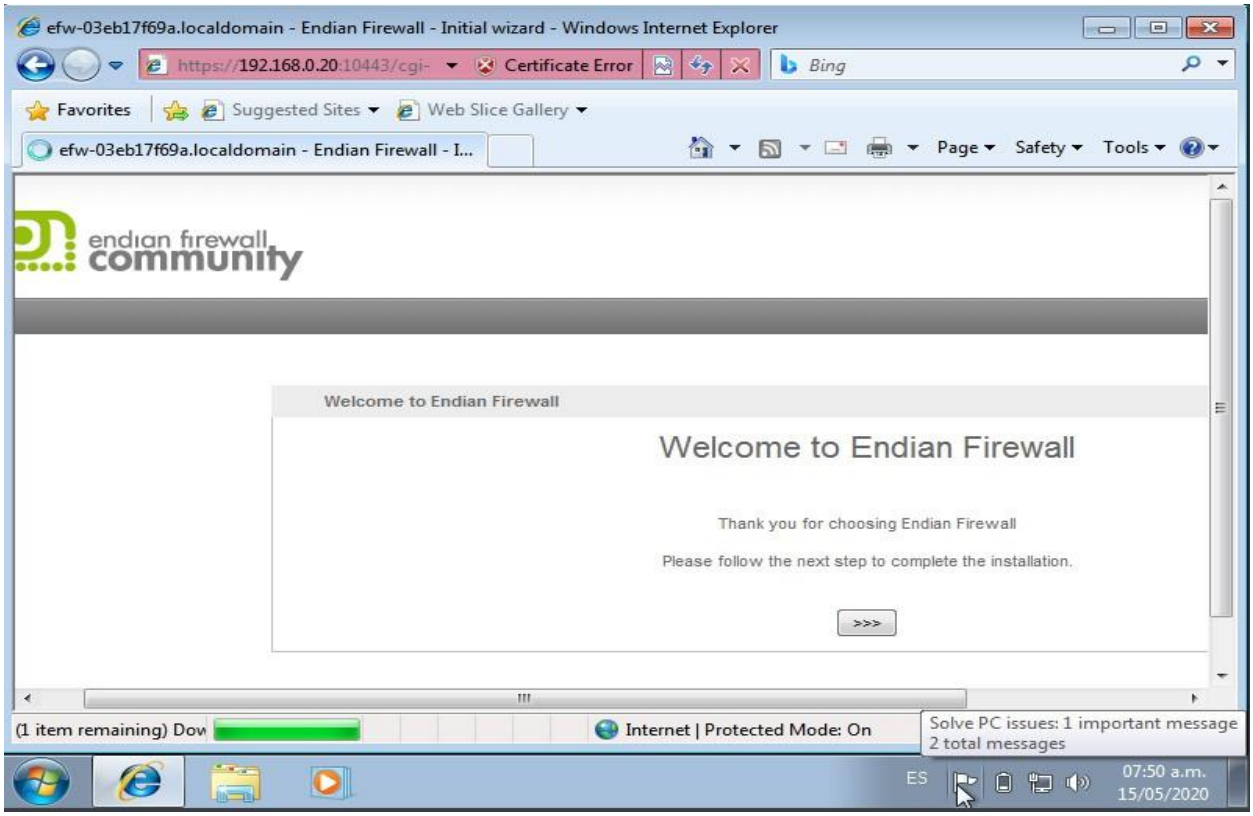
Tenemos nuestras dos máquinas configuradas.



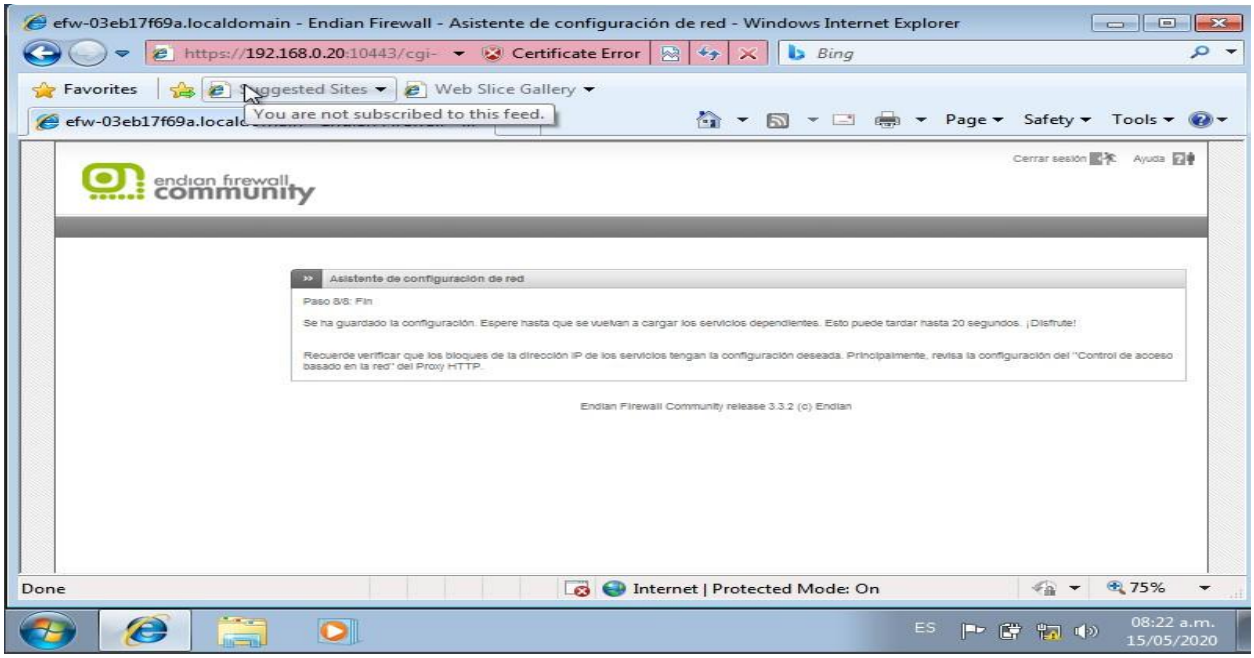
Revisión de Comunicación con debian 192.168.0.20



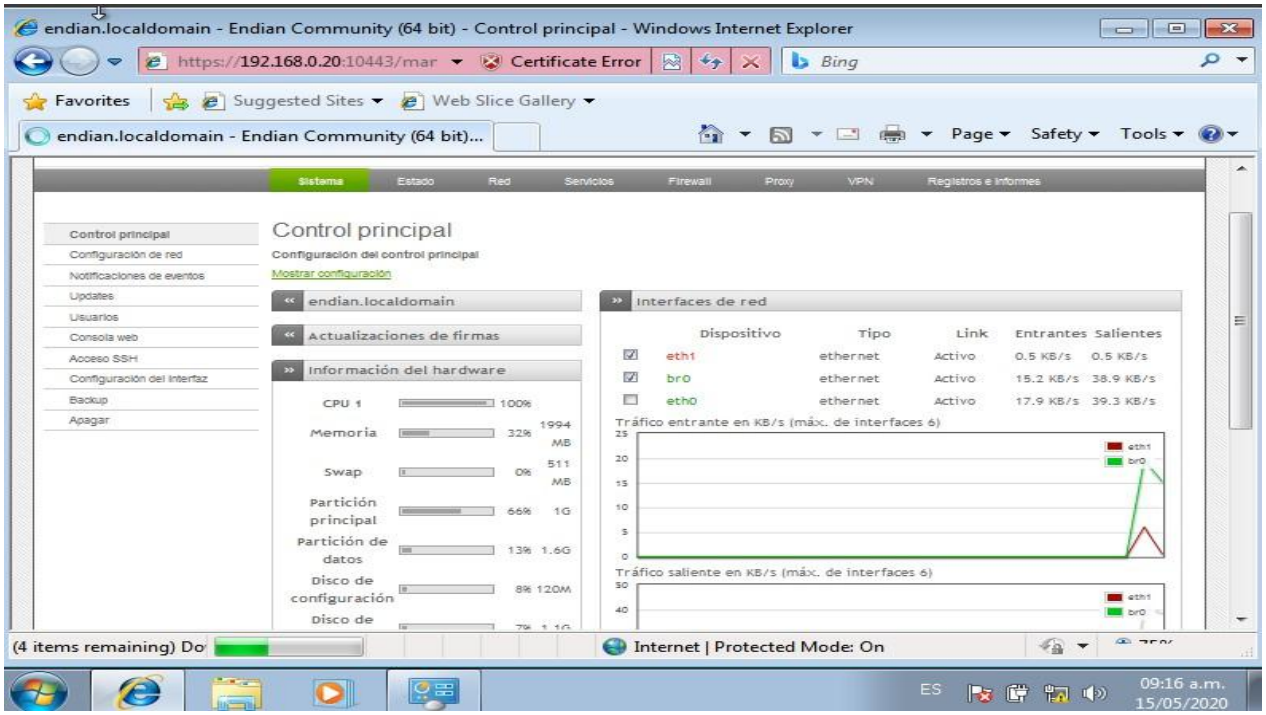
Accedemos a la página de endian firewall a través de la dirección y configuramos diferentes parámetros como el idioma , etc.



Seguimos ocho pasos para configurar la red en endian firewall.



Accedemos al control principal donde encontraremos la interfaz de red , servicios , entre otras herramientas. Con el Dashboard inicial.



Servicios

Como se había mencionado anteriormente la aplicación nos permite ver diferentes servicios de protocolos al cual podemos acceder y modificar.Por lo cual , se habilitan los proxys, firewall , entre otros servicios.

1. Firewall

Protección de red: Controla el tráfico entrante y saliente basado en políticas de seguridad predefinidas o personalizadas, ayudando a proteger la red contra accesos no autorizados y ataques.

2. Servidor VPN

Conectividad segura: Endian Community soporta VPNs usando protocolos como OpenVPN y IPsec, lo que permite conexiones seguras y cifradas para el acceso remoto a la red corporativa.

3. Filtrado de Contenido

Gestión de contenido: Ofrece capacidades de filtrado de contenido web, permitiendo bloquear o permitir acceso a sitios web basados en categorías o URLs específicas. Esto es útil para prevenir el acceso a contenido inapropiado o malicioso.

4. Servidor Proxy

Control de tráfico web: Incluye un proxy HTTP/HTTPS que ayuda a optimizar y controlar el tráfico web, además de proporcionar funciones de caching para mejorar la velocidad de acceso a sitios frecuentemente visitados.

5. Prevención de Intrusiones (IPS)

Detección y prevención: El sistema de prevención de intrusiones monitoriza el tráfico de red para detectar actividades sospechosas o maliciosas, ayudando a bloquear ataques antes de que causen daño.

6. Gestión de Correo Electrónico

Filtrado de spam y malware: Proporciona herramientas para filtrar spam y mensajes de correo electrónico maliciosos, protegiendo a los usuarios de contenido potencialmente peligroso o no deseado.

7. Servidor DNS

Resolución de nombres de dominio: Permite la configuración de un servidor DNS para la resolución de nombres dentro de la red local, facilitando la administración de nombres de dominio internos.

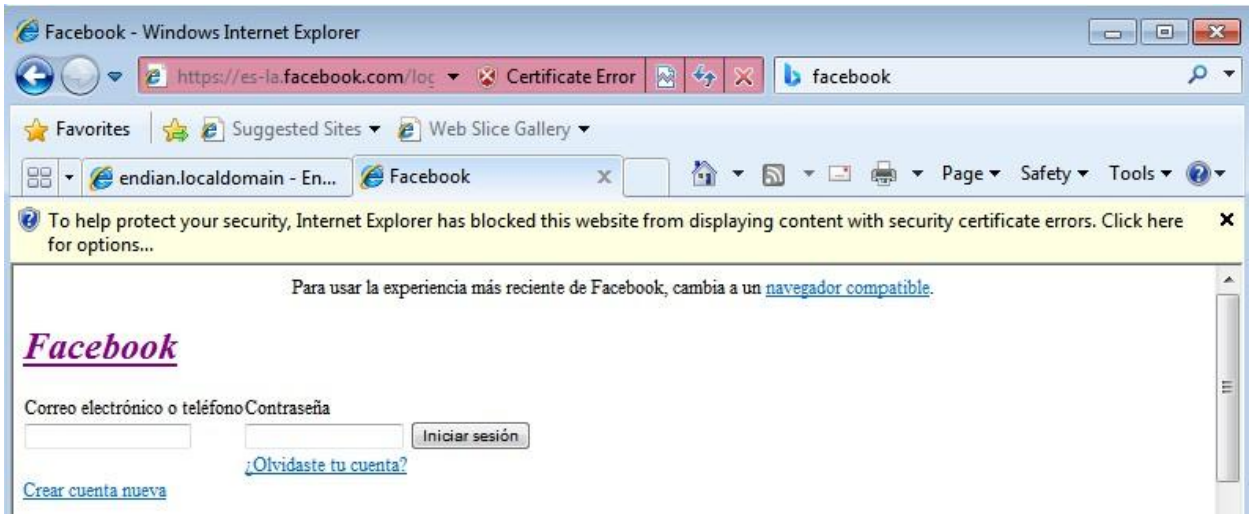
8. Control de Acceso a la Red (NAC)

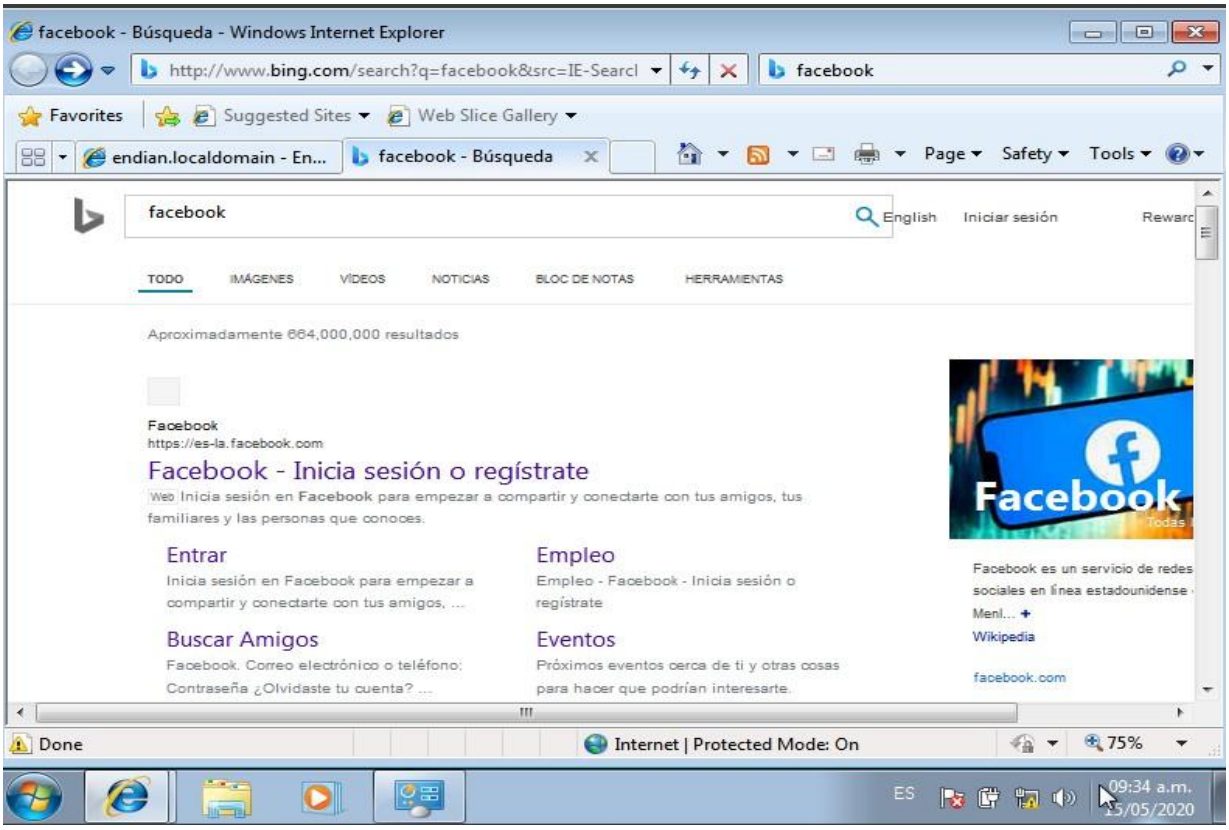
Autenticación y autorización: Ayuda a asegurar que solo dispositivos autorizados puedan conectarse a la red, reforzando la seguridad general de la infraestructura de TI.

9. Monitoreo y Reportes

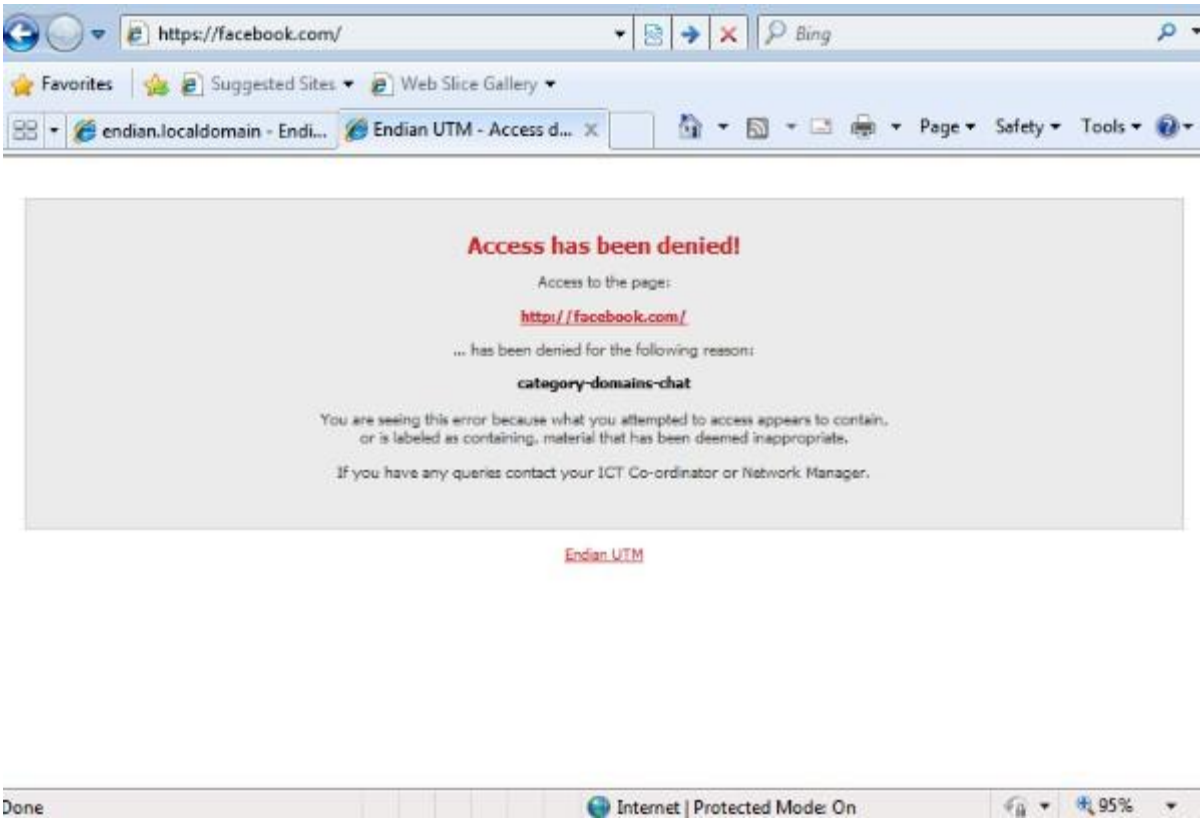
Visibilidad y control: Ofrece herramientas de monitoreo y generación de reportes que proporcionan una visión detallada del uso de la red y la actividad de seguridad, facilitando la gestión y la respuesta a incidentes.

Acceso a páginas como facebook.

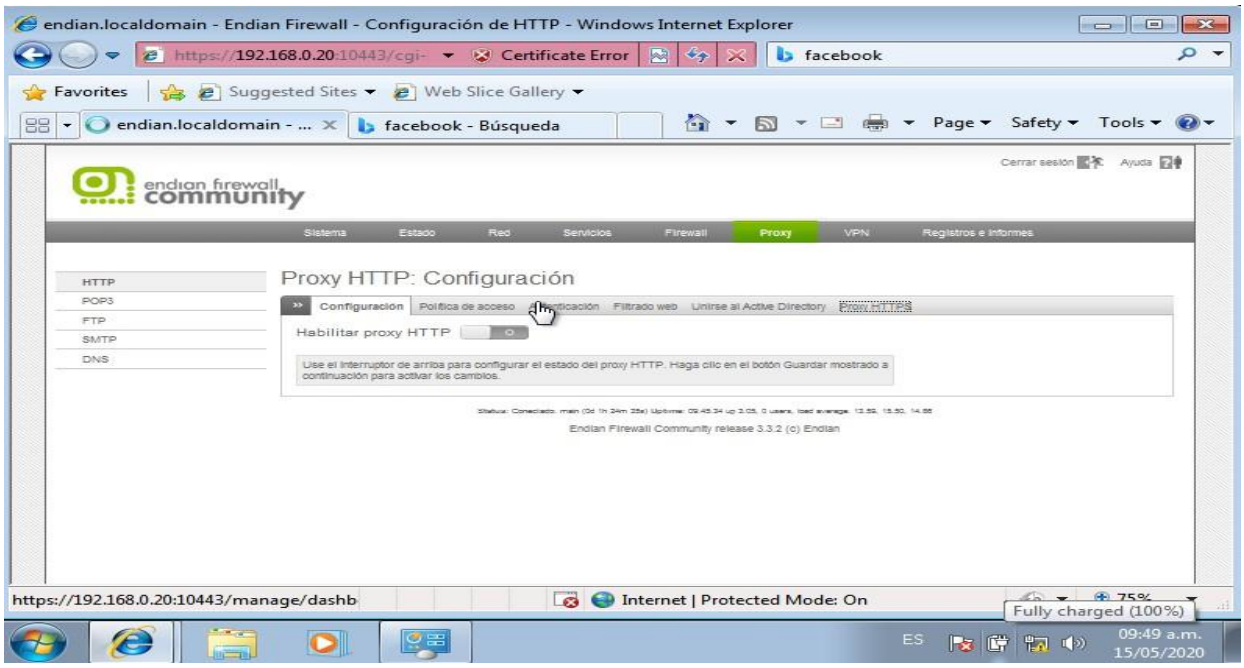




Denegación del acceso de diversas páginas como facebook.



En el apartado de ftp también podemos hacer un análisis de virus y para el control de tráfico web tenemos un proxy HTTP/HTTPS que ayuda a optimizar y controlar el tráfico web, de igual forma puede ser manualmente.



Certificados en Endian Community

En Endian Community Firewall, la funcionalidad del certificado de proxy es crucial para inspeccionar y filtrar el tráfico HTTPS de manera efectiva. Esto es especialmente importante porque HTTPS cifra los datos entre el navegador del usuario y los servidores web, lo que puede impedir que el firewall inspeccione el contenido de las transacciones por motivos de seguridad y cumplimiento. Aquí te explico cómo funciona el certificado de proxy en Endian Community:

1. Generación e Instalación del Certificado

Generación: Primero, Endian Community genera un certificado raíz de autoridad de certificación (CA) propio. Este certificado permite al firewall actuar como una CA intermedia, que puede emitir certificados para cualquier sitio web al que intenten acceder los usuarios dentro de la red.

Instalación en Clientes: Para que el proxy HTTPS funcione correctamente, el certificado raíz de Endian debe ser instalado en el almacén de certificados de confianza de cada cliente en la red (navegadores y sistemas operativos). Esto es crucial porque hace que los certificados emitidos "al vuelo" por el firewall sean aceptados automáticamente por los navegadores de los usuarios, evitando advertencias de seguridad.

2. Interceptación del Tráfico HTTPS

Cuando un usuario dentro de la red intenta acceder a un sitio HTTPS, el proxy de Endian intercepta la solicitud.

En lugar de permitir una conexión directa entre el navegador del usuario y el sitio web, el firewall se coloca en el medio, estableciendo una conexión segura (túnel SSL) con el servidor real en un lado, y una conexión segura separada entre el firewall y el navegador del usuario en el otro.

3. Emisión de Certificados "Al Vuelo"

Para cada conexión HTTPS, Endian genera dinámicamente un certificado para el sitio web destino que está firmado por su certificado raíz.

Dado que el certificado raíz de Endian está instalado y confiado en los navegadores de los usuarios, el certificado generado es aceptado como válido.

4. Inspección y Filtrado

Con ambas conexiones seguras (usuario-firewall y firewall-web) bajo su control, Endian puede inspeccionar el contenido cifrado que pasa a través del proxy.

Esto permite aplicar políticas de filtrado de contenido, bloquear malware, prevenir fugas de datos, y realizar otras funciones de seguridad sobre el tráfico HTTPS, que de otro modo estaría oculto.

5. Consideraciones de Seguridad

Mientras que interceptar y desencriptar HTTPS puede ser poderoso para la seguridad y la administración de la red, también plantea preocupaciones de privacidad y seguridad.

Es esencial que solo los administradores de sistemas confiables manejen la configuración del certificado y que los usuarios estén conscientes de estas prácticas para evitar abusos.

Implementar correctamente un proxy HTTPS con inspección SSL en Endian Community ayuda a las organizaciones a mantener un equilibrio entre seguridad y privacidad, garantizando que el tráfico de red no solo sea seguro sino también conforme a las políticas corporativas.