

FIREWALL PERIMETRAL CON ENDIAN EN ENTORNOS VIRTUALIZADOS

PEDRO JAVIER MOLINA AVILA

pjmolinaa@unadvirtual.edu.co

RESUMEN — Este artículo presenta la implementación de un firewall perimetral utilizando Endian Firewall Community 3.3.2 dentro de un entorno virtualizado en VirtualBox. El proyecto desarrolla la configuración integral de las zonas GREEN, ORANGE y RED, orientadas a la segmentación lógica de la red, la evaluación de riesgos, la aplicación de reglas de filtrado, el uso de NAT y la supervisión del tráfico. Se llevaron a cabo pruebas de conectividad entre segmentos internos y acceso controlado a Internet, validando el comportamiento esperado de cada zona y el aislamiento entre la LAN y la DMZ. Los resultados demuestran que Endian ofrece una solución robusta, estable y altamente funcional para escenarios educativos, de laboratorio y de formación en seguridad informática, permitiendo comprender de manera práctica los principios fundamentales de protección perimetral...

PALABRAS CLAVE — Endian Firewall, Seguridad perimetral, Virtualización, NAT, DMZ.

1 INTRODUCCIÓN

2 La seguridad perimetral se ha consolidado como un elemento indispensable en la protección de infraestructuras tecnológicas, especialmente en un contexto donde las amenazas digitales evolucionan con rapidez. Frente a esta realidad, los firewalls continúan desempeñando un rol central en la defensa de redes, al proporcionar mecanismos de segmentación, control y monitoreo del tráfico. Este proyecto desarrolla la instalación y configuración de Endian Firewall Community 3.3.2 en un entorno virtualizado mediante VirtualBox, con el fin de simular un sistema perimetral compuesto por múltiples zonas de red. A través de esta implementación, se examinan conceptos clave como la creación de zonas seguras, la administración de reglas de filtrado, el uso de NAT para comunicaciones reguladas y la validación del aislamiento entre segmentos internos y externos. La virtualización permite recrear condiciones reales de operación, facilitando la comprensión de arquitecturas perimetrales y fortaleciendo competencias en ciberseguridad y administración de redes.

3 DEFINICIÓN DEL PROBLEMA

Las organizaciones requieren proteger sus redes internas de amenazas externas y controlar el tráfico entre LAN, DMZ y WAN. Muchas empresas carecen de herramientas accesibles o conocimientos para implementar firewalls profesionales, por lo que surge la necesidad de diseñar una solución libre, robusta y funcional.

4 JUSTIFICACIÓN

Implementar un firewall perimetral permite controlar accesos, proteger la red interna, aislar la DMZ, monitorear tráfico y aplicar políticas sin licencias

costosas. Endian es gratuito, intuitivo y posee herramientas integradas como IDS, VPN y proxy.

5 OBJETIVOS

5.1 Objetivo general

Implementar un firewall perimetral basado en GNU/Linux Endian dentro de un entorno virtualizado, estableciendo y configuración las zonas LAN, DMZ y WAN para garantizar la segmentación adecuada de la red, el control del tráfico y la protección integral de los servicios internos frente a accesos no autorizados

Objetivos específicos

- Configuración Endian Firewall con tres interfaces de red.
- Implementar las zonas GREEN, ORANGE y RED.
- Verificar conectividad interna y hacia Internet.
- Configuración reglas NAT para tráfico saliente.
- Analizar resultados mediante el dashboard de Endian.

6 MARCO REFERENCIAL

6.1 Marco teórico

Un firewall filtra tráfico según reglas definidas. La

seguridad perimetral protege el borde de la red. La DMZ alberga servicios expuestos. NAT permite que redes privadas accedan a Internet con una IP pública. Endian Firewall es una distribución enfocada en facilitar estas tareas.

6.2 Estado del arte

Soluciones como pfSense, OPNsense e IPFire ofrecen alternativas de firewall libre. Endian destaca por su simplicidad, herramientas integradas y facilidad para ambientes educativos.

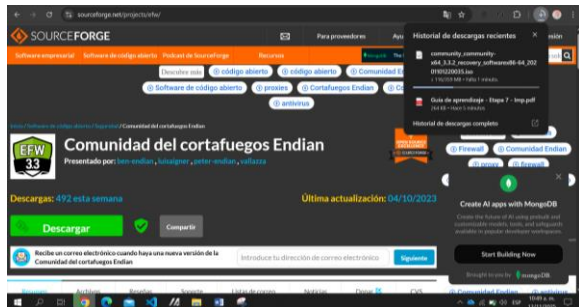
7 METODOLOGÍA

La metodología empleada fue experimental, configurando VirtualBox, instalando Endian, asignando zonas de red y realizando pruebas de conectividad y NAT.

8 DESARROLLO, ANÁLISIS Y RESULTADOS

Se instalaron tres interfaces de red para GREEN, ORANGE y RED. Las pruebas confirmaron conectividad correcta entre zonas y acceso a Internet mediante NAT. Las interfaces mostraron actividad en tiempo real en el dashboard de Endian.

Ilustración 1. Imagen donde se evidencia la descarga de la ISO de Endian



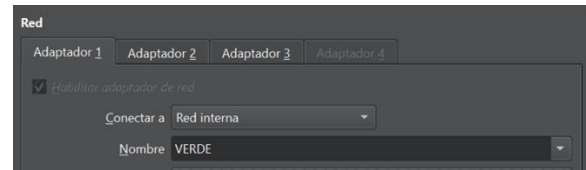
Fuente: Autoría propia

Para la instalación de Endian en virtualBox

- Tipo: Linux
- Versión: Other Linux (64-bit)
- Cambiamos chipset de ICH9 a PIIX3
- Configuramos procesador y asignados 2 CPUs
- Activamos PAE/NX

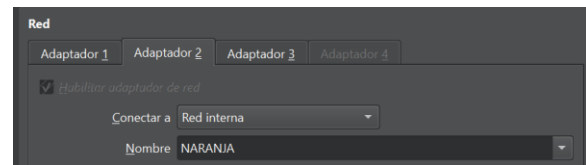
- Asignamos memoria de 1024 MB
- Habilitamos tres adaptadores para las zonas VERDE, NARANJA Y ROA

Ilustración 2. Imagen donde se evidencia que se habilitan el adaptador 1



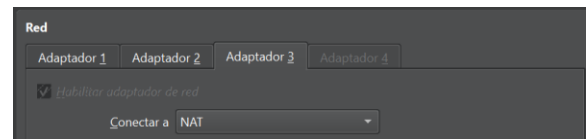
Fuente: Autoría propia

Ilustración 3. Imagen donde se evidencia que se habilita el adaptador 2



Fuente: Autoría propia

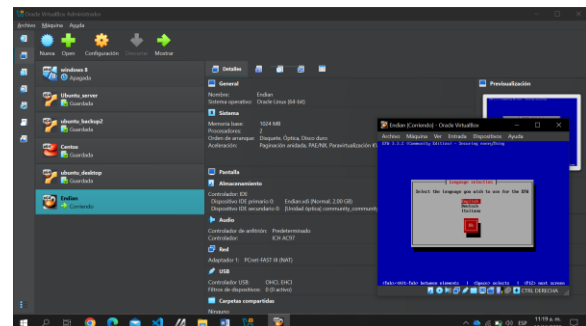
Ilustración 4. Imagen donde se evidencia que se habilita el adaptador 3



Fuente: Autoría propia

Procedemos a instalar Endian
Seleccionamos idioma

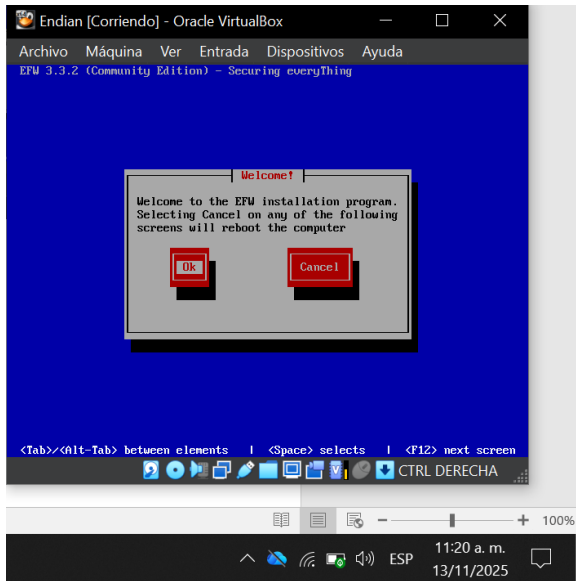
Ilustración 5. Inicio de instalación de Endian



Fuente: Autoría propia

Luego vemos la pantalla de bienvenida del instalador

Ilustración 6. inicio de instalación



Fuente: Autoría propia

Luego nos pregunta que si deseamos continuar que todos los datos en el disco /dev/sda serán borrados.

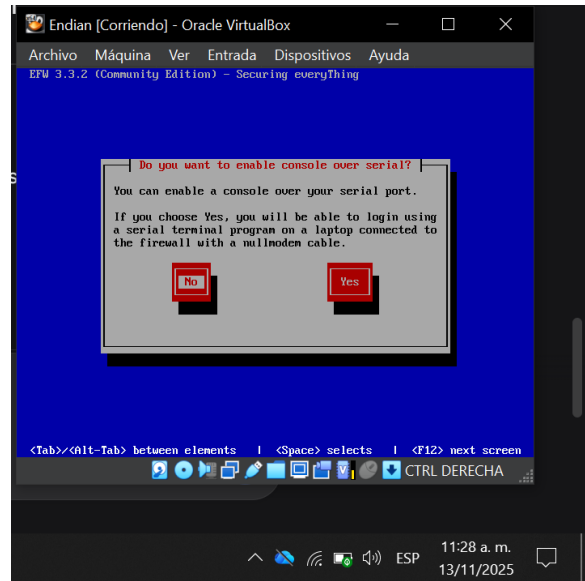
Ilustración 7. Mensaje de bienvenida del instalador



Fuente: Autoría propia

Luego nos pregunta si queremos habilitar consola por puerto serial, para ese caso no es necesario

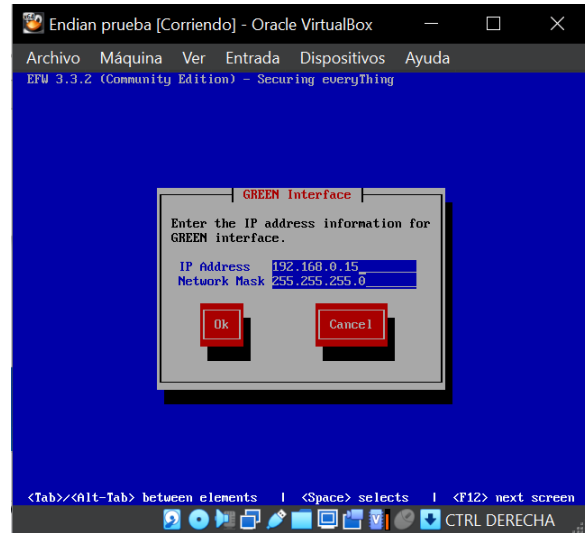
Ilustración 8. imagen de instalación de Endian



Fuente: Autoría propia

Ahora hacemos la configuración GREEN, esta representa nuestra red interna/confiable (LAN)

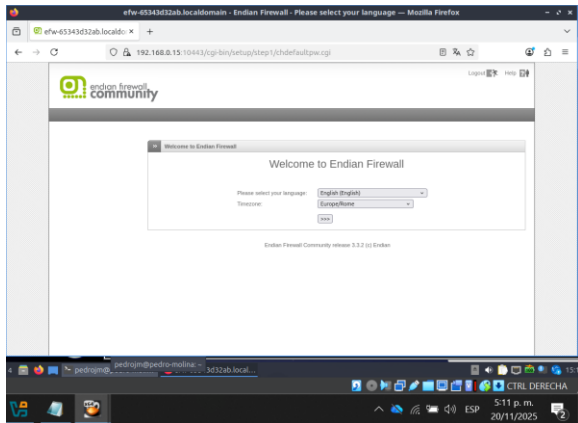
Ilustración 9. Asignación de IP



Fuente: Autoría propia

Luego nos sale el mensaje que la instalación se ha completado

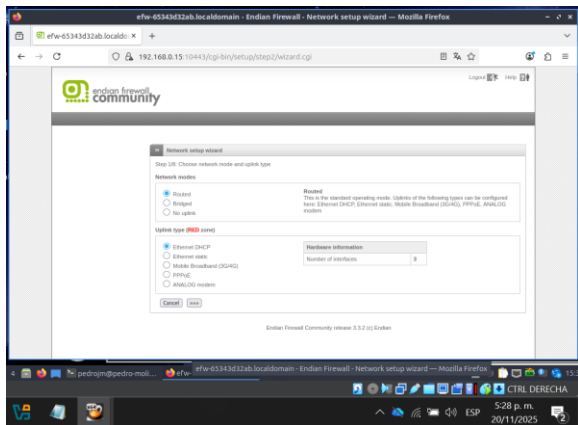
Ilustración 14. Setup Wizard



Fuente: Autoría propia

Luego Network setup wizard - Step 1/8 del asistente de configuración de red ZONA ROJA donde identifica nuestras tres interfaces

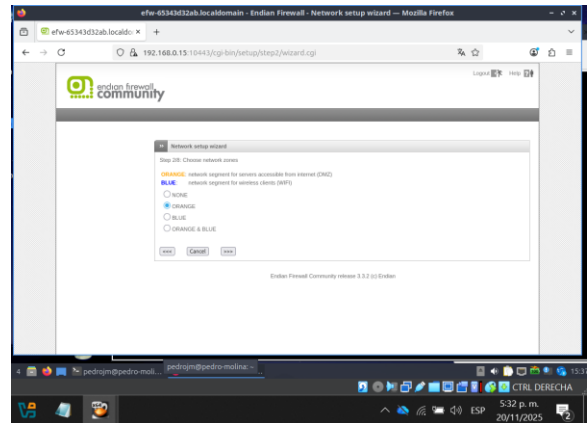
Ilustración 15. Configuración ZONA ROJA



Fuente: Autoría propia

Luego Network setup wizard - Step 2/8 del asistente de configuración de red NARANJA

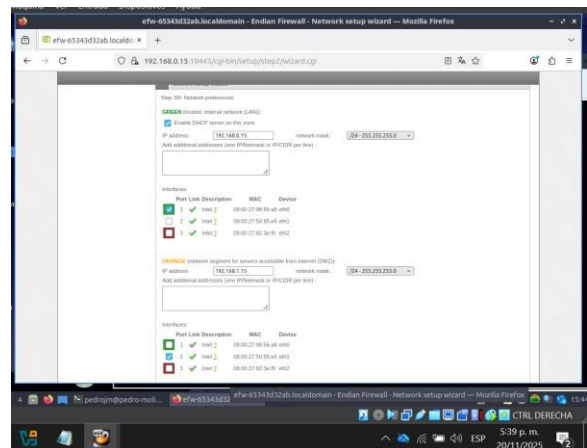
Ilustración 16. Configuración ZONA NARANJA



Fuente: Autoría propia

En el Step 3/8 del sistema de Endian Firewall, se configuran las interfaces GREEN (LAN INTERNA) Y (ORANGE DMZ) donde se asignan las IPs 192.168.0.15/24 a GREEN para gestionar la red interna, y 192.168.1.15/24 a ORANGE para aislar servicios expuestos.

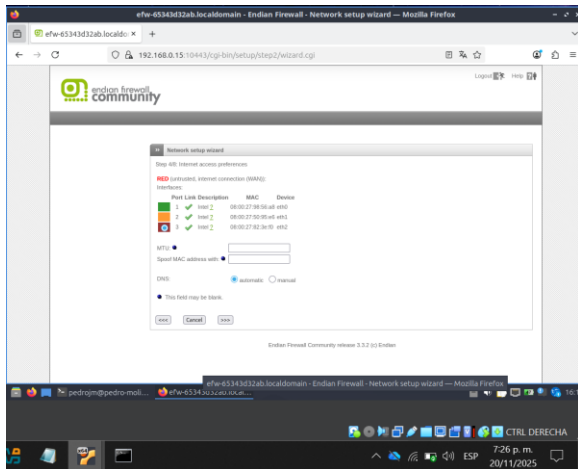
Ilustración 17. Asignación IP ZONA VERDE Y ZONA NARANJA



Fuente: Autoría propia

En el Step 4/8 se configuro la interfaz RED (internet) de Endian Firewall. En los campos MTU y Spoof MAC se deja en blanco para usar valores automáticos ya que la conexión utiliza DHCP. El DNS no se modificó, permitiendo que el firewall obtuviera los servidores del proveedor.

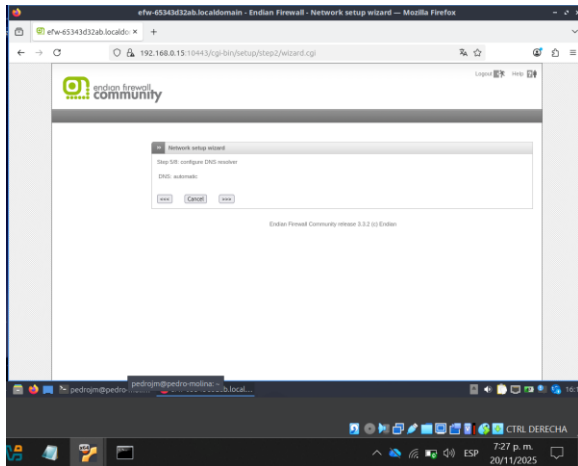
Ilustración 18. se configuro la interfaz RED (internet)



Fuente: Autoría propia

En el Step 5/8, se configuró el resolvidor DNS de Endian Firewall en modo automático. Esto permite que el firewall obtenga los servidores DNS del proveedor de Internet, garantizando la resolución de nombres para la red interna.

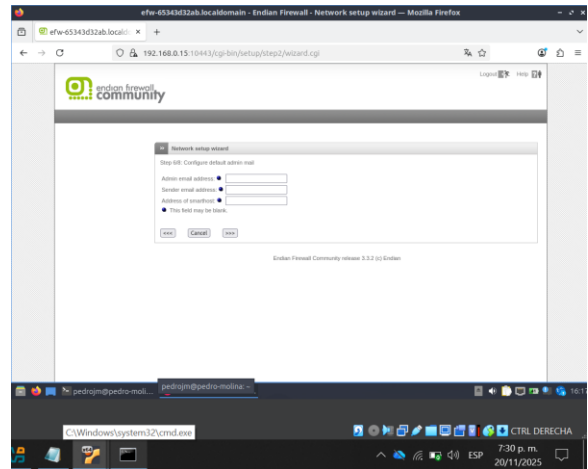
Ilustración 19. Step 5/8



Fuente: Autoría propia

En el Step 6/8 se dejó en blanco permitiendo que el firewall gestione el envío de correos de forma local

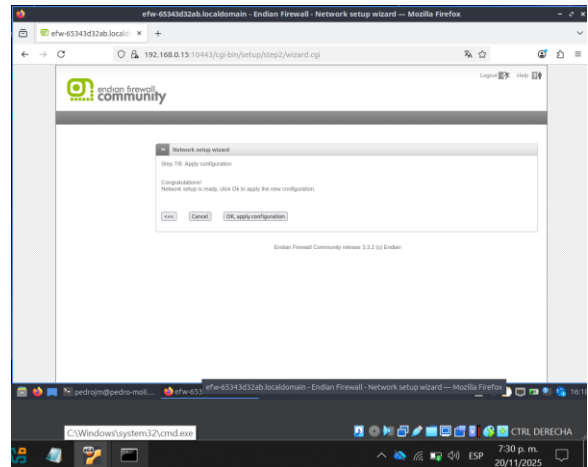
Ilustración 20. Step 6/8



Fuente: Autoría propia

En el Step 7/8 se aplicó la configuración final de Endian Firewall. Al hacer clic en 'OK', el sistema cargó las reglas de firewall, reinició los servicios críticos y quedó operativo. Esta etapa es esencial para validar que todos los parámetros (redes, DNS, correo) funcionan en conjunto.

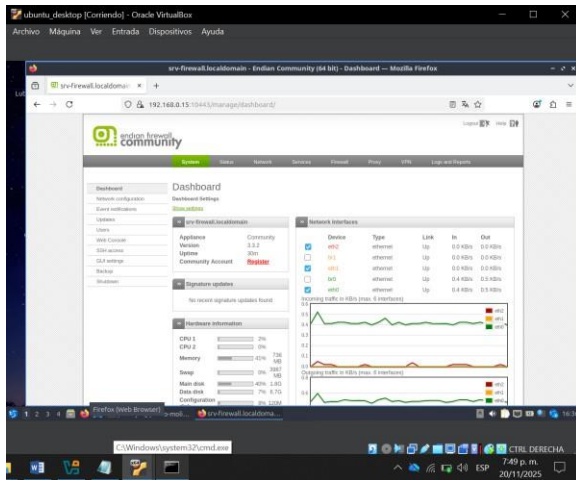
Ilustración 21. En el Step 7/8 se aplicó la configuración final de Endian Firewall.



Fuente: Autoría propia

Tras completar la instalación, se accedió al dashboard de Endian Firewall Community. En la siguiente imagen podemos observar las tres interfaces activas con tráfico en tiempo real confirmando la operación de las zonas GREEN, ORANGE Y RED.

Ilustración 22. dashboard de Endian Firewall Community.

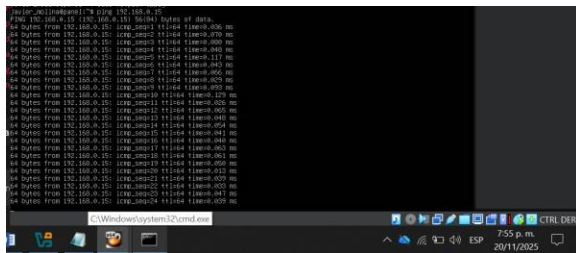


Fuente: Autoría propia

Comprobar que funciona

Se verifico la conectividad básica desde Ubuntu server a la ZONA VERDE usando ping, donde da como resultado 100% de paquetes respondidos con latencia baja.

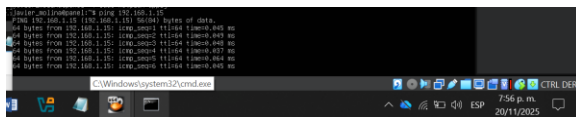
Ilustración 23. Prueba 1



Fuente: Autoría propia

Se verifico la conectividad básica desde Ubuntu server a la ZONA NARANJA usando ping, donde da como resultado 100% de paquetes respondidos con latencia baja.

Ilustración 24. Prueba 2



Fuente: Autoría propia

9 DISCUSIÓN

La implementación demuestra que Endian constituye una alternativa accesible y efectiva para la administración de seguridad perimetral. La segmentación de red y NAT garantizaron aislamiento adecuado entre zonas internas y

la DMZ.

10 CONCLUSIONES

- La implementación de Endian Firewall en un entorno virtualizado demostró ser una solución eficiente y accesible para comprender la seguridad perimetral y la segmentación de redes mediante zonas GREEN, ORANGE y RED
- La configuración de reglas de filtrado y NAT confirmó la teoría de que un firewall perimetral regula eficazmente la comunicación entre redes privadas y externas, facilitando un acceso seguro a Internet.
- La organización de la red mediante una DMZ evidenció el cumplimiento del concepto teórico de exposición controlada de servicios, manteniendo protegida la LAN interna.
- Los resultados de conectividad demostraron que la arquitectura implementada cumple con la función fundamental de un firewall: permitir tráfico legítimo y bloquear el no autorizado, tal como lo plantean los modelos de seguridad de red
- La virtualización en VirtualBox validó la teoría de que estos entornos permiten replicar escenarios reales de infraestructura, facilitando el aprendizaje práctico de administración y seguridad de redes.
- El uso del dashboard de Endian confirmó la importancia del monitoreo en tiempo real para la gestión de la seguridad, coherente con los lineamientos de defensa perimetral y detección temprana de incidentes.
- La instalación y configuración del firewall evidenció que las soluciones libres como Endian son alternativas robustas para entornos educativos, cumpliendo con el objetivo de implementar herramientas accesibles sin comprometer la funcionalidad.

11 REFERENCIAS

- [1] Endian. (2024). Endian Firewall Documentation. <https://www.endian.com>
- [2] Oracle Corporation. (2024). VirtualBox user manual. <https://www.virtualbox.org>
- [3] Tanenbaum, A. S., & Wetherall, D. (2011). Computer networks (5th ed.). Pearson.
- [4] Linux Professional Institute. (2020). Linux essentials certificate: Learning materials. <https://www.lpi.org>
- [5] Stallings, W. (2018). Network security essentials: Applications and standards (6th ed.). Pearson.
- [6] OPNsense Project. (2024). OPNsense documentation. <https://docs.opnsense.org>
- [7] PfSense. (2023). PfSense official documentation. <https://www.pfsense.org>