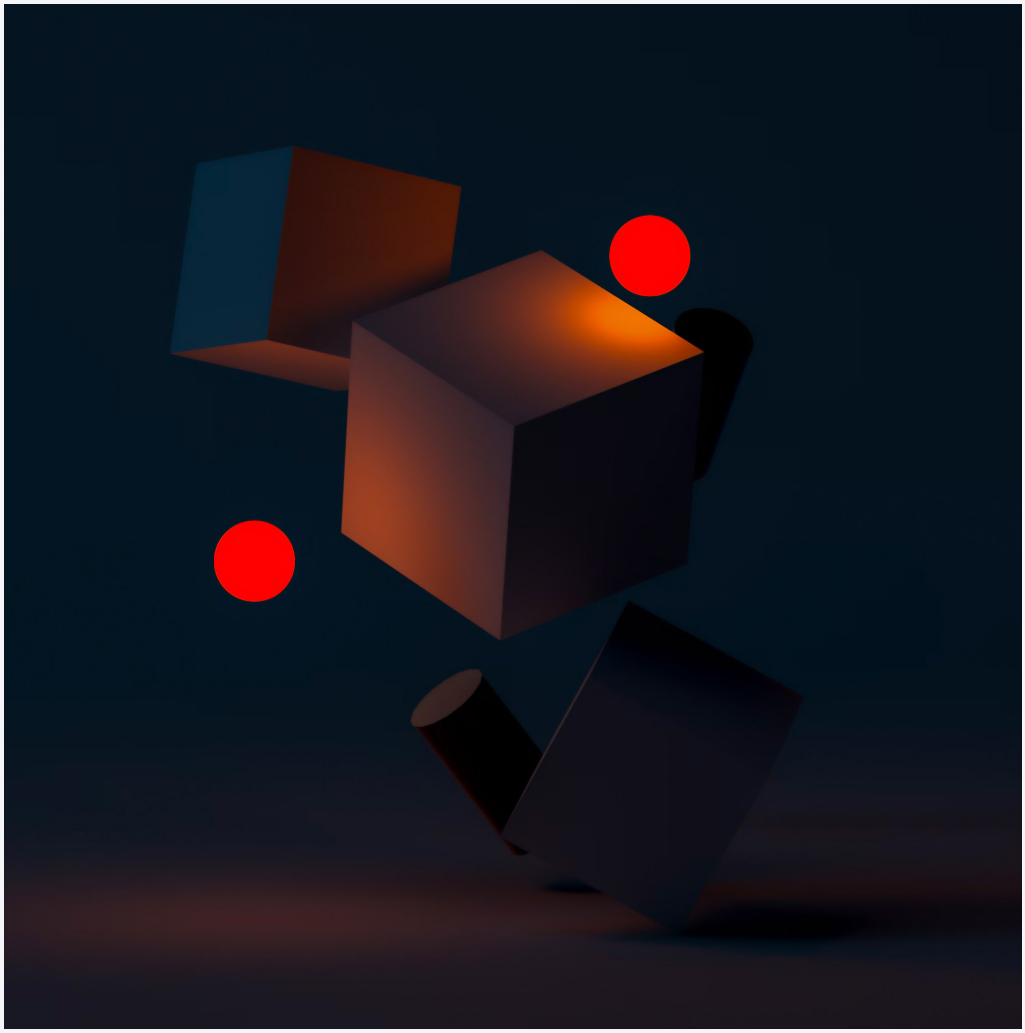

WARRIORS DEFENDER
IDS/IPS
Warriors®
"Security that makes difference"

La solución de Warriors Defender IDS/IPS, permite crear puntos de control y monitoreo de las amenazas de la red,

gracias a su capacidad de operar en su modalidad in-line (IPS/IDS) y en mirror port (IDS), realizando una inspección (deep packet inspection) a detalle de los paquetes de la red. WDIPS implementa firmas capaces de identificar diferentes metodologías y vectores de ataques, así como analisis de protocolos y analisis de fingerprint para el bloqueo de amenazas.



WDIPS permite ser una solución para integrarse con otras herramientas de seguridad perimetral como Firewall, WDIPS inspeccionara el tráfico de la red sin que sea intrusivo para la red o existan problemas de performance. Gracias a su flexibilidad de implementación en diferentes escenarios.

INFO@WARRIORSLABS.COM
WWW.WARRIORSLABS.COM

WDIPS cuenta con un motor de inspección robusto de alto rendimiento en combinación con las mejores firmas de su clase, gracias a la asociación con socios tecnologicos proporcionando a los clientes una tasa de deteccion de amenazas alta y eficiente.

El motor de WDIPS tiene una tasa de bloqueo de hasta un 99% de amenazas, combinando diferentes tecnicas de análisis como:

ANÁLISIS DE PROTOCOLO
REPUTACIÓN DE AMENAZAS
BLOQUEO POR CONTENIDO

y otras funcionalidades que ofrecen protección en diferentes capas, incluyendo detección de ataques ARP, DoS/DdoS, anomalía de protocolos, URL's maliciosas, malware, entro otros.

WDIPS proporciona una visibilidad completa, generando reportes para tomar desiciones de bloqueo adecuadas debido a su analisis de información de forma granular, ofrece vistas de:

TRÁFICO
AMENAZAS DE LA RED
RIESGOS DE SEGURIDAD
FILTROS POR IP ORIGEN
IP DESTINO
PROTOCOLOS
PUESTOS
SEVERIDAD

entre otros con el fin de ayudar a entender claramente los riesgos y tomar las desciciones correctas.

FACILIDAD DE IMPLEMENTACIÓN Y ADMINISTRACIÓN

El despliegue y administración del WDIPS es simple, ya que permite satisfacer los requisitos de seguridad y garantizar la optima conectividad:

- *Protección activa (Modo IPS). Bloqueo de amenaza en tiempo real*
- *Protección pasiva (Modo IDS). Detección y Alertas de amenazas en tiempo real.*

KEY FEATURES

- *10000+ firmas de detección de exploits y amenazas*
- *Modos funcionamiento: IDS (Monitor), IPS (Block), Allow (Rules exception)*
- *Exclusiones de firmas*
- *IDS Mirror Port*
- *Bypass – Modo Bridge. Permite detener el motor de inspección sin realizar cambios fisicos.*
- *Web Server Protection. CC Attack, cros-site request forgery attack, file scanning attack, etc.*
- *Correlación de eventos como: Amenazas, severidad, IP's, puertos, entre otros.*
- *Detección de más de 2000 malwares, incluyendo Virus, Gusanos, Troyanos, Spyware, etc.*
- *Admite la inspección del tráfico de túnel cifrado para aplicaciones desconocidas*
- *Anti Dos, DdoS*
- *ARP Defense*
- *Anti-Escaneo de hosts y puertos*
- *Inspección de trafico web*
- *Reglas personalizadas para filtrado web*
- *Posibildad de generar grupos para aplicar las reglas personalizadas*
- *Categorias precargadas para protección en tiempo real*
- *Protección contra hosts de botnets*
- *Actualización de base de datos de botnet*
- *Prevención de Hosts C&C por IP o Dominio*
- *Reputación de IP. Identifica el tráfico proveniente de IP que pueden asociarse a algun riesgo como: botnet hosts, spammers, Tor nodes, ataque de fuerza bruta*
- *Actualización de base de datos de IP's con mala reputación*

LOGS AND REPORTS:

- *Local Storage puede almacenar hasta 6 meses, con fines de auditoria*
- *Los logs almacenan información del sistema y también actividad relacionada con los eventos de seguridad y alertas.*
- *Es posible mover los logs a servicios de External Logs Storage*
- *Reportes generados en tiempo casi real*
- *Reportes que permiten ir de General a Reportes Granulares a través de filtros*
- *Reportes generados en rangos de tiempo*
- *Visualización del origen de los ataques en base a GeoIP*

ADMINISTRATION:

- *Administración a través de HTTPS, SSH, Console.*
- *Backup and Restore*
- *Monitoreo de Infraestructura (CPU, Memoria, Disco, Trafico de interfaces)*
- *Integración de Herramienta centralizada de Monitoreo. A través de un agente los Logs son enviado a una herramienta externa de mayor capacidad de almacenamiento la cual permite resguardar los datos y centralizar la información de uno o más sensores (WDIPS/WDIDS).*
- *High Availability:*
    - *+ HA Link Aggregation*
    - *+ Geographical HA*
    - *+ Cluster Multiples equipos*


Warriors®
"Security that makes difference"