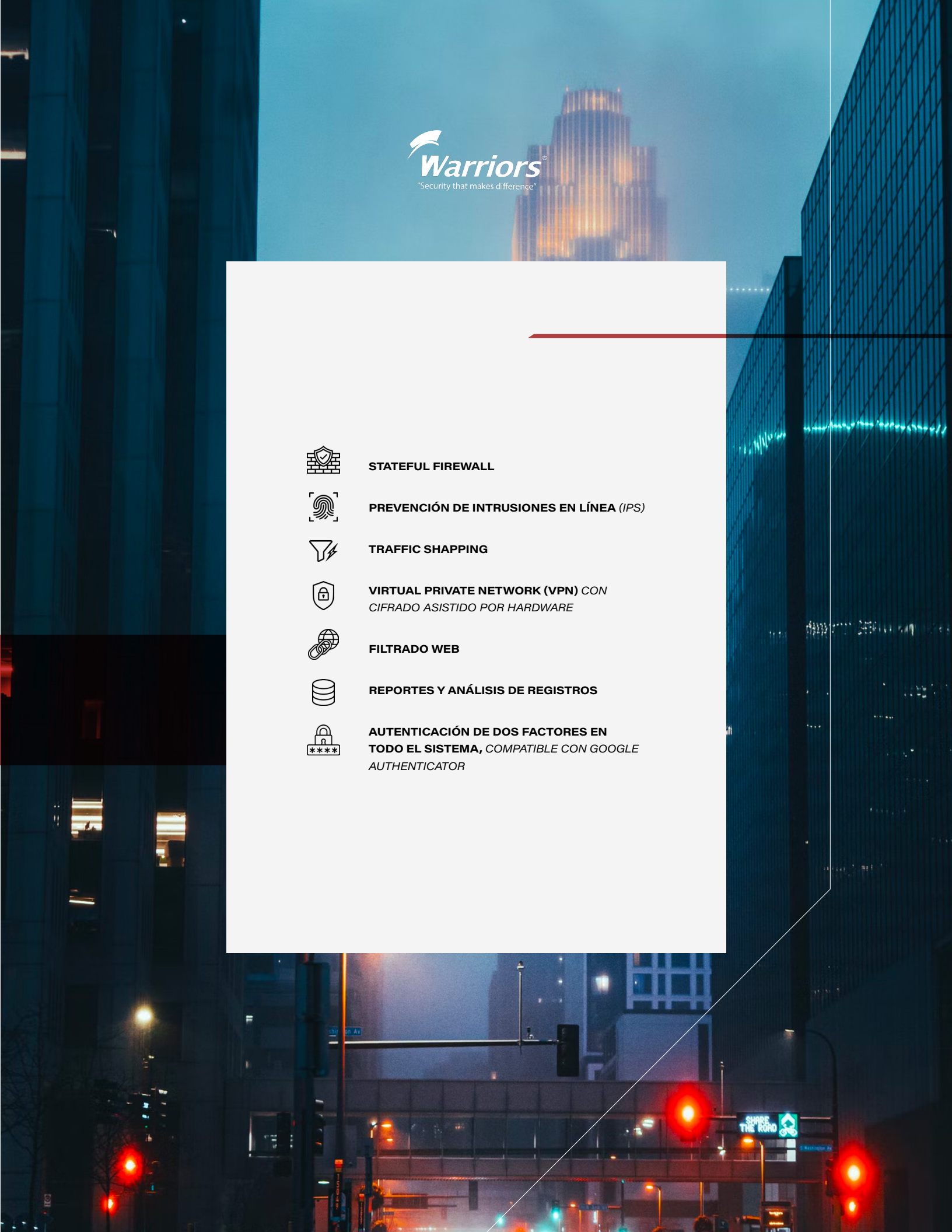

WARRIORS DEFENDER
NEW GENERATION
Warriors®
"Security that makes difference"

WARRIORS DEFENDER NEW GENERATION

Warriors Defender® New Generation *«WDNG»* es una plataforma de seguridad con todas las funciones que mantiene segura su red con características de gama alta como el sistema de prevención de intrusiones, red privada virtual, autenticación de dos factores, portal cautivo, filtrado de contenido, entre otras.

La configuración opcional de alta disponibilidad garantiza un rendimiento estable de la red con conmutación por error automática y estados sincronizados, minimizando las interrupciones. Mantenga su red segura y disponible en todo momento.



- **STATEFUL FIREWALL**
- **PREVENCIÓN DE INTRUSIONES EN LÍNEA** *(IPS)*
- **TRAFFIC SHAPPING**
- **VIRTUAL PRIVATE NETWORK (VPN)** *CON CIFRADO ASISTIDO POR HARDWARE*
- **FILTRADO WEB**
- **REPORTES Y ANÁLISIS DE REGISTROS**
- **AUTENTICACIÓN DE DOS FACTORES EN TODO EL SISTEMA,** *COMPATIBLE CON GOOGLE AUTHENTICATOR*

WWW.WARRIORSLABS.COM
INFO@WARRIORSLABS.COM

PROTEGER SU RED

NUNCA HA SIDO TAN FÁCIL

Proteger su red nunca ha sido tan fácil, utilice la prevención de intrusiones integrada, capaz de crear listas negras basadas en huellas dactilares SSL y la autenticación de dos factores para conectar de forma segura a los usuarios móviles. Mantenga una visión completa del tráfico que fluye a través de su red en todo momento, con sus avanzadas herramientas de captura, análisis, detección y elaboración de informes.

EMPRESAS

Proteja su red empresarial con una solución con múltiples herramientas de protección como: • Firewall • Filtrado Web • Sistema de detección y prevención de intrusiones • Cloud Threat Protection.

INSTITUCIONES EDUCATIVAS

Limite el ancho de banda y distribuya de forma uniforme entre los estudiantes, y utilice el filtrado de contenido para restringir el acceso al contenido no deseado (contenido para adultos y sitios maliciosos).

SERVICIOS AL CLIENTE

Lugares como Cafeterías, Agencias, Hoteles y otros suelen utilizar un portal cautivo para permitir a los clientes el acceso a internet durante un tiempo limitado. Los clientes deben iniciar sesión con un usuario y contraseña o utilizando un código del ticket de compra.

OFICINA REMOTA O HOME OFFICE

Utilice VPN's sitio a sitio para integrar y conectar todas sus sedes en una red segura, o si lo desea utilice VPN's con clientes remotos para aquellos usuarios que trabajan desde sus hogares y puedan acceder a los recursos de la compañía a través de un medio seguro.

STATEFUL INSPECTION FIREWALL

Es un firewall que hace un seguimiento del estado de las conexiones de red (como flujos TCP, comunicación UDP) que viajan a través de él. El firewall está programado para distinguir los paquetes legítimos de los diferentes tipos de conexiones. Sólo los paquetes que coincidan con una conexión activa conocida serán permitidos por el firewall; los demás serán rechazados.

FILTRADO
El firewall puede filtrar el tráfico basado en: origen, destino, protocolo o puertos específicos.

SISTEMA OPERATIVO
La tecnología avanzada de detección del sistema operativo puede utilizarse para permitir o bloquear el tráfico en función del sistema operativo que inicia la conexión.

REGISTRO DE TRÁFICO BASADO EN REGLAS
Cada regla se puede configurar para que genere registros con el fin de poder identificar los orígenes y destinos de conexión, con lo cual se podrá realizar un análisis y permita toma de decisiones más precisas.

POLÍTICAS DE RUTEO Y GATEWAY POR REGLAS
Con el enrutamiento basado en políticas es posible añadir una puerta de enlace a una regla con lo cual se podrá cambiar el enrutamiento para el tráfico seleccionado.

SOPORTE DE ALIAS PARA AGRUPAR: IPS, REDES Y PUERTOS
Los alias ayudan a mantener el conjunto de reglas del firewall ordenadas y fácil de entender, en entornos con múltiples IP públicas y numerosos servidores.

ORGANIZACIÓN DE REGLAS
Además de la agrupación de interfaces, en la que las reglas se gestionan para varias interfaces a la vez, las reglas del firewall también pueden organizarse por categorías para agrupar reglas que, de otro modo, no tendrían relación aparente entre sí.

FIREWALL TRANSPARENTE (CAPA 2)
Interfaces de puente y tráfico de filtro entre ellos, incluso permitiendo un firewall sin IP.

CONTROL GRANULAR DE LA TABLA DE ESTADOS
Capacidad de limitar el tráfico por regla en función de las conexiones simultáneas, los estados por host y las nuevas conexiones por segundo, así como de definir el tiempo de espera de los estados y el tipo de estado.

ENRUTAMIENTO PURO
Desactive el filtrado de paquetes para convertir el sistema en un router puro.

OPTIMIZACIÓN DEL TRÁFICO DE RED

El traffic shapping es el control del tráfico de la red para optimizar o garantizar el rendimiento, reducir la latencia y/o aumentar el ancho de banda utilizable retrasando los paquetes que cumplen determinados criterios

FÁCIL Y FLEXIBLE

La optimización del tráfico con WDNG es muy flexible, ya que genera agrupaciones de acuerdo con el tipo de tráfico. A cada grupo se le define el ancho de banda permitido, así como una prioridad. Las reglas de optimización son administradas de manera independiente a las reglas de firewall u otros ajustes.

LIMITACIONES DE ANCHO DE BANDA

Las limitaciones de ancho de Banda pueden definirse en función de las interfaces, ip origen – destino, dirección del tráfico (entrada o salida) y basado en puertos (aplicaciones).

BALANCEO DE CARGA

El ancho de banda es distribuido de manera uniforme entre todos los usuarios, esto permite un uso optimo de los recursos en todo momento, incluso utilizando más de un enlace a Internet para mejorar la experiencia del usuario.

ADMINISTRACIÓN DE PRIORIDADES

El tráfico puede priorizarse añadiendo listas de espera y definiendo su importancia. Las aplicaciones con mayor importancia pueden consumir más ancho de banda que otras cuando el ancho de banda total disponible es limitado.

PORTAL CAUTIVO

El Portal Cautivo le permite forzar la autenticación, o la re-dirección a una página para el acceso a la red. Esto se utiliza comúnmente en las redes de puntos de acceso para clientes, pero también se utiliza ampliamente en las redes corporativas para proporcionar una capa adicional de seguridad para el acceso inalámbrico a Internet.

RED DE INVITADOS — ACCESO WIFI PARA CLIENTES — DISPOSITIVOS NO CORPORATIVOS

BYOD (bring your own device)

PERSONALICE SU PÁGINA DE ACCESO

WDNG le ofrece un gestor de plantillas con lo cual podrá configurar su propia página de acceso. Al mismo tiempo ofrece funcionalidades adicionales como:
·Re-dirección de URL
·Pagina de inicio de sesión personalizada

ADMINISTRADOR DE ZONAS

Se pueden configurar diferentes zonas en cada interfaz o varias interfaces pueden compartir una configuración de zona. Cada zona puede utilizar una plantilla de portal cautivo diferente o compartirla con otra zona.

ADMINISTRACIÓN MEDIANTE TICKETS

El Portal Cautivo cuenta con un sistema de creación de tickets, la cual los exporta a un archivo csv para utilizarlo con su aplicación favorita. La exportación le permite imprimir los comprobantes crear un folleto de buen aspecto con su logotipo y estilo de empresa.

ADMINISTRACIÓN DE ANCHO DE BANDA

El optimizador de tráfico de red puede ser utilizado para:
·Balancear el ancho de banda y evitar un uso excesivo
·Dar prioridad a protocolos o a hosts en especifico.

AUTENTICACIÓN

Autenticación segura a través de HTTPS o portal de sólo splash con re-dirección de URL a una página determinada. Se pueden utilizar diferentes fuentes para autenticar a un usuario en una zona:
·LDAP [Microsoft Active Directory]
·Radius
·Gestor de usuarios local
·Vales / Tickets
·Contraseña de un solo factor (2FA)
·Sin autenticación (sólo pantalla de inicio)
·Múltiple (una combinación de lo anterior)

PERIODOS DE TIEMPO

La conexión puede terminar después de que el usuario haya estado inactivo durante un cierto tiempo (tiempo de espera inactivo) y/o forzar una desconexión cuando haya pasado un número de minutos, aunque el usuario siga activo la sesión (tiempo límite). En caso de que un usuario se vuelva a conectar dentro del tiempo de espera y/o del tiempo de inactividad, no es necesario iniciar sesión y el usuario puede reanudar su sesión activa.

PORTAL BYPASS

Direcciones MAC o direcciones IP pueden ser colocadas en listas blancas para realizar un bypass al portal cautivo.

INFO@WARRIORSLABS.COM
WWW.WARRIORSLABS.COM

TWO-FACTOR AUTHENTICATION

Autenticación de dos Factores también conocida como 2FA o verificación en dos pasos, es un método de autenticación que requiere de dos componentes, una contraseña + un token. La autenticación de verificación en dos pasos está disponible para el sistema completo.

CONTRASEÑA DE UN SOLO USO

TOTP es un algoritmo (RFC 6238) que calcula una contraseña de un solo uso a partir de una clave compartida y hora actual.

GOOGLE AUTHENTICATOR

WDNG soporta el uso de la aplicación Google Authenticator, esta aplicación permite generar tokens en diversos dispositivos como: Android, iOS, Blackberry. El uso de esta aplicación es totalmente gratuito.

SERVICIOS COMPATIBLES CON 2FA

- *Acceso al sistema WDNG*
- *Portal Cautivo*
- *Redes Virtuales Privadas (VPN)*
- *Filtrado de contenido*

FÁCIL CONFIGURACIÓN

Configurar la autenticación de dos factores es fácil utilizando la aplicación Google Authenticator

- *Integrado en el sistema de autenticación unificado de WDNG*
- *Generación automática de claves*
- *Activación de Tokens por código de barras*

REDES PRIVADAS VIRTUALES (VPN)

Una red privada virtual (VPN) extiende una red privada a través de una red pública, como Internet. Permite que un ordenador envíe y reciba datos a través de redes compartidas o públicas como si estuviera directamente conectado a la red privada, al tiempo que se beneficia de la funcionalidad, la seguridad y las políticas de gestión de la red privada.

TECNOLOGÍAS VPN SOPORTADAS

WDNG ofrece un amplio rango de tecnologías VPN desde las más modernas y seguras VPN SSL o VPN full mesh, VPN IPSec, así como las opciones más antiguas (ahora consideradas inseguras) como LTP y PPTP

SSL VPN

Una potente solución SSL VPN compatible con una amplia gama de sistemas operativos de clientes, incluidos los móviles (Android / IOS).

IPSEC

IPSec permite conectividad con cualquier dispositivo que soporte el estándar IPsec. Esto se utiliza más comúnmente para la conectividad de sitio a sitio y compatible con la mayoría de las soluciones de firewall comerciales. También se puede utilizar para la conectividad de clientes móviles.

FULL MESH VPN

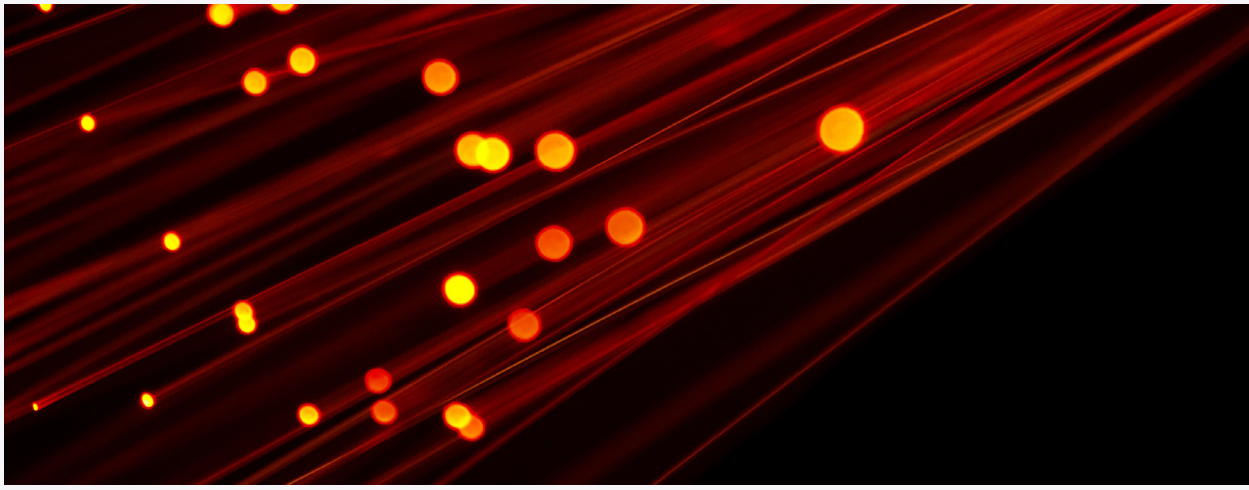
Una solución VPN que puede utilizarse para construir una pseudo-VLAN segura y cifrada a través de la Internet pública.

OLD VERSIONS

WDNG tiene soporte para L2TP y PPTP, solo en caso de requerirse.

HIGH AVAILABILITY / HARDWARE FAILOVER

El Protocolo de Redundancia de Direcciones Común o CARP permite la conmutación por error de hardware. Se pueden configurar dos o más dispositivos Warriors Defender New Generation (WDNG) en un grupo de conmutación por error. Si una interfaz falla en el primario o el primario se desconecta por completo, el secundario pasa a estar activo de forma instantánea.



WDNG utiliza el Protocolo de Redundancia de Direcciones Común o CARP para la conmutación por error de hardware. Se pueden configurar dos o más appliances en un grupo de conmutación por error. Si una interfaz falla en el primario o el primario se desconecta por completo, el secundario se activa. La utilización de esta función de WDNG crea una solución totalmente redundante con una conmutación por error automática y sin problemas. Mientras se cambia al secundario, las conexiones de red permanecerán activas con una interrupción mínima para los usuarios.

CONMUTACIÓN AUTOMÁTICA POR ERROR

Si el dispositivo primario dejara de estar disponible, el firewall secundario tomará el relevo sin intervención del usuario.

TABLAS DE ESTADO SINCRONIZADAS

La tabla de estado del appliance maestro se replica en todos los dispositivos (WDNG) configurados para la conmutación por error. Esto significa que las conexiones existentes se mantendrán en caso de fallo, lo que es importante para evitar interrupciones en la red.

SINCRONIZACIÓN DE LA CONFIGURACIÓN

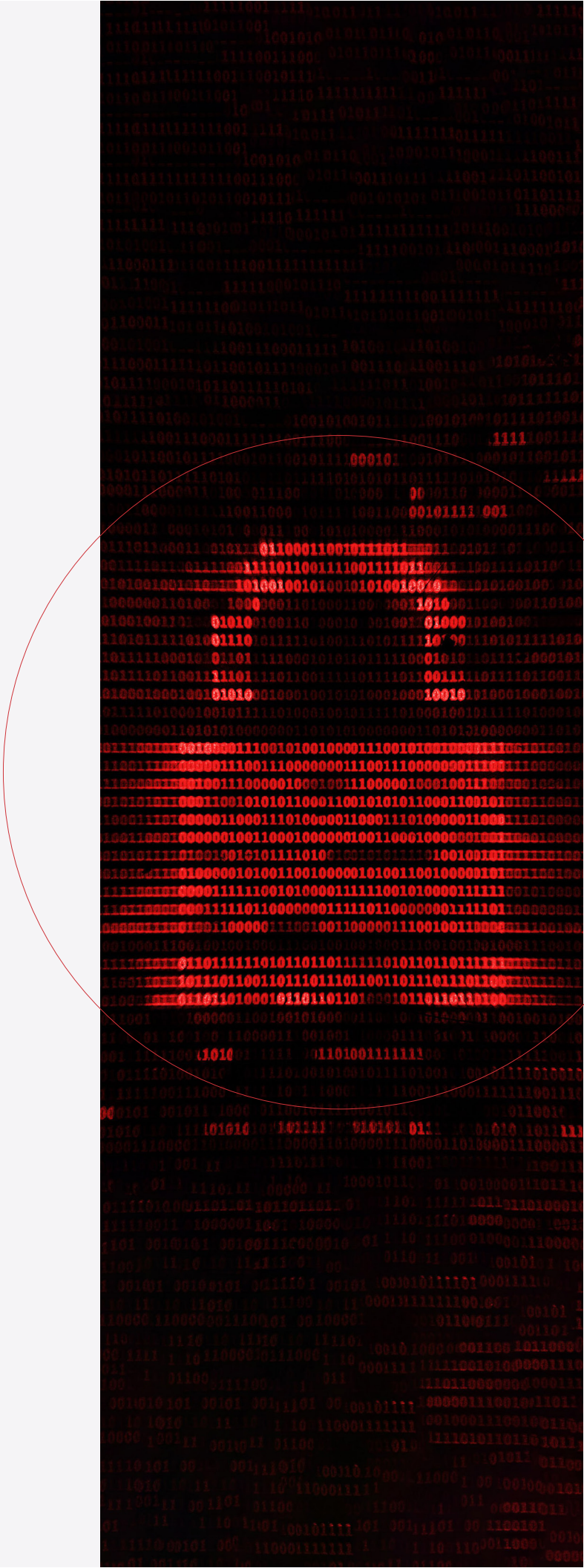
WDNG incluye capacidades de sincronización de la configuración. Los cambios de configuración realizados en el sistema primario se sincronizan automáticamente con el appliance secundario.

VISIÓN GENERAL DEL ESTADO DE LOS SERVICIOS Y REINICIO

Se puede tener una visión general de los servicios que se están ejecutando en el dispositivo de copia de seguridad y reiniciarlos por servicio o todos a la vez directamente desde la interfaz de usuario principal.

DETECCIÓN Y PREVENCIÓN DE INTRUSOS

El sistema de prevención de intrusos de WDNG implementa una optima configuración para mejorar el performance y minimizar el uso del CPU. Este sistema de inspección profunda es altamente eficiente y puede ser utilizado para mitigar amenazas rápidamente.



CONJUNTO DE REGLAS

Todas las categorías de reglas pueden ser fácilmente seleccionadas y habilitarlas con configuraciones por defecto o aplicar configuraciones personalizadas.

EMERGING THREATS RULESET

WDNG ha integrado soporte para el conjunto de reglas de Emerging Threats, el cual es un excelente conjunto de reglas para IDS/IPS contra el malware, que permite mejorar significativamente la seguridad de los dispositivos en la red.

ABUSE.CH

Abuse.ch ofrece varias listas negras para protegerse de las redes fraudulentas. WDNG ha integrado soporte para la lista negra de SSL (SSLBL), un proyecto mantenido por abuse.ch. El objetivo es proporcionar una lista de certificados SSL "malos" que abuse ch ha identificado como asociados a actividades de malware o botnet. SSLBL se basa en las huellas digitales SHA1 de los certificados SSL maliciosos y ofrece varias listas negras.

FEODO TRACKER

Feodo (también conocido como Cridex o Bugat) es un troyano utilizado para cometer fraudes en la banca electrónica y robar información sensible del ordenador de la víctima, como los datos de la tarjeta de crédito o las credenciales. En este momento, Feodo Tracker está rastreando cuatro versiones de Feodo.

PROTECCIÓN AVANZADA CONTRA AMENAZAS

WDNG provee protección avanzada contra amenazas como Malware, Virus y ataques de phishing bloqueando sitios web que son conocidos por contener algún tipo de amenaza. WDNG bloquea dominios sospechosos incluyendo dominios que han expirado, han sido hackeados o han sido registrados recientemente (NRDs), los cuales son utilizados para lanzar ataques maliciosos.

PROTECCIÓN CONTRA LAS ÚLTIMAS AMENAZAS

Protección basada en la nube la cual concentra información de más de 150 millones de sitios web y nuevos sitios son añadidos continuamente, está nube mantiene la reputación de los sitios permitiendo responder de forma rápida y efectiva contra amenazas de malware y virus en tiempo real.

CONTROL DE APLICACIONES

Bloquea o controla las aplicaciones dentro de la organización.

REPORTES

WDNG identifica los protocolos y los atributos de los datos, de esta forma se pueden generar reportes en tiempo real permitiendo analizar cada conexión.

FILTRADO WEB Y SEGURIDAD

Categorización para más de 140 millones de sitios en 40+ categorías personalizables: Blacklist y Whitelist.

POLÍTICAS DE FILTRADO

Crear Perfiles de filtrado basado en:
- *Interfaces de Red*
- *VLAN's*
- *Subnet*
- *Direcciones IP*
- *Usuarios/grupos*

BLOQUEO DE SITIOS POTENCIALMENTE PELIGROSOS RELACIONADA CON:
- *Malware*
- *Phishing*
- *Spam*
- *Potencialmente peligrosos*
- *Otros*

HERRAMIENTAS

STATEFUL FIREWALL
- *Filter by*
  - *+ Source*
  - *+ Destination*
  - *+ Protocol*
  - *+ Port*
  - *+ OS (OSPF)*
- *Límite de conexiones simultáneas*
- *Registro de eventos por regla*
- *Políticas de ruteo*
- *Estandarización de paquetes*
- *Router puro*

ORGANIZACIÓN DE POLÍTICAS
- *Soporte de Alias*
  - *+ Direcciones IP*
  - *+ Rango de puertos*
  - *+ Nombre de Dominios (FQDN)*
- *Agrupación de interfaces*
  - *+ Crear zonas de seguridad con las mismas reglas*

CONTROL DE TABLAS DE ESTADO
- *Tamaño ajustable a las tablas de estados*
- *Limitación de conexiones simultáneas*
- *Limites de nuevas conexiones por segundo*
- *Tiempo límite para sesión*

AUTENTICACIÓN EN DOS PASOS
- *Soporte TOTP*
- *Google Authenticator*
- *Servicios soportados*
  - *+ Portal cautivo*
  - *+ Proxy*
  - *+ VPN*
  - *+ GUI*
  - *+ SSH/Console*

802.1Q VLAN

LINK AGGREGATION AND FAILOVER
- *Load Balance*
- *Round Robin*
- *Cisco Ether Channel*
- *802.3ad LACP*

BORDER GATEWAY PROTOCOL

TIPO DE INTERFACES
- *Interfaces modo puente*
- *Generic Tunnel Interfaces*
- *Generic Routing Encapsulation*
- *802.1ad QinQ*

Network Address Translation
- *Port Forwarding*
- *1:1*
- *Outbound NAT*
- *NAT Reflection*

TRAFFIC SHAPPING
- *Limitador de velocidad*
- *Balanceo de carga*
- *Priorización de tráfico*

IGMP PROXY
- *Multicasting Rounting*
- *Dynamic DNS*

DNS FORWARDER
- *Host Override*
- *Domain Override*

SERVIDOR DNS
- *Host Overrides*
- *Registros tipo A*
- *Registros tipo MX*
- *Lista de Accesos*

FILTRADO POR DNS
- *Soporte OpenDNS*

SERVIDOR DHCP
- *IPv4 & IPv6*
- *Soporte Relay*
- *Access Control List*

MULTI WAN
- *Load Balancing*
- *Failover*

BALANCEO DE CARGA
- *Balancea las peticiones entrantes a multiple servidores*

SERVIDOR DE TIEMPO DE RED

Intrusion Detection & Prevention
- *Funcionamiento en línea*
- *Conjunto de reglas*
  - *+ SSL Blacklist*
  - *+ Feodo Tracker*
  - *+ Emerging Threats*
  - *+ SSL Fingerprint*

CAPTIVE PORTAL
- *Tipos de uso*
  - *+ Red de invitados*
  - *+ Bring your own device*
  - *+ Red para clientes*
  - *+ Multiple zonas*
- *Métodos de autenticación*
  - *+ LDAP*
  - *+ Radius*
  - *+ Usuarios Locales*
  - *+ Ninguno*
- *Administrador de Tickets*
- *Tiempos límites*
- *Limitador de ancho de banda*

+ Balanceo de carga
+ Priorización
+ Protocolos
+ Puertos
+ IP

- Bypass Portal
  + Lista Blanca MAC & IP
- Monitoreo en tiempo real
  + Ancho de Banda en tiempo real
  + Sesiones Activas
  + Tiempo restante

REDES PRIVADAS VIRTUALES (VPN)

- IPsec
  + Site to Site
  + Clientes móviles
- SSL VPN
  + Site to Site
  + Clientes móviles
- Mesh VPN
  + Full mesh rounting
- PPTP (legacy)
- LT2P (legacy)

ALTA DISPONIBILIDAD

- Failover de hardware automático
- Tablas de estado sincronizadas
- Configuración de sincronización

CACHING PROXY

- Multi interface
- Modo Transparente
- SSL Bump
- SSL domain only
- Access Control Lists
- Blacklisting
- Filtrado web basado en categorías
- Soporte ICAP (conexión con diferentes motores de antivirus)

BACKUP AND RESTORE

- Historial de cambios
- Archivo de configuración
- Backups en la nube

HERRAMIENTAS DE DIAGNÓSTICO

- Filter reload status
- Firewall info
- Top users
- Firewall Tables
- Aliases
- Bogons
- Current open sockets
- Show all states
- State reset
- State summary
- Wake on LAN
- ARP Table
- DNS Lookup
- NDP Table
- Ping
- Packet Capture
- Test port
- Trace route

PROXY INVERSO WAF

- Load Balancing
- Header Hardening
- Local Web Hosting
- Authentication
- IP Control Access
- TLS Fingerprint
- TLS Authentication
- TCP UDP Stream
- Web Applicaton Firewall

ANTISPAM

- Mail Gateway
- Virus Filtering
- Spam Protection
  + Graylisting
  + DKIM
  + MX Check
  + Phishing
  + Rate Limit
  + Spam trap
  + Sender Policy Framework
  + Trusted Networks
  + Reject Unknown Sender Domain
  + Reject Unknown Recipient Domain
  + Reject Non FQDN Sender
  + Reject Non FQDN Recipient

REPORTES

- Analizador de tráfico en la red
  + Totalmente integrado
  + Representación gráfica
  + Búsqueda
  + CVS Exporter
- Estado del sistema
  + Round Robin Data
  + Selection and Zoom
  + Traffic graph
  + Monitoreo de tráfico en tiempo real


Warriors®
"Security that makes difference"