

NUMERO DE PROYECTO: 200494

EMPRESA BENEFICIADA: SQUID APPLIED RESEARCH AND TECHNOLOGY SA DE CV

TÍTULO DEL PROYECTO: Dispositivo de Gestión Unificada de Amenazas intuitivo (UTM ó XTM) para la protección de datos y seguridad en redes informáticas, a través de múltiples prestaciones integradas y procesos inteligentes predictivos en un solo equipo



Squid Applied Research and Technology SA. de CV.



OBJETIVO DEL PROYECTO:

Diseño y desarrollo de interfaces gráficas que faciliten la administración y el control de las tecnologías asociadas al UTM.

Análisis, identificación y calibración de modelos inteligentes para mejorar la detección de las posibles amenazas en el funcionamiento de equipos de red, sin detrimento de los recursos y tiempos de respuesta de los equipos asociados.

PRINCIPALES ACTIVIDADES REALIZADAS:

Enrutador

Interfaz de consulta de tablas de ruteo.

Interfaz de selección de parámetros y protocolos de enrutamiento.

Interfaz de administración de puertos y cargas.

Filtro de correo

Interfaz de administración de dominios bloqueados.

Bitácora de amenazas bloqueadas y detectadas.

Interfaz de administración de direcciones bloqueadas.

Filtro Web

Interfaz de administración de dominios bloqueados.

Bitácora de amenazas bloqueadas y detectadas.

Interfaz de administración de direcciones bloqueadas

CONTINUACION...

Antivirus

Interfaz de control de versiones de antivirus.

Bitácora de amenazas bloqueadas y detectadas.

Interfaz de activación y estado de antivirus.

Firewall

Interfaz de administración de protocolos filtrados.

Interfaz de administración de puertos filtrados.

Interfaz de administración de direcciones filtradas.

DNS (Servidor de nombres de Dominio)

Interfaz de administración de nombres de dominio y direcciones IP

Bitácora de nombres de dominio.

Interfaz de direcciones bloqueadas.

DHCP (Servidor de direcciones IP)

Interfaz de configuración banco de direcciones y puertos.

Interfaz de reservación de direcciones.

CONTINUACION...

IPS (Software de prevención de amenazas)

Bitácora de amenazas detectadas.

Interfaz de configuración de tablas de dependencia condicional del sistema inteligente.

Sistema inteligente con modelos gráficos probabilistas para la detección de amenazas y patrones sospechosos.

Administración

Interfaz de usuarios.

Interfaz de protocolos permitidos y bloqueados para la administración.

Interfaz de puertos permitidos y bloqueados para la administración.

Interfaz de administración de permisos.

Interfaz de administración de roles de usuario.

Para esta aplicación Web se entregaron los siguientes elementos:

Manual de usuario de aplicación

Manual técnico de aplicación

Modelación de arquitectura de aplicación

Código fuente del desarrollo

Instalación en sistema de usuario.

Prototipo funcional de modelos inteligentes para los siguientes 3 servicios:

Firewall

Webfilter

IPS

BREVE DESCRIPCIÓN DEL PROYECTO: UTM (en inglés: Unified Threat Management) o Gestión Unificada de Amenazas. Se utiliza para describir los cortafuegos de red que engloban múltiples funcionalidades en una misma máquina. Algunas de las funcionalidades que puede incluir son las siguientes: . Antispam, Antispyware, Filtro de contenidos, Antivirus, Detección/Prevención de Intrusos (IDS/IPS)

RESULTADOS DEL PROYECTO: Se logró el 100% de los objetivos y compromisos planteados, tales como el dispositivo de gestión unificada, con una interfaz gráfica amigable e intuitiva para el usuario final

IMPACTOS DEL PROYECTO:

Se obtuvo una solución tecnológica avanzada que permitió integrar el sistema de Gestión Unificado de Amenazas (UTM ó XTM; por sus siglas en inglés), instalado en unidades dedicadas para la protección de datos y seguridad en redes informáticas; así mismo todos los procesos de auditoría de información están basados en modelos predictivos de ataques informáticos y manteniendo múltiples prestaciones integradas para la seguridad en un sólo equipo, con interfaces gráficas de configuración y administración intuitiva para el usuario

Las interfaces desarrolladas permiten que cualquier usuario con conocimiento de las tecnologías incorporadas, pueda administrar el dispositivo de manera simple y eso facilita la comercialización del producto.

Debido a que el dispositivo UTM puede ser administrado y monitoreado a través de las distintas interfaces y de diversos dispositivos móviles, es más atractivo para los usuarios simple y eso también facilita la comercialización del producto.

Los algoritmos inteligentes predictivos desarrollados permiten predecir con un 90% de eficiencia posibles amenazas a la red a través del monitoreo del tráfico.