

## CYBEROAM CR100ia UTM

En el presente laboratorio se identifica, examina, analiza, valora y evalúa Cyberoam CR100ia, una herramienta escalable para seguridad de red, de naturaleza hardware-software, catalogada como *appliance* de seguridad con controles basados en identidad de usuario, tipo UTM, siendo adecuada para medianas y pequeñas empresas. Integra un rico conjunto de funcionalidades de protección contra *malware*, virus, *spam*, *phishing*, *pharming*, fugas de datos, abuso de ancho de banda, contenidos no deseados, etc., consistente en una combinación de cortafuegos de inspección de estados, VPN, pasarelas anti-virus (correo-e, sitios web, transferencias de ficheros), anti-*spyware* y anti-*spam*, IPS/IDS, filtrado e identificación de contenidos-aplicaciones, gestión del ancho de banda y gestión multi-enlace. Se monitoriza, controla y administra de forma centralizada utilizando una consola rica en prestaciones basada en web. Soporta entornos IP dinámicos DHCP y WiFi y posibilita una generación de informes bien dimensionada, incluso basada en nombre de usuario. Igualmente, soporta autenticación SSO con LDAP-Directorio Activo y servidor Radius, así como balanceo de carga y capacidades de "fail-over" de tolerancia a fallos y alta disponibilidad, permitiendo trabajar con entornos VLAN 802.1Q, así como realizar tareas de cumplimiento regulatorio.

### IDENTIFICACIÓN DE LA HERRAMIENTA. FUNCIONALIDADES PRINCIPALES

La herramienta de seguridad hardware-software Cyberoam CR100ia UTM de Cyberoam –una división de la compañía Elitecore Technologies– puede catalogarse como *appliance*

Cyberoam CR100ia



de seguridad tipo UTM basado en identidad, que se controla, administra y gestiona a través de una consola centralizada. Se han podido constatar, entre otras, las siguientes funcionalidades relevantes:

(i) **Cortafuegos de inspección de estados.** Permite una inspección de paquetes en profundidad con estados. Posibilita establecer una única política de *firewall* que abarca todos los componentes. Previene ataques tipo *DoS/DDoS* como inundación, tanto de fuentes internas como externas. Permite un control de acceso basado en identidad para aplicaciones como *P2P* e *IM* (Mensajería Instantánea). Protege a nivel de aplicación y posibilita gran flexibilidad para establecer políticas por identidad de usuario. La funcionalidad cortafuegos posee la certificación *ICSA Lab*. Permite establecer múltiples zonas de seguridad con niveles separados de aplicación de reglas de acceso para cada zona.

(ii) **VPN** (red privada virtual). Integra VPN basada en *SSL-RC4* (*sin clientes*) y VPN con cliente basado en *IPSec* (el cliente VPN se soporta en diferentes plataformas como Windows 98, Me, NT4, 2000, XP, Vista). Soporta estándares como *IPSec*, *L2TP* y *PPTP* VPN, con VPN de alta disponibilidad para conexiones *L2TP* e *IPSec*. Cumple las certificaciones *VPNC* básica y de inter-operación *AES*. Incluye gestión de *fail-over* con prioridades de

conexión definidas. Posibilita conectividad remota de bajo costo sobre Internet.

(iii) **Pasarela Anti-virus y Anti-*spyware*.** Permite analizar tráfico *HTTP*, *FTP*, *IMAP*, *POP3* y *SMTP*. Detecta y elimina virus, gusanos y caballos de Troya. Posibilita acceso a correos electrónicos en cuarentena para ejecutivos. Permite una identificación de usuario instantánea en caso de amenazas *HTTP*. Posibilita una protección de información confidencial. Utiliza una base de datos de unas 370.000 firmas de virus.

(iv) **Pasarela Anti-*spam*.** Permite analizar el tráfico *SMTP*, *POP3*, *IMAP*; detecta, etiqueta y pone en cuarentena correo *spam*. Aplica tecnología de listas blancas y negras. Permite protección de brotes de virus emergentes. Incorpora tecnología *RPD* (*Recurrent Pattern Detection*) para protección de *spam content-agnostic* como *spam* de imágenes. Posibilita detección de *spam* multi-formato y multi-lingüe.

(v) **IPS.** Utiliza una base de datos de más de tres mil quinientas firmas e incorpora capacidad multi-política con políticas basadas en firmas por defecto y personalizadas, origen y destino. Previene de intentos de intrusión, ataques *DoS*, código malicioso, actividad de puertas traseras y amenazas mezcladas basadas en red. Permite bloquear *proxies* anónimos con firmas *proxy HTTP* y bloquea actividades "*phone home*". La tasa de falsos positivos constatada ha sido baja. Permite aplicar políticas a usuarios. Soporta entornos de IP dinámica como *DHCP* y *Wi-Fi*. En caso de amenazas internas permite la identificación del usuario.

(vi) **Filtrado de contenido-aplicaciones.** Incorpora motor de categorización web automatizada que bloquea sitios no operativos en unos cuarenta millones de sitios o URLs ordenados en más de ochenta categorías. Permite filtrar URL en protocolos *HTTP/*

*HTTPS*. Posibilita desplegar políticas de filtrado basadas en usuario, grupo, departamento y jerarquía. Asegura diversos cumplimiento regulatorios como *CIPA* (*Children's Internet Protection Act*) para escuelas y bibliotecas y previene descargas de *streaming*, juegos, *videos/flash*, *tickers*, etc. Permite acceso basado en tiempo a sitios pre-definidos.

(vii) **Gestión del ancho de banda (basado en identidad de usuario y aplicación).** Permite garantizar un ancho de banda comprometido por jerarquía, departamentos, grupos y usuarios, previniendo congestión de ancho de banda en base a prioridades para aplicaciones críticas.

**Cyberoam CR100ia es una herramienta compacta de seguridad de red catalogada como *appliance* de seguridad multi-funcional tipo UTM basado en identidad. Integra múltiples funcionalidades interrelacionadas, como cortafuegos, IPS/IDS, pasarelas antivirus/anti-*spyware*/anti-*spam*, filtrado de contenidos, VPN (con y sin clientes con *SSL* y con *IPSec*), gestión del ancho de banda y multi-enlace, capacidades de encaminamiento dinámico, autenticación, tolerancia a fallos y alta disponibilidad. Se gestiona de forma centralizada desde una potente consola basada en web.**

(viii) **Gestión multi-enlace.** Permite establecer seguridad sobre múltiples enlaces ISPs utilizando un único *appliance* CR100ia. Posibilita el balanceo de carga de tráfico empleando una distribución de cola circular con pesos. Incorpora mecanismo *fail-over* de enlace que automáticamente conmuta el tráfico de un enlace con fallo a uno operativo. Permite controlar la congestión del ancho de banda asegurando la continuidad del negocio.

(ix) **Generación de informes.** Genera de forma flexible informes por nombre de usuario, descubre tráfico ofreciendo informes en tiempo real, posibilita una visibilidad en forma de patrones de uso y permite una identificación de víctimas y atacantes en la red interna. Genera informes sobre: eventos de intrusión, violaciones de política, categoría web (usuario, tipo de contenido); con motor de búsqueda por palabras clave, de transferencias de datos (por computador, grupo y dirección IP), sobre cumplimiento regulatorio y sobre virus (por usuario y dirección IP).

(x) **Autenticación.** Permite vincular usuario con MAC, se integra con bases de datos externas LDAP/Radius-AAA y con Directorio Activo de MS y Control de Dominios Windows. Utiliza base de datos local y posibilita SSO (*Single Sign On*) Windows automática.

(xi) **Administración y Gestión del sistema.** Utiliza una Consola Central. Incluye un *wizard* para configuración basado en web. Soporta administración basada en rol con múltiples administradores y niveles de usuario. Permite actualizaciones y cambios utilizando una interfaz de usuario web (*HTTPS*), soporta múltiples idiomas. Incluye CLI (*Command Line Interface*) de serie, SSH y Telnet. Opera con SNMP (v1, v2, v3). Soporta servidor NTP.

(xii) **Controles basados en identificación de usuario y grupo.** Permite restricciones de tiempo de acceso, así como cuotas de datos y tiempo. Posibilita la planificación basada en ancho de banda comprometido y basada en controles IM y P2P.

(xiii) **Alta disponibilidad.** Permite las modalidades activa-activa, activa-pasiva con sincronización de estado y *fail-over* con estados. Soporta alerta en el cambio de estado del *appliance* CR100ia.

(xiv) **Logging-Monitorización.** Permite mostrar de forma gráfica la monitorización histórica y la de tiempo real, soporta *syslog*, así como la notificación por correo electrónico de informes, virus y ataques.

(xv) **Operaciones de red.** Soporta *fail-over* multi-enlace, balanceo de carga basada en WRR y política de encaminamiento basada en usuario y aplicación. Incluye cliente DDNS/PPPoE, soporta *proxy* HTTP y *proxy* parental con FQDN. Permite encaminamiento dinámico con protocolos como RIP v1 y v2, OSPF, BGP y reenvío *multicast*.

## CONSOLA DE GESTIÓN CENTRAL. CUADRO DE MANDO

La *Consola Central* de la herramienta aquí evaluada permite monitorizar y gestionar de forma centralizada múltiples *appliances* de seguridad CR100ia. Se ha constatado que posibilita realizar tareas como:

### (i) Gestión centralizada de dispositivos.

El GUI web centralizado permite la gestión de todos los *appliances* CR100ia distribuidos, incluyendo la gestión de políticas, la aplicación de cumplimientos y la monitorización y control. La Consola Central gestiona la tarea de configurar grupos remotos, dispositivos, usuarios y roles de forma sencilla.

(ii) **Implantación de política basada en identidad para soportar requisitos de negocio.** Permite crear e implantar políticas globales a escala empresarial que sean acordes con las guías de recursos humanos corporativos para mantener los niveles de



Fig. 1.- *Appliance* Cyberoam CR100ia UTM.

productividad y medidas de seguridad a través de toda la empresa. Las MSSPs pueden aplicar diferentes políticas a diferentes empresas que necesitan gestionar su seguridad.

### (iii) Gestión centralizada de amenazas y aplicación de políticas de seguridad en respuesta a amenazas de día cero.

Permite crear y aplicar reglas de cortafuegos; políticas IPS a medida, utilizando firmas personalizadas para proteger la empresa de las últimas amenazas; actualiza *appliances* remotos desde la Consola Central y protege oficinas satélite remotas o distribuidas con la misma competencia técnica que la ubicación central.

### (iv) Control de amenazas distribuidas y visibilidad de seguridad de toda la organización.

La Consola Central permite una monitorización central, asegurando una acción rápida que proporcione seguridad no interrumpida a través de todas las redes. Monitoriza las oficinas remotas y distribuidas, obteniendo una visibilidad del estado de la red. Aplica acciones inmediatas para ejecutar en tiempo real seguridad y políticas *firewall* para controlar los ataques. Soporta administración basada en roles y los permisos para los *appliances* y la configuración y gestión de la consola pueden establecerse individualmente para cada usuario administrativo que se añade a la Consola Central. Los administradores con permiso local pueden configurar y gestionar la Consola Central, así como las siguientes funciones de los *appliances* de seguridad desplegados: 1) Reglas de *firewall*. 2) Política de acceso a Internet. 3) Política de ancho de banda. 4) Política de IDP (Intrusión, Detección y Prevención). 5) Categorías. Los administradores sin permiso local sólo pueden gestionar los *appliances* pero no la Consola Central. La Consola Central puede accederse y administrarse desde una *consola* web de administración (vía *HTTPS* aunque se ha constatado que también permite *HTTP*,



Fig. 2.- Interfaz para crear política de ancho de banda con Cyberoam CR100ia UTM.

## EQUIPOS UTILIZADOS EN LA EVALUACIÓN

- ♦ Equipamiento para la consola de gestión central, puestos de trabajo de usuarios, clonación de *appliance* para pruebas de alta disponibilidad, servidores con Windows 2003/2000/XP y Linux, PCs con procesador Intel Core 2 Quad, 3 GHz., con 2Gb de memoria, disco duro de 160 Gb, unidad DVD/CD-ROM, tarjeta gráfica WXGA, tarjeta NIC de red 10/100/1000Base T compatible NE2000/NDIS. Navegadores Internet Explorer, Mozilla Firefox. Servidor LDAP y Directorio Activo Windows. Servidores NTP y Radius.
- ♦ Nueve redes locales, Ethernet 10/100/1000 BaseT con IEEE 802.2-LLC, como soporte físico de las comunicaciones con Protocolo de Control de Acceso al Medio o MAC CSMA/CD. Acceso a Internet.
- ♦ *Hubs / switches* de 16 puertos Ethernet 10/100/1000. *Modems* analógicos para RTB/RTC V.90/ITU-TSS (a 56 Kbps) y tarjetas digitales RDSI-BE 2B+D/Acceso Básico-BRA como acceso conmutado al exterior y conexiones ADSL/cable módem. Acceso GSM/GPRS/UMTS. Ocho routers. Cuatro puntos de acceso Wi-Fi, IEEE 802.11g/b/a. Seis impresoras. Una unidad hardware Cyberoam CR100ia UTM.
- ♦ Analizador de protocolos para monitorizar las comunicaciones intercambiadas en todos los niveles de la arquitectura.
- ♦ Módulos de valoración de mecanismos criptográficos de cifrado, autenticación. Módulo de valoración de criptoanálisis.
- ♦ Módulo de pruebas para medidas de seguridad y rendimiento con diferentes cargas de trabajo y número de usuarios. Generadores de tráfico.
- ♦ Baterías de ataques DoS/DDoS, caballos de Troyanos, *spyware*, *spam*, *phishing*, *pharming*, gusanos, virus de aplicación, virus *streaming*, puertas traseras, fugas de datos, etc., bajo control gestionable de cargas de tráfico. Valoración con virus EICAR.
- ♦ Módulos de inyección de esteganografía y detección con estegano-análisis. Mecanismos de valoración para pruebas "side-channel".

protocolo vulnerable), desde una consola Telnet (protocolo vulnerable si el acceso es remoto) y utilizando una conexión cifrada basada en cliente SSH. Un cuadro de mando ayuda a visualizar todos los *appliances* registrados y eventos que requieren atención. La Consola Central recoge toda la información necesaria de los *appliances* que se visualizarán sobre el cuadro de mando.

## FUNCIONALIDADES CARL Y VPN

**CARL** (*Cyberoam Aggregated Reporting and Logging*) es una funcionalidad basada en web que analiza los *logs* del cortafuegos y genera informes y utiliza un servidor *syslog* para almacenar, analizar y reportar dichos *logs*. **CARL** proporciona informes diarios, semanales, mensuales y anuales acerca del tráfico del cortafuegos, de las brechas de seguridad, etc. Es una gran ayuda para los administradores de red, para que proactivamente protejan las redes antes de que surjan las amenazas, evitando abusos de red, gestionando requisitos de ancho de banda, monitorizando visitas a sitios web y asegurando el uso apropiado de las redes por parte de los empleados. **CARL** permite saber: qué empleados son los que más navegan por la web, indicando qué sitios visitan; cuántos usuarios del lado del *firewall* conectado a la red corporativa interna intentan acceder a sitios web con contenido inapropiado; cuánta actividad de red se origina en cada lado del cortafuegos; qué servidores reciben la mayor parte de los ataques; si se está experimentando un intento de intrusión; y desde dónde se originó. La funcionalidad VPN de la herramienta aquí valorada cifra los datos y los envía al sitio remoto donde se descifra y reenvía al destino deseado. Permite proteger la confidencialidad e integridad de los datos, incluso aunque se transmitan sobre una red pública no confiable. Utiliza tanto SSL como el estándar IPsec; con IPsec se comprueba la identidad de los usuarios que se comunican utilizando autenticación de usuario en base a certificados digitales, claves públicas o claves pre-compartidas.

La solución de Cyberoam aquí evaluada puede utilizarse para establecer conexiones "tunelizadas" VPN entre sitios: LAN a LAN y cliente a LAN. Soporta los siguientes protocolos para autenticar y cifrar tráfico: IPsec, L2TP y PPTP, así como algoritmos de cifrado simétrico de bloque como 3DES, AES con claves hasta 256 bits, Serpent con bloque de 128 bits y con claves de hasta 256 bits, Blowfish con bloque de 64 bits y con clave hasta 448 bits y Twofish con bloque de 128 bits y con clave de hasta 256 bits. Utiliza como algoritmos criptográficos unidireccionales o *hash* para integridad de datos MD5 y SHA-1. La política VPN describe los parámetros de seguridad que se utilizan para las negociaciones a la hora de establecer y mantener un túnel cifrado entre los dos puntos correspondientes local-remoto que se comunican.

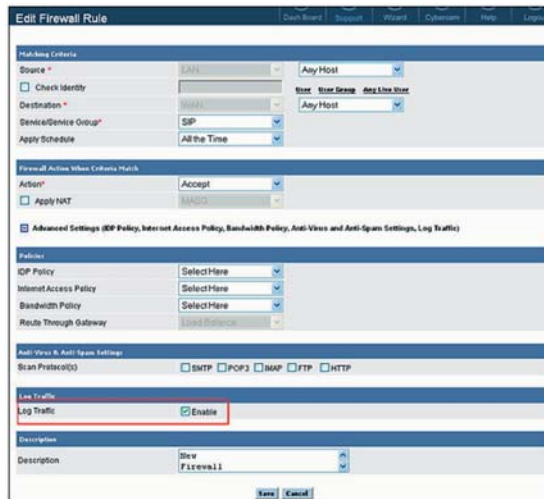


Fig. 3.- Pantalla de edición de reglas de cortafuegos de Cyberoam CR100ia UTM.

VPN limita el dominio de difusión-colisión. La herramienta aquí evaluada soporta VLAN construyendo troncales VLAN entre un *switch* o *router* que cumpla con IEEE 802.1Q y los *appliances* CR100ia. Normalmente el interfaz interno del *appliance* se conecta a un troncal VLAN en un *switch* interno y el interfaz externo se conecta al *router* Internet. Es posible aplicar diferentes políticas de tráfico en cada VLAN que conecta al interfaz interno.

## HARDWARE DEL APPLIANCE CR100ia

Externamente se pueden identificar en la parte frontal de un *appliance* CR100ia UTM los siguientes elementos: (i) Seis puertos (denotados como A, B, C, D, E y F) *Ethernet 10/100/1000*, tipo RJ45 cada uno con dos LED indicadores de actividad. Si se conectan a un computador de gestión se utilizará un cable Ethernet cruzado; en cambio, si se conectan a un *hub* (permite un único dominio de colisión) o a un *switch* (posibilita varios dominios de colisión) se deberá utilizar un cable Ethernet directo. La conectividad puede ser LAN/WAN/DMZ. (ii) Dos puertos USB. (iii) Un puerto RJ45 para la consola de gestión. (iv) Dos botones-pulsadores, uno de reset y otro F/D. (v) Un LED indicador de encendido. (vi) Un LED indicador de actividad del disco duro HDD.

En la parte posterior se pueden identificar los siguientes elementos: (i) Dos salidas de ventiladores. (ii) Una base de enchufe con toma de tierra para la alimentación eléctrica de corriente alterna 115-230 V y consumo de 90W. (iii) Un interruptor de encendido on/off. Internamente utiliza como procesado CPU *multi-core* y sistema operativo del tipo núcleo recortado de servicios.

## CATEGORÍAS PARA FILTRADO. POLÍTICAS Y PLANIFICACIÓN

Las capacidades de filtrado de contenidos de la herramienta aquí evaluada previenen que los usuarios de Internet accedan a sitios web no-productivos o inaceptables que utilizan recursos valiosos del sistema de la red, a la vez

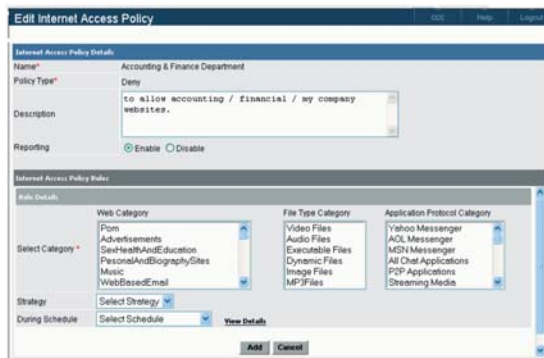


Fig. 4.- Pantalla de edición de política de acceso a Internet.



Fig. 5.- Interfaz de creación de firma con Cyberoam CR100ia UTM.

que también previenen que atacantes y virus puedan ganar acceso a la red corporativa a través de sus conexiones Internet. Asimismo, la solución de Cyberoam aquí valorada previene que los usuarios de Internet accedan a URLs que tengan contenido que la organización considera no deseado. La base de datos de categorías de la presente herramienta cubre páginas web de material para adultos, astrología, juegos, búsqueda de trabajo, armas, etc. La base de datos de categorías consta de tres tipos:

(i) **Categorías web.** Agrupación de dominios y palabras clave. Las categorías se agrupan en cuatro tipos y especifican si la navegación se considera productiva o no: neutral, productiva, no del trabajo, morbosa. (ii) **Tipos de ficheros.** Agrupaciones de extensiones de ficheros. (iii) **Protocolo de aplicación.** Agrupación de protocolos. Aparte de las categorías por defecto, pueden crearse categorías a medida que incrementan la flexibilidad para gestionar el acceso a Internet. Una vez creada una nueva categoría, se debe añadir a una política para que la herramienta CR100ia sepa cuándo aplicarla y para qué grupos y/o usuarios. La herramienta aquí evaluada permite controlar el acceso a diversos recursos con ayuda de políticas; éstas se pueden crear y desplegar desde la Consola de control Central. Se han podido constatar, entre otros, los siguientes tipos de políticas: de acceso a Internet y de ancho de banda.

**Política de acceso a Internet**  
Controla el acceso web del usuario. Especifica qué usuario tiene acceso a qué sitios o aplicaciones y permite definir políticas de seguridad potentes en base a parámetros de política como: usuarios individuales, grupos de usuarios, hora del día, localización/puerto/tipo de protocolo, tipo de contenido, uso de ancho de banda (para audio, vídeo y contenido streaming). Permite/deniega acceso a una categoría de aplicación entera o a extensiones de fichero individuales dentro de una categoría con ayuda de la política; por ejemplo se puede definir una política que bloquee el acceso a todos los ficheros de audio con extensiones .mp3. Se pueden definir dos estrategias basadas en la política de acceso a Internet: (a) Permitir por defecto. Permite el acceso a todas las categorías salvo a las especificadas. (b) Denegar por defecto. Deniega el acceso a todas las categorías salvo a las especificadas. En ambos casos, el acceso a las especificadas depende de la estrategia definida para cada categoría.

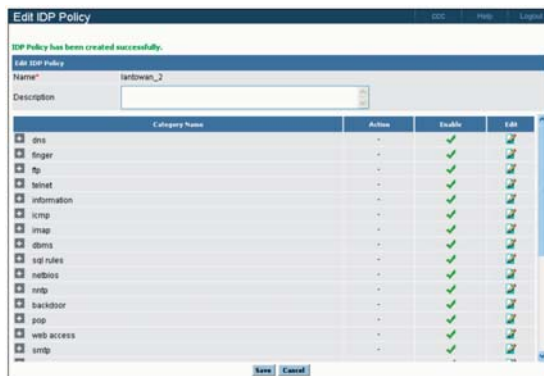


Fig. 6.- Pantalla de edición de política IDP con Cyberoam CR100ia UTM.

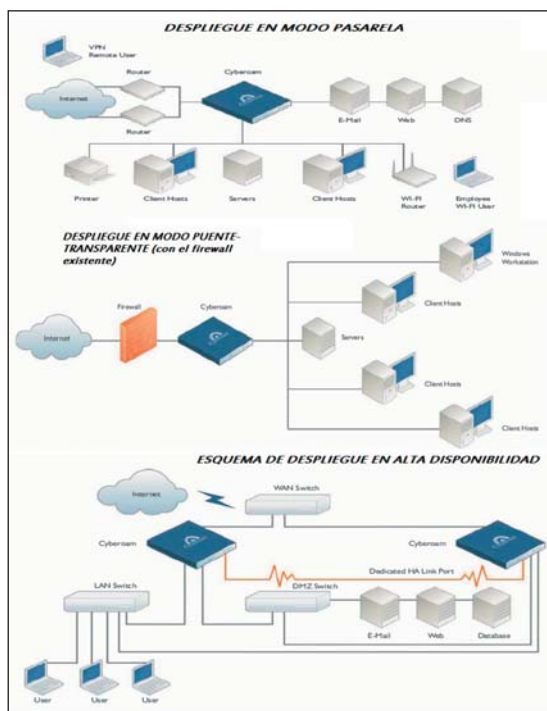


Fig. 7.- Esquemas de algunos despliegues con Cyberoam CR100ia UTM.

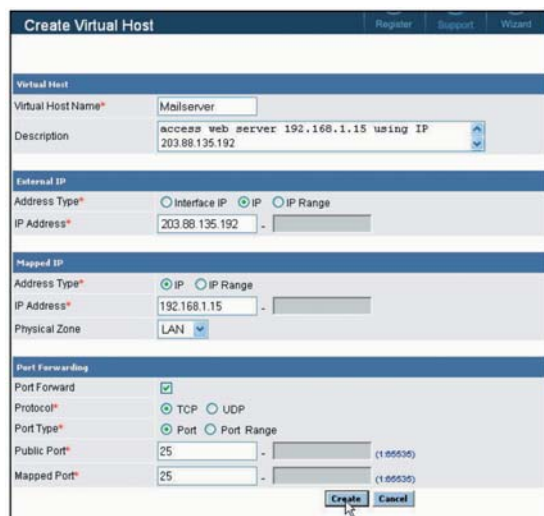


Fig. 8.- Interfaz de creación de un host virtual para el servidor de email con Cyberoam CR100ia UTM.

**Política de ancho de banda**  
Permite asignar y restringir el uso del ancho de banda. El ancho de banda es la cantidad de datos que pasan a través de un medio durante un período de tiempo y se mide en bps. El objetivo primario de la política de ancho de banda es gestionar y distribuir el ancho total según ciertos parámetros y atributos de usuario. La política de ancho de banda asigna y limita el máximo uso de ancho de banda del usuario y controla el tráfico de red y web.

Para configurar una política en esta área se han constatado los siguientes elementos: (a) Para quién se desea crear la política. Se han definido tres posibilidades: para un grupo de usuarios que comparten el ancho de banda asignado; para un usuario particular; y para una regla de cortafuegos (restringe el ancho de banda de cualquier entidad a la que se aplica la regla de firewall). (b) El tipo de política. Se han constatado dos tipos: estricta (el usuario no puede exceder el límite de ancho de banda definido) y comprometida (al usuario se le asigna la cantidad garantizada mínima de ancho de banda y puede aumentar al límite máximo si está disponible). (c) La estrategia de implementación de la política. Se han podido constatar dos formas: total (upstream + downstream) e individual (upstream individual y downstream individual). (d)Cuál es el uso de ancho de banda. La herramienta aquí valorada viene de fábrica con diversas políticas predefinidas disponibles que pueden utilizarse directamente o personalizarse a medida para definir diferentes niveles de acceso para diferentes usuarios. La planificación permite definir una temporalidad a la hora de aplicar reglas de cortafuegos o políticas de acceso a Internet utilizadas para controlar cuándo las reglas de firewall o políticas de acceso a Internet están activas o no. Se han previsto dos tipos de planificaciones: (i) Recurrente. Se utiliza para crear políticas que sean efectivas sólo en horas del día especificadas o en días especificados de la semana. (ii) De una sola vez. Se emplea para crear reglas/políticas de firewall que sean efectivas una vez durante el período de tiempo especificado en la planificación.

**CONSIDERACIONES FINALES**

Se ha sometido la presente herramienta durante veinte días a un continuado y exhaustivo conjunto de diferentes baterías de test. Se ha evaluado la herramienta hardware-software con resultados globales de protección, en el peor de los casos superiores al 93,9%. Se ha podido constatar una tasa de 400.000

sesiones concurrentes, y se ha medido como tasa de nuevas sesiones por segundo el valor 10.000. El caudal medido obtenido para operaciones de cifrado 3DES con claves de 168 bits fue de 80 Mbps, en tanto que el caudal medido para operaciones de cifrado AES con claves de 168 bits fue de 100 Mbps.

La tasa de falsos positivos en la funcionalidad de *spam* fue del 0,007. La tasa de detección de *spam* ha sido del 98%. La *cache* local se ha encontrado efectiva para más del 67% de todos los casos de resolución de *spam*. La capacidad de bloqueo de *phishing/pharming* fue notable, del orden del 89,2%. Se constató también una periodicidad de actualización del anti-virus de unos treinta minutos. La tasa de afectividad AV fue satisfactoria con un mínimo del 87,9%. Cabe destacar en la valoración de resultados de la pasarela AV la flexibilidad de la combinación de origen, destino, identidad, servicio y planificación en los diversos tipos de tráfico L5 http, ftp, smtp, pop3 e imap. La tasa de caudal de operaciones anti-virus fue de 200 Mbps. Los resultados de las medidas de rendimiento del sistema dieron para el caudal a nivel de cortafuegos un valor de 1Gbps; para el caudal a nivel UTM el valor fue de 160 Mbps. Los resultados de las pruebas de rendimiento fueron muy satisfactorias, consiguiendo tasas del 94,3%. No se observaron inestabilidades significativas (menores del 1,5%) ante pruebas de estrés y fatiga con gradientes

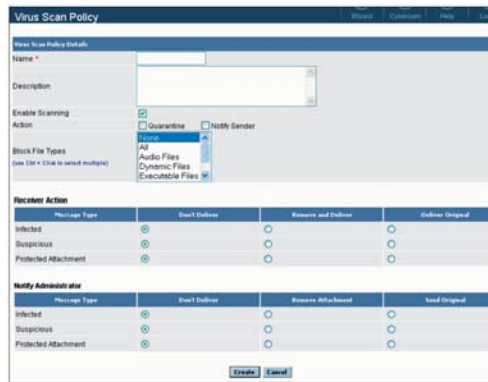


Fig. 9.- Pantalla de creación de política de análisis de virus a medida con Cyberoam CR100ia UTM.

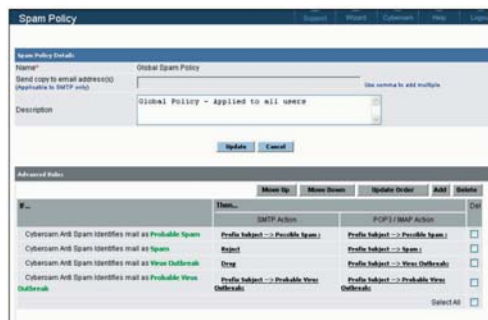


Fig. 10.- Interfaz de gestión de política de spam con Cyberoam CR100ia UTM.

de carga prolongados. Los resultados de los tests relativos al sistema de gestión centralizado fueron del orden del 97,9%. La valoración de los mecanismos de generación de informes personalizados a medida se situó en el 97,8%. El comportamiento ante cortes de fluido eléctrico y re-arranques de la herramienta fue notable. Los mecanismos de tolerancia a fallos y alta disponibilidad, en el peor de los casos, presentaron una valoración del 97,8%.

Se han encontrado en la herramienta hasta 4.093 interfaces VLAN. La tasa de caudal medida para la pasarela IPS fue de 300 Mbps. Los resultados obtenidos en las pruebas de ataques *side channels* efectuadas fueron estándar: para análisis de *timing*, del 91,7%; para análisis de potencia y DPA (*Differential Power Analysis*), del 90,9%; para análisis de fallos, del 92,8%; y para los basados en radiación EM, del 88,1%.

Los test relacionados con la efectividad de las políticas dieron como resultados valores muy satisfactorios, del orden del 97,5%. Los resultados de las pruebas de despliegue transparente en relación a efectividad operativa fueron del 96,9% y los test referentes a las operaciones de actualización de la herramienta dieron como resultado valores en torno al

95,9%. Finalmente, los resultados de las pruebas con los despliegues en pasarela y *proxy* se situaron en el 95,3% y 94,7%, respectivamente. ■

## CONCLUSIONES

- ♦ **OBJETIVO:** herramienta compacta de seguridad de red de naturaleza hardware-software catalogada como *appliance* de seguridad multi-funcional tipo *UTM* basado en identidad. Opera sobre redes basadas en la pila de protocolos TCP/IP con interfaz LAN Ethernet 10/100/1000 Mbps. Integra múltiples funcionalidades interrelacionadas, como *firewall*, *IPS/IDS*, pasarelas anti-virus/anti-spyware/anti-spam, filtrado de contenidos, VPN (con y sin clientes con SSL y con IPsec), gestión del ancho de banda y multi-enlace, capacidades de encaminamiento dinámico (RIP1/2, OSPF, etc.), autenticación (con Directorio Activo-LDAP y Radius), tolerancia a fallos y alta disponibilidad, etc. Todo el UTM se gestiona de forma centralizada desde una consola de control basada en web. Incluye funcionalidades muy útiles de monitorización y generación de informes personalizables a medida.
- ♦ **PUNTUALIZACIONES / LIMITACIONES:** las reglas de cortafuegos por defecto se pueden modificar pero no borrar. Cada *appliance* Cyberoam CR100ia permite acceso HTTPS con la Consola Central. Aunque el CR100ia proporciona por defecto cinco tipos de zonas a nivel *firewall*: LAN, DMZ, WAN, LOCAL y VPN. Es posible definir nuevas zonas a medida. La Consola Central permite configurar y gestionar las funciones: regla de cortafuegos, política de acceso a Internet, política de ancho de banda, política IDP y categorías para filtrado de contenido. Los servicios representan tipos de datos de Internet transmitidos a través de protocolos o aplicaciones concretas; para proteger la red corporativa se configuran reglas de *firewall*: para bloquear servicios de una zona específica, para limitar a algunos o todos los usuarios que acceden a ciertos servicios y para permitir sólo que un usuario específico se comuniquen utilizando un servicio específico.
- ♦ **IMPACTO DE SU UTILIZACIÓN:** permite una generación de informes muy flexible y cuidada. La consola centralizada incluye un potente conjunto de prestaciones y permite restringir el acceso por uso de ancho de banda, tiempo de navegación, volumen de datos transferidos, etc. La creación de grupos permite gestionar eficientemente un gran número de dispositivos de forma sencilla. El rendimiento constatado ha sido notable.
- ♦ **PRESTACIONES / VENTAJAS ESPECÍFICAS:** posibilidad de gestionar entornos con IP dinámica como DHCP y Wi-Fi. Permite el reconocimiento y control de identidad de usuario. Consola intuitiva a la hora de navegar, bien dimensionada, flexible y potente. Fácil despliegue, instalación, configuración y utilización. El mecanismo de actualización está bien dimensionado. Permite identificar el origen de las amenazas internas. Es útil frente a la gestión de amenazas combinadas. Permite tres modos de despliegue: transparente-pasarela-*proxy*, lo que facilita su distribución en una red corporativa genérica. Soporta entornos VLAN-802.1Q, autenticación y SSO con servidores LDAP/DA/Radius, encaminamiento dinámico y servidor NTP.
- ♦ **DOCUMENTACIÓN:** suficiente. Utiliza ficheros .pdf.
- ♦ **ESTRUCTURACIÓN DE LA HERRAMIENTA:** 1) *Appliances* hardware de seguridad Cyberoam CR100ia UTM; 2) Software multifuncional.
- ♦ **CALIFICACIÓN FINAL:** herramienta de seguridad de red contra amenazas internas y externas del tipo *appliance* de seguridad UTM basada en identidad, de buena escalabilidad. Integra un completo conjunto de funcionalidades de tipo *firewall*, VPN, pasarelas anti-virus, anti-spyware, anti-spam, anti-phishing/anti-pharming, IDS/IPS, filtrado de contenidos-aplicaciones, gestión multi-enlace, gestión del ancho de banda, generación de informes, etc. Se controla y administra desde una consola centralizada bien dimensionada basada en web. Incluye diversas funcionalidades adicionales como CARL y Analytical Tool, esta última encargada de comprobar el estado de funcionamiento del sistema y poder diagnosticar posibles problemas. Soporta diversos mecanismos de tolerancia a fallos y alta disponibilidad. A nivel de *firewall*, las reglas se basan en una combinación de zonas origen y destino, dirección IP y servicio. Soporta NAT transversal y H.323. Las acciones *firewall* abarcan globalmente el control basado en política para *IDS/IPS*, filtrado de contenidos, anti-virus/anti-spyware, anti-spam/anti-phishing, gestión del ancho de banda y planificación de acceso. Permite bloquear satisfactoriamente aplicaciones P2P como Skype, *keyloggers*, actividades *phone home* y *proxies* de anonimato como *ultra-surf*.

## EQUIPO DE EVALUACIÓN

DIRECTOR:  
**Prof. Dr. Javier Areitio Bertolín**  
 Catedrático de la Facultad de Ingeniería. ESIDE.  
 Director del Grupo de Investigación Redes y Sistemas.  
**UNIVERSIDAD DE DEUSTO**

