



La serie NG de Cyberoam está conformada por los equipos de siguiente generación para la seguridad de redes, los cuales incluyen funciones y desempeño de seguridad que se requiere para las redes del futuro. La serie NG para MYPES ofrece a las oficinas pequeñas y/o sucursales "los UTMs más rápidos que jamás hayan sido diseñados para este segmento". La combinación del mejor hardware de su tipo, junto con un software igualmente superior, hace posible que la serie NG pueda ofrecer velocidades de rendimiento inigualables, en comparación con cualquier otro equipo UTM para este segmento del mercado. Esto garantiza que puedan soportar las tendencias futuras de las TIC en las organizaciones, como Internet de alta velocidad y un creciente número de dispositivos móviles como herramienta de trabajo en las organizaciones, ofreciendo seguridad compatible con requerimientos futuros para las redes de las oficinas pequeñas.

Con la serie NG de Cyberoam, los negocios obtienen Seguridad, Conectividad y Productividad garantizadas. La Tecnología Capa 8 de Cyberoam considera la identidad del usuario como la Capa 8 o Capa HUMANA en los niveles de protocolos. Esta tecnología incorpora la identidad del usuario a la seguridad; lo cual, hablando de Oficinas Pequeñas, agrega velocidad a la seguridad de la organización al ofrecer visibilidad instantánea de la fuente de los ataques por nombre de usuario en lugar de únicamente la dirección IP. La arquitectura de seguridad extensible de Cyberoam (ESA por sus siglas en inglés) se adapta fácilmente a las mejoras en las funciones que se puedan ir desarrollando de forma rápida y con el mínimo esfuerzo, ofreciendo seguridad preparada para el futuro de las organizaciones.

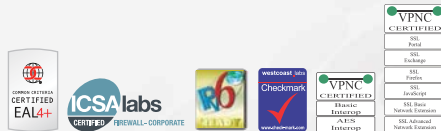
### La serie NG para MYPES

Ofrece "los UTMs más rápidos creados para las MYPE".

La tecnología de Cyberoam denomina la **Capa 8** como la "Identidad del Usuario" en los niveles de protocolos.

C8	USUARIO	
C7	Aplicación	
C6	Presentación	ASCII, EBCDIC, ICA
C5	Sesión	L2TP, PPTP
C4	Transporte	TCP, UDP
C3	Red	192.168.1.1
C2	Enlace de Datos	00-17-BB-8C-E3-E7
C1	Física	

El UTM de Cyberoam le brinda Seguridad desde la Capa 2 hasta la Capa 8 utilizando políticas basadas en la identidad del usuario.



## Las características de los equipos UTM de Cyberoam garantizan Seguridad, Conectividad, Productividad

### Seguridad

#### Seguridad de Red

- Firewall
- Sistema de Prevención de Intrusos

#### Seguridad de Contenido

- Anti-Virus/Anti-Spyware
- Anti-Spam (Entrante/Saliente)
- Seguridad de Contenido HTTPS/SSL

#### Seguridad Administrativa

- GUI de Siguiete Generación



### Conectividad

#### Continuidad del Negocio

- Administración de Múltiples Enlaces
- Alta Disponibilidad

#### Disponibilidad de la Red

- VPN
- Conectividad 3G/4G/WiMAX

#### Conectividad preparada para el Futuro

- Logotipo Gold "IPv6 Ready"



### Productividad

#### Productividad de los Empleados

- Filtrado de Contenido
- Archivo y Control de Mensajería Instantánea

#### Optimización de Recursos TI

- Administración de Ancho de Banda
- Detección de Tráfico
- Visibilidad y Control de Aplicaciones

#### Productividad del Administrador

- GUI de Siguiete Generación



## Interfases

Puertos de Cobre GbE	3
Puertos Personalizables: Internal/DMZ/WAN	Si
Puertos de Consola (RJ45)	1
Puertos USB	2

## Rendimiento del Sistema\*

Firewall Throughput (UDP) (Mbps)	1,000
Firewall Throughput (TCP) (Mbps)	750
Nuevas sesiones por segundo	3,500
Sesiones concurrentes	60,000
IPSec VPN Throughput (Mbps)	110
Número de Túneles IPSec	50
SSL VPN Throughput (Mbps)	50
Anti-Virus Throughput (Mbps)	180
IPS Throughput (Mbps)	140
UTM Throughput (Mbps)	80

## Firewall de Inspección Profunda

- Firewall Capa 8 (Identidad del Usuario)
- Múltiples Zonas de Seguridad
- Criterios de Control de Acceso (ACC) - Identidad de Usuario, Zona Origen y Destino, dirección MAC e IP, Servicio
- Políticas UTM - IPS, filtrado de contenido, filtrado de aplicaciones, Anti-Virus, Anti-Spam y Administración de Ancho de Banda
- Control y Visibilidad de Capa 7 (Aplicaciones)
- Programación de Acceso
- Políticas basadas en NAT de Origen y Destino
- H.323, SIP NAT Transversal
- 802.1q soporte VLAN
- Prevención de ataques DoS & DDoS
- Filtrado MAC & IP y prevención de spoofing

## Anti-Virus y Anti-Spyware Perimetral

- Detección y Eliminación de: Virus, Gusanos, Troyanos
- Protección contra Spyware, Malware, Phishing
- Actualización automática de base de datos de firmas de virus
- Analiza HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IM, Túneles VPN
- Personaliza exploración por usuario individual
- Área de cuarentena auto-servicio
- Explora y entrega por tamaño de archivo
- Bloquea por tipos de archivo
- Agrega renuncia de responsabilidad / firma

## Anti-Spam Perimetral

- Escaneo de correo Entrante
- Lista negra en tiempo real (RBL), verificación encabezado MIME
- Filtro basado en encabezado de mensajes, tamaño, remitente, destinatario
- Etiquetado de línea de asunto
- Lista blanca/lista negra de dirección IP
- Redirige correos spam a una dirección de correo dedicada
- Filtrado de spam con base en imágenes mediante tecnología RPD
- Protección contra brote de virus Hora Cero
- Área de cuarentena auto-servicio
- Resumen de notificaciones de Spam
- Filtrado de spam basado en Reputación IP

## Sistema de Prevención de Intrusos

- Firmas: Predeterminado (4500+), Personalizado
- Políticas IPS: Múltiple, Personalizado
- Creación de políticas basada en usuario
- Actualizaciones automáticas en tiempo real desde redes CRProtect
- Detección de Anomalía de Protocolo
- Prevención de ataque DDoS
- IPS-SCADA - Cuenta con categorías pre-definidas para ICS y firmas SCADA

## Filtrado Web

- Base de datos por categoría Web integrada
- Bloqueo URL, palabra clave, tipo
- Categorías: Predeterminado (82+), Personalizado
- Protocolos soportados: HTTP, HTTPS
- Bloqueo de programas maliciosos, phishing, pharming URLs
- Control de acceso basado en horarios
- Bloqueo personalizado de mensajes por categoría
- Bloqueo de Applets Java, Cookies, ActiveX
- Cumplimiento CIPA
- Control de fuga de datos vía HTTP, HTTPS

## Filtrado de Aplicaciones

- Base de datos de categoría de aplicaciones integrada
- Soporta más de 2000 aplicaciones
- Control de acceso basado en horarios

- Bloqueo de
  - Proxy y Túnel
  - Transferencia de Archivos
  - Redes Sociales
  - Streaming Media
  - Almacenamiento y Respaldo
- Visibilidad Capa 7 (Aplicaciones) y Capa 8 (Identidad Usuario)
- Protección para Redes SCADA
  - Filtrado basado en firmas SCADA-ICS para protocolos
    - Modbus, DNP3, IEC, Bacnet, Omron FINS, Secure DNP3, Longtalk
  - Control de varios comandos y funciones

## Red Privada Virtual

- IPSec, L2TP, PPTP
- Codificación - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Algoritmos Hash - MD5, SHA-1
- Autenticación - Clave pre-compartida, certificados digitales
- IPSec NAT Transversal
- Detección de Dead Peer y soporte PFS
- Grupos Diffie Hellman - 1,2,5,14,15,16
- Soporte de Certificado de Autoridad Externo
- Facilidad de exportar configuración de VPN para Usuarios Remotos (Road Warrior)
- Soporte de nombre de dominio para estaciones de trabajo del túnel
- Redundancia de conexión VPN
- Soporte Overlapping Network
- Soporte VPN Hub & Spoke

## SSLVPN

- Túnel TCP & UDP
- Autenticación - Active Directory, LDAP, RADIUS, Cyberoam
- Autenticación de cliente multi-capas - Certificado, Nombre de usuario / Contraseña
- Refuerzo de políticas de usuario y grupo
- Acceso a la red - Túnel dividido y completo
- Acceso basado en navegador (Portal) - Acceso sin cliente
- Cliente de túnel SSLVPN ligero
- Control de acceso granular a recursos de red de la empresa
- Controles administrativos - Fin de sesión, Detección de Extremo Muerto, Personalización de portal
- Acceso a aplicaciones basado en TCP - HTTP, HTTPS, RDP, TELNET, SSH

## Control de Mensajería Instantánea (IM)

- Yahoo y Windows Live Messenger
- Exploración de virus para tráfico IM
- Permitir/Bloquear inicio de sesión
- Permitir/Bloquear transferencia de archivos
- Permitir/Bloquear Webcam
- Permitir/Bloquear chat uno a uno/grupo
- Bloqueo basado en contenido
- Registro actividades IM
- Archivo de documentos transferidos
- Alertas Personalizadas

## WAN Inalámbrica

- Soporte puerto USB 3G/4G y Wimax
- Enlace primario WAN
- Enlace respaldo WAN

## Administración de Ancho de Banda

- Administración de ancho de banda basada en aplicación e identidad del usuario
- Política de ancho de banda garantizada o incremental
- Detección de tráfico basado en aplicación e identidad del usuario
- Reporte de ancho de banda Multi WAN
- Restricción de ancho de banda basado en categorías Web

## Controles Basados en Identidad del Usuario y Grupo

- Restricción por hora de acceso
- Restricción por cuota de tiempo y datos
- Control de ancho de banda basado en asignación y comportamiento
- Controles P2P e IM basados en horarios

## Red

- Failover - Failover/Failback Automatizado, Multi-WAN failover, failover 3GModem
- Balanceo de carga basado en WRR
- Enrutamiento de políticas basado en Aplicación y Usuario

- Asignación de Dirección IP - Estático, PPPoE, L2TP, PPTP & Cliente DDNS, ProxyARP, servidor DHCP, DHCP relay
- Soporte para Proxy HTTP
- Ruteo Dinámico: RIP v1 & v2, OSPF, BGP, Reenvío Multicast
- Soporte Parent Proxy con FQDN
- Logotipo Dorado "IPv6 Ready"

## Alta Disponibilidad

- Activo-Activo
- Activo-Pasivo con Sincronización de Estado
- Failover profundo
- Alertas por cambio de estado del equipo

## Administración y Manejo del Sistema

- Asistente de configuración basado en Web
- Control de acceso basado en roles
- Actualizaciones de firmware vía Interfaz Web
- Interfaz compatible con Web 2.0 (HTTPS)
- Interfaz de estilos de color
- Interfaz de línea de comandos (Serial, SSH, Telnet)
- SNMP (v1, v2c, v3)
- Soporte multi-idioomas Chino, Hindi, Francés, Coreano
- Soporta Central Cyberoam (Opcional)
- Soporte Protocolo Hora de Red (NTP)

## Autenticación de Usuario

- Base de datos interna
- Integración de Active Directory
- Un solo inicio de sesión Windows automático
- Integración base de datos externa LDAP/RADIUS
- Soporte Thin Client -Microsoft Windows Server 2003, Servicios Terminal y Citrix XenApp - Novell eDirectory
- Soporte RSA SecurID
- Autenticación externa - Usuarios y Administradores
- Vinculación del Usuario con dirección MAC
- Servidores de autenticación Múltiples

## Registro/Monitoreo

- Monitoreo gráfico en tiempo real e histórico
- Soporte Syslog
- Visualizador de Registros - Firewall, IPS, filtrado Web, AntiVirus, AntiSpam, Autenticación, Sistema y Eventos Admin

## Cliente VPN IPsec\*\*

- Inter-operabilidad con los principales portales IPSec VPN
- Plataformas soportadas: Windows 2000, WinXP 32/64-bit, Windows 2003 32-bit, Windows 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 RC1 32/64-bit
- Importación de la configuración en la conexión

## Certificaciones

- Common Criteria - EAL4+
- Firewall ICASA - Corporativo
- Certificación Checkmark UTM Nivel 5
- VPNC - Interoperabilidad básica y AES
- Logotipo dorado "IPv6 Ready"

## Especificaciones del Equipo

Memoria	2GB
Compact Flash	4GB

## Cumplimiento

- CE
- FCC

## Dimensiones

LxAxP(pulgadas)	1.7 x 6 x 9.1
LxAxP(cms)	4.4 x 15.3 x 23.2
Peso	1.5 kg, 3.307 lbs

## Potencia

Voltage de Entrada	100-240 VAC
Consumo	13.2W
Disipación de Calor Total (BTU)	45

## Medio Ambiente

Temperatura de Operación	0 a 40 °C
Temperatura de Almacenamiento	-25 a 75 °C
Humedad Relativa (no condensación)	10 a 90%

\*El rendimiento del Antivirus, IPS y UTM se mide con base en el tráfico http según lineamientos RFC 3511 El rendimiento real puede variar dependiendo de los ambientes de tráfico de red reales.

\*\*Se requiere compra adicional.