

Ahora que el Internet de alta velocidad es una realidad en las empresas, aunado al creciente número de dispositivos por usuario y al uso de datos que se eleva a niveles exponenciales, los equipos de seguridad de siguiente generación deben estar acordes con las necesidades de las redes futuras. La serie NG de Cyberoam proporciona a las empresas un nuevo modelo de seguridad compatible con requerimientos futuros, al ofrecer velocidades de respuesta inigualable en equipos que son los mejores de su tipo, junto con software igualmente avanzado.

Serie NG para empresas Pequeñas y Medianas:

Los equipos de la serie NG para PYMES son los "UTMs más rápidos" que se han creado para este segmento.

Serie NG para Corporativos:

Los equipos de la serie NG para ofrecen un "Firewall de Nueva Generación (NGFW)" para corporativos, y brindan el más alto nivel en cuanto al desempeño que se requiere para las redes futuras de las instituciones.

Con la serie NG de Cyberoam, las empresas de cualquier segmento obtienen Seguridad, Conectividad y Productividad garantizadas. La tecnología de Capa 8 incorpora la seguridad a través de la identidad del usuario, añadiendo velocidad al sistema de seguridad de las empresas. La Arquitectura de Seguridad Expandible (ESA) de Cyberoam soporta mejoras futuras que se pueden desarrollar e implementar rápidamente con el mínimo de esfuerzo.



Cyberoam Serie NG : 15iNG, 25iNG, 25iNG-6P, 35iNG, 50iNG, 100iNG, 2500iNG
Cyberoam Serie NG Wireless : 15wiNG, 25wiNG, 25wiNG-6P, 35wiNG

Firewall de Inspección Profunda

- Firewall Capa 8 (Identidad del Usuario)
- Múltiples zonas de seguridad
- Criterios de control de acceso (ACC) – Identidad del usuario, zona origen y destino, direcciones IP y MAC, servicio
- Políticas UTM - IPS, filtrado Web, filtrado de aplicaciones, anti-virus, anti-spam y administración de ancho de banda
- Control y visibilidad Capa 7 (Aplicación) por horarios
- Acceso programable por horarios
- NAT origen y destino basada en polítics
- H.323, SIP NAT traversal
- Soporte 802.1q VLAN
- Prevención de ataques DoS y DDos
- Filtrado y prevención de spoof MAC e IP-MAC

Anti-Virus y Anti-Spyware Perimetral

- Detección y eliminación de virus, gusanos y troyanos
- Protección contra spyware, malware y phishing
- Actualización automática de base de datos de firmas de virus
- Identifica túneles en HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IM, VPN
- Personalización de escaneo a nivel de usuarios
- Acceso de autoservicio al área de cuarentena¹
- Escaneo y entrega según el tamaño de archivo
- Bloqueo por tipos de archivo
- Agrega acuerdos de contrato/firmas

Anti-Spam Perimetral

- Escaneo de correo entrante/saliente
- Verifica en listas negras (RBL) y encabezados de tipo MIME
- Filtro basado en encabezado de mensaje, tamaño, remitente, destinatario
- Etiqueta línea de asunto
- Redirige correo spam a dirección de eMail dedicada
- Filtrado de spam de imágenes con tecnología RPD
- Protección hora cero contra brote de virus
- Área de cuarentena autoservicio¹
- Lista negra/lista blanca de direcciones IP
- Notificación de spam mediante un resumen²
- Filtrado de spam basado en reputación de IP

Sistema de Prevención de Intrusos

- Firmas: predeterminada (4500+), personalizada
- Políticas IPS: múltiple, personalizada
- Creación de políticas basadas en usuario
- Actualizaciones automáticas en tiempo real desde redes CRProtect
- Detección anómala de protocolo
- Prevención de ataque DDos

Filtrado Web

- Base de datos por categoría Web integrada
- Bloqueo URL, palabra clave, tipo de archivo
- Categorías Web: predeterminada (82+), personalizada
- Protocolos soportados: HTTP y HTTPS
- Bloqueo de URLs con malware, phishing, pharming
- Distribución y jerarquización de ancho de banda basada en categorías
- Bloqueo de java applets, cookies, Active X
- Cumple con CIPA
- Control de fuga de información en cargas de archivos vía HTTP y HTTPS
- Control de acceso basado en horarios
- Mensaje de bloqueo personalizado por categorías

Filtrado de Aplicaciones

- Base de datos integrada por categorías de aplicaciones
- 11+ Categorías de aplicaciones, ejem. juegos, IM, P2P, proxy
- Control de acceso por horarios
- Bloqueo
- Aplicaciones P2P como Skype
- Proxies anónimos como: ultra surf
- Actividades "Phone home"
- Keylogger
- Visibilidad Capa 7 (Aplicaciones) y Capa 8 (Identidad del Usuario)

Web Application Firewall³

- Modelo protección positiva
- Tecnología única "Intuitive Website Flow Detector"
- Protección contra inyecciones SQL, Cross-Site Scripting (XSS), Session Hijacking, URL Tampering, Cookie Poisoning
- Soporte para HTTP 0.9/1.0/1.1
- Registros y reportes Intensivos
- Soporta de 5 a 200 servidores de aplicaciones

Red Privada Virtual (VPN)

- IPsec, L2TP, PPTP
- Encriptación - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Algoritmos Hash - MD5, SHA-1
- Autenticación: preshared key, certificados digitales
- IPsec NAT traversal
- Detección dead peer y soporte PFS
- Grupos Diffie Hellman - 1,2,5,14,15,16
- Soporte a certificados autoritativos externos
- Configuración exportable de conexión Road Warrior
- Soporte a nombres de dominio sobre túneles para el usuario final
- Redundancia de conexión VPN
- Soporte en Overlapping de redes
- Soporte Hub & Spoke VPN

SSL VPN

- Túnel TCP & UDP
- Autenticación – Directorio Activo, LDAP, RADIUS, Cyberoam
- Autenticación multi-nivel, certificados, nombre de usuario/contraseña
- Mejoras de ejecución de usuarios y grupos
- Acceso a la red: ilimitada o completa
- Acceso a (Portal) basado en navegador – Acceso sin cliente
- Cliente ligero de acceso VPN SSL
- Control granular de acceso a todos los recursos de la red de la empresa
- Controles administrativos – Sesión agotada, detección Dead Peer, personalización de portal
- Acceso a aplicaciones basado en TCP - HTTP, HTTPS, RDP, TELNET, SSH

Administración de Mensajería Instantánea (IM)

- Yahoo y Windows Live Messenger
- Exploración de virus para tráfico IM
- Permitir/Bloquear: inicio de sesión, transferencia de archivos, WebCam, chat uno a uno/grupos
- Bloqueo basado en contenido
- Registro de actividades IM
- Archivos transferidos
- Alertas personalizadas

WAN Inalámbrica

- Soporte USB puerto 3G/4G y WiMax
- Enlace WAN primaria
- Enlace WAN de respaldo

Administración de Ancho de Banda

- Administración de ancho de banda basado en aplicaciones e identidad del usuario
- Restricción de ancho de banda basada en categoría
- Política de ancho de banda garantizada y explotable
- Identificación de tráfico basada en aplicaciones e identidad el usuario
- Reporte Multi-WAN de ancho de banda

Controles basados en identidad del usuario y grupo

- Restricción de acceso por horas
- Restricción por tiempo y cuota, controlando P2P e IM
- Ancho de banda asignado y explotable basado en horarios

Networking

- Failover/Failback automatizado, Failover Multi-WAN / Módem 3G/4G
- Balanceo de carga basado en WRR
- Ruteo de política basado en aplicación y usuario
- Asignación de dirección IP - estática, PPPoE, L2TP, cliente PPTP y DDNS, proxy ARP, DHCP server, relay DHCP
- Soporta HTTP Proxy, Parent Proxy con FQDN
- Ruteo Dinámico: RIP v1 y v2, OSPF, BGP, Multicast Forwarding

Alta Disponibilidad⁴

- Activa-Activa
- Activa-Pasiva con sincronización de estado
- Failover sin perder sesiones de conexión
- Alertas de estatus de los equipos en caso de cambios

Administración y Manejo del Sistema

- Asistente para configuración basado en Web
- Control de acceso basado en roles
- Actualizaciones de Firmware vía Web UI
- Compatible con Web 2.0 UI (HTTPS)
- Diferentes estilos de color en la UI
- Interfase línea de comandos (Serial, SSH, Telnet)
- SNMP (v1, v2c, v3)
- Soporte multi-lenguaje: Chino, Hindi, Francés, Coreano
- Consola Central de Cyberoam (Opcional)
- Soporte NTP

Autenticación de Usuario

- Base de datos interna
- Integración Directorio Activo
- Soporte a SSO (Single Sign On) automático
- Integración de base de datos externa LDAP/RADIUS
- Soporte Thin Client - Microsoft Windows Server 2003 Terminal Services y Citrix XenApp
- Soporte RSA SecurID
- Autenticación externa – Usuarios y administradores
- User/MAC Binding
- Múltiples servidores de autenticación

Registro / Monitoreo

- Monitoreo gráfico en tiempo real e histórico
- Notificación vía eMail de reportes, virus y ataques
- Soporte Syslog
- Visualizador de registros - IPS, filtrado Web, anti-virus, anti-spam, autenticación, eventos, sistema y admin

Cyberoam i-View Reporting Integrado⁵ en el equipo

- Herramienta de reporte integrada basada en Web - Cyberoam-iView
- 1000+ reportes detallados
- 45+ reportes de cumplimiento de regulaciones
- Reportes históricos y en tiempo real
- Visualización de múltiples ventanas
- Panel de monitoreo específico, nombre de usuario, host, eMail ID
- Reportes - Seguridad, spam, virus, tráfico, violaciones de políticas, VPN, palabras clave en motor de búsqueda
- Reportes multi-formato - Tabular y gráfico
- Formatos exportables - PDF, Excel
- Programación automatizada de reportes

IPSec VPN Client⁶

- Inter-operabilidad con principales gateways 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, Windows 8 RC1 32/64-bit
- Soporte a importación de configuración de conexiones

Regulaciones

- CE
- FCC
- UL

Certificación

- ICSA Firewall - Corporate
- Certificación Checkmark UTM Nivel 5
- Interoperabilidad VPNC - Basic y AES
- Logo Dorado IPv6 Ready

^{1,2,3,4,5} Disponible en todos los modelos excepto CR15iNG

⁶ Se requiere compra adicional

| Especificaciones | 15iNG | 25iNG/6P | 35iNG | 15wiNG | 25wiNG/6P | 35wiNG |
|---|-------------------|-------------------|-------------------|---|-------------------|-------------------|
| Interfaces | | | | | | |
| Puertos Copper GbE | 3 | 4/6 | 6 | 3 | 4/6 | 6 |
| Puertos de consola (RJ45) | 1 | 1 | 1 | 1 | 1 | 1 |
| Puertos USB | 2 | 2 | 2 | 2 | 2 | 2 |
| Segmentos de Hardware Bypass | - | - | - | - | - | - |
| Puertos personalizables: Internal/DMZ/WAN | Sí | Sí | Sí | Sí | Sí | Sí |
| Rendimiento del Sistema* | | | | | | |
| Firewall Throughput (UDP) (Mbps) | 1,000 | 1,500 | 2,300 | 1,000 | 1,500 | 2,300 |
| Firewall Throughput (TCP) (Mbps) | 750 | 1,000 | 2,000 | 750 | 1,000 | 2,000 |
| Nuevas sesiones por segundo | 3,500 | 5,000 | 11,000 | 3,500 | 5,000 | 11,000 |
| Sesiones concurrentes | 60,000 | 150,000 | 350,000 | 60,000 | 150,000 | 350,000 |
| IPSec VPN Throughput (Mbps) | 110 | 210 | 250 | 110 | 210 | 250 |
| Túneles No. of IPSec | 50 | 100 | 150 | 50 | 100 | 150 |
| SSL VPN Throughput (Mbps) | 50 | 75 | 100 | 50 | 75 | 100 |
| WAF Protected Throughput (Mbps) | -NA- | 45 | 65 | -NA- | 45 | 65 |
| Anti-Virus Throughput (Mbps) | 180 | 300 | 525 | 180 | 300 | 525 |
| IPS Throughput (Mbps) | 140 | 200 | 350 | 140 | 200 | 350 |
| UTM Throughput (Mbps) | 80 | 110 | 210 | 80 | 110 | 210 |
| Autenticación de usuarios y nodos | Ilimitado | Ilimitado | Ilimitado | Ilimitado | Ilimitado | Ilimitado |
| Wireless LAN Integrada (Solamente para Serie WiNG) | | | | | | |
| Estándares Inalámbricos | | | | IEEE 802.11 a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, AES, PSK, 802.1x EAP) | | |
| Antena | | | | Desprendible 3x3 MIMO | | |
| Access Point | | | | Hasta 8 bssid | | |
| Potencia de Transmisión (EIRP) | | | | 11n HT40: +15dBm, 11b CCK: +15dBm, 11g OFDM: +15dBm | | |
| Receiver Sensitivity | | | | -68dBm at 300Mbps, -70dBm at 54Mbps, -88dBm at 6Mbps | | |
| Rango de Frecuencia | | | | 2.412 GHz - 2.472 GHz | | |
| Número de canales seleccionables | | | | 5.200 GHz - 5.825 GHz | | |
| Velocidad de Transmisión de Datos | | | | USA (FCC) - 11 channels, EU (ETSI) / Japan (TELEC) - 13 channels | | |
| | | | | 802.11n: hasta 450Mbps, 802.11b: 1, 2, 5, 11Mbps | | |
| | | | | 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps | | |
| Dimensiones | | | | | | |
| Largo x Ancho x Profundidad (pulgadas) | 1.7 x 6 x 9.1 | 1.7 x 6 x 9.1 | 1.7 x 6 x 9.1 | 1.7 x 6 x 9.1 | 1.7 x 6 x 9.1 | 1.7 x 6 x 9.1 |
| Largo x Ancho x Profundidad (cms) | 4.4 x 15.3 x 23.2 | 4.4 x 15.3 x 23.2 | 4.4 x 15.3 x 23.2 | 4.4 x 15.3 x 23.2 | 4.4 x 15.3 x 23.2 | 4.4 x 15.3 x 23.2 |
| Peso de la Unidad | 1.5 kg, 3.307 lbs | 2.3 kg, 5.07 lbs | 2.3 kg, 5.07 lbs | 1.5 kg, 3.307 lbs | 2.3 kg, 5.07 lbs | 2.3 kg, 5.07 lbs |

NA

| Especificaciones | 50iNG | 100iNG | 2500iNG |
|---|-------------------|-------------------|----------------------|
| Interfases | | | |
| Puertos Copper GbE | 8 | 8 | 14 |
| Puertos 1GbE SFP (Mini GBIC) | - | - | 4 |
| Puertos 1GbE SFP (Mini GBIC) | - | - | 2 |
| Puertos de Consola (RJ45) | 1 | 1 | 1 |
| Puertos USB | 2 | 2 | 2 |
| Segmentos de Hardware Bypass | 2 | 2 | 2 |
| Puertos personalizables: Internal/DMZ/WAN | Sí | Sí | Sí |
| Rendimiento del Sistema* | | | |
| Firewall Throughput (UDP) (Mbps) | 3,250 | 4,500 | 36,000 |
| Firewall Throughput (TCP) (Mbps) | 3,000 | 3,500 | 28,000 |
| Nuevas sesiones por segundo | 30,000 | 60,000 | 200,000 |
| Sesiones concurrentes | 1,000,000 | 1,250,000 | 3,500,000 |
| IPSec VPN Throughput (Mbps) | 400 | 450 | 8,000 |
| Túneles No. of IPSec | 200 | 250 | 3,000 |
| SSL VPN Throughput (Mbps) | 300 | 400 | 1,000 |
| WAF Protected Throughput (Mbps) | 300 | 500 | 1,000 |
| Anti-Virus Throughput (Mbps) | 1,000 | 1,400 | 6,000 |
| IPS Throughput (Mbps) | 750 | 1,200 | 6,000 |
| UTM Throughput (Mbps) | 550 | 750 | 4,000 |
| Autenticación de usuarios y nodos | Ilimitado | Ilimitado | Ilimitado |
| Dimensiones | | | |
| Largo x Ancho x Profundidad (pulgadas) | 1.7 x 14.6 x 17.3 | 1.7 x 14.6 x 17.3 | 3.54 x 17.52 x 23.23 |
| Largo x Ancho x Profundidad (cms) | 4.4 X 37.2 X 44 | 4.4 X 37.2 X 44 | 9 x 44.5 x 59 |
| Peso de la Unidad | 5 kg, 11.02 lbs | 5 kg, 11.02 lbs | 19 kg, 41.8 lbs |
| Potencia | | | |
| Voltaje de Entrada | 100-240VAC | 100-240VAC | 90-260VAC |
| Consumo | 99W | 99W | 258W |
| Disipación de Calor Total (BTU) | 338 | 338 | 881 |
| Suministro de Corriente Redundante | - | - | Sí |

Condiciones ambientales: Temperatura de Operación 0 °C a 40 °C Temperatura de Almacenamiento, -25 °C a 75 °C, Humedad Relativa (Sin condensar) 10% a 90%.

#Si está activado, desviará el tráfico sólo en caso de falla de corriente.

*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.



México D.F.: +52 (55) 1253.9200 | Monterrey: +52 (81) 1253.3900
 Guadalajara: +52 (33) 3540.5148 | 01 800 083 23 23
 Colombia: +57 (1) 381.9083 | Chile: +56 (2) 495.8591

