HOJA DE DATOS

NUBE FIREBOX

Extensión del Perímetro de Seguridad de WatchGuard a la Nube Pública

Es un hecho: los negocios están trasladando los servicios de los servidores locales hacia la nube. Los servidores de correo electrónico, los servidores web, los sistemas de gestión de relaciones con los clientes (CRM) y el almacenamiento de archivos se están trasladando a los servicios en la nube. Con tantos datos confidenciales que se están moviendo a la nube, la seguridad es esencial. La Nube Firebox de WatchGuard les permite a los administradores de la red extender el perímetro de seguridad para proteger a los servidores que se ejecutan en entornos de la nube pública.

Mientras que los proveedores de servicio en la nube son responsables de la seguridad de la nube, la protección de los datos confidenciales que se mueven desde y hacia la nube es su responsabilidad. Bajo este modelo de responsabilidad compartida, es fundamental que los administradores adopten cada medida posible para defender sus datos y desviar a los cibercriminales. La Nube Firebox de WatchGuard acerca la protección de los dispositivos líderes de Gestión Unificada de Amenazas (UTM) Firebox® de WatchGuard a los entornos de nube pública. La Nube Firebox puede implementarse con rapidez y facilidad para proteger a los servidores en una nube pública de ataques como botnets, ataques de scripts entre sitios, intentos de ataques de inyección de código SQL y otros vectores de intrusión.

CREADO PARA EL ENTORNO DE LA NUBE

Las empresas que transfieren sus aplicaciones y servicios a los servicios en la nube pública necesitan proporcionar el mismo nivel de seguridad que ofrecen en sus instalaciones. Firebox Cloud de WatchGuard ofrece servicios de seguridad de Gestión Unificada de Amenazas (UTM) para la detección de ataques y de malware y el filtrado de contenido web, que no están disponibles mediante otros proveedores de nube.

EXTENSIÓN DEL PERÍMETRO DE SEGURIDAD DE WATCHGUARD

Empresas pequeñas a medianas y distribuidas que tienen partes de su infraestructura ejecutándose en la nube pueden simplificar los esfuerzos de configuración y mantenimiento al extender su perímetro de seguridad con la Nube Firebox. El uso de la Nube Firebox junto con dispositivos físicos Firebox elimina la necesidad de familiarizarse con una línea de productos distinta para proteger una nube virtual privada (VPC).

VISIBILIDAD DE GRANDES DATOS

La Nube Firebox de WatchGuard, que es completamente compatible con WatchGuard Dimension. Una solución de visibilidad de seguridad de red apta para funcionar en la nube y una característica estándar en la plataforma de gestión unificada de amenazas insignia y de firewall de última generación de WatchGuard. Dimension brinda un conjunto de herramientas de generación de informes y visibilidad de grandes datos que identifica y extrae al instante tendencias y problemas de seguridad claves y brinda perspectivas que le permiten realizar acciones para establecer políticas importantes de seguridad en todos sus entornos.

MÚLTIPLES OPCIONES DE COMPRA

WatchGuard ha facilitado poner en funcionamiento su instancia de Nube Firebox al ofrecerle múltiples formas de comprar. Puede comprar una licencia propia Bring Your Own License (BYOL) a un Socio de WatchGuard para asegurarse de obtener beneficios de las habilidades y experiencia de su Socio de confianza. También es posible comprar una instancia medida (por ej., por hora) directamente en el mercado.

FUNCIONALIDADES Y BENEFICIOS

- Proteja con rapidez y facilidad las nubes virtuales privadas (VPC) de ataques como botnets, ataques de scripts entre sitios, intentos de ataques de inyección de código SQL y otros vectores de intrusión.
- Ahorre tiempo con una interfaz de usuario (UI) simplificada, creada para cada plataforma en la nube.
- Simplifique el proceso de establecimiento de conexiones seguras con su entorno de nube pública.
- Aumente la visibilidad con Dimension, la solución líder de visibilidad de la red de WatchGuard.
- Compre a su manera con las múltiples opciones de compra que se encuentran disponibles.

Microsoft Azure

awsmarketplace

Nombre del Modelo	Límite del núcleo de CPU	Total de usuarios	Sensores de Host de TDR	Firewall (Gbps)	VPN (Gbps)	Usuarios de VPN
Pequeño	2	50	50	2	0.4	50
Mediano	4	250	150	4	1.5	600
Grande	8	750	250	8	3	6.000
Extra Grande	16	1,500	250	Irrestricto	Irrestricto	10.000

Nota: Los valores de simplificación se aplican solamente al modelo de suscripción BOYL

FUNCIONALIDADES DE LA NUBE

Entornos admitidos	Amazon Web Services (AWS), Microsoft Azure (Solo para BYOL)
Modelos de suscripción	Bring Your Own License (BYOL), a pedido

FUNCIONALIDADES DE SEGURIDAD

Firewall	Inspección de paquetes con control de estado, inspección profunda de paquetes, firewall de proxy
Proxies de aplicación	HTTP, HTTPS, FTP, DNS, TCP/UDP, POP3, POP3S, SMTP, IMAPS
Protección contra amenazas	Ataques DoS, paquetes fragmentados, amenazas mixtas y más
Opciones de filtrado	Búsqueda Segura en Exploradores, Google para Negocios

GESTIÓN

Inicio de sesión y notificaciones	WatchGuard, Syslog, SNMP versión 2/versión 3
Interfaces de usuario	WebUI, Policy Manager (Azure), CLI
Generación de informes	WatchGuard Dimension incluye más de 100 informes predefinidos, resúmenes ejecutivos y herramientas de visibilidad

REDES ESTÁNDAR

QoS	8 colas de prioridad, Diffserv, puesta en cola estricta modificada
Asignación de dirección IP	DHCP (cliente)
NAT	Estático, dinámico, 1:1, IPSec traversal
Otras características	Enrutamiento estático, Independencia de puertos

VPN Y AUTENTICACIÓN

Cifrado	DES, 3DES, AES 128, 192 y 256 bits
IPSec	SHA-2, clave previamente compartida IKE, certificados de terceros, IKE v1/v2, Suite B
Autenticación	RADIOUS, LDAP, Directorio Activo de Windows, RSA SecurID, base de datos interna, SAML 2.0

ALTA SEGURIDAD EN TODOS LOS NIVELES

Con una arquitectura única para ser los productos de seguridad de red más efectivos, más rápidos y más inteligentes del mercado, las soluciones de WatchGuard brindan defensas profundas contra el malware avanzado, el ransomware, los botnets, troyanos, virus, sitios web (drive-by downloads), pérdida de datos, suplantación de identidad (phishing) y mucho más.

Funcionalidades y Servicios	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
Control de Aplicaciones	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway AntiVirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection & Response	✓	
DNSWatch	✓	
Access Portal	✓	
IntelligentAV	✓	
Dimension Command	✓	
Soporte	**Gold** (las 24 horas del día, los 7 días de la semana)	Estándar (las 24 horas del día, los 7 días de la semana)

UN PAQUETE. SEGURIDAD TOTAL.

La flexibilidad de la plataforma integrada de WatchGuard facilita la posibilidad de tener exactamente los componentes de seguridad que requiere su red de negocios. Ya sea que elija comenzar con los fundamentos básicos de seguridad o implementar un arsenal integral de defensas de red, contamos con paquetes de servicios de seguridad que se adaptan a sus requisitos.

ASISTENCIA Y GUÍA DE EXPERTOS

Se incluye una suscripción inicial a Soporte con cada modelo Firebox. El Soporte Estándar que se incluye en el Basic Security Suite brinda garantía de, actualizaciones de software y soporte técnico las 24 horas del día, los 7 días de la semana. Se incluye una actualización del nivel de soporte Gold en el Total Security Suite de WatchGuard.

Para conocer más detalles, comuníquese con su revendedor autorizado de WatchGuard o visite el sitio web www.watchguard.com.

VENTAS EN EE. UU. 1-800-734-9905 VENTAS INTERNACIONALES +1-206-613-0895 www.watchguard.com