HOJA DE DATOS

FIREBOX V

Seguridad de Red de Primer Nivel para su Entorno Virtual

Organizaciones de todos los tamaños están recurriendo a la virtualización para reducir costos y aumentar la eficiencia, disponibilidad y flexibilidad de sus recursos de TI. Pero la virtualización tiene su costo. Los entornos virtuales son difíciles de gestionar y vulnerables a las amenazas de seguridad. El Departamento de TI debe estar preparado. Hoy en día, las aplicaciones pueden asegurarse, los recursos pueden maximizarse y su departamento de TI puede beneficiarse de las recompensas de tener un sistema de gestión único y simplificado, sin riesgos de seguridad a la vista. WatchGuard FireboxV le acerca la seguridad de red de primer nivel al mundo de la virtualización. Con monitoreo en tiempo real, soporte multi-WAN y soluciones escalables para adaptarse a negocios de cualquier tamaño, sus entornos virtuales pueden ser tan seguros como su entorno físico.

Las soluciones virtuales de WatchGuard le ofrecen una flexibilidad de implementación inigualable. Puede elegir implementar una combinación de hardware y aplicaciones virtuales, que funcionan juntos y se administran desde una plataforma de gestión centralizada. Los dispositivos virtuales de WatchGuard presentan todos los servicios de seguridad y de red que se encuentran en nuestros dispositivos físicos y las situaciones previas de implementación pueden ser con clientes, departamentos o aplicaciones, para su infraestructura virtual.

VIRTUALICE EL FIREWALL DE PUERTA DE ENLACE TRADICIONAL PARA LOGRAR UNA FLEXIBILIDAD SIN PRECEDENTES

WatchGuard FireboxV protege no solo el perímetro físico del centro de datos, sino también el "extremo virtual". Ahora puede implementar políticas que protejan los datos de la base de datos corporativa de la infraestructura de mensajería o la información confidencial de RR. HH. de los datos financieros de otros departamentos, incluso cuando se ejecutan con los mismos servidores.

CONSOLIDE MÚLTIPLES FIREWALLS PARA OBTENER UNA EFICIENCIA DE GRAN IMPACTO

Proveedores de servicios: servicios de alojamiento web, en la nube y de seguridad administrada que pueden implementar múltiples instancias de FireboxV en servidores en el perímetro de sus centros de datos. Estos firewalls virtuales se mantienen aislados entre sí, por lo que pueden garantizarse los acuerdos de nivel de servicio (SLA) a cada usuario y un cambio en la configuración de uno no afecta a los otros. Y, sin embargo, el proveedor los puede gestionar al utilizar una única consola amigable al usuario.

ELIMINE COSTOS REDUNDANTES EN HARDWARE MIENTRAS ASEGURA LAS REDES VIRTUALES: CONSOLIDACIÓN DE SUCURSALES

Mientras que sucursales y departamentos más grandes consolidan los servidores locales (archivos, impresiones, voz y más) en un solo dispositivo, se puede implementar un firewall virtual en el servidor físico, aislando todo el tráfico de la red pública de Internet. Un túnel de VPN único puede proporcionar una ruta segura hacia los centros de datos corporativos o nubes privadas virtuales y, de esa forma, generar ahorros en cada ubicación sin comprometer la seguridad.

FUNCIONALIDADES Y BENEFICIOS

- Ejecute dispositivos virtuales en su entorno virtual
- Funcionalidades y Servicios líderes de Gestión Unificada de Amenazas (UTM) y de última generación (NGFW)
- WatchGuard Dimension™, una solución de visibilidad preparada para la nube pública y privada, convierte al instante datos sin procesar en inteligencia de seguridad; está incluido con la compra
- Fácil de descargar, habilitar, implementar y gestionar [consola centralizada, interfaz de usuario web, interfaz de línea de comandos (CLI)]
- Aprovecha la flexibilidad y disponibilidad de vSphere y Hyper-V
- Modelos múltiples para organizaciones de todos los tamaños
- Predios escolares, servicios en la nube/de alojamiento, consolidación de sucursales
- Implementación previa con clientes, departamentos o aplicaciones

Nombre del Modelo	Límite del núcleo de CPU	Total de usuarios	Sensores de Host de TDR	Firewall (Gbps)	VPN (Gbps)	Usuarios de VPN	VLANs
Pequeño	2	50	50	2	.4	50	50
Mediano	4	250	150	4	1.5	600	300
Grande	8	750	250	8	3	6.000	750
Extra Grande	16	1,500	250	Sin límite	Sin límite	10.000	1,500

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, and Explicit Proxy
Protección contra amenazas	Ataques DoS, paquetes fragmentados, amenazas mixtas y más
Opciones de filtrado	Búsqueda Segura en Exploradores, YouTube para Escuelas, Google para Negocios
Suscripciones de seguridad	Bloqueador de ATP, Servicio de Prevención de Intrusiones (IPS), Antivirus Gateway, WebBlocker, Control de Aplicaciones, Prevención de Pérdida de Datos, Reputation Enabled Defense, spamBlocker, Network Discovery, Detección y Respuesta ante Amenazas, Access Portal

GESTIÓN

Inicio de sesión y notificaciones	WatchGuard, Syslog, SNMP versión 2/ versión 3
Interfaces de usuario	Interfaz de usuario web, CLI para secuencia de comandos
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, IKEv1/v2, Suite B
Inicio de Sesión Único (SSO)	Windows, Mac OS X, sistemas operativos móviles, RADIUS, SAML 2.0
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)

MÚLTIPLES OPCIONES DE COMPRA

La flexibilidad de la plataforma integrada de WatchGuard facilita la posibilidad de tener exactamente los componentes de seguridad que requiere su red empresarial. 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, 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