Salix Networks

LION-150a

FIREWALL UTM VPN NG NTWORK APPLIANCE
on Intel® Xeon® processor

Funciones Principales Hardware

- Soporta Procesadores Intel® Atom® C2358
- Expandible con Módulos Salix Ethernet (Sólo LION-150c)
- Puerto Opcional de expansión trasero PCIe
- Puerto de Administración Consola IPMI
- Tamaño y Montaje Rackmount 1U Unidades

Especificación Técnica de Componentes Hardware

Procesador Central del Firewall UTM	
CPU Procesador Central	Intel Atom™ C2358 processor Codenamed “Rangeley” 64 bits
Frecuencia	N/A
BIOS	AMI BIOS 64Mb
Chipset	Intel C226 Chipset (Lynx Point PCH)
Memoria RAM	
Tecnolología	Dual-Channel DDR3 1066/1333/1600 MHz
Capacidad Máxima	16GB
Socket	2 x 240-pin DIMM
Tarjeta de Red Tipo Ethernet	
Controlador	6x Intel Marvell 88E1543
Modulos de RED NIC	2
Puertos LAN Itegrados	6x GbE RJ-45 ports
Tipo de Interface	RJ-45
Tecnología Bypass	2 pairs Gen.3 LAN Bypass
Almacenamiento Interno	
Tipo	SATA
Tamaño	2 x 2.5” HDD kit
Tipos Adicionales	1 x CF card Type II
Controlador	1 x CF card Type II
Dispositivos de Entrada y salida I/O	
Botón Reset	1 x reset button, software reset by default
Puerto de Consola	1 x RJ45
Puerto USB	2 x USB 3.0
Puerto IPMI	Si
Puerto de Admon	uno, Compartido con puerto IPMI
Bahías de Expansión	
PCIe	2x PCIEx8 parar NIC (PCIE Opcional)
PCI	N/A

Enfiamiento	
Procesador	Disipador de Calor Pasivo
System	2 x Ventiladores de Enfiramiento
Hambiente de Operación	
Rango de Temperatura	0 ~ 40ºC
Temp de Almacenamiento	-20 ~ 70ºC
Humedad relativa	5% ~ 90%, sin condensar
Componentes Diversos	
Pantalla LCD	NA
Tecnología Watchdog	Si
Reloj RTC con Batería Li	Si
Componentes Mecánicos	
Dimensiones (W x H x D)	431 x 44 x 468 mm
Peso	5 kg
Montaje	Rack mount
Fuente de Poder	
Tipo / Watts	270W Una Fuente or Redundantes 300W PSUs
Entrada Input	110~240V AC
Soporte de Sistema Firmware	
SalixWall OS	Unix Based Firmware

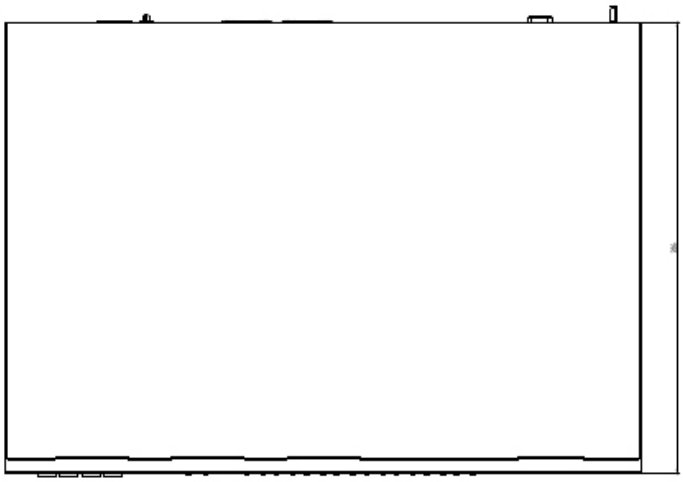
Ceertificaciones	
EMC	CE Emission, FCC Class A, RoHS
Safety	N/A

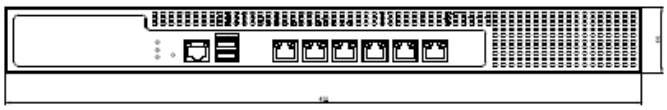
Firewall UTM Appliance

Vistas de Entrada y Salida I/O

- **A** Almacenamiento
- **B** Puerto de Consola
- **C** Puertos 2 x USB 3.0
- **D** Puertos 6 x GbE RJ45
- **F** Puerto Trasero Opcional PCIe
- **G** Cooling fans
- **H** Single Power Supply or Redundant

Dimensiones **431 x 44 x 468 mm**





Modulos Compatibles

Módulo	Puertos	Chipset	Bypass
Salix-SAL428A	4 GbE RJ45	Intel i350-AM4	2 Pairs G3

Salix Networks

LION-150a

FIREWALL UTM NG NTWORK APPLIANCE
Equipo de Seguridad Perimetral Custom

Funciones Básicas

- Bloqueo de Páginas Web, HTTP, HTTPS, Antivirus, etc.
- Balanceo de Cargas y Función Alta Disponibilidad HA.
- Bloqueo de Aplicaciones en Capa 7.
- Control de Banda Ancha con 3 Tipos de QoS
- Acceso Remoto VPN, Sitio a Sitio y Movil , IPSEC, L2TP, OpenVPN.
- Sistema de Detección de Intrusiones IDS/IPS

Especificaciones Técnicas Funciones y Operación

Capacidad del Equipo Throughput

Conexiones Máximas	* 6,00,0000
Rendimiento del firewall	* 4.5 Gbps
Rendimiento de DPI	* 620 Mpbs
Rendimiento antimalware	* 550 Mpbs
Rendimiento de IPS	* 1.3 Gbps
Conexiones DPI máx.	* 260,000
Nuevas conexiones/seg	* 60,000
Tuneles IPSEC site to site	* 50 Tuneles Activos

Modo de Operación

Modo puente de capa 2, Transparente	* Si
Modo pasarela/NAT	* Si

Motor de Inspección de Paquetes

Inspección bidireccional. Analiza el tráfico entrante y saliente de manera simultánea en busca de amenazas.
Inspección de un solo Paso. Analiza el tráfico entrante o saliente de manera una a la vez busca de amenazas,

Prevención de Intrusiones IDS/IPS

Protección basada en medidas correctivas. El sistema de prevención de intrusiones (IPS) perfectamente integrado utiliza las firmas y las demás medidas correctivas para analizar las cargas de paquete en busca de vulnerabilidades y ataques, lo que permite abarcar un amplio espectro de ataques y vulnerabilidades.
Abuso de protocolo. Identifica y bloquea ataques que se abusan de los protocolos para intentar eludir el IPS.
Tecnología antievasión. La normalización extensa de transferencia, la decodificación y las demás técnicas garantizan que ninguna Amenaza ingrese en la red sin ser detectada, mediante el uso de las técnicas de evasión entre las capas 2-7. .

Prevención de Amenazas

Antimalware de Puertas de Enlace. El motor del Lion 600c analiza todo el tráfico entrante, saliente y entre zonas en busca de virus, troyanos, registradores de pulsaciones de teclas y demás malware en archivos de longitud y tamaño ilimitados en todos los puertos, y todas las transferencias de TCP.
Actualizaciones de seguridad constantes. Las actualizaciones de nuevas amenazas se implementan en los firewalls automáticamente Mediante servicios activos de seguridad y no es necesario reiniciar ni interrumpir el trabajo.
Amplia compatibilidad de protocolos. Identifica protocolos Comunes como HTTP/S, FTP, SMTP, SMBv1/v2 y otros, que no envían datos en TCP sin procesar, y decodifica las cargas para realizar una inspección de malware, incluso si no se transfieren en puertos estándares y Conocidos.

Administración de Reportes y Monitoreo

Reporteador de Navegación. Reporte de páginas visitados, tiempo consumido y cantidad de banda ancha utilizada, por usuario, por dirección IP, por equipo.
Monitor en Tiempo Real. Monitor de utilización de Banda ancha en tiempo real, por usuario o por conexión IP.
Graficas de Consumo. Gráficas de consumo por usuario, poe aplicación, por calidad del enlace, etc.

Protección Antivirus y Antispyware

Protección Multicapa. Utiliza las capacidades del firewall como la primera capa de defensa del perímetro, en combinación con protección de extremo para bloquear los virus que ingresan en la red a través de equipos portátiles, unidades de almacenamiento en miniatura y otros sistemas no protegidos.
Protección contra spyware. La sólida protección antispyware analiza y bloquea la instalación de un conjunto integral de programas spyware en equipos de escritorio y portátiles antes de que transmitan datos confidenciales, lo que proporciona mejor rendimiento y mayor seguridad en el equipo de escritorio.

Red Privada Virtual VPN

VPN IPSec para conectividad sitio a sitio. La VPN IPSec de alto Rendimiento permite que el Firewall UTM Lion 600c actúe como un concentrador de VPN para miles de sitios amplios, sucursales u hogares. Permitiendo así unir sucursales de sitio a sitio o también puede conectar una a varios estaciones moviles o laptops a su oficina. Permitiendo conectar uno o varios firewalls Lion u otros firewalls que manegen el protocolo estandar IPSEC.
Acceso remoto de VPN SSL o cliente IPSec. Utiliza una tecnología VPN SSL sin cliente o un cliente IPSec fácil de administrar para obtener Acceso fácilmente a los correos electrónicos, los archivos, los equipos, los Sitios de intranet y las aplicaciones de las diversas plataformas como Voz sobre IP VoIP.
VPN basada en ruta. La capacidad de realizar enrutamiento dinámico en vínculos de VPN garantiza una actividad continua en el caso de que haya un error temporal de túnel de VPN, ya que vuelve a enrutar sin problemas el tráfico entre los extremos mediante rutas alternativas.
Maneja Otros Protocolos VPN. Ademas de IPSEC el firewall UTM Lion 600c majena VPNs topo Pptp, LPT2 y OpenVPN, para poder conectar cualquier dispositivo movil.

Firewalling y Networking

Inspección de paquetes con estado. Todo el tráfico de red se inspecciona Y se analiza, y cumple con las políticas de acceso del firewall.
Protección contra ataques DdoS/DoS. La protección frente a la inundación SYN proporciona una defensa contra ataques DOS mediante el uso del proxy de SYN nivel 3 y las tecnologías de lista negra de SYN nivel 2. Asimismo, proporciona protección frente a DOS/DDoS mediante la protección de inundación UDP/ICMP y los límites de tasas de conexión.
Varias Opciones de Implementación. Los dispositivos Lion serie 600 pueden implementarse en los modos tradicionales NAT-Routing, puente nivel 2 Bridge, modo cableado y conexión de red.
Compatibilidad con IPv6. El Protocolo de Internet versión 6 (IPv6) aún se encuentra en una etapa temprana para sustituir a IPv4. Con el frimware más reciente del firewall Lion, el hardware admitirá las implementaciones de filtrado.
Alta Disponibilidad. El firewall Lion 600c, admite la configuración en Alta disponibilidad en modo activo-activo o activo-pasivo.
MultiWAN. El firewall Lion 600c, permite el manejo de varias conexiones WAN ya sea pormedio de cada interfase de red o por medio de Configuraciones VLAN, esto permite administrar el tráfico que queremos utilizar por diferentes enlaces de Internet que tengamos, tambien permite la configuración Fail Over, si un enlace se cae, entonces la conexión a internet se turna a la siguente Interface WAN disponible.
Balanceo de Cargas. Esta funcionalidad permite balancear por un lado la Navegación a Internet si se cuentan con mas de una Conexión; por otro lado permite tambien el balanceo de dos o mas servidores que se esten publicando hacia Internet, como servidores WEB por ejemplo, eliminando la carga de trabajo de un solo servidor.

Firewall UTM Appliance

Salix Networks

LION-150a

FIREWALL UTM NG NTWORK APPLIANCE
Equipo de Seguridad Perimetral Custom

Funciones Básicas

- Bloqueo de Páginas Web, HTTP, HTTPS, Antivirus, etc.
- Balanceo de Cargas y Función Alta Disponibilidad HA.
- Bloqueo de Aplicaciones en Capa 7.
- Control de Banda Ancha con 3 Tipos de QoS
- Acceso Remoto VPN, Sitio a Sitio y Movil , IPSEC, L2TP, OpenVPN.
- Sistema de Detección de Intrusiones IDS/IPS

Especificaciones Técnicas Funciones y Operación

Resumen de Características del Sistema Operativo	Resumen de Características del Sistema Operativo
Firewall	• Inspección profunda de paquetes libre de reensamblaje • Inspección profunda de paquetes de SSL • Inspección de paquetes con estado • Modo discreto • Compatibilidad con tarjetas de acceso común (CAC) • Protección contra ataques DOS • Protección contra ataques UDP/ICMP/SYN • Descifrado SSL • Seguridad IPv6l
Inspección de Intrusiones IDS/IPS	• Análisis basado en firmas • Actualizaciones automáticas de firmas • Motor de inspección bidireccional • Capacidad de reglas granulares de IPS • Filtrado basado en reputación y GeoIP • Coincidencias de expresión regular"
Antimalware	• Análisis de malware basado en la transmisión • Antivirus para puerta de enlace • Antispyware de puerta de enlace • Inspección bidireccional • Sin límite de tamaño de archivo • Base de datos de malware en la nube"
Control de Aplicaciones	• Bloqueo de componente de aplicación • Administración de ancho de banda de aplicación • Creación de firma personalizada de aplicación • Prevención de fuga de datos • Generación de informes de aplicación mediante NetFlow/IPFIX • Seguimiento de la actividad del usuario (SSO)"
Filtrado de Contenido Web	• Filtrado URL • Tecnología antiproxy • Bloqueo de palabras clave • Categorías de clasificación de CFS para la • Administración del ancho de banda • Modelo de políticas unificado con control de aplicación • 76 categorías de filtrado de contenido • Autenticación propia o vis LDAP de Directorio Activo"
VPN	• VPN IPSec para conectividad sitio a sitio • Acceso remoto de VPN SSL y cliente IPSEC • Puerta de enlace redundante de VPN • Conexión móvil para iOS y AndroidTM • VPN basada en ruta (OSPF, RIP)"
Voz sobre protocolo de Internet (VoIP)	• Control granular de calidad de servicio • Administración del ancho de banda • DPI para el tráfico VoIP • Equipo selector H.323 y compatibilidad con proxy SIP"

Firewall UTM Appliance

Salix Networks

LION-150a

FIREWALL UTM NG NTWORK APPLIANCE
Equipo de Seguridad Perimetral Custom

Funciones Básicas

- Bloqueo de Páginas Web, HTTP, HTTPS, Antivirus, etc.
- Balanceo de Cargas y Función Alta Disponibilidad HA.
- Bloqueo de Aplicaciones en Capa 7.
- Control de Banda Ancha con 3 Tipos de QoS
- Acceso Remoto VPN, Sitio a Sitio y Movil , IPSEC, L2TP, OpenVPN.
- Sistema de Detección de Intrusiones IDS/IPS

Especificaciones Técnicas Funciones y Operación

Resumen de Características del Sistema Operativo	Resumen de Características del Sistema Operativo
Networking	• PortShield • Detección de redes en nivel 2 • IPv6 e IPV4 • Puertos con union LACP • Replicación de puertos • QoS de nivel 2 • Seguridad del puerto • Enrutamiento dinámico • Enrutamiento basado en políticas • Enrutamiento asimétrico • Servidor DHCP • Administración del ancho de banda • Alta disponibilidad activa/en espera con • Sincronización de estado en alta disponibilidad • Balanceo de la carga entrante/saliente • Puente Bridge L2, Modo NAT, DDNS • Routing RIP, RIP2, OSPF,BGP"
Administración y Monitoreo	• GUI web • Interfaz de línea de comandos (CLI) • Monitoreo SNMPv2/v3 • Informes Detallados por actividad y consumo • Administración y generación de informes centralizados • Visualización del tráfico en tiempo real • Administración de políticas centralizada • Inicio de sesión único (SSO) • Compatibilidad e Integración con Directorio Activo y servicios LDAP • Visualización de aplicación y ancho de banda • Administración de IPv4 e IPv6"

Firewall UTM Appliance