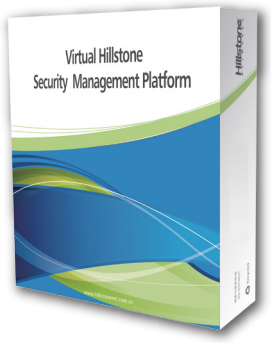
Plataforma Hillstone de Gestión de Seguridad



El Administrador de Seguridad de Hillstone mejora la seguridad de la red al permitir que las empresas puedan segmentar sus redes en múltiples dominios virtuales. Los dominios pueden estar basados en la geografía, por unidad de negocio o función de seguridad. Se proporciona la versatilidad necesaria para administrar la infraestructura de Hillstone al tiempo que simplifica la configuración, la aceleración de los ciclos de implementación, y la reducción de gastos de administración.

Detalles del Producto

Seguridad Multi-Dominio

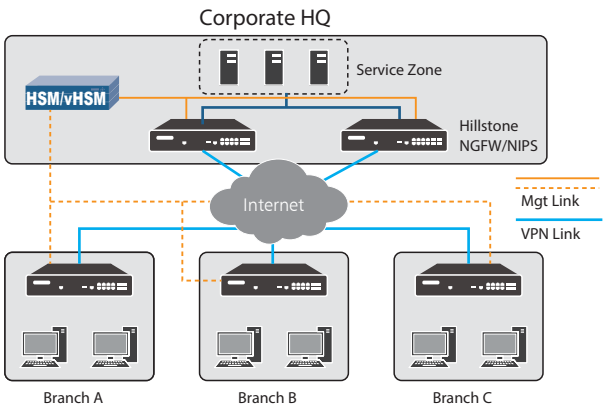
La mayoría de las empresas se enfrentan a los retos de seguridad cuando su negocio se extiende con oficinas ubicadas en varias regiones o países. Las organizaciones necesitan las herramientas para gestionar sus políticas de seguridad globales, mientras que permiten a los administradores regionales la gestión de dispositivos y usuarios en su lugar geográfico o división de negocio. El Administrador de Seguridad de Hillstone le permite al administrador principal de gestión de seguridad segmentar todo en múltiples dominios virtuales. Proporciona la seguridad, visibilidad y control requeridos por las organizaciones, a la vez que reduce los costes de administración, lo que simplifica la configuración y la aceleración de los ciclos de implementación.

SD-WAN

HSM sirve como administrador de seguridad centralizado en la solución SD-WAN de Hillstone, ofrece administración centralizada de políticas y visibilidad global, lo que permite la configuración e implementación con un clic de la red SD-WAN desde una consola central.

Aprovisionamiento y Administración Simplificados

El Administrador Hillstone de Seguridad Multi-dominio simplifica el aprovisionamiento de nuevos dispositivos. Permite que un administrador principal cree grupos de dispositivos para que otros administradores los supervisen y los administren. El administrador principal puede descargar políticas globales, actualizaciones de seguridad y actualizaciones de política, mientras que los administradores locales proporcionan las políticas para los dispositivos locales, usuarios y grupos. El administrador también puede bloquear las reglas y la configuración por objeto usadas para mejorar la seguridad y fiabilidad de la configuración del dispositivo.



Características

Administración Basada en Dominio
- Separa las redes en múltiples dominios virtuales basados en su ubicación, unidad de negocio o función de seguridad
- Define plantillas de políticas de seguridad global y asignarlas a los dominios virtuales
- Se pueden crear múltiples políticas de seguridad globales
- Los dominios virtuales comparten las políticas de seguridad globales y generan políticas separadas para usuarios/grupos y dispositivos específicos
- Los objetos compartidos pueden ser asignados y utilizados por varios dominios

Administración Basada en Roles
- Los administradores son asignados a dominios y dispositivos específicos
- La administración es basada en roles jerárquicos (administrador, operador, auditor) heredarán diferentes privilegios
- Varios administradores pueden trabajar en dominios separados de forma simultánea

Administración Centralizada
- Una sola consola de seguridad administra varios dominios
- Interfaz gráfica para ver, crear y gestionar todos los dominios
- Crea grupos de dispositivos para que gestionen los administradores
- Asigna políticas globales a múltiples dominios administrativos
- Crear administradores basados en funciones para la gestión de políticas y dispositivos
- El registro de dispositivos es soportado por IP, nombre de dominio o plantilla
- Detecta las políticas redundantes, objetos inútiles, y éxitos de política
- Crear instantáneas de política y políticas rollback
- Soporta asistente de políticas
- Administración centralizada de políticas de seguridad de ruta y de NAT
- Administración centralizada de políticas IPS/AV/SLB/URL/iQoS policies
- Gestion Centralizada de las contraseñas del firewall
- Servidor AAA, usuario, gestión de la configuración de roles
- Soporta la administración de dispositivos virtuales

Monitoreo Centralizado
- Monitoreo de todos los componentes del sistema multi-dominio, incluidos Hillstone NGFW, CloudEdge, NIPS, sBDS y ADC desde una ubicación.n central
- Monitorea la disponibilidad del dispositivo incluyendo la CPU, memoria, sesiones simultáneas, y el tráfico de cada dominio
- Monitorea la actividad y la Topologia de cada dispositivo registrado
- Visualiza el estado de la red y las alertas de los enlaces VPN
- Monitorea los eventos de seguridad de cada dominio, incluyendo el IP, URL, las aplicaciones y las amenazas
- Visualiza las tendencias de tráfico del dispositivo, el tráfico de usuarios, el tráfico de aplicaciones
- Supervisión del estado de actualización de licencias y firmas de los dispositivos
- Visualiza las 10 principales amenazas, y las 10 principales URLs accedidas, Estadísticas de la última hora de la amenaza, Estadísticas de la última hora de la alarma

Administración de Registros
- Registros producidos para el tráfico del dispositivo, la utilización de los recursos del sistema, los eventos de seguridad, la seguridad de los datos, el uso de la aplicación y la actualización del dispositivo
- Los registros se pueden filtrar por dispositivo
- Registros producidos para el sistema HSM
- Registros producidos para consultas históricas y copias de seguridad
- Soporte de reenvío de registros al servidor syslog de terceros

Administración de la Configuración
- IP del Dispositivo, nombre del dominio, y registro de la plantilla
- Número de versión del software del dispositivo
- Comparación de los archivos de configuración del dispositivo
- Configuración del archivo de backup y recuperación
- Soporte para bloquear el archivo de configuración del dispositivo
- La actualización de firmas de IPS, APP, AV, URL y Configuración de Administración Centralizada
- Soporte Firewall HA, incluida la gestión de clústeres HA para firewalls Hillstone en modos Activo-Pasivo / Activo-Activo / Activo-Par, relación de grupos HA y visualización de estado

Monitoreo de red VPN
- Monitoreo de topología VPN
- Monitoreo del estado de la red
- Alarma de interrupción de enlace

Sistema de Administracion
- Configuracion de Zona Horaria, Soporte de almacenamiento diario de Hora
- Reparacion automatica de Sistemas en HSM
- Configuracion de sincronizacion Prompt
- Proteccion de password de Sistema en HSM

Alta disponibilidad
- Admite la implementación de HSM HA, roles Maestro / Esclavo
- Modo de preferencia
- Monitorear / Sincronizar Log
- Sincronización automática y sincronización manual
- Alarma de conmutación Maestro / Esclavo

Despliegue Distribuido
- Modos autónomo / Maestro / Esclavo
- Registre hasta 16 dispositivos esclavos en un dispositivo maestro
- Alarma de memoria, alarma de CPU, alarma de disco y dispositivo esclavo, visualización de alarma fuera de línea en el dispositivo maestro

Informes Centralizados
- Más de 30 plantillas de informes incorporados
- Informes personalizados: informe de registro detallado y combinado con filtros personalizados por gravedad del evento, firewall, protocolo, IP de origen / destino, puerto de origen / destino, usuario, aplicación / servicio, interfaz de ingreso, número de regla / política, acción, motivo de cierre.
- Informes disponibles en formato HTML y PDF

Alertas
- Múltiples tipos de alertas incluyendo en tiempo real y alertas basadas en umbrales
- Alertas de eventos de seguridad del dispositivo
- Los vHSM no son compatibles con alertas SMS

IPv6
- Politica de Seguridad de cumplimiento en IPv6, NAT, configuracion y gestion de directorio
- Registro de recopilación y consulta en IPv6
- Monitoreo Presentacion y Recoleccion de datos en IPv6

Inspección del dispositivo
- Inspección manual, inspección regular, inspección inteligente
- Programación de tareas para inspección

Sistema de tickets
- Creación, procesamiento, revisión y despliegue de tickets.
- Importación y revisión de boletos por grupos
- Verificación de redundancia de políticas
- Identificación automática del dispositivo
- Proporcionar API para conectarse con otro sistema de tickets

Gestión SD-WAN
- VPN usando Redes Estrella y Redes en Malla
- Gestión de la red VPN
- Monitoreo del estado del dispositivo y del enlace
- Fácil implementación SD-WAN empresarial

vHSM
- Compatible con VMware WorkStation, EXSi, KVM
- Disponible en plataforma AWS

Especificaciones del Producto

Especificación del Aplicativo HSM

	HSM-500-D4	HSM-100-D4
Log Performance	5,000 EPS	2,500 EPS
Devices Supported (Default / Max.) (1)	15 / 500	15 / 150
Storage Capacity	4 TB	2 TB
Fixed I/O Ports	2 x GE	2 x GE
RAID Levels	RAID 5	RAID 0
Power Supply	Single/dual 550W	Single 450W
Height	1U	1U

Aplicativo Virtual Appliance (vHSM) Especificaciones

	15/25	15/100	15/500	15/1000
Log Performance	1,000 EPS	2,000 EPS	5,000 EPS	10,000 EPS
vCPU Requirement	4	8	18	24
Memory Requirement	4 GB	16 GB	32 GB	64 GB
Port Requirement	2 ports	2 ports	2 ports	2 ports
Hard Disk Requirement (Min.)	100 GB	2 TB	4 TB	8 TB
Virtual Environment Requirement	VMware Workstation/EXSi or KVM			

NOTAS:

(1) El número predeterminado de dispositivos que administra HSM solo es válido con la licencia de la plataforma HSM. Se puede extender al número máximo con la licencia de extensión HSM.

Version: EX-08.01-HSM4.6.0-1020-SP-01