

Plataforma Hillstone de Gestión de Seguridad

HSM-500-D4 / HSM-50 / vHSM



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

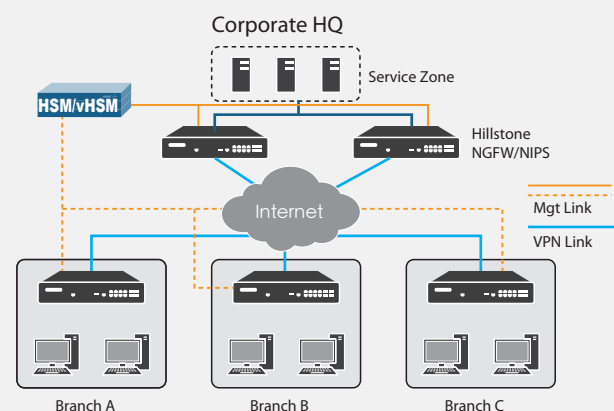
Seguridad Multi-Dominio

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. Múltiples gateways de seguridad, múltiples sitios que requieren diferentes políticas de seguridad y varios administradores pueden crear rápidamente un entorno de seguridad complejo. 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.

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 Principales

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
- Administración centralizada de políticas de seguridad de ruta y de NAT
- Administración centralizada de políticas IPS/AV/SLB/URL/iQoS policies
- Servidor AAA, usuario, gestión de la configuración de roles
- Soporta la administración de dispositivos virtuales

Monitoreo Centralizado

- Monitorea desde una ubicación central todos los componentes del sistema de dominios múltiples, incluyendo los Hillstone NGFW, NIPS, CloudEdge y WAF
- Monitorea la disponibilidad del dispositivo incluyendo la CPU, memoria, sesiones simultáneas, y el tráfico de cada dominio
- Monitorea la actividad y la Topología 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
- Monitorea el estado de la licencia para los dispositivos
- Visualiza las 10 principales amenazas, y las 10 principales URLs accedidas

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

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

Sistema de Administración

- Configuración de Zona Horaria, Soporte de almacenamiento diario de Hora
- Reparación automática de Sistemas en HSM
- Configuración de sincronización Prompt
- Protección 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
- 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

- Política de Seguridad de cumplimiento en IPv6, NAT, configuración y gestión de directorio
- Registro de recopilación y consulta en IPv6
- Monitoreo Presentación y Recolección de datos en IPv6

Especificaciones del producto

Especificación del Aplicativo HSM

Especificación	HSM-500-D4	HSM-50
Rendimiento Registro	5000EPS	2500EPS
Dispositivos Soportados (máximo)	15/500	15/100
Capacidad de Almacenamiento	4T	2T
Puertos I/O fijos	2xGE	2xGE
Niveles de RAID	RAID 5	RAID 0
Fuente de Alimentación	Mono/Dual 550W	Mono 250W
Altura	1U`	1U

Aplicativo Virtual Appliance (vHSM) Especificaciones

Capacidad de gestión (máximo)	15/25	15/100	15/500	15/1000
Rendimiento Registro	1000EPS	2000EPS	5000EPS	10000EPS
vCPU Requerido	4	8	18	24
Requerimiento de Memoria	4GB	16GB	32GB	64GB
Puertos Requerido	2 ports	2 ports	2 ports	2 ports
Requerimiento de Disco Duro	100GB	2T	4T	8T
Requerimiento de Entornos Virtuales	Vmware Workstation/EXSi or KVM			