Guía sobre los beneficios y capacidades de la solución de convergencia serie GCC

Guía de casos de uso del módulo de firewall serie GCC

GRANDSTREAM
CONNECTING THE WORLD

Introducción a la solución de convergencia GCC de Grandstream

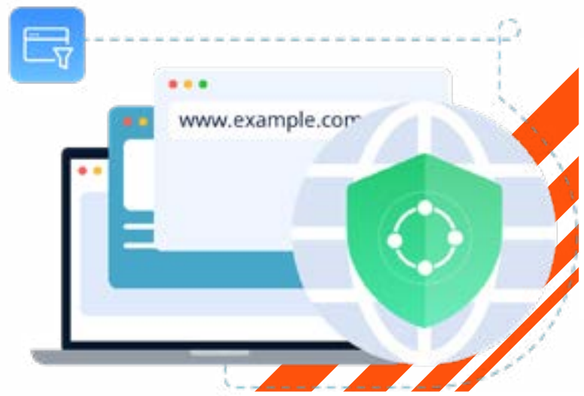
La serie GCC de dispositivos de convergencia de Grandstream es una línea revolucionaria de productos que proporciona una solución todo en uno que combina un router VPN, un IP PBX UCM, un switch de red administrable, o un AP Wi fi y firewall de próxima generación, todo en un solo dispositivo. Como resultado, este dispositivo sirve como un anclaje increíblemente rentable para crear una infraestructura de TI integral para escuelas, oficinas pequeñas, hospitales y casos de implementación similares.

En esta guía de casos de uso, analizaremos específicamente el módulo de firewall de la serie GCC, uno de los cuatro módulos que conforman las capacidades técnicas del dispositivo. El firewall de un GCC se puede aprovechar para proteger las redes de amenazas externas e internas. Desde defensas DoS hasta control avanzado de contenido y filtrado de aplicaciones, las características de este módulo giran en torno al mantenimiento de una infraestructura segura de TI.

Comprensión de las funciones principales del firewall GCC

El módulo de firewall viene con una variedad de características técnicas que se utilizan para crear una infraestructura de TI segura. A continuación se muestra una descripción general rápida de las funciones principales del firewall. Más adelante se proporciona un desglose más conciso de cada herramienta:

1. En primer lugar, se puede configurar un amplio conjunto de políticas de firewall para definir la forma en que el dispositivo GCC maneja el tráfico entrante y saliente por WAN, VLAN y VPN asignadas al dispositivo.



2. A continuación, en la sección Defensa de la seguridad, se pueden ajustar las defensas de denegación de servicio (DoS) y la configuración de protección de paquetes anormales (AP) para proteger una red contra flood attacks, paquetes anormales y evitar la suplantación de identidad.

3. Dentro de la sección Anti Malware, se puede configurar la biblioteca de firmas de virus de GCC y los usuarios pueden monitorear los archivos escaneados y los virus que la herramienta “Anti Malware” localiza y bloquea. Aquí también se pueden ajustar los protocolos de detección y la profundidad del escaneo.

4. El Sistema de Prevención de Intrusiones y el Sistema de Detección de Intrusiones son mecanismos de seguridad que monitorean el tráfico de la red en busca de actividades sospechosas e intentos de acceso no autorizados. Por último, las opciones de control de contenido del GCC ofrecen una amplia gama de herramientas del sistema para filtrar el tráfico según DNS, URL, palabras clave y aplicaciones.

Juntas, estas herramientas crean una solución de firewall integral que se suma con los otros módulos de la serie GCC para crear una infraestructura de TI protegida y segura.

Política de Firewall

Dentro de esta configuración, los usuarios pueden configurar las políticas generales de firewall basadas en WAN, VLAN y VPN del dispositivo GCC. Estas políticas definen exactamente cómo el dispositivo GCC inspeccionará y controlará el tráfico que entra y sale de la red.
La categoría “Política de firewall” contiene una amplia cantidad de herramientas que actúan como infraestructura para el firewall de la red, actuando para evitar el acceso no autorizado y protegiendo contra amenazas a la seguridad.
La configuración de políticas de reglas generales puede permitir a los usuarios hacer lo siguiente:

Política de entrada: Definir la decisión que tomará el dispositivo GCC sobre el tráfico iniciado desde la WAN o VLAN. Las opciones disponibles son: Aceptar, Rechazar y Eliminar.

Enmascaramiento de IP: habilitar el disfraz de IP. Esto disfrazará la dirección IP de los hosts internos.

MSS Clamping: habilitar esta opción permitirá que se negocie el MSS (**tamaño máximo de segmento**) durante la negociación de la sesión TCP.

Registrar tráfico descartar/rechazar: habilitar esta opción generará un registro de todo el tráfico que se ha descartado o rechazado.

Límite de registro de tráfico para descartar/rechazar: especificar el número de registros por segundo, minuto, hora o día. El rango es 1~99999999, si está vacío, no hay límite.

Las reglas de entrada dentro de esta categoría de configuración le permiten definir aún más el flujo de tráfico a través del dispositivo filtrando el tráfico entrante para especificar grupos de redes o puertos WAN y aplicando reglas de red. Un usuario puede configurar estas reglas para aceptar, rechazar o descartar el paquete. Las reglas de entrada ayudan a los usuarios a crear un flujo seguro de datos hacia los dispositivos al decidir qué conexiones de fuentes externas pueden acceder a la red, manteniendo la red protegida del acceso no autorizado y del tráfico malicioso que ingresa a la red. Esto es cada vez más importante para las redes que albergan información confidencial, como instituciones financieras y sectores de atención médica.

De manera similar a las reglas de entrada, también se pueden configurar reglas de salida dentro de la categoría “Política de firewall” para proteger la infraestructura de TI de una red. A la inversa, controla el flujo de tráfico saliente de un sistema, filtrando qué paquetes de datos pueden salir de la red. Esto ayuda a evitar que información confidencial abandone la red y protege contra posibles amenazas internas al bloquear conexiones salientes no autorizadas a destinos o servicios maliciosos. La configuración de reglas de salida es una característica crítica que puede evitar que programas maliciosos en dispositivos comprometidos envíen datos confidenciales fuera de una organización.

Por último, la sección “Política de firewall” contiene reglas de reenvío y configuraciones NAT avanzadas. El primero se puede configurar para permitir y bloquear el tráfico entre diferentes grupos e interfaces, como WAN, VLAN y VPN. Estas configuraciones pueden ayudar a segmentar una red para garantizar que solo los dispositivos/paquetes autorizados para acceder a los diversos grupos de la red puedan evitar el acceso no autorizado a sistemas y servicios como servidores, dispositivos de IoT e infraestructura crítica de TI. Las opciones NAT avanzadas en el dispositivo GCC6000 permiten mapeo SNAT y DNAT.

Defensa de seguridad

Pasando a la categoría de “Defensa de seguridad”, encontrará tanto defensas DoS como protección contra suplantación de identidad. Los ataques de denegación de servicio (DoS) son uno de los ataques cibernéticos más comunes que le pueden ocurrir a su organización, donde el agresor puede abrumar la red hasta el punto de impedir que los usuarios la utilicen así como sus servicios. Los ciberataques de suplantación de identidad son mucho menos llamativos que un ataque DoS. Pueden permitir que un hacker suplate a una fuente confiable en una red para obtener acceso a los servicios de esa red o difundir un malware potencial. Afortunadamente, los dispositivos GCC de Grandstream vienen con una variedad de capacidades para defenderse de estos dos ciberataques.

La configuración DoS de la serie GCC permite una amplia gama de valores que se pueden ajustar para monitorear, alertar y bloquear ataques de denegación de servicio. Cuando está activada, la configuración de “Flood attack” monitorea la cantidad de tipos de paquetes que fluyen a través del módulo del router del dispositivo y luego alerta a un administrador del sistema o comienza a bloquear esos paquetes cuando se cruza un umbral predefinido. El usuario puede configurar defensas contra flood attacks para paquetes TCP, UDP, ICMP y ACK. El equipo GCC también proporciona configuraciones de Defensa de paquetes anormales, otra variación de las defensas DoS. Los paquetes anormales ocurren cuando un ciber atacante envía intencionalmente paquetes con formato incorrecto a un dispositivo de destino, lo que hace que funcione incorrectamente debido a la incapacidad de procesar los paquetes de datos incoherentes. Un GCC puede bloquear una variedad de estos tipos de ataques, incluidos land attacks, smurfs, ataques “Ping of Death”, fragmentos ICMP/SYN y más.

Finalmente, la configuración de Protección ARP dentro de la categoría “Defensa de seguridad” proporciona a las redes varias contramedidas para diversas técnicas de suplantación de identidad. Un dispositivo de la serie GCC puede identificar y eliminar estratégicamente el riesgo de que se intercepte y suplante el tráfico al ofrecer configuraciones para evitar la suplantación externa de la información ARP y de la información IP. Esto evita que los hackers se hagan pasar por fuentes confiables y se infiltren en la red.

Anti Malware

La solución de convergencia GCC de Grandstream, viene con una sólida biblioteca de firmas de virus y antimalware que se actualiza continuamente, para mantener los dispositivos dentro de la red protegidos contra archivos y virus maliciosos. Esto ofrece protección antimalware, IDS/IPS, identificación y control de aplicaciones y seguridad web avanzada. A medida que los paquetes pasan a través de GCC, su herramienta Anti Malware estudiará los archivos y bloqueará los datos sospechosos, evitando que ingresen a la red. El nivel de profundidad con el que el firewall puede inspeccionar estos paquetes también se puede personalizar según el riesgo al que sea propensa la red.

Esta capacidad particular del firewall del GCC requiere una suscripción después de un periodo de prueba gratuito de un año para actualizaciones continuas de la firma del firewall, cuya información de precios se puede encontrar aquí. Si no se renueva un plan de firewall, el servicio de firewall seguirá siendo funcional/utilizable, pero la biblioteca de firmas permanecerá en la última actualización antes de su vencimiento. Puede ver nuestra página aquí para obtener más información sobre los planes antimalware y las capacidades de seguridad elevadas que vienen con una biblioteca de firmas actualizada continuamente.

Prevención de intrusiones

El Sistema de prevención de intrusiones (IPS) y el Sistema de detección de intrusiones (IDS) del módulo de firewall GCC son mecanismos de seguridad que monitorean el tráfico de la red en busca de actividades sospechosas e intentos de acceso no autorizados. El IDS identifica posibles amenazas a la seguridad mediante el análisis de paquetes y registros de red, mientras que IPS previene activamente estas amenazas bloqueando o mitigando el tráfico malicioso en tiempo real. IPS e IDS proporcionan un enfoque en capas para la seguridad de la red, ayudando a proteger contra ataques cibernéticos y salvaguardar la información confidencial. Las funciones de prevención de intrusiones del GCC también permiten configuraciones de Botnet. Una botnet es una red de computadoras comprometidas, infectadas con malware y controladas por un actor malicioso, que generalmente se utiliza para llevar a cabo ciberataques o actividades ilícitas a gran escala.

Una vez activado, IPS/IDS se puede configurar para notificar a un usuario del GCC sobre posibles amenazas de tráfico o para notificar y bloquear el tráfico. Se establece un nivel de protección de seguridad de bajo a extremadamente alto, con la opción de crear un nivel totalmente personalizado para la red. Cuanto mayor sea el nivel de protección, más reglas se seleccionarán entre las categorías “Ataques web”, “Anomalías de red” y “Archivos incorrectos”. Al seleccionar la opción “Personalizado”, un usuario puede elegir la herramienta de prevención de intrusiones específica que desea que utilice su módulo de firewall. La configuración de Botnet es bastante sencilla, donde las IP de Botnet y las herramientas de Nombre de dominio de Botnet se pueden configurar para que se desactiven, solo monitoreen o monitoreen y bloqueen.

Control de contenido

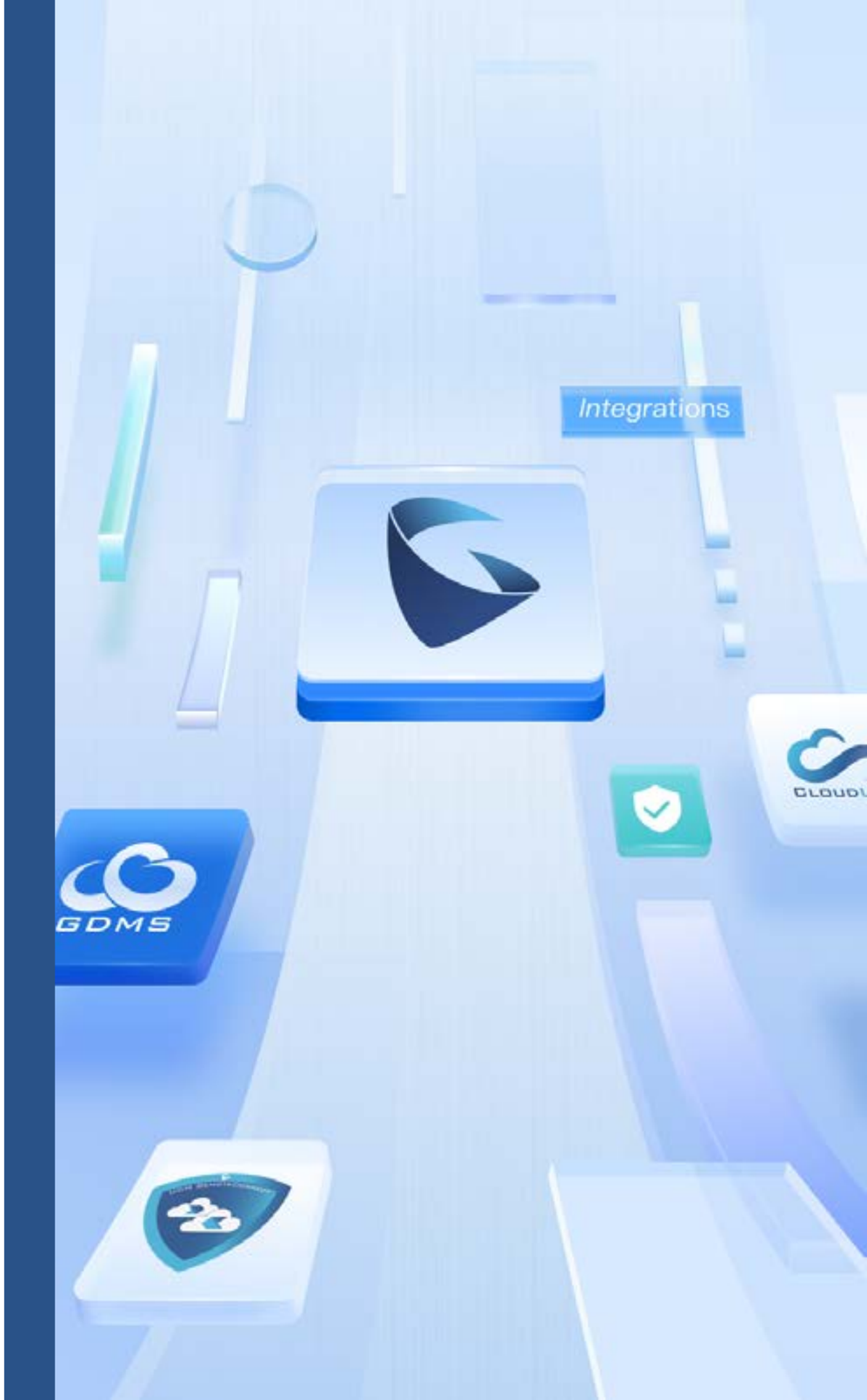
La categoría “Control de contenido” proporciona un conjunto sólido de herramientas que se pueden utilizar para la seguridad de la red. Las configuraciones de filtrado web, filtrado de aplicaciones y filtrado Geo-IP pueden permitir a los usuarios filtrar el tráfico del servicio según DNS, URL, palabras clave y tipo de aplicación. En conjunto, estas configuraciones le dan a la red la capacidad de ajustar cómo los usuarios acceden a la web y para qué pueden usarla.

Esto no solo puede evitar que los usuarios dentro de la red accedan inadvertidamente a sitios web maliciosos, correos electrónicos de phishing u otros tipos peligrosos de material en línea, sino también a servicios que se consideran inapropiados para utilizar dentro de la red de la organización. La función de control de contenido del módulo de firewall del GCC es particularmente efectiva para implementaciones que requieren un filtrado de tráfico más estricto, como escuelas, hoteles y redes que permiten el acceso público.

Con las herramientas de filtrado web, los usuarios pueden filtrar por URL, categoría de URL, palabras clave y biblioteca de firmas de URL.

Filtrado de URL: El filtrado de URL permite a los usuarios filtrar direcciones URL utilizando una coincidencia simple (nombre de dominio o dirección IP) o un comodín (por ejemplo, *ejemplo*).

Filtrado de categorías de URL: Los usuarios pueden filtrar por categorías más amplias del sistema, como “Juegos” y “Entretenimiento”. Las categorías se pueden personalizar mediante una amplia gama de opciones que se proporcionan en una interfaz fácil de usar.



Filtrado de palabras clave: El filtrado de palabras clave permite a los usuarios filtrar utilizando una expresión regular o un comodín (por ejemplo, *ejemplo*). Con el filtrado de palabras clave habilitado, cuando los usuarios intenten acceder a una URL que contenga esa palabra clave, recibirán una alerta de firewall y se les bloqueará el acceso.

Biblioteca de firmas de URL: Se mantiene una biblioteca de “URLs firmadas” validadas como característica de seguridad adicional para proporcionar una forma de firmas digitales, que actúa como un mecanismo de verificación para garantizar que las URLs no hayan sido manipuladas.

La herramienta de filtrado de aplicaciones proporciona a los usuarios del GCC una forma intuitiva de bloquear el acceso a categorías más amplias de sitios web y servicios o páginas específicas directamente. La solución de convergencia GCC de Grandstream tiene una amplia gama de categorías de acceso web predefinidas, y cada categoría contiene una lista de los sitios web más conocidos dentro de la categoría. Por ejemplo, si desea bloquear todos los servicios de transmisión en lugar de un solo sitio web, puede hacerlo fácilmente habilitando la herramienta de filtrado de aplicaciones, eligiendo la categoría de transmisión y eligiendo la opción “Bloquear”.

Esta parte del módulo del firewall de GCC viene con una opción de reconocimiento de IA que, cuando esté habilitada, permitirá que los algoritmos de aprendizaje profundo optimicen la precisión y confiabilidad de la clasificación de las aplicaciones. Juntas, estas características hacen de la herramienta de filtrado de aplicaciones una excelente opción para crear rápidamente una lista de bloqueo para evitar que los usuarios dentro de la red accedan a una amplia gama de páginas web.

Firewall integral para protección de red

Gracias a las herramientas de Política de firewall, Defensa de seguridad, Anti Malware, Prevención de intrusiones y Control de contenido integradas en el módulo Firewall del GCC, se puede construir una solución de seguridad integral para respaldar la infraestructura de TI que crean el resto de los módulos del GCC. Es una barrera natural que funciona en conjunto con las capacidades de enrutamiento, VPN, conmutación e IP PBX del GCC que, al final, proporciona un alto nivel de confianza de que la solución de red creada por el equipo GCC estará protegida.

Si está interesado en obtener más información sobre la solución de convergencia GCC, puede leer esta publicación de blog que brinda una descripción general de alto nivel de las capacidades del dispositivo aquí.

También proporcionamos una herramienta de demostración de GCC que puede utilizar para explorar la GUI y las capacidades de un GCC virtual en un entorno de demostración. Regístrese para acceder a la página aquí.