A Guide to the Benefits and Capabilities of the GCC Convergence Solution

GCC Series Firewall Module Use-Case Guide

GRANDSTREAM
CONNECTING THE WORLD

Grandstream's GCC Convergence Solution Introduction

Grandstream's GCC Series of Convergence Devices is a revolutionary line of products that provides an all-in-one solution that merges a VPN router, IP PBX, managed networking switch, and next-generation firewall all into one device. As a result, this device serves as an incredibly cost-effective anchor to create a comprehensive IT infrastructure for schools, small offices, healthcare practices, and similar deployment verticals.

In this use-case guide, we'll specifically discuss the firewall module of the GCC series, one of the four modules that make up the device's technical capabilities. A GCC's firewall can be leveraged to protect networks from external and internal threats. From DoS defenses to advanced content control and application filtering, this module's features revolve around maintaining a secure IT infrastructure.

Understanding the GCC Firewall's Core Features

The firewall module comes with an array of technical features that are used to create a secure IT infrastructure. Below is a quick overview of the primary functions of the firewall. A more concise breakdown of each tool is provided later on:

1. First, a wide set of Firewall Policies can be set to impact how the GCC device handles inbound and outbound traffic per WAN, VLAN, and VPN assigned to the device.

2. Next, in the Security Defense section, Denial of Service (DoS) defenses and Abnormal Packet (AP) protection settings can be adjusted to secure a network from flood attacks, abnormal packets, and prevent spoofing.

3. Within the Anti-Malware section, the GCC's virus signature library can be configured, and users can monitor scanned files and viruses that are located and blocked by the Anti-Malware tool. Detection protocols and scan depth can also be adjusted here.

4. The Intrusion Prevention System and Intrusion Detection System are security mechanisms that monitor network traffic for suspicious activities and unauthorized access attempts. Lastly, the GCC's Content Control options deliver a vast array of system tools to filter traffic based on DNS, URL, keywords, and applications.

Together, these tools create a comprehensive firewall solution that integrates with the other modules of the GCC series to create a protected and secure IT infrastructure.

Firewall Policy

Within this setting, users can configure the general firewall policies based on WAN, VLAN, and VPN of the GCC device. These policies define exactly how the GCC will inspect and control network traffic that is coming both in and out of the network. The Firewall Policy category contains a wide amount of tools that act as the infrastructure for the network firewall, acting to prevent unauthorized access and protecting against security threats. General rules policy settings can allow users to do the following:

Inbound Policy: Define the decision that the GCC device will take for the traffic initiated from the WAN or VLAN. The options available are Accept, Reject, and Drop.

IP Masquerading: Enable IP masquerading. This will masque the IP address of the internal hosts.

MSS Clamping: Enabling this option will allow the MSS (Maximum Segment Size) to be negotiated during the TCP session negotiation

Log Drop / Reject Traffic: Enabling this option will generate a log of all the traffic that has been dropped or rejected.

Drop / Reject Traffic Log Limit: Specify the number of logs per second, minute, hour, or day. The range is 1~99999999, if it is empty, there is no limit.

Inbound rules within this settings category enable you to further define traffic flow through the device by filtering incoming traffic to specify network groups or port WANs and applying network rules. A user can configure these rules to accept, deny, or drop the packet. Inbound rules help users create a safe flow of data to devices by deciding which connections from outside sources are allowed to access the network, keeping the network protected from unauthorized access and malicious traffic from entering the network. This is increasingly important for networks that house sensitive information such as financial institutions and healthcare verticals.

Similar to inbound rules, outbound rules within the Firewall Policy category can also be set in order to protect a network's IT infrastructure. Inversely, it controls the flow of outgoing traffic from a system, filtering which data packets may leave the network. This helps prevent sensitive information from leaving the network and protects against potential internal threats by blocking unauthorized outbound connections to malicious destinations or services. Outbound rule configuration is a critical feature that can prevent malicious programs on compromised devices from sending sensitive data outside of an organization.

Lastly, the Firewall Policy section contains Forwarding Rules and Advanced NAT configurations. The first can be set to allow and block traffic between different groups and interfaces, such as WANs, VLANs, and VPNs. These settings can help segment a network to ensure only the devices/packets authorized to access the network's various groups can prevent unauthorized access to systems and services such as servers, IoT devices, and critical IT infrastructure. Advanced NAT options on the GCC6000 device support both SNAT and DNAT mapping.

Security Defense

Moving onto the security defense category, you'll find both DoS defenses and spoofing protection. Denial of Service (DoS) attacks are one of the more common cyber attacks that can happen to your organization, where the assaulter can overwhelm the network to a point that prevents users from utilizing it and its services. Spoofing cyberattacks are much less conspicuous than a DoS attack. They can enable a hacker to impersonate a trusted source on a network to gain access to that network's services or spread potential malware. Luckily, Grandstream's GCC devices come with a variety of capabilities to defend against these two cyberattacks.

The GCC's DoS settings enable a wide range of values that can be adjusted to monitor, alert, and block Denial of Service attacks. When turned on, flood attack settings monitor the number of packet types flowing through the device's router module and then either alerts a system admin or begins blocking those packets when a predefined threshold is crossed. Flood attack defenses can be set by the user to TCP, UDP, ICMP, and ACK packets. The GCC also provides Abnormal Packet Defense settings, another variation of DoS defenses. Abnormal packets occur when a cyber attacker sends intentionally malformed packets to a target device, causing it to perform incorrectly due to the inability to process the incoherent data packets. A GCC can block a variety of these types of attacks, including Land Attacks, Smurfs, "Ping of Death" attacks, ICMP/SYN Fragments, and more.

Finally, ARP Protection settings within the Security Defense category provide networks with several countermeasures to various spoofing techniques. A GCC series device can strategically identify and eliminate the risk of having traffic intercepted and spoofed by offering configurations to prevent outside spoofing on ARP information as well as on IP information. This prevents hackers from potentially impersonating trusted sources and infiltrating the network.

Anti-Malware

Grandstream's GCC Convergence Solution comes with a robust anti-malware and virus signature library that is continually updated to keep devices within the network protected from malicious files and viruses. This offers anti-malware protection, IDS/IPS, application identification and control, and advanced web security.
As packets pass through the GCC, its Anti-Malware tool will study the files and blocks suspicious data, preventing them from moving into the network. The level of depth that the firewall can inspect these packets can be customized as well based on the risk that the network is prone to.

This particular capability of the GCC's firewall does require a subscription after a one-year free trial for continued updates to the firewall signature update, which pricing information can be found here. If a firewall plan is not renewed, the firewall service will still be functional/usable but the signature library will remain at the last update prior to expiration. You can view our page here to learn more about the anti-malware plans and the elevated security capabilities that come with a continually updated signature library.

Intrusion Prevention

The GCC firewall module's Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) are security mechanisms that monitor network traffic for suspicious activities and unauthorized access attempts. IDS identifies potential security threats by analyzing network packets and logs, while IPS actively prevents these threats by blocking or mitigating malicious traffic in real time. IPS and IDS provide a layered approach to network security, helping protect against cyberattacks and safeguard sensitive information. The GCC's intrusion prevention features also support Botnet settings. A botnet is a network of compromised computers infected with malware and controlled by a malicious actor, typically used to carry out large-scale cyberattacks or illicit activities.

Once activated, IPS/IDS can be set to notify a GCC user of potential traffic threats or both notify and block the traffic. A security protection level is set from low to extremely high, with the option of creating an entirely customized level for the network. The greater the protection level, the more rules that will be selected between Web Attacks, Network Anomalies, and Bad Files categories. By selecting the Custom option, a user can choose the specific intrusion prevention tool they would like their firewall module to use. Bot net settings are fairly straight forward, where Botnet IPs and Botnet Domain Name tools can be set to be deactivated, monitor only, or monitor and block.

Content Control

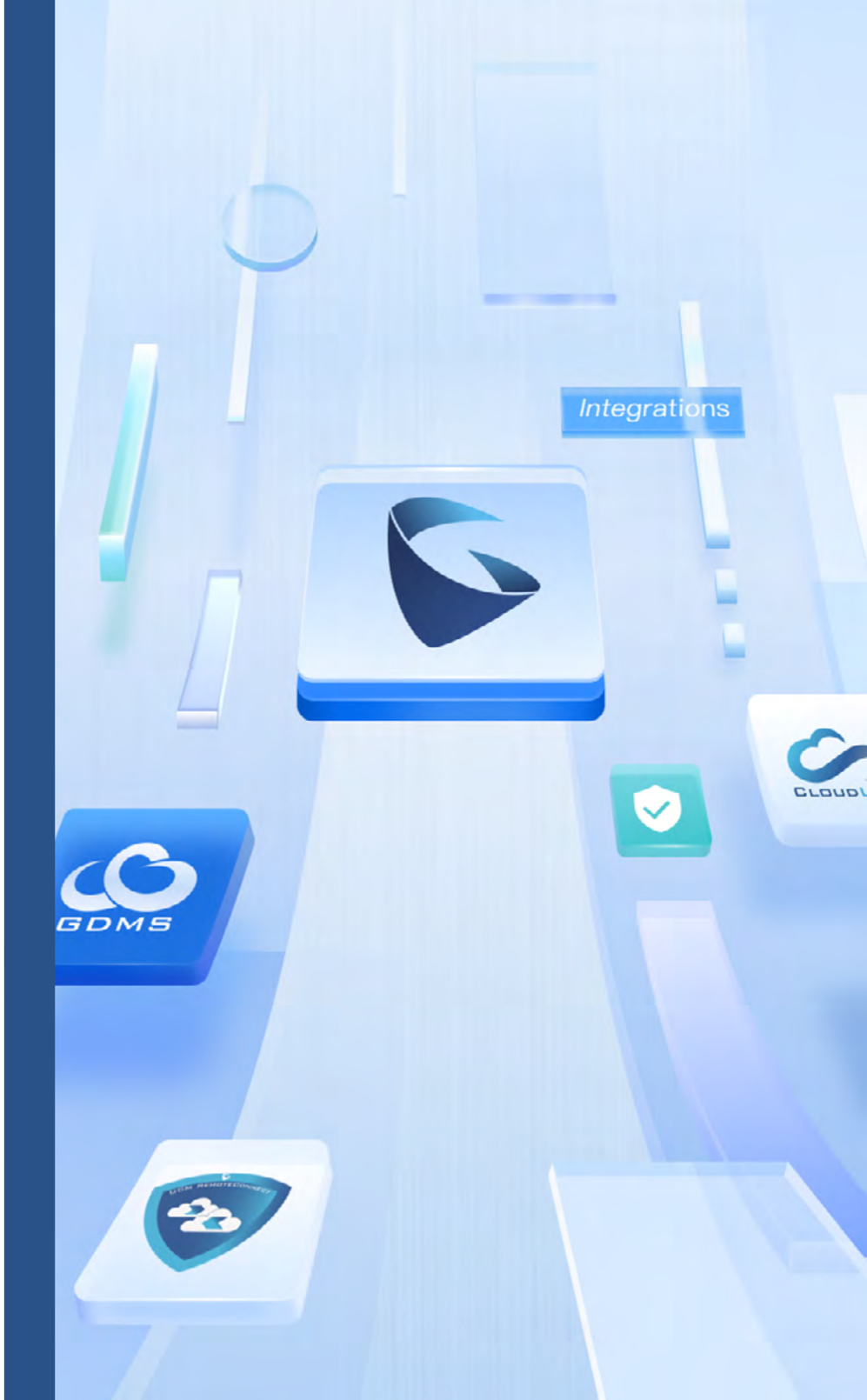
The Content Control category provides a robust set of tools that can be put to use for network security. Web Filtering, Application Filtering, and Geo-IP filtering settings can allow users to filter service traffic based on DNS, URL, keywords, and application type. Together, these settings give the network the ability to fine tune how users access the web and what they are allowed use it for.

This can not only prevent users within the network from inadvertently accessing malicious website, phishing emails, or other dangerous types of online material, but also services that are deemed inappropriate to utilize within the organization's network. The Content Control function of the GCC's firewall module is particularly effective for deployments that require more stringent traffic filtering, such as schools, hotels, and networks that allow public access.

With the Web Filtering tools, users can filter by URL, URL Category, Keywords, and a URL Signature Library.

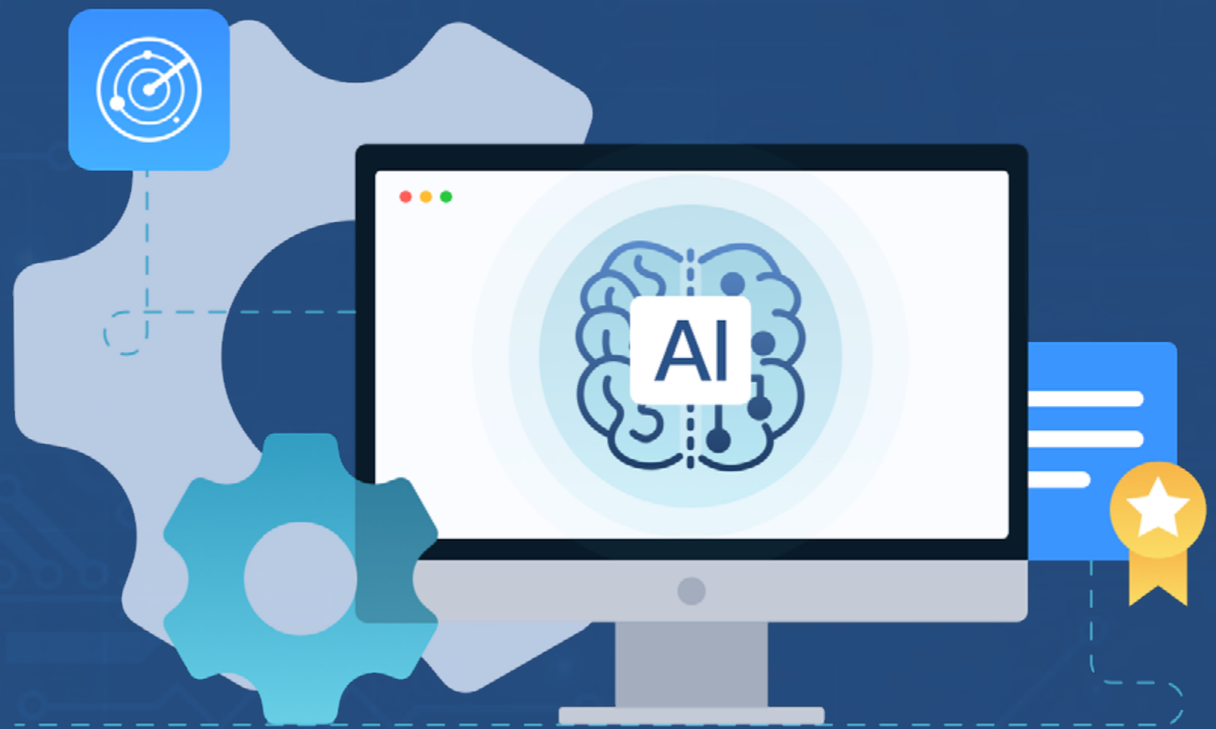
URL Filtering: URL filtering enables users to filter URL addresses using either a Simple match (domain name or IP address) or a Wildcard (e.g. *example*).

URL Category Filtering: Users can filter by broader system categories such as Gaming and Entertainment. Categories can be customized by a wide range of options that are provided on an easy-to-use interface.



Keywords Filtering: Keyword filtering enables users to filter using either a regular expression or a Wildcard (e.g. *example*). With keyword filtering enabled, when users attempt to access a URL that contains that keyword, they will be prompted with a firewall alert and have their access blocked.

URL Signature Library: A library of validated 'signed URLs' is kept as an added security feature to provide a form of digital signatures, acting as a verification mechanism to ensure URLs haven't been tampered with.



The Application Filtering tool provides GCC users with an intuitive way to block access to broader categories of websites and services or specific pages directly. Grandstream's GCC convergence solution has a wide range of predefined web access categories, and each category contains a list of the most known websites within the category. For example, if you want to block all streaming services rather than a single website, this can easily be done by enabling the application filtering tool, choosing the streaming category, and choosing the 'Block' option.

This part of the GCC's firewall module comes with an AI Recognition option that, when enabled, will allow deep learning algorithms to optimize the accuracy and reliability of application classification. Together, these features make the Application Filtering tool a great option to quickly assemble a block list to prevent users within the network from accessing a wide array of web pages.

Comprehensive Firewall for Network Protection

Thanks to the Firewall Policy, Security Defense, Anti-Malware, Intrusion Prevention, and Content Control tools built into the GCC's Firewall module, a comprehensive security solution can be constructed to support the IT infrastructure that the rest of the GCC's modules create. It is a natural barrier that works in tandem with the GCC's routing, VPN, switching, and IP PBX capabilities that, in the end, provides a high level of confidence that the network solution created by the GCC will be protected.

If you are interested in learning more about the GCC Convergence Solution, you can read this blog post that gives a high-level overview of the device's capabilities here.

We also provide a GCC Demo Tool that you can use to explore the GUI and capabilities of a virtual GCC in a demo environment. Sign up for access to the page here.