

# ENHANCE DATA SECURITY USING **SENSITIVITY LABELS**



---

## GAJ OS BULWARK FIRMWARE 4.44

### RELEASE NOTES

---

This firmware update introduces innovative features and enhancements designed to elevate data protection, security, and system usability. Key additions include the ability to create policies based on Microsoft Office Sensitivity Labels, enabling finer control over sensitive data and regulatory compliance, comprehensive FTP virus reporting for detailed monitoring and proactive threat management, and streamlined policy management directly from the DSF (Data Security Firewall) dashboard, simplifying administrative workflows. In addition to these enhancements, significant performance optimizations have been implemented to improve system reliability and efficiency. Several bugs have also been addressed to deliver a seamless and robust user experience. These advancements reflect GajShield's commitment to providing robust, cutting-edge security solutions tailored to the dynamic needs of our users.

### SENSITIVITY LABEL

Microsoft Office Sensitivity labels are a way to classify and protect sensitive data. They help manage and secure information by marking it with labels that indicate its sensitivity level. With this advanced feature in the GajShield firewall, you can configure policies to allow, monitor, or block documents based on their assigned sensitivity labels. By leveraging sensitivity labels, organisations can enforce precise control over sensitive information, ensuring it is safeguarded against unauthorised access and misuse. This robust functionality empowers users to enhance data security, maintain regulatory compliance, and prevent data breaches effectively

Add DLP Template	
Template Name	<input type="text"/>
Service	SMTP Mails
<b>SMTP Mails</b>	
SMTP Mails:	SMTP Mails
Filters:	
1.	Sensitivity Lab matches Confidential
and	
Alert	<input checked="" type="checkbox"/>
Log	<input checked="" type="checkbox"/>
Action	<input type="radio"/> allow <input type="radio"/> proceed <input checked="" type="radio"/> block
Criticality Label	<input checked="" type="radio"/> Not Critical <input type="radio"/> Low <input type="radio"/> Medium <input type="radio"/> High
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	



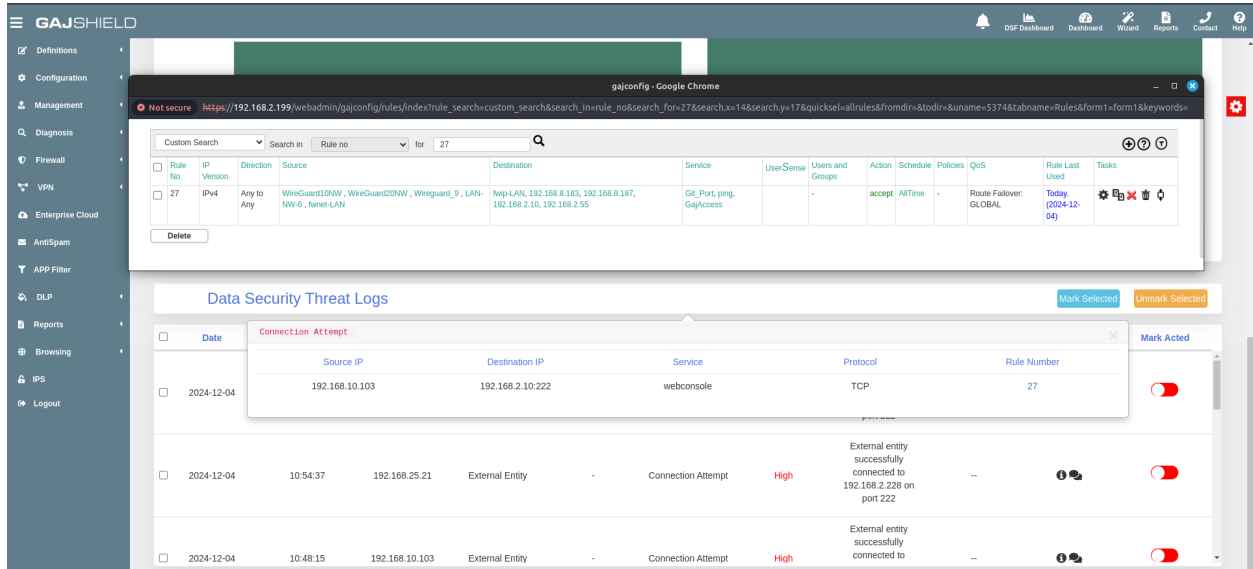
*This feature is only available to customers with an active DLP license on their GajShield firewall.*

### FRONTEND TAB AND CLI OPTION FOR FTP VIRUS LOGS

A new tab titled "FTP Virus Logs" has been introduced in the firewall under reports → Virus → FTP Virus Logs, allowing users to monitor and filter FTP virus traffic effectively. This feature enables the firewall to show the blocked files containing viruses, enhancing the overall security of the system. Additionally, these FTP virus logs are accessible via the command line.

## DSF DASHBOARD

This feature focuses on enhancing the functionality of the DSF Dashboard, with a particular emphasis on improving the visibility and management of Data Security Threat Logs. A key update includes displaying firewall policy rule numbers associated with the "Connection Attempt" category directly within the threat logs. Furthermore, these firewall policy rules can now be conveniently managed directly from the dashboard, streamlining administrative tasks and improving operational efficiency.



The screenshot displays the GAJSHIELD interface. At the top, a search bar shows a search for rule number 27. Below this, a table lists firewall rules. The main section shows "Data Security Threat Logs" with a table of connection attempts. A modal window is open over the first log entry, showing details for rule 27.

Rule No.	IP Version	Direction	Source	Destination	Service	User/Sense	Users and Groups	Action	Schedule	Policies	QoS	Rule Last Used	Tasks
27	IPv4	Any to Any	WireGuard10NW, WireGuard20NW, Wireguard_9_LAN-NW-6, Home-LAN	Wfp-LAN, 192.168.8.183, 192.168.8.187, 192.168.2.10, 192.168.2.55	Git_Prot, ping, GajAccess			accept	AllTime			Route Fallover: GLOBAL	Today (2024-12-04)

Date	Source IP	Destination IP	Service	Protocol	Rule Number	Mark Acted
2024-12-04	192.168.10.103	192.168.2.10:222	webconsole	TCP	27	<input type="checkbox"/>
2024-12-04	10:54:37	192.168.25.21	External Entity	External entity successfully connected to 192.168.2.228 on port 222	High	<input type="checkbox"/>
2024-12-04	10:48:15	192.168.10.103	External Entity	External entity successfully connected to	High	<input type="checkbox"/>

## GMAIL DOMAIN TAB

To prevent confusion in configuration and to facilitate ease of use and analysis of domain entries, the Trusted Domain and Gmail Domain configuration tabs have been separated. The Trusted Domain tab is visible in Browsing → Policy → Trusted Domain which exclusively displays trusted domains, while the Gmail Domain tab is dedicated solely to Gmail domains which is present under section DLP → DLP Policies → Gmail Domain. This separation helps keep everything organized, ensuring that each tab contains its relevant domain data, which streamlines management and enhances clarity for users.


## ENHANCEMENT

The FTP virus logs are now displayed under the "Top Viruses" section in Compliance Reports, enhancing security and providing greater visibility of the logs.


## BUG FIXES

---

- In the NAT rule involving queues, an issue was identified where the rule incorrectly referenced the original port instead of the NATed destination port. This issue has been resolved, and the rule now correctly utilizes the NATed destination port.
- In the Rules section under QoS and Routing, when either Link Load Balance or Link Route Failover is selected, the dropdown now correctly displays the Default and Non-NAT options, which were previously not visible in earlier versions.
- In the **Management** → **Updates** → **Signatures** tab, a gateway timeout during signature updates previously resulted in an "Oops" error page. This has been improved to display a clear and user-friendly message indicating the timeout condition.
- When WAN Failover is configured for IPv6, the Internet Status section on the dashboard was incorrectly displaying an error message, "WAN Failover service stopped," instead of the actual Internet status.

 **Call US :**  
Direct Line:  
+91 (22) 66607450  
Toll Free: 1800-2676-960

 **Email US :**  
[info@gajshield.com](mailto:info@gajshield.com)

 **Locate US :**  
4, Peninsula Centre, Dr. S. S. Rao  
Road, Parel, Mumbai, India - 400012