

DASHBOARD Firewall Page

<https://campus.barracuda.com/doc/73719533/>


























The **Firewall** page displays information about the firewall traffic and services related to networking and firewalling. To access the **Firewall** page, click the **DASHBOARD** tab and select the **Firewall** icon in the ribbon bar.

The elements on the **Firewall** page provide the following information if the features are enabled:

- Security Services
- Networking Services
- Top Threats
- Top Threat Vectors
- Advanced Threat Protection
- Connections
- Top Live Applications
- Top Allowed Applications / Top Blocked Applications
- Top Allowed Users
- Top Allowed URL Categories / Top Blocked URL Categories

Security Services

This element displays the status (enabled or disabled) of security-related services on the Barracuda CloudGen Firewall. Click the arrow icon next to a feature to access the configuration. For information on how to enable security services, see [How to Enable Application Control](#).

SECURITY SERVICES			
	Application Control	On	
	SSL Inspection	Off	
	URL Filter	Off	
	IPS	Off	
	Virus Scanner	Off	
	Advanced Threat Protection	Off	
	DNS Sinkhole	Off	
	File Content Scan	Off	
	Link Protection	Off - applied in 0 Rules	
	Safe Search	Off	
	Google Accounts	Off	
	RPC Tracking	Off	
	Forwarding Ruleset Complexity	7 Access 1 Application Rules; 20 Network Objects	
	Audit Log	Off	
	Guest Access	Off	

The **Security Services** element provides the following information:

























- **Application Control** – Shows if Application Control is enabled on the CloudGen Firewall. For more information, see [Application Control](#).
- **SSL Inspection** – Shows if SSL Inspection is enabled.
- **URL Filter** – Shows if the URL Filter is enabled. For more information, see [URL Filter](#).
- **IPS** – Shows if the Intrusion Prevention System (IPS) is enabled. For more information, see [Intrusion Prevention System \(IPS\)](#).
- **Virus Scanner** – Shows if the Virus Scanner service is enabled. For more information, see [Virus Scanner](#).
- **Advanced Threat Protection** – Shows if Advanced Threat Protection (ATP) is enabled. For more information, see [Advanced Threat Protection \(ATP\)](#).
- **DNS Sinkhole** – Replaces malicious domain responses by fake IP addresses. For more information, see [How to Configure DNS Sinkholing in the Firewall](#).
- **File Content Scan** – Scan files for malicious content. For more information, see [How to Configure File Content Filtering in the Firewall](#).
- **Link Protection** – Protect users from fraudulent links inside of plain-text and HTML emails. For more information, see [How to Configure Link Protection for Mail Security in the Firewall](#).
- **Safe Search** – Shows if Safe Search is in use in the Forwarding Firewall ruleset. For more information, see [How to Enforce Safe Search in the Firewall](#).
- **Google Accounts** – Shows if the firewall filters traffic to Google services based on the domain attached to the G Suite account. For more information, see [How to Configure Google Accounts Filtering in the Firewall](#).
- **RPC Tracking** – Shows if RPC tracking is enabled. For more information, see [RPC Firewall Plugin Modules](#).
- **Forwarding Ruleset Complexity** – Shows the number of access and application rules, as well

as the number of network objects.

- **Audit Log** – Shows if the firewall Audit Log service is enabled. For more information, see [How to Enable the Firewall Audit Log Service](#).
- **Guest Access** – Shows if Guest Access is provided. For more information, see [Firewall Authentication and Guest Access](#).

Networking Services

This element displays the status (enabled or disabled) of networking services. Click the arrow icon next to a feature to access the configuration.

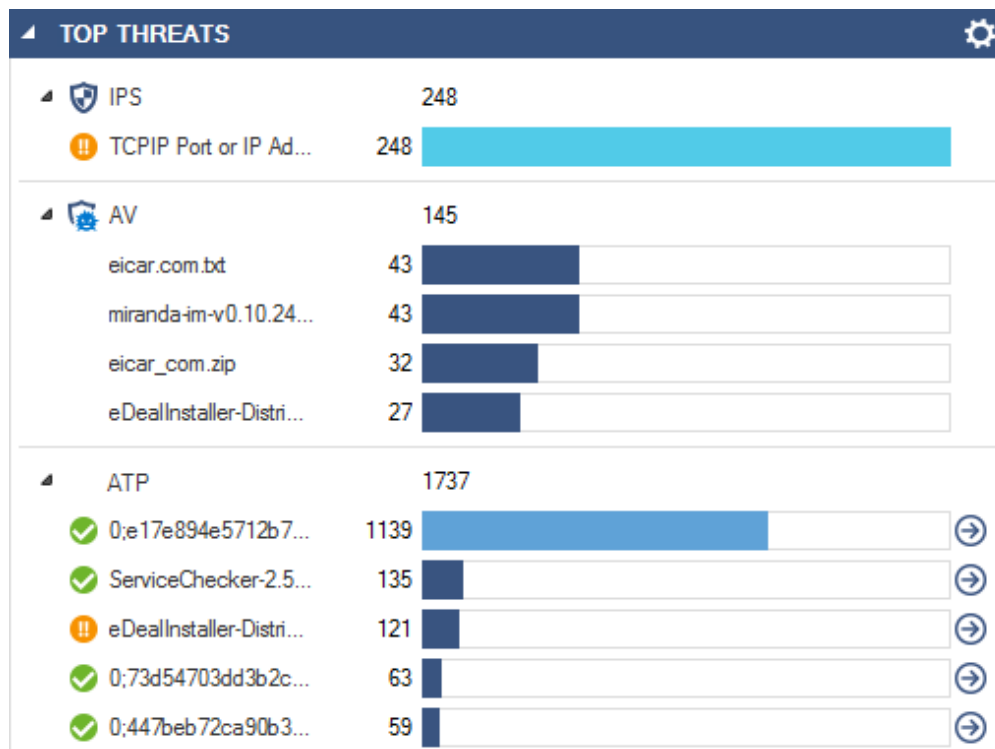
NETWORKING SERVICES			
 QoS	 Off		
 Application Based Provider Selection	 Off		
 VOIP/SIP Proxying	 On		
 TCP Proxying	 Off		
 Bridging	 Off		
 IPv6	 On		
 Dynamic Firewall Rules	 0 of 2 Rules enabled		
 HA Session Sync	 Active - 8 synced, 0 pending		

The **Networking Services** element provides the following information:

- **QoS** – Quality of Service. QoS is part of the CloudGen Firewall Traffic Shaping feature. For more information, see [Traffic Shaping](#).
- **Application Based Provider Selection** – Shows if application-based provider selection is enabled. For more information, see [Application Control](#).
- **VOIP/SIP Proxying** – Shows if VoIP/SIP proxying is enabled. For more information, see [SIP Proxy](#).
- **TCP Proxying** – Shows if TCP proxying is enabled. For more information, see [General Firewall Configuration](#).
- **Bridging** – Shows if bridging is enabled. For more information, see [Bridging](#).
- **IPv6** – Shows if IPv6 is enabled and in use. For more information, see [IPv6](#).
- **Dynamic Firewall Rules** – Shows if dynamic firewall rules are enabled. For more information, see [How to Create and Activate a Dynamic Access Rule](#).
- **HA Session Sync** – Shows if HA sync is active. If the number of pending sessions exceeds 7% of the active sessions, the HA session sync is displayed in a warning state (yellow).

Top Threats

This element shows the top threats by number of incidents. Click the arrow icons next to the feature icons to expand the features and display or hide further information details.



The **Top Threats** element provides the following information:

- **IPS** – Shows the top threats detected by the Intrusion Prevention System (IPS), if enabled. For more information, see [Intrusion Prevention System \(IPS\)](#).
- **AV** – Shows the top threats detected by the Virus Scanner service, if enabled. For more information, see [Virus Scanner](#).
- **ATP** – Shows the top threats detected by Advanced Threat Protection (ATP), if enabled. For more information, see [Advanced Threat Protection \(ATP\)](#).

Top Threat Vectors

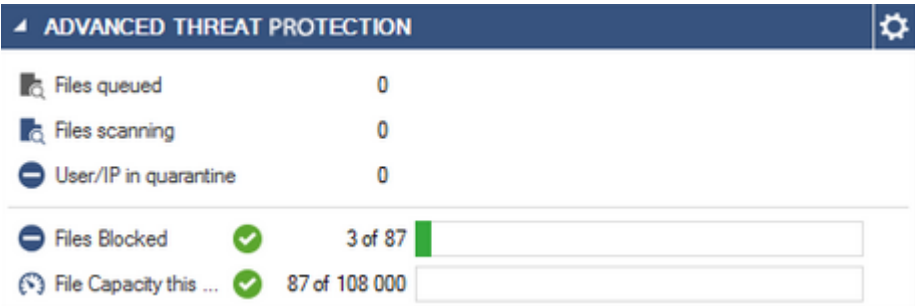
This element provides information on the top threat vectors sorted by user and geolocation.



The **User** column indicates the number of errors stemming from an individual user. The **Geo Sources** column indicates the source country of an attack or a country that has been categorized as unsafe. The **Geo Destinations** column indicates the target country of an attack.

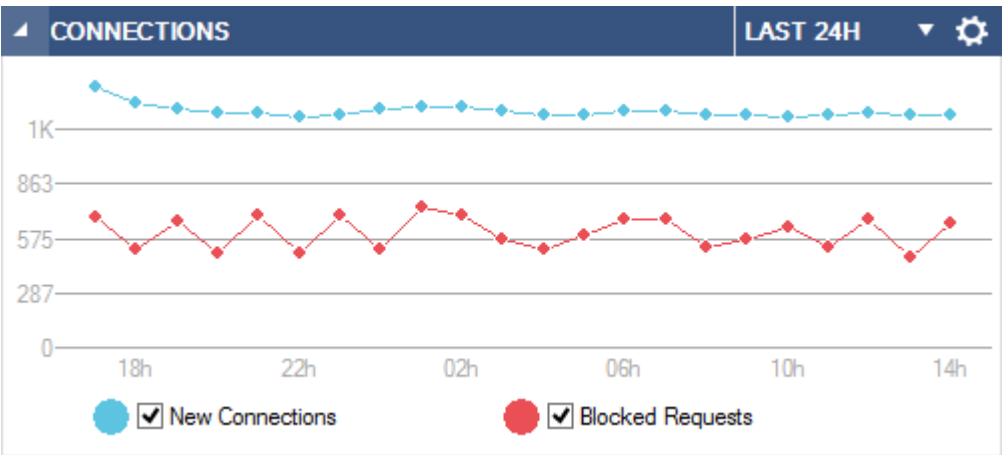
Advanced Threat Protection

This element shows information gathered by Advanced Threat Protection if ATP is enabled. For more information, see [Advanced Threat Protection \(ATP\)](#).



Connections

The **Connections** element shows the number of allowed and blocked connections on the CloudGen Firewall.



Click the link on the top right of the element (**Last 24h**) to change the time display interval, and select the check boxes to toggle the display view.




Top Live Applications

This element displays the currently transferred application and protocol traffic data per second, and provides information on the clients causing the traffic.

TOP LIVE APPLICATIONS			⚙
Application	Sessions	Bandwidth	
 CudaDrive / Copy	1	<div><div></div></div> 936	

Top Allowed Applications

This element shows the top allowed applications by data size.

TOP ALLOWED APPLICATIONS		LAST DAY	⚙
 Web browsing	212.0 MB	<div><div></div></div>	
 Google Safe Bro...	10.5 MB	<div><div></div></div>	
 Google Services ...	7.9 MB	<div><div></div></div>	

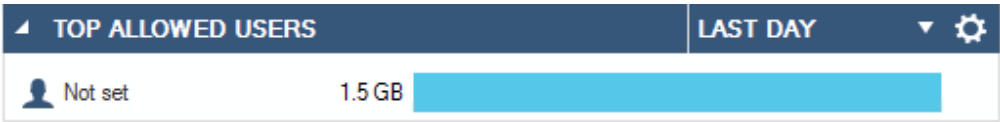
Top Blocked Applications

This element shows the top blocked applications by the number of occurrences.

TOP BLOCKED APPLICATIONS		LAST DAY	⚙
 Facebook Base	4	<div><div></div></div>	
 Facebook Social...	2	<div><div></div></div>	

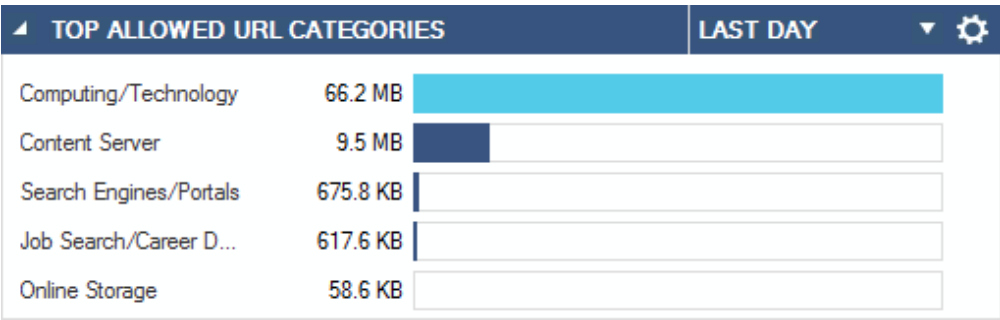
Top Allowed Users

This element shows the top users by the data size.



Top Allowed URL Categories / Top Blocked URL Categories

These elements show allowed and blocked URL categories sorted by data/occurrences.



Figures

1. firewall_security_services_01.png
2. db_fwI_05.png
3. db_fwI_06.png
4. db_fwI_07.png
5. db_fwI_09.png
6. db_fwI_03.png
7. top_live_apps.png
8. allowed_apps_01.png
9. blocked_apps.png
10. allowed_users.png
11. blocked_URL-CAT.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.