

## DASHBOARD Firewall Page





































<https://campus.barracuda.com/doc/43846810/>

The **DASHBOARD > 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

This element displays the status (enabled or disabled) of security-related services on the Barracuda NG 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 2.0](#).

SECURITY SERVICES 		
 Application Control 2.0	 On	
 SSL Interception	 On	
 URL Filter	 Off	
 IPS	 Off	
 Virus Scanner	 On	
 Advanced Threat Detection	 On	
 Safe Search	 On	
 YouTube for Schools	 On	
 RPC Tracking	 Off	
 Forwarding Ruleset Complexity	6 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 2.0 is enabled on the Barracuda NG Firewall. For more information, see [Application Control 2.0](#).
- **SSL Interception** – Shows if SSL Interception is enabled.

- **URL Filter** – Shows if URL filtering 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](#).
- **ATD Protection** – Shows if Advanced Threat Detection (ATD) is enabled. For more information, see [Advanced Threat Detection \(ATD\)](#).
- **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](#).
- **YouTube for Schools** – Shows if YouTube for Schools is in use in the Forwarding Firewall ruleset. For more information, see [How to Enforce YouTube for Schools in the Firewall](#).
- **RPC Tracking** – Shows if RPC tracking is enabled. For more information, see [How to Use the RPC Plugin Module](#).
- **Forward 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	ⓘ Off		➔
🌐 TCP Proxying	ⓘ Off		➔
🔗 Bridging	ⓘ Off		➔
📶 IPv6	✅ On		➔
🔗 Dynamic Firewall Rules	ⓘ No dynamic rules		➔

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

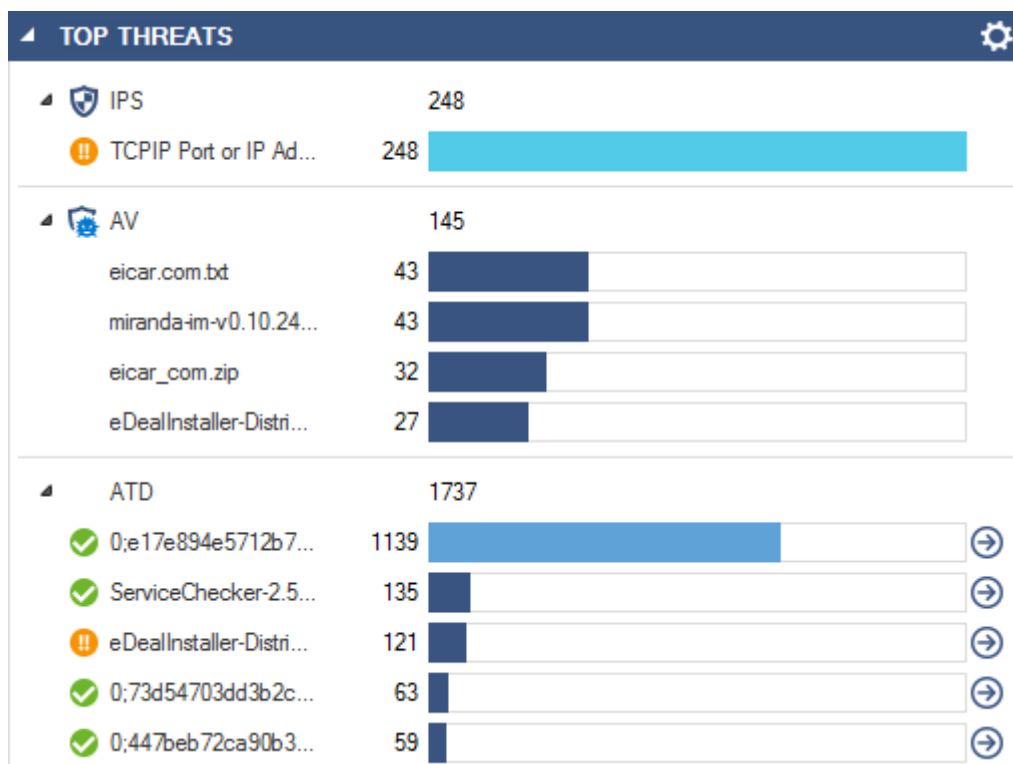
- **Quality of Service (QoS)** – QoS is part of the Barracuda NG Firewall Traffic Shaping feature. For more information, see [Traffic Shaping](#).
- **Application Based Provider Selection** – Shows if application-based provider selection is

enabled. For more information, see [Application Control 2.0](#).

- **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 [How to Use IPv6](#).
- **Dynamic Firewall Rules** – Shows if dynamic firewall rules are enabled. For more information, see [How to Create and Activate a Dynamic Rule](#).

## 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](#).
- **ATD** – Shows the top threats detected by Advanced Threat Detection (ATD) if enabled. For more

information, see [Advanced Threat Detection \(ATD\)](#).

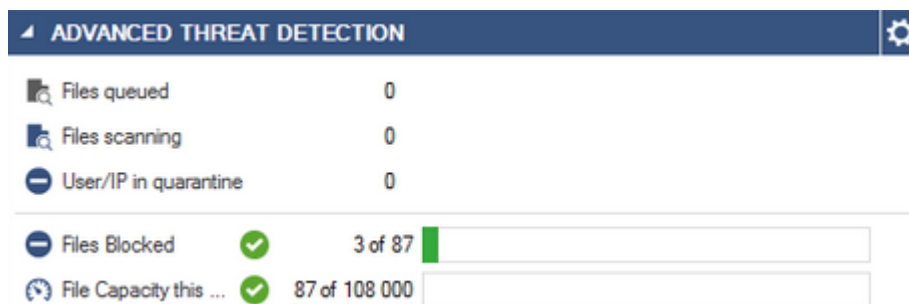
## Top Threat Vectors

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



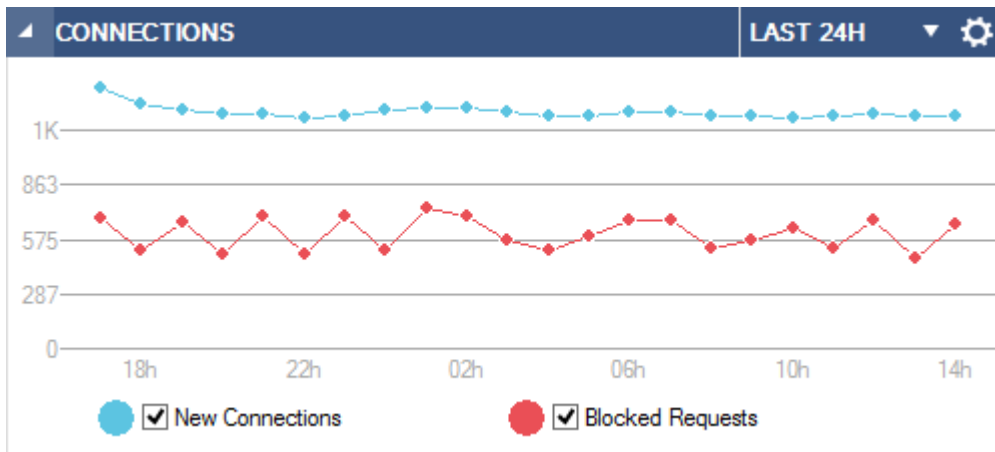
## Advanced Threat Detection

This element shows information gathered by advanced threat detection if ATD is enabled. For more information, see [Advanced Threat Detection \(ATD\)](#).



## Connections

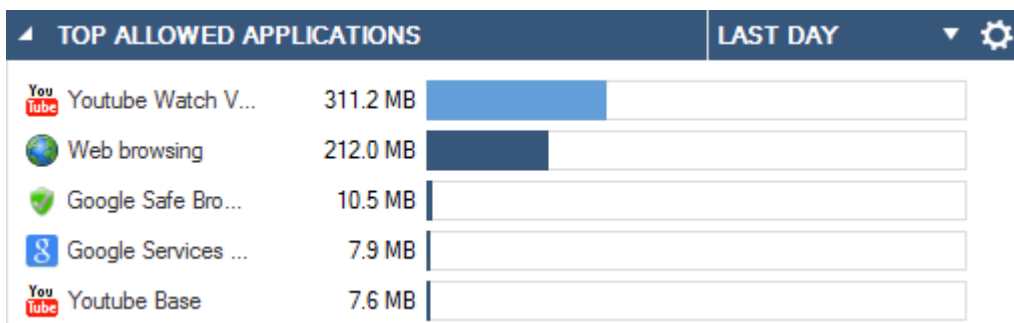
The **Connections** element shows the number of allowed and blocked connections on the Barracuda NG Firewall.



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

### Top Allowed Applications

This element shows the top allowed applications by data size.



### Top Blocked Applications

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



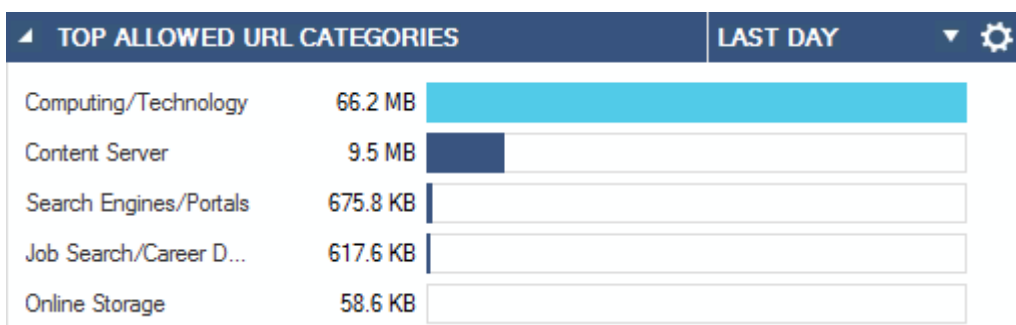
## Top Allowed Users

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.png
2. db\_fwl\_05.png
3. db\_fwl\_06.png
4. db\_fwl\_07.png
5. db\_fwl\_09.png
6. db\_fwl\_03.png
7. allowed\_apps.png
8. blocked\_apps.png
9. allowed\_users.png
10. blocked\_URL-CAT.png

© Barracuda Networks Inc., 2019 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.