Policies

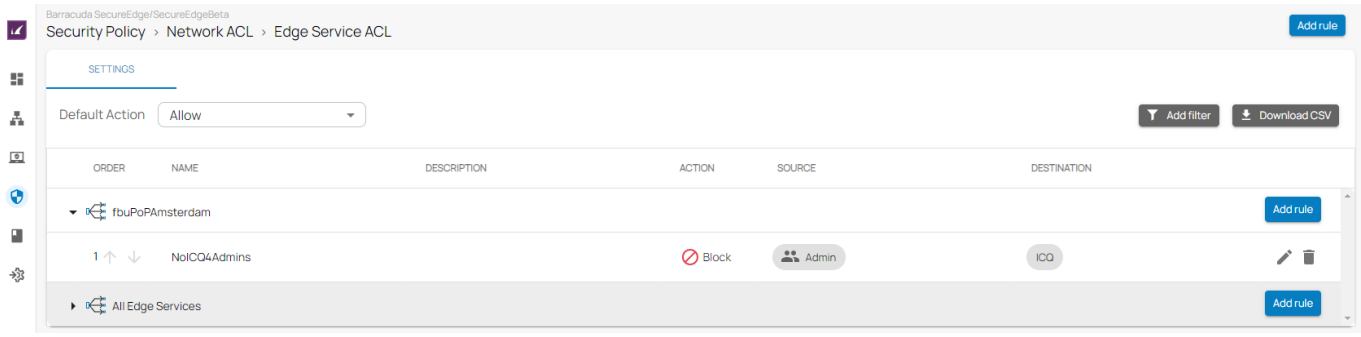
https://campus.barracuda.com/doc/98223635/

Barracuda SecureEdge allows administrative users with appropriate permissions to configure policies to protect internal resources and to secure access from and to the company network. Policies, rules, and access control lists are (pre-)defined rules for handling network traffic and are centrally managed throug https://se.barracudanetworks.com. Policies are automatically applied to all site appliances. Since updates are pulled from the site appliances in 1-minute intervals, it might take up to 8 minutes until the updates apply.

> Policies are being applied by (re-)writing dns records for the SecureEdge agent, it is therefore possible that previously visited pages (i.e., for which a DNS cache entry exists on the agent machine) remain unblocked for several hours, even though there is a blocking security policy configured.

Network Policies

Configure network policies to allow or deny access based on source and destination. You can create access control lists (ACLs) for networks, users, and sites, using either predefined or custom applications. For more information on custom applications, see How to Create Custom Applications. If you want to select users or groups in the policies, you must first connect your Microsoft Entra ID. For more information, see How to Connect Your Microsoft Entra ID with Barracuda Cloud Control.



The following access control lists are available:

- Edge Service ACL
- Site ACL

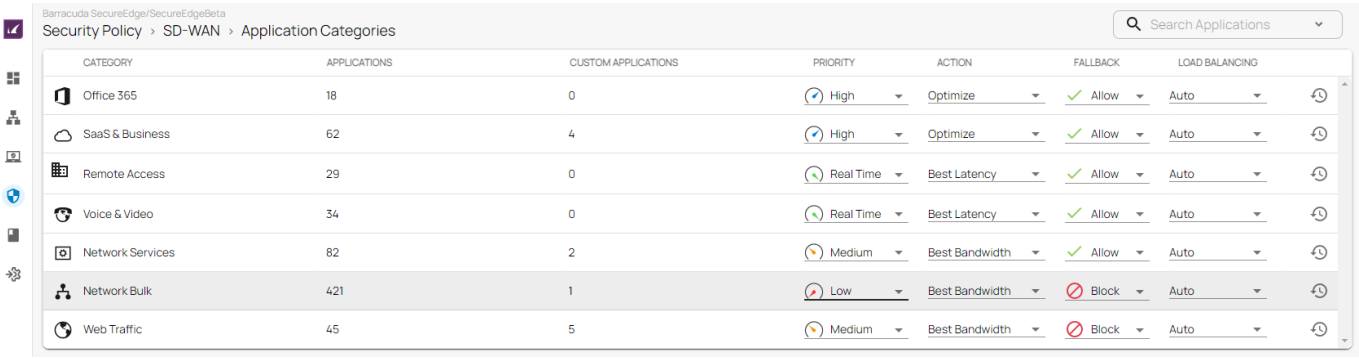
For more information, see Network Policies.

SD-WAN Policies

Barracuda SecureEdge provides a default configuration for SD-WAN Policies using a predefined application database to cover the most common use cases. For the default configuration, Barracuda Networks has defined an SLA for each application and protocol. The SLA decides how the application is routed according to its needs. You can create explicit policies to change the default behaviour, or you can create additional policies specifically matching your requirements. In addition, you can add applications to the database using custom applications, which allow you to extend the predefined application database used by both the SD-WAN policies and security policies.

The matching algorithm works as follows:

1. An application is detected. Custom application definitions take precedence over predefined applications. For more information, see How to Create Custom Applications.
2. If there is an explicit policy for that application, the explicit policy is used. For more information, see SD-WAN Policies.
3. Otherwise, the algorithm looks up the SD-WAN category and applies the Quality of Service / intelligent routing defined in the policy.



The following SD-WAN options are available:

- **Category** – The name of the category.
- **Applications** – Number of applications where the policy applies.
- **Custom Applications** – Number of custom applications where the policy applies.
- **Priority** – The following options are available:
  - **Real Time** – The highest possible priority for the traffic of this policy with no bandwidth restrictions in place. Use this option with caution: it can lead to excessive package drops if the traffic oversubscribes your ISP connection.
  - **High** – High priority for the traffic of this policy. This option will not oversubscribe your ISP connection.
  - **Medium** – Medium priority for the traffic of this policy. This option will not oversubscribe your ISP connection.

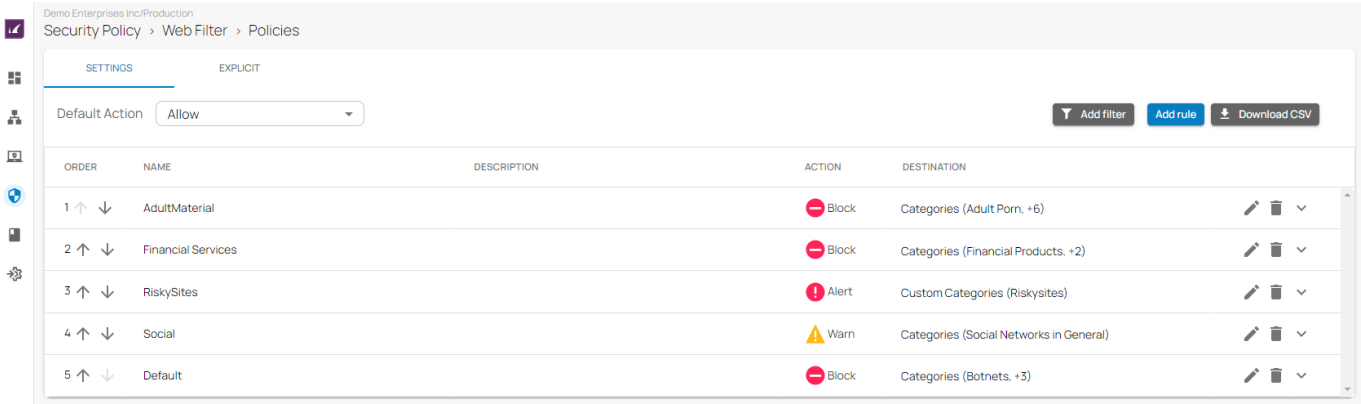
    - **Low** – Low priority for the traffic of this policy. This option will not oversubscribe your ISP connection.
- **Action** – The following options are available:
    - **Optimize** – Based on the probing data, traffic will use the ISP connection with the best bandwidth / latency depending on what the application needs. When applications with different requirements are in the same category, it falls back to the SLA of the individual app.
    - **Best Bandwidth** – Traffic uses ISP connections with the best bandwidth.
    - **Best Latency** – Traffic uses ISP connections with the best latency.
    - **Pin to Group 1** – Traffic will only use ISP connections assigned to this group and, if configured, the fallback link. There must be at least one WAN connection that is not a WWAN in the provider pinning of Group 1.
    - **Pin to Group 2** – Traffic will only use ISP connections assigned to this group and, if configured, the fallback link.
    - **Prefer Group 1** – Traffic uses ISP connections assigned to this group. If no link in the group is available, it will use the other group and then, if configured, the fallback link.
    - **Prefer Group 2** – Traffic uses ISP connections assigned to this group. If no link in the group is available, it will use the other group and then, if configured, the fallback link.
- **Fallback** – Fallback links are only used in case the assigned uplinks are down. The following options are available:
    - **Allow** – Traffic of this policy is allowed to use the fallback link.
    - **Block** – Traffic of this policy is not allowed to use the fallback link.
- **Load Balancing** – The following options are available:
    - **Auto** – VPN traffic uses load balancing, and traffic assigned the option **Optimize** is excluded from load balancing. The load is balanced between two providers in the same provider pinning group.
    - **No** – Load balancing is disabled.
- **Forward Error Correction** – FEC is a method of correcting certain data transmission errors that occur over noisy communication lines, thereby improving data reliability without requiring retransmission. The following options are available:
    - **On** – Forward error correction is enabled.
    - **Off** – Forward error correction is disabled.

For more information, see SD-WAN Policies.

Web Filter Policies

The Barracuda SecureEdge Manager allows you configure Web Filter policies as well as explicit Web Filter Policies to protect against potential threats and enforce corporate policies. Explicit Web Filter policies take precedence over predefined security policies. A Web Filter rule either blocks or allows a domain, category, or custom category from any source, whereas an explicit rule blocks or allows URLs from specified sources. In addition, for the web filter rule, you can now either alert or warn users against suspicious traffic. For more information, see Web Filter Policies and How to Create an Explicit

Web Filter Policy.



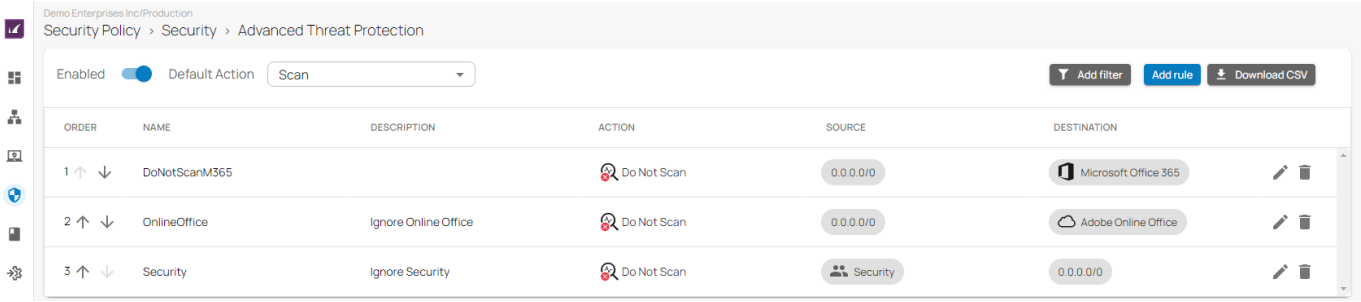
The following filter policies are available:

- Custom Categories
- Web Monitoring

For more information on how to create custom categories, see How to Create Custom Categories, and for more information on web monitoring policies, see How to Configure Web Monitoring in Barracuda SecureEdge.

Security Policies

The default action of a security policy can, for example, be either to block all and define exceptions that are allowed, or to allow all and define exceptions that are blocked. You can change the default action for all security polices individually. For example, web filtering is set to allow all and define exceptions that are blocked, and ACL is set to block all with exceptions that are allowed.



The following security policies are available:

- Advanced Threat Protection
- SSL Inspection
- IPS

Some policies come with preconfigured default rules. In this case, explicit rules have precedence over predefined ones.

The matching algorithm of the rules works as follows:

1. All rules (explicit and default) apply top down. That means the first rule in the list that matches applies. Rules below the first match will not apply.
2. First, the explicit rules are searched for matches. If there is an explicit rule that matches, this explicit rule will be used.
3. Otherwise, the default rules are searched, and if there is a rule that matches, this rule will be used.

For more information, see Security Policies.

Figures