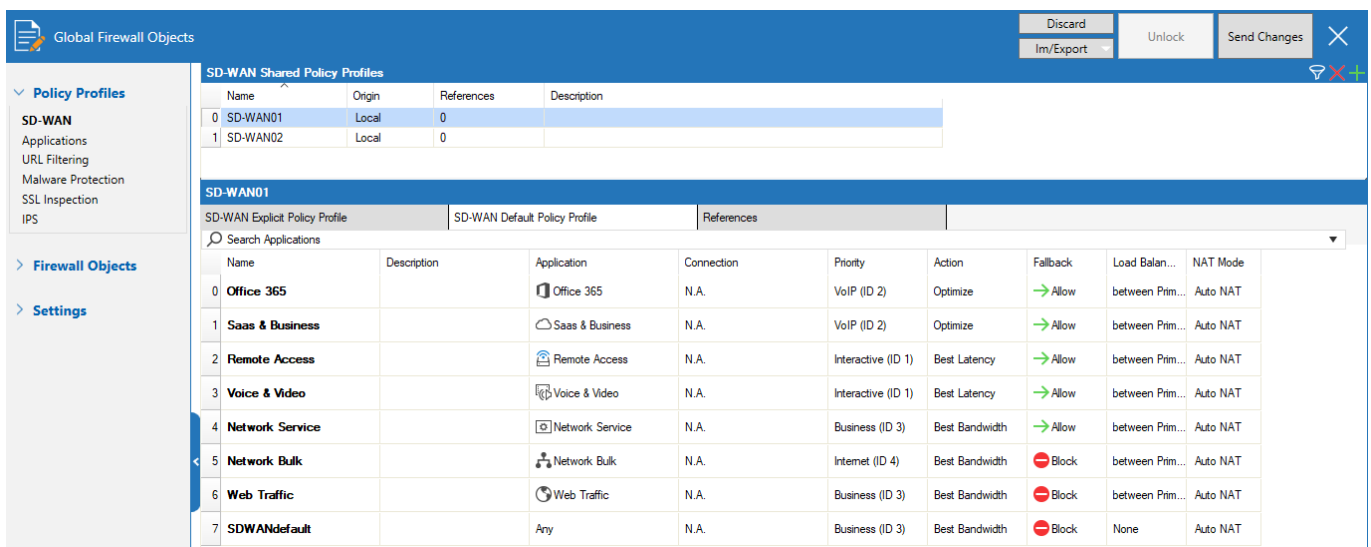


## Policy Profiles

<https://campus.barracuda.com/doc/96766707/>

Policy profiles are centrally managed, (pre-)defined rules for handling network traffic and applications, that allow administrators to define packet behavior after the traffic was processed by access rules. Policy profiles can handle the routing decisions of packets as well as decisions based on application detection or any other layer 7 information. The Barracuda CloudGen Firewall allows administrators to manage, create, and customize general policies on a global-, range-, cluster-, or box level that can then be applied to access rules instead of configuring firewall objects. Policy profiles can be applied to access rules on Control Center-managed or stand-alone firewall units. You can customize default profiles by adding or modifying policies, or you can create new profiles with explicit policies. Policies always work top-down, and explicit policies take precedence over predefined policies.

Policy Profiles are not visible by default and must be enabled for the firewall engine.



The screenshot shows the 'Global Firewall Objects' configuration page. On the left sidebar, 'Policy Profiles' is selected under 'SD-WAN'. The main area displays 'SD-WAN Shared Policy Profiles' with a table containing two entries: SD-WAN01 and SD-WAN02, both of Local origin and 0 references. Below this, the 'SD-WAN01' profile is expanded, showing 'SD-WAN Explicit Policy Profile' and 'SD-WAN Default Policy Profile' tabs. The 'SD-WAN Default Policy Profile' is active, displaying a table of policies:

Name	Description	Application	Connection	Priority	Action	Fallback	Load Balan...	NAT Mode
0 Office 365		Office 365	N.A.	VoIP (ID 2)	Optimize	→ Allow	between Prim...	Auto NAT
1 Saas & Business		Saas & Business	N.A.	VoIP (ID 2)	Optimize	→ Allow	between Prim...	Auto NAT
2 Remote Access		Remote Access	N.A.	Interactive (ID 1)	Best Latency	→ Allow	between Prim...	Auto NAT
3 Voice & Video		Voice & Video	N.A.	Interactive (ID 1)	Best Latency	→ Allow	between Prim...	Auto NAT
4 Network Service		Network Service	N.A.	Business (ID 3)	Best Bandwidth	→ Allow	between Prim...	Auto NAT
5 Network Bulk		Network Bulk	N.A.	Internet (ID 4)	Best Bandwidth	⊘ Block	between Prim...	Auto NAT
6 Web Traffic		Web Traffic	N.A.	Business (ID 3)	Best Bandwidth	⊘ Block	between Prim...	Auto NAT
7 SDWANdefault		Any	N.A.	Business (ID 3)	Best Bandwidth	⊘ Block	None	Auto NAT

Using policy profiles in access rules instead of applying firewall objects requires Barracuda CloudGen Firewall feature release 8.3 or higher. Existing application rules cannot be migrated when using policy profiles, you can switch back to the standard access ruleset with Application Control by reverting the feature level of the firewall. For information on how to enable the feature level, see [How to Manage Ranges and Clusters](#).

This feature is currently only available for IPv4 networks, so any IPv6 references will be ignored when used in the configuration.

The Barracuda CloudGen Firewall provides the following policies:

## SD-WAN Policies

---

SD-WAN provides multipath VPN tunnels across all providers with redundant, reliable, and fail-safe network connections. When the VPN tunnel is up, it can transmit traffic as long as at least one ISP link is operational. Admins can retain full control over how each link is used, or they can configure the advanced balancing and bandwidth management features to optimally use the available bandwidth (for general information, see [SD-WAN](#)). SD-WAN combines a multi-transport VPN tunnel with the following advanced VPN routing, balancing, and shaping features:

- Dynamic Bandwidth and Round Trip Time (RTT) Detection
- Performance-Based Transport Selection
- Adaptive Bandwidth Protection
- Adaptive and Static Session Balancing
- Failover Support
- Multi-Provider Load Balancing

The Barracuda CloudGen Firewall provides a predefined default configuration of SD-WAN policies that allows you to use the advantages of SD-WAN immediately, without even having to set up your own configuration. Barracuda Networks has defined an SLA for each application and protocol that decides how the application is routed in the default configuration. However, if you create explicit policies or custom applications, they apply before the default policies.

For more information, see [How to Configure Policy Profiles](#). For instructions on how to create explicit policies, see [How to Create SD-WAN Policies](#).

## Application Policies

---

Create application policies to allow, block, or customize traffic for detected applications. Custom web applications allow administrators to handle multiple application components, the destination can be either an IP address, network, or domain, which gets resolved to IP addresses. The matching criteria are based on the OSI model layer 7 and are limited to HTTP and HTTPS. The HTTP/S requests and responses are used for matching. For HTTPS, the server name indication (SNI) is used to extract the destination information, whereas for HTTP the header information is used for determination. When TLS Inspection is enabled, the header is used for HTTPS as well. Application policies can be assigned to access rules on all firewalls that are managed by the Control Center where the policy profile has been defined. Policy entries can be edited and changed at any time. Application Control is available on CloudGen Firewall models with a valid Energize Updates subscription (for general information, see [Application Control](#)).

---

For more information, see [How to Configure Policy Profiles](#). For instructions on how to create explicit policies, see [How to Create Application Policies](#).

## URL Filtering Policies

---

Barracuda Networks provides a large database, organized in categories, for URL filtering. You can either use the provided categories to create rules, or you can specify the domains yourself. Malicious URLs are blocked in the default configuration. You can customize a URL filtering policy profile to match individual requirements, or you can create explicit policies. The default action of a policy can be either to block all and define exceptions that are allowed or to allow all and define exceptions that are blocked. A filter rule blocks/allows a domain or category from any source, whereas an explicit rule blocks or allows URLs from specified sources.

For more information, see [How to Configure Policy Profiles](#). For instructions on how to create explicit policies, see [How to Create URL Filtering Policies](#).

## Malware Protection Policies

---

Malware protection offers protection against advanced malware, zero-day exploits, and targeted attacks not detected by the Intrusion Prevention System by scanning downloaded files, using the Avira scanning engine. If [Advanced Threat Protection \(ATP\)](#) is enabled, an ATP scan is also performed, and a hash DB lookup is performed before a user receives a downloaded file. The file, if 10 megabytes or less, is uploaded to the ATP cloud. Archives are unpacked, and the files they contain, which must also be 10 megabytes or less, are sent to the ATP cloud for inspection. Depending on the behavior of a file, it is assigned a threat level that is transmitted to the firewall appliance. If the threat level exceeds the ATP threat level threshold, the file is blocked; otherwise, it is delivered. Malware Protection can be used for HTTP, HTTPS, FTP, and FTPS traffic. For HTTPS and FTPS, you must enable [TLS Inspection in the Firewall](#).

For more information, see [How to Configure Policy Profiles](#). For instructions on how to create explicit policies, see [How to Create Malware Protection Policies](#).

## TLS Inspection Policies

---

TLS Inspection decrypts inbound and outbound TLS connections so the Barracuda CloudGen Firewall appliance can allow features, such as Malware Protection and the Intrusion Prevention System (IPS), to scan traffic that would otherwise not be visible to the firewall service. See [TLS Inspection in the Firewall](#) for general information on the capabilities of the TLS Inspection feature. Configure global TLS

policies to manage the behavior of Control Center-managed Barracuda CloudGen Firewalls when dealing with encrypted traffic.

For more information, see [How to Configure Policy Profiles](#). For instructions on how to create explicit policies, see [How to Create TLS Inspection Policies](#).

## IPS Scanning Policies

---

The Intrusion Prevention System (IPS) monitors local and forwarding traffic for malicious activities and provides various countermeasures, such as blocking suspicious traffic, to avert possible network attacks. For general information on the capabilities of the CloudGen Firewall IPS feature, see [Intrusion Prevention System \(IPS\)](#). When IPS is enabled on the firewall, the IPS engine analyzes the network traffic and continuously compares the bitstream with its internal signatures database for malicious code patterns. The Barracuda CloudGen Firewall supports a range of IPS features, such as TCP stream reassembly, URL obfuscation, and TCP split handshake. Using IPS requires a valid Energize Updates subscription.

For more information, see [How to Configure Policy Profiles](#). For instructions on how to create explicit policies, see [How to Create IPS Policies](#).

## Figures

1. global\_pols.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.