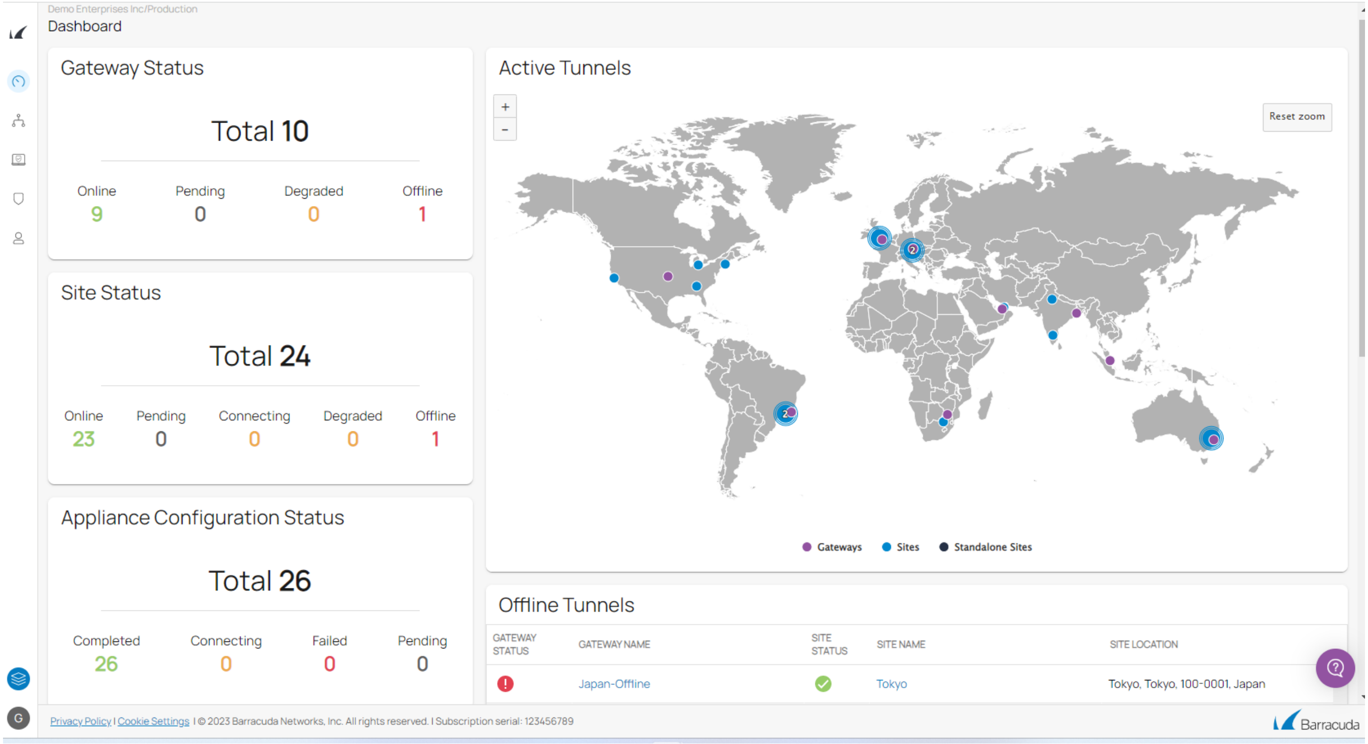
Release Notes

https://campus.barracuda.com/doc/98223573/

Barracuda SecureEdge combines the benefits of next-generation firewalls, secure SD-WAN, and cloud integration and automation to deliver a practical SASE solution. The SecureEdge dashboard provides a comprehensive overview of SD-WAN connections, SD-WAN tunnels, network activity, web and network traffic details, as well as the actionable status and security information of your deployed Barracuda Networks products.

Barracuda SecureEdge Dashboard

Barracuda SecureEdge provides fast and actionable in-product status information and is designed to allow internal and external reporting to stakeholders who do not require access to the web interface. The dashboard provides a customizable status overview with information on SD-WAN connections, security, and transport and traffic details.



Demo Enterprises Inc/Production

Dashboard

Gateway Status

Total 10

Online	Pending	Degraded	Offline
9	0	0	1

Site Status

Total 24

Online	Pending	Connecting	Degraded	Offline
23	0	0	0	1

Appliance Configuration Status

Total 26

Completed	Connecting	Failed	Pending
26	0	0	0

Active Tunnels

Offline Tunnels

GATEWAY STATUS	GATEWAY NAME	SITE STATUS	SITE NAME	SITE LOCATION
!	Japan-Offline	✓	Tokyo	Tokyo, Tokyo, 100-0001, Japan

Privacy Policy | Cookie Settings | © 2023 Barracuda Networks, Inc. All rights reserved. | Subscription serial: 123456789

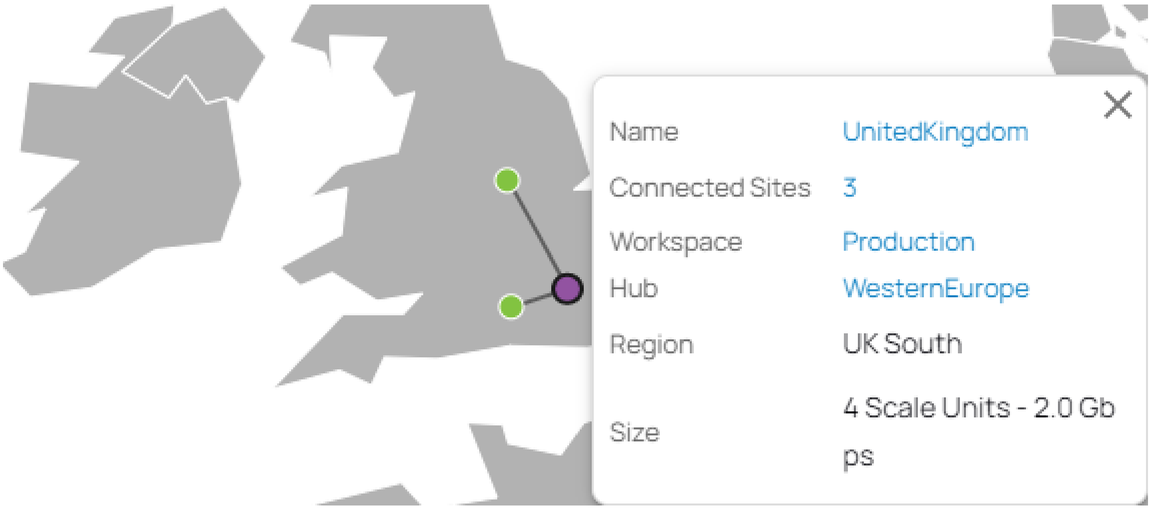
You can deploy virtual WANs with multiple edge services and site appliances. Each site is connected to the edge service using TINA, the Barracuda Networks VPN protocol. TINA is a proprietary extension of the IPsec protocol developed to improve VPN connectivity and availability over the standard IPsec protocol, and uses AES256 cipher for the VPN encryption. Barracuda SecureEdge uses BGP for routing.

Barracuda SecureEdge provides the following:

- An aggregate view of data for multiple connected devices
- Information on details and availability of SD-WAN connections
- Drill-down capabilities for a subset of connected devices to see aggregate statistics
- Customizable dashboard monitoring for a quick overview of filtering statistics aggregated across all connected devices

Barracuda SecureEdge Manager

The Barracuda SecureEdge Manager is the cloud-based central management portal. From here, you can manage all your edge services, sites, tunnels, and appliances, and perform various configuration and maintenance actions.



Name	UnitedKingdom
Connected Sites	3
Workspace	Production
Hub	WesternEurope
Region	UK South
Size	4 Scale Units - 2.0 Gbps

The SecureEdge Manager summarizes information with respect to your selected workspace or tenant and displays details on the status of your associated edge services, sites, tunnels, and configured appliances. Aggregated information on recent system and administrative events can be monitored. In addition, the dashboard provides an active tunnel map, a graphical view that shows where all sites and edge services are being deployed based on their geolocation. Click on a site or edge service in the map to see where it is connected to.

Barracuda CloudGen Firewall Integration

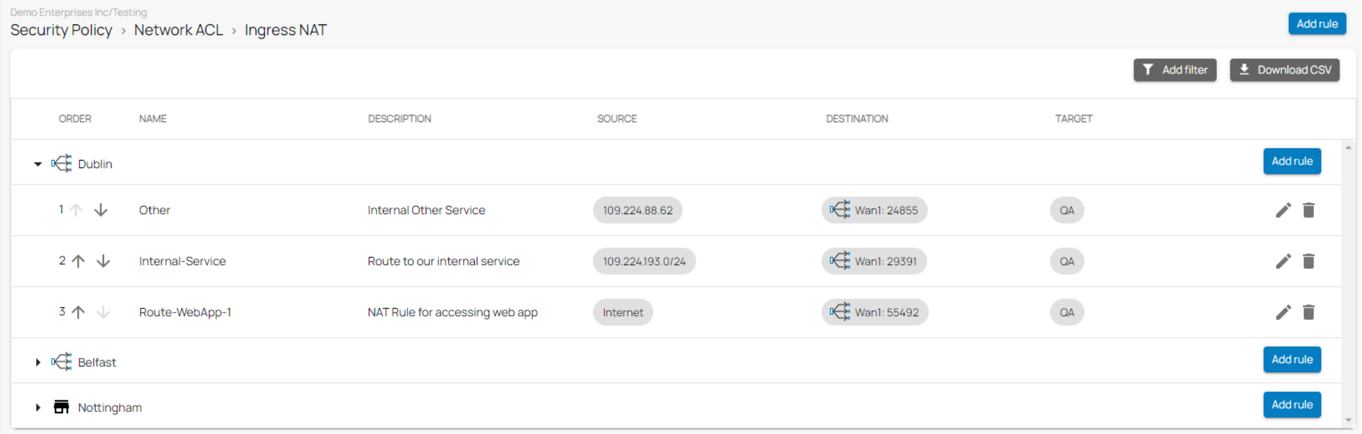
Barracuda CloudGen Firewall appliances can be enrolled with Barracuda SecureEdge as a point of enforcement for resource access policies. The firewall appliances can be either stand-alone or Control Center-managed units. Registration of CloudGen Firewalls on Barracuda SecureEdge is token based.

After completing the registration process, the appliance gets enrolled and automatically appears in Barracuda SecureEdge, which indicates that the connection is established. The appliance details can be verified with respect to host name and serial number, using Barracuda Firewall Admin. On Barracuda CloudGen Firewall High Availability (HA) boxes, enrollment is required only on the primary unit.

For more information, see How to Configure a Barracuda CloudGen Firewall in Barracuda SecureEdge.

Ingress NAT Rules

Ingress traffic can be any form of network traffic whose source lies in an external network, in other words, in the public Internet, to destinations residing inside the host network. You must configure a security policy rule to allow the NAT traffic. In the Barracuda SecureEdge network policies configuration, you can define new ingress NAT rules for sites and on-premises edge services by specifying source, destination, and target criteria.



Demo Enterprises Inc/Testing

Security Policy › Network ACL › Ingress NAT

ORDER	NAME	DESCRIPTION	SOURCE	DESTINATION	TARGET
Dublin					
1	Other	Internal Other Service	109.224.88.62	Wan1: 24855	QA
2	Internal-Service	Route to our internal service	109.224.193.0/24	Wan1: 29391	QA
3	Route-WebApp-1	NAT Rule for accessing web app	Internet	Wan1: 55492	QA
Belfast					
Nottingham					

For more information, see How to Create Ingress NAT Rules.

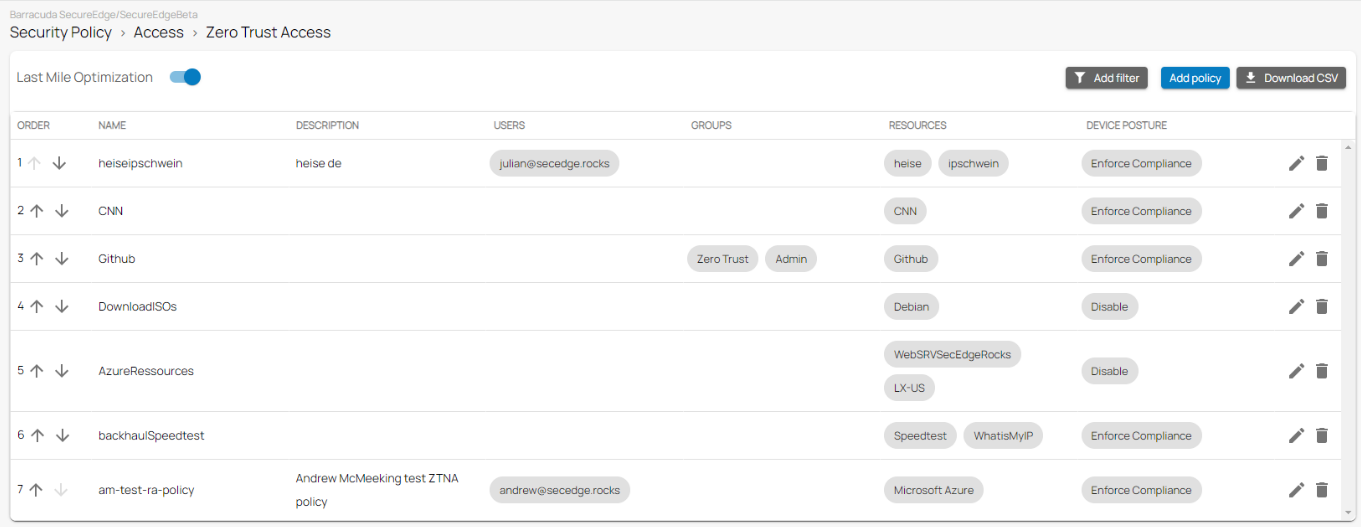
Barracuda SecureEdge Agent

Barracuda SecureEdge allows administrators to enroll users with their respective devices. The Barracuda SecureEdge Agent is a Zero Trust Network Access (ZTNA) agent running on the client that connects to the services offered by Barracuda SecureEdge. The SecureEdge Agent allows users or groups to connect to different resource types, including custom apps or public endpoints such as SaaS services. A single user can enroll multiple devices on the same token. After the enterprise enrollment process is completed, your device protection gets enabled automatically. The Barracuda SecureEdge Agent for Windows, MacOS, iOS, and Android is available from their respective app stores.

For more information, see How to Enroll Users in Barracuda SecureEdge.

Remote Access Policies

Remote access policies are (pre-)defined rules for handling network traffic and are centrally managed through Barracuda SecureEdge. Remote access policies define resources made available to end users of the SecureEdge Agent as well as the associated access criteria. Barracuda SecureEdge allows administrators to create new remote access policies for users or groups that specify access requirements associated with various types of internal and external resources. These policies also define security attributes such as the device posture. When these policies are enabled, you can either enforce compliance or log violations. Certain security features (such as security inspection, firewall enabled, antivirus enabled, block jailbroken devices, and screen lock enabled) can be enabled or disabled with a switch; other update features for the operating system and the SecureEdge Agent can also be enabled/disabled. This action is disabled by default.


Barracuda SecureEdge/SecureEdgeBeta
Security Policy › Access › Zero Trust Access
Last Mile Optimization
Add filter
Add policy
Download CSV

ORDER	NAME	DESCRIPTION	USERS	GROUPS	RESOURCES	DEVICE POSTURE
1	heiseipschwein	heise de	julian@secedge.rocks		heise ipschwein	Enforce Compliance
2	CNN				CNN	Enforce Compliance
3	Github			Zero Trust Admin	Github	Enforce Compliance
4	DownloadISOs				Debian	Disable
5	AzureRessources				WebSRVSecEdgeRocks LX-US	Disable
6	backhaulSpeedtest				Speedtest WhatisMyIP	Enforce Compliance
7	am-test-ra-policy	Andrew McMeeking test ZTNA policy	andrew@secedge.rocks		Microsoft Azure	Enforce Compliance

For more information, see Zero Trust Access Policies.

Barracuda SecureEdge Access

Barracuda SecureEdge Access lets you implement secure access to internal and external enterprise resources, whether they are on-premises or in the cloud, by using a Zero Trust Network Access (ZTNA) solution. Zero Trust builds upon the assumption that the network is hostile. As a result, network locality is not sufficient for establishing trust, and every flow must be authenticated and authorized in a dynamic fashion. This creates an effective separation between the control plane – the supporting system that implements the flow authentication and authorization according to the defined policies – and the data plane.

For more information, see Remote Access.

SecureEdge Integration with IoT Devices

The Barracuda SecureEdge Manager allows administrators to enroll the Barracuda Secure Connector, an IoT device, with the unified cloud service entity known as SecureEdge. Barracuda Secure Connector is a hardware device that offers large-scale remote access capabilities and allows the ever-growing number of IoT devices and micro-networks to securely connect to the corporate data center via VPN.

For more information, see How to Configure IoT Devices in Barracuda SecureEdge.

Barracuda SecureEdge SD-WAN Connector

The Barracuda SecureEdge SD-WAN Connector establishes a connection between the service and a resource that cannot be reached via routing. Registration of the SecureEdge SD-WAN Connector is token based. After retrieving the token from SecureEdge, you can select the edge service or site the device should connect to. Once registered, each SecureEdge SD-WAN Connector will be assigned a single static IP address within the SecureEdge environment. It also provides a feature in which the admin can configure a list of resources that the SecureEdge SD-WAN Connector can connect to, and each resource can be reached via the Barracuda SecureEdge Agent if a policy for it exists.

For more information, see How to Configure the SecureEdge SD-WAN Connector.

Barracuda XDR

The SecureEdge Manager allows you to stream logs to the Extended Detection and Response (XDR) service. You can integrate the Barracuda XDR service via the SecureEdge Manager and stream logs for security threats.

For more information, see How to Configure Barracuda XDR in SecureEdge.

What's New in Version 9.0.1

SafeSearch Enforcement

The SafeSearch enforcement feature is now available in the Barracuda SecureEdge Manager. It allows you to enforce SafeSearch per workspace for internet search engines.

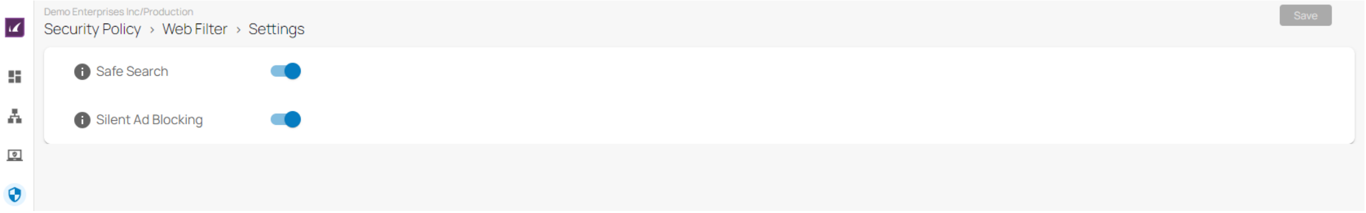
Supported search engines:

- Google
- Yahoo
- Bing
- YouTube
- DuckDuckGo

For more information, see How to Enable Safe Search in Barracuda SecureEdge.

Silent Ad Blocking

The Barracuda SecureEdge Manager allows you to create a web policy per workspace that silently blocks online advertisements and banners.


Demo Enterprises Inc/Production
Security Policy › Web Filter › Settings
Save

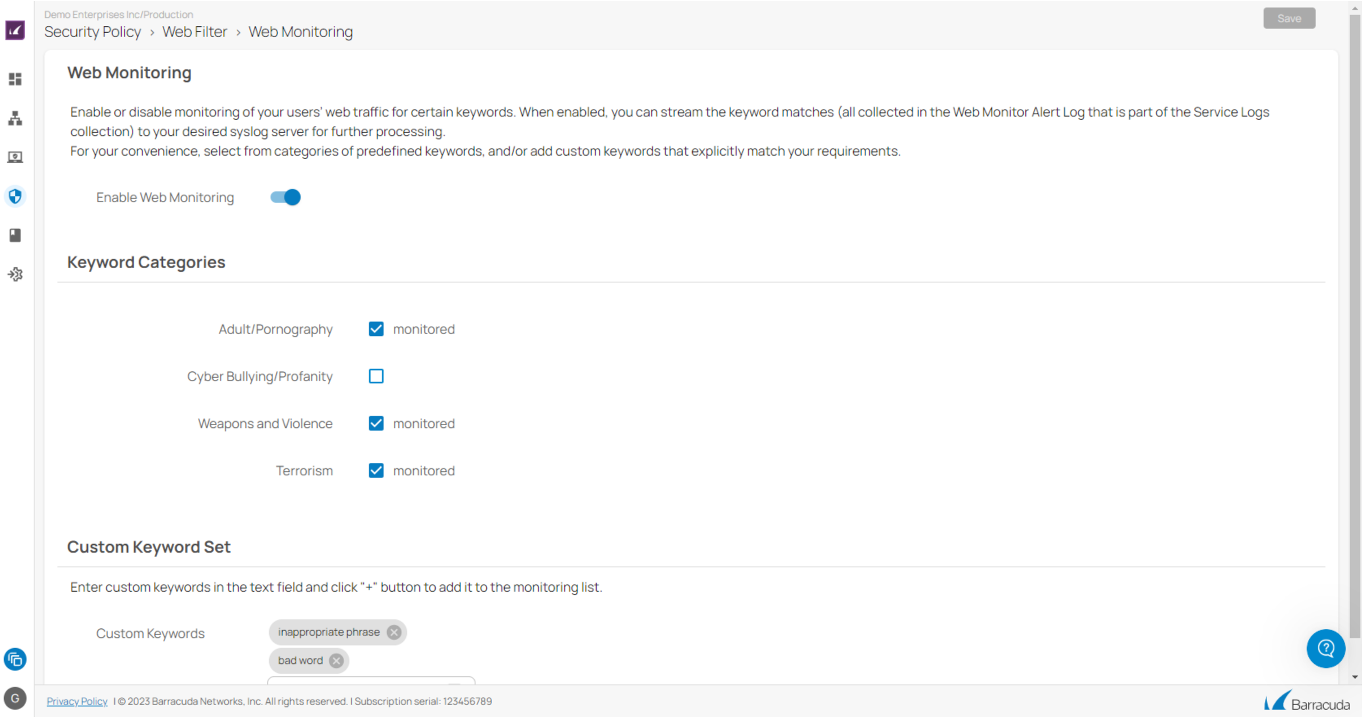
Safe Search: ●

Silent Ad Blocking: ●

For more information, see How to Enable Silent Ad Blocking.

Web Monitoring Policies

The Barracuda SecureEdge Manager allows you to configure Web Monitoring policies, so that suspicious keywords can be detected in search engines such as Google, Yahoo, Bing, DuckDuckGo, and YouTube.



Demo Enterprises Inc/Production
Security Policy › Web Filter › Web Monitoring
Save

Web Monitoring

Enable or disable monitoring of your users' web traffic for certain keywords. When enabled, you can stream the keyword matches (all collected in the Web Monitor Alert Log that is part of the Service Logs collection) to your desired syslog server for further processing.
For your convenience, select from categories of predefined keywords, and/or add custom keywords that explicitly match your requirements.

Enable Web Monitoring: on

Keyword Categories

Adult/Pornography	☑ monitored
Cyber Bullying/Profanity	☐
Weapons and Violence	☑ monitored
Terrorism	☑ monitored

Custom Keyword Set

Enter custom keywords in the text field and click "+" button to add it to the monitoring list.

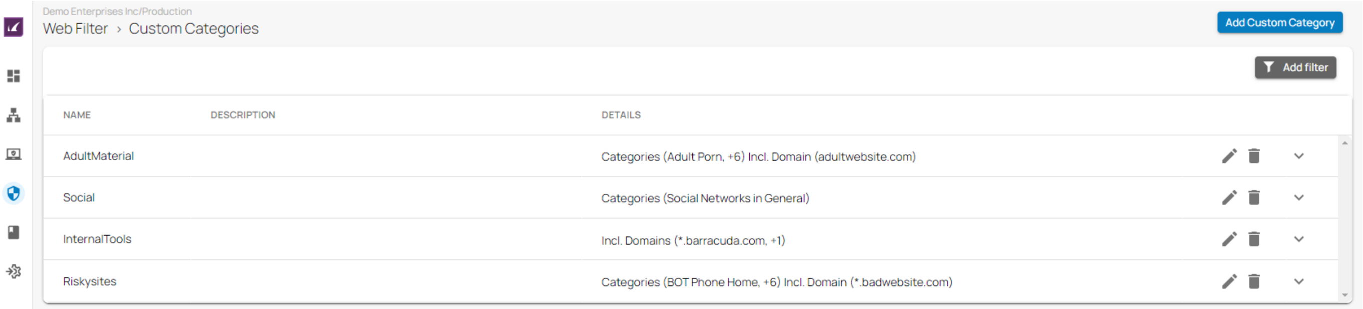
Custom Keywords: inappropriate phrase ⊗, bad word ⊗

Privacy Policy | © 2023 Barracuda Networks, Inc. All rights reserved. | Subscription serial: 123456789
Barracuda

For more information, see How to Configure Web Monitoring in Barracuda SecureEdge.

Custom Categories

You can now create your own custom categories to filter traffic from specific domains, specific categories, or a combination of domains and categories.



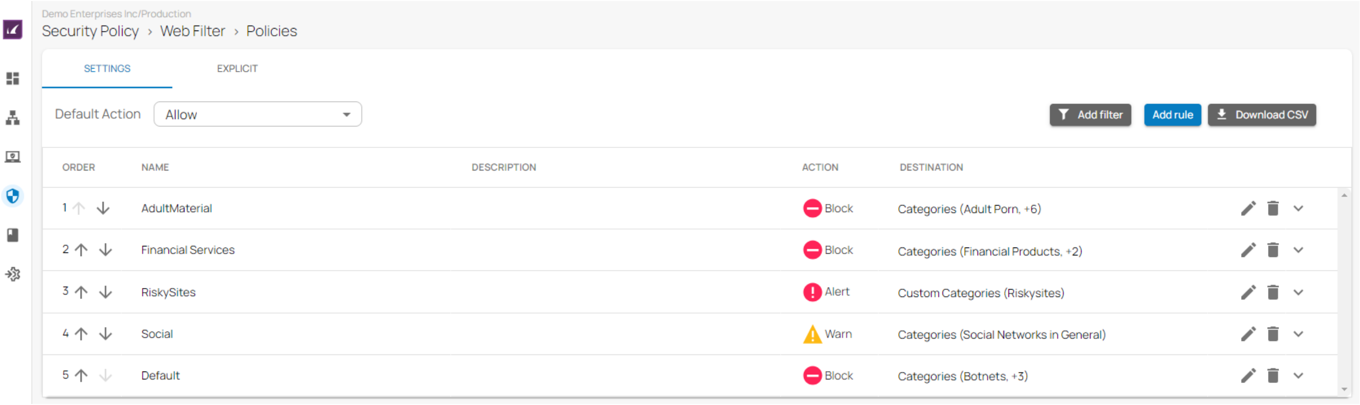
Demo Enterprises Inc/Production
Web Filter › Custom Categories
Add Custom Category
Add filter

NAME	DESCRIPTION	DETAILS
AdultMaterial		Categories (Adult Porn, +6) Incl. Domain (adultwebsite.com)
Social		Categories (Social Networks in General)
InternalTools		Incl. Domains (*.barracuda.com, +1)
Riskysites		Categories (BOT Phone Home, +6) Incl. Domain (*.badwebsite.com)

For more information, see How to Create Custom Categories.

Additional Policy Modes

The Barracuda SecureEdge Manager allows administrators to configure Web Filter policies to protect against potential threats and enforce corporate policies. The Web Filter policies now also offer the actions Alert and Warn. With the enhanced Web Filter rule, you can also either alert or warn users against suspicious traffic.



Demo Enterprises Inc/Production

Security Policy › Web Filter › Policies

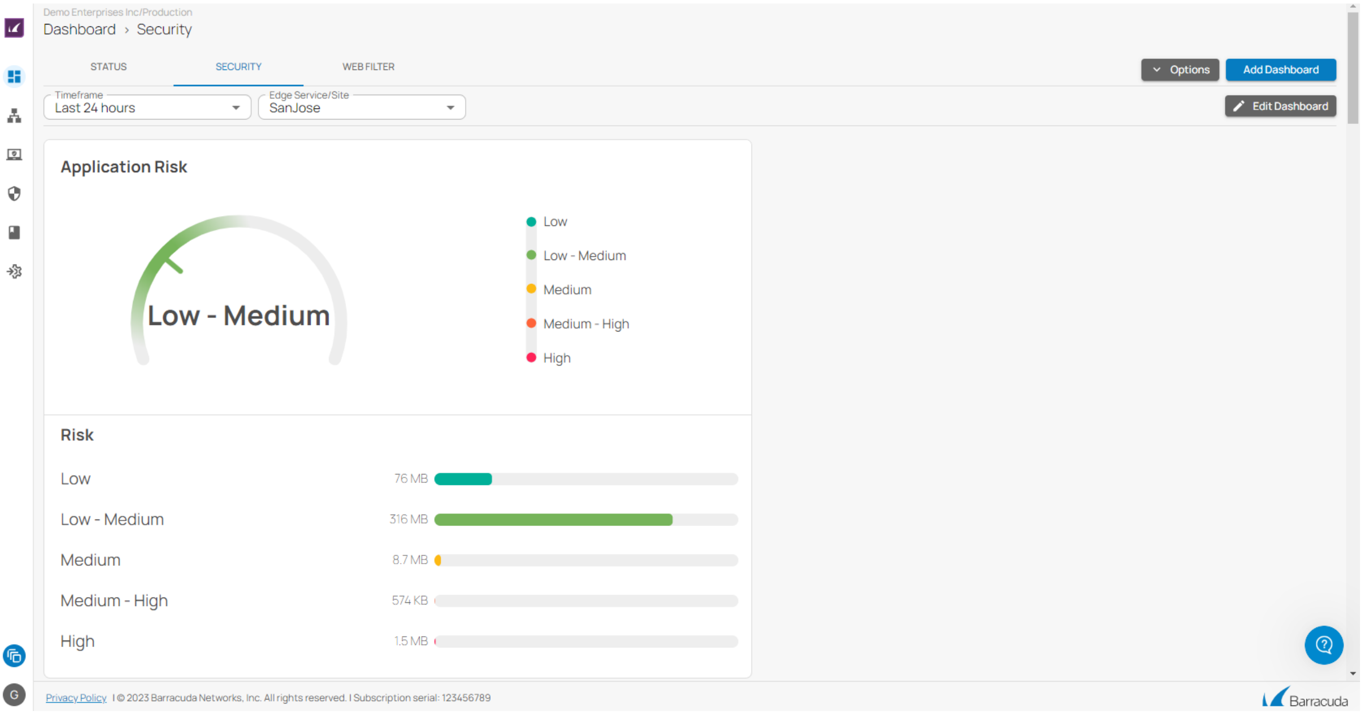
Default Action: Allow

ORDER	NAME	DESCRIPTION	ACTION	DESTINATION
1	AdultMaterial		Block	Categories (Adult Porn, +6)
2	Financial Services		Block	Categories (Financial Products, +2)
3	RiskySites		Alert	Custom Categories (Riskysites)
4	Social		Warn	Categories (Social Networks in General)
5	Default		Block	Categories (Botnets, +3)

For more information, see Web Filter Policies and How to Create an Explicit Web Filter Policy.

SecureEdge Dashboard

A new, enhanced Barracuda SecureEdge dashboard is now available. The main dashboard of SecureEdge consists of three customizable pages: a general dashboard, an SWG dashboard, and a security dashboard.



Demo Enterprises Inc/Production

Dashboard › Security

Timeframe: Last 24 hours

Edge Service/Site: SanJose

Application Risk

Low - Medium

Risk

Low	76 MB
Low - Medium	316 MB
Medium	8.7 MB
Medium - High	574 KB
High	1.5 MB

Privacy Policy | © 2023 Barracuda Networks, Inc. All rights reserved. | Subscription serial: 123456789

For more information, see Dashboard and How to Customize a SecureEdge Dashboard.

Bridging Features

The Barracuda SecureEdge Manager allows you to create a switch bridge for Private Edge services and sites. In addition, you can also create an inline bridge that is available only for stand-alone sites, which includes both HA and non-HA pairs.

For more information, see:

- Bridging
- How to Create a Switch Bridge
- How to Create an Inline Bridge on an Existing Stand-Alone Site
- How to Create an Inline Bridge on a Stand-Alone Site

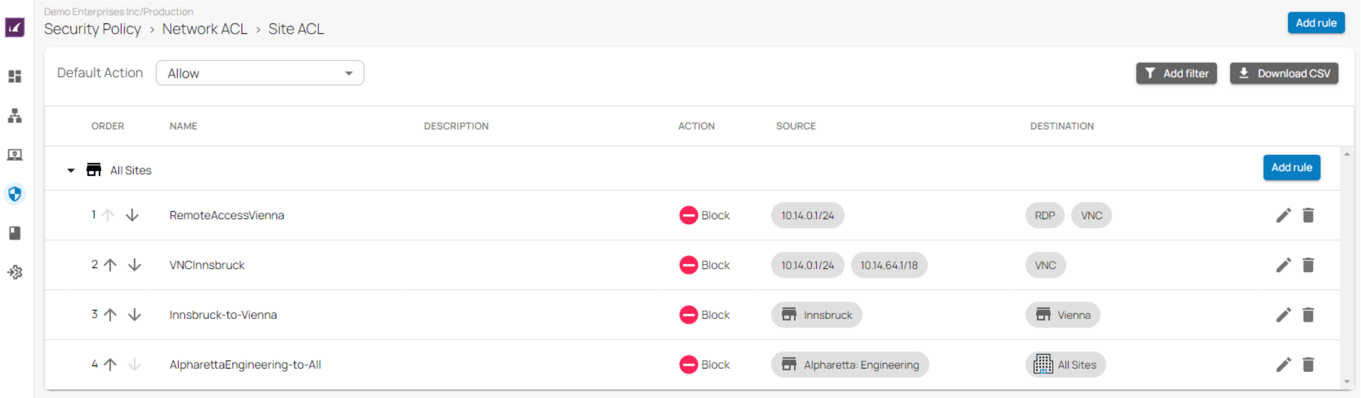
Health Check for WAN Interfaces

For selected sites or Private Edge services, you can configure health check for WAN interfaces.

For more information, see How to Enable Health Check for WAN Interfaces.

ICMP for Access Control Lists

The Barracuda SecureEdge Manager allow you to configure access control and security policies via the **Security Policy** icon in the Cloud UI. With access control lists, you can now configure ICMP either to allow or deny access based on source and destination.



Demo Enterprises Inc/Production
Security Policy › Network ACL › Site ACL

Default Action: Allow

All Sites

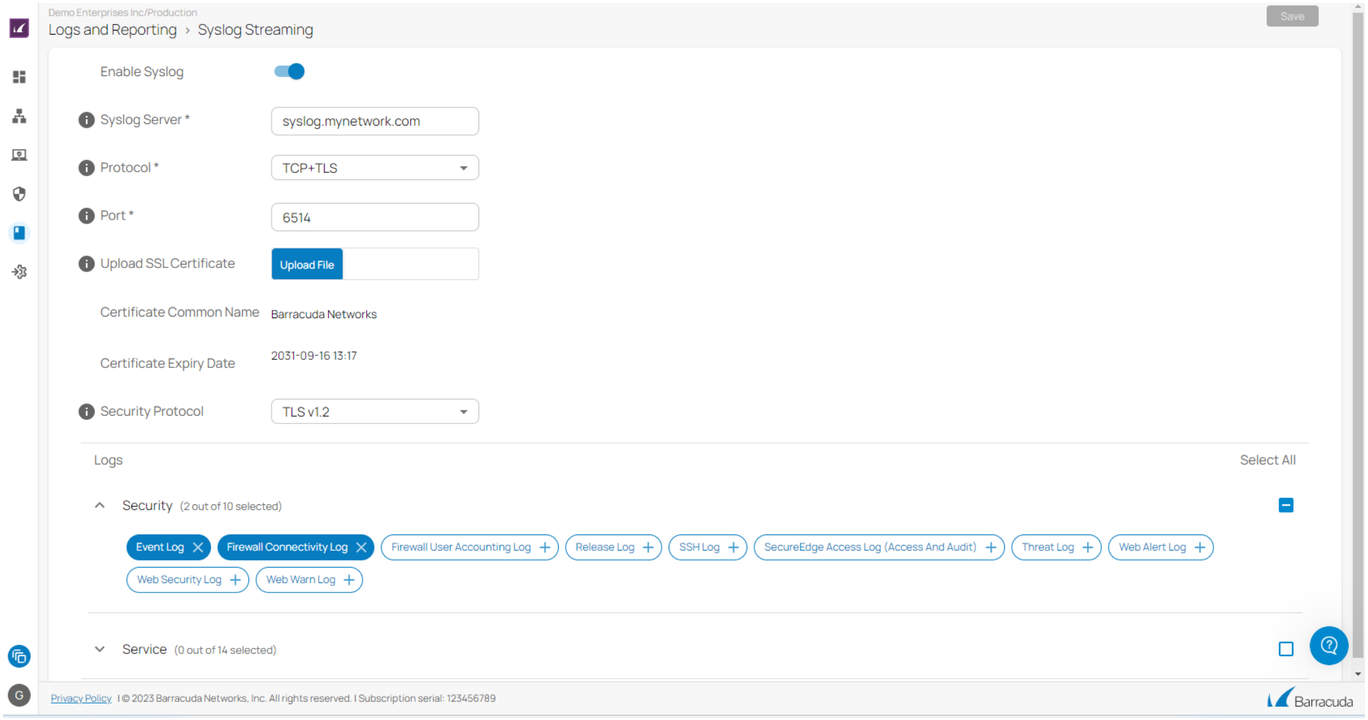
ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION
1	RemoteAccessVienna		Block	10.14.0.1/24	RDP VNC
2	VNCInnsbruck		Block	10.14.0.1/24 10.14.64.1/18	VNC
3	Innsbruck-to-Vienna		Block	Innsbruck	Vienna
4	AlpharettaEngineering-to-All		Block	Alpharetta: Engineering	All Sites

For more information, see Network Policies.

- For information on Edge Service ACL, see How to Create an Edge Service ACL.
- For information on Site ACL, see How to Create a Site ACL.

Updated Syslog Streaming Capabilities

The Barracuda SecureEdge Manager allows administrators to configure syslog streaming. New log files have been added such as the web alert log, web security log, web warn log, and web monitor alert log.


Demo Enterprises Inc/Production
Logs and Reporting › Syslog Streaming

Save

Enable Syslog: on
Syslog Server *: syslog.mynetwork.com
Protocol *: TCP+TLS
Port *: 6514
Upload SSL Certificate: Upload File
Certificate Common Name: Barracuda Networks
Certificate Expiry Date: 2031-09-16 13:17
Security Protocol: TLS v1.2

Logs — Select All

Security (2 out of 10 selected)
Event Log ✕ | Firewall Connectivity Log ✕ | Firewall User Accounting Log + | Release Log + | SSH Log + | SecureEdge Access Log (Access And Audit) + | Threat Log + | Web Alert Log + | Web Security Log + | Web Warn Log +

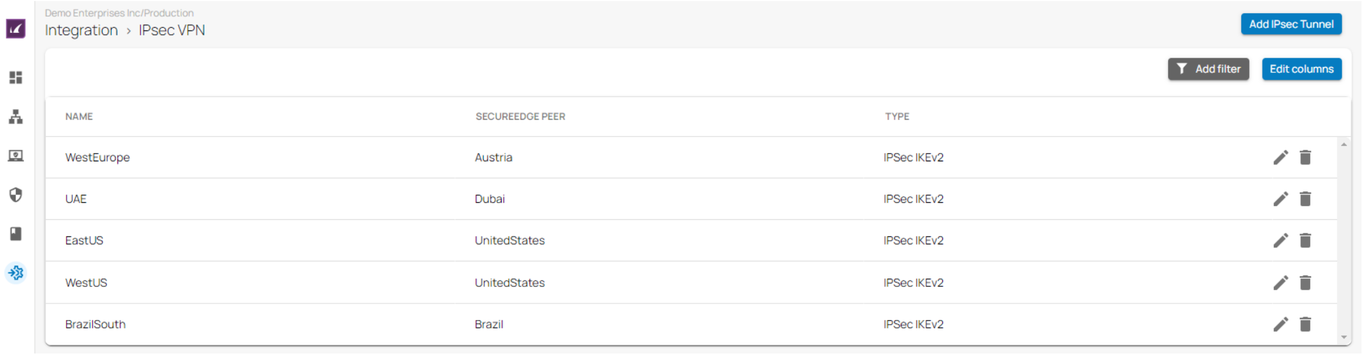
Service (0 out of 14 selected) □

Privacy Policy I © 2023 Barracuda Networks, Inc. All rights reserved. I Subscription serial: 123456789

For more information, see How to Configure Syslog Streaming in SecureEdge.

IPsec VPN

Barracuda SecureEdge can establish IPsec VPN tunnels to any standard-compliant third-party IKEv2 IPsec VPN gateway. The IPsec VPN protocol is the industry-standard VPN protocol and allows you to create site-to-site IKEv2 VPN tunnels to third-party VPN gateways.


Demo Enterprises Inc/Production
Integration › IPsec VPN

NAME	SECUREEDGE PEER	TYPE
WestEurope	Austria	IPsec IKEv2
UAE	Dubai	IPsec IKEv2
EastUS	UnitedStates	IPsec IKEv2
WestUS	UnitedStates	IPsec IKEv2
BrazilSouth	Brazil	IPsec IKEv2

For more information, see How to Configure a Site-to-Site IPsec IKEv2 VPN Tunnel on SecureEdge Using Static Routing.

For more information on Teridion Integration in SecureEdge, see How to Connect Barracuda SecureEdge to Teridion via IPsec Static Routing and How to Connect Barracuda SecureEdge to Teridion via Dynamic Routing (BGP) over IPsec.

Available Hotfixes

Hotfix 1099 - Cumulative 9.0.0 for CloudGen Firewall and SecureEdge.

Summary:

- This hotfix now bonds interfaces to have the correct MAC addresses.
- The VPN service no longer produces errors when forward error correction is used in combination with bandwidth probing.
- Fixes CVE-2023-2650 (OpenSSL).
- TINA site-to-site transports no longer malfunction if a PPPoE provider has been configured.

To download the package, go to https://dlportal.barracudanetworks.com/#/packages/5682/cumulative-1099-9.0.0-187145908.tgz.

To download the new update package including the hotfixes, go to https://dlportal.barracudanetworks.com/#/packages/5684/update.GWAY-9.0.0-0511+2hotfixes.tgz

Hotfix 1104 - SecureEdge Security

Summary:

- This hotfix now fixes a kernel crash in VPN with enabled FEC.

Hotfix 1102 - Cumulative 9.0.0 for CloudGen Firewall and SecureEdge.

Summary:

- This hotfix now includes syslog streaming and Barracuda XDR capabilities for SecureEdge.
- Fixes a kernel crash caused by configuration changes and session re-evaluations.

Hotfix 1110 - SecureEdge Security

Summary:

- Fixes a routing issue on Azure Virtual WAN Edge Services.
- Allows configuration of several PPPoE devices.
- This hotfix now allows site-to-site traffic for IPsec tunnels with static routing over SecureEdge Azure Services.

Known Issues 9.0.1

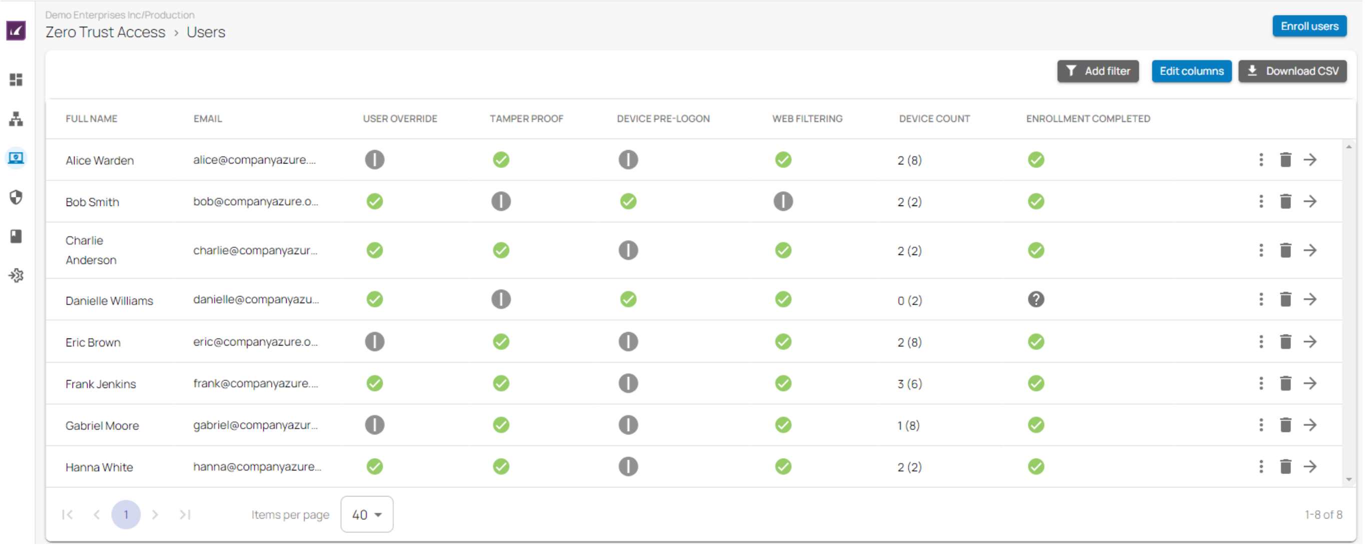
- **Authentication** – The AzureAD user authentication via SecureEdge Manager does not work if the AzureAD user does not have a group affiliation. [BNNGF-92162]

- **IPsec VPN** – The IPsec IKEv2 VPN tunnel does not work with SD-WAN PIN policies. [BNNGF-92515]
- Re-imaging boxes via a USB drive with two ISO images does not work. The newest ISO image does not override the older one and makes the /art directory full. [BNNGF-92603]
- **Bridge** – Reconfiguring a WSG Bridge, leads to broken ARP negotiation and causes internet outages. [BNNGF-92703]
- **SecureEdge Access Agent** – The SecureEdge Access Agent does not work when the VPN service is not listening on fallback port 443. [BNNGF-93219]

What's New in Version 9.0.2

SecureEdge Access Mass Enrollment

The Barracuda SecureEdge Manager allows administrators for mass enrollment for SecureEdge Access with their respective devices. You can now enroll multiple groups and users at the same time



FULL NAME	EMAIL	USER OVERRIDE	TAMPER PROOF	DEVICE PRE-LOGON	WEB FILTERING	DEVICE COUNT	ENROLLMENT COMPLETED
Alice Warden	alice@companyazure....	ⓘ	✓	ⓘ	✓	2 (8)	✓
Bob Smith	bob@companyazure.o...	✓	ⓘ	✓	ⓘ	2 (2)	✓
Charlie Anderson	charlie@companyazur...	✓	✓	ⓘ	✓	2 (2)	✓
Danielle Williams	danielle@companyazu...	✓	ⓘ	✓	✓	0 (2)	?
Eric Brown	eric@companyazure.o...	ⓘ	✓	ⓘ	✓	2 (8)	✓
Frank Jenkins	frank@companyazure....	✓	✓	ⓘ	✓	3 (6)	✓
Gabriel Moore	gabriel@companyazur...	ⓘ	✓	ⓘ	✓	1 (8)	✓
Hanna White	hanna@companyazure...	✓	✓	ⓘ	✓	2 (2)	✓

For more information, see How to Enroll Users in Barracuda SecureEdge.

SecureEdge Access Global and User Settings

As of the 9.0.2 release, administrators can configure additional SecureEdge Access settings on global and user level. You are provided with several new safety features for SecureEdge Access, such as:

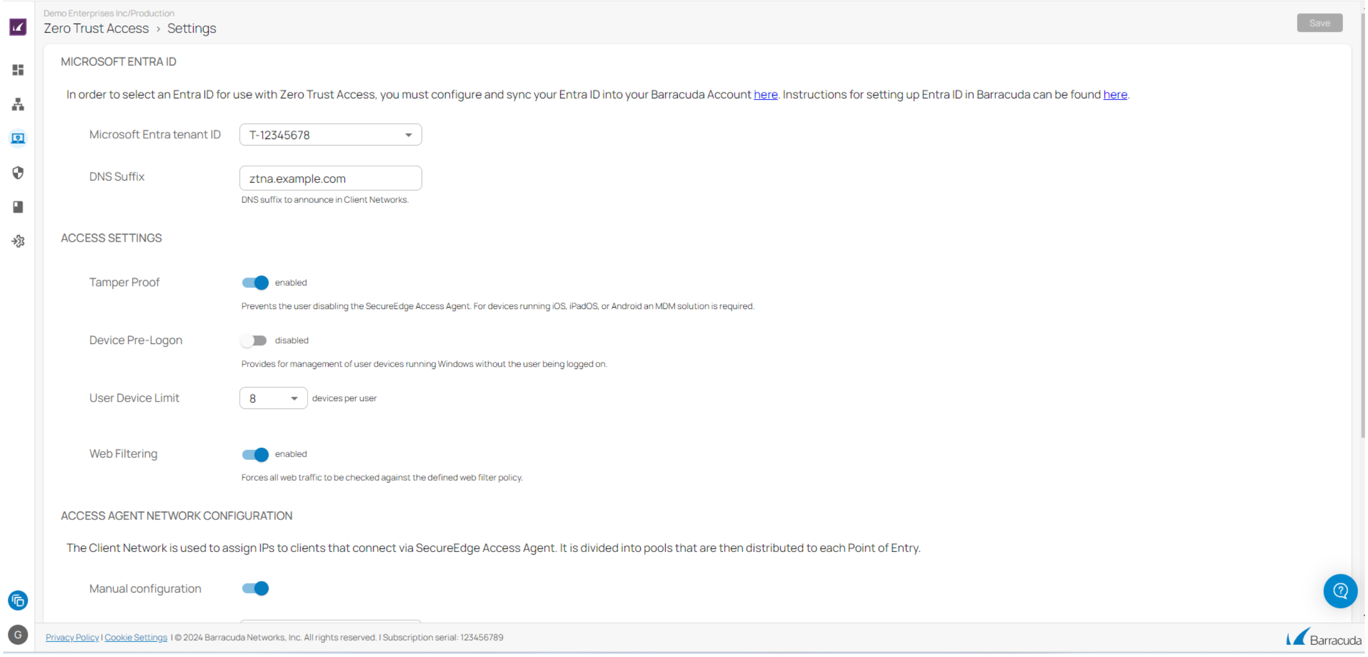
- **Tamper Proof** – User can no longer disable the SecureEdge Access Agent, unenroll the SecureEdge Access Agent, or quit SecureEdge Access Agent by right-clicking on the system tray.
- **Device Pre-Logon** – Enables numerous accounts on Windows to share the same enrollment link. Administrators can manage user devices running Windows without the user being logged

in.

- **User Device Limit** – Refers to the number of devices the user is allowed to enroll.

In addition, you can now override the global SecureEdge Access/Default settings of the ZTNA features and create settings on a user level.

- **User Override** – You can override ZTNA features on each user level.



Demo Enterprises Inc/Production
Zero Trust Access › Settings

MICROSOFT ENTRA ID

In order to select an Entra ID for use with Zero Trust Access, you must configure and sync your Entra ID into your Barracuda Account here. Instructions for setting up Entra ID in Barracuda can be found here.

Microsoft Entra tenant ID: T-12345678

DNS Suffix: ztna.example.com
DNS suffix to announce in Client Networks.

ACCESS SETTINGS

Tamper Proof: enabled
Prevents the user disabling the SecureEdge Access Agent. For devices running iOS, iPadOS, or Android an MDM solution is required.

Device Pre-Logon: disabled
Provides for management of user devices running Windows without the user being logged on.

User Device Limit: 8 devices per user

Web Filtering: enabled
Forces all web traffic to be checked against the defined web filter policy.

ACCESS AGENT NETWORK CONFIGURATION

The Client Network is used to assign IPs to clients that connect via SecureEdge Access Agent. It is divided into pools that are then distributed to each Point of Entry.

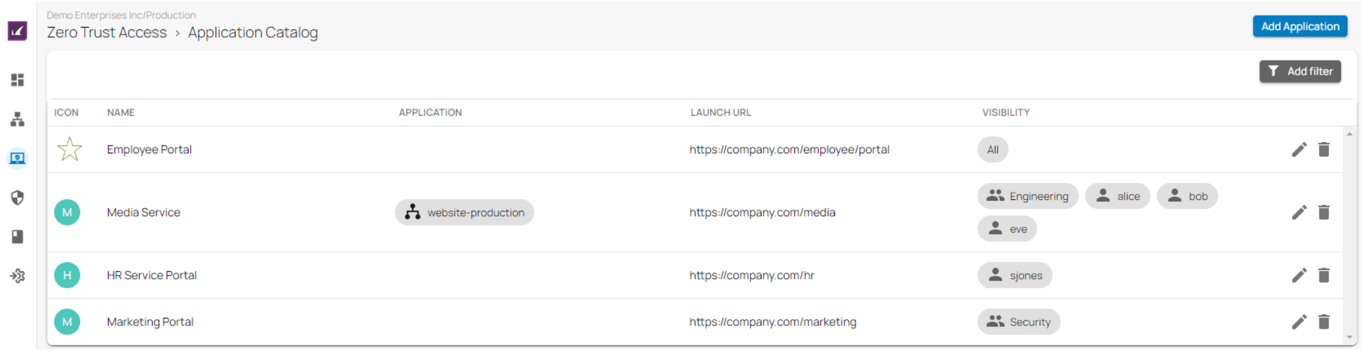
Manual configuration

Privacy Policy | Cookie Settings | © 2024 Barracuda Networks, Inc. All rights reserved. | Subscription serial: 123456789

For more information, see How to Configure SecureEdge Access Global Settings and How to Configure SecureEdge Access User Settings.

Application Catalog Entries

The Barracuda SecureEdge Manager allows administrators to define applications to appear in the SecureEdge Access Agent app for quick access.



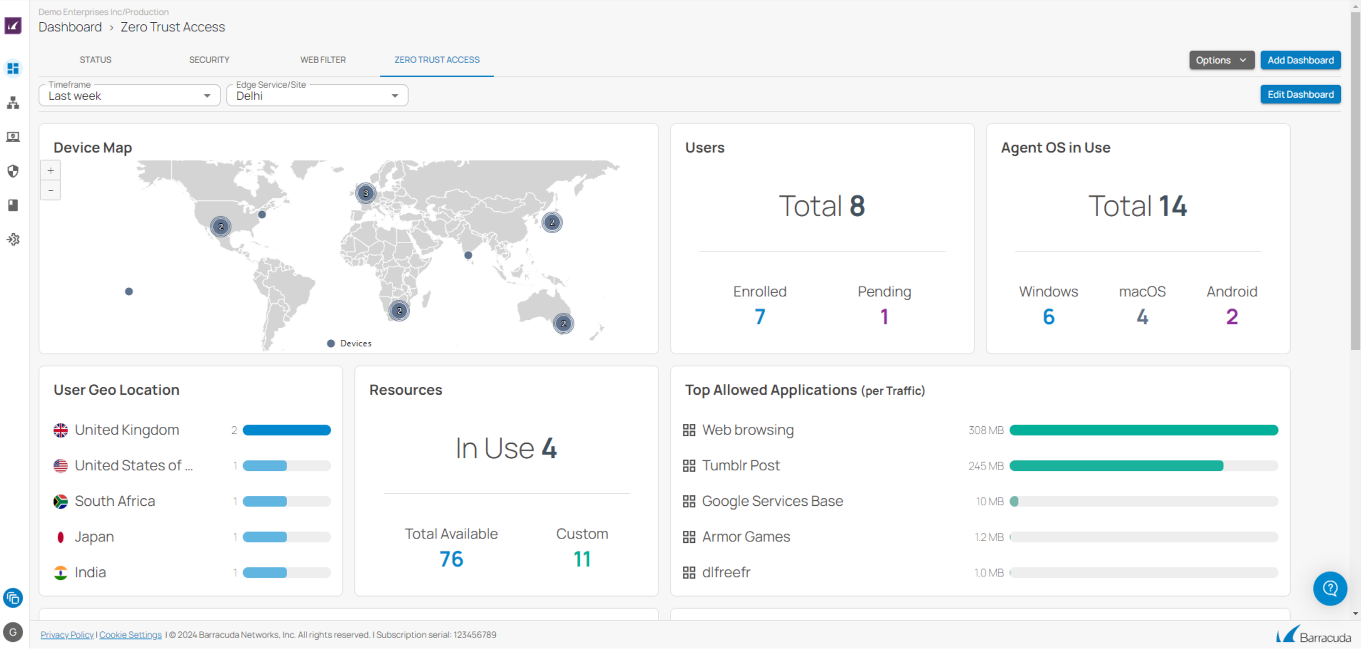
Demo Enterprises Inc/Production
Zero Trust Access › Application Catalog

ICON	NAME	APPLICATION	LAUNCH URL	VISIBILITY
☆	Employee Portal		https://company.com/employee/portal	All
M	Media Service	website-production	https://company.com/media	Engineering alice bob eve
H	HR Service Portal		https://company.com/hr	sjones
M	Marketing Portal		https://company.com/marketing	Security

For more information, see How to Configure Application Catalog Entries

SecureEdge Zero Trust Access Dashboard

A new, Barracuda SecureEdge Zero Trust Access dashboard is now available. The Barracuda SecureEdge Manager allows you to create and customize your own SecureEdge Zero Trust Access dashboards in order to simplify the management of traffic information and status for connected users, resources, and custom applications.


Demo Enterprises Inc/Production
Dashboard › Zero Trust Access
STATUS
SECURITY
WEB FILTER
ZERO TRUST ACCESS
Options
Add Dashboard
Edit Dashboard
Device Map
Devices
Privacy Policy | Cookie Settings | © 2024 Barracuda Networks, Inc. All rights reserved. | Subscription serial: 123456789
Barracuda

Timeframe: Last week

Edge Service/Site: Delhi

Users: Total 8 — Enrolled 7, Pending 1

Agent OS in Use: Total 14 — Windows 6, macOS 4, Android 2

User Geo Location

United Kingdom	2
United States of ...	1
South Africa	1
Japan	1
India	1

Resources: In Use 4 — Total Available 76, Custom 11

Top Allowed Applications (per Traffic)

Web browsing	308 MB
Tumblr Post	245 MB
Google Services Base	10 MB
Armor Games	1.2 MB
dlfreefr	1.0 MB

For more information, see How to Customize a SecureEdge Zero Trust Access Dashboard.

Known Issues 9.0.2

- **ACL Rule** – Setting up the source or destination criteria to all sites and all private Edge Services results in the same networks configured on the box. [SWCS-3988]

Known Issues Related to Azure Log Analytics (OMS)

- On boxes with Azure Log Analytics (OMS) activated, the phibs service does not restart automatically after update. To get the service running, a reboot is required.

Figures