Barracuda Industrial Security

Solutions for Industrial Control Systems (ICS) and Operational Technology (OT)

Product Overview

www.pmddatasolutions.com

Table of contents

ABOUT BARRACUDA NETWORKS . . . 3

SECURING INDUSTRIAL ENVIRONMENTS . . . 4

CHALLENGES AND USE CASES . . . 5

- Transparent micro-segmentation and isolation . . . 5
- On-demand secure remote access . . . 5
- Visibility and permission enforcement . . . 6
- Security automation . . . 6
  - Secure connection between IT and OT . . . 6
  - OT network micro-segmentation . . . 6
  - Virtual patching & OT device-specific security . . . 7
  - Bridged segmentation for every OT entity . . . 7
- Management, reporting, and response automation . . . 8

HARDWARE FACTS . . . 9

- Model comparison . . . 9
- CloudGen Firewall F93A.R. . . . 10
- CloudGen Firewall F183RA . . . 11

CENTRAL ADMINISTRATION . . . 12

- Barracuda Firewall Control Center . . . 12
  - Lifecycle management . . . 12
  - Scalable deployment . . . 13
  - Cloud deployment . . . 13
  - Zero-touch deployment . . . 13
  - Enterprise- and service provider licensing . . . 13
  - Comparison of Barracuda Firewall Control Center models . . . 13

SUPPORTED SCADA PROTOCOLS . . . 14

- S7 sub-protocols . . . 14
- S7+ sub-protocols . . . 15
- IEC 60870-5-104 sub-protocols . . . 16
- IEC 61850 sub-protocols . . . 16
- DNP3 sub-protocols . . . 17
- MODBUS sub-protocols . . . 17

AVAILABLE SUBSCRIPTIONS . . . 18

- Availability matrix . . . 18
- Energize Updates . . . 18
- Barracuda Firewall Insights . . . 19
- Advanced Threat Protection . . . 19
- Malware Protection . . . 19
- Warranty Extension (WE) . . . 20
- Instant Replacement (IR) . . . 20
- Comparison “Warranty Extension - Instant Replacement” . . . 20
- Premium Support . . . 21

ACCESSORIES . . . 22

- USB modem specifications . . . 22

ORDERING INFORMATION . . . 23

- Barracuda CloudGen Firewall - rugged . . . 23
- Barracuda Firewall Control Center . . . 25
  - Virtual Edition . . . 25
  - Microsoft Azure . . . 25
  - Amazon Web Services (AWS) . . . 25
  - Google Cloud Platform (GCP) . . . 25

APPENDIX I - CERTIFICATES . . . 26

- CE Declaration of Confirmity . . . 26
- UN 38.3 Compliance . . . 27

APPENDIX II - USEFUL LINKS . . . 28

APPENDIX III - FEATURES AND CAPABILITIES . . . 29

- Barracuda CloudGen Firewall . . . 29
  - Firewall . . . 29
  - Application control . . . 29
  - Intrusion prevention system . . . 30
  - Malware protection . . . 30
  - Advanced threat protection . . . 30
  - Web filter . . . 31
  - Traffic intelligence & SD-WAN . . . 31
  - Routing & networking . . . 31
  - VPN . . . 31
  - System management . . . 32
  - Logging/monitoring/accounting . . . 32
  - Additional functions . . . 32
  - DNS . . . 32
  - Authoritative DNS Server . . . 32
  - DHCP . . . 33
  - Mail security . . . 33
  - Web proxy . . . 33
  - Rest API extensions . . . 33
  - Cloud-specifics . . . 34
- Advanced Remote Access . . . 34
  - VPN & Network Access Clients . . . 34
  - CudaLaunch & SSL VPN . . . 35
- Barracuda Firewall Control Center . . . 35
  - Configuration management . . . 35
  - Status monitoring . . . 36
  - Trust center . . . 36
  - License center . . . 36
  - Central software update . . . 36
  - Secure remote exec. environment (SSHv2) . . . 36
  - Administrative model . . . 36
  - Reporting and accounting . . . 37
  - Additional functions . . . 37

www.pmddatasolutions.com

About Barracuda Networks

Barracuda Networks provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 200,000 organizations worldwide. Barracuda's expansive product portfolio delivers protection against threats targeting email, web, and network intrusions, as well as products that improve application delivery, network access, message archiving, backup, and data protection, on-premises or in the cloud.

Barracuda's high-value, subscription-based IT solutions provide end-to-end network and data security that helps customers address security threats, improve network performance, and protect and store their data.

Barracuda's international headquarters are in the heart of northern California's Silicon Valley.

www.pmddatasolutions.com

Securing industrial environments with Barracuda

With the introduction of the fourth industrial revolution and smart production concepts the need for connected industrial devices increased massively over the years. However, the typical operational technology (OT) network has some key requirements that makes it differ significantly from a regular IT network.

By nature, a typical OT network has to ensure that the production floor is active all the time. There is no room for downtimes and technicians need to be enabled to carry out maintenance or replacement tasks on short notice.

Having to run a 24x7 production floor with hundreds of production cells that - in an ideal world - all need to be protected, segmented and connected also requires the managing device to centrally hold configuration files and licenses and assign them as required. There is nothing worse than an inactive production cell.

In terms of hardware requirements, there are also different specifications that need to be tackled, enhanced ingress protection (IP) levels, shock resistance and increased temperature ranges. Last but not least everything needs to fit into the switchboard cabinet, neatly mounted on a DIN rail.

OT deployments need an extra portion of robustness to cope with significantly longer product life cycles (often more than 10 years) and highly regulated security and safety requirements.

Barracuda offers highly secure, very compact, and rugged devices for advanced network security, encrypted communications, and cost-effective connectivity. Full integration into the Barracuda Firewall Control Center architecture guarantees hassle-free centralized management for tens of thousands of devices, if needed even in a dark environment.

www.pmddatasolutions.com

Challenges and use cases

The digital transformation of industrial control system (ICS) and operational technology (OT) environments, which include an extended adoption of advanced technologies and connection to regular IT networks, has led to new security challenges due to the lack of air gapping. The rising connectivity between manufacturing plants, critical infrastructure facilities, and smart buildings, and their corresponding external environments has exposed critical operational technology (OT) networks to a threat landscape ranging from targeted attacks to generic ransomware.

To ensure proper security control and risk management, organizations are deploying dedicated security solutions either within the OT network and on the perimeter between IT and OT, or between the internet and OT. In the following, you find some use cases around this topic.

Transparent micro-segmentation and isolation

Micro-segmentation of a factory floor is a must-have from a security standpoint and the more granular the better. This ensures that when a product cell is subject for maintenance or - in worst case - is compromised, all other product cells can remain in active state. In other words, the possible attack surface is smaller with micro-segmentation done right. However, simply placing a big firewall into place and doing segmentation via virtual network segments will not result in the intended security improvement. What happens to the factory floor when dealing with a firmware update of this central firewall or hardware issues? Down-time is no valid option.

Now, Barracuda CloudGen Firewall and its rugged models where purpose-built to ease the process of micro-segmentation significantly:

- RSTP integration for link redundancy and improved resilience
- Bridge deployment with full security enforcement
- Detection, reporting, and enforcement of industrial protocols and sub protocols
- Reset/re-image within minutes with visual feedback (e.g., blinking/flashing lights) rather than audible signals that may not be audible on factory floors
- Quick automatic licensing from existing license pool on the Firewall Control Center instead of cumbersome online activation
- Reporting and alerting on unused firewall rules to avoid traffic bypassing the firewall
- Central logging from hundreds of devices via Barracuda Firewall Insights

On-demand secure remote access

Complex machinery often requires occasional maintenance or control windows by the manufacturer. For security reasons it is mandatory that access to these devices is not enabled all times but needs to be enabled on-demand by the production cell technician. Every rugged Barracuda CloudGen Firewall provides the option to enable remote access temporarily (self expiring) on-demand via a simple-to-use application or web-based user interface. The application can be facilitated by mounting a tablet device at the production cell.

www.pmddatasolutions.com

Visibility and permission enforcement

Depending on the specific requirement for a production floor, it might be mandatory to keep the floor tightly locked down and thoroughly audited.

To ensure that such environments are not compromised, CloudGen Firewall enforces various authentication methods and automatically logs users access. This visibility and permission enforcement allows to have multiple user groups with different access rights. E.g., one group may issue read commands while another group may issue write commands. Again: all of the commands are automatically logged.

Security automation

While Barracuda CloudGen Firewall and Firewall Control Center (see below) already provide various powerful automation tools, Barracuda also partnered up with SCADAfence. Combining the anomaly detection and intimate knowledge of industrial protocols provided by SCADAfence with the security, networking and automation by CloudGen Firewall provides an unmatched level of visibility and protection of the factory floor.

The combined solution is based on the automation API that is available for all CloudGen Firewall appliances right out of the box. Let us glance at a couple of refined use cases for security automation with CloudGen Firewall and SCADAfence:

Secure connection between IT and OT

The Barracuda CloudGen Firewall is implemented between the IT network and the OT network and between the OT network and the internet. The SCADAfence platform monitors the internal network communication and provides the CloudGen Firewall with detailed information on the industrial assets, alerts on anomalous network behavior, and warnings of risks and vulnerabilities. Once SCADAfence detects an anomaly, CloudGen Firewall automatically blocks the respective malicious source at the OT network ingress point.

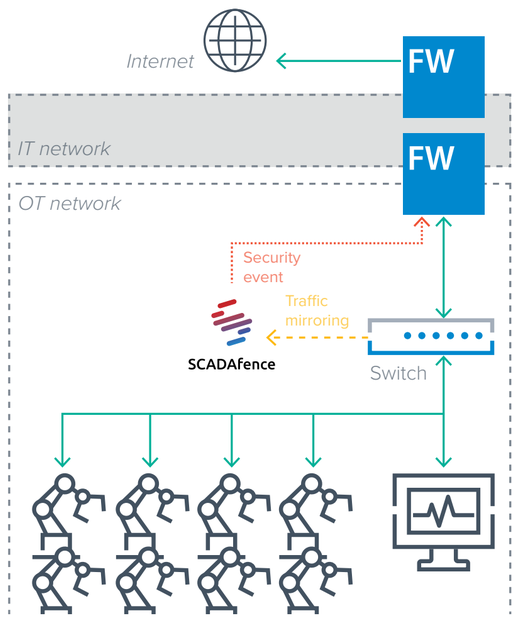


Figure 1 - Secure connection between IT and OT

OT network micro-segmentation

In this scenario, in addition to securing the outbound communications, the Barracuda CloudGen Firewall is also implemented in the internal OT network to create micro-segmentation between different zones. In this use case, OT production areas are divided into zones to create small network segments. Each segment has a designated purpose, and access between the segments is limited or blocked.

As already mentioned earlier, micro-segmentation in OT networks limits the potential damage caused by malicious attacks and non-malicious human errors.

By leveraging SCADAfence's internal OT network visibility and asset management, the Barracuda CloudGen Firewall can be easily configured to limit communications between different zones based on actual network traffic analysis.

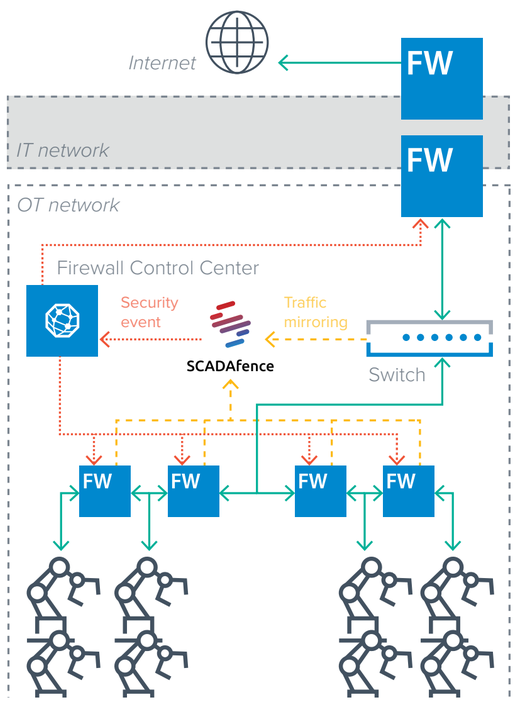


Figure 2 - OT network micro-segmentation

www.pmddatasolutions.com

Virtual patching & OT device-specific security

Adding CloudGen Firewall units to protect specific OT devices allows administrators to enforce specific security policies for sensitive or vulnerable devices. This is especially powerful when there are specific devices that are more critical for the process and, therefore, require increased security control. In addition, if there are legacy devices with known vulnerabilities that are unpatchable, placing a firewall adjacent to them allows you to block unwanted communications and to significantly reduce the potential attack surface. The combination of SCADAfence and Barracuda enables you to identify the most critical or vulnerable devices according to their network activities and vulnerabilities. Once these devices are identified, the firewalls can be properly configured based on their actual role in the environment.

Bridged segmentation for every OT entity

CloudGen Firewall devices are implemented between the IT network and the OT network. In addition, a rugged version protects every entity of the OT network in bridge mode. Every CloudGen Firewall is centrally managed by the Firewall Control Center. The SCADAfence platform monitors the internal network communication and provides the Firewall Control Center with detailed information on the industrial assets, alerts on anomalous network behavior, and warnings of risks and vulnerabilities. Once SCADAfence detects an anomaly, it automatically notifies the Firewall Control Center.

The Firewall Control Center automatically distributes the information to all deployed CloudGen Firewall instances, where the respective malicious source is automatically blocked.

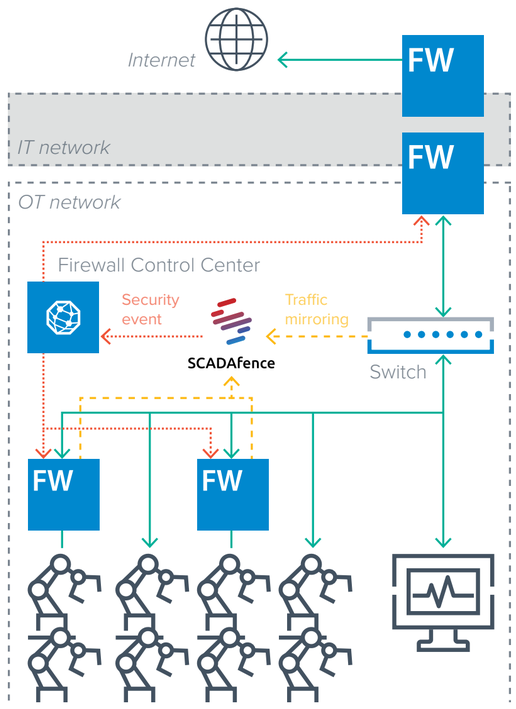


Figure 3 - Virtual patching & OT device-specific security

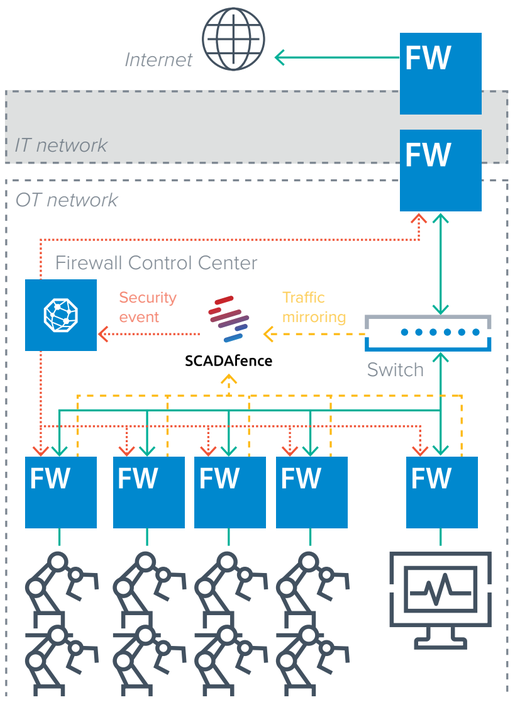


Figure 4 - Bridged segmentation for every OT entity

www.pmddatasolutions.com

Management, reporting, and response automation

The key element for managing CloudGen Firewall deployments is Barracuda Firewall Control Center. This virtual appliance is purpose-built for managing the entire life-cycle via a single user interface and enables “automated” management (e.g., a security policy is changed automatically across all managed devices).

Now, lifecycle management of the Barracuda devices is also compatible to the world’s leading version control and data management system for automated production: Auvesy versiondog. From within versiondog a USB key can be created that is then used by floor personnel for re-imaging the affected device within minutes in case of a needed replacement. Licensing changes are automatically accommodated in the background by the Firewall Control Center.

Updates to licensing and antivirus/IPS signatures are facilitated without internet access by the factory floor devices with the Firewall Control Center acting as the proxy accessing only Barracuda Networks resources.

Deploying CloudGen Firewall in bridge-mode is a common use case. As the drop-in deployment of security devices relies on a transparent layer 2 bridge it would be easy to circumvent security by just bypassing the security device. To avoid this the usage of the firewall bridge rule can be monitored with Firewall Control Center.

For centralized reporting across thousands of deployments, Barracuda provides an additional solution called Barracuda Firewall Insights for consolidating network traffic analysis and reports.

Last but not least all functions of the security device itself as well as the central management can be automated via REST-API functionality. This allows to automate response to incidents discovered by, e.g., SCADAfence (see above).

www.pmddatasolutions.com

Hardware facts

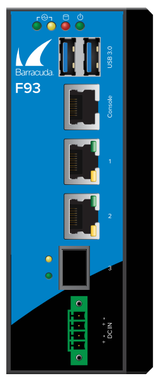
Model comparison

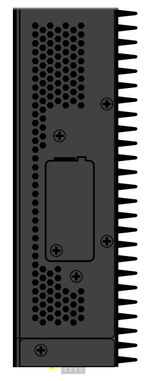
Barracuda offers different models of rugged appliances. For easier navigation through the available models, please find an overview on the differences below:

MODEL COMPARISON	F93A.R	F183RA
More detailed information available on	page 10	page 11
INTERFACES		
Firewall throughput	1.5 Gbps	2.1 Gbps
VPN throughput	240 Mbps	320 Mbps
IPS throughput	400 Mbps	790 Mbps
NGFW throughput	400 Mbps	800 Mbps
Threat protection throughput	380 Mbps	700 Mbps
Concurrent sessions	80,000	100,000
New session/s	8,000	9,000
INTERFACES		
Copper ethernet NICs (1 GbE RJ45)	2x	5x
SFP fiber ethernet NICs (1 GbE)	1x	2x
USB	2x	1x
AVAILABLE SOFTWARE/FEATURE SUBSCRIPTIONS (EXCERPT, MORE DETAILED ON **PAGE 18FF.**)		
Energize Updates	**Mandatory**	
Firewall Insights	**Optional**	
Advanced Threat Protection	**Optional**	
Malware Protection	**Optional**	
Advanced Remote Access	**Optional**	
AVAILABLE HARDWARE/SUPPORT SUBSCRIPTIONS (EXCERPT, MORE DETAILED ON **PAGE 18FF.**)		
Warranty Extension	**Optional**	
Instant Replacement	**Optional**	
Premium Support	depends on product mix and size of deployment	
STANDARDS AND CERTIFICATIONS		
Shock and vibration resistance	IEC 60068, IEC 60950, IEC 61000, ISTA 2A	IEC 60068, IEC 60950, IEC 61000, ISTA 2A
Protection classification	IP20	IP20 standard
		IP30 with I/O rubber covers and power supply via Phoenix 6-pin
CE emissions	✓	✓
CE electrical safety	✓	✓
FCC emissions	✓	✓
ROHS compliant	✓	✓

www.pmddatasolutions.com

CloudGen Firewall F93A.R





INTERFACES	
Copper ethernet NICs (1 GbE RJ45)	2x
SFP fiber NICs (1 GbE)	1x
USB 3.0	2x
ESD protection	15KV
PERFORMANCE [AS OF FIRMWARE RELEASE 8.0.X]	
Firewall throughput [Gbps][a]	1.5
VPN throughput [AES-128, TINA std hash, Mbps][b]	240
VPN throughput [AES-256, TINA std hash, Mbps][b]	200
VPN throughput [AES-256, SHA256, Mbps][b]	180
VPN throughput [AES-256, MD5, Mbps][b]	200
VPN throughput [AES-256, GCM, Mbps][b]	180
IPS throughput [Mbps][c]	400
NGFW throughput [Mbps][d]	400
Threat protection throughput [Mbps][e]	380
Concurrent sessions	80,000
New sessions/s	8,000
Max. number of concurrent users[f]	50-100
MEMORY	
RAM [GB]	4
MASS STORAGE	
Type	SSD
Size ([GB] or better)	100
SIZE, WEIGHT, DIMENSIONS	
Weight appliance [lbs] / [kg]	2.6 / 1.2
Appliance size: width x depth x height [in]	2.04 x 5.9 x 5.11
Appliance size: width x depth x height [mm]	52 x 150 x 130
Weight carton with appliance [lbs] / [kg]	4.8 / 2.2
Carton size: width x depth x height [in]	10 x 10 x 12
Carton size: width x depth x height [mm]	254 x 254 x 305
Form factor	Compact, DIN rail mount
HARDWARE	
Cooling	Fanless
ENVIRONMENTAL	
Noise emission [db/A]	n/a
Operating temperature [°F] / [°C]	-40 to +167 / -40 to +75
Storage temperature [°F] / [°C]	-40 to +185 / -40 to +85
Operating humidity (non-condensing)	5% to 95%
Magnetic isolation protection	1.5KV built-in

MTBF [SYSTEM]	
MTBF [yrs.][g]	> 9
POWER AND EFFICIENCY	
Power supply	Single
Power supply type	Phoenix 4-pin with lock
Power type [AC/DC]	DC
Input ratings [Volts]	12-36
Max. power draw [W]	60
Max. power draw @ 24V [Amps]	2.5
Max. heat dissipation [W]	60
CERTIFICATIONS AND COMPLIANCE (ALSO SEE PAGE 26)	
CE emissions	✓
CE electrical safety	✓
FCC emissions	✓
ROHS compliant	✓
Shock and vibration resistance	IEC 60068
	IEC 60950
	IEC 61000
	ISTA 2A
Protection classification	IP20
PACKAGING CONTENT	
Appliance	✓
DIN rail mount bracket	✓
Quick start guide	✓

All performance values are measured under optimized conditions and are to be considered as „up to“ values and may vary depending on system configuration and infrastructure:

a Firewall throughput measured with large packets (MTU1500) UDP packets, bi-directional across multiple ports.

b VPN performance is based on 1415 Byte UDP packets, bidirectional using BreakingPoint traffic generator.

c IPS throughput is measured using large packets (MTU1500) UDP traffic and across multiple ports.

d NGFW throughput is measured with IPS, application control, and web filter enabled, based on BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirectional across multiple ports.

e Threat protection throughput is measured with IPS, application control, web filter, and cloud-based antivirus and SSL inspection enabled (as part of an active Advanced Threat Protection subscription), based on BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirectional across multiple ports.

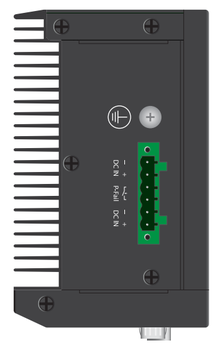
f Depending on feature set; for more detailed information on sizing, please use the free sizing application "Firewall Blueprint" for iOS - available for iPhones and iPads.

g MTBF according to common usage. High load on SSD and extreme environmental conditions might reduce MTBF.

Errors and omissions excepted. Specifications subject to change without notice.

www.pmddatasolutions.com

CloudGen Firewall F183RA



INTERFACES	
Copper ethernet NICs (1 GbE RJ45)	5x
SFP fiber NICs (1 GbE)	2x
USB 2.0	1x
USB 3.0	1x
Serial / console (DB9 RS232)	1x
ESD protection	15KV
PERFORMANCE [AS OF FIRMWARE RELEASE 8.0.X]	
Firewall throughput [Gbps] [a]	2.1
VPN throughput [AES-128, TINA std hash, Mbps] [b]	320
VPN throughput [AES-256, TINA std hash, Mbps] [b]	300
VPN throughput [AES-256, SHA256, Mbps] [b]	190
VPN throughput [AES-256, MD5, Mbps] [b]	270
VPN throughput [AES-256, GCM, Mbps] [b]	190
IPS throughput [Mbps] [c]	790
NGFW throughput [Mbps] [d]	800
Threat protection throughput [Mbps] [e]	700
Concurrent sessions	100,000
New sessions/s	9,000
Max. number of concurrent users [f]	75-150
MEMORY	
RAM [GB]	4
MASS STORAGE	
Type	SSD
Size ([GB] or better)	100
SIZE, WEIGHT, DIMENSIONS	
Weight appliance [lbs] / [kg]	2.2 / 1.0
Appliance size: width x depth x height [in]	3.07 x 5 x 5.75
Appliance size: width x depth x height [mm]	78 x 127 x 146
Weight carton with appliance [lbs] / [kg]	4.8 / 2.33
Carton size: width x depth x height [in]	10 x 10 x 12
Carton size: width x depth x height [mm]	254 x 254 x 305
Form factor	Compact, DIN rail mount
HARDWARE	
Cooling	Fanless
ENVIRONMENTAL	
Noise emission [db/A]	n/a
Operating temperature [°F] / [°C]	-40 to +167 / -40 to +75
Storage temperature [°F] / [°C]	-40 to +185 / -40 to +85
Operating humidity (non-condensing)	5% to 95%
Magnetic isolation protection	1.5KV built-in

MTBF [SYSTEM]	
MTBF [yrs.] [g]	> 9
POWER AND EFFICIENCY	
Power supply	Single
Power supply type	Phoenix 6-pin with lock
Optional power supply	External power brick
Power type [AC/DC]	DC
Input ratings [Volts]	12-36
Max. power draw [W]	60
Max. power draw @ 24V [Amps]	2.5
Max. heat dissipation [W]	60
CERTIFICATIONS AND COMPLIANCE (ALSO SEE PAGE 26)	
CE emissions	✓
CE electrical safety	✓
FCC emissions	✓
ROHS compliant	✓
Shock and vibration resistance	IEC 60068
	IEC 60950
	IEC 61000
	ISTA 2A
Protection classification	IP20 standard
	IP30 with I/O rubber covers and power supply via Phoenix 6-pin
PACKAGING CONTENT	
Appliance	✓
DIN rail mount bracket	✓
I/O rubber covers	✓
Quick start guide	✓

All performance values are measured under optimized conditions and are to be considered as „up to“ values and may vary depending on system configuration and infrastructure:

a Firewall throughput measured with large packets (MTU1500) UDP packets, bi-directional across multiple ports.

b VPN performance is based on 1415 Byte UDP packets, bidirectional using BreakingPoint traffic generator.

c IPS throughput is measured using large packets (MTU1500) UDP traffic and across multiple ports.

d NGFW throughput is measured with IPS, application control, and web filter enabled, based on BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirectional across multiple ports.

e Threat protection throughput is measured with IPS, application control, web filter, and cloud-based antivirus and SSL inspection enabled (as part of an active Advanced Threat Protection subscription), based on BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirectional across multiple ports.

f Depending on feature set; for more detailed information on sizing, please use the free sizing application "Firewall Blueprint" for iOS - available for iPhones and iPads.

g MTBF according to common usage. High load on SSD and extreme environmental conditions might reduce MTBF.

Errors and omissions excepted. Specifications subject to change without notice.

www.pmddatasolutions.com

Central administration

Barracuda Firewall Control Center

To centralize management across many different firewalls and remote access users, the Barracuda Firewall Control Center enables administrators to manage and configure security, content, traffic management, and network access policies from a single interface. Template-based configuration and globally available security objects enable efficient configuration across thousands of locations.

The Firewall Control Center helps significantly to reduce the cost associated with security management while providing extra functionality both centrally and locally at the managed gateway. Software patches and version upgrades are centrally controlled from within the management console and deployment can be applied to all managed devices.

Highly customizable administrative roles can be defined to delegate administrative capabilities for specific departments or locations.

Lifecycle management

Scalable CloudGen Firewall deployments offer companies sustainable investment protection. Energize Updates automatically provide the latest firmware and threat definitions to keep the appliance up to date. With a maintained Instant Replacement subscription, organizations receive a new appliance with the latest specifications every four years.

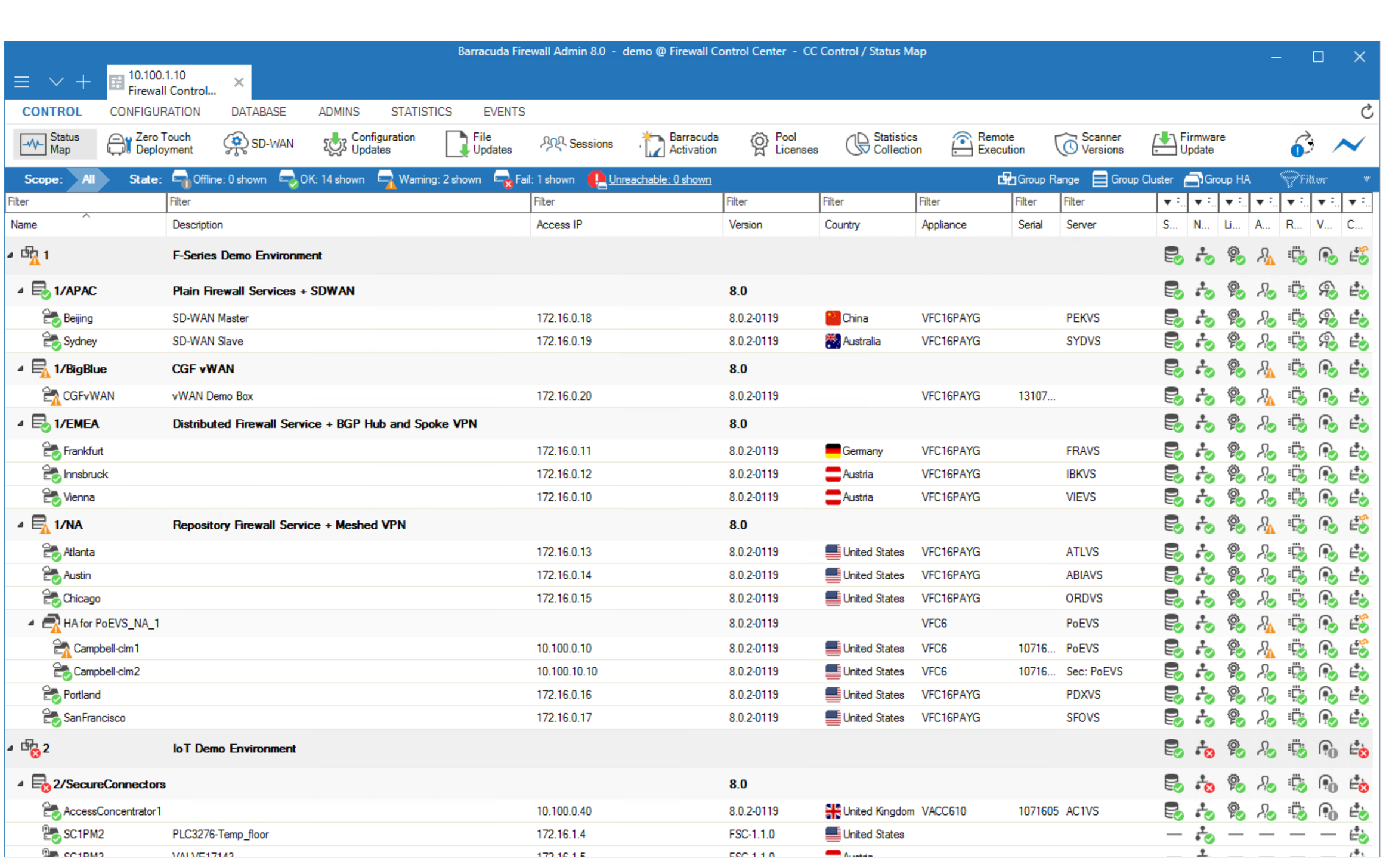


Figure 5 - Firewall Control Center's Status Map displays a drill down status overview of all centrally managed CloudGen Firewall deployments.

www.pmddatasolutions.com

Scalable deployment

Managing the security posture in an OT network can be painful and extremely time consuming. Managing a single firewall deployment may take only 10 minutes per day. With regular central management tools a single deployment can cross the 10-minutes limit very quickly and the larger the network and the smaller the network segments the more hours will be required just to keep the network running.

With Barracuda Firewall Control Center, managing numerous deployments takes the same amount of time as managing one. For more details, please click here.

Cloud deployment

Moving infrastructure to the cloud does not stop at administration tools. Therefore, the Firewall Control Center is available for direct deployment in public cloud offerings like Microsoft Azure, Amazon Web Services, and Google Cloud Platform in a Bring-Your-Own-License model.

Zero-touch deployment

Especially for OT-typical large rollouts without having IT personnel on the ground at remote locations, Firewall Control Center supports zero-touch deployment for all Barracuda components.

This feature allows to send firewall appliances directly to locations without having to pre-setup them beforehand.

After unpacking the appliance and powering it up, the appliance automatically connects to the zero-touch deployment service where it receives are very basic set of information. This information is just enough to create a high-secure TINA VPN connection to the private Firewall Control Center the appliance shall be assigned to.

The full configuration is sent to the appliance via the VPN tunnel and the rugged CloudGen Firewall becomes part of the security infrastructure without the need of dedicated and trained IT security professionals at the location.

Enterprise- and service provider licensing

The Firewall Control Center lets you centrally manage all licensing flexible and independently of hardware. This makes this type of licensing a perfect fit for large numbers of deployments across a wide geographic area.

For more information on this type of licensing, please see the dedicated whitepaper “Enterprise and Service-Provider Licensing“ available on barracuda.com.

Comparison of Barracuda Firewall Control Center models

FEATURES	VC400 VIRTUAL ENVIRONMENT	VCC400 PUBLIC CLOUD	VC610 VIRTUAL ENVIRONMENT	VCC610 PUBLIC CLOUD	VC820 VIRTUAL ENVIRONMENT
Max. no. of managed gateways [Recommended]	Unlimited [20]	Unlimited [20]	Unlimited [hardware-dependent]	Unlimited [hardware-dependent]	Unlimited [hardware-dependent]
Manageable configuration groupings	1	1	Unlimited	Unlimited	Unlimited
Multi-administrator support	✓	✓	✓	✓	✓
Role-based administration	✓	✓	✓	✓	✓
Revision control system	✓	✓	✓	✓	✓
Central statistics	✓	✓	✓	✓	✓
Central syslog host / relay	✓	✓	✓	✓	✓
Firewall audit information collector / viewer	✓	✓	✓	✓	✓
Barracuda access monitor	✓	✓	✓	✓	✓
High availability	Optional	Optional	Optional	Optional	HA license included
Multi-tenancy	-	-	Yes (via configuration groupings)		Yes (5 tenants)
Additional tenant for multi-tenancy	-	-	-	-	Optional

www.pmddatasolutions.com

Supported SCADA protocols

Following, you find an overview on supported protocols that are used in industrial OT environments. For more detailed and most-recent information, please consult the Application Explorer hosted on BarracudaCampus.

S7 sub-protocols

- S7 UserData - Mode Transition
- S7 Stop
- S7 Warm Restart
- S7 Run
- S7 UserData - Cyclic Data
- S7 Cyclic Data Unsubscribe
- S7 Cyclic Data Memory
- S7 Cyclic Data DB
- S7 UserData - Block Functions
- S7 List Blocks
- S7 List Blocks of Given Type
- S7 Get Block Info
- S7 UserData - CPU Functions
- S7 Read SZL
- S7 Notify Indication
- S7 Alarm-8 Indication
- S7 Alarm-8 Unlock
- S7 Alarm Ack
- S7 Alarm Ack Indication
- S7 Alarm Lock Indication
- S7 Alarm Query
- S7 Message Service
- S7 Notify-8 Indication
- S7 Diagnostic Message
- S7 Alarm-8 Lock
- S7 Scan Indication
- S7 Alarm Unlock Indication
- S7 Alarm-SQ Indication
- S7 Alarm-S Indication
- S7 UserData - Time Functions
- S7 Read Clock
- S7 Set Clock
- S7 UserData - Programmer Commands
- S7 Remove Diagnostic Data
- S7 Erase
- S7 Request Diagnostic Data
- S7 Variable Table
- S7 Read Diagnostic Data
- S7 Forces
- S7 UserData - Other Functions
- S7 PLC Password
- S7 PBC BSend/BRecv
- S7 Request/Response
- S7 PLC Stop
- S7 Write
- S7 Download
- S7 CPU Services
- S7 Upload
- S7 PLC Control
- S7 Setup Communication
- S7 Read
- S7 Other
- S7 Ack
- S7 Server Control
- S7 User Data
- S7 Comm (legacy)

www.pmddatasolutions.com

S7+ sub-protocols

- S7+ Notification
- S7+ Notification (new version)
- S7+ Notification (old version)
- S7+ Other
- S7+ Extended Keep Alive
- S7+ Keep Alive
- S7+ Other / Not classified
- S7+ Request/Response
- S7+ Abort
- S7+ Add Link
- S7+ Begin Sequence
- S7+ Create Object
- S7+ Delete Object
- S7+ End Sequence
- S7+ Error
- S7+ Explore
- S7+ Get Link
- S7+ Get Multiple Variables
- S7+ Get Variable
- S7+ Get Variable Address
- S7+ Get Variable Substream
- S7+ Invoke
- S7+ Other
- S7+ Remove Link
- S7+ Set Multiple Variables
- S7+ Set Variable
- S7+ Set Variable Substream

www.pmddatasolutions.com

IEC 60870-5-104 sub-protocols

- IEC 60870-5-104 Process Information in Monitoring Direction
- IEC 60870-5-104 Measured Value - Short Floating Point Number
- IEC 60870-5-104 Packed Single-Point Information with Status Change Detection
- IEC 60870-5-104 Measured Value - Normalized Value without Quality Descriptor
- IEC 60870-5-104 Single-Point Information with Time Tag
- IEC 60870-5-104 Measured Value - Short Floating Point Number with Time Tag
- IEC 60870-5-104 Packed Output Circuit Information of Protection Equipment with Time Tag
- IEC 60870-5-104 Double-Point Information
- IEC 60870-5-104 Step Position Information
- IEC 60870-5-104 Measured Value - Scaled
- IEC 60870-5-104 Integrated Totals
- IEC 60870-5-104 Double-Point Information with Time Tag
- IEC 60870-5-104 Step Position Information with Time Tag
- IEC 60870-5-104 Bitstring of 32 Bits with Time Tag
- IEC 60870-5-104 Event of Protection Equipment with Time Tag
- IEC 60870-5-104 Single-Point Information
- IEC 60870-5-104 Bitstring of 32 Bit
- IEC 60870-5-104 Measured Value - Normalized
- IEC 60870-5-104 Measured Value - Normalized Value with Time Tag
- IEC 60870-5-104 Measured Value - Scaled Value with Time Tag
- IEC 60870-5-104 Integrated Totals with Time Tag
- IEC 60870-5-104 Packed Start Events of Protection Equipment with Time Tag
- IEC 60870-5-104 System Information in Monitoring Direction
- IEC 60870-5-104 End of Initialization
- IEC 60870-5-104 System Information in Control Direction
- IEC 60870-5-104 Counter Interrogation Command
- IEC 60870-5-104 Read Command
- IEC 60870-5-104 Interrogation Command
- IEC 60870-5-104 Reset Process Command
- IEC 60870-5-104 Delay Acquisition Command
- IEC 60870-5-104 Test Command with Time Tag
- IEC 60870-5-104 File Transfer
- IEC 60870-5-104 File Ready
- IEC 60870-5-104 Section Ready
- IEC 60870-5-104 Directory
- IEC 60870-5-104 Call Directory, Select File, Call File, Call Section
- IEC 60870-5-104 ACK File - ACK Section
- IEC 60870-5-104 Segment
- IEC 60870-5-104 Query Log - Request Archive File
- IEC 60870-5-104 Process Information in Control Direction
- IEC 60870-5-104 Single Command
- IEC 60870-5-104 Set Point Command - Normalized Value
- IEC 60870-5-104 Set Point Command - Scaled Value
- IEC 60870-5-104 Set Point Command - Normalized Value with Time Tag
- IEC 60870-5-104 Regulating Step Command
- IEC 60870-5-104 Bitstring of 32 Bits
- IEC 60870-5-104 Single Command with Time Tag
- IEC 60870-5-104 Set Point Command - Short Floating - Point Number with Time Tag
- IEC 60870-5-104 Bitstring of 32 Bits with Time Tag
- IEC 60870-5-104 Double Command
- IEC 60870-5-104 Set Point Command - Short Floating Point Number
- IEC 60870-5-104 Double Command with Time Tag
- IEC 60870-5-104 Regulating Step Command with Time Tag
- IEC 60870-5-104 Set Point Command - Scaled Value with Time Tag
- IEC 60870-5-104 Parameter in Control Direction
- IEC 60870-5-104 Parameter of Measured Value - Normalized Value
- IEC 60870-5-104 Parameter of Measured Value - Scaled Value
- IEC 60870-5-104 Parameter of Measured Value - Short Floating Point Number
- IEC 60870-5-104 Parameter Activation

IEC 61850 sub-protocols

- IEC 61850 Goose
- IEC 61850 MMS
- IEC 61850 SMV
- IEC 61850 General

www.pmddatasolutions.com

DNP3 sub-protocols

- DNP3 Control Functions
- DNP3 Operate
- DNP3 Select
- DNP3 Direct Operate
- DNP3 Direct Operate no ACK
- DNP3 Time Synchronization
- DNP3 Delay Measurement
- DNP3 Record Current Time
- DNP3 Transfer Functions
- DNP3 Read
- DNP3 Write
- DNP3 Confirm
- DNP3 Application Control
- DNP3 Cold Restart
- DNP3 Initialize Application
- DNP3 Start Application
- DNP3 Stop Application
- DNP3 Warm Restart
- DNP3 Initialize Data
- DNP3 Configuration
- DNP3 Save Configuration
- DNP3 Enable Spontaneous Messages
- DNP3 Assign Class
- DNP3 Disable Spontaneous Messages
- DNP3 Activate Configuration
- DNP3 Response Messages
- DNP3 Unsolicited Response
- DNP3 Authentication Response
- DNP3 Response
- DNP3 Other
- DNP3 Authentication Request
- DNP3 Authentication Error
- DNP3 Freeze Functions
- DNP3 Freeze and Clear
- DNP3 Freeze with Time
- DNP3 Immediate Freeze
- DNP3 Freeze and Clear no ACK
- DNP3 Immediate Freeze no ACK
- DNP3 Freeze with Time no ACK
- DNP3 File Access
- DNP3 Open File
- DNP3 Delete File
- DNP3 Abort File
- DNP3 Authenticate File
- DNP3 Close File
- DNP3 Get File Info

MODBUS sub-protocols

- MODBUS Data Access
- MODBUS Read Coils
- MODBUS Read Discrete Inputs
- MODBUS Read Holding Registers
- MODBUS Write Single Register
- MODBUS Read/Write Multiple Registers
- MODBUS Write Single Coil
- MODBUS Write Multiple Coils
- MODBUS Write Multiple Registers
- MODBUS Mask Write Register
- MODBUS Read FIFO Queue
- MODBUS Read Input Register
- MODBUS File Access
- MODBUS Read File Record
- MODBUS Write File Record
- MODBUS Diagnostics
- MODBUS Read Exception Status
- MODBUS Get Communication Event Log
- MODBUS Report Server ID
- MODBUS Diagnostic Check
- MODBUS Get Communication Event Counter
- MODBUS Encapsulated Interface Transport
- MODBUS Read Device Identification
- MODBUS CAN-Open General Reference
- MODBUS (legacy)

www.pmddatasolutions.com

Available subscriptions

Availability matrix

	F93A.R	F183RA
AVAILABLE SOFTWARE/FEATURE SUBSCRIPTIONS		
Energize Updates (EU)	**Mandatory**	
Firewall Insights	Optional	
Malware Protection	Optional	
Advanced Threat Protection	Optional	
AVAILABLE HARDWARE/SUPPORT SUBSCRIPTIONS		
Warranty Extension	Optional	
Instant Replacement	Optional	
Premium Support	Optional	

High Availability (“HA”):

All subscriptions have to be licensed separately for the HA partner. For further information, please contact your local partner or Barracuda Sales at sales@barracuda.com.

Energize Updates

Barracuda Energize Updates help you secure your investment in the ever-changing IT world. Benefit from security updates to patch or repair any security vulnerabilities, keep your Barracuda product up-to-date and fully functional at all times, and get access to our award-winning support.

Energize Updates are available for all rugged CloudGen Firewall models. Monthly subscription; available for up to 5 years. Purchasing at least 12 months of Energize Updates is required with every unit.

Energize Updates includes:

- Basic support, i.e., email support 24/7, and phone support Monday through Friday (9:00 am - 5:00 pm)
- Firmware maintenance including new firmware updates with feature enhancements and bug fixes
- Early release firmware program (optional)
- Unlimited number of client-to-site VPN connections
- Security updates to patch/repair any security vulnerabilities
- Regular updates for Application Control database
- IPS signature and pattern updates.

www.pmddatasolutions.com

Barracuda Firewall Insights

Barracuda Firewall Insights allows to consolidate security, application flow, and connectivity information from hundreds or even thousands of firewalls on the extended WAN – regardless of whether they are hardware, virtual, or cross-cloud-based deployments.

For a Firewall Insights deployment, every device requires an active Firewall Insights subscription and access to the central Firewall Insights server.

Firewall Insights server is available as a virtual image or KVM, VMWare, and Hyper-V with the following requirements:

SSD data size: Unlimited (min. 2 TB)

RAM: Unlimited (min. 32 GB)

CPU cores: Unlimited (min. 8)

IOPS: Unlimited (min. 24,000)

Advanced Threat Protection

Prevent malicious files—even unknown ones—from entering the organization. Avoid network breaches, identify zero-day malware exploits, targeted attacks, advanced persistent threats and other advanced malware that routinely bypass traditional signature based IPS and antivirus engines before they do harm to your network.

Compatibility and Licensing:

Available for all rugged hardware models for up to 5 years.

Requires a valid Web Security or Malware Protection subscription.

In case the monthly file capacity is reached, the system stops forwarding files to the ATP cloud for the rest of the current month.

MODEL	# OF FILES INSPECTED
F93A.R	108,000
F183RA	108,000

Malware Protection

The Malware Protection subscription provides gateway-based protection against malware, viruses, spyware, and other unwanted programs inside SMTP/S, HTTP/S, POP3/S, FTP, and SFTP traffic.

Key benefits of Malware Protection:

- Configurable archive recursion depth
- Quarantine functionality for proxy
- Configurable unknown archive policy
- Configurable maximum archive size
- Archiver package support
- Office file-types support
- Proactive detection of new threats
- Advanced heuristics detection techniques
- Hundreds of thousands signatures

Compatibility and Licensing:

Available for all rugged hardware models. The number of protected IPs (capacity) applies.

Monthly subscription; available for up to 5 years.

In High Availability (HA) environments each unit needs to be licensed separately.

www.pmddatasolutions.com

Warranty Extension (WE)

Provides an extended warranty, and ships a replacement unit on the next business day (best effort) with standard mail upon notification of a failed unit.

Must be purchased within 60 days of hardware purchase and is a continuous subscription from date of activation. Monthly subscription; available for up to 5 years.

Instant Replacement (IR)

One hundred percent uptime is important in corporate environments, but sometimes equipment can fail. In the rare case that a Barracuda product fails, Barracuda ships a replacement unit on the same or next business day. And by means of the Hardware Refresh Program, we ensure that customers benefit from the latest hardware improvements and firmware capabilities:

- Enhanced support providing phone and email support 24/7
- Hard disk replacement on models that have swappable RAID drives
- Free hardware refresh after four years of continuous IR coverage.

Must be purchased within 60 days of hardware purchase and is a continuous subscription from date of activation. Monthly subscription; available for up to 5 years.

Comparison “Warranty Extension - Instant Replacement”

	WARRANTY EXTENSION	INSTANT REPLACEMENT
Replacement	Next business day (best effort)	Same day or next business day
Shipment	Standard	Express
Hard disk replacement (swappable RAID)	Standard shipping	Standard shipping
Support	Basic Support (with EU)	Enhanced Support
Available subscriptions	up to 3 years	up to 5 years
Free hardware refresh after 4 years	-	✓

www.pmddatasolutions.com

Premium Support

Premium Support ensures that an organisation's network is running at its peak performance by providing the highest level of 24/7 technical support for mission-critical environments. A dedicated Premium Support Account Manager and a team of technical engineers provide fast solutions to high-priority support issues, thereby ensuring that Barracuda Networks equipment maintains continuous uptime.

Key benefits of Premium Support:

- Dedicated phone and email support 24/7
- Priority response time to resolve mission-critical issues
- Priority Level Agreement (PLAs) to guarantee that issues are handled, resolved, and closed quickly
- Dedicated Support Account Manager who is familiar with the customer's environment
- Proactive ticket monitoring and reporting to provide comprehensive information and control

Note:

Available for all rugged hardware models for up to 5 years.

For more information on Premium Support please visit https://www.barracuda.com/support/premium.

www.pmddatasolutions.com

Accessories

USB modem specifications

Barracuda Networks cannot guarantee signal reception. In case your deployment is located in a basement or in a place with insufficient signal reception make sure that the signal quality is sufficient, especially prior to purchasing large quantities.
The SIM card is not included and has to be obtained independently through a mobile phone provider.

	MODEM M40	MODEM M41	MODEM M42
Region	EMEA / APAC	North America	North America (Verizon)
PERFORMANCE			
Download / Upload	up to 150 Mbit/s / up to 50 Mbit/s	up to 150 Mbit/s / up to 50 Mbit/s	up to 150 Mbit/s / up to 50 Mbit/s
SUPPORTED FREQUENCIES			
LTE	800/850/900/1800/2100/2600 MHz	700/850/1700/1900/2600 MHz	700/750/850/1700/1900 MHz
UTMS/HSPA/HSPA+	850/900/1900/2100 MHz	850/900/1700/1900/2100 MHz	850/1900 MHz
GSM	850/900/1800/1900 MHz	850/900/1800/1900 MHz	-
ENVIRONMENTAL DATA, QUALITY, AND RELIABILITY			
Operating temperature	-40 to 85 °C / -40 to 185 °F	-40 to 85 °C / -40 to 185 °F	-40 to 85 °C / -40 to 185 °F
RoHS compliant	lead-free	lead-free	lead-free
Manufactured in	ISO/TS 16949 cert. production sites	ISO/TS 16949 cert. production sites	ISO/TS 16949 cert. production sites
ELECTRICAL DATA			
Power supply DC	3.0 to 3.6 V	3.0 to 3.6 V	3.0 to 3.6 V
Power consumption	Idle: 1.8 mA / LTE max power: 815 mA	Idle: 1.8 mA / LTE max power: 815 mA	Idle: 1.8 mA / LTE max power: 815 mA
Certifications and approvals	FCC, CE, RED (R&TTE) RCM / NCC / KC / Giteki / Softbank	FCC, CE, RED (R&TTE) AT&T / T-Mobile / Anatel / Rogers (Canada)	FCC, CE, RED (R&TTE) Verizon

www.pmddatasolutions.com

Ordering information

Barracuda CloudGen Firewall - rugged

Calculation of co-terminus subscriptions:

To allow customers to consolidate their maintenance and subscription offerings to a single end or renewal date, daily rates for all subscription types are offered. These daily rates should be used to extend expiring subscriptions to coincide with the dates of subscriptions expiring in the future. Barracuda does credit early termination of subscriptions using these daily rates.

BARRACUDA CLOUDGEN FIREWALL F93A.R		EMEA / INTERNATIONAL	NORTH AMERICA
Appliance	CloudGen Firewall F93A.R - hardware unit	BNGiF93a.R	BNGF93a.R
	CloudGen Firewall F93A.R - demo unit	BNGiF93a.R--demo	BNGF93a.R--demo
	CloudGen Firewall F93A.R - cold spare unit	BNGiF93a.R--c	BNGF93a.R--c
	CloudGen Firewall F93A.R - hardware only for enterprise licensing (pool)	BNGiF93a.R--hwo	BNGF93a.R--hwo
Appliance-based licensing	Energize Updates (monthly; for up to 5 years)[1]	BNGiF93a.R-e<duration>	BNGF93a.R-e<duration>
	Malware Protection (monthly; for up to 5 years)[1]	BNGiF93a.R-m<duration>	BNGF93a.R-m<duration>
	Advanced Threat Protection (monthly; for up to 5 years)[1]	BNGiF93a.R-a<duration>	BNGF93a.R-a<duration>
	Advanced Remote Access (monthly; for up to 5 years)[1]	BNGiF93a.R-vp<duration>	BNGF93a.R-vp<duration>
	Firewall Insights (monthly; for up to 5 years)[1]	BNGiF93a.R-fi<duration>	BNGF93a.R-fi<duration>
	Premium Support (monthly; for up to 5 years)[1]	BNGiF93a.R-p<duration>	BNGF93a.R-p<duration>
	Instant Replacement (monthly; for up to 5 years)	BNGiF93a.R-h<duration>	BNGF93a.R-h<duration>
	Warranty Extension (monthly; for up to 3 years)	BNGiF93a.R-we<duration>	BNGF93a.R-we<duration>
Enterprise licensing (a.k.a. pool licensing)	Pool account	BNGiF93p	BNGF93p
	Pool base license capacity	BNGiF93pu	BNGF93pu
	Energize Updates (monthly; for up to 5 years)	BNGiF93p-e<duration>	BNGF93p-e<duration>
	Malware Protection (monthly; for up to 5 years)	BNGiF93p-m<duration>	BNGF93p-m<duration>
	Advanced Threat Protection (monthly; for up to 5 years)	BNGiF93p-a<duration>	BNGF93p-a<duration>
	Advanced Remote Access (monthly; for up to 5 years)	BNGiF93p-vp<duration>	BNGF93p-vp<duration>
	Firewall Insights (monthly; for up to 5 years)	BNGiF93p-fi<duration>	BNGF93p-fi<duration>
	Premium Support (monthly; for up to 5 years)	BNGiF93p-p<duration>	BNGF93p-p<duration>
Accessories	External power adapter (not included in packaging)	BNGiF93A.PA009	BNGF93A.PA009
	Spare DIN rail mount kit	BNGiF93A.RK018	BNGF93A.RK018
	USB modem 4G/LTE	BNGiM40a	BNGM41a
	USB modem 4G/LTE - Demo	BNGiM40a--demo	BNGM41a--demo
	USB modem 4G/LTE - Instant Replacement (monthly; for up to 5 years)	BNGiM40a-h<duration>	BNGM41a-h<duration>
	USB modem 4G/LTE - Warranty Extension (monthly; for up to 3 years)	BNGiM40a-we<duration>	BNGM41a-we<duration>
	USB modem 4G/LTE (Verizon)	-	BNGM42a
	USB modem 4G/LTE - Demo	-	BNGM42a--demo
	USB modem 4G/LTE - Instant Replacement (monthly; for up to 5 years)	-	BNGM42a-h<duration>
	USB modem 4G/LTE - Warranty Extension (monthly; for up to 3 years)	-	BNGM42a-we<duration>

1 *Not required if appliance is operated in conjunction with enterprise licensing.*

www.pmddatasolutions.com

BARRACUDA CLOUDGEN FIREWALL F183RA		EMEA / INTERNATIONAL	NORTH AMERICA
Appliance	CloudGen Firewall F183RA - hardware unit	BNGiF183Ra	BNGF183Ra
	CloudGen Firewall F183RA - demo unit	BNGiF183Ra--demo	BNGF183Ra--demo
	CloudGen Firewall F183RA - cold spare unit	BNGiF183Ra--c	BNGF183Ra--c
	CloudGen Firewall F183RA - hardware only for enterprise licensing (pool)	BNGiF183Ra--hwo	BNGF183Ra--hwo
Appliance-based licensing	Energize Updates (monthly; for up to 5 years)[2]	BNGiF183Ra-e<duration>	BNGF183Ra-e<duration>
	Malware Protection (monthly; for up to 5 years)[2]	BNGiF183Ra-m<duration>	BNGF183Ra-m<duration>
	Advanced Threat Protection (monthly; for up to 5 years)[2]	BNGiF183Ra-a<duration>	BNGF183Ra-a<duration>
	Advanced Remote Access (monthly; for up to 5 years)[2]	BNGiF183Ra-vp<duration>	BNGF183Ra-vp<duration>
	Firewall Insights (monthly; for up to 5 years)[2]	BNGiF183Ra-fi<duration>	BNGF183Ra-fi<duration>
	Premium Support (monthly; for up to 5 years)[2]	BNGiF183Ra-p<duration>	BNGF183Ra-p<duration>
	Instant Replacement (monthly; for up to 5 years)	BNGiF183Ra-h<duration>	BNGF183Ra-h<duration>
	Warranty Extension (monthly; for up to 3 years)	BNGiF183Ra-we<duration>	BNGF183Ra-we<duration>
Enterprise licensing (a.k.a. pool licensing)	Pool account	BNGiF183Rp	BNGF183Rp
	Pool base license capacity	BNGiF183Rpu	BNGF183Rpu
	Energize Updates (monthly; for up to 5 years)	BNGiF183Rp-e<duration>	BNGF183Rp-e<duration>
	Malware Protection (monthly; for up to 5 years)	BNGiF183Rp-m<duration>	BNGF183Rp-m<duration>
	Advanced Threat Protection (monthly; for up to 5 years)	BNGiF183Rp-a<duration>	BNGF183Rp-a<duration>
	Advanced Remote Access (monthly; for up to 5 years)	BNGiF183Rp-vp<duration>	BNGF183Rp-vp<duration>
	Firewall Insights (monthly; for up to 5 years)	BNGiF183Rp-fi<duration>	BNGF183Rp-fi<duration>
	Premium Support (monthly; for up to 5 years)	BNGiF183Rp-p<duration>	BNGF183Rp-p<duration>
Accessories	External power supply unit (not included in packaging)	BNGiPSUR1a	BNGPSUR1a
	USB modem 4G/LTE	BNGiM40a	BNGM41a
	USB modem 4G/LTE - Demo	BNGiM40a--demo	BNGM41a--demo
	USB modem 4G/LTE - Instant Replacement (monthly; for up to 5 years)	BNGiM40a-h<duration>	BNGM41a-h<duration>
	USB modem 4G/LTE - Warranty Extension (monthly; for up to 3 years)	BNGiM40a-we<duration>	BNGM41a-we<duration>
	USB modem 4G/LTE (Verizon)	-	BNGM42a
	USB modem 4G/LTE - Demo	-	BNGM42a--demo
	USB modem 4G/LTE - Instant Replacement (monthly; for up to 5 years)	-	BNGM42a-h<duration>
	USB modem 4G/LTE - Warranty Extension (monthly; for up to 3 years)	-	BNGM42a-we<duration>

2 *Not required if appliance is operated in conjunction with enterprise licensing.*

www.pmddatasolutions.com

Barracuda Firewall Control Center

Virtual Edition

FIREWALL CONTROL CENTER VC400	EMEA / INTERNATIONAL	NORTH AMERICA
Barracuda Firewall Control Center VC400 - Standard Edition	BNCiVC400a	BNCVC400a
Energize Updates (monthly; for up to 5 years)	BNCiVC400a-e<duration>	BNCVC400a-e<duration>
Premium Support (monthly; for up to 5 years)	BNCiVC400a-p<duration>	BNCVC400a-p<duration>

FIREWALL CONTROL CENTER VC610	EMEA / INTERNATIONAL	NORTH AMERICA
Barracuda Firewall Control Center VC610 - Enterprise Edition	BNCiVC610a	BNCVC610a
Energize Updates (monthly; for up to 5 years)	BNCiVC610a-e<duration>	BNCVC610a-e<duration>
Premium Support (monthly; for up to 5 years)	BNCiVC610a-p<duration>	BNCVC610a-p<duration>

FIREWALL CONTROL CENTER VC820	EMEA / INTERNATIONAL	NORTH AMERICA
Barracuda Firewall Control Center VC820 - Global Edition	BCCiVC820a	BCCVC820a
Energize Updates (monthly; for up to 5 years)	BCCiVC820a-e<duration>	BCCVC820a-e<duration>
Premium Support (monthly; for up to 5 years)	BCCiVC820a-p<duration>	BCCVC820a-p<duration>
Additional Tenant (Range) for Firewall Control Center VC820 (monthly)	BNCi-b1	BNC-b1

Microsoft Azure

FIREWALL CONTROL CENTER VCC400	EMEA / INTERNATIONAL	NORTH AMERICA
Barracuda Firewall Control Center VCC400 - Standard Edition	BNCiCAZ400a	BNCCAZ400a
Virtual subscription (incl. Energize Updates; monthly; for up to 5 years)	BNCiCAZ400a-v<duration>	BNCCAZ400a-v<duration>
Premium Support (monthly; for up to 5 years)	BNCiCAZ400a-p<duration>	BNCCAZ400a-p<duration>

FIREWALL CONTROL CENTER VCC610	EMEA / INTERNATIONAL	NORTH AMERICA
Barracuda Firewall Control Center VCC610 - Enterprise Edition	BNCiCAZ610a	BNCCAZ610a
Virtual subscription (incl. Energize Updates; monthly; for up to 5 years)	BNCiCAZ610a-v<duration>	BNCCAZ400a-v<duration>
Premium Support (monthly; for up to 5 years)	BNCiCAZ610a-p<duration>	BNCCAZ610a-p<duration>

Amazon Web Services (AWS)

FIREWALL CONTROL CENTER VCC400	EMEA / INTERNATIONAL	NORTH AMERICA
Barracuda Firewall Control Center VCC400 - Standard Edition	BNCiCAW400a	BNCCAW400a
Virtual subscription (incl. Energize Updates; monthly; for up to 5 years)	BNCiCAW400a-v<duration>	BNCCAZ400a-v<duration>
Premium Support (monthly; for up to 5 years)	BNCiCAW400a-p<duration>	BNCCAW400a-p<duration>

FIREWALL CONTROL CENTER VCC610	EMEA / INTERNATIONAL	NORTH AMERICA
Barracuda Firewall Control Center VCC610 - Enterprise Edition	BNCiCAW610a	BNCCAW610a
Virtual subscription (incl. Energize Updates; monthly; for up to 5 years)	BNCiCAW610a-v<duration>	BNCCAZ400a-v<duration>
Premium Support (monthly; for up to 5 years)	BNCiCAW610a-p<duration>	BNCCAW610a-p<duration>

Google Cloud Platform (GCP)

FIREWALL CONTROL CENTER VCC400	EMEA / INTERNATIONAL	NORTH AMERICA
Barracuda Firewall Control Center VCC400 - Standard Edition	BNCiCLD400a	BNCCLD400a
Virtual subscription (incl. Energize Updates; monthly; for up to 5 years)	BNCiCLD400a-v<duration>	BNCCAZ400a-v<duration>
Premium Support (monthly; for up to 5 years)	BNCiCLD400a-p<duration>	BNCCLD400a-p<duration>

FIREWALL CONTROL CENTER VCC610	EMEA / INTERNATIONAL	NORTH AMERICA
Barracuda Firewall Control Center VCC610 - Enterprise Edition	BNCiCLD610a	BNCCLD610a
Virtual subscription (incl. Energize Updates; monthly; for up to 5 years)	BNCiCLD610a-v<duration>	BNCCAZ400a-v<duration>
Premium Support (monthly; for up to 5 years)	BNCiCLD610a-p<duration>	BNCCLD610a-p<duration>

www.pmddatasolutions.com

CE Declaration of Conformity

Barracuda Networks

We,
Manufacturer's Name: Barracuda Networks
Manufacturer's Address: 5225 Hellyer Ave. Suite 150
San Jose, CA 95138
USA

Hereby, declare under our sole responsibility that the requirements set out in the Directives 2014/35/EU, 2014/30/EU, 2014/53/2014, 2011/65/EU, 2012/19/EU has been fully fulfilled on our product indication below:

Barracuda CloudGen Firewall

The object of the declaration described above is in conformity with the relevant Union harmonization legislation:

Electrical Safety (LVD) 2014/35/EU
Electromagnetic compatibility directive (EMC) 2014/30/EU
Radio Equipment Directive (RED) 2014/53/EU
Restriction of Hazardous Substances Directive (RoHS) 2011/65/EU
Waste Electrical and Electronic Equipment Directive (WEEE) 2012/19/EU

The following standards and technical specifications have been applied:

EN 55032:2015 + AC:2016 Class A
EN 55024:2010+AS:2015 Class A
EN 61000-3-2:2014 Class A
EN 61000-3-3:2013
EN 300 328 V2.1.1
EN 301 893 V2.1.1
EN 301 489-1 V2.2.0
EN 301 489-17 V3.2.0
EN 62311:2008
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Signed for and on behalf of:

Signature, Date, Place : _____ February 1, 2019, USA
Name and Job Title : Ken Martin / SVP, World Wide Manufacturing Ops.

www.pmddatasolutions.com

Barracuda

February 21, 2020

To Whom It May Concern:

Barracuda Networks Inc. (”Barracuda”) hereby confirm that the Barracuda CloudGen Firewall complies with the UN Manual Test and Criteria, Part III, subsection 38.3, Revision 6, Amendment 1 (38.3). This is based on documents gathered from our supply chain which integrates the lithium cell battery into the system.

Thank you for your attention to this matter.

Best Regards,

Ken Martin
SVP Worldwide Manufacturing Operations
Barracuda Networks Inc.

www.pmddatasolutions.com

Appendix II - Useful links

- Barracuda Campus for online trainings and knowledge datenbase:

  https://campus.barracuda.com

- Detailed information on Energize Updates subscription:

  https://www.barracuda.com/support/updates

- Online application explorer including list of supported protocolls:

  https://campus.barracuda.com/product/cloudgenfirewall/browse/application-explorer

- Product information portal

  https://campus.barracuda.com/doc/71860836/

- End-of-Support (EoS) / End-of-Life (EoL) for hardware

  https://campus.barracuda.com/doc/71860841/

- End-of-Support (EoS) for firmware

  https://campus.barracuda.com/doc/71860849/

- GDPR statement

  https://www.barracuda.com/company/legal/gdpr

www.pmddatasolutions.com

Appendix III - Features and capabilities

BARRACUDA CLOUDGEN FIREWALL **FIREWALL**	F93.R	F183R
Stateful packet forwarding (per rule)	✓	✓
Transparent proxy (TCP; per rule)	✓	✓
Inline graphical packet analyser	✓	✓
NAT (src, dst, nets), PAT	✓	✓
Policy-based NAT (per rule)	✓	✓
Protocol support (IPv4, IPv6 [8])	✓	✓
IP-less configuration via named networks (IPv4, IPv6)	✓	✓
Wildcard network objects	✓	✓
Gigabit performance	✓	✓
Object oriented rule set	✓	✓
Virtual rule sets	✓	✓
Virtual rule test environment	✓	✓
Realtime connection status	✓	✓
Historical access caches	✓	✓
Event triggered notification	✓	✓
Load balancing for protected servers	✓	✓
Multipath load balancing	✓	✓
Firewall-to-firewall compression (stream & packet compression)	✓	✓
Dynamic rules with timer triggered deactivation (per rule)	✓	✓
Bridging mode / routing mode (mixed)	✓	✓
Virtual IP (proxyARP) support	✓	✓
Transparent IP to user mapping	✓	✓
User authentication	x.509, Microsoft® NTLM, RADIUS, RSA SecurID, LDAP/ LDAPS, Microsoft® Active Directory®, TACACS+, local	
RPC protocol support (ONC-RPC, DCE-RPC)	✓	✓
VoIP support (H.323, SIP, SCCP (skinny))	✓	✓
Deep inspection of ICS / SCADA protocols	✓	✓
DHCP relaying with packet loop protection & configurable agent-ID policy	✓	✓
Standby mode	Active-Active (with external load balancer only) and Active-Passive	
Network notification on failover	✓	✓
Key-based authentication	✓	✓
Encrypted HA communication	✓	✓
Provider/link failover	✓	✓
Transparent failover without session loss	✓	✓

BARRACUDA CLOUDGEN FIREWALL **APPLICATION CONTROL**	F93.R	F183R
Deep packet inspection	✓	✓
Application behavior analysis	✓	✓
Thousands of applications and protocols supported (Skype, BitTorrent, etc.)	✓	✓
Social media application support (Facebook, Google+, etc.)	✓	✓
Media streaming application support (YouTube, Netflix, etc.)	✓	✓
Proxy and anonymizer detection (Hide Me, Cyberghost, etc.)	✓	✓
Application objects based on category, risk, properties, and popularity	✓	✓
Predefined categories such as business, conferencing, instant messaging, media streaming, etc.	✓	✓
Interception of SSL/TLS encrypted traffic	✓	✓
Inspection of SSL/TLS encrypted traffic	✓	✓
Filtering of SSL/TLS encrypted traffic	✓	✓
Creation of customized applications	✓	✓
Deep application context	✓	✓
Google SafeSearch enforcement	✓	✓
Google Accounts enforcement	✓	✓
Application Based Provider Selection	✓	✓
Bandwidth and QoS assignment	✓	✓
Application logging	✓	✓
Application blocking	✓	✓
Application monitor and drill-down function	✓	✓
Reporting	✓	✓

8 IPv6 firewall forwarding traffic, IPS, and application control - only in conjunction with administration via Barracuda Firewall Admin.

www.pmddatasolutions.com

BARRACUDA CLOUDGEN FIREWALL **INTRUSION PREVENTION SYSTEM**	F93.R	F183R
Inline intrusion prevention	✓	✓
Regular online pattern updates	✓	✓
Packet anomaly protection	✓	✓
Packet reassembly	✓	✓
TCP stream reassembly	✓	✓
TCP checksum check	✓	✓
TCP split handshake protection	✓	✓
TCP stream segmentation check	✓	✓
Generic patter filter	✓	✓
Active ARP handling	✓	✓
Malformed packet check	✓	✓
SMB & NetBIOS evasion protection	✓	✓
HTML decoding	✓	✓
HTML decompression	✓	✓
HTML obfuscation protection	✓	✓
URL OBFUSCATION PROTECTION		
Escape encoding support	✓	✓
Microsoft %u encoding support	✓	✓
Path character transformations and expansions supported	✓	✓
RPC FRAGMENTATION PROTECTION		
MS-RPC (DCE) defragmentation supported (RFC 1151)	✓	✓
SUN-RPC (ONC) defragmentation supported (RFC 1151)	✓	✓
FTP EVASION PROTECTION		
Detection of inserted spaces in FTP command lines	✓	✓
Detection of additional telnet control sequences in FTP commands	✓	✓
DENIAL OF SERVICE, SPOOFING & FLOODING PROTECTION		
IP spoofing protection	✓	✓
Port scan protection	✓	✓
Sniffing protection	✓	✓
SYN/DoS/DDoS attack protection	✓	✓
LAND attack protection	✓	✓
Teardrop / IP fragment attack protection	✓	✓
UDP flood protection	✓	✓
ICMP fragment protection	✓	✓
ICMP flood ping protection	✓	✓
Reverse routing path check	✓	✓
IPS exceptions (allow listing)	✓	✓
IPS EXCEPTIONS BASED ON		
Source / destination	✓	✓
Port & port range	✓	✓
Signature / CVE	✓	✓

BARRACUDA CLOUDGEN FIREWALL **MALWARE PROTECTION**	F93.R	F183R
Single-pass mode	✓	✓
Proxy mode	✓	✓
Configurable archive recursion depth	✓	✓
Quarantine functionality for proxy	✓	✓
Configurable unknown archive policy	✓	✓
Configurable maximum archive size	✓	✓
Archiver package support	✓	✓
Office file-types support	✓	✓
Proactive detection of new threats	✓	✓
Advanced heuristics detection techniques	✓	✓
Number of signatures	Hundreds of thousands	
Frequency of signature updates	Multiple updates per day	
Dynamic, on-demand analysis of malware programs (sandbox)	✓	✓

BARRACUDA CLOUDGEN FIREWALL **ADVANCED THREAT PROTECTION**	F93.R	F183R
Dynamic analysis of documents with embedded exploits (PDF, Office, etc.)	✓	✓
Detailed forensics for both, malware binaries, and web threats (exploits)	✓	✓
High resolution malware analysis (monitoring, execution from the inside)	✓	✓
TypoSquatting and link protection for emails	✓	✓
Support for multiple operating systems (Windows, Android, etc.)	✓	✓
Flexible malware analysis in the cloud	✓	✓
SUPPORTED FILE TYPES		
Microsoft executables (exe, msi, dll, class, wsf)	✓	✓
Adobe PDF documents	✓	✓
Android APK files	✓	✓
ZIP archives	✓	✓
RAR archives	✓	✓
macOS executables (dmg)	✓	✓
Microsoft Office (doc, docx, xls, xslx, ...)	✓	✓
Microsoft Office macro enabled (doc, docx, xls, xslx, ...)	✓	✓
OpenOffice (odt, ods, rtf, ...)	✓	✓
Javascript (manual scan)	✓	✓
Other archives (7z, lzh, bz, bz2, chm, cab, tar, gzip, gz)	✓	✓
SUPPORTED PROTOCOLS		
HTTP	✓	✓
HTTPS	✓	✓
FTP	✓	✓
FTPS	✓	✓
SMTP	✓	✓
SMTPS	✓	✓

www.pmddatasolutions.com

BARRACUDA CLOUDGEN FIREWALL **WEB FILTER**	F93.R	F183R
Block / allow lists (per rule)	✓	✓
Filter categories	95	
Number of URLs categorized	>100 million	
Alexa top 1 million coverage	> 90%	
Temporal constraints	✓	✓
User specific / group specific restrictions	✓	✓
Cached online category database	✓	✓
Local update interval	N/A	
Online update interval	continuously	

BARRACUDA CLOUDGEN FIREWALL **TRAFFIC INTELLIGENCE & SD-WAN**	F93.R	F183R
VPN-based SD-WAN (incl. Traffic shaping insude VPN tunnels)	✓	✓
Optimized direct internet uplink selection	✓	✓
Distribution of site-to-site VPN across up to 24 uplinks	✓	✓
Quality of service (QoS)	✓	✓
Automatic backup uplink activation	✓	✓
Automatic activation of alternate QoS policy upon main WAN failure and backup uplink activation	✓	✓
Dynamic bandwidth and latency detection between VPN peers	✓	✓
Performance-based transport selection	✓	✓
Adaptive bandwidth protection	✓	✓
Adaptive session balancing	✓	✓
Traffic replication	✓	✓
Firewall / VPN compression	✓	✓
Zero-touch deployment	✓	-
Data deduplication	✓	✓
Link aggregation	✓	✓
Maximum overall bandwidth per interface	✓	✓
On-the-fly reprioritization via firewall status GUI	✓	✓
Ingress shaping per interface	✓	✓
Application-specific bandwidth assignment	✓	✓
Application-based provider selection	✓	✓
URL-filter-category specific provider selection	✓	✓

BARRACUDA CLOUDGEN FIREWALL **ROUTING & NETWORKING**	F93.R	F183R
HA capable with transparent session failover	✓	✓
GbE ethernet support	✓	✓
Max number of physical interfaces	24	n/a
Integrated switch	-	n/a
Integrated DSL modem	-	n/a
802.1q VLAN support	✓	✓
xDSL support (PPPoE, PPTP (multi-link))	✓	✓
DHCP client support	✓	✓
ISDN support (EuroISDN (syncppp, rawip))	-	-
Link monitoring (DHCP, xDSL, ISDN)	✓	✓
Policy routing support	✓	✓
Ethernet channel bonding	✓	✓
Multiple networks on interface, IP aliases	✓	✓
Multiple provider / WAN link support	✓	✓
Configurable MTU size (per route)	✓	✓
Jumbo frames (up to 9,000 bytes)	✓	✓
IPinIP and GRE tunnels	✓	✓
PPTP	✓	✓
BGP	✓	✓
Virtual routing and forwarding (VRF) instances	20	✓[9]
Dynamic VPN routing	✓	✓
Dynamic routing (BGP, OSPF, RIP)	✓	✓

BARRACUDA CLOUDGEN FIREWALL **VPN**	F93.R	F183R
Encryption support	AES-128/256, 3DES/ DES, CAST, Blowfish, Null	
Private CA (up to 4,096 bit RSA)	✓	✓
External PKI support	✓	✓
x.509v3 policy extensions (fully recognized)	✓	✓
Certificate revocation (OCSP, CRL)	✓	✓
Site-to-site VPN with traffic intelligence	✓	✓
Dynamic mesh VPN	✓	✓
WAN traffic compression via data deduplication	✓	✓
Star (hub and spoke) VPN network topology	✓	✓
Client VPN	✓	✓
Microsoft® domain logon (Pre-logon)	✓	✓
Strong user authentication	✓	✓
Replay protection	✓	✓
NAT traversal	✓	✓
HTTPS and SOCKS proxy compatible	✓	✓
Redundant VPN gateways	✓	✓
Native IPsec for third-party connectivity	✓	✓
PPTP/L2TP (IPsec; client VPN only)	✓	✓
Dynamic routing (OSPF, BGP) over VPN	✓	✓

9 For detailed information regarding VRF instances on virtual deployments, please check Barracuda Campus.

www.pmddatasolutions.com

BARRACUDA CLOUDGEN FIREWALL **SYSTEM MANAGEMENT**	F93.R	F183R
Central management	✓	✓
Local management	✓	✓
Comprehensive GUI-based configuration management	✓	✓
WebUI-based configuration management	-	-
Command-line interface (CLI) available	✓	✓
SSH-based access	✓	✓
Multiple administrators	✓	✓
Role-based administrators	✓	✓
Real-time accounting and visualization	✓	✓
Easy roll-out and recovery	✓	✓
USB installation and recovery	✓	✓
Zero-touch deployment	✓	-
Full life-cycle management	✓	✓
In-band management	✓	✓
Dedicated management interface	✓	✓
Serial interfaces	✓	✓
Central management interface	✓	✓
All management via VPN tunnel	✓	✓

BARRACUDA CLOUDGEN FIREWALL **LOGGING/MONITORING/ACCOUNTING**	F93.R	F183R
System health, activity monitoring	✓	✓
Human readable log files	✓	✓
Statistics	✓	✓
Active event notification	Email / Execute program / SNMP trap / Apple push notification service / Slack notification	
Real-time accounting and reporting	✓	✓
Syslog streaming (fully GUI configurable)	✓	✓

BARRACUDA CLOUDGEN FIREWALL **ADDITIONAL FUNCTIONS**	F93.R	F183R
SNMP queries	✓	✓
SMS control	✓	✓
NTP4 time server and clients	✓	✓

BARRACUDA CLOUDGEN FIREWALL **DNS**	F93.R	F183R
Multi-domain support	✓	✓
DNS operation types	Master, slave, forwarder, cacher	
Split DNS	✓	✓
Health probing	✓	✓
DNS doctoring	✓	✓

BARRACUDA CLOUDGEN FIREWALL **AUTHORITATIVE DNS SERVER**	F93.R	F183R
Local DNS cache	✓	✓
Inbound link balancing	✓	✓
Multi-domain support	✓	✓
Zone transfer (allows / prevent)	✓	✓
Time-to-live (TTL) enforcement	✓	✓
A server record support (A)	✓	✓
Name server record support (NS)	✓	✓
Mail server record support (MX)	✓	✓
TXT / SPF record support (TXT)	✓	✓
Canonical name support (CNAME)	✓	✓
Services available record support (SRV)	✓	✓
Pointer resource record support (PTR)	✓	✓
Customizable DNS record support (OTHER)	✓	✓
Health checks per IP	✓	✓
Configurable health check interval	✓	✓
Configurable update interval for dynamic IPs	✓	✓
Support for static uplinks	✓	✓
Support for dynamic uplinks	✓	✓

www.pmddatasolutions.com

BARRACUDA CLOUDGEN FIREWALL **DHCP**	F93.R	F183R
DHCP server	✓	✓
DHCP relay	✓	✓
Lease DB visualization & management	✓	✓
Multi-homing, multi-netting	✓	✓
Class-based filtering	✓	✓
Dynamic DNS support	✓	✓

BARRACUDA CLOUDGEN FIREWALL **MAIL SECURITY**	F93.R	F183R
Supported protocols	SMTP, SMTP with StartTLS, SMTPS, POP3, POP3S	
SSL Interception	✓	✓
DNS block list	✓	✓
Antivirus for email	optional	
Advanced Threat Protection for email	optional	

BARRACUDA CLOUDGEN FIREWALL **WEB PROXY**	F93.R	F183R
Supports cache hierarchies (parenting, neighboring)	✓	✓
Cache hierarchies supporting protocols	ICP, HTCP, CARP, Cache Digest, WCCP	
Proxying and caching (HTTP, FTP, and others)	✓	✓
Proxying for SSL (no inspection)	✓	✓
Transparent caching	✓	✓
HTTP server acceleration	✓	✓
Caching of DNS lookups	✓	✓
Central user authentication	Native NTLM, RADIUS, RSA ACE, LDAP, MS Active Directory, TACACS+	
Support for external virus scanning (ICAP)	✓	✓

BARRACUDA CLOUDGEN FIREWALL **REST API EXTENSIONS**	F93.R	F183R
Please note that the following is a non-exhaustive list. For more details, please refer to campus.barracuda.com.		
REST for all common access rule operations	Create / delete / list / change	
REST calls for network objects (stand-alone + CC)	✓	✓
REST calls for service objects (CC + stand-alone)	✓	✓
REST calls for enabling and activating IPS	✓	✓
REST calls to allow you to manage box administrators	✓	✓
REST calls to allow you to manage tokens	✓	✓
CLI tool to enable REST by default on cloud firewalls	✓	✓

www.pmddatasolutions.com

BARRACUDA CLOUDGEN FIREWALL **CLOUD-SPECIFICS**	**MICROSOFT AZURE**	**AMAZON WEB SERVICES**	**GOOGLE CLOUD PLATFORM**
In addition to supporting features as mentioned above in column "Virtual", the public cloud editions support unique capabilities.			
Cloud-SDK support	✓	✓	✓
Auto Scaling Cluster	-	✓	-
Cold Standby Cluster	-	✓	-
Log File Streaming and Custom Metrics for AWS CloudWatch	-	✓	-
Log File Streaming to Azure OMS	✓	-	-
Azure Virtual WAN support	✓	-	-

ADVANCED REMOTE ACCESS
VPN & NETWORK ACCESS CLIENTS

ARCHITECTURE	
Integrated VPN client	✓
Integrated health agent and managed personal firewall	✓ [13]
Full NAC policy support	✓ [13]
Customizable user interface	✓
Low power consumption network stack	✓
SUPPORTED OS VARIANTS	
Microsoft Windows Vista (32-bit, 64-bit)	✓
Microsoft Windows 7 (32-bit, 64-bit)	✓
Microsoft Windows 8 (32-bit, 64-bit)	✓
Microsoft Windows 10 (32-bit, 64-bit)	✓
Linux (kernel 2.4, kernel 2.6)	✓
macOS (10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11)	✓
MANAGEMENT	
Central management of VPN configuration	✓
VPN diagnostic log	✓
VPN system diagnostics report	✓
VPN status monitoring	✓
Attack access cache	✓
Packet log (capture)	✓
VPN groups	✓
Silent client setup	✓
Password protection of settings	✓ [10], [11]

AUTHENTICATION SUPPORT	
Microsoft® Certificate Management (Crypto API)	✓ [10]
Microsoft® Active Directory	✓ [10]
LDAP	✓ [12]
RADIUS	✓ [12]
MSNT	✓ [10], [12]
RSAACE	✓ [12]
External X509 certificates	✓
SMS PASSCODE	✓ [12]
RSA tokens	✓ [12]
Smart cards	✓ [13]
Microsoft domain logon support (prelogon)	✓ [13]
Two-factor authentication (RSA SecurID, Radius, TOTP)	✓ [13]
PERSONAL FIREWALL CAPABILITIES	
Dynamic adapter object & user object handling	✓
RPC handling	✓
Multiple rule sets support	✓
Client side policy enforcement	✓
Application control	✓
Adapter control	✓
User context enforcement	✓
NetBIOS protection	✓
DoS attack protection	✓
Executable scripts	✓

10 Only for Microsoft operating systems.
11 Also prevents changes to client settings by users with administrator rights.
12 Queried by Barracuda CloudGen Firewall VPN server on behalf of client.
13 For manufacturer with Microsoft Crypto Service Provider.

www.pmddatasolutions.com

ADVANCED REMOTE ACCESS **CUDALAUNCH & SSL VPN**	**CUDALAUNCH** **WINDOWS**	**MACOS**	**IOS**	**ANDROID**	**BROWSER-BASED SSL VPN**
Access to web apps (reverse proxied internal apps)	✓	✓	✓	✓	✓
Access to tunnel web apps (internal apps via SSL tunnel)	✓	✓	✓	✓	-
RDP (via SSL tunnel)	✓	✓	✓	✓	-
SSL tunnels for native client apps	✓	✓	✓	✓	-
IP VPN connections (connect device to network)	TINA VPN	-	IPsec	TINA VPN	-
Built-in demo setup	✓	✓	✓	✓	✓
Central administration via CloudGen Firewall and Firewall Admin	✓	✓	✓	✓	✓
Automatic self-configuration and management of VPN connections	✓	✓	✓	✓	-
Integration with CloudGen Firewall User Authentication	✓	✓	✓	✓	✓
Access policies utilizing multi-factor and multi-policy authentication	✓	✓	✓	✓	✓
Client certificate authentication	✓	✓	✓	✓	-
Single sign-on to internal apps	✓	✓	✓	✓	✓
Launchpad favorites (apps or VPN connections)	✓	✓	✓	✓	-
User attributes (ability for end users to edit)	✓	✓	✓	✓	✓
Dynamic firewall rule control (for system administrators)	✓	✓	✓	✓	✓
Custom help or info text for your organization	✓	✓	✓	✓	✓
Manually edit and create IP VPN connections	✓	✓	✓	✓	-
Debug log for easy support	✓	✓	✓	✓	-
Multi-factor authentication (up to 6 schemes)	✓	✓	✓	✓	✓
SUPPORTED MULTI-FACTOR AUTHENTICATION SCHEMES					
MS Active Directory	✓	✓	✓	✓	✓
LDAP	✓	✓	✓	✓	✓
Radius	✓	✓	✓	✓	✓
RSA SecurID	✓	✓	✓	✓	✓
TacPlus	✓	✓	✓	✓	✓
NGF Local	✓	✓	✓	✓	✓
MSNT	✓	✓	✓	✓	✓
Time-based OTP	✓	✓	✓	✓	✓

BARRACUDA FIREWALL CONTROL CENTER **CONFIGURATION MANAGEMENT**	**STANDARD EDITION (VC400 / VCC400)**	**ENTERPRISE EDITION (VC610 / VCC610)**	**GLOBAL EDITION (VC820)**
Tenants	1	1 [14]	5
Configuration groups [15]	1	Unlimited	Unlimited
Maximum managed gateways [recommended]	Unlimited [20]	Unlimited [200]	Unlimited [1000+ depends on HW]
Configuration templates (repositories)	✓	✓	✓
Shared configuration data	✓	✓	✓
Zero-touch deployment	✓	✓	✓
Operating system parameters	✓	✓	✓
Networking/routing parameters	✓	✓	✓
FW/VPN policies, application gateway parameters	✓	✓	✓
Flat file data storage	✓	✓	✓
Database characteristics (transaction orientation, locking, etc.)	✓	✓	✓
Backup and restore functionality	✓	✓	✓
Gateway configuration archive for speed install	✓	✓	✓
Configuration update monitoring	✓	✓	✓
Full RCS versioning	✓	✓	✓
VPN graphical tunnel interface	✓	✓	✓
Dynamic mesh site-to-site VPN support	✓	✓	✓
Barracuda Network Access Client policy management	✓	✓	✓
Multi-release management	-	✓	✓
Multi-platform management	✓	✓	✓

14 The public cloud edition VCC610 supports two tenants.
15 “Configuration Groups“ (“cluster“ in the firmware) refers to an administratively bundled group of CloudGen Firewall appliances and not to a load sharing cluster.

www.pmddatasolutions.com

BARRACUDA FIREWALL CONTROL CENTER **STATUS MONITORING**	**STANDARD EDITION (VC400 / VCC400)**	**ENTERPRISE EDITION (VC610 / VCC610)**	**GLOBAL EDITION (VC820)**
Gateway health state	✓	✓	✓
Launch pad functionality	✓	✓	✓
Customizable layout	✓	✓	✓

BARRACUDA FIREWALL CONTROL CENTER **TRUST CENTER**	**STANDARD EDITION (VC400 / VCC400)**	**ENTERPRISE EDITION (VC610 / VCC610)**	**GLOBAL EDITION (VC820)**
Gateway x.509 certificate CA	✓	✓	✓
Gateway SSH key management	✓	✓	✓
VPN server for management tunnels to gateways	✓	✓	✓
Virtual IP addresses for gateways (ProxyARP)	✓	✓	✓
Dynamic gateway IP address support	✓	✓	✓

BARRACUDA FIREWALL CONTROL CENTER **LICENSE CENTER**	**STANDARD EDITION (VC400 / VCC400)**	**ENTERPRISE EDITION (VC610 / VCC610)**	**GLOBAL EDITION (VC820)**
License timestamp server	✓	✓	✓
License status display	✓	✓	✓
Central event message list	✓	✓	✓
Event forwarding (SNMP, mail)	✓	✓	✓
Event log	✓	✓	✓

BARRACUDA FIREWALL CONTROL CENTER **CENTRAL SOFTWARE UPDATE**	**STANDARD EDITION (VC400 / VCC400)**	**ENTERPRISE EDITION (VC610 / VCC610)**	**GLOBAL EDITION (VC820)**
Real-time version display	✓	✓	✓
Kernel and OS updates	✓	✓	✓
Barracuda CloudGen Firewall updates & log viewer	✓	✓	✓

BARRACUDA FIREWALL CONTROL CENTER **SECURE REMOTE EXEC. ENVIRONMENT (SSHV2)**	**STANDARD EDITION (VC400 / VCC400)**	**ENTERPRISE EDITION (VC610 / VCC610)**	**GLOBAL EDITION (VC820)**
Job scheduling	✓	✓	✓
Script management	✓	✓	✓
Execution log viewer	✓	✓	✓

BARRACUDA FIREWALL CONTROL CENTER **ADMINISTRATIVE MODEL**	**STANDARD EDITION (VC400 / VCC400)**	**ENTERPRISE EDITION (VC610 / VCC610)**	**GLOBAL EDITION (VC820)**
Fully GUI-based access (Barracuda Firewall Admin management tool)	✓	✓	✓
Strong authentication & AES encryption	✓	✓	✓
Configurable role-based administration	✓	✓	✓
Adjustable view on configuration tree	✓	✓	✓
Configurable administrative domains	-	✓	✓
Multiple domains per administrator	-	✓	✓
Configurable access on OS level	✓	✓	✓
Configurable access notification	✓	✓	✓

www.pmddatasolutions.com

BARRACUDA FIREWALL CONTROL CENTER **REPORTING AND ACCOUNTING**	**STANDARD EDITION (VC400 / VCC400)**	**ENTERPRISE EDITION (VC610 / VCC610)**	**GLOBAL EDITION (VC820)**
Historical reports on gateway activity	✓	✓	✓
Customer-based gateway activity reports	✓	✓	✓
Policy distribution	✓	✓	✓
Firewall Control Center resource utilization	✓	✓	✓
Gateway-resource utilization	✓	✓	✓
Central log host	✓	✓	✓
Streaming/relaying to external log host	✓	✓	✓
Barracuda Report Server integration	✓	✓	✓

BARRACUDA FIREWALL CONTROL CENTER **ADDITIONAL FUNCTIONS**	**STANDARD EDITION (VC400 / VCC400)**	**ENTERPRISE EDITION (VC610 / VCC610)**	**GLOBAL EDITION (VC820)**
NTP4 time server for gateways	✓	✓	✓
Integrated DNS server	✓	✓	✓
High availability	Optional	Optional	HA license included
SIEM syslog interface	✓	✓	✓
Revision control system	✓	✓	✓
Access monitor	✓	✓	✓

BARRACUDA FIREWALL INSIGHTS	**F93.R**	**F183R**
AVAILABLE DASHBOARDS		
SD-WAN dashboard	✓	✓
SD-WAN tunnel status dashboard	✓	✓
Security and web traffic dashboard	✓	✓
Network traffic dashboard	✓	✓
GENERAL REPORT TYPES		
Customizable reports	✓	✓
On-demand reports	✓	✓
Scheduled reports	✓	✓
PRE-DEFINED REPORTS		
Predefined productivity reports	✓	✓
Predefined web activity reports	✓	✓
Predefined safety and liability reports	✓	✓
Predefined network activity reports	✓	✓
Predefined threat and security reports	✓	✓
Predefined infection activity reports	✓	✓
Predefined traffic reports	✓	✓
CLOUDGEN FIREWALL DASHBOARD		
Overview of allowed and blocked sessions along with an explanation	✓	✓
Threats overview by user, source, and destination	✓	✓
Web activity and productivity: Categories, users, and domains accessed by number of requests, bandwidth, and browse time	✓	✓
SUMMARY REPORTS		
Safety and liability	✓	✓
Network activity	✓	✓
Threat summary	✓	✓
Web traffic summary	✓	✓
Total usage	✓	✓
SCADA traffic per hour or day (S7, S7+, DNP3, Modbus, IEC60870-5-104 traffic)	✓	✓

	F93.R	**F183R**
SAFETY AND LIABILITY REPORTS (BASED ON USER AND REQUESTS)		
Traffic to adult-rated sites	✓	✓
Anonymizer sites	✓	✓
File-sharing and P2P	✓	✓
Intolerance and hate	✓	✓
Spyware	✓	✓
Violence and terrorism	✓	✓
Based on user and requests	✓	✓
SECURITY REPORTS BY SUBTYPE (BASED ON USER, TIME, SRC IP, AND DST IP)		
ATP	✓	✓
IPS	✓	✓
Virus	✓	✓
Malware	✓	✓
Spyware	✓	✓
Blocked file content	✓	✓
OT, IIOT, AND SCADA REPORTS		
Traffic summary	✓	✓
Traffic per protocol	✓	✓
SCADA traffic per hour or day (S7, S7+, DNP3, Modbus, IEC60870-5-104 traffic)	✓	✓

www.pmddatasolutions.com

Document version 1.3
Applies for firmware version 8.0.x

Barracuda Networks, Inc.
barracuda.com

© BARRACUDA NETWORKS, INC. SPECIFICATIONS SUBJECT TO CHANGE WITHOUT NOTICE. ALL OTHER BRANDS AND NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. ALL LOGOS, BRAND NAMES, CAMPAIGN STATEMENTS, AND PRODUCT IMAGES CONTAINED HEREIN ARE COPYRIGHT AND MAY NOT BE USED AND/OR REPRODUCED, IN WHOLE OR IN PART, WITHOUT EXPRESS WRITTEN PERMISSION BY BARRACUDA NETWORKS MARKETING.

www.pmddatasolutions.com