

# Barracuda WAF Control Center

Centralized Management for the Barracuda Web Application Firewall



The Barracuda WAF Control Center is **a centralized management system that allows administrators to manage multiple geo-dispersed Barracuda Web Application Firewalls with varying configurations from a single console.** A single Barracuda WAF Control Center can manage hardware, virtual, and cloud deployments and enables efficient, secure administration for system administrators.

- ✓ Security
- Storage
- ✓ Application Delivery

## The Barracuda Advantage

- Single pane of glass to manage all Barracuda Web Application Firewall form factors
  - Hardware, virtual appliances, or cloud instances
- Allows organizations to scale the coverage of web application security without added overheads
- Available as a virtual appliance or cloud instance
  - Hypervisor support for VMware, Hyper-V, and XenServer
  - Available for Amazon Web Services (AWS) and Microsoft Azure

## Product Spotlight

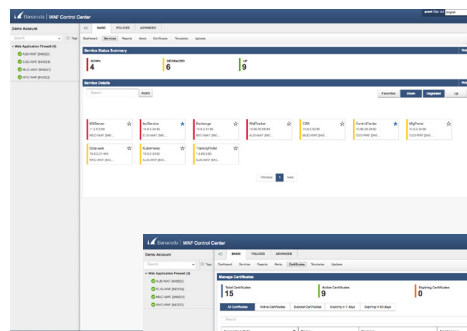
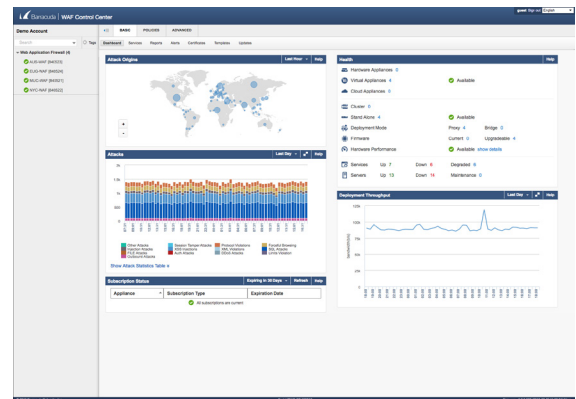
- Powerful, scalable centralized management
- Ability to enforce consistent configuration across hybrid deployments
- Role-based administration for multi-tenancy
- Centralized reporting provides the status of all configured services and certificates

## Single-Pane-of-Glass Dashboard

The Barracuda WAF Control Center has an intuitive tag-based management system that's easy to use and manage. You can also easily arrange group-connected Barracuda Web Application Firewalls by location, application, function, and more. MSSP-friendly multi-tenancy with role-based access controls enables secure administration.

## Simplify Web Application Firewall Management

The optimized services tab enables monitoring of all configured applications and services. The centralized notifications view collects and shows all alerts and notifications from connected devices. The SSL certificate manager enables management of certificates across all connected devices. Additionally, you can manage firmware and updates across devices from a central control center, as well as easily manage connected devices using a combination of tags.



Subscription Date	Name	Status	Application	Services	Address
12/15/2015	10.0.0.1	Online	10.0.0.1	10.0.0.1	10.0.0.1
12/15/2015	10.0.0.2	Online	10.0.0.2	10.0.0.2	10.0.0.2
12/15/2015	10.0.0.3	Online	10.0.0.3	10.0.0.3	10.0.0.3
12/15/2015	10.0.0.4	Online	10.0.0.4	10.0.0.4	10.0.0.4
12/15/2015	10.0.0.5	Online	10.0.0.5	10.0.0.5	10.0.0.5
12/15/2015	10.0.0.6	Online	10.0.0.6	10.0.0.6	10.0.0.6
12/15/2015	10.0.0.7	Online	10.0.0.7	10.0.0.7	10.0.0.7
12/15/2015	10.0.0.8	Online	10.0.0.8	10.0.0.8	10.0.0.8
12/15/2015	10.0.0.9	Online	10.0.0.9	10.0.0.9	10.0.0.9
12/15/2015	10.0.0.10	Online	10.0.0.10	10.0.0.10	10.0.0.10

## Technical Specs



### Centralized Monitoring

- Simplified services view with easy filtering
- Centralized status view of all connected devices
  - Health
  - Attacks
  - Deployment throughput
  - Subscriptions



### Multi-Platform Support

- Virtual
  - VMware
  - Hyper-V
  - XenServer
- Cloud
  - Amazon Web Services (AWS)
  - Microsoft Azure



### Administration

- Fully GUI-based configuration
- Multi-tenant capable
- MSSP friendly
- Role-based administration (RBAC)



### Configuration Management

- Shared security policies
- Configuration templates
- Centralized firmware and security update management



### Notification and Reporting

- Centralized notification and alerts view
- Batched email notifications with configurable thresholds
- Centralized reporting across connected devices
- Centralized SSL/TLS certificate reporting

FEATURE	VIRTUAL APPLIANCE
CPU Cores	4
Memory	4 GB
Max. Connected Web Application Firewall Device	40
Supported Hypervisors	VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer

FEATURE	AWS	AZURE
Minimum Instance Sizes	M3/M4 Large or above	D2 or above
Max. Connected Web Application Firewall Devices	40	40