What's New in the Barracuda Web Application Firewall

https://campus.barracuda.com/doc/30114094/

What’s new in version 10.0.1 Cloud

- **Multiple IP Address(es) Support for Amazon Web Services**: The Barracuda CloudGen WAF on AWS can now be used with multiple IP addresses, either manually or automatically. During service creation, the admin can choose to either manually enter a new IP address from the AWS console, or ask the Barracuda CloudGen WAF to automatically get one using the AWS APIs. **Note:** This feature does not work with autoscaling at this time. HA and clustering will work with manual IP assignment.
- **SR-IOV/ENA support**: In AWS, the Barracuda CloudGen WAF can now be deployed on instance types supporting **ENA/SR-IOV** .
- **Support for new Instance Types on AWS**: The Barracuda CloudGen WAF on AWS now supports an extensive list of t., m., and c. instances on AWS. The full list is available at: https://campus.barracuda.com/doc/28967064/
- **Openstack Autoscaling**: Barracuda Web Application Firewall Vx now supports autoscaling on OpenStack.
- **Backup Restore**: It is now possible to restore all backup files stored in the cloud for a particular Barracuda CloudGen WAF on AWS or Azure (as determined by serial number). To access and restore from a backup file stored in the cloud that was created from a different system, please contact Barracuda Networks Technical Support for assistance.
- **API Discovery with OpenAPI Spec Import**: It is now possible to discover OpenAPI applications and automatically configure the JSON firewall protection with the Barracuda CloudGen WAF.
- **Disaster Recovery for Multi-IP instances on Azure & AWS**: In earlier releases, if a backup that contained mutli-IP configurations on Azure was uploaded to a new instance, it would use the older IPs and require IP reconfiguration. With this new feature, this can be done automatically by the admin by clicking on “Multi IPs Refresh” on the **Services** page. This works only on non-clustered units at this time.

What’s new in version 10.0.1

- **Client Profile**: Enables the creation and validation of all client profiles (client fingerprints).
- **Advanced Client Analysis**: Once subscribed to the Advanced Bot Mitigation service, the Barracuda WAF can be configured to send HTTP requests and response metadata to the Barracuda Application Intelligence Network (AIN). This data is used to analyze client behavior, and detect and block advanced bots/attackers.
- **Client Risk scores**: Metadata from each request and response is sent to the cloud-based Barracuda Application Intelligence Network. This information is analyzed for each session, and the risk of the client is computed based on the traffic and client’s behavioral characteristics. The

score is used to identify the client as a good bot/bad bot, a good user, or an attacker.

- **Action Policies**: New action policies have been added.
- **UI Enhancements**
  - The **SECURITY POLICIES > Action Policy> Locked Out Clients** page is enhanced to display client fingerprints of the locked-out clients.
  - The **SECURITY POLICIES > Action Policy >Clear Locked Out Clients** page is enhanced to allow the administrator to unblock client fingerprint(s) that are blocked by the Barracuda Web Application Firewall.
- **Deprecated Feature**
  - The Secure Browsing tab has been moved from the **Websites** to the **Advanced** tab. The Secure Browsing tab is visible ONLY if **Enable Secure Browsing** is enabled. Secure Browsing feature will be removed from the product in a later release.

What's new in version 10.0

Advanced Bot Protection

Provides our customers with the ability to effectively defend against bots, crawlers, and automated attacks.

> Some features require an additional subscription. The extended trial is available. Please contact your sales team now.

Advanced Bot Protection is a suite of features that include:

- Client Tracking and Rating
  - Active and Passive Client Fingerprinting to identify clients down to a browser. This means that blocking can be done at browser level rather than IP address, making the block more effective.
  - Integration with third-party feeds to identify and block bots.
  - Computation of risk scores for each request based on detected violations.
- Credential Stuffing Detection and Brute Force Protection enhancements
  - Credential Stuffing detection: Detection of credential stuffing attacks using Advanced Bot Protection Cloud service. This uses a large database of previously leaked credentials to verify and block credential attacks.
  - Brute Force enhancements: Enforcement of Brute Force policies based on a client fingerprint.

- Protection Mechanisms
  - Comment Spam / Referrer Spam detection: Inspection of links sent in HTML Form parameters (as POST requests) or injected in HTTP Referer headers.

    - Google reCAPTCHA: Enhanced client validation using Google reCAPTCHAv2.
- New Reports and Dashboard enhancements
    - Bot traffic Analysis
    - Top Good or Bad Bots
    - Bots by Categories
    - Captcha Summary Report
    - Bot Spam
    - Credential Stuffing Trends

- Cloud layer for advanced analysis [Requires subscription – extended trial available]
    - Provides credential stuffing protection.
    - Client Fingerprint analysis.
    - Lookup services for Client Fingerprints and Credentials.
- SSL enhancements - Support for TLSv1.3 for both service side SSL and server-side SSL.
- Usability enhancements
    - Enhancements to the certificate page to support multiple thousands of certificates and their management.
    - Enhancements to the logging to show expired certificates.
    - Enhancement to the UI by introducing the “Bot Mitigation” tab for all the configurations related to Advanced Bot Protection.

- Throughput usage data collection - Support for tracking WAF throughput usage statistics when connected to WAF Control Center v2.3.

What’s new in version 9.2.1 Cloud

- **Config JSON checkpoints** : provide administrators a human-readable configuration file. These files are JSON formatted files which can be modified and downloaded from the Barracuda WAF. Furthermore, they can also be stored in a version-controlled repository, such as Git or CVS.
- **Generating a signed certificate using Let’s Encrypt**: Barracuda WAF now provides integration with Let’s Encrypt to generate, sign, install, and renew certificates for domain names bound with applications protected by the Barracuda Web Application Firewall.
- **Enabling Telemetry Data**:Users can now select the type of data that they intend to send to Barracuda Networks. By enabling telemetry, users define the type of data that the WAF should collect and share with the Barracuda Networks.
- **Barracuda WAF Deployment on OpenStack**: Barracuda WAF can now be deployed on OpenStack as a virtual machine to protect applications running on Openstack as well as externally.
- **UI Enhancements in System Configuration**: The fields in the **ADVANCED > System Configuration > Advanced** section are reorganized into groups for better user experience.

What’s new in version 9.2 Cloud

- **JSON File-Based Configuration Management (AWS and Azure)**: Teams utilizing infrastructure-as-code process can integrate Barracuda CloudGen WAF into their infrastructure definitions using JSON snippets. This simplifies the overall configuration management of Barracuda CloudGen WAF and makes it easy to organize and maintain as it can be used for versioning, reviewing, and auditing.
- **Slack Integration (All Models)**: Barracuda CloudGen WAF is now able to push WAF alerts and notifications to the configured slack channel.
- **WCC + WAF Integration (AWS)**: Using the Cloud Formation Template, administrators can direct the Barracuda CloudGen WAF to automatically join to Barracuda WAF Control Center (WCC) in autoscaling environments.
- **Consolidated ARM Templates (Azure)**: Multiple existing non VMSS marketplace templates have been merged into a single template.Two existing VMSS marketplace templates have also been merged to a single template.
- **CloudGen WAF Rebranding**: All the public cloud WAF VM's will be re-branded to CloudGen WAF.

What’s new in version 9.2

- **Integration with the Gemalto Safenet Luna Network HSM**: With Firmware 9.2, the Barracuda Web Application Firewall now integrates with the Gemalto SafeNet Luna Network HSM’s for added security in SSL/TLS transactions. The Gemalto SafeNet Luna HSM is a hardened physical device that stores all SSL/TLS certificates in tamper-proof hardware for additional security. All hardware and virtual WAF models 660 and above will support this integration.
- **Integration with the Barracuda Reporting Server**: The Barracuda Reporting Server is a purpose-built hardware appliance that rapidly generates reports while maintaining or improving accuracy of the reporting data. With this release, the Barracuda WAF and CloudGen WAF product lines integrate with the Barracuda Reporting Server to provide centralized log storage and reporting.
- **Role-Based Access Control for REST APIv3**: In Firmware 9.1, the revamped REST APIv3 for management and control of the Barracuda WAF and CloudGen WAF product lines was launched. In this release, a granular and comprehensive Role-based access control capabilities for the REST APIv3 have been added. With these features, you can now fully control administrative access to various API calls, and integrate this with access control systems.
- **Two-Factor Authentication for Administrator Access and Role-Based Access Control Enhancements**: It is now possible to configure Two-Factor Authentication for admin UI access. This includes integrations with RADIUS/LDAP based systems, RSA SecurID, and SMS passcodes. Role-Based access control settings are more granular with all operations on the web interface having READ/WRITE permission toggles, with a WRITE being the default permission.
- **Networking Enhancements**: In earlier firmware releases, it was not possible to include the WAN interface (eth0) as part of a link bond. This restriction is now removed, and eth0 can be

part of the bond.
- **Enhancements for Virtual Instances**: Virtual Barracuda WAF units now support multi-ports (86x and 96x) and 10GigabitEthernet interfaces (96x) where the hypervisor supports these capabilities.
- **Enhancements for GDPR Compliance**: To ensure compliance with the European Union's General Data Protection Regulations (GDPR), two new capabilities - Log Encryption, Problem Report Encryption have been introduced. Enabling these features requires turning them on the GDPR Compliance toggle in System preferences. When this capability is turned on, a passphrase should be configured. This passphrase is then used to encrypt all logs and problem reports that are generated from the unit.
- **New Application Templates for Drupal and Joomla**: New application templates for crating and configuring security policies for Drupal and Joomla are now available. These templates can be used to easily create a new service using the configuration wizard. They contain security rules specific to each web application.

What's New in Version 9.1 Video

Watch this video for an overview of new features in version 9.1. These features are also described in the sections below.

What's New in Version 9.1 Cloud

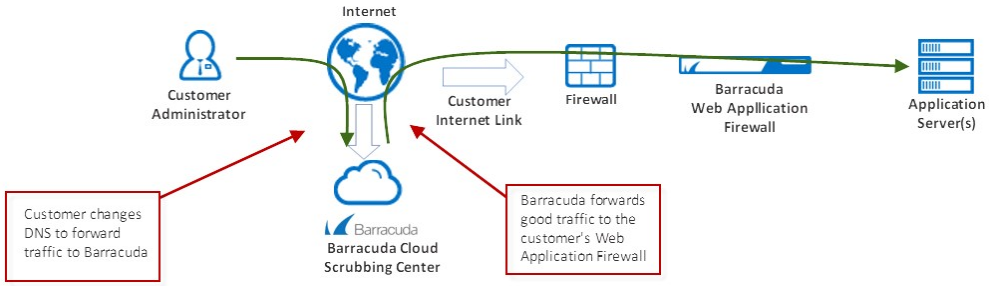
- **Support for Virtual Machine Scale Sets and Bootstrapping on Microsoft Azure**: The Barracuda Web Application Firewall on Azure can now be deployed in an Azure Virtual Machine Scale Set for dynamic scaling. With the VMSS integration, the Barracuda Web Application Firewall can be configured to bootstrap based on a service configuration defined in the ARM Template at launch. Alternatively, an existing configuration backup can be placed in an Azure Blob, and the Barracuda Web Application Firewall VMSS instances can bootstrap from this configuration. This capability is now available only for hourly models at this time. The ARM template for deploying the Barracuda Web Application Firewall in available on the Azure Marketplace at this time.
- **Support for configuration backup to Azure Blob Storage**: It is now possible to export configuration backups to Azure Blob Storage. This is possible with both manual backups and scheduled backups.

What's New in Version 9.1

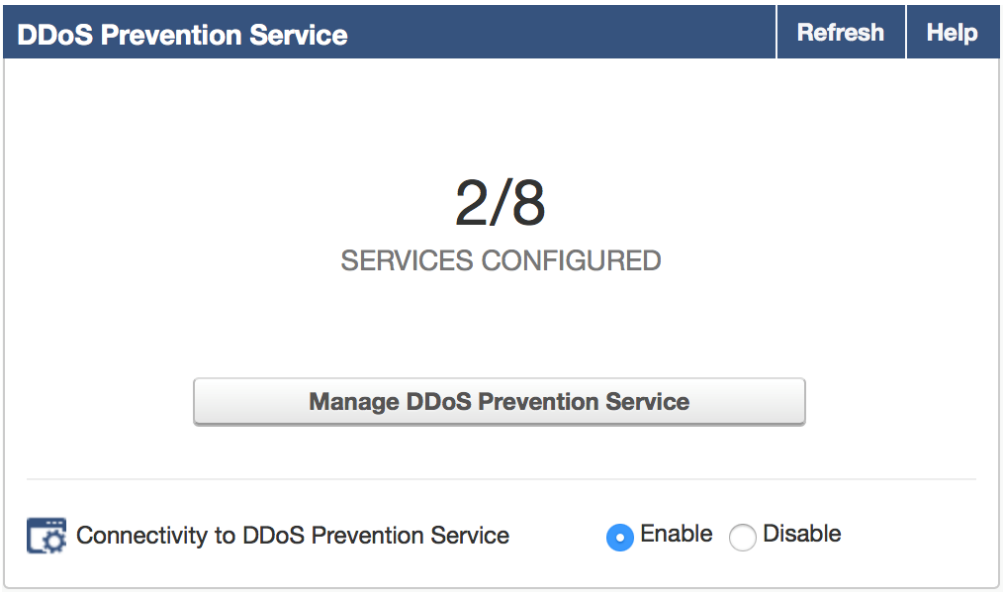
- **REST APIv3**: With the release of Firmware 9.1, we have released a new version (v3) of the Barracuda Web Application Firewall's REST API. The new REST API v3 is fully compliant with the

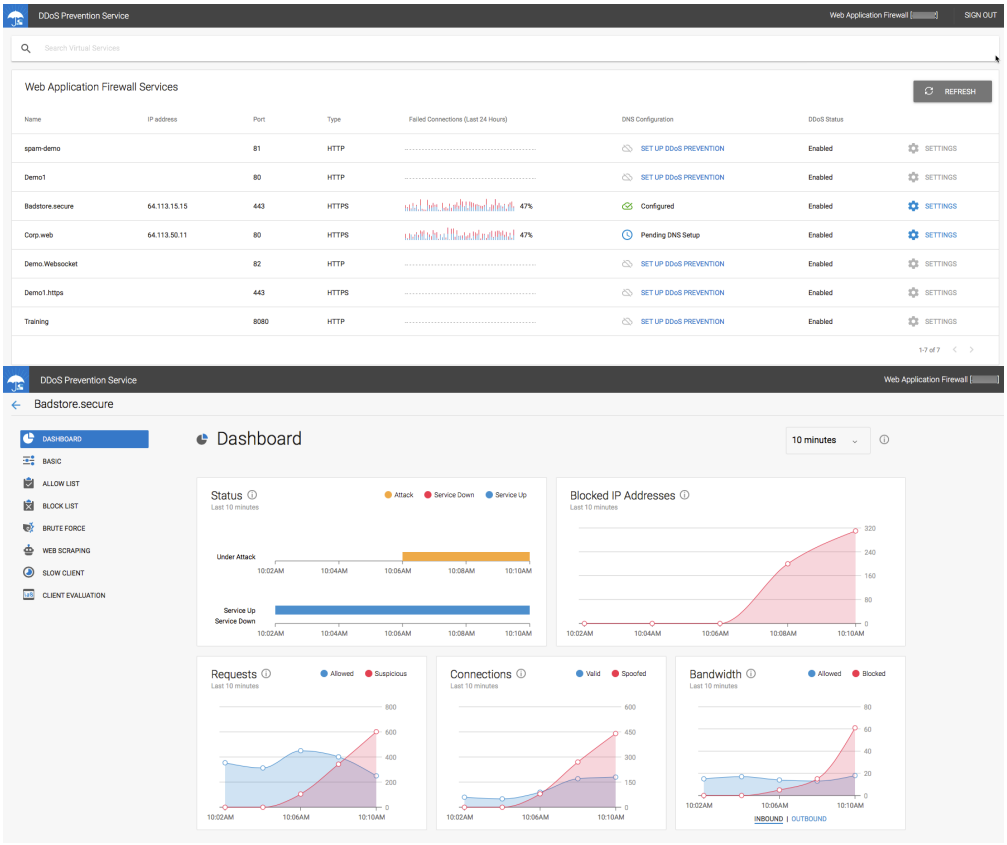
OpenAPI standard, and API documentation has been built using the Swagger Framework. The Swagger-based documentation is now live on Barracuda Campus. With Swagger, you do not need to manually copy paste various parts to create your configuration scripts; instead, Swagger allows you to specify variables, such as IP addresses, and other settings, and generates the code sample directly. You can then use the sample with minimal changes to build your scripts.

- **Integrations with Puppet, Terraform and Ansible**: The Barracuda Web Application Firewall now integrates with Puppet, Terraform and Ansible for automated deployments. The sample code for these integration is now available on our public GitHub Repository at: https://github.com/barracudanetworks/waf-automation
- **Integration with Barracuda Active DDoS Prevention**: With version 9.1, the Barracuda Web Application Firewall integrates closely with the Barracuda Active DDoS Prevention Service. The Barracuda Active DDoS Prevention is a service that protects you against volumetric DDoS attacks. Combined with the Application DDoS protection features of the Barracuda Web Application Firewall, Barracuda Active DDoS Protection gives you comprehensive protection from all types of DDoS attacks.



The Barracuda Active DDoS Prevention Service can be configured and managed directly from your Barracuda Web Application Firewall. It requires a separate subscription.





- **New models for Barracuda Web Application Firewall Vx**: New Vx models have been launched for the Barracuda Web Application Firewall. With this, customers will no longer have to purchase separate core licenses for Vx installations that support more than 200Mbps of traffic. The newly introduced models are: 760Vx (500Mbps), 860Vx (1Gbps) and 960Vx (5Gbps). The specifications for all the Vx models are now updated and are available on the main website and in the Barracuda Campus documentation.
- **Proxy Protocol support for HTTPS Services**: Proxy protocol is now supported for all HTTPS Services. Earlier, the Proxy Protocol was supported only when WebSockets were enabled. This limitation is no longer in effect and hence the Proxy Protocol can be enabled independently.

For detailed information on fixes and enhancements in the Firmware Version 9.0, see Release Notes Version 9.1.

What's New in Version 9.0.1 Cloud

- **Multi NIC and Multi IP per NIC Support for Azure**: The Barracuda Web Application Firewall instances on Microsoft Azure can now support multiple NIC's (WAN and LAN) for better separation of traffic. In addition, the WAN interface can now support multiple IP addresses. The Multi IP support now enables customers to host multiple applications with their own IP addresses on Azure instances. To make configuration tasks much easier for administrators, we have added the ability to generate new IP addresses directly from the **BASIC > Services** page of the Barracuda Web Application Firewall. When an administrator needs a new IP address, they

can simply click a button, and the Barracuda Web Application Firewall will generate it using the Azure APIs. All clustered units will automatically generate their own IP addresses, and synchronize this information with other units.

- **Granular Role-Based Administration with LDAP Groups**: It is now possible to assign specific LDAP groups for a given Admin Role. It is also possible to assign priorities for each Admin role for more fine grained control over permissions, in cases where a specific role is attached to multiple LDAP groups.
- **Microsoft Operations Management Suite (OMS) Integration**: The Barracuda Web Application Firewall now integrates with Microsoft's Operations Management Suite. With this integration, any Barracuda Web Application Firewall deployed anywhere – on-premises hardware, virtual or cloud, can be configured to send logs to the Microsoft OMS system. Simply configure the relevant Microsoft OMS Workspace as an export log server, configure the correct log headers, and the logs will start showing up on the relevant OMS Workspace. For additional ease-of-use, we have provided an OMS ARM template. This ARM template will automatically setup a Workspace with three dashboards:
  - Attack Statistics Dashboard
  - Application Performance Dashboard
  - Audit Logs Dashboard

  When the Barracuda Web Application Firewall instances send logs to this Workspace, the graphs on these dashboards are automatically populated and provide a complete view of the deployment.
- **Configuration Backup to Amazon S3**: It is now possible to backup Barracuda Web Application Firewall configuration to an S3 bucket. This backup includes the ability to perform scheduled backups to a pre-configured S3 bucket.
- **Disable "admin" account on AWS instances**: When launching Barracuda Web Application Firewall instances using AWS CloudFormation Templates, it is now possible to irreversibly disable the default "admin" account. This capability is available when launch the Barracuda Web Application Firewall stack with backup based boostrapping, where the backup has an alternative external RBA source (such as LDAP/AD) configured.
- **Support for configuring NTP Servers and Time Zone from CloudFormation Templates**: It is now possible to configure NTP Servers and Time Zone for Barracuda Web Application Firewall instances that are launched using CloudFormation Template. Multiple NTP servers can be configured from the template, and the Time Zone and NTP settings are now synchronized across clustered units.

For detailed information on fixes and enhancements in the Firmware Version 9.0, see Release Notes Version 9.0.1 Cloud.

What's New in Version 9.0.1

- **User Interface Enhancements**: The **BASIC > Services** page has now been enhanced for better usability and performance. The **Services** page can now be viewed in full-width, using the entire screen space to display information. In addition, multiple changes have been

implemented to speed up page load times and configuration updates.

For detailed information on fixes and enhancements in the Firmware Version 9.0, see Release Notes Version 9.0.1.

What's New in Version 9.0

- **Integration with Barracuda Advanced Threat Protection:** Barracuda Networks' Advanced Threat Protection (ATP) implements full-system emulation which provides the deepest visibility into malware behavior while simultaneously being the toughest one to evade. With this release, the Barracuda Web Application Firewall now integrates with the Barracuda ATP system to ensure that all file uploads do not contain any hidden malware. BATP integration is available as a separate license with the Barracuda Web Application Firewall.
- **Integration with the Barracuda NextGen Firewall F-Series:** Web Application Firewall's are deployed to block web application attacks that evade the perimeter firewall. In such situations, the Barracuda Web Application Firewall can be configured to block attackers from accessing the site. Till now, these attackers were allowed into the network and blocked only at the Barracuda Web Application Firewall level. With the release of 9.0, the Barracuda Web Application Firewall can now push blocked client configuration out to the Barracuda NextGen Firewall F-Series, ensuring that attackers are blocked at the perimeter and not allowed into the network at all.
- **Integration with the Barracuda Vulnerability Remediation Service:** The Barracuda Vulnerability Remediation Service (BVRS) allows administrators to scan applications for vulnerabilities on-demand or on a schedule. Detected vulnerabilities can be mitigated by pushing configuration changes to the Barracuda Web Application Firewall's security policy. This can happen either automatically based on a schedule, or manually in a single click. Administrators can also audit each vulnerability's history and view logs of blocked requests for each vulnerability separately.
- **Integration with the HPE ArcSight SIEM:** With release 9.0, the Barracuda Web Application Firewall now integrates with the HPE ArcSight SIEM. Syslogs can now be sent to ArcSight in the CEF format to be integrated with existing reporting systems.
- **New Hardware:** The 86x and 96x series hardware now come with more ports and link bonding capabilities. The 86x series is available with 8 GigabitEthernet ports. The 96x series is available with 8 GigabitEthernet ports and 2 TenGigabitEthernet ports. Interface choices include Copper or Fiber, with bypass options, and all models are capable of supporting link bonding, including 802.3ad/LACP.

For detailed information on fixes and enhancements in the Firmware Version 9.0, see Release Notes Version 9.0.

What's New in Version 8.1.1

- **Enhanced Bootstrapping Support for AWS CloudFormation deployments:** With this release, you can now bootstrap Barracuda Web Application Firewall instances on AWS using previously exported configuration templates or backups. This allows for easy transfer of configuration between staging and production environments. The configuration template or backup file is placed in an S3 bucket, and passed to the CloudFormation Template at launch. The Barracuda Web Application Firewall instances that are brought up will then use these files to automatically configure themselves at boot. The latest Hourly AMI and CloudFormation Templates with these features will be available on the AWS Marketplace page shortly.
- **Geo IP and IP Reputation Policy enforcement at Layer 7:** In cloud deployments, the Barracuda Web Application Firewall is typically positioned behind a Load Balancer, such as the AWS Elastic Load Balancer. Incoming traffic from the Load Balancer has the Load Balancer's IP address as the client IP address. In such cases, GeoIP and other IP reputation based policies will not work. With this enhancement, the Barracuda Web Application Firewall now looks for the IP address contained in the HTTP X-Forwarded-For header, which is the original client IP, and uses this information to enforce Geo IP and IP Reputation policies. To enable easier policy fixes with this feature, it is now possible to apply a Policy Fix directly from the Web Firewall Logs for requests detected by this feature.
- **Changes to default Cipher Lists for HTTPS services:** Weak ciphers such as (SEED-SHA, IDEA-CBC-SHA, ECDHE-RSA-RC4-SHA, ECDHE-ECDSA-RC4-SHA and RC4-SHA) are no longer enabled by default. If your application requires that these ciphers are supported, then they need to be enabled explicitly by using a "Custom" cipher list for the service.
- **New Reports:** New reports have been added to the System Summary Reports to show CPU and Memory Utilization trends. In addition, a new Exception List report has been added un the Config Summary section. This report provides a detailed listing of all the IP Reputation Pools and the exempted IP addresses for associated Services and IP addresses.

For detailed information on fixes and enhancements in the Firmware Version 8.1.1, see Release Notes Version 8.1.1 .

What's New in Version 8.1

- **Enhanced Web Scraping Protection**: To tackle increasingly sophisticated web scrapers, this release adds support for enhanced web scraping that provides multiple protection mechanisms against scrapers. This includes embedding web-based honeypots to trap scrapers, headless browser detection, mouse and keyboard detection and detection of clients based on common automation tools like PhantomJS. At the same time search engine crawlers are whitelisted and validated using reverse DNS lookups on their IP addresses. This also helps identify fake googlebots, etc.
- **Granular Binding of Security Policies**: Security Policies can now bind at a URL or domain level. Earlier these policies had to be associated at a service or VIP level. This allows having separate policies for applications that are on the same server and IP. For example, http://barracuda.com/partner and http://barracuda.com/collaborate could be on the same VIP but can now have different policies associated with them, e.g. WordPress and

SharePoint policy respectively.

- **Support for AMQP formatting in Exported Logs**: AMQP (1.0 version) protocol support added to export logs to external aggregators that are compliant to AMQP message queuing, including Microsoft Azure's Event Hub. AMQP is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns and is being increasingly supported in SIEM solutions and message-oriented middleware.
- **URL Profile Optimization**: Many applications generate different URLs for similar content, like for different products in an ecommerce portal. From a security perspective the profile remains the same with similar URL parameters, FORMs, access methods, etc. Under Adaptive Profiling, this can generate a large number of URL and parameter profiles. URL optimizers can now be used to coalesce such URLs into a single profile for easier management and better system performance.
- **Support for Auto-Scaling in AWS**: The Barracuda Web Application Firewall cluster in AWS can now auto-scale without admin intervention. Earlier dynamic scaling support required an admin to spin up additional instances manually that then synchronized amongst each other. The auto-scale feature allows the cluster to scale out automatically within limits that can be specified. With this feature, the Barracuda Web Application Firewall can now be launched automatically using CloudFormation templates and integrates with various AWS services, including IAM, Cloudwatch, S3 and SNS. The Barracuda Web Application Firewall is now also certified as part of the AWS Security Competency Program.
- **SAN Certificate CSR**: This release adds the ability to create Certificate Signing Request (CSR)/self-signed for SAN certificates. SAN certificates are commonly used for Microsoft applications and are even recommended in some instances. SAN Certificates allows organizations to specify alternative domains for a service. For example a SAN certificate for www.example.com could have the alternative domains www.examples.net and www.ex.com listed as alternative names for the same service. This partially solves the multi-domain limitation with wildcard certificates though SAN Certificates are more expensive than single domain certificates and are often limited to 3-5 domains.
- **Support for JSON Key Profiles**: This is an enhancement to the JSON security module, where the administrator can define granular policies for JSON Keys, akin to URL and parameter profiles.
- **Load Balancing across Server Name Resolution**: When a server uses hostname as the identifier, rather than IP address, and if it resolves to multiple IPs, the system performs load balancing across these IP addresses. This is especially important in IaaS environments.
- **Integration with Barracuda Vulnerability Manager, HPE Fortify OnDemand and HPE Fortify WebInspect Vulnerability Scanners:**Barracuda Web Application Firewall can now import and virtually patch vulnerabilities discovered by running the Barracuda Vulnerability Manager, HPE Fortify OnDemand and HPE Fortify WebInspect Vulnerability scanners. This is in addition to the scanners already supported.
- **Integration with Denim ThreadFix:**The Denim ThreadFix tool provides the capability to translate the reports from multiple scanners into a format that can be imported by the Barracuda Web Application Firewall. This integration now allows the Barracuda Web Application Firewall to integrate with over 20 different vulnerability scanners for simplified virtual patching of vulnerabilities.
- **Support for HTTP/2 and Websockets (BETA)**:
    - The Barracuda Web Application Firewall provides Beta support for HTTP/2 Offloading. This

means that the Barracuda Web Application Firewall can provide an HTTP/2 connection front-end to clients while the back-end connection to the server is via HTTP/1.1.
    - The Barracuda Web Application Firewall can now also support WebSocket traffic. With WebSocket support, the Barracuda Web Application Firewall behaves as a pass through proxy and does not intercept or analyze the traffic.

For detailed information on fixes and enhancements in the Firmware Version 8.1, see Release Notes Version 8.1 .

What's New in Version 8.0.1

- **Support for SSL/TLS Version based Redirection**: Due to vulnerabilities, administrators are disabling older versions of SSL/TLS. With this release, you can configure the Barracuda Web Application Firewall to redirect clients to the relevant error page, making it easier to identify the cause of any error.
- **Support for Cipher Suite override based on SSL/TLS versions**: Because specific cipher suite and SSL/TLS version combinations have vulnerabilities, the Barracuda Web Application Firewall can now be configured to limit allowed cipher suites for a given SSL/TLS protocol version.

For detailed information on fixes and enhancements in the Firmware Version 8.0.1, see Release Notes Version 8.0.1.

What's New in Version 8.0

- **Support for JSON Payload Inspection**: RESTful applications are increasingly adopting JSON over XML as a data interchange format. With this release, the Barracuda Web Application Firewall can parse and inspect JSON content in requests. Protection includes input validation as well as JSON sanity checks to shield JSON parsers from DoS attacks.
- **Enhancements to Logs and Reporting**: Among other things, these include a new multi-line log entry layout, visual cues for response codes, severity and action taken, easier page navigation with page numbering, and additional information about the vulnerabilities in the details. Drill down capability that was added to the reporting module earlier has been enhanced to provide multi-drill downs allowing more choice to the user.
- **Increased Granularity for Client Certificates**: While client certificates have been supported at a Service (Virtual IP) level for a long time, this release adds support for client certificate policies at the more granular URL space level. Different URL spaces within a service can now have different client certification policies.
- **Improved Centralized Management**: This firmware co-releases with an on-prem version of Barracuda Control Server (BCS) 4.0 which provides a scalable, centralized console for unified management, control and visibility into multiple Barracuda Web Application Firewall units. This

is a separately licensed product. For more information, refer to Barracuda Control Server.

For detailed information on fixes and enhancements in the Firmware Version 8.0, see Release Notes Version 8.0.

What's New in Version 7.9.1

- **Support for SAML v2**: SAML Service Provider (SP) capabilities have been added. This allows offloading SAML-based federated authentication and authorization where identity is provided by a remote Identity Provider. This also provides interoperability with Microsoft Azure AD.
- **Dashboard Enhancement**: A Heat map of attacks based on Geo-Location of attack sources has been added to the dashboard on the Status page.
- **Logs UI Enhancement**: The user interface for the Access, Web Firewall and Audit logs now occupy the full browser width.
- **Azure Optimizations**: Optimizations have been introduced to enhance the performance of small instances in the Azure cloud.

For detailed information on fixes and enhancements in the Firmware Version 7.9.1, see Release Notes Version 7.9.1.

What's New in Version 7.9

The main themes for this release are reporting and notification enhancements, application security enhancements like URL encryption and PFS support, and a new infrastructure for templates.

- **New UI Skin**: The product gets a spiffy new UI across the board.
- **Reporting Enhancements**: The new reporting modules carry over 40 ready-to-use reports, including new reports by geography. For example, you can schedule a report providing a breakdown by country of the traffic hitting your services, or drill down to regions attacking you most. With a couple of clicks, you can filter security and traffic reports by time frame, services and Top Count. Together, these provide a very rich set of reports out-of-the-box that you can view instantly or schedule for periodic delivery.
- **New Notifications Page**: A new page, BASIC > Notifications, allows you to configure events to be notified, generated from hardware components, attacks, or various system modules. To avoid inundating the recipients, it allows you to set individual thresholds for each notification type. Only when an event trigger exceeds this threshold in a given time interval will the notification be sent out.
- **URL Encryption**: When you turn this on for one or more portals of your web application, the Barracuda Web Application Firewall encrypts every URL in the response body before sending it to clients. Neither the original URLs nor the directory structure are ever exposed externally. When a client clicks on a link, the Barracuda Web Application Firewall decrypts it, translates it to

the original, then forwards it to the protected server. Any tampering found during decryption results in the request being denied - thus providing a very strong mechanism for forceful browsing prevention. It can also work along with adaptive profiling.

- **SSL Enhancements**: Perfect Forward Secrecy (PFS) with ECDSA and RSA certificates and associated ciphers are now supported. The key exchange mechanism supported is Elliptic Curve DHE. These are increasingly relevant in a post-Snowden world, as communications intercepted today can never be decrypted even far into the future due to the ephemeral nature of the PFS scheme. You can also customize backed SSL, including SNI extensions in the TLS header if the server requires it.
- **New Templates Module**: A new, powerful wizard-based UI template mechanism has been added. You can create custom templates for any object or policy in the system. Templates capture the attributes of the object along with its "children" objects. For example, a template for a service would contain service attributes like VIP, Port, Mask, Vsite, etc. as well as nested templates for Servers, Rule Groups, Authentication Policies, SSL Security, etc. Create a service template from one unit and deploy it on another, and the whole hierarchy is auto-populated.
- **User Access Control Enhancements**: Authentication Services now allow multiple domains for a service. A user can authenticate across multiple domains using the login format "domain\username". User logins without domain specified are authenticated using the default domain configured for the service. Support for dual authentication using LDAP and RSA SecurID / Radius with OTP has also been added.
- **Admin Account Password Security Enhancements**: Barracuda Web Application Firewall administrator accounts can now be configured with password policies like minimum strength, expiry and maximum retries before account lockout.

For detailed information on fixes and enhancements in the Firmware Version 7.9, see Release Notes Version 7.9.

What's New in Version 7.8

Security

- **DDoS Enhancements**: Administrators can define policies for specific URL spaces to ensure suspicious clients are challenged with a CAPTCHA for verification. These challenges thwart DDOS attacks on process and memory intensive resources of the back-end applications from bots and crawlers. Configure challenges using the WEBSITES > DDoS Prevention page. Additionally, CAPTCHA challenges can also be invoked as a Follow Up Action to other attacks, such as SQL Injection, via the Security Policies > Action Policy feature. Use this to detect and thwart automated tool attempts to repeatedly scan the website for vulnerabilities and waste resources. For example, sqlmap tool scanning for SQLi can be blocked.
- **Barracuda Blocklist Integration**: Barracuda Blocklist is an extensive IP reputation system that lists IP addresses that are open proxies or are botnet infected. The system relies on honeypots to flag both web and spam botnets, which are used interchangeably, depending on the need. Under a DDoS attack, these addresses can be blocked with a single click to deflate

the attack, with minimal false positive risk. Configure this on the WEBSITES > DDoS Prevention page.
- **True File type checks for File Uploads**: In earlier releases, file extension checks could be evaded on a file upload by changing the extension to match one of the whitelisted extensions. As of this release, such evasions are detected by fingerprinting the file, thus establishing its true MIME type for comparison to the whitelist. For example, this prevents a hacker from changing a file extension from .exe to .doc to upload it, since it will be evaluated to application/octet-stream and blocked (assuming the latter has not been added to the Allowed Mime Types on the WEBSITES > Parameter Protection page).
- **Kerberos Authentication**: The AAA module has been enhanced to support Kerberos authentication to back-end services like OWA and SharePoint using Kerberos. The front-end authentication is form based while the back-end uses the Kerberos protocol.
- **Clickjacking Protection**: Clickjacking and UI redressing attacks can now be prevented by enabling Clickjacking protection from the WEBSITES > Advanced Security page.

Cryptography

- **SNI support**: SNI (Server Name Indication) extension to SSL is now supported. This is particularly useful in a virtual hosting scenario where organizations may have several domains hosted on a single server using the same IP address and each domain has a distinct SSL certificate.
- **CRL (Certification Revocation Lists) support**: Client certificate CRLs can be automatically retrieved over HTTP and can be updated periodically by the system.
- **Backup Enhancements**: System backups can now be done over FTPS.
- **Performance and Stability improvements:** Rearchitected SSL modules now ensure higher transactions per second and throughput support with less memory footprint and reduced risk of race conditions than earlier releases.

Networking

- **Synchronization for Network elements**: The following objects are now synchronized across the cluster: (1) VLANs (2) Static routes (3) Interface routes and (4) ACLs. Interfaces in Management network group will not be synced in cluster.
- **Backup Enhancements:** NTLM V2 is now supported while taking system backup.
- **Deployment**: System IP can now be on a VLAN interface.
- **Persistence Enhancements**: The Load balancing module can use HTTP header based persistence for directing traffic to back-end servers.

Usability improvements

- Clients locked out by the configured Follow Up Action of Block Client can now be unblocked manually by the administrator on the WEBSITES > Advanced Security page.
- Parameter profile viewing preferences have been added on the WEBSITES > Website Profiles page.
- In a clustered setup, the Join Cluster operation is now available when the Failback Mode is manual, no longer only when in automatic mode.

- NIC speed, duplexity and statistics can now be viewed and edited from ADVANCED > Advanced Networking, under the configuration for Network Group: System. This is only available when Show Advanced Settings is set to *Yes* under ADVANCED > System Configuration.
- Access Logs now have a host filter.
- Interface routes and Custom Virtual Interfaces can now be edited.
- The login page can now display a custom message to comply with FISMA, which requires federal systems to display an access notice on the login pages.
- A new tool indicates how an IP address is categorized in the Geo IP database.
- The data path can be manually restarted after an attack definitions update.

Logging and Reporting

- The logging module has been enhanced to integrate with IBM QRadar SIEM System.

For detailed information on fixes and enhancements in the Firmware Version 7.8, see Release Notes Version 7.8.

What's New in Version 7.7

Firmware version 7.7 of the Barracuda Web Application Firewall is a major firmware release enhancing security and networking capabilities including:

Security

- **Protection From Slow Client Attacks**: Tools designed by network and security experts to test the robustness of their networks are now being used by the hacker community to attack the applications. Some of these attacks are done using Slowloris, PyLoris, QSlowLoris, slowhttprequest type of tools. The Barracuda Web Application Firewall augments its security capability by adding a variable traffic window detection algorithm to thwart these attacks. See Slow Client Attack Prevention .
- **Access Blocked Based On Client IP Reputation**: Protecting your network against botnet requires a multi-pronged strategy. One step in that direction is to control access to the applications based on IP reputation. The reputation of an IP address is dependent on attributes such as geographic location of the IP address or its identity as an anonymous proxy. The Barracuda Web Application Firewall now provides an easy way to block out clients based on Geo Location, Anonymous Proxy identity or Satellite ISP identity. See IP Reputation Based Filters.
- **Armored Browser Integration**: The Barracuda Web Application Firewall now integrates with the Quarri Protect On Q armored browser to extend security coverage to the client side.
- **Enhanced Shared Security Policies**: CSRF can be enabled using the shared security policy. Enhanced max instances check for parameters which prevent a class of HTTP Parameter pollution attacks, for wild card parameter profiles.
- **Finger Print Evasion**: Administrators can now change the system generated tokens such as ncforminfo, BNES_ or BNIS_.

- **Networking**
  - **Advanced Routing Capabilities**: A virtual site is now a networking entity with its own routing tables and ACLs, allowing services on the Barracuda Web Application Firewall to be grouped by their routing requirements. See Networking .
  - **Network ACL**: Traffic to the server networks can be restricted using network layer ACLs. Network ACLs can now be configured for traffic that is being NATed or proxied via the Barracuda Web Application Firewall.

Deployment

  - **Active-Active HA**: Two Barracuda Web Application Firewalls in a clustered environment can be configured to have active services on them, and to failover/failback if one of the units fail. See High Availability .
  - **IPv6 Enhancements**: Enhanced stability and improvements in the IPv6 functionality.

Usability improvements

  - Integration with Cenzic for vulnerability patch management.
  - Bulk edit for Services page.
  - Persistence of node expansion state in the **BASIC > Services** page.

Logging and reporting enhancements

  - Service level SNMP stats: The enhanced SNMP MIB now supports multiple statistics at the application level.
  - System Logs, (e.g., server up and server down events) are now displayed on the web interface.
  - Syslog NG integration.
  - Integration with Splunk and Arcsight now available.
  - For detailed information on fixes and enhancements in the Firmware Version 7.7, see Release Notes Version 7.7.

Figures

1. DDoS.jpg
2. DPS.png
3. Services_On_DPS.png
4. Dashboard.png