8.0.0 Cloud Release Release Notes

https://campus.barracuda.com/doc/79462517/

Version 8.0.0 is a Cloud-only release. Support for hardware and virtual firewalls regarding new features and improvements will be covered in the next release. Upgrading from previous versions is not possible.

Before installing the new firmware version:

Do not manually reboot your system at any time while the update is in process, unless otherwise instructed by Barracuda Networks Technical Support. Upgrading can take up to 60 minutes. For assistance contact Barracuda Networks Technical Support.

First-Generation ATP to Second-Generation Barracuda ATP Cloud Migration

Changelog

To keep our customers informed, the **Known Issues** list and the release of hotfixes resolving these known issues are now updated regularly.

- 2018-12-21 – **Hotfix 892 - Cumulative released**. For more information, see Hotfix 892.
- 2019-08-05 – **Hotfix 1011 - Cumulative Update for Azure Networking**. This hotfix provides multiple updates related to networking, which improves the overall stability of networking in Azure. For more information, see Hotfix 1011.

Legacy Services Announcement

Services and features eventually reach their natural end of life for various reasons, including replacements by new and improved technologies and changes to the marketplace. Not continuing to maintain legacy features in our software allows us to concentrate on more important parts. The following services are no longer available in all releases 8.0.0 and higher.

- SSH Proxy
- FTP Gateway
- Mail Gateway
- SPAM Filter
- DNS (temporarily disabled in 8.0.0)
- Public Key Infrastructure Service
- NG Web Filter (IBM/ISS)

What´s New in Version 8.0.0

New Platform

Barracuda CloudGen Firewall version 8.0.0 incorporates a substantial update for optimal integration into the underlying platform and includes numerous updates to the latest kernel technology.

Automated Connectivity for Azure Virtual WAN

Barracuda CloudGen Firewalls support Microsoft's Azure Virtual WAN technology to allow fast, secure, and uninterrupted network availability with your cloud-hosted or hybrid datacenter and your branch offices through Microsoft's global network. The CloudGen Firewall in combination with Virtual WAN fully enables automated large-scale branch connectivity, unified networks and policy management, and optimized routing using the Microsoft global network.

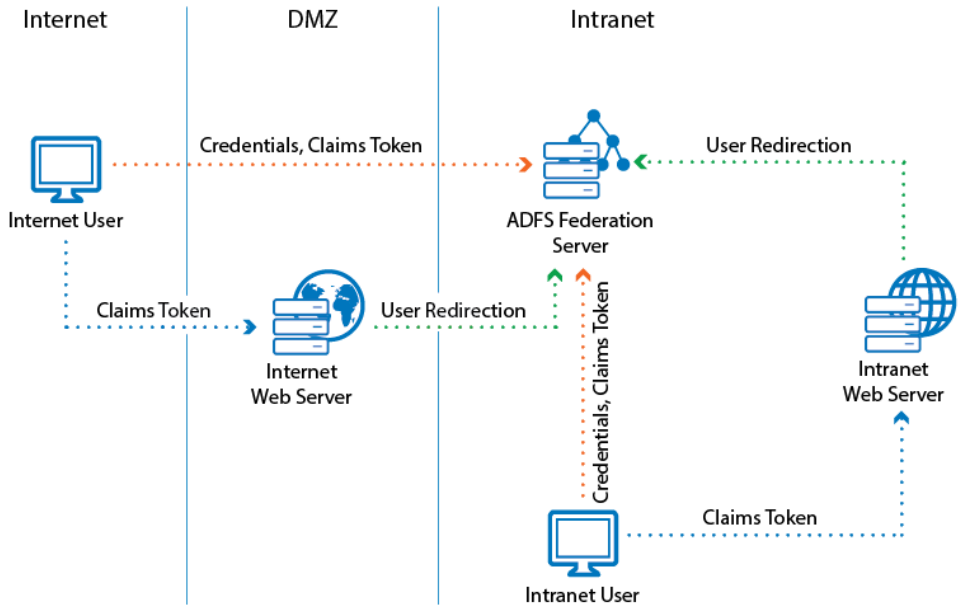
For more information, see Azure Virtual WAN.

Azure Accelerated Networking and AWS Elastic Network Adapter (ENA) Support

Single-Root I/O Virtualization (SR-IOV) technology enables multiple virtual host operating systems to share PCI-e IO-devices. This technology also provides increased performance for the CloudGen Firewall. This requires AWS instances that support the Elastic Network Adapter (ENA).

For more information, see Public Cloud.

Active Directory Federation Services (AD FS) Authentication



Active Directory Federation Services (AD FS) is a single sign-on (SSO), inline authentication solution offered by Microsoft. It allows applications to authenticate against AD without having to store credentials locally. The Active Directory acts as an identity provider; the application is the "service provider". Using AD FS is useful for users who want to authenticate only once across multiple organizations during a single session where one organization asserts the authenticity of the same user to another organization during the same session. For example, this enables users to get access to the web portal of a second service provider without any credentials after having previously signed on successfully to the web portal of the first service provider.

For more information see How to Configure AD FS Authentication.

VPN IPv6 Payloads

With the exception of SD-WAN for IPv6 payloads, IPv6 payloads in VPN tunnels are now supported and work only for TINA site-to-site tunnels.

AutoVPN

For Barracuda-only environments, setting up a site-to-site VPN tunnel has been highly improved. The new AutoVPN feature provides robust VPN connections through TINA tunnels that are automatically set up with dynamic routing between local networks. AutoVPN is suited for creating multiple boxes in the cloud and connecting them with a TINA site-to-site VPN tunnel.

Automatic setup of VPN tunnels is initiated via the command-line interface (CLI) and currently supports only connecting cloud instances.

For more information, see AutoVPN.

Managed Identities for Azure Resources

To be able to use the cloud service fabric API in Azure, the firewall VM must now authenticate using Managed Identities. Compared to creating Service Principals, this simplifies the entire process and can be performed completely in the Azure portal. Azure PowerShell is no longer required. The Managed Identities for Azure Resources feature provides Azure services with an automatically managed identity in Azure Active Directory (Azure AD). After enabling this feature in Azure, the Barracuda CGF detects the managed identity and automatically enables cloud integration.

For more information on how to enable Managed Identities, see Barracuda CloudGen Firewall Managed Identities in Microsoft Azure.

Enhanced Default Firewall Ruleset in the Cloud

CloudGen Firewalls that are run in the cloud are bound to the infrastructure preconditions set by the respective cloud operator. When a new firewall instance is deployed in the cloud, the firewall automatically creates and fills network objects during provisioning with subnets in the same VNET/VPC. The default ruleset now grants access when backend instances want to access the Internet, and redirects load balancer probes to a local service. The latter access rule is deactivated by default and uses port #6500.

For more information, see Default Forwarding Firewall Rules and Default Host Firewall Rules.

REST API Extensions

- REST for all common access rule operations: create / delete / list / change
- REST calls for network objects (stand-alone + CC (global cluster firewall objects))
- 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 (place in user data)

For more information, see https://campus.barracuda.com/product/cloudgenfirewall/api/8.0

Known Issues

- **AutoVPN** – In rare cases, if the cloud infrastructure is not available, AutoVPN must re-run to

configure the tunnels properly.

- **AutoVPN** – AutoVPN does not work on managed boxes and does not report an error when you try to do so. DOC
- **Azure-accelerated networking** – For every NIC, two devices show up (one for the hv_netvsc driver, and one for Mellanox). Use only every other device in boxnet (e.g. eth0, eth2, eth4). For every added NIC in Azure, the boxnet dynnet driver must be configured to create **2** devices.
- **Control Center** – Managing SCs in a Control Center 8.0.0 is not supported.
- **Google Cloud** – In rare cases, the serial console stops working.
- **HTTP Proxy Service** – URL filtering in combination with the HTTP Proxy service currently does not work. URL filtering in the firewall is not affected and works as designed.
- **IPFIX** – IPFIX reporting does not work. [BNNGF-55994]
- **VPN** – It is not possible to configure IKEv2 VPN tunnels with DH Groups 25-27. [BNNGF-56058]
- **VPN** – WAN Optimization is not supported. [BNNGF-55933]
- **WebUI** – Switching from Firewall Admin to the Web Interface causes the firewall to be unreachable. If needed, enable the Web Interface with the CLI command `cloud-enable-webui`.
- **Barracuda OS** – Phion rel-check reports dirty release on some installed RPMs.

Figures

1. adfs_overview.png