Migration Notes

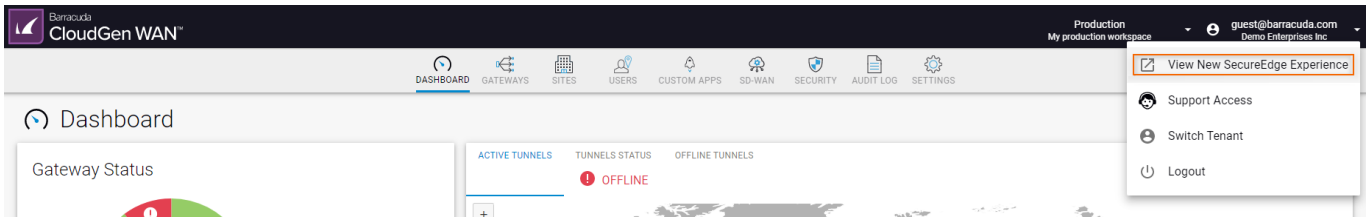
https://campus.barracuda.com/doc/98223572/

Refer to the sections below to learn about what you need to consider when migrating to Barracuda SecureEdge.

Initial Firmware Release

The initial release of Barracuda SecureEdge marks the product launch.

When migrating from Barracuda CloudGen WAN, you can switch to the new interface by expanding your login name and selecting **View New SecureEdge Experience**.



- For information on general product features, read the Release Notes.
- For setup instructions, see Getting Started.

Note that to reach a maximal homogeneous SecureEdge network, newly deployed sites will automatically update/align their firmware version to the SecureEdge Edge Services they are connecting to. This will happen regardless of the defined update window on the Barracuda SecureEdge Manager. This mechanism is in place to prevent attaching sites to the SecureEdge network with potentially outdated and/or incompatible firmware versions.

To use the SecureEdge Agent fallback port (TCP 443) and IKEv2 tunnels (UDP 500 and UDP 4500) on your existing Edge Service for Virtual WAN, you may have to redeploy your Edge Service for Virtual WAN.
To verify that the ports are enabled on your Edge Service for Virtual WAN, run the command: `telnet` <public IP of NVA> 443.

Important Note related to Backward-Compatibility

- If you configure a **WARN** or **ALERT** policy on Barracuda SecureEdge, it will be converted to a **BLOCK** policy on appliances running firmware version 8.3.x or 9.0.0.
- Please make sure to update your SecureEdge Agent to the latest version 1.0.3 before you update the point of entry to the latest firmware version 9.0.1.

For ACL rules: Selecting source or destination criteria to all sites and all private Edge Services results in the same networks configured on the box. This is a known issue and affects the following:

- All users with at least one private Edge Service. However, there is no effect if you have other Edge Services or sites.
- All security policies using the object ALL-Sites as source or destination match all LANs from all private Edge Services in the same workspace in addition to all site LANs. It should contain only site LANs, but this might affect existing policies, so you must adjust accordingly. This is a known issue.
- There is a new object called Private Edge Service that also contains all sites and private Edge Service LANs. You can use this object only when a new policy is configured. This should use only specific LANs. This is a known issue.

Figures

1. CloudUI.png