Zero Touch Deployment

https://campus.barracuda.com/doc/73719477/

To deploy managed CloudGen Firewalls using Zero Touch Deployment (ZTD), the Control Center must be configured to connect to the Zero Touch Deployment service. During the ordering process, for orders specified as ZTD orders, the firewall is associated with the Barracuda Cloud Control account that is used by the Control Center to query the cloud-based Zero Touch service for new, unconfigured firewalls. BCC accounts using one-time passwords for authentication are not supported for Zero Touch Deployments. After the order is confirmed, the firewall is displayed on the **Zero Touch Deployment** page of the Control Center and in the **Appliances** tab of the Zero Touch Deployment web UI. If the firewall is not already associated with the Control Center, it can now be claimed to create the association between the Control Center and the firewall. Claimed appliances are no longer visible in other Control Centers using the same credentials to sign in. To claim a firewall, the admin must enter the serial number and linking code included in the order confirmation email.

The admin creates and configures the firewall configuration on the Control Center and pushes a basic configuration for the claimed firewall to the ZTD service. This basic configuration contains enough information for the managed firewall to connect to the Control Center. To make sure the configuration is assigned to the correct appliance, select a property that is used as a filter. The firewall can be selected based on the serial number, the public IP address, or the IP address of the DHCP interface. Alternatively, you can just assign the configuration to the next available appliance.

Meanwhile, the firewall is shipped to the remote location. Connect the DHCP client port of the firewall to the network and power the firewall on. The DHCP client port depends on the firewall model:

- **SC2.x** – DHCP client port listens on port WAN.
- **F12 - F800** – DHCP client listens on port p4.
- **F900** – DHCP client listens on port A4.
- **F1000** – DHCP client listens on port D4.

The firewall receives an IP address via DHCP and connects to the Zero Touch Deployment service, then downloads and activates the basic configuration. The firewall connects to the Control Center via a remote management tunnel and downloads the full configuration. The firewall is now fully operational and managed by the Control Center.



STATUS:

Networking Requirements for Zero Touch Deployment

- ZTD relies on a correct time system. Make sure that the time settings on your CloudGen Firewall or Control Center are configured correctly. For more information, see How to Configure Time Server (NTP) Settings.
- Configure DNS. The firewall must be able to resolve hostnames. For more information, see How to Configure DNS Settings.
- ZTD uses ports 443 (REST HTTPS) and 692 (remote mgmt tunnel) for configuration. Ensure that these ports are open and not used for any other purpose.

Preparing a Firewall for Zero Touch Deployment

Before the configuration can be pushed to the remote firewall, the Control Center must be configured to connect to the Zero Touch service. The admin can then view and configure all firewalls purchased with the zero touch option.

For more information, see How to Configure a Firewall for Zero Touch Deployment.

Deploying a Firewall Using Zero Touch Deployment

Follow these steps to set up the firewall at the remote location to connect to the Zero Touch Deployment service.

For more information, see How to Deploy a Hardware Firewall with Zero Touch Deployment.

Zero Touch Deployment Service Web Interface

The Zero Touch Deployment service web interface allows you to view all connected appliances, progress, troubleshooting and audit logs.

For more information, see Zero Touch Deployment Service Web Interface.

Figures

1. ZeroTouchDeployment_smaller.gif

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.