Backing Up and Restoring your System Configuration

In This Article:

You can backup various system configuration and user settings on your Barracuda Web Application Firewall using the **ADVANCED > Backup** section. These files allow you to restore your current system, or duplicate the configuration on another Barracuda Web Application Firewall using the **Restore Backups** section on the **ADVANCED > Backup**s page.

It is recommended to take a backup of your system on a regular basis. This is required in case of restoring this information on a replacement Barracuda Web Application Firewall or in the event of your current system data corruption.

If you are restoring a backup file on a new Barracuda Web Application Firewall that is not configured, you need to configure the new system IP address and DNS information on the **BASIC > IP Configuration** page.

Note the following about the backup file:

- Do not edit backup files. Any configuration changes you want to make has to be done through the Web interface. The configuration backup file contains a checksum that prevents the file from being uploaded to the system if any changes are made.
- The following information is not included in the backup file:
  - System password
  - System IP address information
  - Certificate private key if **Allow Private Key Export** is set to *No* when uploading a certificate in the **BASIC > Certificates** page.

Backing Up the System Configuration

To backup your system configuration, perform the following steps:

1. Go to the **ADVANCED > Backups** page.
2. Enter the server details to which you want to save the backup files in the **Backup Destination Settings** section. For more information on **Destination** options, refer to the online help.
3. Set **Encrypt Backup** to Yes to encrypt the backup files with the encryption key specified in the **Backup Encryption Key** field. Note that the backup file can be decrypted using the same encryption key.
4. You can take a manual backup or schedule a backup to automatically save the backup files to the **Destination** location configured in the **Backup Destination Settings** section. For more information on **Manual Backups** and **Scheduled Backups**, refer to the online help.

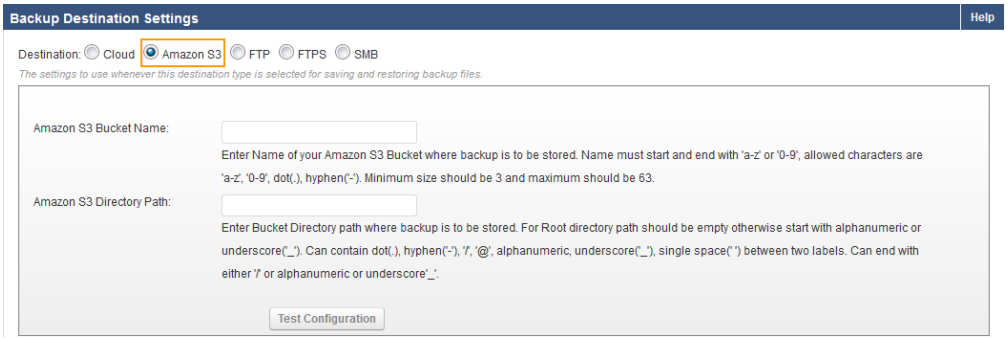
System configuration backup is generated automatically at the time of firmware update. The generated backup file(s) resides locally on the Barracuda Web Application Firewall, and can be found under **Saved Configuration Backups**. You can either download and restore these backup configurations or delete them.

Backing Up the Barracuda Web Application Firewall Instance(s) System Configuration in Amazon Web Services

You can backup the configuration of the Barracuda Web Application Firewall on Amazon Web Services to an associated S3 bucket for future retrieval. To take a backup, navigate to the **ADVANCED > Backups** page and specify the Amazon S3 bucket name and the directory path of the S3 bucket. The backup file stored in the Amazon S3 bucket can later be used for manual configuration or auto scaling the instances.

Steps To Backup System Configuration to Amazon S3 Bucket

1. Go to the **ADVANCED > Backups** page.
2. In the **Backup Destination Settings** section:
    1. Set **Destination** to **Amazon S3** and specify values for the following:
    2. **Amazon S3 Bucket Name** – Enter the name of the Amazon S3 bucket where the backup needs to be stored.
    3. **Amazon Directory Path** – Enter the directory path where the backup needs to be stored in the Amazon S3 bucket.
3. Click **Save**.



To deploy the Barracuda Web Application Firewall instance using the backup stored in Amazon S3, see the "Backup Bootstrapping" section in the Bring-Your-Own-License (BYOL) Auto Scaling article.

Backing Up the Barracuda Web Application Firewall Instance(s) System Configuration in Microsoft Azure

You can backup the configuration of the Barracuda Web Application Firewall on Microsoft Azure to an associated “Storage Blob” for future retrieval. To take a backup, navigate to the **ADVANCED > Backups** page and specify the Microsoft Azure account details and the blob path. The backup file stored in the Microsoft Azure Blob can later be used for manual configuration or auto scaling the instances.

Note that this feature is not compatible with "Azure Blob" in Microsoft Azure Government.

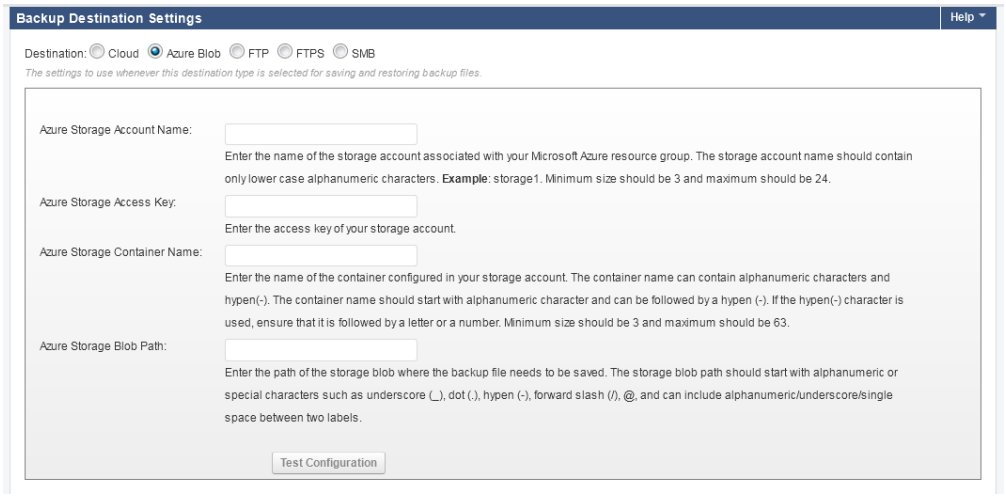
Steps to Backup System Configuration to Microsoft Azure Storage Blob

1. Go to the **ADVANCED > Backups** page.
2. In the **Backup Destination Settings** section:
3. Set **Destination** to Azure Blob and specify values for the following:
    1. **Azure Storage Account Name**: Enter the name of the storage account associated with your Microsoft Azure resource group.
    2. **Azure Storage Access Key**: Enter the access key of your storage account.
    3. **Azure Storage Container Name**: Enter the name of the container configured in the storage account in which the backup file needs to be saved.
    4. **Azure Storage Blob Path**: Enter the path of the storage blob where the backup file needs to be saved. The storage blob path should start with alphanumeric or special characters such as

underscore (_), dot (.), hypen (-), forward slash (/), @, and can include alphanumeric/underscore/single space between two labels. Example: exampleblob1/@abc/.

1. If you want to save the backup file in the root directory, keep the storage blob path empty.
2. If you want to create a new storage folder, enter a valid path for the folder to which the backup file needs to be saved.

4. Click **Save**.



To deploy the Barracuda Web Application Firewall instance using the backup stored in Azure Blob, see the Auto Scaling the Barracuda CloudGen WAF Instances in Microsoft Azure article.

Restoring the Configuration to your System

To restore the configuration to your current or to another system, perform the following steps:

1. Go to the **ADVANCED > Backups** page.
2. In the **Restore Backups** section:
    1. Select the server where your backup file(s) is saved from the **Restore From** drop-down list.
    2. Click **Browse** and select the backup file that needs to be restored.
    3. Select **Exclude Management Interface Configuration** to *Yes* or *No*.
        1. If set to *Yes*, Management interface configuration will not be restored from the backup.
        2. If set to *No*, all ACL rules, VLAN configuration and routes (static and interface routes) will be restored from the backup. **Note**: Custom virtual interfaces are not restored from the backup.
3. Click **Save**.

Few sensitive parameters such as "Azure AD User/Password" and "Service Principal Details" configured under the **BASIC > Azure Configuration** page are excluded in the backup file. This is done as a security measure to prevent any accidental leakage of the data. Hence, it is **ALWAYS** recommended to configure these parameters on the Barracuda Web Application Firewall User Interface after restoring the backup file. If you fail to configure these parameters, certain operations such as, service creation, service deletion will also fail.

Restoring SSL Services that are Associated with Non-Exportable Private Key Certificates

If **Allow Private Key Export** is set to **No** when uploading a certificate in the BASIC > Certificates page, the private key associated with the certificate will not be included in the backup file. Hence, all the SSL services will go down after restoring the backup file. To restore the services, do the following:

1. Continue with the steps below after performing the steps mentioned in the **Restoring the Configuration to your System** section.

2. Go to the **BASIC > Certificates** page, and upload the certificate(s) associated with the SSL services in the **Upload Certificate** section.
3. Go to the **BASIC > Services** page, edit the SSL service(s) and associate the certificate(s) with the service(s).

Restoring Multiple IP Addresses Configured System Backup in Microsoft Azure

To restore multiple IP addresses backup, perform the steps mentioned in the Restoring the Configuration to your System section.

If multiple IP address services backup is restored on to the other system, the IP address of services remain same as it was in the system from where the backup was taken. The administrator should manually change the IP address of each service (except the service created with the system IP address), and allocate the new IP address from the configured subnet. Before changing the IP addresses, ensure that your **Resource Group** is configured in '**Azure Advanced Networking**' on the **BASIC > Azure Configuration** page, as the **Azure Advanced Networking** settings will not be restored from the backup.

Figures