

## Backing Up and Restoring Your System Configuration

<https://campus.barracuda.com/doc/4259981/>

You can back up various system configurations 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 > Backups** page.

Barracuda Networks recommends taking a backup of your system on a regular basis, in case this information needs to be restored on a replacement Barracuda Web Application Firewall, or in the event of data corruption on your current system.

If you are restoring a backup file on a new Barracuda Web Application Firewall that is not yet configured, you must first 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 must 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:

Module Name	Information/configuration not restored
DNS Configuration	Primary DNS Server Secondary DNS Server
WAN IP Configuration	IPv4/IPv6 Address IPv4/IPv6 Subnet Mask IPv4/IPv6 Gateway Address Allow Administration Access VLAN ID
LAN IP Configuration	IPv4/IPv6 Address IPv4/IPv6 Subnet Mask Allow Administration Access VLAN ID
Management IP Configuration	IPv4/IPv6 Address IPv4/IPv6 Subnet Mask IPv4/IPv6 Gateway Address VLAN ID Allow Administration Access
Azure Configuration	

Cluster Settings	Cluster Shared Secret Cluster Name Failback Mode Cluster ID Monitor Link
Clustered Systems	Clustered Systems
Templates	
Scheduled Backups	Time of Backup
Primary Network HSM Server	Network HSM Partition Password
Appearance > General	System Name
Centralized Management	Username
Attack Types Identity Theft Patterns Input Types	Added Attack Patterns
Logging	Default System Log Level
Import API Spec (JSON Security)	Imported API specifications file
Telemetry Data	Parameter Name Enabled Parameters
Network Interfaces	NIC Interface Duplexity NIC Interface Name
Edit NIC Advanced Configuration	Auto-Negotiation Status
Web Interface Settings	Web Interface HTTP Port
Manual Backups	Status
Web Interface	Image URL
Time	Time Zone
Password	System Password

## 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.

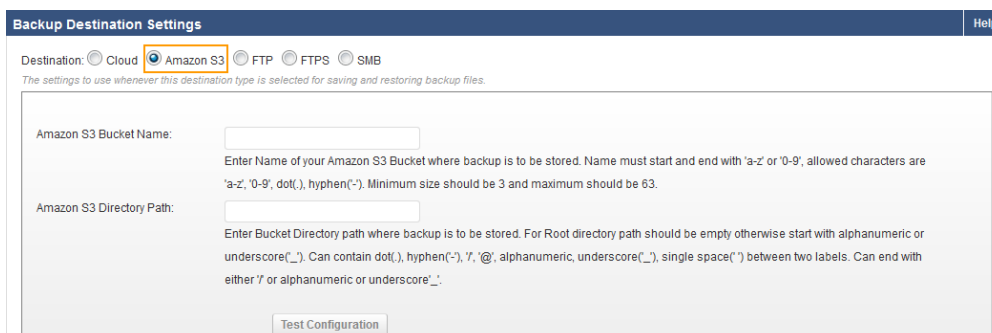
- Always ensure to keep the following ports open to allow the Barracuda Web Application Firewall to connect and communicate to [fttcp.prod.bac.barracudanetworks.com](http://fttcp.prod.bac.barracudanetworks.com) for saving cloud backups: 80, 8000, 23557 and 48320 . Otherwise, cloud backups might fail.
- A system configuration backup is generated automatically at the time of a firmware update. The generated backup file(s) reside 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, go 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:
    - **Amazon S3 Bucket Name** – The name of the Amazon S3 bucket where the backup will be stored.
    - **Amazon Directory Path** – The directory path where the backup will be stored in the Amazon S3 bucket.
3. Click **Save**.



**Backup Destination Settings** Help

Destination: ☐ Cloud ☒ **Amazon S3** ☐ FTP ☐ FTPS ☐ SMB

The settings to use whenever this destination type is selected for saving and restoring backup files.

Amazon S3 Bucket Name:   
Enter Name of your Amazon S3 Bucket where backup is to be stored. Name must start and end with 'a-z' or '0-9', allowed characters are 'a-z', '0-9', dot(.), hyphen(-). Minimum size should be 3 and maximum should be 63.

Amazon S3 Directory Path:   
Enter BucketDirectory path where backup is to be stored. For Root directory path should be empty otherwise start with alphanumeric or underscore(\_). Can contain dot(.), hyphen(-), /, @, alphanumeric, underscore(\_), single space(" ") between two labels. Can end with either / or alphanumeric or underscore\_.

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.

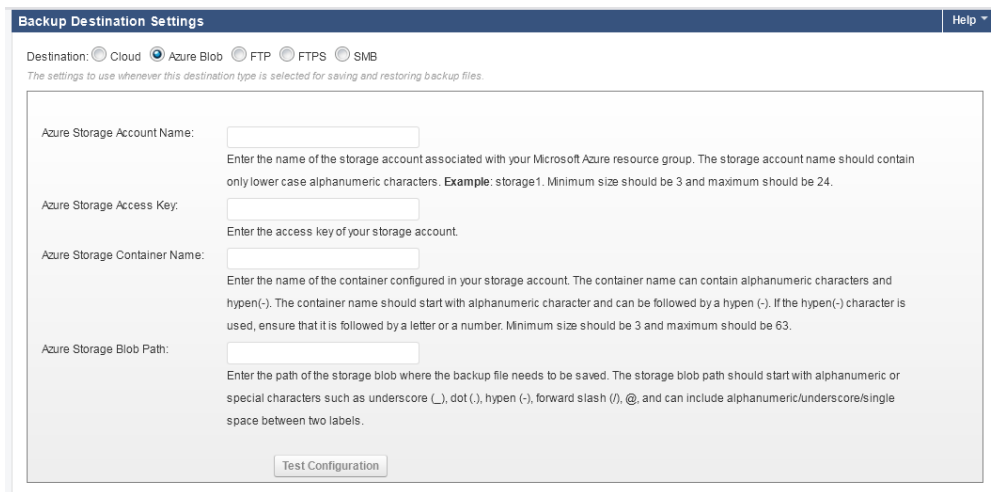
## Backing Up the Barracuda Web Application Firewall Instance(s) System Configuration in Microsoft Azure

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, go 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**: The name of the storage account associated with your Microsoft Azure resource group.
  2. **Azure Storage Access Key**: The access key of your storage account.
  3. **Azure Storage Container Name**: The name of the container configured in the storage account in which the backup file will be saved.
  4. **Azure Storage Blob Path**: The path of the storage blob where the backup file will be saved. The storage blob path should start with alphanumeric or special characters such as underscore (\_), dot (.), hyphen (-), forward slash (/), or @, 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 will 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 Web Application Firewall 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 you want to restore.
  3. Set **Exclude Management Interface Configuration** to Yes or No.
    1. If set to Yes, the 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**.

Bulk allocation of IP addresses for services restored from a configuration backup does not work on instances with less than 2 cores.

Some sensitive parameters such as Azure AD User/Password and Service Principal Details configured on the **BASIC > Azure Configuration** page are excluded from the backup file. This is a security measure to prevent accidental leakage of the data. Consequently, it is **ALWAYS** recommended to configure these parameters in the Barracuda Web Application Firewall web Interface after restoring the backup file. If you fail to configure these parameters, certain

operations such as service creation or service deletion will 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 on the **BASIC > Certificates** page, the private key associated with the certificate will not be included in the backup file. Consequently, all the SSL services will go down after restoring the backup file. To restore the services, do the following:

1. Follow the steps in **Restoring the Configuration to your System** section above, and then continue with step 2.
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 a multiple IP addresses backup, perform the steps mentioned in the [Restoring the Configuration to your System](#) section.

If a multiple IP address services backup from one system is restored onto a different system, the IP address of services remains 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

1. Backup\_Settings.png
2. Azure\_Blob.png

© 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.