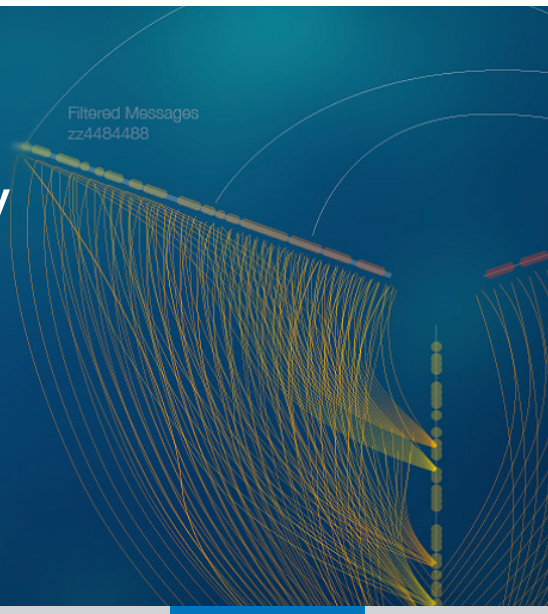
BarracudaCampus

Barracuda

Barracuda **Email Security Gateway**
Certified Engineer - ESG01



Course Handbook

ESG
Barracuda
Email Security Gateway

Official training material for Barracuda certified trainings and Autorized Training Centers.

Edition 2018 | Revision 1.0

campus.barracuda.com | campus@barracuda.com

Table of Contents

Deployment Options

Initial Setup - Routing Inbound Mail

Initial Setup - Routing Outbound Mail

User Interface – Basic Configuration

User Interface – BlockAccept

User Interface – Users

User Interface – Domains

User Interface – Advanced Configuration

Understanding the Message Log

Cloud Protection Layer

Email Encryption and Data Loss Prevention

1.1 General Information

1.1.1 Modules

This course covers deployment, setup, and advanced configuration of the Barracuda Email Security Gateway.

The training is either webinar based or provided as video-course divided into 6 seperate modules containing the following topics:

- Deployment Options
- Routing Inbound Mail
- Routing Outbound Mail
- User Interface – Basic Configuration
- User Interface – Block/Accept
- User Interface – Users
- User Interface – Domains
- User Interface – Advanced Configuration
- Understanding the Message Log
- Cloud Protection Layer
- Email Encryption and Data Loss Prevention

1.1.2 Audience

- System Administrators
- Network Engineers
- System Integrators
- Security Consultants

1.1.3 Prerequisites

- Basic networking knowledge
- Basic knowledge of email infrastructures

Deployment Options

1.1 Introducing the Email Security Gateway

The Barracuda Email Security Gateway is an integrated hardware and software solution designed to protect your email server from spam, virus, spoofing, phishing and spyware attacks. Outbound filtering and encryption options also prevent confidential or sensitive information from being purposely or inadvertently leaked outside the organization (Data Loss Prevention). The optional cloud protection layer (CPL) shields email servers from inbound malware and DoS attacks while filtering out normal spam and other threats before it ever touches the network's perimeter.

1.1.1 Key Features

- Spam and virus filtering, including:
  - The optional Barracuda Exchange Antivirus Agent, a free add-in that you can install on your Microsoft Exchange mailbox server(s).
  - Advanced Threat Protection, a subscription-based service that offers protection against advanced malware, zero-day exploits, and targeted attacks.
- Global or per-user quarantine
- Prevents spoofing, phishing and malware
- Data loss prevention (DLP) with outbound email filtering
- SMTP/TLS site-to-site encryption
- Invalid bounce suppression
- Policy enforcement for compliance and corporate policies
- Configuration backup to the cloud

1.1.2 Cloud Protection Layer - Pre Filtering

- Free Cloud Protection Layer provides:
  - Email spooling up to 96 hours
  - Inbound email filtering
  - Barracuda Real-Time Protection
  - Advanced Threat Protection
  - IP block/accept policies
  - Recipient and sender policies

1.1.3 Where to Start

Begin by selecting a deployment mode, depending on the email server configuration that currently exists at the site, as well as whether to deploy the Barracuda Email Security Gateway:

- Behind the corporate firewall
- In front of the corporate firewall in the DMZ

Barracuda recommends deploying the Barracuda Email Security Gateway behind a corporate firewall.

1.1.4 Clustering the Barracuda Email Security Gateway

Clustering two or more Barracuda Email Security Gateways makes sense if the organization requires high availability, scalability, data redundancy and/or fault tolerance. Clustering also provides centralized management of policy because once you configure one of the devices, configuration settings are synchronized across the cluster almost immediately. Clustered systems can be geographically dispersed and do not need to be located on the same network.

1.1.5 Device Deployment

- For on-premises deployment offering a wide ranges of models. Optional cloud protection layer (CPL).

1.1.6 Virtual Deployment

Provides same protection as hardware appliances, supporting various hypervisors and sizing options. Optional cloud protection layer (CPL).

1.1.7 Public Cloud Hosting

- Amazon Web Services (AWS)
- Microsoft Azure

1.2 Supported Platforms for the Email Security Gateway

The Barracuda Email Security Gateway is offered without per-user or per-feature fees, and is also available as a virtual appliance or in a public cloud environment (Amazon Web Services (AWS), or Microsoft Azure).

1.2.1 Hardware Appliance

- Hardened OS
- Eight models to choose from

MODEL COMPARISON	100*	200	300*	400*	600*	800*	900*	1000*
CAPACITY								
Active Email Users	1-50	51-500	300-1,000	1,000-5,000	3,000-10,000	8,000-22,000	15,000-30,000	25,000-100,000
Domains	10	50	250	500	5,000	5,000	5,000	5,000
Message Log Storage	8 GB	10 GB	12 GB	24 GB	72 GB	120 GB	240 GB	512 GB
Quarantine Storage			20 GB	60 GB	180 GB	360 GB	1 TB	2 TB
HARDWARE								
Rackmount Chassis	1U Mini	1U Mini	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize	2U Fullsize
Dimensions (in)	16.8 x 1.7 x 9	16.8 x 1.7 x 9	16.8 x 1.8 x 16	16.8 x 1.8 x 16	16.8 x 1.7 x 22.6	17.4 x 3.5 x 25.5	17.4 x 3.5 x 25.5	17.2 x 3.5 x 27.3
Weight (lb)	8	8	11	12.1	26	46	52	52
Ethernet	1 x 10/100	1 x Gigabit	1 x Gigabit	1 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit
AC Input Current (amps)	1.0	1.0	1.2	1.4	1.8	4.1	5.4	7.2
Redundant Disk Array (RAID)				•	Hot Swap	Hot Swap	Hot Swap	Hot Swap
ECC Memory					•	•	•	•
Redundant Power Supply						Hot Swap	Hot Swap	Hot Swap
FEATURES								
Advanced Threat Protection[1]	•	•	•	•	•	•	•	•
Outbound Email Filtering	•	•	•	•	•	•	•	•
Email Encryption	•	•	•	•	•	•	•	•
Cloud Protection Layer	•	•	•	•	•	•	•	•
MS Exchange/LDAP Accelerator			•	•	•	•	•	•
Per-User Settings and Quarantine			•	•	•	•	•	•
Delegated Help Desk Role			•	•	•	•	•	•
Syslog Support			•	•	•	•	•	•
Clustering & Remote Clustering				•	•	•	•	•
Per Domain Settings				•	•	•	•	•
Single Sign-On				•	•	•	•	•
SNMP/API				•	•	•	•	•
Customizable Branding					•	•	•	•
Per-User Score Settings					•	•	•	•
Delegated Domain Administration					•	•	•	•

[1] Also available in Vx (Virtual Edition). Specifications subject to change without notice.

Available Features Include:

- Redundant Disk Array (RAID)
- ECC Memory
- Redundant Power Supply
- Connectors:
  - Standard VGA
  - PS/2 keyboard/mouse
  - Ethernet (chart above)

Instant Replacement Service

- Replacement unit shipped next business day
- 24/7 technical support
- Free hardware refresh every four years

1.2.2 Virtual Appliance

- Hardened OS
- Common hypervisor support including; VMware ESX and Workstation, Oracle VirtualBox, Citrix Xen, and Microsoft Hyper-V
- Same protection features as the hardware appliance
- Seven models to choose from

MODEL COMPARISON	100	300	400	600	800	900	1000
FEATURES							
Active email users	1-50[1]	Up to 1,000	Up to 5,000	Up to 10,000	Up to 22,000	Up to 30,000	Up to 100,000
Number of CPU Cores Allowed	1	2	4	6	12	24	Unlmited
Outbound Filtering	•	•	•	•	•	•	•
Cloud Protection Layer	•	•	•	•	•	•	•
Email Encryption	•	•	•	•	•	•	•
Advanced Threat Protection*	•	•	•	•	•	•	•
MS Exchange/LDAP Accelerator		•	•	•	•	•	•
Per User Settings & Quarantine		•	•	•	•	•	•
Delegated Help Desk Role		•	•	•	•	•	•
Syslog Support		•	•	•	•	•	•
Clustering & Remote Clustering			•	•	•	•	•
Per Domain Settings			•	•	•	•	•
Single Sign-on			•	•	•	•	•
SNMP/API			•	•	•	•	•
Customizable Branding				•	•	•	•
Per User Score Settings				•	•	•	•
Delegated Domain Administration				•	•	•	•

[1] Limited to providing antispam and antivirus protection for up to 50 email addresses.

1.2.3 Barracuda Energize Updates - Hardware and Vx models

- Standard technical support
- Hourly spam definition updates
- Barracuda Reputation Databases
- Fingerprint and intent analysis definitions
- Hourly virus definition updates

1.2.4 Public Cloud Hosting

Cloud hosting of the Barracuda Email Security Gateway virtual machine is currently supported in various sizes, payment, and licensing options on:

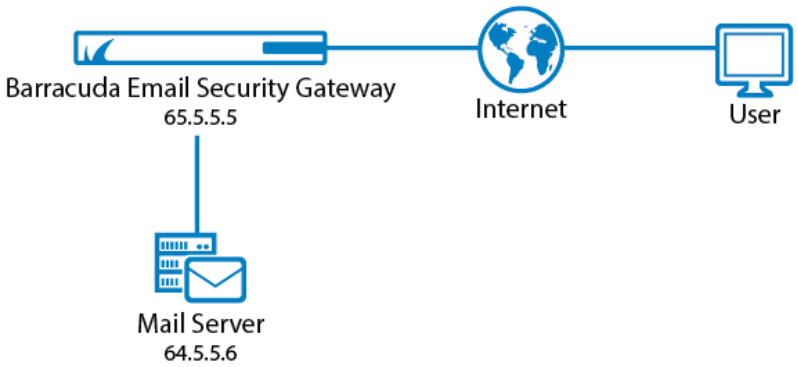
- Amazon Web Services (AWS)
- Microsoft Azure.

1.3 Deployment in the DMZ

You can deploy your Barracuda Email Security Gateway behind your corporate firewall or in front of your corporate firewall in the DMZ. However, for maximum security, **Barracuda recommends deploying the Barracuda Email Security Gateway behind a corporate firewall**.

1.3.1 Barracuda Email Security Gateway in the DMZ

The figure below shows the Barracuda Email Security Gateway in front of your corporate firewall in the DMZ. In this example, the Mail Server has an IP address of 64.5.5.6



In this type of setup, perform the following tasks:

1. Assign an available external IP address to the Barracuda Email Security Gateway.
2. Change the MX (Mail Exchange) records on the DNS (Domain Name Server) to direct traffic to the Barracuda Email Security Gateway. Create an A record and an MX record on your DNS for the Barracuda Email Security Gateway.

The following example shows a DNS entry for a Barracuda Email Security Gateway with a name of barracuda and an IP address of 64.5.5.5.

- barracuda.yourdomain.com IN A 64.5.5.5

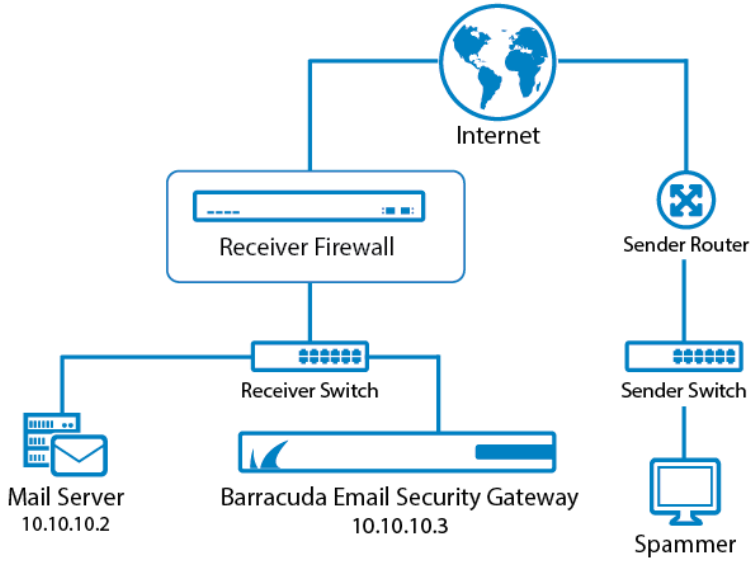
The following example shows the associated MX record with a priority number of 10:

- IN MX 10 barracuda.yourdomain.com

1.4 Deployment Behind the Corporate Firewall

You can deploy your Barracuda Email Security Gateway behind your corporate firewall or in front of your corporate firewall in the DMZ. However, for maximum security, **Barracuda recommends deploying the Barracuda Email Security Gateway behind a corporate firewall as described here**.

The figure below shows the Barracuda Email Security Gateway behind your corporate firewall. In this example, the Mail Server has an IP address of 10.10.10.2 and the Barracuda Email Security Gateway has an IP address of 10.10.10.3.



In this type of setup, perform the following tasks:

1. Forward (port redirection) incoming SMTP traffic on port 25 to the Barracuda Email Security Gateway at 10.10.10.3.
2. Configure the Barracuda Email Security Gateway to forward filtered messages to the destination mail server at 10.10.10.2.

There is no need to modify any MX records for this type of setup.

1.5 Clustering the Barracuda Email Security Gateway

1.5.1 Benefits of Clustering

Clustering Barracuda Email Security Gateways enables organizations to meet their high availability and fault tolerance requirements while also providing centralized management of policy, scalability and data redundancy. Linking multiple Barracuda Email Security Gateways is easy to do with a few parameter settings, and once you configure one of the devices, configuration settings are synchronized across the cluster almost immediately. Clustered systems can be geographically dispersed and do not need to be located on the same network.

1.5.2 Requirements for Clustering

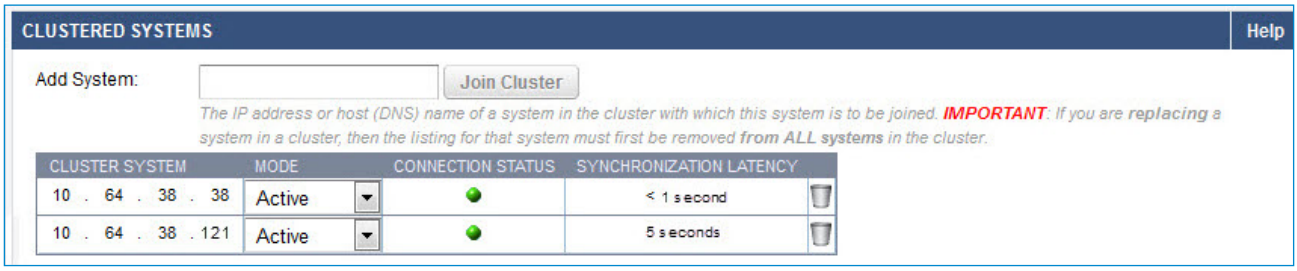
- Be the same model (400 and above).
- Have the same version of firmware installed.
- Be configured for the same time zone.
- Have a unique external IP address. This means that every Barracuda Email Security Gateway behind a NAT must have a unique external IP address and must be reachable by that external IP address.

How to Cluster the Barracuda Email Security Gateway

To cluster two Barracuda Email Security Gateways together, where one system is designated as "Barracuda1" and the other is designated "Barracuda2", do the following:

1. Complete the installation process for each system as described in Step 2 - Install the Barracuda Email Security Gateway in Barracuda Campus. Each Barracuda Email Security Gateway in a cluster must be the same model and be on exactly the same firmware version.
2. From the **ADVANCED > Task Manager** page on the Barracuda1 system, verify that no processes are running. Complete this step for the Barracuda2 system as well. No processes should be running when you add a system to a cluster.
3. Configure the Barracuda2 system as you would like Barracuda1, and any other system you might add to the cluster, to be configured. Make a backup of the configurations of each Barracuda Email Security Gateway.
4. From the **ADVANCED > Clustering** page on the Barracuda1 system, enter a **Cluster Shared Secret** password for the cluster, and click **Save**.
5. Optional: In the **Cluster Hostname** field on Barracuda1, enter the DNS/hostname (FQDN) by which other Barracuda Email Security Gateways in the cluster will attempt to communicate with this one. If this field is left blank, the IP address entered below will be used. This field is also useful for limiting user access to a cluster - **Limiting Access to a Cluster** below.

6. From the **ADVANCED > Clustering** page on the Barracuda2 system, do the following:
   a. Enter the same **Cluster Shared Secret** password, and click **Save**.
   b. Optionally enter the DNS/hostname (FQDN) in the **Cluster Hostname** field for Barracuda2.
   c. In the Clustered Systems section, enter the IP address of the Barracuda1 system and click **Join Cluster**. At this point, the configuration of the Barracuda1 system will automatically propagate to Barracuda2.
7. On each Barracuda system, refresh the **ADVANCED > Clustering** page, and verify that:
   a. Each system's IP address appears in the Clustered Systems list
   b. The Connection Status of each server is green - Figure below.
8. Distribute the incoming mail traffic to each Barracuda Email Security Gateway using a Barracuda Load Balancer (preferred) or another load balancing device, or by using multiple DNS MX records of equal priority.



Add a Barracuda Email Security Gateway to a Cluster

Begin by making a backup of the configuration of any system in the cluster, then perform these steps on the Barracuda Email Security Gateway you want to add to the existing cluster:

1. Complete the installation process and ensure that the new Barracuda Email Security Gateway is the same model# and running the same firmware version as all systems in the cluster.
2. From the **ADVANCED > Task Manager** page, verify that no processes are running. Do this on all other systems in the cluster as well.
3. From the **ADVANCED > Clustering** page, enter the **Cluster Shared Secret** password for the cluster, and click **Save**.
4. Optional: In the **Cluster Hostname** field, enter the DNS/hostname (FQDN) by which other Barracuda Email Security Gateways in the cluster will attempt to communicate with this one.
5. On a Barracuda Email Security Gateway already in the cluster, change any value in the configuration and click Save. This ensures proper synchronization of the configuration.
6. On the **ADVANCED > Clustering** page on the new Barracuda Email Security Gateway to be added to the cluster, enter the IP address of any system in the cluster in the **Add System** field and click the **Join Cluster** button. At this point, the configuration of the cluster will automatically propagate to the newly added system.

1.5.3 Limiting End-user Access to the Cluster

You can choose to dedicate a single Barracuda Email Security Gateway as the Quarantine Host to serve up the end-user interface through which users will access their quarantine inboxes, even though their actual quarantine inbox (primary or secondary) may be hosted by another Barracuda Email Security Gateway in the cluster. By not directing email to the Quarantine Host, you can:

- Enhance network security by limiting end-user access (port 8000 by default) and administration to only one Barracuda Email Security Gateway on the Internet
- Insulate the user interface performance from any peaks in email volume

To configure one Barracuda Email Security Gateway as the Quarantine Host, from the **BASIC > Quarantine** page, enter that system's hostname in the **Quarantine Host** field.

Removing a Barracuda Email Security Gateway From a Cluster

1. Log into the system to be removed and change or clear the **Cluster Shared Secret** on the **ADVANCED > Clustering** page. Click **Save Changes**. Changing the cluster shared secret prevents the systems in the cluster from communicating with one another.
2. On the same system, delete all other systems from the **Clustered Systems** list.
3. On any system that remains in the cluster, go to the **ADVANCED > Clustering** page. In the **Clustered Systems** list, delete the system to be removed from the cluster. **This step is very important** when removing a failed Barracuda Email Security Gateway from a cluster.

1.5.4 Exporting the Message Log

In a clustered environment, the maximum number of lines in a Message Log export is 10,000. To export more lines, use the Date Range feature in your Message Log search.

1.5.5 Centralized Policy Management With a Quarantine Host

You can optionally designate one Barracuda Email Security Gateway as the "host" of the cluster such that all administration of configuration settings and access to per-user quarantine for the cluster can only be accessed and set from that node. This option has two advantages: it provides for additional security by limiting access to administration of the cluster, and it protects the user interface from mail processing load since, with this configuration, you do not direct any email traffic to the host node.

To assign one Barracuda Email Security Gateway as the host of the cluster, enter the hostname of that device in the Quarantine Host field on the **BASIC > Quarantine** page and do not direct any email to that device.

1.5.6 Redundancy of user quarantine data on the cluster

Each user account has a primary and backup server in the cluster. Regardless of how many Barracuda Email Security Gateways there are in the cluster, there are always two appliances that have the same quarantine information (configuration and quarantine messages).

1.5.7 Data Not Synchronized Across the Cluster

Clustering provides 100% redundant coverage of the propagated data. However, for practical reasons, some data is not propagated to the other clustered systems when a new system joins. Energize updates do not synchronize across systems in a cluster. The following Barracuda Email Security Gateway configurations are considered unique and will not sync to match other Barracuda Email Security Gateways in a cluster:

- IP Address, Subnet Mask, and Default Gateway (on the **BASIC > IP Configuration** page)
- Primary DNS Server and Secondary DNS Server (on the **BASIC > IP Configuration** page)
- Serial number (this will never change)
- Hostname (on the **BASIC > IP Configuration** page)
- Any advanced IP configuration (Barracuda Email Security Gateway 600 and above, on the **ADVANCED > Advanced Networking** page)
- Administrator password
- Guest password
- Time Zone (on the **BASIC > Administration** page)
- Cluster hostname (on the **ADVANCED > Clustering** page)
- Cluster Shared Secret, though this must be the same for the cluster to work properly (on the **ADVANCED > Clustering** page)
- Local Host Map (on the **ADVANCED > Clustering** page)
- SMTP Welcome Banner (on the **ADVANCED > Email Protocol** page)
- SMTP Port (on the **BASIC > Outbound** page)
- Web Interface HTTP Port (on the **BASIC > Administration** page)
- Web Interface HTTPS/SSL port (on the **ADVANCED > Secure Administration** page)
- Any other secure administration configuration, including saved certificates (on the **ADVANCED > Secure Administration** page)
- Quarantine Host (on the **BASIC > Quarantine** page)
- All SSL/TLS information, including saved certificates (on the **ADVANCED > Secure Administration** page)

- Whether to only display local messages in the message log (Only view local messages on the **BASIC > Message Log > Preferences** page)
- Whether the latest release notes have been read
- All customized branding (Barracuda Email Security Gateway 600 and above, on the **ADVANCED > Appearance** page)

1.6 Virtual Deployment

Barracuda offers the following types of images for the Barracuda Email Security Gateway Vx deployment. Follow the instructions for your hypervisor to deploy the Barracuda Email Security Gateway Vx appliance.

Image Type	Supported Hypervisors
OVF	• VMware ESX and ESXi (vSphere Hypervisor) versions 4.x • VMWare ESX and ESXi (vSphere Hypervisor) versions 5.x and 6.x • Sun/Oracle VirtualBox and VirtualBox OSE version 3.2
VMX	• VMware Server 2.x • VMWare Workstation 6.x, Player 3.x, and Fusion 3.x
XVA	• Citrix XenServer 5.5+
VHD	• Microsoft Hyper-V 2008 R2, 2012, 2012 R2, and 10

1.6.1 Deploy OVF Images

If you plan to deploy the virtual appliance using the VMware vCenter web client, download and deploy the OVA file rather than the OVF file. The OVA file can be downloaded by selecting the vCloud option from the Barracuda Virtual Appliance Download page in Barracuda Campus.

VMware ESX and ESXi 4.x

Use the OVF file ending in **-4x. ovf** for this hypervisor .

1. Download and expand the Barracuda Email Security Gateway Vx ZIP folder.
2. From the **File** menu in the vSphere Client, select **Deploy OVF Template**.
3. Select **Import from file**, navigate to the extracted folder, and locate the Barracuda Email Security Gateway Vx OVF file. Click **Next**.
4. Enter a name for the virtual appliance. Click **Next**.
5. Select the resource pool for your virtual appliance. Click **Next**.
6. Select a datastore and disk formats. Click **Next**.
7. Click **Finish**.
8. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Email Security Gateway Vx** below.
9. On the **Virtual Machines** tab, right-click the Barracuda Email Security Gateway VM that you created. Select **Power > Power On** to run it.

10. Follow the Barracuda Email Security Gateway Vx Quick Start Guide instructions in Barracuda Campus to set up your virtual appliance.

VMware ESX and ESXi 5.x and 6.x

Use the OVF file ending in **-5x.ovf** or in **-6x.ovf** for this hypervisor.

1. Download and expand the Barracuda Email Security Gateway Vx ZIP folder.
2. Launch vSphere Client and select the appropriate host and resource pool.
3. From the **File** menu in the vSphere Client, select **Deploy OVF Template**.
4. Click **Browse**, navigate to the extracted folder, and select the Barracuda Email Security Gateway Vx OVF file. Click **Next**.
5. Verify that you are installing the correct Barracuda virtual appliance. Click **Next**.
6. Enter a name for the virtual appliance. Click **Next**.
7. Select the destination storage for the virtual machine. Click **Next**.
8. Select a disk format. To ensure maximum stability when deploying your Barracuda Vx appliance, specify the disk format as **Thick Provision Eager Zeroed**. Click **Next**.
9. Map the network to the target network for this virtual appliance. Click **Next**.
10. Review the deployment options. Click **Finish** to deploy the virtual appliance.
11. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Email Security Gateway Vx** below.
12. Locate the appliance within the appropriate virtual machine and resource pool. Select it and power it on by clicking the green arrow.
13. Click the **Console** tab. You can monitor the appliance as it is prepared for use.
14. Follow the Barracuda Email Security Gateway Vx Quick Start Guide instructions in Barracuda Campus to set up your virtual appliance.

Sun/Oracle VirtualBox and VirtualBox OSE 3.2

Use the OVF file ending in **-4x. ovf** for this hypervisor.

1. Download and expand the Barracuda Email Security Gateway Vx ZIP folder.
2. From the **File** menu in the VirtualBox client, select **Import Appliance**.
3. Navigate to the extracted folder and locate the Barracuda Email Security Gateway Vx OVF file.
4. Select the file and click **Next**.
5. On the **Import Settings** screen, follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Email Security Gateway Vx** below. Click **Finish**.
6. Start the appliance.

7. Follow the Barracuda Email Security Gateway Vx Quick Start Guide instructions in Barracuda Campus to set up your virtual appliance.

1.6.2 Deploy VMX Images

VMware Server 2.x

Use the **.vmx** and **.vmdk** files for this hypervisor.

1. Download and expand the Barracuda Email Security Gateway Vx ZIP folder.
2. Navigate to the extracted folder and move the files ending in **.vmx** and **.vmdk** into a folder in your datastore (which you can locate from the **Datastores** list on your server's summary page).
3. From the VMware Infrastructure Web Access client's **Virtual Machine** menu, select **Add Virtual Machine** to Inventory.
4. Navigate to the folder in your datastore used in step 2 and select the file ending in .**vmx**. Click **OK**.
5. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Email Security Gateway Vx** below.
6. Start the appliance.
7. Follow the Barracuda Email Security Gateway Vx Quick Start Guide instructions in Barracuda Campus to set up your virtual appliance.

VMware Workstation 6.x, Player 3.x, and Fusion 3.x

Use the **.vmx** file for this hypervisor.

1. Download and expand the Barracuda Email Security Gateway Vx ZIP folder.
2. From the **File** menu, select **Open a Virtual Machine**.
3. Navigate to the extracted folder and select the file ending in **.vmx**.
4. Use the default settings and click **Finish**.
5. Follow the recommendations in **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Email Security Gateway Vx** below.
6. Start the appliance.
7. Follow the Barracuda Email Security Gateway Vx Quick Start Guide instructions to set up your virtual appliance.

1.6.3 Deploy XVA Images

Citrix XEN Server 5.5+

Use the .xva file for this hypervisor. For XEN Server, you first import the virtual appliance template and then create a new virtual appliance based on that template.

Step 1. Import the virtual appliance template:

1. Download and expand the Barracuda Email Security Gateway Vx ZIP folder.
2. From the **File** menu in the XenCenter client, select **Import**.
3. Click **Browse**, navigate to the extracted folder, and select the file ending in **.xva**. Click **Next**.
4. Select a server for the template. Click **Next**.
5. Select a storage repository for the template. Click **Import**.
6. Select a virtual network interface for the template. Click **Next**.
7. Review the template settings. Click **Finish** to import the template.

Step 2. Create a new virtual appliance:

1. Right-click the virtual appliance template and select **New VM wizard**.
2. Select the virtual appliance template. Click **Next**.
3. Enter a name for the virtual appliance. Click **Next**.
4. For the DVD drive, select **<empty>**. Click **Next**.
5. Select a home server. Click **Next.**
6. Specify the number of virtual CPUs and memory for the virtual appliance. Follow the recommendations below under **Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Email Security Gateway Vx**. Click **Next**.
7. Select a virtual disk. Click **Next**.
8. Select a virtual network interface. Click **Next**.
9. Review the virtual appliance settings. Click **Create Now**.
10. When the virtual appliance is ready, right-click it and then click **Start**.
11. Follow the Barracuda Email Security Gateway Vx Quick Start Guide instructions in Barracuda Campus to set up your virtual appliance.

1.6.4 Deploy VHD Images

Microsoft Hyper-V 2008 R2, 2012, 2012 R2, and 10

Use the **.vhd** file for this hypervisor.

1. Download and expand the Barracuda Email Security Gateway Vx ZIP folder.
2. Launch the **WinServerSetup.bat** file located in the extracted folder. This batch file corrects a compatibility issue and takes less than a minute to run.
3. Navigate to the extracted folder and verify that the **HyperV** folder contains the following subfolders:

- Virtual Machines
- Virtual Hard Disks
- Snapshots

4. In Hyper-V Manager, right-click your VM host and select **Import Virtual Machine**.
5. On the **Before You Begin** page of the **Import Virtual Machine** wizard, click **Next**.
6. On the **Locate Folder** page:
   a. Click **Browse**, navigate to the extracted folder, and select the HyperV folder. Click **Select Folde**r.
   b. Click **Next**.
7. On the **Select Virtual Machine** page, click **Next**.
8. On the **Choose Import Type** page, select **Copy the virtual machine (created a new unique ID)**. Click **Next**.
9. On the **Choose Destination: Choose Folders for Virtual Machine Files** page, click **Browse** to search for the location where you want to store the VM files. Click **Next**.
10. On the **Choose Storage Folders: Choose Folders to Store Virtual Hard Disks** page, click **Browse** to search for the location where you want to store the virtual hard disks for the VM. Click **Next**.
11. For Microsoft Windows 10, you can modify the RAM and Hard Disk space allocations after completing step 12.
12. On the **Configure Memory** page, enter a size for the **Startup RAM** that meets the requirements specified below. Keep the default settings for the other fields. Click **Next**.
13. On the **Connect Network** page, select the network interface that you want to use for management access of the VM. Click **Next**.
14. On the **Summary** page, verify that all the settings are correct. Click **Finish**.
15. For Microsoft Windows 10, go to the **Actions** pane and click on **Settings** under **Barracuda Email Security Gateway**. Under Hardware, ensure that their is enough memory and hard disk space as specified below.
16. Start your virtual appliance.
17. Follow the Barracuda Email Security Gateway Vx Quick Start Guide instructions to set up the virtual appliance.

Allocating Cores, RAM, and Hard Disk Space for the Barracuda Email Security Gateway Vx

Model	Cores	RAM - Recommend Minimum	Hard Disk - Recommend Minimum
100 Vx	1	2.5 GB	50 GB
300 Vx	2	5 GB	50 GB
400 Vx	4	10 GB	50 GB
600 Vx	6 (1)	15 GB	200 GB
800 Vx	12	24 GB	400 GB
900 Vx	24	48 GB	1 TB
1000 Vx	48(2)	96 GB	2 TB

(1) To increase the performance of this model, you should plan on adding 2.5 GB of RAM for each additional core. Also plan to add additional hard disk space. To purchase licenses for additional cores, contact your Barracuda sales representative.

(2) Recommended value; can increase to an unlimited number of cores.

Allocating Cores

In your hypervisor, specify the number of cores to be used by the Barracuda Email Security Gateway Vx. Each Barracuda Email Security Gateway Vx model can use only the number of cores specified in the table above. For example, if you assign 6 cores to the Barracuda Email Security Gateway 300 Vx (which supports only 2 cores), the hypervisor disables the 4 extra cores that cannot be used.

To add cores to your appliance:

18. Shut down the Barracuda Email Security Gateway Vx in your hypervisor.
19. In the virtual machine CPU settings, add cores.

Your hypervisor license and version might limit the number of cores that you can specify for your appliance. In some cases, you must add cores in multiples of two.

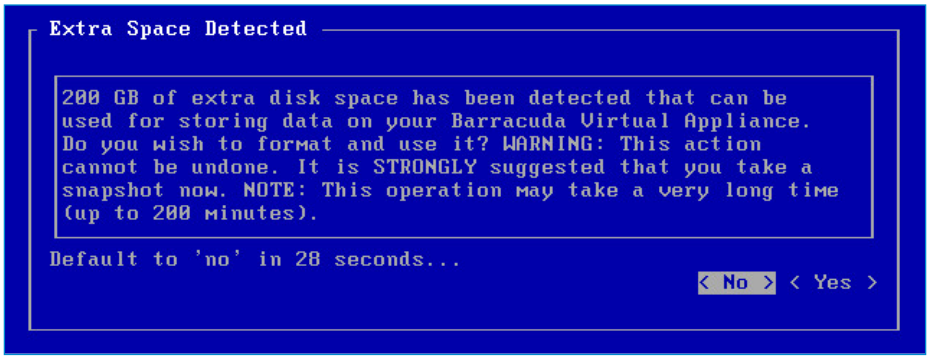
Allocating Hard Disk Space

Barracuda requires a minimum of 50 GB of hard disk space to run your Barracuda Email Security Gateway Vx. From your hypervisor, you can specify the size of the hard disk or add a hard disk.

To specify the allocated hard disk space or add a hard disk to your appliance:

20. Shut down the Barracuda Email Security Gateway Vx in your hypervisor.
21. Take a snapshot of the virtual machine.
22. In the virtual machine settings, specify the new size for the hard disk or add a new hard disk.
23. Restart the virtual machine. As the appliance is booting up, view the console for Barracuda Email Security Gateway Vx.

    When the blue Barracuda console screen appears and asks if you want to use the additional hard disk space, enter **Yes**.



If you do not respond to the prompt in 30 seconds, the answer defaults to **No** . Resizing can take several minutes, depending on the amount of hard disk space specified.

Next Step

For instructions on how to set up the Barracuda Email Security Gateway Vx, the Barracuda Email Security Gateway Vx Quick Start Guide in Barracuda Campus.

1.7 Public Cloud Hosting

Barracuda Email Security Gateway virtual machine is currently supported on:

1.7.1 Amazon Web Services (AWS)

Before you begin

1. Create an Amazon Web Services account.
2. Create a Virtual Private Cloud (VPC) on Amazon Web Services. See Creating a VPC, Internet Gateway and Subnet in Barracuda Campus.
3. Choose either the BYOL or Hourly/Metered licensing option:

- **Bring Your Own License (BYOL)** – This option involves first obtaining a Barracuda Email Security Gateway license token, either by:
  - Providing the required information for a free evaluation at https://www.barracuda.com/purchase/evaluation OR
  - Purchasing online at https://www.barracuda.com/purchase. With this license option, there will be no **Barracuda Email Security Gateway Software** charges, but **Amazon Elastic Compute Cloud (Amazon EC2) usage** charges on Amazon do apply.
- Barracuda offers the same three models for both the Hourly/Metered and BYOL options as shown below. After obtaining your license token, visit the AWS Marketplace to continue the process.
- **Hourly / Metered** – In this licensing option, you complete the purchase/evaluation of the Barracuda Email Security Gateway entirely within the AWS Marketplace. Once the instance is launched, it will be provisioned automatically. In this option, you will be charged hourly for both the **Barracuda Email Security Gateway Software** and **Amazon Elastic Compute Cloud (Amazon EC2)** usage on Amazon. For pricing information, the AWS Marketplace. Barracuda offers the same three models for both the Hourly/Metered and BYOL options as shown on the next page.

Barracuda Email Security Gateway Virtual Appliance Instance Types on AWS

The table below lists the available Barracuda Email Security Gateway virtual appliance models, the corresponding Instance Type to be used in Amazon Web Services and the default CPU and Memory for the instance.

Barracuda Email Security Gateway Model	Old Instance Types	New Instance Types	vCPU	Memory
BSF Cloud Edition – Level 3	m1.medium, m3.medium	t2.small	1	3.7 GB
BSF Cloud Edition – Level 4	m1.large, m3.large	t2.medium, t2.large, m4.large, c4.large	2	7.5 GB
BSF Cloud Edition – Level 6	m1.xlarge, m3.xlarge	m4.xlarge, m4.2xlarge, c4.xlarge, c4.2xlarge	4	15 GB

If you need to add additional storage space after deployment, due to the Amazon Web Services (AWS) structure, the only current option is to redeploy and restore the configuration on a larger instance.

To complete deployment, follow instructions in the Barracuda Campus article How to Deploy the Barracuda Email Security Gateway on Amazon Web Services.

1.7.2 Microsoft Azure

Microsoft Azure is a public cloud service, with instances that use one virtual network interface with a dynamic IP address per virtual appliance. The Barracuda Email Security Gateway can be deployed as a virtual appliance in the Microsoft Azure cloud to protect your email server from spam, virus, spoofing, phishing and spyware attacks. Outbound filtering and encryption options also prevent confidential or sensitive information from being purposely or inadvertently leaked outside the organization.

Licensing Options

The Barracuda Email Security Gateway is available on Microsoft Azure with the **Bring Your Own License (BYOL)** and **Hourly / Metered** options.

Bring Your Own License (BYOL)

With the Bring Your Own License (BYOL) option, you are required to get the Barracuda Email Security Gateway license token, either by:

- Providing the required information for a free evaluation at https://www.barracuda.com/purchase/evaluation OR
- Purchasing online at https://www.barracuda.com/purchase. With this license option, there will be no **Barracuda Email Security Gateway Software** charges, but **Microsoft Azure usage** charges on Microsoft will be applicable.

- You can either begin with the free evaluation OR purchase the Barracuda Email Security Gateway license directly after deploying the VM or when accessing the VM web interface for the first time.

BYOL Models and Instance Types

For BYOL, the Barracuda Email Security Gateway virtual appliance is available in three sizes on Microsoft Azure. The following table lists each size level with their corresponding instance type, cores, and memory allocated to each instance type. You'll select the Instance Type in the next step in **How to Deploy the Barracuda Email Security Gateway on Microsoft Azure**. If you want to increase the performance of a license that you have already purchased, you can buy additional cores from Barracuda and reconfigure for a larger instance type.

Initial Setup - Routing Inbound Mail

2.1 Physical Deployment and Initial Configuration

2.1.1 Checklist for Unpacking

Before installing your Barracuda Email Security Gateway, match the items on this list with the items in the box. If any item is missing or damaged, please contact your Barracuda Networks Sales representative.

- Barracuda Email Security Gateway (check that you have received the correct model)
- AC power cord
- Mounting rails (Barracuda Email Security Gateway 600, 800, and 900 only)

Also required for installation:

- VGA monitor
- PS2 keyboard
- Ethernet cables

To physically install the Barracuda Email Security Gateway:

1. Fasten the Barracuda Email Security Gateway to a standard 19-inch rack or other stable location.

   Important: Do not block the cooling vents located on the front and rear of the unit.

2. Connect a CAT5 Ethernet cable from your network switch to the Ethernet port on the back of your Barracuda Email Security Gateway.

   The Barracuda Email Security Gateway supports both 10BaseT and 100BaseT Ethernet. Barracuda Networks recommends using a 100BaseT connection for best performance.

   The Barracuda Email Security Gateway 600 and higher supports Gigabit Ethernet and has two usable LAN ports. On these models, plug the Ethernet cable into the LAN 2 port.

   Do not connect any other cables to the other connectors on the unit. These connectors are for diagnostic purposes.

3. Connect the following to your Barracuda Email Security Gateway:
   - Power cord
   - VGA monitor
   - PS2 keyboard
4. After you connect the AC power cord the Barracuda Email Security Gateway may power on for a few seconds and then power off. This is standard behavior.

5. Press the **Power** button located on the front of the unit. The login prompt for the administrative console is displayed on the monitor, and the light on the front of the system turns on. For a description of each indicator light, refer to Barracuda Email Security Gateway Panel Indicators, Ports, and Connectors.

2.1.2 APC UPS Support

An APC (American Power Conversion) UPS (Uninterruptible Power Supply) device with a USB interface is supported with the Barracuda Email Security Gateway. No configuration changes are needed on the Barracuda Email Security Gateway to use one. When the APC UPS device is on battery power, the web interface will display an alert, and the Barracuda Email Security Gateway will shut down safely when there is an estimated time of 3 minutes of battery power remaining.

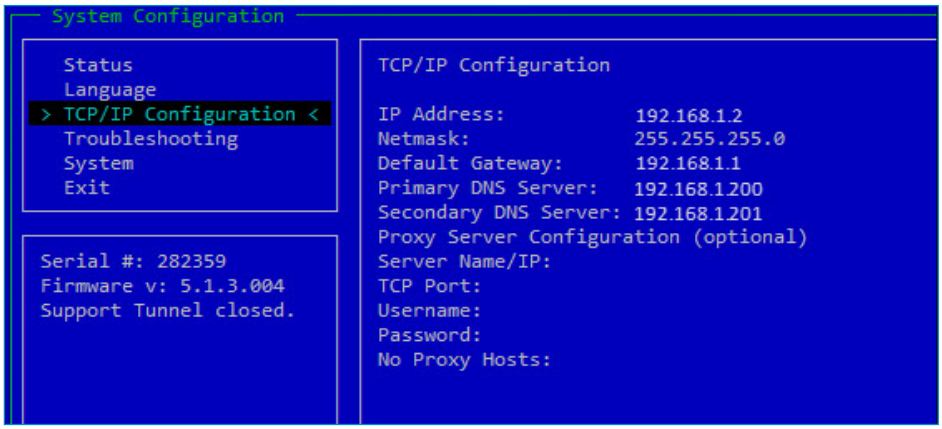
2.1.3 Configure IP Address and Network Settings

The Barracuda Email Security Gateway is given a default IP address of 192.168.200.200. You can change this address by doing either of the following:

- Connect directly to the Barracuda Email Security Gateway with a keyboard and monitor and specify a new IP address through the console interface.
- Log into the Barracuda Email Security Gateway web interface as admin and change the IP address on the **BASIC > IP Configuration** page.

To connect directly to the Barracuda Email Security Gateway to set a new IP address:

1. At the **barracuda login** prompt, enter admin for the login and admin for the password. The **User Confirmation Requested** window will display the current IP configuration of the system.



2. Using the Tab key, select **Yes** to change the IP configuration.
3. Enter the new IP address, netmask, and default gateway for your Barracuda Email Security Gateway, and select **OK** when finished.

4. Select **No** when prompted if you want to change the IP configuration. Upon exiting the screen, the new IP address and network settings will be applied to the Barracuda Email Security Gateway.

2.1.4 Configure Your Corporate Firewall

If your Barracuda Email Security Gateway is located behind a corporate firewall, you need to open specific ports to allow communication between the Barracuda Email Security Gateway and remote servers.

To configure your corporate firewall:

1. Using the following table as a reference, open the specified ports on your corporate firewall:

Port	Direction	Protocol	Used for
22	Out	TCP	Remote diagnostics and technical support services (recommended)
25	In/Out	TCP	SMTP
53	Out	TCP/ UDP	Domain Name Server (DNS)
80(1)	Out	TCP	Virus, firmware, security and spam rule definitions
123	Out	TCP	NTP (Network Time Protocol)
8000(2) (default)	Out	TCP	Virus, firmware, security and spam rule definitions

(1) If your firewall allows unrestricted outbound traffic on port 80, then no further action is necessary. If there are restrictions on outbound traffic on this port, you must configure your firewall as described in Ports for Firmware and Definition Updates to allow the Barracuda Email Security Gateway access to firmware and definition updates.

(2) If your firewall allows unrestricted outbound traffic on port 8000, then no further action is necessary.

2. If appropriate, change the NAT routing of your corporate firewall to route incoming email to the Barracuda Email Security Gateway. Consult your firewall documentation or your corporate firewall administrator to make the necessary changes.

After specifying the IP address of the system and opening the necessary ports on your firewall, you need to configure the Barracuda Email Security Gateway from the web interface. Make sure the computer from which you configure the Barracuda Email Security Gateway is connected to the same network, and the appropriate routing is in place to allow connection to the Barracuda Email Security Gateway's IP address from a web browser.

2.2 Routing Inbound Mail

The next step in setting up your Barracuda Email Security Gateway is to route incoming email to the system so it can scan incoming messages for spam and viruses.

Note that inbound mail will be blocked if the domain receiving the mail has not been configured on the Email Security Gateway.

You will configure domains at a later time.

You can use either of the following methods to route messages to the Barracuda Email Security Gateway:

- Use port forwarding to redirect incoming SMTP traffic (port 25) to the Barracuda Email Security Gateway if it is installed behind a corporate firewall running NAT (Network Address Translation). Configure this option on the **ADVANCED > Advanced Networking** page. For more information about port forwarding, refer to your firewall documentation or network administrator.
- MX records are used when your Barracuda Email Security Gateway is located in a DMZ with a routeable public IP address. If your Barracuda Email Security Gateway is in the DMZ (not protected by your corporate firewall), do the following to route incoming messages to the system:

1. Create a DNS entry for your Barracuda Email Security Gateway. The following example shows a DNS entry for a Barracuda Email Security Gateway with a name of **barracuda** and an IP address of **66.233.233.88**:

   ```
   barracuda.yourdomain.com IN A 66.233.233.88
   ```

2. Change your DNS MX Records. The following example shows the associated MX record with a priority number of 10:

   ```
   IN MX 10 barracuda.yourdomain.com
   ```

You can configure specific SMTP settings from the **ADVANCED > Email Protocol** page. After you route incoming email to the Barracuda Email Security Gateway, it will begin filtering all email it receives and routing good email to the mail server.

Test Spam and Virus Scanning With a Local (Test) User Set

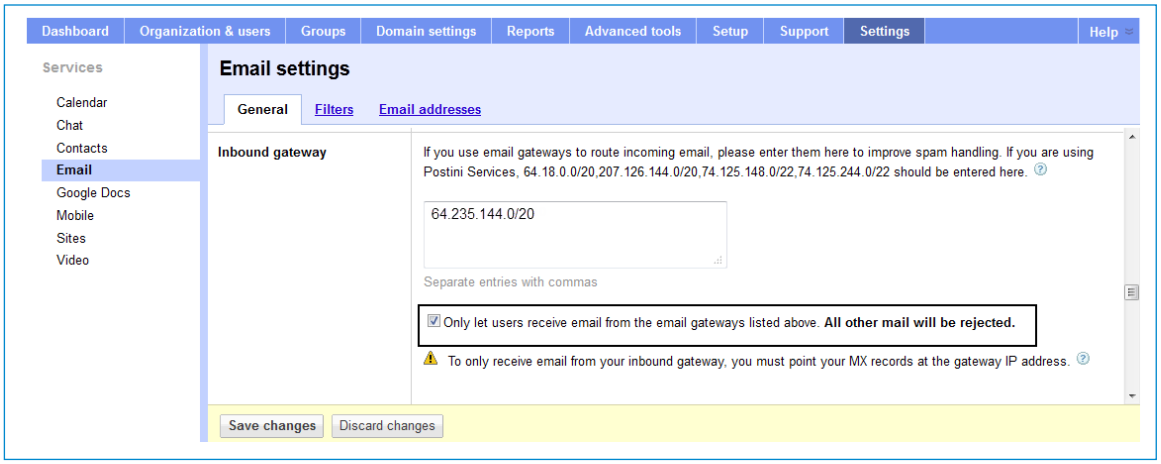
With the Barracuda Email Security Gateway 400 and higher, you have the option to use the **Explicit Users to Scan For** feature to test a subset of locally defined users before fully deploying the Barracuda Email Security Gateway. See the **ADVANCED > Explicit Users** page.

2.3 G Suite Inbound Configuration

This section addresses configuring G Suite Business and Education editions with the Barracuda Email Security Gateway as your inbound mail gateway. Outbound will be covered in a later section.

Inbound Configuration - G Suite

1. Log into the G Suite Domain Management Portal.
2. Navigate to the **Settings** tab and then select **Email** under the **Services** section.
3. Navigate to **Inbound Gateway** and enter the public IP addresses of the Barracuda Spam Email Security Gateway(s), specifying either the block of addresses or individual IP addresses.



Make sure to check the box: **Only let users receive email from the email gateways listed above. All other mail will be rejected.** Follow additional instructions for configuring G Suite to bypass the Barracuda Email Security Gateway for internal mail, if needed, in the Barracuda Campus article How to Configure G Suite for Inbound and Outbound Mail.

Configure the Barracuda Email Security Gateway

1. Navigate to **DOMAINS > Domain Manager** and specify your domain in New Domain Name, then click Add Domain.
2. Click the Manage Domain link and then **BASIC > IP Configuration**. Add the G Suite destination mail servers as follows:

G Suite Destination Mail Server
ASPMX.L.GOOGLE.COM
ALT1.ASPMX.L.GOOGLE.COM
ALT2.ASPMX.L.GOOGLE.COM
ASPMX2.GOOGLEMAIL.COM
ASPMX3.GOOGLEMAIL.COM

Also add the **Destination Server** name/IP address or hostname that receives email after spam and virus scans. It is usually best to use a hostname rather than an IP address so that the destination mail server can be moved and DNS updated at any time without having to make changes to the Barracuda Email Security Gateway configuration.

If you set **Use MX Records** (on the same page) to **Yes**, you must enter a domain name for this field. If multiple servers are specified, then the delimiter used determines the behavior (see below). Note that you can either configure **Use MX Records** for ***all*** domains from the **BASIC > IP Configuration** page, or you can configure it per-domain from **DOMAINS > Domain Manager > Manage Domains**, then using the **BASIC > IP Configuration** page for the domain you choose to manage. It is *NOT* recommended to set **Use MX Records** to **Yes** to avoid a potential mail loop.

- **Comma** (",") or semi-colon (";") - Each entry in the list will used in round-robin fashion, with relative weights determined by the number of times a particular entry is listed.
- **Space** (" ") - Each entry in the list will be treated as a failover list, with an entry being used only if all entries preceding it in the list are unreachable.

For more information about what it means to use MX records, please see Using MX Records.

2.4 Routing Mail Through Amazon Web Services

In order to preserve the quality of the Amazon Web Services environment for sending email, Amazon Web Services enforces default limits on the amount of email that can be sent from EC2 accounts. Before you put your Barracuda Email Security Gateway into production, **you need to request Amazon Web Services to remove the default email sending limits.**

To do so, visit https://portal.aws.amazon.com/gp/aws/html-forms-controller/contactus/ec2-email-limit-rdns-request, sign into your Amazon Web Services account and fill in the three required fields on the form, as shown in Figure 1 below. While you await a response to the request, you can send small amounts of test email through the Barracuda Email Security Gateway. If you do not take this step, you may experience large queues of mail and/or deferred mail that will eventually be delivered, but may be delayed.

Here is a recommended, generic **Use Case Description** that you might use in the form:

> We are putting the Barracuda Email Security Gateway into a production environment and, as such, require consistent mail delivery.

Continue with instructions in Barracuda Campus at How to Deploy the Barracuda Email Security Gateway on Amazon Web Services.

2.5 Office 365 for Inbound Mail

Office 365 addresses and user interfaces can change, so please refer to Microsoft documentation for details on configuration. To prepare your Barracuda Email Security Gateway deployment to connect with Office 365, see Microsoft documentation on:

- Setting up connectors to route mail between Office 365 and your own email servers, and
- Prerequisites for your email server environment

You can specify the Barracuda Email Security Gateway as an *inbound mail gateway* through which all incoming mail for your domain passes before reaching your Office 365 account. The Barracuda Email Security Gateway filters out spam and viruses, and then passes the mail on to the Office 365 mail servers. Use the **Inbound Configuration instructions** below to configure.

You can likewise specify the Barracuda Email Security Gateway as the *outbound mail gateway* through which all mail is sent from your domain via your Office 365 account to the recipient. As the outbound gateway, the Barracuda Email Security Gateway processes the mail by filtering out spam and viruses and applying any outbound policies (blocking, encrypting, etc.) before final delivery. In a later section you will configure Office 365 mail servers to pass all outgoing mail from your domain to the Barracuda Email Security Gateway.

Inbound Configuration

To restrict all mail sent to your organization to only that which is sent from the Barracuda Email Security Gateway:

1. Create a connector for MS Exchange in Office 365. You will need the IP address of the Barracuda Email Security Gateway. Once you configure the connector, any Internet mail that does not originate from this IP address range will be rejected by Office 365.
2. Optionally add the requirement for TLS encryption. If you do so, then all mail from your partner organization sent from the IP address or address range you specify must be sent using TLS. Any mail that does not meet this restriction will be rejected.

For further details about configuring Office 365 with connectors, see Microsoft documentation on setting up connectors for secure mail flow with a partner organization.

Initial Setup - Routing Outbound Mail

3.1 Simple configuration of outbound relay of mail

3.1.1 About Scanning Outbound Mail

The Barracuda Email Security Gateway may be configured to scan outgoing mail simultaneously with scanning inbound mail. Virus Scanning and Rate Control are applied to outbound mail as well as the following filters, if specifically enabled, which are configurable from the **BASIC > Spam Checking** and **BLOCK/ACCEPT** pages:

- Spam Scoring, with Block or Quarantine actions
- IP Address Filtering
- Sender Domain Filtering
- Sender Email Address Filtering
- Recipient Filtering
- Content Filtering (Subject, Header and Body)
- Attachment Filtering
- Fingerprint Analysis
- Image Analysis
- Intent Analysis

The following scanning tools are **not** applied to outbound mail:

- SPF (Sender Policy Framework), a sender authentication mechanism
- DKIM (DomainKeys), an email authentication system designed to verify the DNS domain of an email sender
- Regional Settings, the application of special spam analysis rules for particular languages
- Per-user Whitelist/Blocklist
- Per-domain Whitelist/Blocklist
- IP Reputation checks

These are the policies that can be applied to outbound mail using the **BLOCK/ACCEPT** pages:

- Encryption
- Quarantine
- Block
- Redirection

To scan outgoing mail with the Barracuda Email Security Gateway, you must configure outbound operation on the **BASIC > Outbound** page. There you'll specify your trusted outbound mail server IP address or domain name (either your mail server or another trusted relay), identify a Smart host if you have one, and, optionally, an authentication type. The Barracuda Email Security Gateway supports SMTP/SASL authentication and LDAP. If you are relaying though a Smart host, you must also configure the Smart host to send to the Internet.

Be aware that configuring the Barracuda Email Security Gateway to scan outbound as well as inbound mail will increase the load on the system. This should be considered when choosing a Barracuda Email Security Gateway model/size.

When configuring outbound mail, ensure that your network firewall blocks all port 25 traffic that doesn't originate from your Barracuda Email Security Gateway.

3.1.2 How to Route Outbound Mail from the Barracuda Email Security Gatewayl

In most cases, the only thing that needs to be done is to enter the IP address of the outgoing mail server or other trusted relay server in the **Relay Using Trusted IP/Range** field on the **BASIC > Outbound** page, as described in **Simple configuration of outbound relay of mail** below. Outbound mail is scanned for spam, as is inbound mail, as well as filtered for policies you create from the **BLOCK/ACCEPT** filtering pages.

If you need to configure additional options for outbound relay, click the **Help** button on the **BASIC > Outbound** page.

Simple configuration of outbound relay of mail

1. Configure your mail server to relay outbound mail to the Barracuda Email Security Gateway. If you have a Microsoft Exchange Server, enter your Smart host IP address in the next step and configure the Smart host on your mail server to relay outgoing mail to the Barracuda Email Security Gateway.
2. Enter the IP address or host/domain name of your default mail server or another trusted relay server that can relay outbound mail through the Barracuda Email Security Gateway to the Internet. Use the **Relay Using Trusted IP/Range** and/or the **Relay Using Trusted Host/Domain** fields.

To protect your system against domain spoofing, it is strongly recommended to use IP addresses and NOT domain names for specifying Trusted Relays. As such, it is recommended to specify your mail server and/or trusted outbound relay servers in the **Relay Using Trusted IP/Range** field as opposed to specifying a host/domain name.

However, if you are using the **Relay Using Trusted Host/Domain** field, it is recommended to configure either SMTP AUTH or LDAP authentication on this page as well.

Note that LDAP Routing is available on the Barracuda Email Security Gateway 600 and higher, configurable on the **ADVANCED > LDAP Routing** page.

If using your default mail server to relay outbound mail through the Barracuda Email Security Gateway, enter the IP address of your **Destination Mail Server** as specified on the **BASIC > IP Configuration** page or in the **DOMAINS > Manage Domain > BASIC > IP Configuration** page per-domain setting.

3.2 Advanced Outbound Relay Settings

The following steps cover additional options for outbound relay:

1. To configure the Barracuda Email Security Gateway to relay outgoing mail through your normal outbound SMTP host or Smart host to the Internet, enter the IP address or hostname and TCP port in the **Outbound SMTP Host/Smart Host** fields. This is the destination server through which outbound email will be sent from the Barracuda Email Security Gateway for routing to the Internet, and whose IP address will appear in the outgoing mail headers.
2. To enforce using a secure TLS connection to send mail through the Barracuda Email Security Gateway (inbound and outbound) for all domains, set **Force TLS** to **Yes**. SMTP over TLS/SSL defines the SMTP command STARTTLS. This command advertises and negotiates an encrypted channel with the peer for this SMTP connection. This encrypted channel is only used when the peer also supports it.
3. To authenticate senders of outbound email, specify the authentication type in the **Enable SASL/SMTP Authentication** field. (SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based protocols. To use SASL, a protocol includes a command for identifying and authenticating a user to a server and for optionally negotiating protection of subsequent protocol interactions.)
   - **SMTP AUTH Proxy -** SMTP AUTH/SASL authentication enables the SMTP "AUTH" command to authenticate users before allowing them to relay outgoing mail through this Barracuda Email Security Gateway. Either set **Use Destination Mail Server as SMTP AUTH Proxy** to **Yes** or fill in the IP address of another proxy server that is set up to support the SMTP AUTH authentication command (e.g. MS-Exchange or Sendmail) to authenticate senders of outbound mail. To use this authentication method, you must also enable 'Use name and password' or a similar option in your email client. Also, since the password transmits in cleartext, it is recommended to secure transmission by enabling **SMTP over TLS** on the **ADVANCED > Email Protocol** page on the Barracuda Email Security Gateway.
   - **LDAP -** Use your LDAP directory to authenticate senders. Fill in the LDAP settings as described in the **Relay Using Authentication** on the **LDAP** tab.
4. To limit outbound relay capability to certain users or domain names, enter them in the **Senders With Relay Permission** field. To prevent against domain spoofing, it is recommended not to specify sender email address or domain names that can relay outbound mail through the Barracuda Email Security Gateway. Please use this setting only for trusted senders, and note that it is recommended to use one of the sender authentication methods described above as well for added security.

Basic Outbound/Relay Settings

- **Outbound SMTP Host** (Smart host) - The IP address or host name of the destination server through which outbound email will be sent from the Barracuda Email Security Gateway for routing to the Internet, and whose IP address will appear in the outgoing mail headers.
- **Port** - The TCP port of your SMTP host or Smart host through which you want to relay outbound mail.
- **Username** - Only necessary if required for authentication with the SMTP host or Smart host.
- **Password** - Only necessary if required for authentication with the SMTP host or Smart host.
- **Force TLS** - (Optional): Set to Yes if you want to enforce using a secure TLS connection for all mail leaving the Barracuda Email Security Gateway (inbound and outbound). SMTP over TLS/SSL defines the SMTP command STARTTLS. This command advertises and negotiates an encrypted channel with the peer for this SMTP connection. This encrypted channel is only used when the peer also supports it.

To configure relay using authentication and other relay options, click the **Help** button on the **BASIC > Outbound** page.

3.2.1 Advanced Routing of Outbound Mail

If you want outbound email go to through a specific host before final routing to the Internet and/or default MX records, you can specify that SMTP server on the **DOMAINS > Smart Hosts** page.

Example: You might want all emails to gmail.com to go through an additional virus scanning service or cloud-hosted relay service.

3.3 Office 365 for Outbound Mail

Office 365 addresses and user interfaces can change, so please refer to Microsoft documentation for details on configuration. To prepare your Barracuda Email Security Gateway deployment to connect with Office 365, see Microsoft documentation on:

- Setting up connectors to route mail between Office 365 and your own email servers, and
- Prerequisites for your email server environment

You can specify the Barracuda Email Security Gateway as an *inbound mail gateway* through which all incoming mail for your domain passes before reaching your Office 365 account. The Barracuda Email Security Gateway filters out spam and viruses, and then passes the mail on to the Office 365 mail servers.

You can likewise specify the Barracuda Email Security Gateway as the *outbound mail gateway* through which all mail is sent from your domain via your Office 365 account to the recipient. As the outbound gateway, the Barracuda Email Security Gateway processes the mail by filtering out spam and viruses and applying any outbound policies (blocking, encrypting, etc.) before final delivery. By using the configuration described in **Outbound Configuration** below, you instruct the Office 365 mail servers to pass all outgoing mail from your domain to the Barracuda Email Security Gateway.

Outbound Configuration

To restrict all mail leaving your organization to only that which is sent from the Barracuda Email Security Gateway:

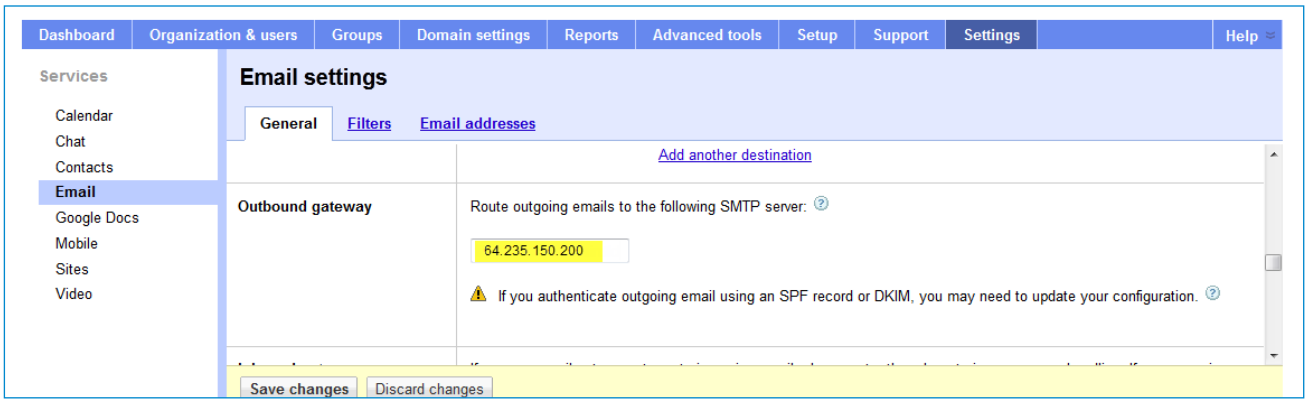
1. Create a connector for MS Exchange in Office 365 for outbound mail. You will need the IP address of the Barracuda Email Security Gateway. Before you set up a new connector, check any connectors that are already listed here for your organization. For more information, see Microsoft documentation on setting up connectors to route mail between Office 365 and your own email servers. The outbound mail gateway will be the IP address of the Barracuda Email Security Gateway.
2. Log into the Barracuda Email Security Gateway web interface as **admin**. Go to the **BASIC > Outbound** page and follow instructions under Simple configuration of outbound relay of mail to configure outbound mail.

3.4 G Suite for Outbound Mail

This section addresses configuring G Suite Business and Education editions with the Barracuda Email Security Gateway as your outbound mail gateway.

Outbound Configuration

1. Navigate to the **Settings** tab and then select **Email** under the **Services** section.
2. Navigate to **Outbound Gateway** and enter the IP address of the Barracuda Email Security Gateway that is the outbound mail gateway.



More information about outbound gateways can be found in Set up an outbound mail gateway in Google documentation.

> G Suite IP Addresses can change so please refer to Google documentation.

Additional settings:

- nslookup -q=TXT _netblocks.google.com 8.8.8.8
- server: google-public-dns-a.google.com
- address: 8.8.8.8
- Non-authoritative answer:

  _netblocks.google.com text =”v=spf1 ip4:216.239.32.0/19ip4:64.233.160.0/19ip4:66.249.80.0/20 ip4:72.14.192.0/18ip4:209.85.128.0/17ip4:66.102.0.0/20ip4:74.125.0.0/16 ip4:64.18.0.0/20ip4:207.126.144.0/20ip4:173.194.0.0/16 ?all”

3.4.1 Configuring the Barracuda Email Security Gateway

1. Navigate to **DOMAINS > Domain Manager** and specify your domain in **New Domain Name**, then click **Add Domain**.
2. Click the **Manage Domain** link and then **BASIC > IP Configuration**. Add the G Suite destination mail servers as follows:

G Suite Destination Mail Server
ASPMX.L.GOOGLE.COM
ALT1.ASPMX.L.GOOGLE.COM
ALT2.ASPMX.L.GOOGLE.COM
ASPMX2.GOOGLEMAIL.COM
ASPMX3.GOOGLEMAIL.COM

Also add the **Destination Server** name/IP address or hostname that receives email after spam and virus scans. It is usually best to use a hostname rather than an IP address so that the destination mail server can be moved and DNS updated at any time without having to make changes to the Barracuda Email Security Gateway configuration.

If you set **Use MX Records** (on the same page) to **Yes**, you must enter a domain name for this field. If multiple servers are specified, then the delimiter used determines the behavior (see below). Note that you can either configure **Use MX Records** for *all* domains from the **BASIC > IP Configuration** page, or you can configure it per-domain from **DOMAINS > Domain Manager > Manage Domains**, then using the **BASIC > IP Configuration** page for the domain you choose to manage. It is *NOT* recommended to set **Use MX Records** to **Yes** to avoid a potential mail loop.

- **Comma** (“,”) or semi-colon (“;”) - Each entry in the list will used in round-robin fashion, with relative weights determined by the number of times a particular entry is listed.
- **Space** (“ “) - Each entry in the list will be treated as a failover list, with an entry being used only if all entries preceding it in the list are unreachable.

For more information about what it means to use MX records, please see the article Using MX Records in Barracuda Campus.

For more details, inbound configuration, and how to configure G Suite to bypass the Barracuda Email Security Gateway for internal Mail, see How to Configure G Suite for Inbound and Outbound Mail.

User Interface – Basic Configuration

4.1 Dashboard

The **BASIC > Dashboard** page provides an overview of the health and performance of your Barracuda Email Security Gateway, including:

- Hourly and daily email statistics that display the number of inbound and outbound messages blocked, tagged (inbound messages only), quarantined, sent (outbound messages only), redirected (outbound messages only), encrypted (outbound only), rate controlled and allowed (inbound only) for the last 24 hours and 28 days.
- The subscription status of Energize Updates.
- Performance statistics, including CPU temperature and system load. Performance statistics displayed in red signify that the value exceeds the normal threshold. These values will fluctuate based on the amount of traffic that is being handled, but if any setting remains consistently in the red for a long period of time, the administrator should contact Barracuda Support.

4.1.1 Product Tips

At the top of the **BASIC > Dashboard** page you'll see the **Product Tips** bubble. This space is populated with usage tips, new programs and features from Barracuda Networks specific to your product, and with a link to the release notes for the latest firmware update. These tips are updated frequently from Barracuda Central.You have the following options in managing this feature:

To hide a particular message permanently, click the **Hide** link.

To hide the Product Tips section of the page, set **Show Product Tips** in the **Product Tips** section of the **BASIC > Administration** page to **No**.

4.1.2 Email Statistics - Inbound

This section of the **BASIC > Dashboard** page summarizes how inbound mail traffic is handled by the Barracuda Email Security Gateway based on how you have configured the system. Actions reported include Blocked, Blocked:Virus, Rate Controlled, Quarantined, Allowed:Tagged and Allowed. Statistics are tallied by hour, by current calendar day starting at midnight, and total since installation (or since the last reset).

If you have not configured any domains for receiving inbound mail on the **DOMAINS** page, and you configure the Barracuda Email Security Gateway only for processing outbound mail, it is possible to see some messages logged as inbound mail traffic. For example, if a message is received addressed to the default domain configured under **BASIC > IP Configuration** page, then the email will be counted as an inbound message.

4.1.3 Email Statistics - Outbound

Outbound mail traffic is summarized in this table on the **BASIC > Dashboard** page much the same way as inbound traffic, except that a count of outbound message Blocked due to custom policy or spam are reported separately, outbound messages are not tagged, and messages counted as Sent are the counterpart of inbound Allowed messages.

If you have not configured the Barracuda Email Security Gateway for outbound mail and only expect inbound mail, it is still possible to see some messages logged as outbound traffic. If a spammer tries to relay a message through the Barracuda Email Security Gateway by spoofing a valid domain as the sender to an invalid recipient, the Barracuda Email Security Gateway will block the message and it will appear in the outbound email statistics table as Blocked.

As an example, consider that mydomain.com is configured as a valid domain on the **DOMAINS** page and badomain.com is not. A spammer sends a message from **sender@mydomain.com** to the IP address of the Barracuda Email Security Gateway, addressed to **recipient@badomain.com**. The message will show as Blocked with a reason of 'invalid domain' in the Message Log and will be included in the outbound mail Blocked statistics.

4.2 Message Log

The **BASIC > Message Log** page displays details about all email traffic that passes through the Barracuda Email Security Gateway. You can view message source and analysis by clicking on a message; you will also see spam scoring for the message and Bayesian analysis, if enabled.

This data is captured initially in the Mail Syslog and appears on the mail facility at the *debug priority level* on the specified syslog server.

- The Message Log stores data for up to 6 months.
- Actual number of messages are allocated 75% of available storage, which includes quarantine messages.
- If your organization needs to access more message log data than 6 months' worth, Barracuda recommends using a syslog server or a Barracuda Message Archiver.

The Message Log is a window into how the current spam and virus settings are filtering email coming through the Barracuda Email Security Gateway, and sorting data using the wide variety of filters can quickly provide a profile of email by allowed, tagged, quarantined or blocked messages by domain, sender, recipient, time, subject, size, reason for action taken or score.

Watch the Message Log after making changes to the spam and virus settings to determine if the Barracuda Email Security Gateway spam checking and quarantine behavior is tuned per the needs of the organization.

4.2.1 Monitor and Classify Incoming Emails

Once email is flowing through the Barracuda Email Security Gateway, the administrator can view the **BASIC > Message Log** page to get an idea of how many messages are being blocked, quarantined, tagged or allowed, with reasons for each of those actions. Reviewing this log will give an idea of how current settings are filtering messages, and the page enables adding or removing message senders to or from the whitelist. For details on filtering messages in the log, click the **Help** button on the **BASIC > Message Log** page.

If you enable Bayesian filtering on the **BASIC > Spam Checking** page, you will then see Spam and Not Spam buttons on the **BASIC > Message Log** page in the tool bar. Use these actions to train the Bayesian database. Bayesian training works only on messages with 11 words or more. With Bayesian filtering enabled, if a message is not classified as spam by the Barracuda Email Security Gateway, but it appears to be spam, you can elect to submit that message to Barracuda Central from the **BASIC > Message Log** page. For best Bayesian accuracy, it is recommended that you reset your Bayesian database every 6 months. Note that Bayesian filtering is turned off by default.

4.2.2 Monitor and Classify Outgoing Emails

If you have configured the Barracuda Email Security Gateway to filter outbound mail, watch the log on the **BASIC > Outbound Quarantine** page. Based on **Outbound Spam Scoring Limits** you specify on the **BASIC > Spam Checking** page, as well as any Block/Accept filters you configure, outbound messages will be quarantined or blocked as needed and listed on the **BASIC > Outbound Quarantine** page. Look for false positives and adjust spam scoring accordingly. Any message listed in the outbound quarantine can be delivered, whitelisted, deleted, or rejected by an administrator.

How to Export the Message Log Entries

The Message Log contents can be exported, but not the actual messages. To export Message Log entries, click the **Export** drop-down and select one of the following:

- **Export Selected** – Save selected lines of the Message Log to a CSV file. First, select the lines you want to export, then select Export Selected from the Export drop-down. You will be prompted for a file name to save to your local desktop or network.
- **Export All** – Save the entire Message Log to a CSV file. You will be prompted for a file name to save to your local desktop or network.

In a clustered environment, the maximum number of lines in a Message Log export is 10,000.

4.3 Spam Checking

4.3.1 How Spam Scoring Works

As a message passes through the last of all of the defense layers, it is scored for spam probability. This score ranges from 0 (definitely not spam) to 10 or higher (definitely spam). Based on this score, the Barracuda Email Security Gateway either tags (inbound messages only), quarantines, blocks or allows (or sends, for outbound) the message.

Once you have more experience with the Barracuda Email Security Gateway, you can adjust how aggressively the system deals with spam. For example, you may decide to tag (inbound only) or quarantine spam instead of blocking it. Details of spam scoring limits for your Barracuda Email Security Gateway are discussed in the Help file on the **BASIC > Spam Checking** page.

On the Barracuda Email Security Gateway 400 or higher you can set the spam scoring values on a per-domain basis, and these scoring values take precedence over the global spam scoring settings. On the Barracuda Email Security Gateway 600 and higher, spam scoring can be set on a per-user basis (inbound only), from the DOMAINS tab.

- **Bayesian Filtering - Optional**

  If you enable Bayesian filtering on the **BASIC > Spam Checking** page, you will then see **Spam** and **Not Spam** buttons on the **BASIC > Message Log** page in the tool bar. Use these actions to train the Bayesian database. Bayesian training works only on messages with 11 words or more. With Bayesian filtering enabled, if a message is not classified as **Spam** by the Barracuda Email Security Gateway, but it appears to be spam, you can elect to submit that message to Barracuda Central from the **BASIC > Message Log** page. For best Bayesian accuracy, it is recommended that you reset your Bayesian database every 6 months. Note that Bayesian filtering is turned off by default.

- **Spam Scoring for Outbound Mail**

  Based on **Outbound Spam Scoring Limits** you specify on the **BASIC > Spam Checking** page, as well as any Block/Accept filters you configure, outbound messages will be quarantined or blocked as needed and listed on the **BASIC > Outbound Quarantine** page. Look for false positives and adjust spam scoring accordingly.

- **Spam and Quarantine Notifications**

  Separate non-delivery notifications (NDR) can be configured to alert the sender when a message is blocked or quarantined due to spam scoring or policy (content filtering).

4.4 Virus Checking

Virus scanning is automatically enabled on the Barracuda Email Security Gateway and the system checks for definition updates on a regular basis (hourly by default). Virus Scanning takes precedence over all other mail scanning techniques and is applied even when mail passes through the Connection Management layers. As such, even email coming from "whitelisted" IP addresses, sender domains, sender email addresses or recipients are scanned for viruses and blocked if a virus is detected.

Use the **BASIC > Virus Checking** page in the web interface to enable or disable virus checking. If you enable Barracuda Real-Time Protection, the Barracuda Email Security Gateway will check unrecognized spam and virus fingerprints against the latest virus threats logged at Barracuda Central that have not yet been downloaded by the Barracuda Email Security Gateway Energize Updates. See the online help on the **BASIC > Virus Checking** page for more details about this setting.

4.4.1 Advanced Threat Protection

The subscription-based **Advanced Threat Protection (ATP) service** analyzes inbound email attachments in a separate, secured cloud environment, detecting new threats and determining whether to block such messages. ATP offers protection against advanced malware, zero-day exploits, and targeted attacks not detected by the Barracuda Email Security Gateway virus scanning features. ATP is available with the Cloud Protection Layer (CPL).

Extended Malware Protection (Available on model 600 and higher)

With version 6.1 and higher, Barracuda offers a subscription to provide additional anti-malware scanning with the Avira virus scan engine. To subscribe, see the Subscription Status section of the **BASIC > Dashboard** page.

4.4.2 Internal Virus Scanning For Your Microsoft Exchange Mail Server

The Barracuda Email Security Gateway offers an add-in that you can download from the web interface and install on your Microsoft Exchange Server to provide internal virus scanning within your network. The **Barracuda Exchange Antivirus Agent** runs as a Windows service on your 2003, 2007 or 2010 MS Exchange Server and works together with MS Exchange to scan internal mail traffic for viruses. Scanning is based on constantly updated virus signatures from the Barracuda Email Security Gateway.

Any time a new virus signature is released, the Barracuda Exchange Antivirus Agent will scan all internal mail traffic for that virus as well as mail previously stored on the server, depending on how you configure settings for the agent. See the **ADVANCED > Exchange Antivirus** page on the Barracuda Email Security Gateway web interface for instructions on downloading and configuring the add-in for your organization's needs.

4.5 Quarantine

4.5.1 Enable or Disable Quarantine?

By default, the Barracuda Email Security Gateway does not quarantine incoming messages, but you may want to enable quarantine if, for example, your organization requires it, or if you want to reduce load on the mail server while giving users a chance to determine what they consider to be "spam" or "not spam". There are three options available for configuring quarantine with the Barracuda Email Security Gateway as described below, with the pros and cons of each.

- **Turn Quarantine off**. Barracuda Networks recommends disabling quarantine unless, for example, your organization has a business requirement to provide quarantine of messages suspected to be spam or you don't want those messages stored on the mail server. Disabling quarantine means less management either by the administrator or by the user and, in the case of per-user quarantine, saves system resources that would otherwise be used to store the messages until the user delivers or deletes them. To disable Quarantine completely:
  - Check the **Disable** check box next to **Quarantine** in the **Spam Scoring Limits** section of the **BASIC > Spam Checking** page
  - Make sure nothing on the **BLOCK/ACCEPT** pages is set to **Quarantine**.
- **Use Global Quarantine**. With global quarantine, messages aren't stored on the Barracuda Email Security Gateway; they are forwarded to a mailbox as designated by the administrator. This saves on data storage. Global quarantine identifies email to quarantine, rewrites the "From" address of the message and sends it to the Quarantine Delivery Address specified on the **BASIC > Quarantine** page. Global quarantine does require some time and effort by the administrator to manage quarantined messages. Enable at the system level or at the domain level.
  - From the **BASIC > Quarantine** page, set the **Quarantine Type** to **Global** and configure settings as described below for global quarantine.
  - From the **BASIC > Spam Checking** page, if you want messages to be quarantined based on score, make sure that the **Disable** check box next to **Quarantine** in the **Spam Scoring Limits** section is NOT checked.
  - Set filters on the **BLOCK/ACCEPT** pages to **Quarantine** per your organization's policies.
  - Enter a **Quarantine Delivery Address** on the **BASIC > Quarantine** page.This mailbox can either be on the mail server that the Barracuda Email Security Gateway protects or a remote mail server. **Note:** If you have a Barracuda Email Security Gateway 400 or above, you can specify the quarantine delivery address on a per-domain basis by going to the **DOMAINS** tab and clicking the **Manage Domains** link, then using the **BASIC > Quarantine** page for that domain to configure the address.

Note that with global quarantine, users will have no control over whitelisting or blocklisting of email addresses, which they do have with per-user quarantine.

- Use *Per-User* Quarantine. Giving users a quarantine inbox gives them greater control over how their messages are quarantined, but also requires them to manage their quarantine inbox on the Barracuda Email Security Gateway. Since per-user quarantine entails storing quarantined messages on the Barracuda Email Security Gateway until the user delivers or deletes, them, you may want to only provide a quarantine inbox to a subset of power users.

  Keep in mind that quarantined email stored on the Barracuda Email Security Gateway requires storage capacity, so system load will vary with the average size of emails.

  If many emails come into your organization include large attachments (as with architecture firms, marketing firms, etc.), the system may push the edge of performance more quickly than if emails tend to be small in size. Use the **Mail/Log Storage** indicator in the **Performance Statistics** pane of the **BASIC > Dashboard** page to monitor disk storage on the Barracuda Email Security Gateway.

As the administrator, you can configure a **Retention Policy** to limit the amount of disk space used for storing each user's quarantined messages, thereby conserving system resources on the Barracuda Email Security Gateway. Alternatively, messages can be scheduled for regular purging based on age and/or size.

4.5.2 Spam Scoring and Quarantine

After a message travels through the initial filtering layers of the Barracuda Email Security Gateway, it is assigned a score based on the probability that it is spam. The administrator can decide how to deal with messages based on the **Spam Scoring** levels (from 0 to 10): allow, tag, quarantine or block, as set on the **BASIC > Spam Checking** page.

- Tagging the message means the user will receive the message in their regular mailbox with the subject text modified to indicate that the message might be spam.
- Quarantining the message means that the message will either be delivered, with the subject text modified to indicate that the message might be spam, to a special "quarantine inbox" assigned to a user or to a "global" quarantine mailbox designated by the administrator.
- Blocking the message means it will not be delivered.

Messages can also be determined to be quarantined (as opposed to allowed, blocked or tagged) by custom policies you set based on domain name, IP address, region, content filters and other filtering tools in the **BLOCK/ACCEPT** pages. **Spam Scoring** and some block/accept policy settings can be further refined at the domain level and/or per-user level, depending on what the administrator enables on the **USERS > User Features** page at the global level and what the **Domain Admin** role enables on the **USERS > User Features** page at the domain level.

4.5.3 Quarantine Notifications

The Barracuda Email Security Gateway can send notifications at predefined intervals and in selected languages to let users know that they have quarantined messages. The notification interval and email address can be set at the global level on the **BASIC > Quarantine** page and overridden at the domain level if allowed by the administrator. Because creating a quarantine digest for each user requires lots of system I/O, it is recommended to set the **Notification Start Time** on the **BASIC > Quarantine** page to outside of peak traffic time frames during the weekday. The default start time is 3:35pm (15:35). Users can override the **Notification Interval** of daily, weekly or never from their **PREFERENCES** tab if enabled by the administrator.

Multiple quarantine notifications can be sent out in a 24 hour period to let users know that they have quarantined mail. Configure this option by entering multiple times for **Notification Start Time**. Note that sending multiple notifications could affect system performance.

If you enable quarantine notifications, be sure to open port 8000 on your firewall (or whatever port you are using for the web interface) if you want the Barracuda Email Security Gateway to send quarantine notifications outside of the network.

4.6 IP Configuration

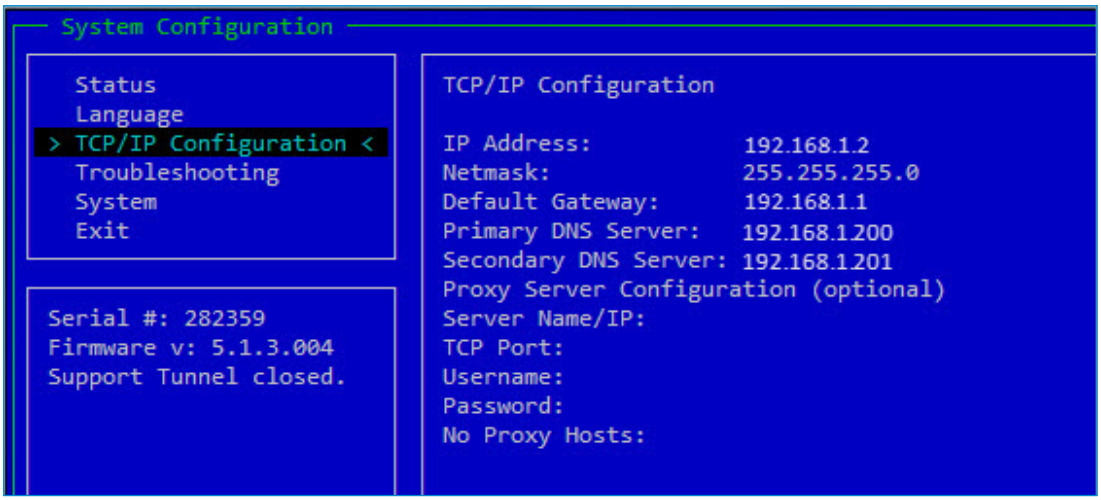
4.6.1 Configure IP Address and Network Settings

The Barracuda Email Security Gateway is given a default IP address of 192.168.200.200. You can change this address by doing either of the following:

- Connect directly to the Barracuda Email Security Gateway with a keyboard and monitor and specify a new IP address through the console interface.
- Log into the Barracuda Email Security Gateway web interface as admin and change the IP address on the **BASIC > IP Configuration** page. See Configure the Barracuda Email Security Gateway From the Web Interface below for details.

To connect directly to the Barracuda Email Security Gateway to set a new IP address:

1. At the **barracuda login** prompt, enter admin for the login and admin for the password. The **User Confirmation Requested** window will display the current IP configuration of the system.



2. Using the Tab key, select **Yes** to change the IP configuration.
3. Enter the new IP address, netmask, and default gateway for your Barracuda Email Security Gateway, and select **OK** when finished.
4. Select **No** when prompted if you want to change the IP configuration. Upon exiting the screen, the new IP address and network settings will be applied to the Barracuda Email Security Gateway.

4.6.2 Configure Your Corporate Firewall

If your Barracuda Email Security Gateway is located behind a corporate firewall, you need to open specific ports to allow communication between the Barracuda Email Security Gateway and remote servers.

To configure your corporate firewall:

1. Using the following table as a reference, open the specified ports on your corporate firewall:

Port	Direction	Protocol	Used for
22	Out	TCP	Remote diagnostics and technical support services (recommended)
25	In/Out	TCP	SMTP
53	Out	TCP/UDP	Domain Name Server (DNS)
80(1)	Out	TCP	Virus, firmware, security and spam rule definitions
123	Out	UDP	NTP (Network Time Protocol)
8000(2) (default)	Out	TCP	Virus, firmware, security and spam rule definitions

(1) If your firewall allows unrestricted outbound traffic on port 80, then no further action is necessary. If there are restrictions on outbound traffic on this port, you must configure your firewall as described in Ports for Firmware and Definition Updates to allow the Barracuda Email Security Gateway access to firmware and definition updates.

(2) If your firewall allows unrestricted outbound traffic on port 8000, then no further action is necessary.

2. If appropriate, change the NAT routing of your corporate firewall to route incoming email to the Barracuda Email Security Gateway. Consult your firewall documentation or your corporate firewall administrator to make the necessary changes.

Configure the Barracuda Email Security Gateway From the Web Interface

1. From a web browser, enter the IP address of the Barracuda Email Security Gateway followed by port 8000.
2. Example: `http://192.168.200.200:8000`
3. Log into the web interface by entering admin for the username and admin for the password. **For maximum security, Barracuda recommends changing the administrator password on the BASIC > Administration** page.
4. On the **BASIC > IP Configuration** page, enter the required information in the fields as described in the following table:

Fields	Description
TCP/IP Configuration	The IP address, subnet mask, and default gateway of your Barracuda Email Security Gateway. The TCP port is the port on which the Barracuda Email Security Gateway receives incoming email. This is usually port 25.
Destination Mail Server TCP/IP Configuration	The hostname or IP address of your destination mail server; for example *mail.yourdomain.com*. This is the mail server that receives email after it has been checked for spam and viruses. You should specify your mail server's hostname rather than its IP address so that the destination mail server can be moved and DNS updated at any time without any changes needed to the Barracuda Email Security Gateway. TCP port is the port on which the destination mail server receives all SMTP traffic such as inbound email. This is usually port 25.
DNS Configuration	The primary and secondary DNS servers you use on your network. It is strongly recommended that you specify a primary and secondary DNS server. Certain features of the Barracuda Email Security Gateway rely on DNS availability.
Domain Configuration	Default Host Name is the host name to be used in the reply address for email messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Email Security Gateway. The Default Host Name is appended to the default domain. Default Domain is a required field and indicates the domain name to be used in the reply address for email messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Email Security Gateway.
Accepted Email Recipients Domains	The domains managed by the Barracuda Email Security Gateway. Make sure this list is complete. The Barracuda Email Security Gateway rejects all incoming messages addressed to domains not in this list. **Note**: One Barracuda Email Security Gateway can support multiple domains and mail servers. If you have multiple mail servers, go to the **DOMAINS** tab and enter the mail server associated with each domain

5. Click **Save**.

If you changed the IP address of your Barracuda Email Security Gateway, you are disconnected from the web interface and will need to log in again using the new IP address.

If you have a model 100:

- Go to the **Users** page and perform at least one of the following:
  - Enter the email address(es) on which the Barracuda Email Security Gateway is to perform spam and virus scanning under **User Configuration**, one entry per line.
  - To have email addresses automatically added to the Barracuda Email Security Gateway as mail arrives, make sure the **Enable User Addition** option is turned on.

Note: If no users are specified, *AND* the **Enable User Addition** option is set to **No**, then no scanning of *ANY* incoming email will be performed.

4.7 Administration

Many of the *initial* settings you should configure on the Barracuda Email Security Gateway are found on the **BASIC > Administration** page. Some of these settings are key for securing the appliance on your network, and many cover general management of the appliance, email notifications and alerts, encryption settings, and monitoring tools such as SNMP and APIs.

Securing the Barracuda Email Security Gateway

To secure your Barracuda Email Security Gateway on the network, configure the following:

- Set a secure password.
- Lock down the user interface ports. Barracuda Networks recommends using the non-standard port 8000 for internal access to the web interface, which is configured with the **Web Interface HTTP Port** setting.
- Limit access to the web interface by IP address with the **Administrator/IP Range** setting as described below.
- Limit IP addresses/networks that are allowed to change configuration information on the Barracuda Email Security Gateway through the Barracuda API, using the **Allowed API IP/Range** setting.

The page contains the following sections:

- Password Change
- Select Time zone
- Default Barracuda Locale
- Administrator IP/Range
- Allowed API IP/Range
- Web Interface Settings
- Message Log Options
- Mail Journaling
- Email Encryption Service
- SNMP Manager
- SNMP Traps
- SNMP Thresholds
- Email Notifications
- Secondary Authorization
- Governance, Risk Management and Compliance (GRC) Account
- Product Tips
- System Management

4.7.1 Password Change

Change the password for the admin user to access the Barracuda Email Security Gateway web interface.

Click **Save Password**.

4.7.2 Time

The current time is automatically updated on the Barracuda Email Security Gateway via Network Time Protocol (NTP). When the Barracuda Email Security Gateway resides behind a firewall, NTP requires port 123 to be opened for outbound UDP traffic.

CAUTION! Changing the Time Zone will cause the Barracuda Email Security Gateway to **REBOOT**.

It is important that the time zone be set correctly on the Barracuda Email Security Gateway. This current time determines the delivery times for messages and appears in certain mail reading programs.

4.7.3 Default Barracuda Locale

Sets the default quarantine message language, except for outbound quarantine when the **Notification Interval** is set to **Immediate**, as configured on the **BASIC > Quarantine** page. Also sets the default encoding for handling unknown character sets during filtering. Note that, for a **Notification Interval** of **Immediate**, outbound quarantine notification language is determined by the **Default Language** setting on the **ADVANCED > Bounce/NDR Settings** page.

4.7.4 Administrator IP/Range

The IP addresses/networks added here are allowed to access the web interface for the Barracuda Email Security Gateway. To best secure the Barracuda Email Security Gateway, limit access to the web interface by IP address with this setting. If no IP address is specified in this field, then ***all*** systems are granted access with the correct administrator password.

Enter a **Netmask** of `255.255.255.255` to specify an individual IP (instead of an entire network).

4.7.5 Allowed API IP/Range

(Available on certain models) The IP addresses/networks listed here are allowed to change configuration information on the Barracuda Email Security Gateway through the Barracuda API. For improved security, specify a password that must be included in all URLs that access the API, in the format `&password=`*`password`*.

See the Barracuda Email Security Gateway API Guide for details on using the Barracuda API.

4.7.6 Web Interface Setting

- **Web Interface HTTP Port** - The web interface is accessed through this port. Changing the value of this setting requires changing the port used to access the interface in the browser. When machines are clustered, this value is **not** synchronized between machines, so all machines must be configured with the same port number.
- **Session Expiration Length** - The amount of time allowed (in minutes) with no activity before a web interface user session expires and the user is required to log in again.

4.7.7 Message Log Options

- **Show Message Body in Message Log** - Set to **Yes** or **No** to enable or disable the feature to view the entire message. For Bayesian learning purposes, the full message should be left visible to help assist in the classification of messages to **Spam** or **Not Spam**.
- **Enable Message Log Retention** - If your organization requires retention of message data or if you want to save the data for creating reports at a later date, set this feature to Yes and also set a value for the **Days to Keep Messages** feature to the maximum number of days to retain the data. If there is no need to retain message log data, set this feature to **No**.

4.7.8 Mail Journaling

- **Destination Email Address** - Email address used to keep a copy of all non-blocked messages sent through the Barracuda Email Security Gateway. The email address you specify for journaling should be reserved only to receive these journaled email copies and not for receiving other types of emails. Note that no message body is available for outbound messages that are encrypted by the Barracuda Email Security Gateway.

  To send to a domain that is just an IP address, the IP address must be placed inside square brackets. For example, to journal to a Barracuda Message Archiver located in your internal network at 192.168.2.4, the exact text to enter will be:

  ```
  archiver@[192.168.2.4]
  ```
- **Bounce Address** - Email address to which email messages will be sent that the Barracuda Email Security Gateway could not deliver to the journal account - either because the receiving server for the **Destination Email Address** was unavailable or because the server refused the message. The bounce message will never be sent to the original sender.
- **Do Not Journal Per-User Quarantined Email** - If you have entered a **Destination Email Address**, then setting to **Yes** means that, if **Quarantine Type** on the **BASIC > Quarantine** page is set to **Per-User**, messages arriving in per-user quarantine inboxes will not be journaled at that time. If, however, the quarantined message is then manually delivered from the **BASIC > Message Log** or from the user's quarantine inbox, the message will then be journaled.

4.7.9 Email Encryption Service

Email encryption protects private, sensitive and valuable information for entities such as health care providers or governmental agencies that is communicated via email. To encrypt outbound email based on policy you set in the BLOCK/ACCEPT pages, select the **Encrypt** action for outbound filters on those pages.

You must first do the following:

1. From the **DOMAINS > Domain Manager** page, click **Validate** for each domain from which you want to send encrypted messages. You will be presented with several options for validation.
2. Configure encryption at the domain level using the **DOMAINS > Domain Manager > Manage Domain > ADVANCED > Encryption** page for each domain from which you want to encrypt outbound email.

Use the following fields to prepare for using the encryption feature for outbound email:

- **Valid Test Email Address** - To test connection with the Barracuda Email Encryption Service, enter a valid test email address and click the **Test Encryption Connection** button.
- **Barracuda Message Archiver** - Enter the IP address of your Barracuda Message Archiver to enable archiving of encrypted email, as well as replies to those emails.

  Port 4234 should be open for transmission of encrypted mail to the Barracuda Message Archiver.

- **Queue Encrypted Mail** - If set to **Yes**, messages that match encryption policy, but are sent from domains that have not yet been validated for encryption, will be queued. These messages can be viewed on the **ADVANCED > Queue Management** page. If the domain is not validated, the message will not be encrypted or delivered. Please see the **ADVANCED > Queue Management** page for details. If this setting is **No**, and the domain is not validated, messages will eventually be delivered unencrypted, bypassing encryption policy.
- **Sender Email Address/Domain Exemptions** - Senders you list here will be exempt from all encryption policies.
- **Recipient Email Address/Domain Exemptions** - Recipients you list here will be exempt from all encryption policies.

4.7.10 SNMP Manager

(Available on certain models) Settings for SNMP access between the Barracuda Email Security Gateway and an SNMP monitor or some other program for querying system information or trapping performance data. For details on using the Barracuda SNMP agent, see Barracuda Campus documentation.

- **Enable SNMP Agent** - Allows the Barracuda Email Security Gateway to accept and respond to SNMP queries.
- **SNMP Version** - Version of SNMP to be used by the Barracuda Email Security Gateway. **v3** is the recommended setting as it is more secure.
  - **v2c** - Allows open access to your SNMP traffic.

- **SNMP Community String** - The community string, or password, used to define (authenticate) SNMP access. The default community string used by the Barracuda Email Security Gateway to communicate SNMP information is **cudaSNMP**.

- **v3** - Encrypts SNMP traffic and limits access to only password-authenticated users. ***Recommended***.
  - **User** - A name to be used for authenticating SNMP v3 queries. An actual user account with this name need not exist on the Barracuda Email Security Gateway.
  - **Password** - The password to be used for the above account. Must be at least 12 characters long.
  - **Authentication Method** - The authentication method supported by your SNMP monitor. **SHA** is the more secure method.
  - **Encryption Method** - The encryption method supported by your SNMP monitor. **AES** is the more secure method.

- **Allowed SNMP IP/Range** - The only IP address(es) allowed to connect to the Barracuda Email Security Gateway via SNMP. If no IP addresses or networks are specified here, then SNMP access will be possible from **any** system.

You can access SNMP MIBs from Barracuda Campus documentation to use to monitor objects either from custom scripts or from your SNMP monitor.

4.7.11 SNMP Traps

Enter the IP address(es) of your SNMP monitor server(s) to which you want the Barracuda Email Security Gateway to send SNMP traps. The default port is **162**. Note that you MUST set **Send SNMP/Email Notifications** in the **Email Notifications** section of the page to **Yes** to enable sending traps.

4.7.12 SNMP Thresholds

If you wish to use SNMP traps and have configured one or more SNMP Trap IP addresses above, you can enable any of the following three traps:

- **SNMP In Queue Threshold** - Send a trap if the number of messages in the incoming queue exceeds this value.
- **SNMP Out Queue Threshold** - Send a trap if the number of messages in the outbound queue exceeds this value.
- **SNMP Notify Queue Threshold** - Send a trap if the number of messages in the notify queue exceeds this value.

4.7.13 Email Notifications

- **System Alerts Email Address** - The email address to which the Barracuda Email Security Gateway should send automated alerts, including LDAP (available on model 300 and higher) lookup or server errors and automated backup failures. Multiple addresses in a list should be separated with commas.

- **System Contact Email Address** - The email address to which Barracuda Central should send additional information about security bulletins and customer service issues. Multiple addresses in a list should be separated with commas. The contents of this field are transmitted to Barracuda Central.
- **Send SNMP/Email Notifications** - Select **Yes** to enable the Barracuda Email Security Gateway to send notifications to the **System Alerts Email Address** via SNMP for these conditions:
  - The inbound message queue size exceeds normal thresholds
  - The outbound message queue size exceeds normal thresholds
  - The average latency exceeds normal thresholds
  - Problem with RAID disk storage

4.7.14 Secondary Authorization

To protect email privacy, you can enable this feature to require a password before the **Admin, Domain Admin** or **Helpdesk** roles can view entries or email message contents (although the Helpdesk role can only view message entries, not contents) in message lists (logs) across the system. This includes: the global Message Log, per-domain Message Logs, queue management, outbound quarantine and quarantine inboxes. The **GRC** account can also be limited to only seeing message entries but not message contents when monitoring the outbound quarantine. For more information on the **GRC** role, see the **Governance, Risk Management and Compliance (GRC) Account** section in this page. Email privacy options include:

- **Enable Secondary Authorization** - Require a password for the **Admin, Domain Admin** or **Helpdesk** roles to view entries or email contents (except **Helpdesk** role) in logs per above, subject to the following settings.
- **Enable Privacy For** -
  - **Message Lists** - Selecting this option means that the indicated roles cannot view the entries in any logs as listed above unless the password you create here is entered.
  - **Message Content** - Selecting this option enables the indicated roles to view the entries in any logs as listed above, but does not allow the viewing of message contents unless the password you create here is entered. The **Helpdesk** role cannot view message contents.

CAUTION! The password must be re-entered every time a setting for this feature is changed. If the password is lost, you must contact Barracuda Networks Technical Support. Once the password is entered, it is active for 10 minutes, at which point the password must be re-entered for the session.

- **Include Privacy for GRC** - If you set this option to **Yes**, the same password protection applies to the **GRC** role, so that the **GRC** can view message entries in the Outbound Quarantine, but not message contents.
- **New Secondary Authorization Password** - Use to change the password as described above, and then enter the password again in the **Re-enter New Password** field.

4.7.15 Governance, Risk Management and Compliance (GRC) Account

The **GRC** role is used as a way to provide governance, risk management and compliance to email content. **This account always exists on the Barracuda Email Security Gateway, but must be enabled to be active.** The administrator can enable or disable the GRC account at any time. The GRC account only has access to **Outbound Quarantine** logs and has the job of reviewing the messages in the log, determining which ones can be delivered based on policy. The GRC can take the following actions with outbound quarantined messages:

- **Deliver** - GRC determines that the message is allowed, per policy, and clicks the **Deliver** button.
- **Reject** - GRC determines that the message is not allowed for delivery, per policy, and clicks the **Reject** button. If the admin user has configured it on the **ADVANCED > Bounce/NDR Settings** page, this action sends a bounce message to the sender in addition to deleting the message.
- **Delete** - GRC determines that the message is not allowed to be sent and clicks the **Delete** button. The message will then be removed from the Outbound Quarantine log.

When the GRC logs in, only two pages are visible in the web interface: the **Outbound Quarantine** page and a **Password** page. From the Password page, the GRC can change the current GRC password.

See Secondary Authorization on the previous page to enable email contents privacy, requiring a password before the **GRC** role can view message entries or contents in the **Outbound Quarantine.**

4.7.16 Product Tips

The top of the **BASIC > Dashboard** page displays, by default, a **Product Tips** section to alert you about usage tips, new features and programs from Barracuda Networks that are specific to your Barracuda Networks product. After reading a tip, clicking the **Hide** link will remove the specific product tip from the list.

Also included in the **Product Tips** is a link to the latest release notes if you have not read them since the last firmware update. If you close Product Tips by clicking the X in the upper right corner, it will reappear when you refresh the page. To disable the Product Tips, set **Show Product Tips** to **No**.

4.7.17 System Management

CAUTION! Use of these controls may cause interruptions in email delivery.

- **Clear Statistics** - Clears both inbound and outbound statistical data used to populate charts and tables on the **BASIC > Dashboard** page based on messages received up until now. The message log remains intact, however, and future messages received will be used to create new statistical data.
- **Clear Inbound Statistics** - Clears ONLY inbound statistical data used to populate charts and tables on the **BASIC > Dashboard** page based on inbound messages received up until now. The message log remains intact, however, and future messages received will be used to create new statistical data.
- **Clear Outbound Statistics** - Clears ONLY Outbound statistical data used to populate charts and tables on the **BASIC > Dashboard** page based on outbound messages received up until now. The message log remains intact, however, and future messages received will be used to create new statistical data.
- **Clear Message Log** - Clears all messages out of the message log. This will not clear the Bayesian Database. It may take several minutes to fully purge the messages from the drive (anywhere from 2 hours to 4 days is possible depending on the size of the Message Log). During this time, disk usage may or may not drop at a noticeable rate.

Important: DO NOT use this functionality to free space on the drive unless no further email is flowing in. In many cases, email will arrive faster than it is purged, thus negating the clearing of the Message Log for space reasons.

- **Shutdown** - Shuts down and powers off the unit.
- **Restart** - Reboots the unit.
- **Online/Offline** - Puts the unit into online/offline mode. A unit in offline (maintenance) mode will stop accepting incoming email until it is put back online.

IMPORTANT: Take the Barracuda Email Security Gateway OFFLINE before doing a firmware upgrade. This will ensure that the inbound queue is emptied and all incoming messages are scanned and routed before the upgrade process begins.

- **Reload** - Reapplies the system configuration.

- **Retry** - For email that is waiting in the **Out** queue. Clicking **Retry** will initiate the process to retry sending the messages immediately. The button will then be disabled until the requeue process has completed. See the **ADVANCED > Queue Management** page to view either the inbound or outbound message queue and for details on the outbound queue process.

Single Sign-On is a per-domain setting available on the Barracuda Email Security Gateway 400 and higher.

4.8 Outbound

Outbound mail through the Barracuda Email Security Gateway is subject to the same spam and virus scanning and, for the most part, the same custom policy as inbound mail with some exceptions. The following scanning tools are ***not*** applied to outbound mail:

- IP Reputation, a sender authentication mechanism
- SPF (Sender Policy Framework), a sender authentication mechanism
- DKIM (DomainKeys), an email authentication system designed to verify the DNS domain of an email sender
- Per-user Whitelist/Blocklist
- Per-domain Whitelist/Blocklist

4.8.1 How to relay outbound mail to the Barracuda Email Security Gateway

In most cases, the only thing that needs to be done is to enter the IP address of the outgoing mail server or other trusted relay server in the Relay Using Trusted IP/Range field on this page per Simple configuration of outbound relay of mail described below.

How to Filter Outbound Mail:

With this configuration, outbound mail will only undergo virus scanning and rate control. To apply custom policy to outbound mail, use the **BLOCK/ACCEPT** filtering pages and select **Outbound** for desired filters.

If you need to configure additional options for outbound relay, those are outlined following **Simple configuration** of outbound relay of mail below. Following the additional options are explanations of each section on the page:

- Basic Outbound/Relay Settings
- Relay Using Authentication
- Relay Using Trusted IP/Range
- Relay Using Trusted Host/Domain
- Senders with Relay Permission

Simple configuration of outbound relay of mail:

1. Configure your mail server to relay outbound mail to the Barracuda Email Security Gateway. If you have a Microsoft Exchange Server, enter your Smart host IP address in the next step and configure the Smart host on your mail server to relay outgoing mail to the Barracuda Email Security Gateway.

2. Enter the IP address or host/domain name of your default mail server or another trusted relay server that can relay outbound mail through the Barracuda Email Security Gateway to the Internet. Use the **Relay Using Trusted IP/Range** and/or the **Relay Using Trusted Host/Domain** fields.

WARNING: To protect your system against domain spoofing, it is strongly recommended to use IP addresses and NOT domain names for specifying Trusted Relays. As such, it is recommended to specify your mail server and/or trusted outbound relay servers in the **Relay Using Trusted IP/Range** field as opposed to specifying a host/domain name.

However, if you are using the **Relay Using Trusted Host/Domain** field, it is recommended to configure either SMTP AUTH or LDAP authentication on this page as well. LDAP Routing is available on the Barracuda Email Security Gateway 600 and higher, configurable on the **ADVANCED > LDAP Routing** page.

If using your default mail server to relay outbound mail through the Barracuda, enter the IP address of your Destination Mail Server as specified on the **BASIC > IP Configuration** page or in the **DOMAINS > Manage Domain > BASIC > IP Configuration** page per-domain setting.

Additional options for outbound relay: (all optional)

3. To configure the Barracuda Email Security Gateway to relay outgoing mail through your normal outbound SMTP host or Smart host to the Internet, set the values in the **Basic Outbound/Relay Settings** section as described below.
4. To authenticate senders of outbound email, specify the authentication type in the SASL/SMTP Authentication field. (SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based protocols. To use SASL, a protocol includes a command for identifying and authenticating a user to a server and for optionally negotiating protection of subsequent protocol interactions.)
   - **SMTP AUTH Proxy** - SMTP AUTH/SASL authentication enables the SMTP "AUTH" command to authenticate users before allowing them to relay outgoing mail through this Barracuda Email Security Gateway. Either set **Use Destination Mail Server as SMTP AUTH Proxy** to **Yes** or fill in the IP address of another proxy server that is set up to support the SMTP AUTH command (e.g. MS-Exchange or Sendmail) to authenticate senders of outbound mail. To use this authentication method, you must also enable 'Use name and password' or a similar option in your email client. Also, since the password transmits in cleartext, it is recommended to secure transmission by enabling **SMTP over TLS** on the **ADVANCED > Email Protocol** page on the Barracuda Email Security Gateway.
   - **LDAP** - Use your LDAP directory to authenticate senders. Fill in the LDAP settings as described below.
5. To limit outbound relay capability to certain users or domain names, enter them in the **Senders With Relay Permission** field.

WARNING: To prevent against domain spoofing, it is recommended not to specify sender email address or domain names that can relay outbound mail through the Barracuda Email Security Gateway. Use this setting ONLY for trusted senders, and note that it is recommended to use one of the sender authentication methods described above as well for added security.

Basic Outbound/Relay Settings

- **Outbound SMTP Host (Smart Host)** - IP address or host name of the destination server through which outbound email will be sent from the Barracuda Email Security Gateway for routing to the Internet, and whose IP address will appear in the outgoing mail headers.
- **Port** - The TCP port of your SMTP host or Smart host through which you want to relay outbound mail.
- **Username** - Only necessary if required for authentication with the SMTP host or Smart host.
- **Password** - Only necessary if required for authentication with the SMTP host or Smart host.
- **Force TLS** - (Optional): Set to Yes if you want to enforce using a secure TLS connection for all outbound mail. SMTP over TLS/SSL defines the SMTP command STARTTLS. This command advertises and negotiates an encrypted channel with the peer for this SMTP connection. This encrypted channel is ONLY used when the peer also supports it. Outbound mail will not be sent if it is not supported.

4.8.2 Relay Using Authentication

SASL/SMTP Authentication - Select an authentication type of *SMTP AUTH Proxy, LDAP,* or none *(Off)*. If you're specifying **Relay Using Trusted Host/Domain** or if you're specifying **Senders with Relay Permission** below, it is recommended that you use authentication as well to prevent domain spoofing. **Barracuda Networks strongly recommends against specifying either Relay Using Trusted Host/Domain or Senders with Relay Permission.**

- **SMTP AUTH Proxy** - Click on this tab to configure SMTP AUTH:
  - **Use Destination Mail Server as SMTP AUTH Proxy** - If you are using SMTP AUTH via the **Destination Mail Server** configured on the **BASIC > IP Configuration** page, select **Yes**. To use a different server as an SMTP AUTH proxy, enter the IP address and TCP **Port** here for the server and make sure that the server is set up to support the SMTP AUTH command (e.g. MS-Exchange or Sendmail).
- **LDAP** - Click on this tab and use the following settings to connect to your LDAP server:
  - **LDAP Server** - Hostname or IP address of your LDAP or Active Directory server.
    For example: ldap05.barracudanetworks.com
  - **LDAP Port** - Port for LDAP or Active Directory server. For example: 389

- **LDAP/Exchange Username** - Distinguished Name (DN) of a user in your directory that has read access to all information about valid users. This is the LDAP/Exchange Username under which LDAP queries will be performed. Some examples:
  - `CN=admin`
  - `OU=Unix Users`
  - `OU=CD USERS`
  - `DC=Cudadev`
  - `DC=local`
- **LDAP/Exchange Password** - Password for the user specified above.
- **LDAP Filter** - List of attributes to check during account verification. For example: `(samaccountname=%u)`
- **LDAP Search Base** - Base DN for your directory. For example, if your domain is test.com, your Base DN might be `dc=test,dc=com`.

- **Only allow SMTP AUTH with TLS** - If Yes, the Barracuda Email Security Gateway will only advertise and use SMTP AUTH when the mail client is using SMTP over a TLS connection. To use this setting, you must first configure SMTP over TLS on the **ADVANCED > Email Protocol** page.

4.8.3 Relay Using Trusted IP/Range

Be sure to exempt all trusted IP address(es) entered here from Rate Control. In the **Rate Control Exemption IP/Range** field on the **BLOCK/ACCEPT > Rate Control** page, enter all IP addresses you've entered here as trusted relays.

- **IP/Network address** - IP address of an outbound mail server or other trusted source that can relay outgoing mail to the Barracuda Email Security Gateway for routing to the Internet. This will either be your default mail server, which is specified on the **BASIC > IP Configuration** page in the Destination Mail Server TCP/IP Configuration section (global setting) or on the **DOMAINS > Manage Domain > BASIC > IP Configuration** page (per-domain setting), or another trusted relay server in your network.
- **Netmask** - Netmask or subnet of your default mail server and/or other trusted outbound relay servers.
- **Comment** - Optional note about the server specified.

4.8.4 Relay Using Trusted Host/Domain

- **Host/Domain Name** - Enter the host name or domain name of an outbound mail server or other trusted source that can relay outgoing mail to the Barracuda Email Security Gateway for routing to the Internet.

To prevent against domain spoofing, it is strongly recommended to specify trusted outbound relays ONLY by IP address (using **Relay Using Trusted IP/Range**), if possible, rather than by domain name. If using this setting, it is recommended to use sender authentication as well.

4.8.5 Senders with Relay Permission

- **Sender Email/Domain** - To limit permission to certain users or domains to relay outbound mail through the Barracuda Email Security Gateway, enter those email addresses and/or domain names here.

To prevent against domain spoofing, it is strongly recommended to specify trusted outbound relays ONLY by IP address (using **Relay Using Trusted IP/Range**), if possible, rather than by domain name. If using this setting, it is recommended to use sender authentication as well.

4.9 Outbound Quarantine

For outbound mail, there is no per-user quarantine mechanism on the Barracuda Email Security Gateway as there is with inbound mail. Messages that meet or exceed the scoring level you set on the **BASIC > Spam Checking** page for the quarantine of outbound messages, and messages that violate outbound policies you have configured on various **BLOCK/ ACCEPT** pages will be placed in outbound quarantine for the system.

These messages are logged and can be viewed on the **BASIC > Outbound Quarantine** page. At the domain level, messages in outbound quarantine can be viewed and managed by domain under **DOMAINS > Manage Domain > OUTBOUND QUARANTINE > Outbound Quarantine**.

Configure outbound quarantine settings discussed here from the **BASIC > Quarantine** page.

Immediate notifications can be sent to the administrator via the specified **Notification Address** whenever an outbound message is placed into quarantine. As with inbound quarantine notifications, a quarantine summary can be sent on a daily or weekly basis, if at all.

An **Age Retention Policy** can be specified for outbound mail, indicating when "old" quarantined outbound messages should be removed from the Barracuda Email Security Gateway. Use this option together with the **Size Limit** (KB) and **Size Retention Policy** to limit the amount of disk space allotted on the Barracuda Email Security Gateway for storing quarantined outbound mail. Regardless of these settings, quarantined outbound messages are always retained for at least 3 days.

4.10 Reports

4.10.1 Generate System Reports

The Barracuda Email Security Gateway has a variety of system reports that can help you keep track of such statistics as the top spam senders and the top viruses detected by the system.

Reports can be created for data collected at the global level as well as at the per-domain level. You can run reports and configure report settings from the **BASIC > Reports** page, and online help for that page includes:

- a table listing all reports
- the kind of data each report includes for inbound and/or outbound mail
- types of graphs available

You can either generate a system report on demand, or schedule reports for regular delivery to specific users.

4.10.2 On-demand or Emailed reports?

On demand reports can cover data for a specified date range, but generating a report to *view* instead of to *send as an email* can potentially consume excessive system resources on the Barracuda Email Security Gateway. For this reason, to minimize impact of report generation on the Barracuda Email Security Gateway performance, reports of over 7 days in length can only be generated through email.

4.10.3 Automate the Delivery of Scheduled System Reports

The **Reporting Email Options** section of the **BASIC > Reporting** page lets you configure the Barracuda Email Security Gateway to automatically deliver system reports daily, weekly or monthly to specific users by entering their email addresses in the field next to each report type.

You can enter as many email addresses as you like for each report as long as each address is separated by a comma. If you do not want a daily report to be distributed, do not enter an email address next to that report type.

Each scheduled report covers traffic for the selected **Date Range** and **Start** and **End** times, and can be automatically generated either *Daily*, *Weekly* or *Monthly*. The **Traffic Summary** report is a good status reporting tool, and having it emailed to your mail box every day is helpful for monitoring the system.

4.10.4 Report Format Options

Report output format options include HTML, PDF, and Text.

5.1 IP Reputation

External IP blocklists, also known as DNSBLs or RBLs, are lists of Internet addresses that have been identified as potential originators of spam. These lists can be used to block potential spammers from sending mail into the network. External IP blocklists are efficient and an important part of the spam blocking process. Using RBLs increases the effectiveness and message handling capacity of the Barracuda Email Security Gateway. IP Reputation checks are only performed on *inbound* email traffic.

Configure the following settings on the **BLOCK/ACCEPT > IP Reputation** page.

Warning: Use of any blocklist may occasionally generate "false positives" (legitimate messages that are blocked). The blocklists that are enabled by default contain little or no false positives for most users.

5.1.1 Barracuda Reputation

Barracuda Reputation is maintained by Barracuda Central and includes a list of IP addresses of known, good senders as well as known spammers. Updates to the Barracuda Reputation database are delivered to the Barracuda Email Security Gateway via Barracuda Energize Updates. There are two parts to the Barracuda Reputation controls:

- **Barracuda Reputation Blocklist (BRBL)** - The BRBL is a database of IP addresses that have been manually verified to be a noted source of spam. Incoming connection requests from IP addresses on this list are terminated, and no information about the incoming message (other than the originating IP address) is kept. Checks are made against the BRBL prior to any other external IP blocklists, and can only be overridden by the following:
  - any whitelists configured by the admin or an end-user;
  - any IP address in the **Barracuda Reputation, External RBL IP Exemption Range** list configured below.

It is *strongly* recommended that the BRBL option be set to ***Block***.

- **Email Categorization** - This feature allows administrators more control over what they believe to be spam, even though those messages may not meet the technical definition of spam. Emails that originate from Barracuda-verified sources (including what was formerly known as the Barracuda Reputation Whitelist) are categorized into one of the following Categories based on the sending domain name and IP address:
  - **Transactional Emails** - Emails related to a specific transaction or order, and automated notifications. Includes order and delivery confirmations and notices; bills and invoices; bank statements; account update notices. This category should always be set to ***Whitelist*** to ensure that critical emails are allowed through.

- **Mailing Lists** - Mailing lists and newsgroups for special interest groups such as Google and Yahoo Groups. Recommended **Action**: *Whitelist*.
- **Corporate Emails** - Emails sent from an authenticated organization's Barracuda-verified mail server. Meant for general corporate communications only. This category should always be set to ***Whitelist*** to ensure that business emails are allowed through.
- **Marketing Materials** - Promotional emails and newsletters from companies such as Constant Contact. Recommended **Action**: *Off*.
- **Social Media** - Social media notifications from sites such as Facebook, LinkedIn and Twitter. Recommended **Action**: *Whitelist*.

The administrator can specify an **Action** to take on messages in that Category, or set the Action to **Off** in order to use all other spam scanning measures and processes that determine the action to take. A message may fall into multiple Email Categories, each of which can be associated with a different **Action**. In these situations, the action with the higher precedence will be taken on that message, as listed below in descending order of precedence:

- **Whitelist** - Deliver the message.
- **Block** - Do not deliver the message. The complete contents can still be viewed from the Message Log.
- **Quarantine** - Put the message into quarantine.
- **Tag** - Prepend the Subject line of the message with the Category's **Subject Tag**, and deliver the message.
- **Off** - Do not take any action based on this categorization, and continue with all other spam scanning and processing measures.

Messages that are categorized by this feature will bypass Rate Control checks.

5.1.2 Custom External RBLs

You can add any additional free or subscription blocklists. Change the selected action for a blocklist by selecting the desired action and clicking **Save**.

5.1.3 RBL Options

Submit RBL Exemptions to Barracuda Central - Send your list of RBL Exempt IP addresses to Barracuda Central.

5.1.4 Barracuda Reputation, External RBL IP Exemption Range

Enter a list of individual and/or ranges of IP addresses that may be on an RBL, but from which you want to accept messages anyway. Incoming connection requests from these IP addresses bypass RBL scanning. Messages from these addresses are subject to all other spam scanning techniques. In comparison, messages from the Allowed IP/Range of addresses specified on the **BLOCK/ACCEPT > IP Filters** page are subject only to virus scanning checks.

Senders of messages categorized by the Email Categorization feature cannot be exempted. They will still be subject to Barracuda Reputation and External RBL checks even if their sending IP address is listed here.

5.2 Rate Control

The Rate Control mechanism, configured on the **BLOCK/ACCEPT > Rate Control** page, counts the number of connections to the Barracuda Email Security Gateway in a half hour period. The threshold set is the maximum number of connections allowed from any one IP address, for both inbound and outbound traffic, in this half-hour time frame. If the number of connections from a single IP address exceeds the specified threshold, the Barracuda Email Security Gateway will defer any further connection attempts from that particular IP address until the next time frame. Deferred connections will be logged as such in the Message Log with the **Reason** listed as ***Rate Control***.

Common setting is for 20-30 emails/ half hour, but if you have high volume recipients in your network, you may need to set at 50 or higher.

After modifying the Rate Control configuration, five (5) or more unique IP addresses must connect within 30 minutes before Rate Control will take effect.

5.2.1 Rate Control Exemption IP/Range

You can specify any IP address or IP range to exclude from IP-based Rate Control. Only Rate Control is bypassed. Email messages are still scanned for spam and virus content.

5.2.2 Sender Based Rate Control

You can set a **Maximum Recipients Per Sender / 30 Minutes for Sender Based Rate Control**. You can also specify senders you want to exempt from **Rate Control** in the **Rate Control Exemption Sender Email Address** (Outbound Only) text box.

Rate Control based on sender email address, applicable only to outbound email, works as follows:

If the number of outbound recipients from a single (sender) email address exceeds the specified **Maximum recipients per Sender / 30 minutes** threshold, the Barracuda Email Security Gateway will defer any further connection attempts from that particular sender until the next time frame. Deferred outbound connections will be logged as such in the Message Log with the **Reason** listed as *Rate Control*.

5.3 IP Filters

Use the **BLOCK/ACCEPT > IP Filters** page to whitelist or block specific IP addresses or ranges of IP addresses.

5.3.1 Whitelisting IP/Ranges

Whitelisted IP addresses/networks bypass spam scoring as well as all other Blocklists. Virus scanning still applies. Use the **Allowed IP/Ranges** section of the page for whitelisting.

An IP whitelist is one of two ways to bypass IP Reputation Blocklists. The other way is to add an entry to the Barracuda Reputation, External RBL IP Exemption Range on the **BLOCK/ACCEPT > IP Reputation** page. Messages accepted from RBL Exemption addresses are subject to the complete set of spam scoring algorithms.

5.3.2 Blocking IP/Ranges

Use the Blocked IP/Range section of the page to add IP addresses or networks that you want to block, tag or quarantine.

Note that outbound messages are never tagged.

All whitelists take precedence over blocked IP addresses/networks. The action taken for blocked IP addresses can be specified by selecting the proper option (available options include: block, quarantine or tag).

- The tag or quarantine action may still result in a block if another spam filtering layer detects it as spam, or it matches against a blocklist.
- The Blocked IP/Ranges list takes precedence over the **Barracuda Reputation, External RBL IP Exemption Range** on the **BLOCK/ACCEPT > IP Reputation** page.

5.4 Sender Filters

5.4.1 Allowed Email Addresses and Domains

Organizations can define their own allowed sender domains or email addresses for sender authentication using the **BLOCK/ACCEPT > Sender Filters** page, but the safest way to indicate valid senders on the Barracuda Email Security Gateway is to whitelist (allow) the IP addresses of trusted email servers on the **BLOCK/ACCEPT > IP Filters** page, then blocklist (block, quarantine or tag) their domain names on the **BLOCK/ACCEPT > Sender Filters** page to prevent domain name spoofing.

Sender filters are checked against the following headers:

- For global settings (this page): "envelope from"
- For per-domain settings: "envelope from"
- For per-user settings: "envelope from", "header from", and "reply-to" fields

Messages from whitelisted senders bypass:

- spam scoring
- intent analysis
- Bayesian filtering
- keyword filters

Virus scanning and rate control are still applied.

5.4.2 Blocked Email Addresses and Domains

Add any domains, subdomains, and/or email senders from which you wish to block, tag or quarantine messages. Blocking a domain automatically blocks all subdomains.

Valid entries for the Email Address/Domain fields:

- domains
- individual email addresses
- TLDs (top level domains)

Blocklisting email addresses is not recommended. This is due to the fact that spammers rarely, if ever, use the same sender email address more than once. Consequently, adding such email addresses to a blocklist could eventually increase unnecessary load on the Barracuda Email Security Gateway as it compares sender email addresses to an ever-growing blocklist that may be of no value.

5.4.3 Encrypted Sender Addresses and Domains (Outbound Only)

Add any domains, subdomains, and/or email senders for which outbound messages should always be encrypted. Valid entries for the Email Address/Domain fields are as described on the previous page.

BEFORE using encryption, you must validate the sending domain and complete encryption configuration. See the **DOMAINS > Manage Domain > ADVANCED > Encryption** page. Also note that this list will be overridden by a list of any domains and email addresses that you enter in the Sender Email Address/Domain Exemptions field on the **BASIC > Administration** page.

5.4.4 Redirected Sender Addresses and Domains (Outbound Only)

If you want to redirect email from certain senders, domains or subdomains to another gateway, add those email addresses, domains or subdomains to the **Redirected Sender Addresses and Domains** section of the page.

If you are using an email encryption service, add any email addresses, domains or subdomains for which you want to redirect outbound messages for encryption. You must specify the IP address of the server or service in the **Redirection Mail Server TCP/IP Configuration** section of the **BASIC > IP Configuration** page.

If you want to relay outbound messages through an alternate mail server to the Destination Mail Server specified on the **BASIC > IP Configuration** page, you can specify a Redirection Mail Server on that page.

Valid entries for the **Email Address/Domain** fields are as described on the previous page.

5.5 Sender Authentication

Sender Authentication is a key feature of the Barracuda Email Security Gateway for protecting your network and users from spammers who might "spoof" a domain or otherwise hide the identity of the true sender. The following techniques are used to verify the "from" address of a message.

5.5.1 Sender Policy Framework (SPF)

Sender Policy Framework (SPF) is an open standard specifying a method to prevent sender address forgery. The current version of SPF protects the envelope sender address, which is used for the delivery of messages.

5.5.2 How it SPF Works

SPF works by having domains publish reverse MX records to display which machines (IP addresses) are designated as valid mail sending machines for that domain. When receiving a message from a domain, the recipient can check those records to make sure mail is coming from a designated sending machine. If the message fails the SFP check, it may be spam. Enabling this feature does create more performance overhead for the system due to the multiple DNS queries needed to retrieve a domain's SPF record; for this reason, the default setting for the **Enable SPF** feature on the **BLOCK/ACCEPT > Sender Authentication** page is **No** (off).

Messages that fail SPF check can be tagged or blocked and will be logged as such. Messages that pass SPF checks will still be scanned for spam. **The recommended setting is to Tag messages identified by SPF as spam so that if there is any possibility that a message is legitimate, it will be allowed to go on to the next stage of processing**.

5.5.3 Exemptions from SPF Checking - Trusted Forwarders

You may specify a list of Trusted Forwarder IP addresses, on the **BASIC > IP Configuration** page, which will be ignored when performing SPF checks, as well as rate control and IP Reputation checks. Trusted Forwarders are mail servers that are set up specifically to forward email to the Barracuda Email Security Gateway from outside sources. The Barracuda Email Security Gateway scans the IP addresses in the **Received From** headers list of each email and performs an SPF check on the first IP address that is not in the list of Trusted Forwarders.

5.5.4 DomainKeys Identified Mail (DKIM) Inspection

DomainKeys is a method of email authentication that enables a sending domain to cryptographically sign outgoing messages, allowing the sending domain to assert responsibility for a message. When receiving a message from a domain, the Barracuda Email Security Gateway can check the signature of the message to verify that the message is, indeed, from the sending domain and that the message has not been tampered with. Because most spam messages contain spoofed addresses, DomainKeys can help greatly in the reduction of spam.

5.5.5 How DomainKeys Works

DomainKeys uses a public and private key-pairs system. An encrypted public key is published to the sending server's DNS records and then each outgoing message is signed by the server using the corresponding encrypted private key. For incoming messages, when the Barracuda Email Security Gateway sees that a message has been signed, it will retrieve the public key from the sending server's DNS records and then compare that key with the message's DomainKeys signature to determine its validity. If the incoming message cannot be verified, the Barracuda Email Security Gateway knows it contains a spoofed address or has been tampered with or changed.

The benefits of enabling this feature include:

- Email sender is validated
- Email body is validated
- Validation through DNS is difficult to foil
- DomainKeys works well with email forwarding because it doesn't deal with the relay server IP address

You can choose to tag, block or quarantine both DKIM signed messages that fail the DKIM database check as well as unsigned messages, depending on how you configure **DomainKeys Inspection** on the **BLOCK/ACCEPT > Sender Authentication** page. You can also exempt domains from being tagged, quarantined or blocked if they fail this check. As stated elsewhere in this guide, it is safest to NOT exempt domain names from any kind of spam filtering due to the possibility of domain name spoofing by spammers.

Messages that pass DKIM checks will still be scanned for spam.

5.5.6 EmailReg.org Exemptions

If a domain is registered at http://EmailReg.org, the Barracuda Email Security Gateway will allow all email from that domain. If, however, you want all email from any domains that are registered at EmailReg.org to undergo header, subject and body filtering, you can add them to this table as an exemption to that rule. If you put any domain in the **Blocked Sender Domain/Subdomain** table that is ALSO registered at EmailReg.org, the Barracuda Email Security Gateway will block all email from that domain.

5.5.7 Invalid Bounce Suppression

The **Invalid Bounce Suppression** feature is used to determine whether or not the bounce address specified in a message is valid. It is designed to reduce the number of bounce messages to forged return addresses; i.e., you don't want to get bounced messages from spammers who spoof your domain or email address. Every email sent from the Barracuda Email Security Gateway is tagged with an encrypted password and expiration time. With **Invalid Bounce Suppression** enabled, any bounced email received by the Barracuda Email Security Gateway that does not include that tag is blocked. Each blocked message is recorded in the Message Log with the reason "Invalid Bounce".

To use the Invalid Bounce Suppression feature:

- Configure Outbound Relay on the **BASIC > Outbound** page.
- Configure Invalid Bounce Suppression on the **BLOCK/ACCEPT > Sender Authentication** page and enter a **Bounce Suppression Shared Secret** as a non-null password which will be included in the headers of valid emails sent from and bounced back to the Barracuda Email Security Gateway. Email bounces that don't include the password will be blocked if this feature is enabled. In a clustered environment, the **Bounce Suppression Shared Secret** will be synchronized across all Barracuda Email Security Gateways in the cluster.

5.5.8 Other Settings for Sender Authentication

These settings are configured on pages other than the **BLOCK/ACCEPT > Sender Authentication** page.

5.5.9 Mail Protocol (SMTP) Checking

The Barracuda Email Security Gateway can perform thorough checks on incoming email for RFC 821 compliance, require mail clients to introduce themselves with an SMTP "HELO" or "EHLO" command before stating a sender, and otherwise manage SMTP protocol to block spammers. See the **ADVANCED > Email Protocol** page for these and other optional SMTP settings.

5.5.10 Domain-Based Message Authentication, Reporting, and Conformance (DMARC)

DMARC is a sender email authentication mechanism that provides protection against phishing attacks and improves spam accuracy by blocking spam in spoofed messages. DMARC is built on top of the email authentication mechanisms Sender Policy Framework (SPF) and DomainKeys Inspection (DKIM). To set DMARC policies, you must have both an SPF and a DKIM record published for the domain. This feature is available using the Cloud Protection Layer (CPL).

5.5.11 Sender Spoof Protection

The Barracuda Email Security Gateway has the option to prevent "spoofing" of an organization's own domain by blocking emails with that domain name in the "From" field that are sent from outside the organization. Note that sender spoof protection should not be enabled if the organization sends messages from outside their internal email infrastructure (e.g., in the case of marketing bulk-mail services).

The **Sender Spoof Protection** feature can be configured at the global level from the **ADVANCED > Email Protocol** page or at the per-domain level on the **DOMAINS > Manage Domain > ADVANCED > Email Protocol** page. At the domain level, however, this feature is labeled as **Reject messages from my domain**.

Note that if the administrator enables **Sender Spoof Protection** at the global level it will supersede any whitelist entry created at the per-user level by a ***User, Helpdesk*** or ***Domain Admin*** account holder.

5.6 Recipient Filters

5.6.1 Allowed Email Addresses and Domains

Specify any domains, subdomains, and/or email recipients to "whitelist" on the **BLOCK/ACCEPT > Recipient Filters** page. Listed recipients' messages **are not scored for spam but are still checked for viruses**. Whitelisted recipients can also have some messages blocked due to IP controls.

Valid entries for the Email Address/Domain fields are domains, individual email addresses, or a pattern of email addresses. Entries in the Email Address field should be in one of the following formats:

- **/@mydomain.com/** - Whitelists all email addresses that end with "@mydomain.com".
- **/mydomain.com/** - Whitelists all email address in all subdomains of mydomain.com, in addition to mydomain.com.
- **user@domain.com** - Whitelists only that one email address.
- **/list-.*@domain.com/** - Whitelists all email addresses in "domain.com" that start with "list-" (eg, list-reply@domain.com, list-notify@domain.com, list-bounce@domain.com, etc.)

Do not use wildcards (such as *) or the @ sign when entering a domain. For example, enter `customer.com` instead of `*@customer.com`.

5.6.2 Blocked Email Addresses and Domains

Specify any domains, subdomains, and/or email recipients to "blocklist". Listed recipients, with blocking selected, do not receive messages that are not whitelisted by IP, recipient domain, or recipient email address. If quarantine or tag is selected and these messages match in another spam filter layer, then these recipients' messages may still have their email blocked. Note that outbound messages are never tagged.

Valid entries for the Email Address/Domain fields are as described above.

5.6.3 Encrypted Email Addresses and Domains (Outbound Only)

Specify any domains, subdomains, and/or email recipients to which outbound messages should be encrypted. Valid entries for the Email Address/Domain fields are as described above.

BEFORE using encryption, you must validate the sending domain and complete encryption configuration. See the **DOMAINS > Manage Domain > ADVANCED > Encryption** page. Also note that this list will be overridden by a list of any domains and email addresses that you enter in the **Sender Email Address/Domain Exemptions** field on the **BASIC > Administration** page.

5.6.4 Redirected Email Addresses and Domains (Outbound Only)

If you want to redirect outbound email for certain recipients, domains or subdomains to another gateway, add those email addresses, domains or subdomains here. Or, if you are using an email encryption service, add any email addresses, domains or subdomains for which you want to redirect outbound messages for encryption. You must specify the IP address of the server or service in the **Redirection Mail Server TCP/IP Configuration** section of the **BASIC > IP Configuration** page. If you want to relay outbound messages through an alternate mail server to the **Destination Mail Server** specified on the **BASIC > IP Configuration** page, you can specify a **Redirection Mail Server** on that page.

Valid entries for the **Email Address/Domain** fields are as described on the previous page.

5.7 Attachment Filters

5.7.1 About Attachment Filtering

Configure on the **BLOCK/ACCEPT > Attachment Filters** page.

- Attachment filters apply to both ***inbound*** and ***outbound*** mail.
- Filters can be set to off for specified file patterns or types.
- All email messages, ***except those from whitelisted senders***, go through attachment filtering.

5.7.2 Inbound Mail Attachment Filtering

For inbound mail, you can specify attachment filename patterns, common text attachment file types, and attachment MIME types on the **BLOCK/ACCEPT > Attachment Filters** page that you want to:

- block
- quarantine
- specifically not take action with (set to ***off***).

5.7.3 Outbound Mail Attachment Filtering

For ***outbound*** mail, specify the attachment filename patterns and file types you want to:

- block
- quarantine
- encrypt
- redirect
- specifically not take action with (set to off).

Important: Any messages that match encryption policy on the **BLOCK/ACCEPT > Attachment Filters** page that are sent from email addresses or domains that are exempt from encryption will not be encrypted. Use the **Sender Email Address/Domain Exemptions** field on the **BASIC > Administration** page to specify exemptions to attachment filtering.

5.7.4 Filename Pattern Filters

When you specify filename patterns in the table on the **BLOCK/ACCEPT > Attachment Filters** page, to indicate actions to take with messages that include attachments that match, follow these examples:

- To take an action for all .zip files, you would specify ***.zip**

- To take an action with all files that include the word jobs, you would enter `*jobs*`

Actions you specify for ***inbound*** or ***outbound*** file types apply to files found in zip and other archive files if you check the **Check Archives** box for that file type.

5.7.5 Attachment Filter Actions

- **Block** - Block the email message and attachment(s) based on the specified attachment.
- **Quarantine** - Quarantine the email message and attachment(s) based on the specified attachment.
- **Encrypt** - Applies to ***outbound*** messages only. Encrypt the email message and attachment(s) based on the specified attachment. The workflow for sending and receiving encrypted email is detailed on the **ADVANCED > Encryption** page.

> **BEFORE** using encryption, you must validate the sending domain and complete encryption configuration. See the **DOMAINS > Manage Domain > ADVANCED > Encryption** page.

- **Redirect** - Applies to ***outbound*** messages only. Redirect email message and attachment(s). See the **BASIC > IP Configuration** page to configure a **Redirection Mail Server**.
- **Off** - No action is taken on the email message and attachment(s) based on the specified attachment. Applies to ***inbound*** and ***outbound*** mail.

5.7.6 Attachment File Type Filters

Use File Type filters such as **Documents - MS-Access, Documents - Adobe PDF**, or **Executables - Windows Executables**, for example, to take one of the actions listed above with common attachment file types. See the **BLOCK/ACCEPT > Attachment Filters** page for the complete list.

> File attachments will be examined both for the mimetype of the file and the file extension. For this reason, if attachments are being blocked that you want to be *allowed*, then make sure that the file extensions of the attachments are appropriate to the file type (see the **Description** field). For example, an attached text file that has a filename extension of .xls would be blocked if the *Documents-MS-Excel* attachment file type is set to block.

Actions you specify for ***inbound*** or ***outbound*** file types apply to files found in zip and other archive files if you check the **Check Archives** box for that file type.

5.7.7 Blocking Attachments With Macros

For MS Office documents, you can set **Block Macros (MS Office Attachments)** to **Yes** if you want to block all attachments that include macros. This feature applies to both inbound and outbound mail.

5.7.8 Attachment MIME Type Filters

Specify MIME types, using the formats of the examples in the table on the **BLOCK/ACCEPT > Attachment Filters** page, and select one of the actions listed above to take with email messages with attachments.

Regular expressions may NOT be used.

Here are some example MIME types; see the **BLOCK/ACCEPT > Attachment Filters** page for a complete list.

Example MIME Types
text/css
application/msword
application/octet-stream

5.7.9 Password Protected Archive Filtering

Use the **Action for Password Protected Archives** setting to specify one of the actions listed above to take with an email message if attached archive files (zip,tar, etc.) require a password to unpack.

5.8 Content Filtering

From the **BLOCK/ACCEPT > Content Filtering** page you can set custom content filters based on the subject line, message headers, message body and attachment file content. You can use keywords or Regular Expressions to create filters. Administrators generally do not need to set their own filters for the purposes of blocking spam, as these forms of rules are delivered to the Barracuda Email Security Gateway automatically through Barracuda Energize Updates.

5.8.1 Using Regular Expressions

The online help for the **BLOCK/ACCEPT > Content Filtering** page includes a link to a Regular Expressions help page that covers expressions you can use for advanced filtering. HTML comments and tags embedded between characters in the HTML source of a message are also filtered.

5.8.2 Using Pre-made Filter Patterns

In the **Predefined Filters** section of the **BLOCK/ACCEPT > Content Filtering** page, you can specify actions to take with messages based on pre-made patterns in the subject line or message body. Predefind filters include credit card, Social Security numbers, privacy information such as driver's license numbers, phone numbers, expiration dates, and HIPAA data. These filters are automatically checked and acted upon by seleced actions for inbound or outbound messages, as described below.

Entering a large number of filters could slow mail processing. Recommended maximum is approximately 30 filters. Also note that using keyword filtering is not the most effective way to filter spam and could lead to false positives. A more effective practice is to report spam that got through your Barracuda Email Security Gateway to Barracuda Central so that new rules can be added to the Barracuda Central database. To submit messages determined to be spam, select the message(s) on the **BASIC > Message Log** page and select ***Submit to Barracuda Central*** from either the **Spam** or **Not Spam** drop-downs on the tool bar.

Content Filtering For Inbound Mail

- Whitelist
- Block
- Quarantine
- Tag

- Off

Content Filtering For Outbound Mail

- Whitelist
- Block
- Quarantine
- Encrypt
- Redirect
- Off

5.8.3 Attachment Content Filters

You can take actions with inbound or outbound messages that contain attachments that include text matching the patterns you enter on the **BLOCK/ACCEPT > Content Filters** page. Attachment Content Filtering is limited to text type files such as MS Office files, html, pdf files and other document files.

To create a new attachment content filter, in the **Pattern** text box on the page, enter keywords or regular expressions with which to filter the content of text type attachments.

5.8.4 Attachment Block Notifications

You can enable or disable notification emails to senders of messages that are blocked due to file attachment content filters. Configure these notifications for inbound and outbound mail from the **ADVANCED > Bounce/NDR Settings** page in the web interface. From that page you can also enter custom message text to insert in the notifications. Attachment content filters are configured in the Attachment Content Filters section of the **BLOCK/ACCEPT > Content Filters** page.

5.9 Reverse DNS

The Barracuda Email Security Gateway does a reverse DNS lookup on inbound and outbound IP connections and finds the hostname associated with the IP address of the sender. By configuring rules on the **BLOCK/ACCEPT > Reverse DNS** page, you can choose to apply **Common Reverse DNS Rules** by country or create **Custom Reverse DNS Rules** to quarantine or block outbound messages from those domains.

5.9.1 Blocking by Top Level Domain (TLD)

The last part of a hostname is known as the top level domain, or TLD. Most TLDs include a country identifier, such as .ca for Canada, .ru for Russia, etc. If most or all of the mail that you receive from a particular country is spam, you can use the **Common Reverse DNS Rules** to tag (inbound only), block or quarantine any message that has an associated hostname that includes that country's TLD. Email which is not blocked is subject to all of the usual spam and virus checks.

5.9.2 Whitelist Override for TLDs

Use the **Custom Reverse DNS Rules** to quarantine or block outbound messages from hostnames ending with values that you specify. List the sending domains or subdomains you want to whitelist on the **BLOCK/ACCEPT > Sender Filters** page. You can use the **Custom Reverse DNS Rules** to whitelist all or part of a hostname from which you want to always allow mail, both inbound and outbound. With the whitelist option you can thereby override the **Common Reverse DNS Rules** settings for TLDs. If you have blocked any TLDs in **Common Reverse DNS Rules**, for example, you can use the **Custom Reverse DNS Rules** whitelist option to allow mail from one or more hostnames within that TLD.

5.9.3 Messages With a Missing PTR record

Use the **Block Missing PTR Records** setting to enable blocking mail from IP addresses with no PTR (reverse DNS) record defined.

Caution! Many mail servers do not have their reverse DNS configured properly, which may cause legitimate mail to be blocked when **Block Missing PTR Records** is set.

5.10 Regional Settings

5.10.1 Character Set Policies

Action can be taken on ***inbound*** messages based on the character set used in the message. Select the desired action for each language and click **Save**.

5.10.2 Regional Settings

These settings enhance the ability of the Barracuda Email Security Gateway to detect spam in ***inbound*** and ***outbound*** Chinese and Japanese language messages by activating special spam analysis rules for these languages. After making a change, click **Save**.

- **Chinese (PRC) Government Compliance** - This option may need to be enabled if your Barracuda Email Security Gateway resides in the People's Republic of China (PRC). Set this option to No if your Barracuda Email Security Gateway is located outside the PRC.
- **Chinese Language Spam Rules** - Enable this option if your company receives a significant amount of valid Chinese language email. Otherwise, this option should be disabled.
- **Japanese Language Spam Rules** - Enable this option if your company receives a significant amount of valid Japanese language email. Otherwise, this option should be disabled.

5.10.3 GeoIP Policies

Using this feature requires that you first set up the free Cloud Protection Layer service with your Barracuda Email Security Gateway. See Cloud Protection Layer for more information about the service.

You can select to **Block** messages based on country of origin on the **Inbound Settings > Regional Policies** page, allowing you to reduce unwanted Inbound emails. Note that this setting applies to all domains you have verified in the Cloud Protection Layer for processing email, unless you change these settings for a specific domain. In that case, the domain-level settings override the global system settings.

Once you select a country from the drop-down menu and click **Add**, the ISO code for the selected country displays in the table. For a complete list of country codes, see http://www.nationsonline.org/oneworld/country_code_list.htm.

When bulk editing countries for regional policies, use the ISO 3166 alpha 3 code. See the ISO Online Browsing Platform (OBP): https://www.iso.org/obp/ui/#search

User Interface – Users

6.1 Account View

With the **USERS > Account View** page, you can view, edit, delete and change passwords on accounts, depending on your role and associated permissions. If your account permissions allow, you will be able to click the **Edit Role** link in the **Administrator Actions** column and change the role for that account on the **Edit Role** popup. You'll also be able to access details about roles from the Help button on the popup. Accounts are only associated with inbound mail.

Things you can do on the **USERS > Account View** page:

- View and Modify Account Information
- Filter the entries displayed
- Customize the display
- User Account Cleanup tool - Remove Invalid Accounts

6.1.1 Account View

This section displays a list of all per-user accounts for this domain. A filter is provided to limit the display to only users with specific attributes (e.g., users with quarantine disabled). The total number of accounts found is displayed next to the filter and reflects the results of applying that filter. The following attributes are available:

- **Account Address** - The email address of the per-user account.
- **Role** - The role associated with the account: User, Helpdesk, Domain Admin
- **Notify Interval** - Reflects the user's selected interval for quarantine notifications:
  - Daily
  - Weekly
  - Never
- **Quarantine** - The status of the user's quarantine. If **Yes**, then the user's quarantine inbox has been enabled, and all quarantined messages will be stored in the user's quarantine account. If **No**, then all quarantined mail is forwarded to the intended recipient's mailbox instead of being placed in quarantine.
- **Spam Scan** - The status of spam scanning for the user. If **Yes**, then all mail addressed to that user will undergo spam scanning. If **No**, then any messages where that user is the only recipient will not be scanned for spam.
- **Size (KB)** - The current size of the user's quarantine area in KB. It is helpful for Retention Policies (if enabled), and can be useful in determining which users are not cleaning out their quarantine areas.
- **Message Count** - The current number of items in a user's quarantine area. It is helpful for Retention Policies (if enabled), and can be useful in determining which users are not cleaning out their quarantine areas.

- **Oldest Message** - This is the oldest message in a user's quarantine area. It is helpful for Retention Policies (if enabled), and can be useful in determining which users are not cleaning out their quarantine areas.
- **Administrator Actions** - List of basic actions available to an Administrator to manage a particular user's account: are:
  - Edit Account
  - Edit Role
  - Change Password - Only changes the local Barracuda Email Security Gateway password for the user.
  - Delete Account

For addition and removal of specific features, go to the **USERS > User Features** tab.

See the Help file on the page for procedures to create and apply filters to the display.

6.1.2 User Account Cleanup

You can periodically check for and remove user accounts that are no longer valid by clicking **Remove All Invalid Accounts** in the **User Account Cleanup** section. The Barracuda Email Security Gateway then checks each account against your mail/directory server and removes any from the unit that are no longer valid in the directory.

6.2 User Features

The **USERS > User Features** page applies to accounts related to managing inbound mail and contains the following sections:

- Mail Client Add-ins
- Default User Features
- User Features Override

6.2.1 Mail Client Add-in

(Models 300 and higher)

The Barracuda Outlook Add-in for Microsoft Outlook clients enables users to:

- Classify messages as *Spam* or *Not Spam* directly from the mail client.
- Click the **Encrypt Message** button in a New Message window if the user wishes to encrypt the message contents.
- Whitelist the sender of a message.

The Barracuda Outlook Add-In can be downloaded from the Barracuda Email Security Gateway and installed in Outlook clients. Download options to install the add-in include:

- **Allow Users To Download Outlook Add-In** - Enable users to download an Outlook add-in from the **Login** page by selecting **Yes** and clicking **Save**.
- **Outlook Add-In Deployment Kit** - Use a Windows GPO to push the add-in to your users' workstations. The Windows zip file, which you can either open or save to your system, includes the following:
  - 32 bit MSI installer file for use with Outlook 2003, Outlook 2007, and Outlook 2010 32-bit
  - 64 bit MSI installer file for use with Outlook 2010 and 2013 64-bit.
  - ADM (administrative template) for customizing the add-in behavior Please see the Barracuda Email Security Gateway Outlook Add-In Deployment Guide in Barracuda Campus.

6.2.2 Default User Features

(Models 300 and higher)

This section is used to specify which features your users will be allowed to access when they log into their accounts. The settings chosen in the **Default User Features** section are applied to all new and existing user accounts that are created for ALL domains. Domain Admin role will be able to control user access to the following features ONLY if they are enabled (set to **Yes**) here. If any features are disabled (set to **No**), they will not be visible to Domain Admins and will not appear to users when they log in.

For example:

- If the **Whitelist/Blocklist** setting is set to **Yes,** the Domain Admin can control the user's ability to create a personal whitelist or blocklist. If the setting is No, the Domain Admin will NOT see this feature, nor will users associated with that domain. To create exceptions for specific users, see the **User Features Override** section of the page. Click **Save** after making any updates.

The following options are available:

- **Quarantine Enable/Disable** - Controls the user's ability to enable/disable their personal quarantine inbox.
- **Spam Scan Enable/Disable** - Controls the user's ability to modify their personal spam settings.
- **Notification Change** - Controls the user's ability to change the frequency and language of their quarantine summary notifications.
- **Whitelist/Blocklist** - Controls the user's ability to add email addresses and domains into their personal whitelist blocklist.

User whitelist entries are overridden by global filters configured on the Barracuda Email Security Gateway. If necessary, users can request that the administrator add IP or email address entries to the global whitelist.

- **Use Bayesian** - Controls the user's ability to manage their personal Bayesian database.
- **Scoring Change** - Controls the user's ability to change the spam scores at which their emails are tagged, quarantined, and blocked.

6.2.3 User Features Override

(Models 300 and higher)

Use this section to change the settings for user accounts that already exist. Enter one or more email addresses that you wish to change in the **User Account(s)** list box, select the options you wish to modify and click **Save Changes**.

Available choices are:

- **Yes** - If the **Default User Features** setting for the feature is **No**, then the users specified in the **User Accounts** will have access to this feature due to the override.
- **No** - Disables the feature for the specified user(s) if this feature is set to **Yes** in the **Default User Features** section.
- **Unchanged** - Leaves the feature status unchanged for the specified user(s).

The Override functionality is supported when the corresponding feature in the domain-level **Default User Features** section is set to **Yes**. You cannot override any feature that is set to **No** in the domain-level **Default User Features** section. The table below summaries when overrides apply at the domain level depending on global and domain level **Default User Features** settings.

	User Features Override	
Override supported?	**Global Default User Feature setting (this page)**	**Domain-level Default User Feature setting**
supported	Yes	Yes
not supported	Yes	No
supported	No	Yes or No

With **per-user** quarantine enabled, if user features are enabled, then disabled, or if **per-user** quarantine is later disabled, account holders will lose previously configured per-user settings. For example, if an account holder has created a whitelist and blocklist in his/her account and the administrator disables the whitelist/blocklist feature or disables **per-user** quarantine, the account holder's whitelist/blocklist will be removed and cannot be restored.

6.3 User Add/Update

User accounts are created automatically for users when all of the following conditions are met:

1. Quarantine is enabled on the **BASIC > Quarantine** page.
2. "Per-User" is selected as the quarantine type on the **BASIC > Quarantine** page.
3. Messages that rate a *quarantine* status arrive for a user who does not already have a quarantine account.

User accounts can also be created (or disabled) manually by an administrator by entering the email address(es) in the **USERS > User Accounts** text box and selecting the appropriate "Enable User(s) Quarantine" setting.

It may take a minute or two before the user account is created. If you look for the account on the **USERS > Account View** page and don't see it, look for a message in the upper left of the page that says **Running Tasks:** *Account Creation*. This message will disappear after the account creation task is complete and you'll see the new account you created in the **Accounts** window.If there is a problem creating the account, you'll see an error message in a red bubble at the top of the page.

- **User Account(s)** - Enter email address(es) of accounts to be created / disabled (one email address per line).
- **Enable User(s) Quarantine** - Select **Yes** to create a quarantine account for specified user(s), or **No** to disable specified quarantine account(s). Disabled quarantine accounts will not quarantine any new messages, but any pre-existing quarantined messages will still be accessible. Any user preferences (such as Whitelist/Blocklist) allowed to users by the administrator will also be available.
- **Email New User(s)** - Email new account login information to user(s) upon either manual or automatic creation of an account.

6.4 Retention Policies

6.4.1 Retention Policies and Purging Old Messages

As the administrator, you can configure retention policy to limit the amount of disk space used for storing each user's quarantined messages, thereby conserving system resources on the Barracuda Email Security Gateway.

From the **USERS > Retention Policies** page, you can enable the user to easily schedule quarantined messages for regular purging based on age (in number of days), disk space used (specified in kilobytes), or both. Setting the **Age Limit** to a 7-14 day range is recommended assuming that older quarantined emails may lose importance with time.

Note that regardless of these settings, no messages younger than 3 days will be removed. For example, if the maximum size limit on email size is 10MB and a quarantined email has a 19MB attachment, the email will be retained for 3 days, giving the user time to examine and process that email before it is automatically deleted by the Barracuda Email Security Gateway.

6.4.2 Minimize Excessive Email Storage

Barracuda recommends training users to manage their own quarantine areas, since constant reliance on the Barracuda Email Security Gateway to automatically remove quarantined messages based on either age or disk usage may impact system performance.

Affects on performance are affected by the number of user quarantine areas that are kept on the Barracuda Email Security Gateway, the amount of email that is quarantined each day, and the number of tasks the system performs (e.g., reporting, or message body filtering).

6.4.3 Track Who is Using the Most Storage

Use the filters on the **USERS > Account View** page to quickly determine which users have the largest quarantine areas. Each account entry shows Yes/No in the **Quarantine** column ("Yes" indicates per-user quarantine is in effect for that user) and number of Kbytes of email stored in their quarantine inbox in the **Size** column. Individual user quarantine areas can be disabled from the **USERS > Add/Update** page so that any repeat offenders can be prevented from utilizing the Barracuda Email Security Gateway quarantine areas. When a user's quarantine is disabled, emails sent to that user that would normally have been placed in quarantine will simply be delivered to the user's actual mailbox with the subject line prepended with a quarantine tag.

If the system has been quarantining mail for any period of time without any Retention Policies being set, then turning this feature on for the first time may result in a big performance impact since there may be a large number of messages to be processed. The same is true if retention policies are re-enabled after having been turned off for any period of time. After the initial purging, the performance impact should stabilize since the system will be able to keep large quarantine fluctuations to a minimum. Retention policies are run daily starting at approximately 02:30 AM.

Configure Retention Policies

On the **USERS** > **Retention Policies** page:

Size Based Retention

- **Size Retention Policy** - Set to **On** to limit disk space per user for storing quarantined messages.
- **Size Limit (KB)** - Amount of disk space in kilobytes allotted per user of quarantine message storage if **Size Retention Policy** is turned **On**.

Age Based Retention

- **Age Retention Policy** - Set to **On** to have the system delete quarantined messages based on the **Age Limit** in days. Recommendation is **On**.
- **Age Limit (Days)** - Limit the time a user may keep a quarantined message on the Barracuda Email Security Gateway.

User Interface – Domains

7.1 Domain Manager

The Barracuda Email Security Gateway has three levels of management and configuration:

- Global level
- Per-domain level
- User level

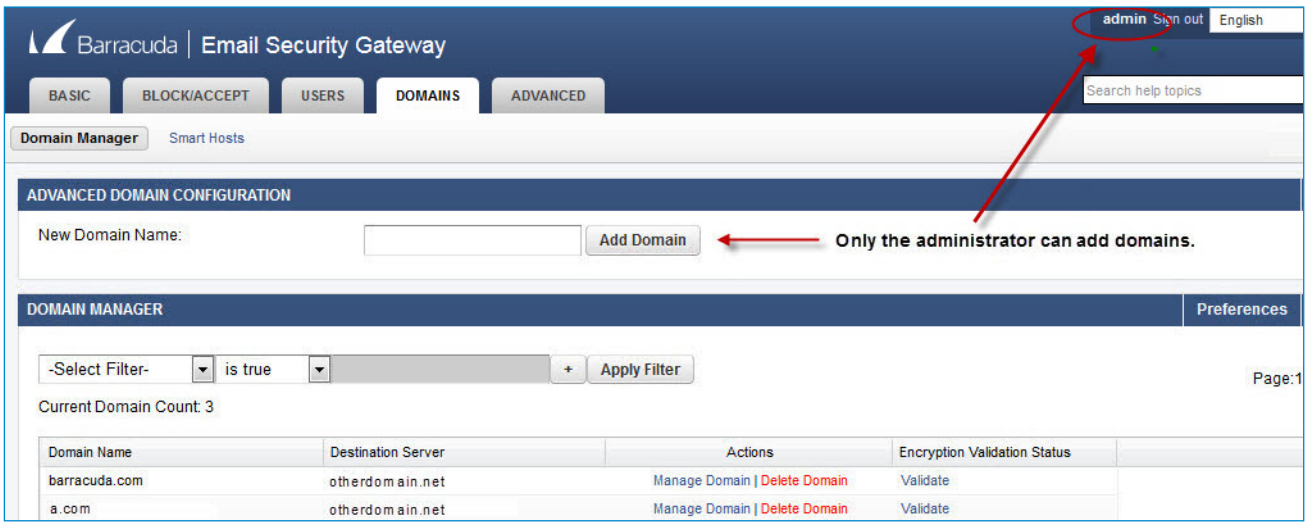
Only administrators can configure global settings. Setting values on a per-domain basis overrides the values configured at the global level in the web interface. However, if you have never changed a particular setting for a domain, any global level changes to that feature will be applied for that domain. This also means that any changes you make to the global values of the Barracuda Email Security Gateway will NOT be inherited by the domains that you edit and for which you have changed configuration values.

7.1.1 Configuring Domains

The Barracuda Email Security Gateway only accepts emails addressed to domains that it has been configured to recognize. Settings for individual domains can be configured by the administrator and, with some restrictions, by the **Domain Admin** and **Helpdesk** account roles as described in Roles and Navigating the Web Interface. All three roles will see a **DOMAINS** tab from which they can click **Manage Domain** next to the domain for which to edit the domain-level settings.

Clicking the **Manage Domain** link for a particular domain will show some or all of the **BASIC, USERS, BLOCK/ACCEPT, OUTBOUND QUARANTINE** and **ADVANCED** tabs, depending on the permissions level of the logged in account role.

Only an administrator can add or delete domains using the controls available in the **DOMAINS** page. The administrator can also add domains from the **BASIC > IP Configuration** page. Domains added from either page will be initially configured with whatever you have specified your default global settings to be.



If the administrator deletes a domain, *all user* accounts associated with that domain will also be deleted from the Barracuda Email Security Gateway.

7.1.2 Domain Level Settings

Some settings are only configurable at the domain level, while others are configurable at both the global and domain levels, with the domain level setting taking precedence. The ***Domain Admin*** role or the ***Admin*** role can override some global settings for spam and virus checking and quarantine at the domain level.

> Setting values on a per-domain basis overrides the values configured at the global in the web interface. However, if you have never changed a particular setting for a domain, any global level changes to that feature will be applied for that domain. This also means that any changes you make to the global values of the Barracuda Email Security Gateway will NOT be inherited by the domains that you edit and for which you have changed configuration values.

Basic configuration of a domain consists of identifying the name of the domain (and/or a specific sub-domain) and specifying a destination mail server. Additional settings available for a domain are dependent on the model of your Barracuda Email Security Gateway, and can include any or all of the following:

- Destination Mail Server
- Enabling of spam scanning and setting spam score limits for the domain
- Enabling or disabling virus scanning
- Per-user quarantine enable/disable
- Control over which features users can see and configure for their accounts (see Controlling Access to Account Features).
- A defined global quarantine email address (for the domain only)
- Option to reject messages from same domain name. If set to **Yes**, the Barracuda Email Security Gateway will reject email where the FROM envelope or header address domain matches the domain (in the TO address). This feature provides protection from 'spoofing' of the domain.
- Option to require an encrypted TLS connection when receiving email ***from*** either ALL or specified domains. See the **ADVANCED > Email Protocol** page at the domain level for details.
- Option to require an encrypted TLS connection when relaying email ***to*** specified destination domains. See the **ADVANCED > Email Protocol** page at the domain level for details.
- IP address/range, Sender domain, Sender email and Recipient filtering.

> BLOCK/ACCEPT policies created at the per-domain level do NOT apply to outbound messages - they only apply to inbound messages for that domain.

- LDAP configuration
- Option to specify local database of valid recipients (if not using LDAP) and alias linking
- Single Sign-On with various authentication mechanisms
- Emailreg.org: option to require header, body or subject content filtering on mail from registered email addresses
- Ability to validate the domain and specify an image for branding encrypted email messages and notifications sent to the recipient. Note that encryption policy can only be set at the global level by the administrator.

7.2 Smart Hosts

For outbound mail, if your network requires ALL outbound mail to go through a particular mail server, enter that server in the **Outbound SMTP Host (Smart Host)** field on the **BASIC > Outbound** page. This is the destination server through which outbound email will be sent from the Barracuda Email Security Gateway for routing to the Internet, and whose IP address will appear in the outgoing mail headers. Individual servers specified there will override that setting for the specified domain(s).

7.2.1 Per-Domain Configuration

You can specify relay servers or Smart hosts for specific domains. If you want outbound email to a particular domain to go through a specific host before routing to the Internet and/or default MX records, you can specify that SMTP server on the **DOMAINS > Smart Hosts** page. For example, you might want all emails to yourcompany.com to go through an additional virus scanning service or cloud-hosted relay service.

User Interface – Advanced Configuration

8.1 Email Protocol

The **ADVANCED > Email Protocol** page provides for the following settings:

- Mail Protocol (SMTP) Checking
- SMTP Configuration
- SMTP over TLS/SSL

8.1.1 Mail Protocol (SMTP) Checking

- **SMTP HELO/EHLO Required** - Specifies whether mail clients connecting to the Barracuda Email Security Gateway need to introduce themselves with an SMTP "HELO" or "EHLO" command before stating a sender and recipient. Setting this option to Yes may stop automated spam-sending programs; however, the recommended setting is No as many MTAs (message transfer agents) have problems when this command is required.
- **Enforce RFC 821 Compliance** - Specifies whether the Barracuda Email Security Gateway requires that the SMTP "MAIL FROM" and "RCPT TO" commands contain addresses that are enclosed by '<' and '>'. It also requires that the SMTP "MAIL FROM" and "RCPT TO" commands do not contain RFC 822 style phrases or comments. Turning on this option stops messages sent from spam senders; however, this may also block some Windows mail programs such as MS Outlook, and other MTAs, that do not adhere to the RFC 821 standard.
- **Require Fully Qualified Domain Names** - Block mail that uses a non fully-qualified domain name in the 'From' address.
- **Sender Spoof Protection** - Reject inbound mail that has a "From" domain matching a domain added on the Barracuda Email Security Gateway. Both the **Header To/From** and **Envelope To/From** fields are checked. This option is only enabled if all mail ***from*** the configured domains goes directly to the mail server, and not through the Barracuda Email Security Gateway.

This setting does not reject emails with identical *"From"* and *"To"* domains. To reject such emails, each individual domain must be configured. Go to **DOMAINS > Domain Manager**, click **Manage Domain** for the relevant domain, then go to **ADVANCED > Email Protocol** for that domain and set **Reject messages from my domain** to **Yes**.

An IP whitelist can override this setting if spoof protection is desired, and a filtered domain's mail server needs to deliver mail through the Barracuda Email Security Gateway to another domain that is filtered. The recommended setting is No so that remote users can still send mail through the Barracuda Email Security Gateway.

- **Allow Empty Inbound Sender Domain** - Some spammers may send emails with nothing in the From field. Setting this feature to **No** means that the Barracuda Email Security Gateway will not accept inbound messages that do not contain a sender.
- **Allow Empty Outbound Sender Domain** - Setting this feature to **No** means that the Barracuda Email Security Gateway will not send outbound messages that do not contain a sender.

8.1.2 SMTP Configuration

- **Incoming SMTP Timeout** - Sets a limit on the amount of idle time, in seconds, allowed in an incoming SMTP session. Spammers can keep connections open for extended periods of time, thus occupying system resources on the Barracuda Email Security Gateway. Messages in SMTP transactions that exceed the threshold are displayed in the Message Log as being "Deferred" with "Sender Timeout" as the reason for the deferral.
- **Messages Per SMTP Session** - The maximum number of messages allowed in one SMTP session. If the number of messages in one session exceeds this threshold, the rest of the messages are blocked and the last message accepted is displayed in the Message Log. The sender is immediately disconnected and is required to make a new connection to continue sending messages, which may ultimately trigger a Rate Control deferral.
- **Maximum Errors Per SMTP Session** - Sets a limit on the number of errors allowed during one SMTP session. If the number of errors in one session exceeds this threshold, the rest of the messages are blocked and the last message accepted is displayed in the Message Log. The sender is immediately disconnected and is required to make a new connection to continue sending messages, which may ultimately trigger a Rate Control deferral.
- **Recipient Delimiter** - This feature enables gathering all quarantined mail for a user who uses address tagging and directing all of that user's mail to one quarantine inbox. If you have ***Per-User*** quarantine enabled, enter a one character delimiter (such as a '+') in this field and configure the same character delimiter on your mail server. If a user receives mail to user+ebay@example.com, and user+bank@example.com, these messages will all be sent to the user@example.com inbox.

If **New User Quarantine State** is set to **On** on the **BASIC > Quarantine** page, and if this feature is disabled, multiple quarantine inboxes could be created for a user who uses address tagging.

- **Maximum Message Size** - The maximum size, in bytes, of any ***inbound*** email message that will be accepted. If the message exceeds this size limit, the sending server will be told the message is too large and the entire message will be ignored. This setting does not apply to outbound email.

- **SMTP Welcome Banner** - The banner that is presented to the SMTP client connecting to the Barracuda Email Security Gateway. This value must be unique across the network. If this value is not unique, and mail attempts to go to a server with the same welcome banner, then mail delivery fails. If this value is left blank, the Barracuda Email Security Gateway will manage the setting.
- **Remove Barracuda Headers** - This feature is used to strip off any custom X-headers that the Barracuda Email Security Gateway has applied before the message leaves the device.

8.1.3 SMTP over TLS/SSL

SMTP over TLS/SSL defines the SMTP command, STARTTLS. This command advertises and negotiates an encrypted channel with the peer for this SMTP connection. This encrypted channel is only used when the peer (receiving server) also supports it.

Important! If you set **Enable SMTP over TLS/SSL** to **No**, domain administrators will not be able to require SMTP over TLS for any domain.

To configure SMTP over TLS/SSL at the domain level:

To require SMTP over TLS connections from sending domains and/or for outgoing messages from the Barracuda Email Security Gateway to a particular domain, configure on the **DOMAINS** > **Manage Domain** > **ADVANCED** > **Email Protocol** page for that domain.

8.2 SMTP Responses

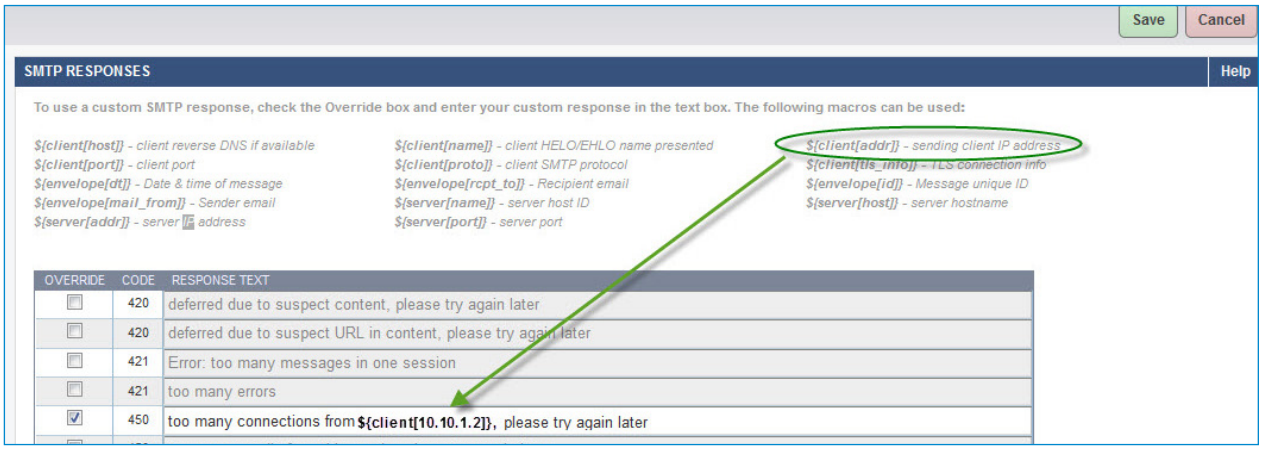
This feature is for advanced administrators and internet service providers.

8.2.1 Customizing SMTP Responses

From the **ADVANCED > SMTP Responses** page in the web interface you can choose to override default SMTP error response messages with customized text. Only ASCII characters are supported. To create the customized text:

1. Check the error code line to enable use of an alternate/customized message.
2. Edit the default text. You can optionally use one or more of the macros shown in the top section of the page to insert server hostname, client HELO/EHLO, sending client IP address and/or other email message information into the response message.

Use macros from the top of the page to insert customized information such as an IP address. In this example, the phrase **your IP** is replaced using the **${client[addr]} - sending client IP address** macro.



8.3 Energize Updates

8.3.1 Updating the Definitions from Energize Updates

This should be one of the steps the administrator performs in the initial installation of the Barracuda Email Security Gateway. The **ADVANCED > Energize Updates** page allows you to manually update the Virus, Policy, Extended Malware, and Security Definitions used on your Barracuda Email Security Gateway or to have them updated automatically. Barracuda Networks recommends that the **Automatic Updates** option be set to **On** for all three types of definitions so that your Barracuda Email Security Gateway receives the latest rules as soon as they are made available by Barracuda Networks.

IMPORTANT:

If you are using the Barracuda Exchange Anti-Virus Add-in with your MS Exchange mail server, you MUST set the **Automatic Updates** option to **On** in the **Virus Definition Updates** section of the **ADVANCED > Energize Updates** page. This is necessary to ensure that the Barracuda Exchange Anti-Virus Add-in receives constant updates of virus signatures from the Barracuda Email Security Gateway.

8.4 Firmware Update

8.4.1 Updating the Firmware on your Barracuda Email Security Gateway

This should be one of the steps the administrator performs in the initial installation of the Barracuda Email Security Gateway. Use the **ADVANCED > Firmware Update** page to manually update the firmware version of the system or revert to a previous version. The only time you should revert back to an old firmware version is if you recently downloaded a new version that is causing unexpected problems. In this case, call Barracuda Networks Technical Support before reverting back to a previous firmware version.

8.4.2 Updating the Firmware of Clustered Systems

If a system is part of a cluster, Barracuda recommends changing the system's **Mode** in the **Clustered Systems** section of the **ADVANCED > Clustering** page to ***Standby*** before upgrading its firmware, and then repeating this process on each system in the cluster. Once the firmware on each system has been upgraded, you can then change the mode on each system back to ***Active***.

Changing a clustered system to Standby mode before upgrading prevents a system on a more recent firmware version from trying to synchronize its configuration with a system on an earlier firmware version. If you have the latest firmware version already installed, the **Download Now** button on the **ADVANCED > Firmware Update** page is disabled.

IMPORTANT:

Before upgrading, **BE SURE TO TAKE THE Barracuda Email Security Gateway OFFLINE**. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. **DO NOT MANUALLY REBOOT THE SYSTEM at any time during an upgrade**, unless otherwise instructed by Barracuda Networks Technical Support.

8.5 Cloud Control

Before you can use the Barracuda Cloud Protection Layer (CPL), you must set up your free Barracuda Cloud Control (BCC) account. BCC gives you access to CPL, and provides central management for multiple Barracuda Email Security Gateways (as well as other Barracuda hardware and virtual appliances).

You can connect one or more Barracuda Email Security Gateways to Barracuda Cloud Control by doing the following:

1. If you don't already have an account with Barracuda Networks, click the **Create a New Barracuda Cloud Control Account** link on the **ADVANCED > Cloud Control** page.
2. Fill in the required information in the popup window to create the account and click **Save Changes**. Once the changes are saved, you'll receive a confirmation email in the email account you listed. Respond to the email to complete the new account setup.
3. Log into your Barracuda Email Security Gateway as the administrator. From the **ADVANCED > Firmware Upgrade** page, check to make sure you have the latest firmware installed. If not, download and install it now.
4. From the **ADVANCED > Cloud Control** page, select **Yes**, enter the Barracuda Networks username and password and click **Save Changes** to connect to Barracuda Cloud Control.

   Your Barracuda Email Security Gateway can connect with only one Barracuda Cloud Control account at a time.

5. Log into Barracuda Cloud Control with your username and password and you will see your Barracuda Email Security Gateway statistics displayed on the **BASIC > Dashboard** page. To access the web interface of your Barracuda Email Security Gateway, click on the link in the **Products** column in the Cloud Control pane on the left side of the page. Or you can click on the product name in the **Product** column of the **Unit Health** pane on the right side of the page.
6. Follow steps 3 and 4 to connect every subsequent Barracuda Email Security Gateway to Barracuda Cloud Control.
7. To stop the synchronization between your Barracuda Email Security Gateway and Barracuda Cloud Control, from the **ADVANCED > Cloud Control** page on the Barracuda Email Security Gateway, enter the Barracuda Cloud Control username and password for the particular account associated with that device and click **No** for **Connect to Barracuda Cloud Control**. Do this when you know that there will be a loss of connectivity between the Barracuda Email Security Gateway and Barracuda Cloud Control due to the appliance being physically moved or other network connectivity issues.

Note that reports cannot be emailed from the Barracuda Email Security Gateway when using Barracuda Cloud Control. The Barracuda Cloud Control Status field indicates whether or not this Barracuda Email Security Gateway is connected to Barracuda Cloud Control.

8.6 Secure Administration

8.6.1 Web Interface HTTPS/SSL Configuration

SSL (Secure Socket Layer) ensures that your passwords are encrypted and that all data transmitted to and received from the Barracuda Email Security web interface is encrypted as well. All Barracuda Email Security Gateways support SSL access without any additional configuration. However, some sites may wish to enforce using a secured connection to access the web interface, or prefer to use their own trusted certificates.

The SSL configuration referred to here is related only to the web interface. There is no need to explicitly configure SSL for traffic between the Barracuda Email Security Gateway and your mail servers.

How to Enforce SSL-only Access (recommended)

1. On the **ADVANCED > Secure Administration** page, select **Yes** to enable **HTTPS/SSL Access Only** to the web interface. Setting this to No will still allow the Barracuda Email Security Gateway to accept non-SSL connections.
2. Select **Yes** to **Use HTTPS Links in Emails** for per-user quarantine messages sent from the Barracuda Email Security Gateway.
3. Enter your desired **Web Interface HTTPS/SSL Port** for the web interface. The default is 443.
4. Click **Save**.

If you wish to change the certificate that is used, you must first create and upload it to the Barracuda Email Security Gateway before changing the **Certificate Type** in the **SSL Certificate Configuration** section of the **ADVANCED > Secure Administration** page. See the online help for detailed instructions. The Barracuda Email Security Gateway supports the following types of certificates:

- **Private (Self-signed)** - A certificate created locally for your specific organization, by your organization. This type of certificate provides strong encryption without the cost of purchasing one from a trusted Certificate Authority (CA). However, web browsers are unable to verify the authenticity of the certificate, so warnings about the unverified state may be displayed. To avoid this warning, download the **Private Root Certificate** into each browser that accesses this Barracuda Email Security Gateway. To create a self-signed certificate, see **Certificate Generation** below.
- **Trusted (Signed by a trusted CA)** - A certificate signed by and purchased from a trusted CA. Web browsers are able to recognize and verify these certificates as coming from a trusted source, so in most circumstances there is no need for a Private Root Certificate to be downloaded for every Web browser. The following types of Trusted Certificates are supported:
  - Obtained from a Third-Party CA

- Microsoft Certificate Services
- Wildcard Certificates

The **Default** certificate provided on the Barracuda Email Security Gateway is signed by Barracuda Networks. On some browsers, using these may generate benign warnings which can be safely ignored.

8.6.2 Certificate Generation

See the help page on the **ADVANCED > Secure Administration** page to create your own **Private (self-signed)** certificate for strong SSL encryption.

8.6.3 Trusted Certificate

For uploading Trusted Certificates onto the Barracuda Email Security Gateway. The Barracuda Email Security Gateway supports the following types of Trusted Certificates:

- Obtained from a Third-Party CA
- Microsoft Certificate Services
- Wildcard Certificates

See the help page on the **ADVANCED > Secure Administration** page for instructions.

8.6.4 Certificate Obtained from a Third-Party CA

Trusted certificates are issued by designated providers, or Certificate Authorities, who must adhere to local laws on encryption methods. Please consult your domain registrar or a local directory to locate a CA that is certified for your area.

See the help page on the **ADVANCED > Secure Administration** page to create and install a CA-generated certificate.

8.6.5 Microsoft Certificate Services

Microsoft Certificate Services enables some Microsoft servers to act as a Certificate Authority. For more complete information regarding Microsoft Certificate Services, please visit Microsoft TechNet. See the help on the **ADVANCED > Secure Administration** page to create and install a certificate using Certificate Services.

8.6.6 Wildcard Certificates

Wildcard certificates are domain-level certificates (as opposed to the normal host-level certificates). Wildcard certificates can be installed across a number of systems within a single domain. If you are using a wildcard certificate, an IIS server would be one of the more likely places on your network where it would already be installed. See the help on the **ADVANCED > Secure Administration** page for instructions.

8.7 Outbound Footers

Use the **ADVANCED > Outbound Footers** page to add a footer to each outbound message processed by the Barracuda Email Security Gateway.

Make sure to use the same character set in the footer that you'll use in outbound messages. If you are use multiple character sets, the footer text may not be displayed properly.

- **Attach Footer** - Indicate whether or not to attach a footer to each outbound message.
- **Text Footer** - Text/ASCII version of footer text.
- **HTML Footer** - HTML version of footer text.

8.7.1 Footer Exemptions

Use this section of the page to exclude email addresses from having a footer appended to their messages.

- **Email Addresses** - Messages sent from these email addresses will not have a footer appended to them. Enter one email address per line.

8.8 Explicit Users

8.8.1 Explicit Users to Scan For

(Available on certain models) You can specify a list of email addresses that will be scanned for spam or viruses. If there are any entries listed in email address field, no other accounts will be scanned for spam. Accounts added to this list have spam protection. RBLs, rate control, virus checking and recipient validation are applied to all incoming mail regardless of this list. Use the **Explicit Users to Scan For** option to test a subset of users before fully deploying the Barracuda Email Security Gateway.

IMPORTANT:

Do not use Trusted Relays in conjunction with Explicit Users to Scan For feature.

8.8.2 Explicitly Accepted Users and Alias Linking

if LDAP or Active Directory are NOT available to verify the authenticity of the recipient's email address, use the **Explicitly Accepted Users** feature for recipient verification. In the **Explicitly Accepted Users and Alias Linking** text box on the **ADVANCED > Explicit Users** page, specify a list of valid recipients (**Explicitly Accepted Users**) for which the Barracuda Email Security Gateway should accept email. Enter one email address per line.

Set Only accept email for these recipients:

- **Yes** - Restricts incoming email to the specifically listed addresses. All other incoming email will be rejected.
- **No** - Causes incoming email recipients to be checked against this list first, before proceeding to other verification modes. Any per-domain lists of Explicitly Accepted Users will be checked in this case.

Use the **Alias linking** feature to help you manage multiple quarantine inboxes with one 'primary' account if you are using per-user quarantine. You can enter multiple email addresses to be linked to that primary account in the **Explicitly Accepted Users and Alias Linking** text box. These accounts can be on the same domain or different domains.

The Alias Linking feature provides for the following:

- You can designate a 'primary' user account to associate with other user accounts such that each email address linked with the primary can log into the Barracuda Email Security Gateway to view their quarantined messages using the same password as the primary user account (the first in the list).

- When you link accounts, if the linked accounts (listed after the primary) don't yet exist, they will not be created, but those email addresses can be used as aliases for logging in with the same password as the primary account. If the linked accounts listed after the primary account already exist, those account passwords will expire and those users must log in with the primary account password.
- All quarantined mail for those linked accounts will be forwarded to the primary account quarantine mailbox. For example, you might want all quarantined mail for a domain to go to one user account on that domain.

See the help on the **ADVANCED > Explicit Users** page to configure Alias Linking.

Examples of Alias Linking:

- Email address with aliases where the first email address is in a different domain. All quarantined email will be routed to bsmith@abc.com:
  - bsmith@abc.com bob@xyz.com bobby@xyz.com
- Entire domain delivered to a single primary account. All quarantined email addressed to abcd.com will be routed to primaryBox@abcd.com:
  - primaryBox@abcd.com @abcd.com

If you have multiple domains it may be easier to maintain a list of Explicitly Accepted Users and Alias Linking lists on a per-domain basis. You can do this by navigating to the **DOMAINS > Manage Domain > USERS > Valid Recipients** page for each domain.

The number of entries in the text box for Explicitly Accepted Users and Alias Linking is limited based on the model of Barracuda Email Security Gateway. On models 600 and lower the maximum is 1000 and on models 800 and above the limit is 5000 per domain and in this global list.

8.9 Bounce/NDR Settings

Bounce notifications and Non-Delivery Receipts (NDRs) are configured for various features of the Barracuda Email Security Gateway including quarantine, and blocking of messages for various reasons.

8.9.1 Spam NDR (Bounce) Configuration

- **NDR on Block** - Controls whether notifications are sent to senders when a message is blocked due to spam scoring. The recommended setting is No. When considering this setting, keep in mind that if the email came from an illegitimate source such as a spammer, sending a bounce notification is not necessary. Additionally, many spammers spoof valid domains, and you don't want to send bounce messages to your domain if it is being spoofed. Sending bounce messages to illegitimate senders is known as 'backscatter'. Backscatter can increase the load on your Barracuda Email Security Gateway and may generate a lot of email to fake addresses. Configurable for inbound and outbound messages.
- **Check SPF for NDR Recipients** - When a bounce message is about to be sent, the **Check SPF for NDR Recipients** option first validates the email against the sender's Sender Policy Framework (SPF) records; if the email passes the SPF rules, the bounce message will be sent. If there are no SPF records, the bounce will not be sent.

  This configuration option differs from the **SPF Configuration** settings on the **BLOCK/ACCEPT > Sender Authentication** page in that the **SPF Configuration** settings decide whether SPF lookups should be used to determine the spam status of a message, whereas the **Check SPF for NDR Recipients** option decides whether an SPF lookup should be performed after a message has already been determined to be spam. This is to avoid sending email bounces to forged sender addresses.

  Regardless of this setting, no bounce message will ever be issued for messages that were determined to be spam because of SPF match failures; thus, it is unnecessary to enable this option if general SPF checking has been enabled.

8.9.2 Quarantine NDR configuration (Outbound Only)

Select Yes to send a notification to the sender of an outbound message that the Barracuda Email Security Gateway quarantines. Select No to disable sending the notification if you don't anticipate quarantined outgoing messages or want to avoid additional email traffic to your users.

8.9.3 Attachment Content Block Notification

Notifications are sent to the sender when an email message is blocked due to attachment content filtering policies.

- **Notify on Content-Based File Interception** - If this option is set to **Yes**, a bounce message is sent to the sender indicating that an email was blocked by the Barracuda Email Security Gateway and the reason the email was blocked. Configurable for inbound and outbound messages.

8.9.4 Virus NDR (Bounce) Configuration

Configure notifications to intended recipients and/or admin when messages are blocked due to a virus.

- **Notify Intended Recipient of Virus Interception** - For inbound mail only, set to **Yes** if you want to have a non-delivery report (NDR) sent to the intended recipient of a message that was blocked because it contained a virus.
- **Notify Admin of Virus Interception** - For inbound and outbound mail, set to Yes if you want to have a non-delivery report (NDR) sent to the administrator when a message is blocked because it contained a virus. The NDR is sent to the **System Alerts Email Address** as configured on the **BASIC > Administration** page.

8.9.5 Bounce/NDR Language and Text

This section of the page displays the text that will be used in the designated situations. If the selected NDR message language is Custom, then the text of the NDRs can be edited in this section.

Each text area must have the header separated from the body with a blank line. It is recommended that the header portion of the message contain the word Subject. The Subject line of text should then be followed by a blank line, then followed by the body of the message.

See the **ADVANCED > Bounce/NDR Settings** page for more details on customizing bounce messages.

8.10 Clustering

Clustering two or more Barracuda Email Security Gateways makes sense if your organization requires high availability, scalability, data redundancy and/or fault tolerance. Clustering also provides centralized management of policy because once you configure one of the devices, configuration settings are synchronized across the cluster almost immediately. Clustered systems can be geographically dispersed and do not need to be located on the same network.

8.10.1 Features and benefits of clustering

Clustering Barracuda Email Security Gateways enables organizations to meet their high availability and fault tolerance requirements while also providing centralized management of policy, scalability and data redundancy. Linking multiple Barracuda Email Security Gateways is easy to do with a few parameter settings, and once you configure one of the devices, configuration settings are synchronized across the cluster almost immediately. Clustered systems can be geographically dispersed and do not need to be located on the same network.

- **Centralized Policy Management** – You can configure your spam, virus, and custom email delivery policies from any Barracuda Email Security Gateway in the cluster – all changes are immediately replicated to the other Barracuda Email Security Gateways in the cluster. Alternatively, you can designate one Barracuda Email Security Gateway as the "host" from which to perform administration of the cluster. To do this, you would simply set that device to be the "Quarantine Host" and not direct any email traffic to it. There are two benefits to this configuration:
  - Enables you to tighten security by restricting web interface access to only one Barracuda Email Security Gateway in the cluster
  - Optimizes performance of the Web interface by isolating it from the impact of spikes in email volume on the network
- **Data Redundancy and Guaranteed Configuration Updates** – Quarantined messages are replicated across the cluster such that each user has a primary quarantine inbox on one Barracuda Email Security Gateway and a secondary inbox on another Barracuda Email Security Gateway. This redundancy and fault tolerance ensure that all user data remains available if a single node in the cluster fails.
- **Federated Search** – Clustering Barracuda Email Security Gateways provides you with a centralized view of all messages in a cluster through a distributed database architecture. With federated search, you can locate any messages across the cluster by issuing a query from any single Barracuda Email Security Gateway. This distributed database architecture restricts network traffic to only messages returned with query results.

- **Scalability** – As your email traffic volume grows, you can simply add one or more additional Barracuda Email Security Gateways.

  Note that clustering is supported on Barracuda Email Security Gateway models 400 and higher, and each Barracuda Email Security Gateway in the cluster must be the same model.

- **Secure Access and Data Transmission** – Clustering utilizes encrypted and secure communications for user access, message replication and configuration synchronization across the cluster.
- **Restricted Access to Configuration** – Transmission of configuration data between devices on the cluster is secured by a shared password, or "shared secret", which the administrator creates and assigns to every Barracuda Email Security Gateway. This prevents access to configuration parameters from other Barracuda Email Security Gateways outside the cluster or other network devices.
- **Limiting User Access** – As mentioned above, you can choose to dedicate one Barracuda Email Security Gateway on the cluster as the "Quarantine Host" to limit users' access to that node when checking their quarantine inboxes. In this configuration, quarantine notifications from all Barracuda Email Security Gateways in the cluster will direct users to that Quarantine Host, and you would direct all email to the **other** nodes on the cluster.

How to Cluster the Barracuda Email Security Gateway

Note that clustered systems can be geographically dispersed and do not need to be located on the same network. Important: Every Barracuda Email Security Gateway in a cluster must meet the following requirements:

- Be the same model (400 and above).
- Have the same version of firmware installed.
- Be configured for the same time zone.
- Have a unique external IP address. This means that every Barracuda Email Security Gateway behind a NAT must have a unique external IP address and must be reachable by that external IP address.

Follow instructions in the Barracuda Campus article How to Cluster the Barracuda Email Security Gateway or in the help on the **ADVANCED > Clustering** page.

8.10.2 Limiting End-user Access to the Cluster

You can dedicate a single Barracuda Email Security Gateway as the **Quarantine Host** to serve up the end-user interface through which users will access their quarantine inboxes, even though their actual quarantine inbox (primary or secondary) may be hosted by another Barracuda Email Security Gateway in the cluster. By not directing email to the Quarantine Host, you can:

- Enhance network security by limiting end-user access (port 8000 by default) and administration to only one Barracuda Email Security Gateway on the Internet
- Insulate the user interface performance from any peaks in email volume

To configure one Barracuda Email Security Gateway as the Quarantine Host, from the **BASIC > Quarantine** page, enter that system's hostname in the **Quarantine Host** field.

Removing a Barracuda Email Security Gateway From a Cluster

1. Log into the system to be removed and change or clear the **Cluster Shared Secret** on the **ADVANCED > Clustering** page.
2. Click **Save Changes**.

   Changing the cluster shared secret prevents the systems in the cluster from communicating with one another.
3. On the same system, delete all other systems from the **Clustered Systems** list.
4. On any system that remains in the cluster, go to the **ADVANCED > Clustering** page. In the **Clustered Systems** list, delete the system to be removed from the cluster. This step is very important when removing a failed Barracuda Email Security Gateway from a cluster.

8.10.3 Exporting the Message Log

In a clustered environment, the maximum number of lines in a Message Log export is 10,000. To export more lines, use the Date Range feature in your Message Log search. For more information, see How to Export the Message Log in Barracuda Campus.

8.10.4 Centralized Policy Management With a Quarantine Host

You can optionally designate one Barracuda Email Security Gateway as the "host" of the cluster such that all administration of configuration settings and access to per-user quarantine for the cluster can only be accessed and set from that node. This option has two advantages: it provides for additional security by limiting access to administration of the cluster, and it protects the user interface from mail processing load since, with this configuration, you do not direct any email traffic to the host node.

To assign one Barracuda Email Security Gateway as the host of the cluster, enter the hostname of that device in the Quarantine Host field on the **BASIC > Quarantine** page and do not direct any email to that device.

8.10.5 Redundancy of user quarantine data on the cluster

Each user account has a primary and backup server in the cluster. Regardless of how many Barracuda Email Security Gateways there are in the cluster, there are always two appliances that have the same quarantine information (configuration and quarantine messages).

8.10.6 Data Not Synchronized Across the Cluster

Clustering provides 100% redundant coverage of the propagated data. However, for practical reasons, some data is not propagated to the other clustered systems when a new system joins. Energize updates do not synchronize across systems in a cluster. The following Barracuda Email Security Gateway configurations are considered unique and will not sync to match other Barracuda Email Security Gateways in a cluster:

- IP Address, Subnet Mask, and Default Gateway (on the **BASIC > IP Configuration** page)
- Primary DNS Server and Secondary DNS Server (on the **BASIC > IP Configuration** page)
- Serial number (this will never change)
- Hostname (on the **BASIC > IP Configuration** page)
- Any advanced IP configuration (Barracuda Email Security Gateway 600 and above, on the **ADVANCED > Advanced Networking** page)
- Administrator password
- Guest password
- Time Zone (on the **BASIC > Administration** page)
- Cluster hostname (on the **ADVANCED > Clustering** page)
- Cluster Shared Secret, though this must be the same for the cluster to work properly (on the **ADVANCED > Clustering** page)
- Local Host Map (on the **ADVANCED > Clustering** page)
- SMTP Welcome Banner (on the **ADVANCED > Email Protocol** page)
- SMTP Port (on the **BASIC > Outbound** page)
- Web Interface HTTP Port (on the **BASIC > Administration** page)
- Web Interface HTTPS/SSL port (on the **ADVANCED > Secure Administration** page)
- Any other secure administration configuration, including saved certificates (on the **ADVANCED > Secure Administration** page)
- Quarantine Host (on the **BASIC > Quarantine** page)

- All SSL/TLS information, including saved certificates (on the **ADVANCED > Secure Administration** page)
- Whether to only display local messages in the message log (Only view local messages on the **BASIC > Message Log > Preferences** page)
- Whether the latest release notes have been read
- All customized branding (Barracuda Email Security Gateway 600 and above, on the **ADVANCED > Appearance** page)

8.11 Appearance

The **ADVANCED > Appearance** page settings are used throughout the Barracuda Email Security Gateway.

- **System Name**: The name used for references to the Barracuda Email Security Gateway. This name is used on the web interface and for per-user quarantine correspondence. Special characters, multibyte and high ASCII characters are not allowed.

8.11.1 Web Interface

These settings affect the web interface appearance.

- **Image** shows the current image to use on the web interface in place of the Barracuda Networks logo.
- **Upload New Image** allows a new logo to be uploaded for the web interface. The recommended size is 160x65 pixels and must be of one of the following file types: jpg, gif, or png. The file size must be under 100KB.
- **Image URL** is the URL to which the user is directed when the web interface logo is clicked.
- **Reset** reverts the web interface image to the factory default and clears out any values entered in the Image URL field.

8.11.2 Quarantine Email

- **Image** shows the current image that will be used in the quarantine messages sent to users.
- **Upload New Image** allows a new image to be uploaded for use in quarantine summary messages. The recommended size is 480x66 pixels and must be of one of the following file types: jpg, gif, or png. The file size must be under 100KB.
- **Reset** reverts the quarantine email image to the factory default.

8.12 LDAP Routing

8.12.1 LDAP Routing Directory Server Configuration

The LDAP routing feature provides two different ways to use data stored in your LDAP server. First, if you have different email users' accounts on different servers all referenced by the same LDAP, then you can use this feature to forward mail to the correct server. Second, you can map external email addresses to internal email addresses based on information stored in LDAP.

Use the **ADVANCED > LDAP Routing** page to configure:

- To provide for failover from one LDAP server to another, enter multiple LDAP hostnames or IP addresses in the **LDAP Server** field, with each separated by a space character.
- LDAP Routing is a ***global*** setting. When enabled, these settings will take precedence over any other destination server settings defined on the **DOMAINS > Domain Manager** page. When an email comes in for a user, an LDAP lookup is performed for that user. If there are no results, then the mail server defined for the user's domain in the **DOMAINS > Domain Manager** page is used.

Configure the following so that the Barracuda Email Security Gateway can connect to the LDAP server.

Click **Save** when complete.

- **LDAP Server** - The hostname or IP address of the server that is utilized for LDAP lookups.
- **LDAP Port** - Port used to connect to the LDAP service on the specified LDAP Server. Typically port 389 is used for regular LDAP and LDAP using the StartTLS mode for privacy. Port 636 is assigned to the LDAPS service (LDAP over SSL/TLS).

  For organizations using Active Directory for their LDAP server and which have multiple domains serviced from separate servers, the Barracuda Email Security Gateway may need to read the LDAP directory from the ***Global Catalog***. The Global Catalog is a virtual LDAP tree which the primary domain controller constructs and which unifies disparate domain views. If available, the Global Catalog is typically found on port(s) 3268 and/or 3269, which are analogous to 389 and 636, respectively.
- **Bind DN (Username)** - Distinguished Name (DN) of a user in your directory that has read access to all information about valid users.
- **Bind Password** - Password for the user specified in Bind DN.
- **LDAP Search Base** - The starting search point in the LDAP tree. For example, if your domain is test.com, your search base DN might be `dc=test,dc=com`.

8.12.2 Destination Mail Server Mapping (DMSM)

This allows customers with multiple email accounts on different servers all referenced by the same LDAP to forward mail sent to an account to the correct server. The LDAP entry for the user holds attributes telling which server their account is stored on. The Barracuda Email Security Gateway will query these attributes when looking up the user so the email message will be forwarded to the correct server. If the Destination Mail Server Attribute is not defined, then the destination mail server(s) defined on the Domains > Domain Manager page will be used for message delivery.

See the help on the **ADVANCED > LDAP** Routing page to configure.

8.12.3 Alias Rewriting Configuration

Alias rewriting is typically used to map external email addresses to internal email addresses based on information stored in LDAP. For example, you could map the external address *sue@domain.com* to the internal address *sue@localdomain.net*.

- **Enable Alias Rewriting** - Enable rewriting of recipient email address based on LDAP lookup.
- **LDAP Search Filter** - Use the following filters to look for the correct alias mapping:
  - **%s** - for recipient address
  - **%u** - for the username part of the email address
  - **%d** - for the domain part of the email address
- **Alias Attribute** - The LDAP attribute containing the alias email address for each user. In OpenLDAP installations, the attribute that is populated for rewriting is usually mailLocalAddress OR mailRoutingAddress.

8.13 Exchange Antivirus

8.13.1 What is the Barracuda Exchange Antivirus Agent?

The Barracuda Exchange Antivirus Agent is a Microsoft Exchange Server transport agent that works with the Barracuda Email Security Gateway to scan internally generated mail, as well as external mail traffic, for viruses, thereby limiting the inadvertent spread of infected attachments. The Barracuda Exchange Antivirus Agent only scans messages with attachments, including embedded messages with attachments. It does not scan text-only attachments (such as HTML), message headers, bodies, or in-line attachments. Mail that has already been scanned by the Barracuda Email Security Gateway is also scanned by the Barracuda Exchange Antivirus Agent.

Important:

- With the Barracuda Exchange Antivirus Agent installed, messages that are deemed malicious are **deleted** and will not be quarantined.
- You cannot run multiple Exchange Antivirus engines at the same time on the same server. You can, however, have a file-level antivirus engine and one Barracuda Exchange Antivirus Agent engine running on the same server.
- If you have a file-level antivirus antivirus engine running with the Barracuda Exchange Antivirus Agent engine, then you need to exempt the following directories and files from the file-level antivirus scan:
  - C:\Program Files\Barracuda
  - C:\Windows\Temp\BAR*.*

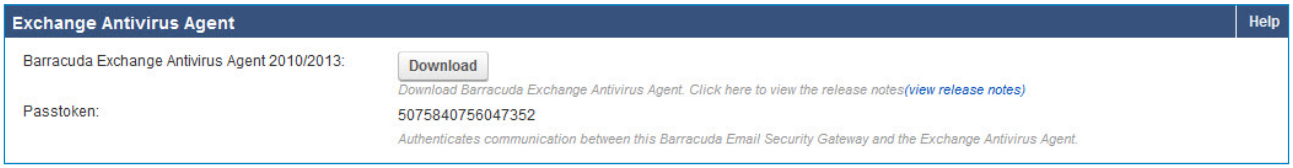
You can download the transport agent as described below from your Barracuda Email Security Gateway and install it on all Exchange servers with the Hub Transport role. If you want to scan outbound mail for viruses, you also need to install the agent on Exchange servers with the Edge Transport role. The Barracuda Exchange Antivirus Agent updates virus signatures hourly and scans messages:

- between local mailboxes
- between the Internet and local mailboxes

Microsoft Exchange Server does not support the Barracuda Email Security Gateway quarantine tool for viewing infected messages, information on false positives, or other infected message details. All threat statistics that Microsoft Exchange Server provides to the Barracuda Exchange Antivirus Agent are listed in the **Exchange Antivirus Statistics** section of the **ADVANCED > Exchange Antivirus** page on the Barracuda Email Security Gateway web interface.

Download the Agent

1. Log into the Barracuda Email Security Gateway as admin and go to the **ADVANCED > Exchange Antivirus** page.
2. Click the **Download** button and, when prompted, save the file.



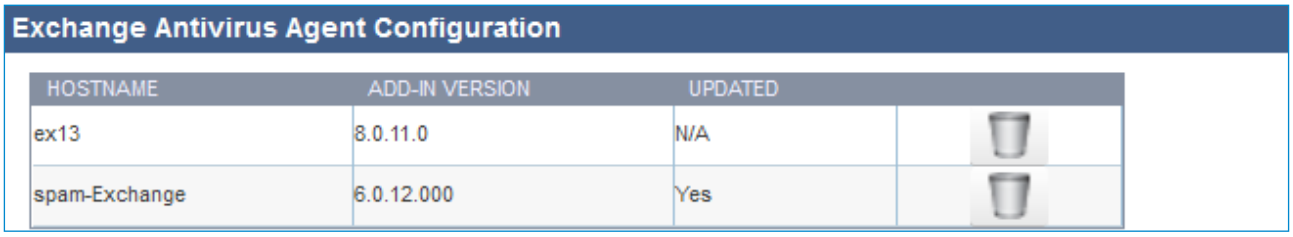
Install the Agent

To install the Barracuda Exchange Antivirus Agent on Exchange Server 2013 or higher, you must be a member of an Exchange Server Organization Management security group. If you have recently added yourself to this group, please log out before re-running the installer. Before installing the Barracuda Exchange Antivirus Agent, set the **Automatic Update** option to **On** for **Virus Definitions** on the **ADVANCED > Energize Updates** page on the Barracuda Email Security Gateway. For either version of Exchange Server, perform the following steps:

1. Log into Microsoft Exchange Server as an administrator.
2. Use the browser on your Microsoft Exchange Server to connect to the Barracuda Email Security Gateway web interface.
3. Log into Barracuda Email Security Gateway as **admin** and navigate to the **ADVANCED > Exchange Antivirus** page.
4. In the **Exchange Antivirus Agent** section, click **Download** for the Barracuda Exchange Antivirus Agent that works with your version of Exchange Server.
5. Run the Windows Installer. Follow the setup wizard instructions.
6. Click **Finish** when the wizard completes installing the agent. Once installed, the Barracuda Exchange Antivirus Agent is active and begins providing virus protection.

View Exchange Servers in the Barracuda Email Security Gateway web interface

After you have installed the Barracuda Exchange Antivirus Agent, refresh the **ADVANCED > Exchange Antivirus** page to view a list of Exchange Servers in a table in the **Exchange Antivirus Configuration** section. The table will look something like this:



8.13.2 Exchange Antivirus Agent Statistics

Once you've installed the Barracuda Exchange Antivirus Agent on your Exchange Server, you can refresh the **ADVANCED > Exchange Antivirus** page and see statistics about messages processed and quarantined by the agent.

- **Items Scanned** - Total number of messages scanned, including quarantined messages, by the Barracuda Exchange Antivirus Agent.
- **Attachments Scanned** - Number of files scanned, including those attached to quarantined messages.

8.13.3 Threats Blocked

Anything that is reported as malware by the Barracuda Exchange Antivirus Agent running on your Exchange Server will be listed in this section of the page.

8.14 Remote IMAP/POP

The Barracuda Email Security Gateway provides an email-retrieval and forwarding utility which fetches email from remote mail servers and forwards it to your local machine's delivery system. You can repeatedly poll each account at a specified interval. This utility can gather mail from servers supporting POP3 and IMAP and is configured from the **ADVANCED > Remote IMAP/POP** page.

Note that all email will be DELETED from the remote mail server after retrieval by the Barracuda Email Security Gateway.

There are two types of operations for each account from which the **Remote Accounts** utility retrieves mail: Global and User. With the User type, it is assumed that all messages in the user's account are intended for a single recipient. The Global type is used when multiple recipients under the same domain are specified for a particular server account.

From the **ADVANCED > Remote IMAP/POP** page you can specify polling interval, SSL (yes/no), user account passwords and email addresses.

Configure Remote Accounts

You can configure these fields on the **ADVANCED > Remote IMAP/POP** page for remote accounts:

- **Server Name/IP** - The hostname or IP address of the remote mail server.
- **Polling Interval (seconds)** - The time interval at which the Remote Accounts utility will poll the specified account. The interval must be a multiple of 30 seconds with a minimum value of 30.
- **Protocol** - The protocol defined: POP3 or IMAP.
- **Port** - Defines the port to listen on the remote mail server from which email will be fetched. By default, this field is not set (blank), which means following the defined **Protocol**, which is 110 for POP3 and 143 for IMAP.
- **SSL** - Used to indicate whether or not SSL is being used.
- **User** - The username of the remote mail server account.
- **Password** - The password of the remote mail server account.
- **Type** - The type of operation for retrieval: either **Global** or **User**.
- **Email Address/Domain** - Defines either the destination email address for a single recipient or the domain name for multiple recipients. When **Type** is set to **Global**, this entry defines the domain which will be used to determine per-domain processing rules. Only email whose recipients match this domain will be processed. When **Type** is set to **User**, this entry defines the email address to which all fetched email for this account will be delivered.

8.15 Queue Management

The Queue displays inbound email messages that are queued for scanning and delivery, and outbound messages that have been scanned and are queued for delivery. This queue only displays email that is 'local' to this Barracuda Email Security Gateway. If this appliance is part of a cluster, messages queued on the other Barracuda Email Security Gateways in the cluster will not appear in this queue.

The **ADVANCED > Queue Management** page is divided into 2 panes:

- The queue contains various details of the messages
- The Preview Pane, when enabled, appears on the right, left or bottom and displays the contents of a message

Click on a message in the queue to view it in the Preview Pane, or double-click on it to bring it up in a separate Message Details browser window.

See the help in the **ADVANCED > Queue Management** page for details on the information provided in the queue, managing the queue and re-queuing messages.

8.16 Backups

8.16.1 Three Kinds of Backup Files

The **ADVANCED > Backup** page lets you back up and restore three kinds of backup files for your Barracuda Email Security Gateway:

- System configuration
- Bayesian databases - global and per-user (if your model supports per-user)
- Explicit Users to Accept For and Alias Linking data

You should back up your system on a regular basis in case you need to restore this information on a replacement Barracuda Email Security Gateway or in the event that your current system data becomes corrupt.

To prepare the system for backing up, first configure your backup server information, then select which, if not all, backups you want to create, and, if desired, a schedule of automated backups on the **ADVANCED > Backup** page. If you are restoring a backup file on a new Barracuda Email Security Gateway that is not configured, you first need to assign your new system an IP address and DNS information on the **BASIC > IP Configuration** page of the new system.

Important notes about backups:

- **Do not edit backup files**. Any configuration changes you want to make need 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.
- You can safely view a backup file in Windows WordPad or TextPad. You should avoid viewing backup files in Windows Notepad because the file can become corrupted if you save the file from this application.
- The firmware version running on the system when the backup file was generated should match the firmware version on the system you are restoring onto. If it does not match, you will see a warning at the top of the page when you attempt to restore.
- **Information not backed up with the system configuration file** includes system password, system IP information, DNS information and clustering settings. For a complete list of settings that are not backed up, please click the **Help** button on the **ADVANCED > Backup** page.
- For Automated Backups, you must select a server type. If you select FTP, note the following. The Barracuda Email Security Gateway, by default, initiates ftp in passive mode. **If your backup times out**, and your ftp server is running in passive mode, and you have a firewall between your Barracuda Email Security Gateway and your ftp server, you may need to open ports on your firewall to allow passive-mode ftp connections. The port range depends on your ftp

server configuration. Ideally, the firewall should be configured so that only that range of ports is accessible to the ftp server machine. Make sure that there aren't any other TCP services with port numbers in the port range listening on the ftp server machine.

Restoring a Backup

Restoring a backup simply requires browsing your local system with the click of a button on the **ADVANCED > Backup** page and selecting a backup file. Please click the **Help** button on that page for details about restoring backups.

- Do not restore a configuration file onto a machine that is currently part of a cluster. All cluster information will be lost and the units will need to be re-clustered if this happens.
- If you need to restore a backup from one Barracuda Email Security Gateway model to a different model, please contact Barracuda Technical Support before proceeding. Note that settings on one model may not apply to a different model.

See the help on the **ADVANCED > Backups** page for more details.

8.17 Troubleshooting

The following diagnostic tools should help you troubleshoot most problems. See also Replacing a Failed System in Barracuda Campus.

8.17.1 Basic Troubleshooting Tools

The **ADVANCED > Troubleshooting** page provides a suite of tools that help troubleshoot network connectivity issues that may be impacting the performance of your Barracuda Email Security Gateway.

For example, you can test your Barracuda Email Security Gateway's connection to the Barracuda Networks update servers to make sure that it can successfully download the latest Energize Update definitions. You can also ping or telnet to other devices from the Barracuda Email Security Gateway, perform dig/NS-lookup, TCP dump and perform a trace route from the Barracuda Email Security Gateway to any another system.

8.17.2 Connect to Barracuda Support Servers

In the Support Diagnostics section of the **ADVANCED > Troubleshooting** page, you can initiate a connection between your Barracuda Email Security Gateway and the Barracuda Networks Technical Support Center which will allow technical support engineers to troubleshoot any issues you may be experiencing.

8.17.3 Rebooting the System in Recovery Mode

If your Barracuda Email Security Gateway experiences a serious issue that impacts its core functionality, you can use diagnostic and recovery tools that are available from the reboot menu (see below) to return your system to an operational state.

Before using the diagnostic and recovery tools, the administrator should do the following:

- Use the built-in troubleshooting tools on the **ADVANCED > Troubleshooting** page to help diagnose the problem.
- Perform a system restore from the last known good backup file.
- Contact Barracuda Networks Technical Support for additional troubleshooting tips.

As a last resort, you can reboot your Barracuda Email Security Gateway and run a memory test or perform a complete system recovery, as described below.

To perform a system recovery or hardware test:

1. Connect a monitor and keyboard directly to your Barracuda Email Security Gateway.
2. Reboot the system by doing one of the following:

   - In the web interface: Go to the **BASIC > Administration** page, navigate to the **System Management** section, and click **Restart**.

- At the front panel of the Barracuda Email Security Gateway: Press the **Power** button on the front panel to turn off the system, and then press the **Power** button again to turn the system on.

The splash screen displays with the following three boot options:

- Barracuda
- Recovery
- Hardware_Test

3. Use your keyboard to select the desired boot option, and press the **Enter** key. You must select the boot option within three seconds after the splash screen appears. If you do not select an option within three seconds, the Barracuda Email Security Gateway starts up in Normal mode (first option). For a description of each boot option, refer to Reboot Options below.

To stop a hardware test, reboot your Barracuda Email Security Gateway by pressing the Ctrl-Alt-Del keys.

Reboot options

The table below describes the options available at the reboot menu.

Reboot options	Description
Barracuda	Starts the Barracuda Email Security Gateway in the normal (default) mode. This option is automatically selected if no other option is specified within the first three seconds of the splash screen appearing.
Hardware_Test	Performs a thorough memory test that shows most memory related errors within a two-hour time period. The memory test is performed outside of the operating system and can take a long time to complete. Reboot your Barracuda Email Security Gateway to stop the hardware test.
Recovery	Displays the Recovery Console, where you can select the following options: • **Barracuda Repair (no data loss)** – Repairs the file system on the Barracuda Email Security Gateway. • **Full Barracuda Recovery (all data lost)** – Restores the factory settings on your Barracuda Email Security Gateway and clears out the configuration information. • **Enable remote administration (reverse runnel)** – Turns on reverse tunnel that allows Barracuda Networks Technical Support to access the system. Another method for enabling remote administration is to click Establish Connection to Barracuda Support Center on the ADVANCED >Troubleshooting page. • **Diagnostic memory test** – Runs a diagnostic memory test from the operating system. If problems are reported when running this option, Barracuda recommends running the Hardware_Test option next.

8.18 Task Manager

8.18.1 Using the Task Manager to Monitor System Tasks

The **ADVANCED > Task Manager** page provides a list of tasks that are in the process of being performed and displays any errors encountered when performing these tasks. Some of the tasks that the Barracuda Email Security Gateway tracks include:

- Clustered environment setup
- Configuration and Bayesian data restoration
- Removal of invalid users

If a task takes a long time to complete, you can click the **Cancel** link next to the task name and then run the task at a later time when the system is less busy. The **Task Errors** section will list an error until you manually remove it from the list. The errors are not automatically phased out over time.

8.18.2 Running Tasks

All background tasks that are currently running on the Barracuda Email Security Gateway are listed in this section of the page. Click the **Cancel** link next to a task name to stop that task from running.

8.18.3 Task Errors

If any task scheduled by the Administrator results in an error, this task remains in this list on the page until manually removed by the Administrator.

Understanding the Message Log

9.1 How The Message Log Works

One of the most powerful monitoring tools on the Barracuda Email Security Gateway is the Message Log, which displays details about all email traffic that passes through the Barracuda Email Security Gateway. Information displayed inside the Message Log can be one of the best analysis tools to determine if your block/allow policies are correct for your organization and for tuning those policies.

You can view message source and analysis by clicking on a message; you will also see spam scoring for the message and Bayesian analysis, if enabled.

- This data is captured initially in the Mail Syslog and appears on the mail facility at the *debug priority* level on the specified syslog server.
- The Message Log stores data for up to 6 months.
- Actual number of messages are allocated 75% of available storage, which includes quarantine messages.
- If the organization needs to access more message log data than 6 months' worth, Barracuda recommends using a syslog server or a Message Archiver.

9.1.1 Secured Message Contents

- When the Encryption feature is enabled on the Barracuda Email Security Gateway, the message body will not be displayed on the **BASIC > Message Log**, **BASIC > Outbound Quarantine**, or the **ADVANCED > Queue Management** pages.

Only the sender of the encrypted message(s) and the recipient can view the body of a message encrypted by the Barracuda Email Encryption Service. For Mail Journaling and the download features in the Message Viewer of the Message Log, the message body will not be sent to the Mail Journaling account and cannot be downloaded to the Desktop.

9.1.2 Exporting the Message Log

- The Message Log contents can be exported, but not the actual messages. To export Message Log entries, click the **Export** drop-down and select either **Export Selected** or **Export All**.
- In a clustered environment, the maximum number of lines in a Message Log export is 10,000.

9.2 Message Log Filters

The Message Log is a window into how the current spam and virus settings are filtering email coming through the Barracuda Email Security Gateway, and sorting data using the wide variety of filters can quickly provide a profile of email by:

- allowed messages
- deferred messages
- tagged messages
- quarantined messages
- blocked messages

Messages can be sorted by:

- domain
- sender
- recipient
- time
- subject
- size
- reason for action taken
- score

...as well as other filters. See the **BASIC > Message Log** page for more information on filtering.

Watch the Message Log after making changes to the spam and virus settings to determine if the Barracuda Email Security Gateway spam checking and quarantine behavior is tuned per the needs of the organization.

9.2.1 Monitor and Classify Outgoing Emails

If the Barracuda Email Security Gateway has been configured to filter outbound mail, watch the log on the **BASIC > Outbound Quarantine** page. Based on **Outbound Spam Scoring Limits** you specify on the **BASIC > Spam Checking** page, as well as any Block/Accept filters you configure, outbound messages will be quarantined or blocked as needed and listed on the **BASIC > Outbound Quarantine** page. Look for false positives and adjust spam scoring accordingly. Any message listed in the outbound quarantine can be delivered, whitelisted, deleted, or rejected by an administrator.

Cloud Protection Layer

10.1 Introducing Barracuda Cloud Control

Barracuda Cloud Control is free and enables administrators to manage, monitor and configure multiple Barracuda Email Security Gateways at one time from one console. If you are using the Cloud Protection Layer (CPL) feature of the Barracuda Email Security Gateway, you will manage it using Barracuda Cloud Control. For information specific to the Barracuda Cloud Control product configuration and management, see the Barracuda Cloud Control Overview.

The same tabbed pages are available on the Barracuda Cloud Control for managing all aspects of your Barracuda Email Security Gateway configuration that you see in each individual web interface, and you can create aggregated reports for multiple Barracuda Email Security Gateways from the Barracuda Cloud Control console.

Use CPL for:

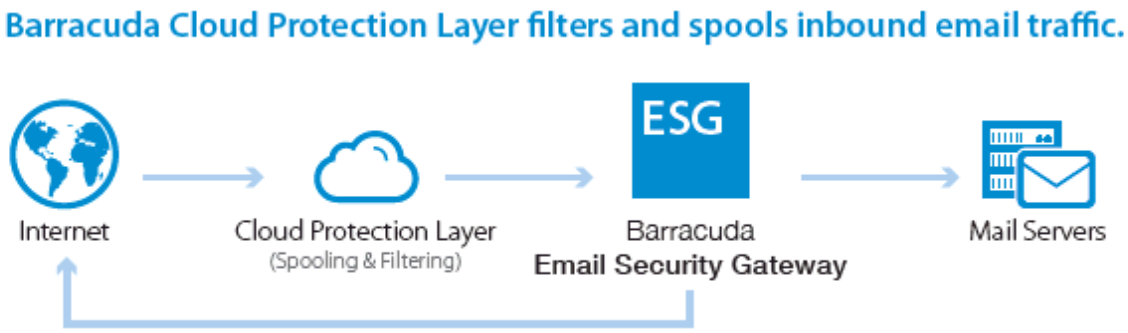
- Blocking threats before they reach your network
- Advanced Threat Protection in the cloud
- Preventing phishing and zero day attacks
- Email continuity when your mail server goes down – if the mail server becomes unavailable, mail is spooled for up to 96 hours.

You need to configure Barracuda Cloud Control on the **ADVANCED > Cloud Control** page of the Barracuda Web Security Gateway, as covered in the **Cloud Control** section of this handbook.

10.2 Features of the Barracuda Cloud Protection Layer

The optional Cloud Protection Layer feature of the Barracuda Email Security Gateway is an additional layer of cloud-based protection that blocks threats before they reach the network, prevents phishing and zero day attacks, and provides email continuity.

Once email passes through the Cloud Protection Layer, the Barracuda Email Security Gateway filters email according to the more granular policies, further recipient verification, quarantining, and other features you configure on the appliance or virtual machine. Use Barracuda Cloud Control for access to CPL and for central management of multiple Barracuda Email Security Gateway(s).



10.2.1 Features of CPL

- Email Continuity:
  - polls mail server regularly
  - spools mail up to 96 hours if mail server goes down
- Advanced Threat Protection (ATP) –
  - Optional, subscription-based
  - Protects against advanced malware, zero-day exploits, and targeted attacks not detected by the Barracuda Email Security Gateway virus scanning features.
  - ATP service analyzes inbound email attachments in a separate, secured cloud environment, detecting new threats and determining whether to block such messages.
- Link Protection – Rewrites a deceptive URL in an email message to a safe Barracuda URL and delivers that message to the user.
- Typosquatting protection –
  - Checks for common typos in the URL domain name in email message
  - Rewrites misspelled URLs to correct domain name so that the user visits the intended website.

- Email surge suppression during peak traffic and spam spikes, which offloads a significant volume of spam email from your Barracuda Email Security Gateway to be filtered via the cloud.
- Automatic updates in real time, leveraging threat intelligence from Barracuda Labs and Barracuda Central to continuously stay ahead of quickly morphing threats.
- Enhanced Spam accuracy: CPL submits sender domains to BRTS to help improve spam accuracy, and checks whether the sending domain resides on BRTS; if so, the message is blocked/quarantined. Offloads the Barracuda Email Security Gateway.

Email Encryption and Data Loss Prevention

11.1 Email Encryption

Email encryption:

- Prevents confidential or sensitive information from being leaked outside the organization (Data Loss Prevention).
- Is configured at the per-domain level with the **DOMAINS > Manage Domain > ADVANCED > Encryption** page.
- Uses the Barracuda Message Center.
- Can be used from within MS Outlook with the **Barracuda Outlook Add-In** for Microsoft Exchange Server.
- Prevents the message body from being displayed in the **Message Log**.

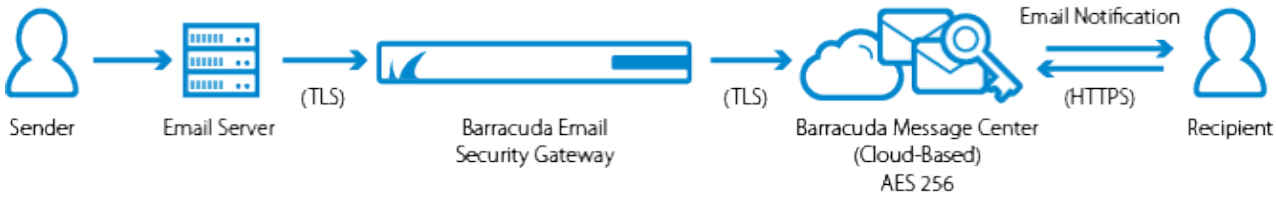
Only the sender of the encrypted message(s) and the recipient can view the body of an encrypted message.

11.1.1 Encryption Policies:

- Are configurable by sender domain, email address, recipient, etc., and ONLY at the global level on **BLOCK/ACCEPT** pages.
- Apply to all domains from which encrypted email messages are sent.
- Cause emails that match policy settings to be sent securely (via TLS) to the Barracuda Message Center for the recipient to retrieve.

11.1.2 Recipients of encrypted messages:

- Are notified by the Barracuda Message Center (BMC)
- Can log into the BMC with password from the notification email **Cloud Control** page of the Barracuda Web Security Gateway, as covered in the **Cloud Control** section of this handbook.multiple Barracuda Email Security Gateway(s).



11.2 Data Loss Prevention (DLP)

For health care providers, governmental agencies and other entities who need to protect private, sensitive and valuable information communicated via email, the Barracuda Email Security Gateway includes DLP (Data Loss Prevention) features. DLP enables your organization to satisfy email compliance filtering for corporate policies and government regulations such as HIPAA and Sarbanes-Oxley.

Advanced content scanning is applied for keywords inside commonly used text attachments, as well as email encryption. DLP encryption protects private, sensitive and valuable information communicated via outbound mail ONLY.

Configure any of the following pre-defined data loss patterns (specific to U.S.) in the **Predefined Filters** section of the **BLOCK/ACCEPT > Content Filtering** page to meet HIPAA and other email security regulations:

Predefined Filters

DATA LEAKAGE PREVENTION	SUBJECT	BODY	ATTACHMENT
Credit Cards	Off	Off	Off
Social Security Numbers	Off	Off	Off
Privacy	Off	Off	Off
HIPAA	Off	Off	Off

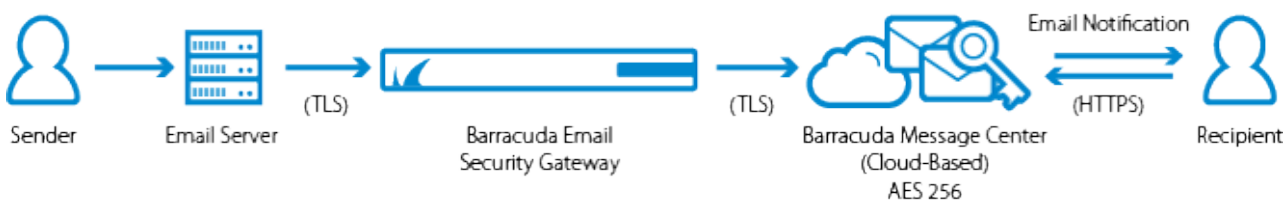
As shown, you can specify filters in any of the following parts of a message:

- subject
- body
- attachment

For each filter, you specify one of the following actions to take with emails that match the specified pattern:

- Block
- Quarantine
- Encrypt
- Redirect
- Off (the feature is turned off for that predefined filter)

Encryption is performed by the Barracuda Email Encryption Service, which also provides a web interface, the Barracuda Message Center, for recipients to retrieve encrypted messages.



When the Barracuda Email Encryption Service encrypts the contents of a message, the *message body will not be displayed* in the Message Log. Only the sender of the encrypted message(s) and the recipient can view the body of an encrypted message.

11.2.1 DLP Versus TLS Encryption

DLP secures data-at-rest, while Transport Layer Security (TLS) encryption secures data-in-motion.

- DLP provides encryption of data in a message depending on filters you apply as described above, but it does not provide a secure channel for actual transmission of the message. That's the job of TLS, which you can configure separately on the Barracuda Email Security Gateway on the BASIC > Outbound and ADVANCED > Email Protocol pages.
- TLS provides a secure channel for data transmission, and ensures that all content, emails, and attachments are encrypted during transit. This is known as Data-in-Motion security, because the data is secure during the actual transmission process. However, TLS does not provide security for data at rest, which means that data such as emails and attachments could be getting stored without any encryption, on the sending and receiving servers as well as any other servers and gateways that may be involved in filtering and delivering the email.

See How to Use DLP and Encryption of Outbound Mail in Barracuda Campus for details on configuration.

Barracuda®