The Barracuda Email Security Gateway is an email firewall aimed at filtering and managing outgoing and incoming emails to ensure the users safety and to prevent data leaks. It is offered as a full package as either a virtual device or in a public cloud environment. The service protects against malware, spam, phishing, and Denial of Service attacks with customizable policies to make the system even more secure. Since it is cloud based, the Barracuda service pre-filters the emails before it actually hits a user’s network allowing for a more secure network. It also allows for email spooling in case the user’s network goes down.

The Barracuda Email Security Gateway is offered in the form of eight different models. Each model mostly depends on how many users that the system is supporting with the base supported users being between 1-50 users. The last model supports up to 100000 users. Each model also has certain features. Depending on what model is chosen, the bundled features increase. The base model comes with Advanced Threat Detection, Outbound Email Filtering, Email Encryption, and Cloud Protection Layer. The base model provides everything for basic protection. Each model after this contains these same features or adds onto these features. The base system costs 769 dollars without any options chosen while the top tier system is 98999 dollars without any selected options.

Advanced Threat Detection (ATD) is a feature of the system that essentially inspects each email attachment and determines if they are malicious or dangerous and destroys them if they are suspected. ATD combines the inspection techniques of heuristic, behavioral, and sandboxing to create the system. Attachments are “detonated” by opening them in a sandbox environment and determining their behaviour. The results from each sandbox detonation is recorded and used to further the protection of each user on the Barracuda service.

Spam protection is another feature included in the base package. Barracuda has a long history in this field and claims to be the leader of it. The system has a large number of security layers that maximizes security. It looks at the emails very carefully to determine if the sender is a known spammer and to determine if the embedded domains lead to other spam or malware locations. It also looks at embedded information in linked images to further protect users from going to malicious web pages.

Virus protection is another feature offered in the base package. Barracuda takes this portion of their system very seriously as it has the highest chance of causing a financial loss. It does this by using three layers of virus scanning on each incoming email and file. It also decompresses its archives for maximum protection. There is also protection against internal email by the use of a Microsoft Exchange Plug-In.

Email Spooling is also a feature of the Barracuda system. In the case of an email server failure or connectivity issue, the incoming emails are spooled on the Cloud Protection Layer for up to 96 hours. It also allows for the option of another location to be chosen for the emails destination. Administrators can see the status of all spooled emails and if the email has been delivered to a given location.

Pre-filtering is another feature that is included in the system. It is a cloud based service that looks at the emails before it reaches the purchased gateway system. It is continuously updated by Barracuda Central, which is the 24/7 service provided by Barracuda to keep its services up to date and to provide customer support. It also ensures that the service scales with the users email volume.

Barracuda Email Security Gateway is also bundled with email encryption. Email that is marked for encryption is sent via TLS to the Barracuda Message Center. The Center then uses AES with 256-bit keys to encrypt each email making it incredibly difficult to crack. Encryption is very clearly a main necessity of email safety and integrity.

The Firewall also provides outbound filtering to ensure that the organization does not accidently become marked for spam. Humans make errors and these errors could cause an organization to become a botnet used for spam or DDoS attacks. By using similar virus and spam analyzation as used in previous features, the Barracuda system can prevent malicious data from being sent out to the internet. It also allows for administrators to enforce custom policies to manage what can be sent out and to prevent data loss.

The Barracuda Email Security Gateway is more than just a firewall. While it is solely aimed at email service protection it clearly provides maximum security. It is very current due to its cloud based nature and provides some useful features that reduces the limitations that exist on traditional firewalls. It removes the limitation of internal users being trustworthy and it also removes the limitation of malware protection since it does come bundled with malware protection. It also does deep inspection on each sent and received email keeping it up to date with today’s current trends. For Email security, the Barracuda Email Security Gateway seems like it would be an extremely safe and secure option to implement in a network.

*Barracuda Email Security Gateway.* Barracuda.com. <https://www.barracuda.com/products/emailsecuritygateway/features#section_5>