Securing Email with Email Encryption

Email encryption is used to ensure that only the intended recipient is able to access the email and any attachments. Traditionally, deployment email encryption services has been complex and cumbersome. In addition, use of email encryption requires the sender and recipient to exchange their encryption keys prior to sending and receiving emails. Both of these factors severely limit the usefulness and adoption of secure practices for exchanging email. In face of complexity, many users decide to bypass organizations policies, exposing sensitive and confidential data.

Barracuda Networks offers simple, yet secure email encryption. Email encryption is available as a feature in both the Barracuda Spam & Virus Firewall and the Barracuda Email Security Service. A cloud-based approach to email encryption ensures that keys are stored centrally. Key management happens automatically, without any added overhead for either the users or administrators.

Distinguishing between Data-at-Rest and Data-in-Motion Security

Why is Transport Layer Security (TLS) not sufficient?

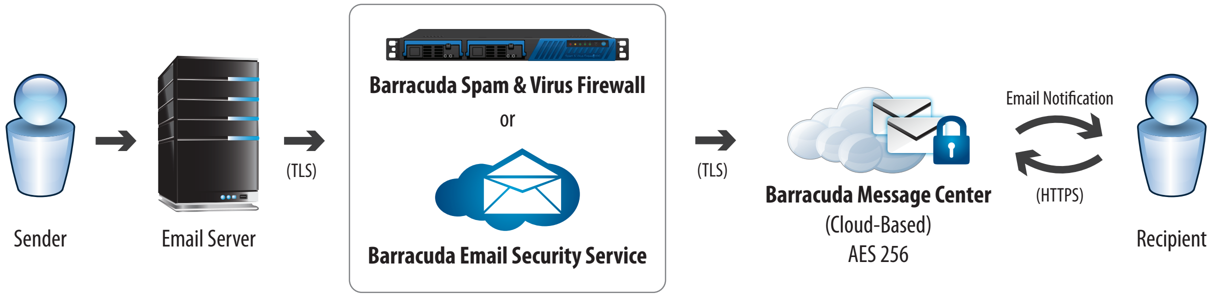
Transport Layer Security (TLS) provides a secure channel for transmitting data. Thus all content, emails and attachments are encrypted while they are transmitted. This is known as Data in Motion security, as the data is secure by moving from one server to another. However, TLS does not provide security of the data at rest. Thus, data (emails and attachments) are stored without any encryption on the sending and receiving server, as well as any other servers and gateways involved in filtering and delivering email. Therefore, these multiple servers are usually involved in email delivery.

In addition, any server that terminates the TLS connection can act as an email proxy, or forward the received email to another server. Any of these servers might not adhere to the same security requirements as the sending server. Terminating TLS connections before the final destination email server is often done for filtering email, enforcing policies and archiving. Thus with TLS, the sender has no way guaranteeing security of email.

	Transport Layer Security	Encryption with Barracuda Spam & Virus Firewall or Barracuda Email Security Service
Security of data in motion	Yes	Yes
Security of data at rest	No	Yes
Prevent forwarding without security	No	No
Secure Replies	No	Yes

Barracuda Networks email encryption solution

The Barracuda Spam & Virus Firewall and the Barracuda Email Security Service, include secure, cloud-based outbound email encryption. Multiple policies allow administrators to specify exactly which outbound emails to encrypt. Emails that match policy are securely (via TLS) sent to the Barracuda Message Center.



Key Management

The Barracuda Message Center utilizes Advanced Encryption Service with a 256-bit cipher, commonly known as AES 256. The first time an email is received for a recipient, a unique key is generated. Emails (including attachments) are encrypted using the recipient's key.

Recipient Interaction

After the process of encryption is complete, a separate notification email is sent to the recipient. The recipient is required to click on the link in the notification email to log into the Barracuda Message Center using a Web browser. Data transfer between the Barracuda Message Center and the recipient is via HTTPS. The recipient will be required to choose a password when they log into the Barracuda Message Center for the first time. Subsequent accesses will have to be authenticated with this password.

Once the recipient is logged in, they are able to view all encrypted messages that are sent to them. Recipients are able to reply to the email or download the email for storing on their computer. Any replies are also sent via the Barracuda Message Center to ensure security.

Security of data and keys

All keys and encrypted content are securely held in the Barracuda Message Center. State of the art data centers ensure physical security of everything while strict access control ensures that only authorized personnel have access to the Barracuda Message Center. As a final measure of security, the data centers and the keys used to encrypt the data are stored in separate areas.

Summary

The Barracuda Spam & Virus Firewall and the Barracuda Email Security Service both include email encryption. The following table summarizes the key features of email encryption available.

	Barracuda Spam & Virus Firewall	Barracuda Email Security Service
Email Retention Period	45 days	60 days
Email Encryption Technology	AES 265 bit	AES 256 bit
Customizable branding for Barracuda Message Center	Yes	Yes
Secure, Per recipient keys	Yes	Yes
Encryption Policies		
Sender-Based	Yes	Yes
Recipient-Based	Yes	Yes
Domain-Based	Yes	Yes
Download-Ability	Yes	Yes
Keyword-Based	Yes	Yes

For questions about the Barracuda Email Security Service, please visit http://www.barracuda.com/bess or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit http://www.barracuda.com/products.

The Barracuda Email Security Service is a full-featured, comprehensive cloud-based email filtering service that protects both inbound and outbound email against the latest spam, viruses, worms, phishing and denial of service attacks. The Barracuda Email Security Service leverages advanced security technologies from the industry-leading Barracuda Spam & Virus Firewall and features rich cloud-based protection.

About Barracuda Networks Inc.

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 130,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif. For more information, please visit www.barracudanetworks.com.

BARRACUDA NETWORKS

Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
+1 408.342.5400
www.barracuda.com
info@barracuda.com