Barracuda

Securing Email with Email Encryption

White Paper

Email encryption is used to ensure that only the intended recipient is able to access the email and any attachments. Traditionally, deploying 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 the face of complexity, many users decide to bypass their organizations' policies, potentially exposing sensitive and confidential data.

Barracuda Networks offers simple yet secure email encryption. Email encryption is available as a feature in both the Barracuda Email Security Gateway (hardware appliance) and the Barracuda Email Security Service (cloud-based). 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 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.

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. As a result with TLS, the sender has no way to guarantee the security of the email.

	Transport Layer Security	Encryption with Barracuda Email Security Gateway 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

Both the Barracuda Email Security Gateway and the Barracuda Email Security Service provide secure, cloudbased outbound email encryption, with multiple policies available that allow administrators to specify exactly which outbound emails to encrypt. Emails that match policy can then be sent securely (via TLS) 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 containing a link to log into the Barracuda Message Center is sent to the recipient. The Barracuda Message Center must be accessed with a web browser using HTTPS. The recipient will be required to choose a password when logging into the Barracuda Message Center for the first time. Subsequent accesses will be authenticated with this password.

Once recipients are 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 to store 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 an additional measure of security, the data centers and the keys used to encrypt the data are stored in separate areas.

Summary

The following table summarizes the key email encryption features that are offered by the Barracuda Email Security Gateway and the Barracuda Email Security Service.

	Barracuda Email Security Gateway	Barracuda Email Security Service
Email Retention Period	30 days	30 days
Email Encryption Technology	AES-256	AES-256
Customizable Branding for Barracuda Message Center	Yes	Yes
Secure, Per-Recipient Keys	Yes	Yes
Encryption Policies		
Keyword-Based	Yes	Yes
Sender-Based	Yes	Yes
Recipient-Based	Yes	Yes
Domain-Based	Yes	Yes

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com