

# STARTTLS EMAIL ENCRYPTION USING THE BARRACUDA SPAM FIREWALL

## SSL/TLS EMAIL ENCRYPTION

STARTTLS is the emerging industry SMTP feature for encryption of email communications. The STARTTLS command is used to negotiate an encrypted session using TLS, adding an increased layer of security by encrypting the email transmission channel as messages cross the Internet. This seamless encryption method is transparent to both sender and receiver and provides an easy-to-use and safe method of communicating over the Internet.

Using STARTTLS, once a connection has been successfully established between two servers, all email traffic between is encrypted, protecting message content during transfer. In order for STARTTLS to work effectively, both the source and destination email environments must support the technology and be able to negotiate encryption using shared keys.

The Barracuda Spam Firewall and the Barracuda Spam Firewall – Outbound product lines as well as most email clients support STARTTLS. This has profound advantages, especially in situations where the user is outside the organization or is using an unencrypted Internet connection. With STARTTLS, users can remain confident that their email is secure from the moment it is sent to the moment it is received.

## HOW DOES STARTTLS PROTECT EMAIL?

STARTTLS can perform many email security functions, including:

- » Verify the identity of the client and/or server in an email transmission
- » Encrypt email transmissions (without requiring verification of the identity)
- » Authenticate a user to be relayed through an email server (similar to SMTP AUTH)

## WHO BENEFITS FROM STARTTLS?

STARTTLS provides security advantages for numerous industries and entities. From legal firms and public corporations to medical practices and technology companies, all businesses have a vested interest in ensuring any confidential material contained within an email message remains private. The Barracuda Spam Firewall provides everything needed to ensure your email traffic is protected.

## STARTTLS AND EMAIL COMPLIANCE

In the last decade, government restrictions and regulations such as the Graham-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act, and HIPAA (Health Insurance Portability and Accountability Act) have given rise to the necessity for encrypting sensitive communication over electronic communications such as email and instant messaging. The use of STARTTLS is more than prudent; for many firms it is a vital requirement.

RELEASE 2

DEC 2006

**SMTP (Simple Mail Transfer Protocol)** is a protocol for sending email messages between servers.

**TLS (Transport Layer Security)** is a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet. TLS is made up of two layers: the TLS Record Protocol, which ensures that the connection is private and reliable by using symmetric data encryption; and the TLS Handshake Protocol, which allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

REGULATION	EMAIL ENCRYPTION REQUIREMENT
Graham-Leach-Bliley	Requires confidentiality and security of customer financial information.
Sarbanes-Oxley	Requires confidentiality, accuracy, and security of corporate financial information
HIPAA	Requires confidentiality and portability of patient identification and health-related information.

## YOUR INTERNAL EMAIL ENVIRONMENT AND STARTTLS

Security between the client and server will prevent users on the network from accessing confidential communications. This is especially paramount in situations where the user is outside the corporate firewall, thus exposing their email to anyone on the Internet. A STARTTLS connection between the client and server is important, and is more common than secure connections between disparate email networks such as inter-office, or inter-corporation email.

## AN IDEAL STARTTLS SETUP

The easiest way to ensure your email environment, and those of your partners, fully harnesses the security potential of STARTTLS is to have a Barracuda Spam Firewall protect both your email environment, and that of your partners.



The Barracuda Spam Firewall is easy to use, features a high level of encryption as well as leading anti-spam and virus protection technologies, making it the pinnacle of email security solutions. No other product comes close to offering the power, ease of use, and affordability of Barracuda Networks' products.

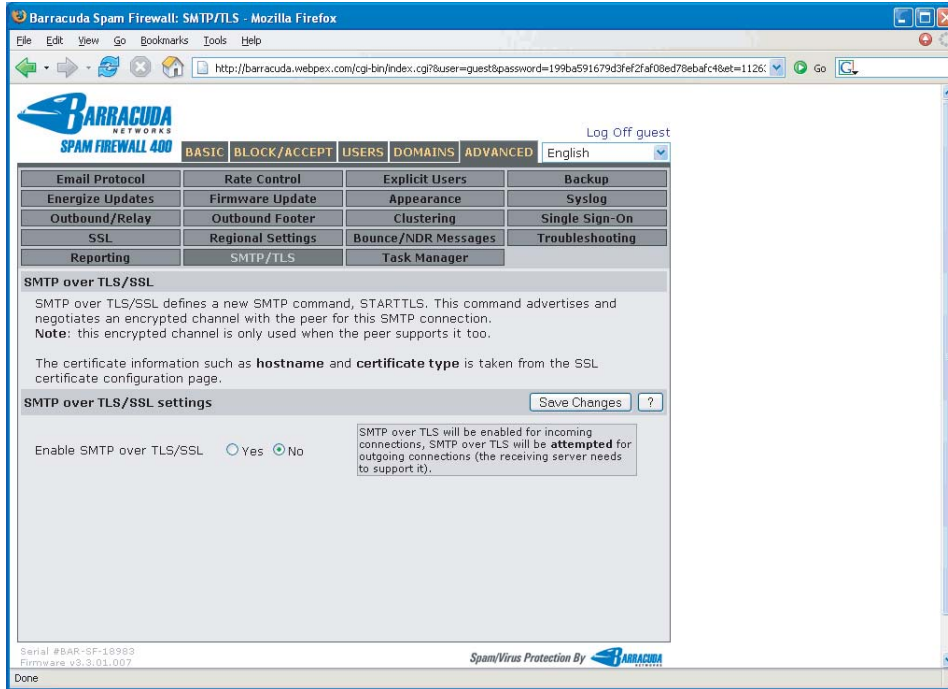
## CONFIGURING THE BARRACUDA SPAM FIREWALL TO USE STARTTLS

Configuring the Barracuda Spam Firewall to use STARTTLS is simple. Start by logging onto your Barracuda Spam Firewall, select the Advanced tab and click on the SMTP/TLS menu option. Once on this page click the "Yes" radio button to enable SMTP over TLS/SSL. It is important to remember that STARTTLS will only be secure if both the sender and recipients' environments have it enabled. This is easily achieved if both environments are enhanced and protected with the Barracuda Spam Firewall.

## THE BARRACUDA SPAM FIREWALL

Winner of numerous industry honors, including Network Computing's Editor's Choice Award and the 2004 and 2005 Well-Connected Awards, Barracuda Networks' flagship product, the Barracuda Spam Firewall, provides spam and virus protection for over 20,000 customers around the world. Customers include industry leaders such as Adaptec, Barnes & Noble, CBS, Forbes, IBM, NASA, and the U.S. Treasury Department.

**SSL (Secure Sockets Layer)** is a protocol for transmitting and encrypting private documents via the Internet. SSL uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message.



The Barracuda Spam Firewall is available in six models and supports from 1,000 to 30,000 active users with no per user licensing fees. The Barracuda Spam Firewall can be installed in front of the email server in typically less than five minutes and is automatically updated hourly to block new forms of spam and viruses. The Barracuda Spam Firewall's layered approach minimizes the processing of each email, which yields the performance required to process millions of messages per day. Unlike software solutions, the Barracuda Spam Firewall reduces the load placed on the email server by off-loading both spam and virus filtering. Barracuda Networks also offers the Energize Update subscription service to automatically update the Barracuda Spam Firewall with the latest spam rules and virus definitions.

Considering the advantages of STARTTLS encryption capabilities, the time is right for your organization to benefit from this enabling technology. Contact a Barracuda Networks representative today at 1-888-ANTI-SPAM for a free 30-day evaluation.



**Barracuda Networks, Inc.**

385 Ravendale Drive  
Mountain View, CA 94043

**tel:** +1 408.342.5400

**fax:** +1 408.342.1061

[www.barracuda.com](http://www.barracuda.com)