SSL Inspection on Secure Web Gateways

White Paper

Secure Sockets Layer (SSL) is an encryption technology that secures TCP/IP transactions. It is most commonly used to secure data transmissions between a web server and a client browser. In addition to securing mission-critical enterprise applications, financial transactions, medical records, and online purchases, SSL is increasingly being used by web and social media portals to maintain user privacy and secure content transfer. For instance, Twitter enabled SSL by default in August, 2011.[1] Facebook offered SSL as a privacy option earlier that year.[2] One of the most trafficked sites on the Internet, Google Search, started encrypting search queries in September 2013.[3] It is estimated that 30% of outbound Internet traffic is now encrypted using SSL, according to an article published by CSO Online.[4]

Ironically, SSL encryption also poses a security and productivity concern for enterprises and schools since this traffic is generally invisible to secure web gateways. Without this protection, hackers may spread malware. Users can bypass corporate Internet usage policies and kids can be exposed to unsafe and inappropriate Internet content.

Regulating SSL-encrypted traffic requires the web gateway to act as a web proxy and 'inspect' or 'scan' the traffic by decrypting and re-encrypting the transactions. Traditional firewalls, 'pass-by' web security gateways that only inspect the web traffic off a span or mirror port, and Unified Threat Management devices (UTMs) struggle with this because of the complexity and processing resources required to scan SSL traffic.

Barracuda Solves this Challenge

Barracuda security solutions are designed to provide SSL traffic regulation with an optimal combination of security and performance.

The Barracuda Web Security Gateway content security appliance takes a layered approach to SSL regulation.

- For basic policy management, the appliance blocks HTTPS web requests at Layer 3 by monitoring DNS responses generated by these requests and constructing an internal database that maps IP addresses to domain names. The appliance can enforce domain-level access policies on SSL-encrypted web requests without scanning the content with this approach. This technique ensures complete data security since it does not decrypt and re-encrypt the content.
- For more granular policy management and malware protection, Barracuda Web Security Gateways[5] can scan or inspect SSL traffic by acting as a secure intermediary for SSL traffic between the client browser and the web server. This content is decrypted and inspected to enforce usage policies, as well as scanned for virus and malware. After processing, the traffic is re-encrypted and routed to the proper destination.

Web browser proxies HTTPS requests through the Barracuda Web Security Gateway

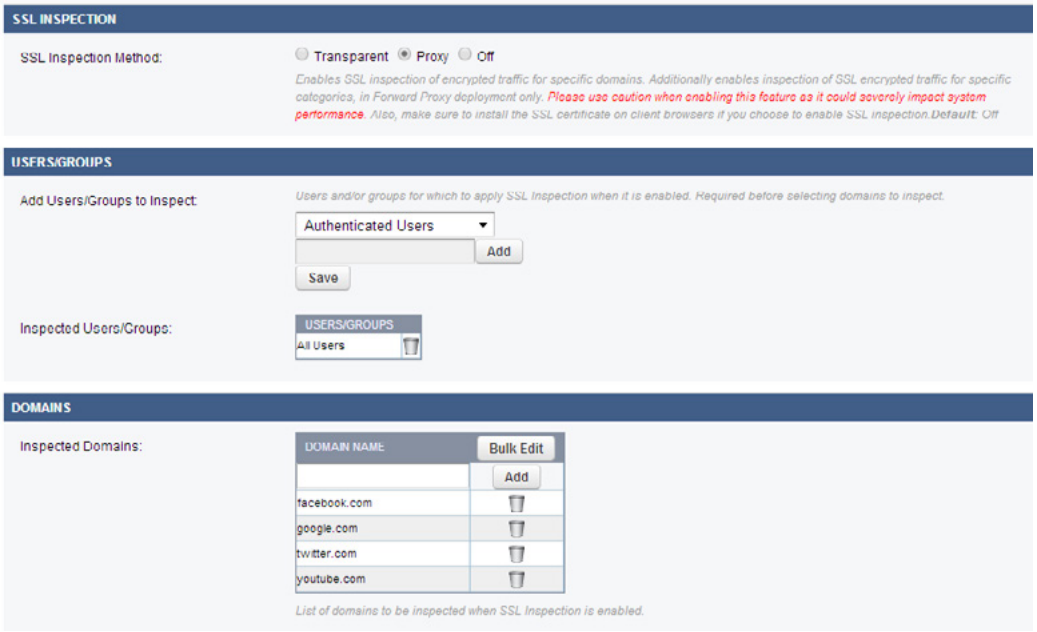
Barracuda Web Security Gateway decrypts SSL traffic for inspection

Barracuda Web Security Gateway re-encrypts SSL traffic before sending to destination server

SSL inspection also enhances the powerful Web Application Control, Web Application Monitoring and Suspicious Keyword Tracking features on the Barracuda Web Security Gateway. Through these, administrators can regulate specific actions on social-media portals such as Facebook, monitor social-media posts for suspicious keywords and, archive social-media content for forensics even when the traffic is encrypted.

SSL inspection is also available on Barracuda Next-Generation Firewalls. These powerful application-aware firewalls enable administrators to apply granular access control, bandwidth shaping, and WAN optimization policies to SSL-encrypted web traffic.

Decrypting and re-encrypting traffic for SSL inspection is generally a performance-intensive operation. Barracuda solutions make it easy to minimize performance overhead by allowing administrators to apply SSL inspection to specific domains, content categories, and users or groups.



Barracuda security solutions provide comprehensive protection and visibility across all aspects of web traffic. SSL inspection combined with granular policy management allow organizations to securely leverage Internet-based applications and web content without impacting network performance and compromising security.

References

[1]http://www.zdnet.com/blog/networking/twitter-adds-ssl-security/1374

[2]https://www.facebook.com/notes/facebook/a-continued-commitment-to-security/486790652130

[3]http://searchengineland.com/post-prism-google-secure-searches-172487

[4]http://www.csoonline.com/article/735005/rising-ssl-traffic-to-degrade-firewall-performance

[5]Barracuda Web Security Gateway 610, 810, 910, 1010, 1011 and Barracuda Web Security Gateway 610 Vx virtual edition

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.

3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com