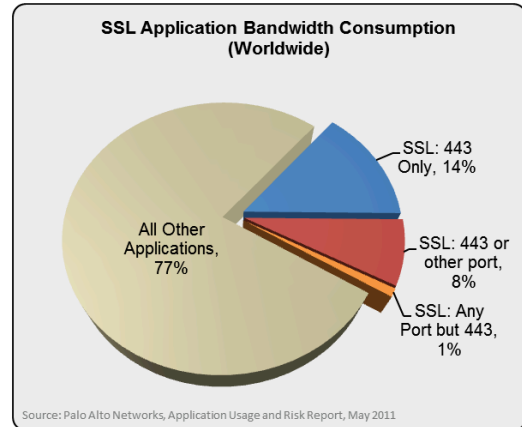


Introduction

Recent analysis of live enterprise networks show that the reach of SSL is exploding with roughly 36% of total enterprise bandwidth being consumed by applications that can run SSL or hop ports. While SSL certainly provides security for the individual session, it can also create a problem for enterprise security by obscuring the traffic from network security solutions such as IPS, anti-malware and data-loss prevention (DLP) solutions. To make matters worse, the very sites and applications that are adopting SSL are the same ones that hackers favor for launching and maintaining their on-going attacks. The result is that enterprise security is rapidly losing visibility into one of the most active fronts in the ongoing battle against malware and network intrusions. This app note provides a brief review of modern SSL usage and lays out best practices and policies based on the Palo Alto Networks next-generation firewall that IT and security teams can implement to selectively identify, decrypt and inspect high-risk SSL traffic while maintaining an appropriate balance of performance.



Fighting Blind: The Convergence of Social Media, SSL and Advanced Threats

Social media is a well-established hub for social engineering, malware infection and command-and-control. This broad category of applications include social networking, web-based email, instant messaging, web-based file transfer and a variety of blogs, message boards and micro-blogging platforms such as Twitter. As a group these applications have become favorite targets for hackers because they provide easy, largely uncontrolled access to the weakest link in enterprise security – the end user. In particular, these applications provide many opportunities to gain the trust of a target user and offer a wealth of links, scripts, ads and images all of which can be used to exploit an unsuspected user. Additionally, the very popularity of these applications makes it easy for an attacker's traffic to blend in with normal user traffic and pass without suspicion. This characteristic is true for outbound traffic as well as inbound, with a variety of bots and malware being known to use social networking, micro-blogging and message boards as command and control channels for the management of a botnet or ongoing intrusion.

In an effort to improve privacy for their users, many of these applications have begun to use SSL as a default protection for all traffic. This has ironically taken a bad IT security situation and made it worse, by encrypting the very channels that hackers are using to attack the network. Now instead of trying to hide in plain sight or being forced to use a circumventor application that may draw unwanted attention, the attackers can simply ride within the SSL connection between the application and the target user. This provides a near perfect platform for an attacker with a wealth of targets, a full complement of attack vectors and built-in cloaking from security solutions.

Step #1: Reduce the Attack Surface

- Identify which applications are in use, who the users are and determine business vs personal policy criteria
- Establish an allowed list of social media applications (Standardize on common platforms, block others)
- Establish an allowed list of features (Allow Facebook base, but not Facebook Apps)
- Enforce controls by user role (Marketing can post to social networking, others are read-only)
- Block unneeded or high-risk applications (P2P, encrypted IM, proxies, encrypted tunnels etc.)

Step #2: Prevent Threats in Allowed Traffic

Palo Alto Networks supports policies that can allow traffic based on application and user, and then apply full threat prevention including IPS, anti-malware, file-type controls and DLP controls.

- Fully enable vulnerability protections
- Fully enable antivirus and anti-spyware
- Apply data-filtering and DLP rules to outbound traffic

Application	Service	Action	Profile	Options
any	any	✓	[Icons]	[Icon]
Custom-app	any	✓	[Icons]	[Icon]
dns				
p2pFSdemo				
facebook-base	service-http	✓	[Icons]	[Icon]
webex-base				
facebook-base	any	✓	[Icons]	[Icon]
ssh	any	✓	[Icons]	[Icon]
ssl				
Webmail	any	✓	[Icons]	[Icon]

Step #3: Ensure Visibility Into Social Networking Traffic

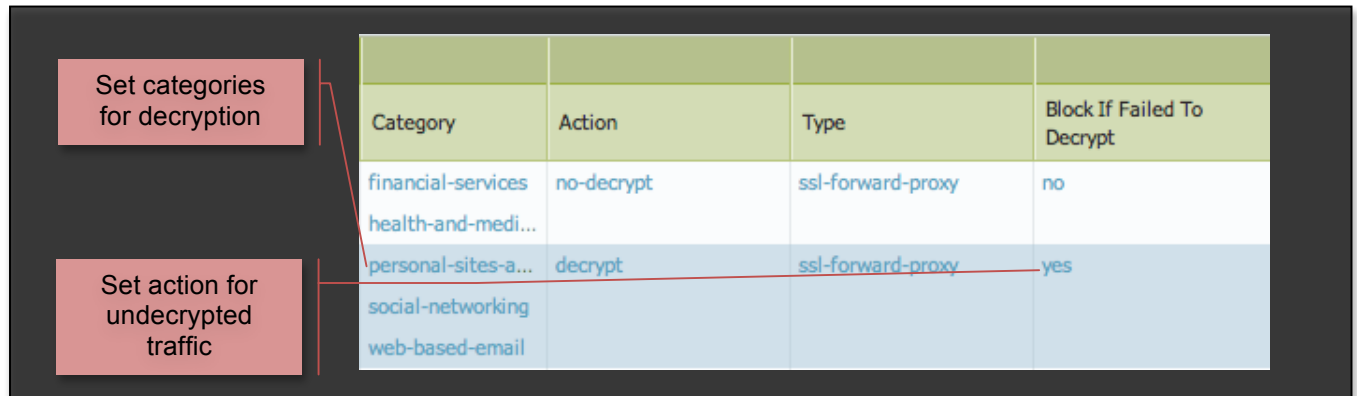
Palo Alto Networks support policies to selective decrypt SSL to specific applications, URLs or URL categories. SSL decryption is by turned off by default, so users will need to specify the traffic to be decrypted. The decryption process occurs in the firewall itself and is re-encrypted before sending on to the original destination.

- Select SSL from the left-side panel of the Policies tab

Name	Tag	Zone	Address
No-Decrypt SSL	none	trust	any
Decrypt SSL	none	trust	any

- Opt-in allowed social media applications for SSL decryption
- Define if traffic should be allowed or blocked if decryption is unsuccessful

Selective SSL Decryption for Threat Prevention



Category	Action	Type	Block If Failed To Decrypt
financial-services	no-decrypt	ssl-forward-proxy	no
health-and-medi...			
personal-sites-a...	decrypt	ssl-forward-proxy	yes
social-networking			
web-based-email			

Summary

As with any enterprise security policy, individual policy decisions will vary as organizations match their security controls to their unique needs and tolerances for risk. However, as more and more critical traffic becomes encrypted by SSL, enterprises will increasingly be forced to find ways to decrypt high-risk traffic without the performance impacts of decrypting ALL traffic. The simple guidelines discussed above simply illustrate a policy driven model that can enable an enterprise to strike the appropriate balance and retain full visibility and control over traffic even when encrypted.