BLUE COAT®

Security
Empowers
Business

IMPLEMENTING DATA PRIVACY REQUIREMENTS FOR ENCRYPTED TRAFFIC

SOLUTION BRIEF

Blue Coat Encrypted Traffic Management Combines Visibility and Control of Encrypted Traffic with Global Threat Intelligence

Users are increasingly turning to web, mobile and cloud applications to get their work done. These applications generally use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to encrypt the traffic to keep their communications and transactions private; from an enterprise's perspective, however, this encrypted traffic creates blind spots in the network that can hide activity that violates an enterprise's acceptable use policies or poses a threat to the security of the organization.

Advanced Persistent Threats (APTs) and malware often use SSL to evade detection; according to Gartner Research, 50% of all network attacks will hide in SSL by 2017. When you consider more than 35% of an enterprise's network traffic is encrypted, and this percentage is expected to grow 20% annually, you begin to see the enormity of the risks. Enterprises need visibility and control of this encrypted traffic to ensure consistent security and policy enforcement. Unfortunately, current security tools either have no visibility into SSL or create bottlenecks that disrupt the performance and operations of the network in their efforts to decrypt and inspect SSL traffic. Independent testing indicates that "turning on" visibility into SSL within today's next generation firewalls can degrade the performance of the devices by up to 80%, rendering the capabilities ineffective, impractical or very expensive, as additional hardware has to be purchased, deployed and managed to try to achieve a satisfactory experience. Additionally, simply turning on SSL inspection, without comprehensive policy enforcement, can break existing compliance and Human Resources (HR) policies.

A new approach is needed. One that eliminates the blind spot and combats the hidden threats in encrypted traffic a, while maintaining alignment with the enterprise's privacy and acceptable use policies and regulatory compliance efforts. It must also ensure there is no denigration of the cryptography levels established by the organization or the overall performance of the network. Lastly, as cost is always a key factor, the solution must be cost-effective, enhancing the existing security infrastructure, not forcing wholesale changes or upgrades, so the enterprise can maximize their investments.

AT-A-GLANCE

PROBLEM

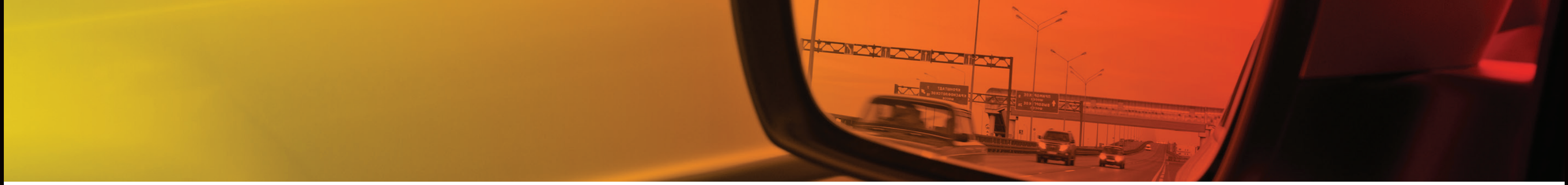
SSL/TLS encrypted traffic introduces a security blind spot and is increasingly used to hide advanced threats

SOLUTION

Blue Coat Encrypted Traffic Management Solutions

BENEFITS

- Eliminate the visibility blind spot caused by SSL/TLS
- Ensure the highest-level of encrypted traffic
- Cost-effectively enhance and preserve the existing security infrastructure
- Preserve data privacy and compliance through comprehensive policy enforcement



Blue Coat Gives Enterprises Complete Visibility into Encrypted Traffic

Blue Coat's Encrypted Traffic Management solutions give enterprises the visibility they need into encrypted traffic to expose advanced malware and enforce corporate policies to reduce risks and support compliance. The solution is built on the purpose-built Blue Coat SSL Visibility Appliance, which automatically sees all SSL/TLS traffic to deliver a comprehensive view of the applications and potential threats contained in encrypted traffic.

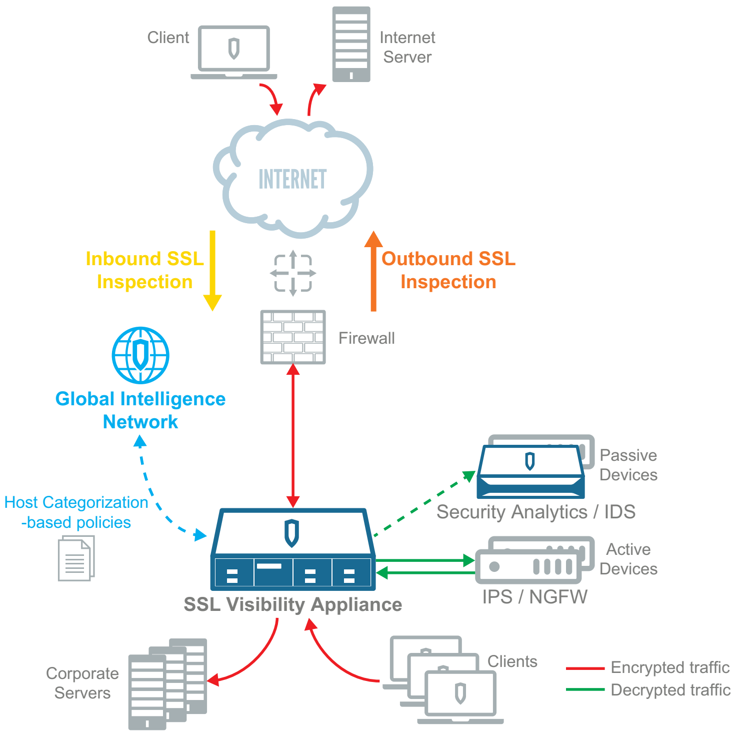


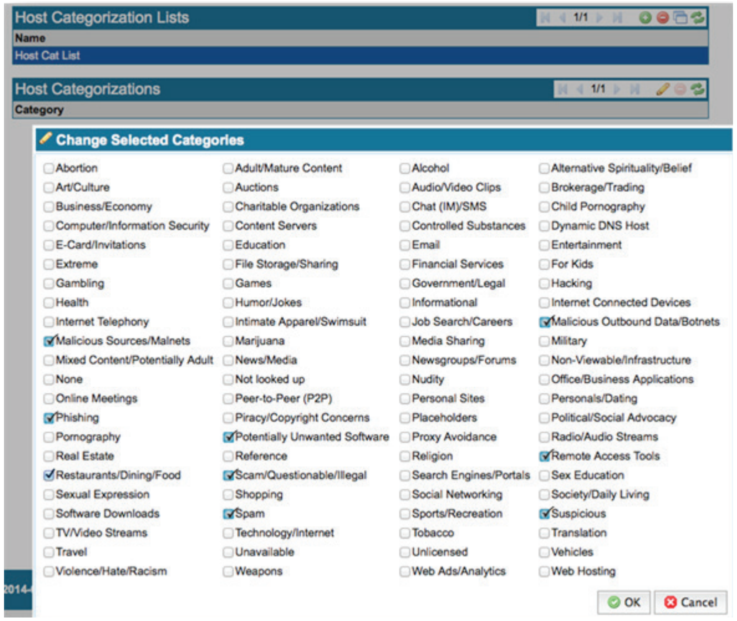
Figure 1 - The Blue Coat SSL Visibility Appliance deployed within a network

The SSL Visibility Appliance adds policy-based SSL inspection and management capabilities to an enterprise's security architecture, providing decrypted traffic feeds to existing security tools, such as intrusion detection and prevention systems (IDS/IPS), security analytics, sandbox or anti-malware analysis, next generation firewalls (NGFW) and data loss prevention (DLP) systems, to optimize their effectiveness.. This unique "decrypt once-feed many" design provides critical visibility, while eliminating costly capacity upgrades across multiple security devices. Powerful enforcement policies also allow the enterprise to control exactly which types of traffic are and are not inspected to ensure employee data privacy is maintained.

Achieving Simple, Effective Policy Enforcement

Policy enforcement needs to meet the unique needs of the enterprise; every enterprise has different risk tolerance levels and security requirements, which can be influenced by industry, geographic and government regulations. Blue Coat delivers the flexibility and extensibility enterprises need to effectively balance their security and data privacy demands.

The SSL Visibility Appliance provides a powerful, granular policy engine that expedites and simplifies the enforcement and management of security policies for SSL/TL encrypted traffic. While



Host Categorization Lists

Name

Host Cat List

Host Categorizations

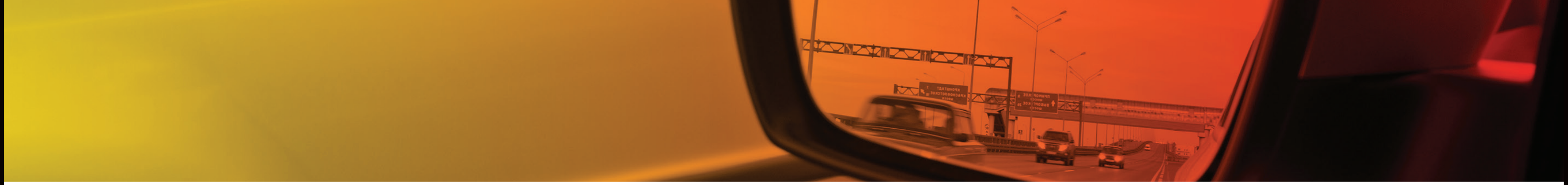
Category

Change Selected Categories

☐ Abortion
☐ Art/Culture
☐ Business/Economy
☐ Computer/Information Security
☐ E-Card/Invitations
☐ Extreme
☐ Gambling
☐ Health
☐ Internet Telephony
☑ Malicious Sources/Malnets
☐ Mixed Content/Potentially Adult
☐ None
☐ Online Meetings
☑ Phishing
☐ Pornography
☐ Real Estate
☑ Restaurants/Dining/Food
☐ Sexual Expression
☐ Software Downloads
☐ TV/Video Streams
☐ Travel
☐ Violence/Hate/Racism
☐ Adult/Mature Content
☐ Auctions
☐ Charitable Organizations
☐ Content Servers
☐ Education
☐ File Storage/Sharing
☐ Games
☐ Humor/Jokes
☐ Intimate Apparel/Swimsuit
☐ Marijuana
☐ News/Media
☐ Not looked up
☐ Peer-to-Peer (P2P)
☐ Piracy/Copyright Concerns
☑ Potentially Unwanted Software
☐ Reference
☑ Scam/Questionable/Illegal
☐ Shopping
☑ Spam
☐ Technology/Internet
☐ Unavailable
☐ Weapons
☐ Alcohol
☐ Audio/Video Clips
☐ Chat (IM)/SMS
☐ Controlled Substances
☐ Email
☐ Financial Services
☐ Government/Legal
☐ Informational
☐ Job Search/Careers
☐ Media Sharing
☐ Newsgroups/Forums
☐ Nudity
☐ Personal Sites
☐ Placeholders
☐ Proxy Avoidance
☐ Religion
☐ Search Engines/Portals
☐ Social Networking
☐ Sports/Recreation
☐ Tobacco
☐ Unlicensed
☐ Web Ads/Analytics
☐ Alternative Spirituality/Belief
☐ Brokerage/Trading
☐ Child Pornography
☐ Dynamic DNS Host
☐ Entertainment
☐ For Kids
☐ Hacking
☐ Internet Connected Devices
☑ Malicious Outbound Data/Botnets
☐ Military
☐ Non-Viewable/Infrastructure
☐ Office/Business Applications
☐ Personals/Dating
☐ Political/Social Advocacy
☐ Radio/Audio Streams
☑ Remote Access Tools
☐ Sex Education
☐ Society/Daily Living
☑ Suspicious
☐ Translation
☐ Vehicles
☐ Web Hosting

2014-

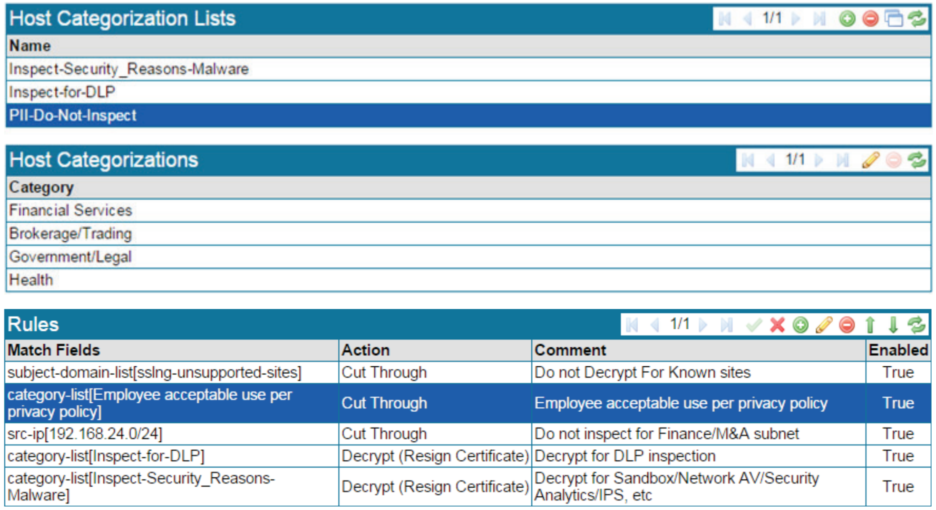
Figure 2 - Host Categorization enables comprehensive policy enforcement



fundamental parameters can be used to establish inspection and decryption policies, such as source and destination IP addresses and lists, Certificate Authority (CA) and server certificate status, destination TCP port, and subject name / domain name and Lists, the most impactful method for policy enforcement is the Host Categorization service. This unique capability allows enforcement policies to be established based on simple, familiar categories, such as ***Financial Services, Health, Malicious Sources/Malnets, Phishing*** and more.

The Host Categorization service is a license-based option that utilizes Blue Coat's comprehensive, collaborative threat database, the Global Intelligence Network, to maintain category accuracy and effectiveness. This innovative database is an established, proven intelligence hub that categorizes over 1 billion requests each day, and results in the blocking of over 3.5 million requests found to be malicious. The Global Intelligence Network supports over 55 languages and offers over 85 up-to-date, categories to 75 million users worldwide; it's a 24/7, real-time guardian against malicious network traffic within organizations worldwide.

Leveraging the unprecedented insights of the Global Intelligence Network, the Host Categorization service within the SSL Visibility Appliance helps enterprises create granular policies that balance their data privacy and security requirements. Enterprises are empowered to set policies that inspect both ingress and egress network traffic (per the US–CERT organization's recommendation (Alert TA14-353A), while identifying which traffic to cut through, without decryption, to adhere to privacy policies.



Host Categorization Lists

Name
Inspect-Security_Reasons-Malware
Inspect-for-DLP
PII-Do-Not-Inspect

Host Categorizations

Category
Financial Services
Brokerage/Trading
Government/Legal
Health

Rules

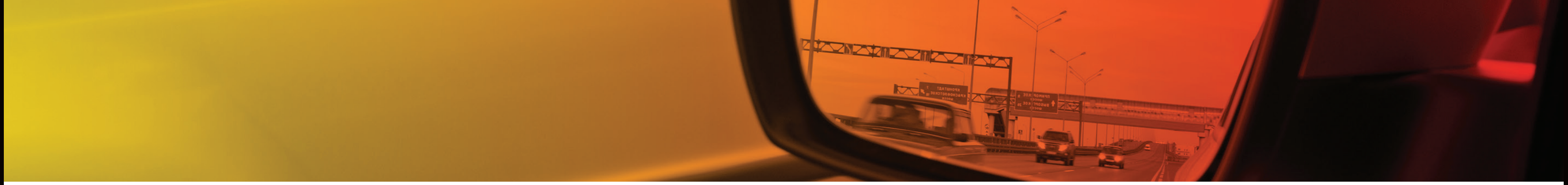
Match Fields	Action	Comment	Enabled
subject-domain-list[sslng-unsupported-sites]	Cut Through	Do not Decrypt For Known sites	True
category-list[Employee acceptable use per privacy policy]	Cut Through	Employee acceptable use per privacy policy	True
src-ip[192.168.24.0/24]	Cut Through	Do not inspect for Finance/M&A subnet	True
category-list[Inspect-for-DLP]	Decrypt (Resign Certificate)	Decrypt for DLP inspection	True
category-list[Inspect-Security_Reasons-Malware]	Decrypt (Resign Certificate)	Decrypt for Sandbox/Network AV/Security Analytics/IPS, etc	True

Figure 3 - Simple, yet powerful categories and rules are used for inspect, decrypt and pass-thru policies

Best practice examples of rules that make up many enterprise policies can be seen below:

COMMON SECURITY POLICIES FOR SSL/TLS ENCRYPTED TRAFFIC

BLOCK, REJECT OR INSPECT AND DECRYPT	DO NOT INSPECT OR DECRYPT / CUT THROUGH
• Rejecting / Blocking SSL traffic in bad categories such as Malicious Outbound Data/Botnets and Malicious Sources / Malnets • Rejecting / Blocking traffic utilizing obsolete and weak cipher suites such as RC4 and DES • Rejecting / Blocking traffic using key exchange mechanisms that don't support Perfect Forward Secrecy (PFS) – such as RSA • Rejecting / Blocking traffic utilizing invalid certificates	• Cut-through SSL traffic to sites in the Employee Acceptable Use categories such as Banking, Finance and Health – per the organization's Privacy Policies.



BLUE COAT®

Security
Empowers
Business

The Blue Coat Difference – Preserving Data Privacy and Compliance, While Enabling Comprehensive Security

Establishing and enforcing effective policies for inspecting and decrypting SSL/TLS traffic is imperative to the protection of an enterprise's networks. Blue Coat delivers a holistic approach to enable enterprises to mitigate risks and enforce policies that support compliance efforts and strengthen their overall security posture. With Blue Coat, enterprises can:

- **Cost-effectively improve risk posture** – eliminating the encrypted traffic blind spot by automatically seeing all SSL/TLS traffic, all ports and applications, without the need for complex scripting or configuration.
- **Achieve granular policy enforcement** – using Host categorization to ensure security, while preserving data privacy in support of regulatory compliance.
- **Enhance their existing security infrastructure** – feeding decrypted traffic feeds to active and passive devices simultaneously to strengthen an enterprise's security posture and improve the utility and return-on-investment of the existing infrastructure.

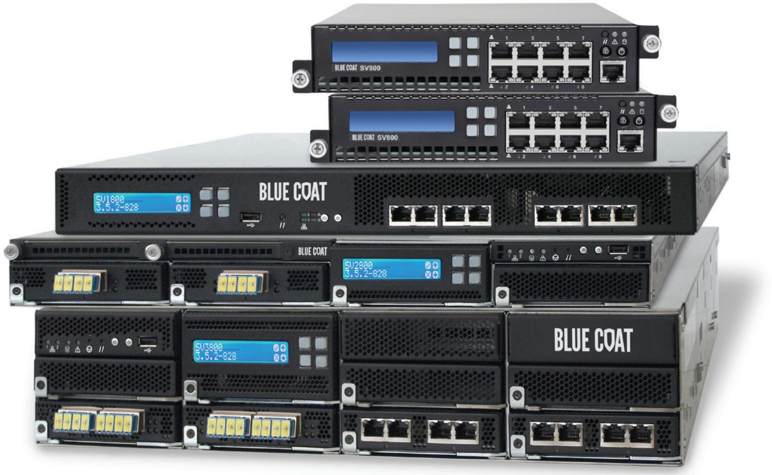


Figure 4 - The Blue Coat SSL Visibility family of appliances

For more information on how Blue Coat can assist you in managing your encrypted traffic in support of compliance mandates, please contact us or your local Blue Coat authorized Channel Partner today.

Find a Blue Coat Partner – https://www.bluecoat.com/partners/partner-locator

Contact Blue Coat – https://www.bluecoat.com/contact-us

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000