Issue 2

Are Cybercriminals Hiding in Your SSL Traffic?

Your threat detection strategy isn't working on 50% of network attacks

SSL encrypted traffic is pervasive in today's enterprises and is expected to grow rapidly over the next several years. According to Gartner, SSL/TLS traffic now comprises 15-25% of total web traffic. For many businesses, it is already well over 50%. The bad guys have noticed.

While SSL/TLS provides privacy and authentication, it also creates a blind spot for enterprise security. Cybercriminals can use SSL to hide their exploits from an organization's security controls, including Next Generation Firewalls (NGFW), Intrusion Prevention Systems (IPS), Unified Threat Management (UTM), secure gateways, Data Loss Prevention (DLP), anti-malware solutions, and more. Cybercriminals are well aware of SSL/TLS encryption blind spots and are using it to their advantage: to hide attacks, evade detection, and bypass critical security controls.

You can't protect what you can't see

Most organizations lack the ability to inspect and decrypt SSL communications to detect these threats. This undermines traditional layered defenses and creates an unacceptable risk of breach and data loss. Bad guys are misusing SSL/TLS more, but most organizations have not calculated this increase into their planning.

In the following research, Gartner reports that less than 20% of organizations with NGFW, IPS, or UTM appliances decrypt inbound or outbound SSL traffic. That means 80% of the organizations that use

these security devices might be allowing cybercriminals to bypass the organization's existing security controls by leveraging SSL tunnels to sneak malware into the corporate network, hide command and control traffic, and pilfer sensitive data.

Gartner believes that by 2017, more than 50% of the network attacks, both inbound and outbound, will use encrypted SSL/TLS communications. Attackers are focusing on the use of SSL/TLS, because they know the majority of organizations blindly trust encrypted communications and don't (or can't) decrypt, making them unable to assess and block threats that leverage SSL/TLS.

The reason for this blind spot is twofold:

1. Security systems can't inspect encrypted traffic or their performance can't keep up.

Featuring research from Gartner

2. Security systems lack the cryptographic keys and digital certificates from across the network needed to decrypt traffic.

This inability to inspect SSL/TLS encrypted traffic undermines traditional layered defenses and increases the risk of information breach and data loss. Dedicated SSL decryption appliances, load balancing systems, and NGFW can now perform high speed SSL/TLS decryption to identify hidden threats. However, if these systems don't have access to cryptographic keys and certificates they cannot decrypt incoming traffic where bad guys are launching attacks and inserting malicious code.

Eliminate the blind spots in SSL traffic

High-performance decryption to find threats in SSL/TLS traffic requires the keys and certificates used by web servers, load balancers, applications servers, and other systems. Having automatic, secure access to all enterprise keys and digital certificates maximizes the amount of decrypted traffic, enables inspection of SSL traffic, and eliminates blind spots that are otherwise hidden in encrypted traffic. Every extra key and certificate available for decryption means one less place for cybercriminals to hide, infiltrate your network, and steal data.

Ensuring that SSL/TLS decryption systems have access to keys and certificates is difficult for most organizations:

1. **How to find the keys**. Applications that use SSL/TLS are spread across the organization. Finding keys and certificates and matching them to applications and administrators can be difficult to say the least. In most organizations there are hundreds, if not thousands, of keys and certificates used by public-facing web and application servers.

2. **How to distribute for decryption**. Keys and certificates need to be safely distributed to appliances for decryption. The scope and size of the task of distributing keys and certificates have frustrated many administrators. Even if they can locate their keys and certificates, getting them into a system is time consuming. And the process of collecting and distributing keys can introduce new security and compliance risks if keys are not handled properly.

3. **How to stay updated to keep decrypting**. Keeping keys and certificates up to date as they expire or are renewed or replaced is a challenge. And organizations are increasing their dependency on SSL/TLS as data protection and privacy requirements grow. As the number SSL/TLS certificates and keys expand, there is typically no certainty as to where they've come from and who is responsible for them. So the percentage of decrypted traffic decreases and risk grows.

Maximize decryption and uncover threats

To combat the threat of SSL/TLS encryption blind spots, companies need to decrypt outgoing or incoming SSL traffic and pass the content to security devices for further processing, analysis, and policy administration. Decrypting SSL/TSL traffic gives existing security tools the clear-text visibility they need to enforce protection, increasing their effectiveness and value.

1. To make sure threats don't go undetected, all the keys and certificates required for decryption need to be available and securely distributed to decryption systems.

2. Automation is essential for the discovery of keys and certificates as well as for secure distribution, installation, and validation that keys are working and enabling decryption – not only to get started quickly, but for on-going decryption operations.

3. As keys and certificates are renewed and replaced, all updates need to be distributed immediately to keep decryption working and threat detection running.

Venafi Trust Protection Platform integrates with leading high-performance SSL/TLS decryption appliances to create a strong front-line defense. Its robust key and certificate management maximizes the amount of inbound and outbound encrypted traffic that can be decrypted and inspected. Venafi finds all keys and certificates, establishes ownership, and automates distribution, installation, and validation. The Venafi Trust Protection Platform integrates with leading SSL decryption systems, NGFW, IPS, UTM, secure gateways, DLP, anti-malware solutions, and more to automate the entire process, eliminating the blind spots in your threat detection strategy. To learn more on how to strengthen your security visit venafi.com.

Source: Venafi

From the Gartner Files:

Security Leaders Must Address Threats From Rising SSL Traffic

SSL encryption provides confidentiality for the encapsulated traffic but weakens enterprise defense-in-depth efficiency, exposing endpoints and DMZ servers to threats from outbound and inbound traffic. This research will help enterprise security leaders to create a traffic decryption strategy.

Gartner Foundational

This research is reviewed periodically for accuracy. It was last reviewed on 8 January 2015.

Impacts

- An increasing share of enterprise network traffic is encrypted, creating gaps in defense-in-depth effectiveness that security leaders should not ignore.
- Complex sets of laws and regulations on privacy, along with a high risk of conflict with employees, kill most security leaders' outbound Web traffic decryption projects.
- Security leaders face limited technology choices for enterprise network traffic decryption, and these solutions often induce high costs and poor user experience.

Recommendations

- Evaluate the security risks coming from uninspected encrypted network traffic. Update relevant risk indicators accordingly, and request a sign-off from key stakeholders for acknowledged risks.
- Prepare for a legal assessment of traffic decryption with network diagrams, types of decryption to occur, whitelists and data logged, in addition to the safeguards being taken.
- Review existing privacy and network usage policy to determine if decrypting the traffic requires a policy update. Engage with HR and worker representatives throughout the entire decision and implementation life cycle.
- Leverage existing network security solutions to enforce the outbound Web policy on SSL traffic, based on server reputation or the information available from the SSL certificate. Then, establish a prioritized list of the traffic profiles you need to decrypt.

Analysis

The inspection of network traffic is a core component of a network security policy strategy and often involves more than one technology. In the interests of enterprise security, communications to internal and external servers are encrypted. Paradoxically, this Secure Sockets Layer (SSL) traffic "blinds" other network security mechanisms from inspecting this traffic. Full coverage of the enterprise network with best-of-breed traffic inspections is beyond the capabilities of many enterprises. Oftentimes, security solution architects have to make compromises — one of these compromises is decrypting traffic because of an insufficient awareness of related threats and the inherent complexity of decryption projects.

Gartner conducted an industry survey of network security vendors and enterprises this year to find out how organizations are tackling the challenge of traffic decryption (see Note 1). The survey revealed that less than 50% of enterprises with dedicated secure Web gateways decrypt outbound Web traffic. Less than 20% of organizations with a firewall, an intrusion prevention system (IPS) or a unified threat management (UTM) appliance decrypt inbound or outbound SSL traffic. However, more than 90% of organizations with a public website and a Web application firewall (WAF) decrypt inbound Web traffic.

In response to attacks and compromises, many major public Web services have already switched to HTTPS by default (Google, Yahoo, Twitter and Facebook) or will soon (Wikipedia).[1] Mobile application toolkits and HTML5 frameworks remove most of the complexity of enabling SSL communication by default. As a consequence,

the amount of encrypted traffic represents an increasing share of enterprise network traffic, with steady growth every year. Web traffic encrypted using SSL (HTTPS) accounts for 15% to 25% of total outbound Web traffic and often carries sensitive or personal data.[2]

Already, malware is using SSL to remain under the radar of network security solutions. For example, the pervasive Zeus botnet uses SSL communication to upgrade after the initial email infection. Following the Boston Marathon bombing, a malware attached to a spam message was also using SSL to communicate with its command and control server.[3] With more and more encrypted traffic, this trend is likely to expand rapidly. Gartner believes that, in 2017, more than half of the network attacks targeting enterprises will use encrypted traffic to bypass controls, up from less than 5% today.

Organizations without traffic decryption plans are blind not only to these new sophisticated attacks but also to any attacks that take place over encrypted connections. These enterprises will suffer or may already have suffered from undetected malware activity. Security leaders who seek to include encrypted traffic in their global network security strategies face numerous technical, organizational and human challenges.

Impacts and Recommendations

An increasing share of enterprise network traffic is encrypted, creating gaps in defense-in-depth effectiveness that security leaders should not ignore

For most organizations, SSL traffic is already a significant portion of their outbound Web traffic and is increasing. It represents on average 15% to 25% of the total Web traffic, with strong variations based on the vertical market.[2] The amount of Web inbound traffic that is encrypted varies highly among enterprises, mainly depending on the availability of a secure client Web area or an e-commerce component. Internal traffic for business applications might also be encrypted.

Internal, inbound and outbound traffic each carries different risks and creates different challenges (see Table 1). Even if Web SSL represents a majority of the encrypted traffic, a recent report from Palo Alto Networks, based on real enterprise traffic, shows that 23.8% of the applications using SSL were not using the standard SSL ports.[4] Enterprises with non-standard-encrypted traffic need to ensure that this is explicitly authorized.

According to a Gartner survey of network security vendors, less than 20% of firewalls, UTM and IPS deployments include network traffic decryption (see Note 1). This means the encrypted traffic

FIGURE 1 Impacts and Top Recommendations for Building a Traffic Decryption Strategy

Impacts	Top Recommendations
An increasing share of enterprise network traffic is encrypted, creating gaps in defense-in-depth effectiveness that security leaders should not ignore.	• Evaluate the security risks from uninspected encrypted network traffic, and update relevant risk indicators. • Quantify your current encrypted traffic mix, and anticipate a 10% to 20% yearly growth.
Complex sets of laws and regulations on privacy, along with a high risk of conflict with employees, kill most security leaders' outbound Web traffic decryption projects.	• Prepare for a legal assessment of traffic decryption, in addition to the safeguards being taken.
Security leaders face limited technology choices for enterprise network traffic decryption, and these solutions often induce high costs and poor user experience.	• Leverage existing network security solutions to enforce the outbound Web policy on SSL traffic. Then, establish a prioritized list of the traffic profiles you need to decrypt.

Source: Gartner (December 2013)

Table 1. Risks Based on the Nature of the Encrypted Traffic

Uninspected Encrypted Traffic	Threats
Employees' Web browsing over HTTPS	• Malware infection • Covert channel with the command and control server • Data exfiltration
Employees on an internal network connecting securely to DMZ servers	• Lateral expansion from infected hosts
Internet users connecting to the enterprise's public servers using encrypted protocols	• Reduced defense in-depth, with only one protection technology inspecting the incoming traffic

Source: Gartner (December 2013)

often is not protected with intrusion prevention technology. Defense in-depth is reduced to what dedicated solutions can provide.

For inbound traffic, decryption is often part of a performance optimization project with an application delivery controller (ADC) performing SSL offloading and, therefore, enabling the inspection of traffic. Ninety percent of enterprises with an ADC or a WAF decrypt inbound traffic.

However, the situation is not so good for outbound Web traffic: Gartner estimates that less than 50% of enterprises with secure Web gateways (SWGs) use them to decrypt and inspect SSL traffic. Along with the lack of coverage from firewalls and network IPSs, a majority of outbound SSL traffic is not inspected by any network security technology. Many network security solutions can decrypt only HTTPS and are unable to decrypt other protocols (such as SMTPS, IMAPS, SFTP or SSH), which could prevent an organization from achieving its expected coverage for encrypted traffic inspection. Enterprise data loss prevention and endpoint protection are alternate solutions that can compensate in some situations for the lack of network protection.

Organizations that leverage a man in the middle (MITM) approach to intercept and decrypt SSL traffic make themselves attractive targets to attackers (see Note 3). Decrypting the traffic exposes data that would be otherwise unavailable on the organization's network (credit card numbers, personal information and so on). Even when traffic is immediately re-encrypted on network security devices, this information might leak through the log files or be stored locally in temporary files.

Recommendations:

- Weigh the risks coming from uninspected encrypted network traffic, and update the key risk indicators accordingly. Raise awareness among key stakeholders.
- Initiate a multiyear plan to improve your organization's coverage of encrypted traffic, and start with inbound and outbound Web traffic.
- Quantify your current encrypted traffic mix, and anticipate a 10% to 20% yearly growth when evaluating future network security purchases.

Complex sets of laws and regulations on privacy, along with a high risk of conflict with employees, kill most security leaders' outbound Web traffic decryption projects

Gartner clients cite organizational complexity as the first reason why they would not tackle a decryption project before dealing with the technical issues. Local privacy laws could prevent or restrict an organization from decrypting traffic that is considered private communications (see Note 2). Enterprises should charge their legal departments to validate that they comply with local laws and regulations for:

1 Decrypting traffic

2 Intercepting communications that were not monitored due to encryption

3 Storing data ("data retention") previously unavailable due to encryption

Multinational enterprises could face additional challenges with regulations that vary based on the location of the employees. "Hub and spoke" architectures might create even more complex situations, with remote employees being in one country and the decryption being performed in another country.

Decrypting Traffic

The act of decrypting should not fall under any specific regulation. However, intercepting outbound SSL traffic requires replacing the public server certificate with a certificate created by the surveillance device (see Note 3). Stringent legal interpretation of MITM interception could tie interception to the network security device, viewing traffic interception as usurpation of the website's identity.

Employee Surveillance

Monitoring employees' communications and storing communications data are often restricted by law. In the U.S., the Electronic Communications Privacy Act (ECPA) and several state laws impact how enterprises can monitor their employees. Similar laws exist in certain European nations and in other countries (see Note 2). Adding encrypted communications to an existing surveillance program expands the scope of the program and might require updating the privacy policy and employee notifications for these reasons:

- Employees expect encrypted communications to be private.

- Data carried over the encrypted channel is more likely to include personal or confidential data, such as personally identifiable information (PII) and electronic personal health information (ePHI).

Enterprises should re-examine policies for Internet, social media and email usage to ensure they cover encrypted traffic, update the policies if need be, and inform employees if required or advised by the HR department.

Whitelisting categories of websites is a complementary compliance tactic. Gartner clients often put banking and health websites on a whitelist and do not decrypt this traffic. Webmail requires specific attention, since it is a vector for threats, but also carries private communications.

To reassure key stakeholders from the legal department, HR and worker councils, security teams should explain the level of automation for network traffic decryption and subsequent re-encryption, the amount of logged information, and the approval workflow for monitoring or changing security policy (see "Conduct Digital Surveillance Ethically and Legally: 2012 Update").

Data Retention

Network security appliances that perform traffic decryption can log connection metadata (IP and port, time stamp, and protocol headers). In the case of a dedicated decryption appliance forwarding decrypted traffic to a full-packet capture device, the whole data is stored. An enterprise firewall with application and user control features might also store additional application data and user identities in its log.

To improve the organization's compliance with local data retention laws (see Note 2), security teams in charge of the decryption project should check the amount of information logged on decrypted traffic for different protocols and reduce the amount of logged traffic when possible. It is also important to assess the right duration for data retention since minimum and maximum data retention durations might apply from distinct regulatory constraints.

Prepare for Environment Changes

Recent leaks about state-level access to encrypted communications increase the uncertainty around encryption technologies and regulations. As a safety measure, it is important to get ready for important changes around the legitimacy of existing encryption algorithms or the obligation to use new mechanisms. Organizations should prepare for such an eventuality with a privacy continuity plan, similar in nature to a business continuity plan. The privacy continuity plan would cover the impacts and action plan across the entire organization, in case an encryption algorithm (such as AES) or a protocol implementation (such as SSL or IPsec) suddenly becomes deprecated or vulnerable, such as what happened with RC4.[5] It should also prepare the organization for situations where changes in the software implementation or encryption algorithm prevent the inspection of traffic for security reasons.

For more Gartner research on privacy, see "Roundup of Privacy Research, 1Q13."

Recommendations:

- Prepare for a legal assessment of traffic decryption with network diagrams, types of decryption to occur, whitelists and data logged, in addition to the safeguards being taken.
- Review the existing privacy and network usage policy to determine if decrypting the traffic requires a policy update. Engage with HR and worker representatives throughout the entire decision or implementation life cycle.
- Make available to employees the elements that demonstrate how privacy issues are handled, including a list of whitelisted domains, sample log data and access restrictions for sensitive data.
- Draft a privacy continuity plan to anticipate situations where a flaw is found in an encryption algorithm or software implementation.

Security leaders face limited technology choices for enterprise network traffic decryption, and these solutions often induce high costs and poor user experience

Setting up outbound traffic decryption is complex, relying on MITM interception that impacts the enterprise network and user experience (see Note 3). A network security solution intercepting outbound HTTPS traffic analyzes a minimum of three connections for each SSL connection intercepted: (1) decrypting the client's SSL connection; (2) inspecting the decrypted HTTP; and (3) encrypting the SSL connection to the server.

Decrypting Traffic Has Multiple Effects on the Enterprise Network

Embedded hardware acceleration, when available on network security platforms, often provides limited value. A recent study from NSS Labs reported that decrypting SSL traffic on a firewall implies a loss of 74% for throughput and 87.8% for transactions per second.[6] The network latency also suffers, especially during the initial steps of the SSL connection. By the end of 2013, 1024-bit RSA keys will be deprecated by certificate authorities in favor of 2048-bit keys.[7] Longer keys will increase the workload needed by the SSL decryption engine, and worsen the existing situation.

Enabling traffic decryption or re-encryption on a firewall, SWG or an IPS will reduce the overall performance of the appliance, often by more than 80%, which, depending on the traffic mix for the organization, often means effectively doubling the network traffic inspection spend. It impacts also the overall cost of the network security solution. It forces security buyers to purchase significantly more expensive appliances to handle the additional workload. This reflects on initial hardware purchase costs, as well as on every support and software option since they are often priced as a percentage of the initial appliance cost.

This performance degradation reflects on user experience, and can prove unacceptable from an employee productivity standpoint. Gartner clients who have initiated SSL decryption projects report that the performance impact is noticeable and is not limited to encrypted traffic when decryption is being performed on the network security platform. Users complain about it, which leads to some projects being halted quickly after the production launch.

Some protocols and applications cannot be proxied, which could create disruptions for business-critical applications that were previously "untouched," thanks to SSL encryption. Before enabling traffic decryption, organizations should seek from their network security vendors a list of known applications that need to be whitelisted.

The performance impact might be lower for inbound traffic, especially in a setup where incoming SSL is decrypted but not re-encrypted ("SSL offloading").

Mitigation Techniques Exist but Are Not Yet Mature

Enterprises can use dedicated decryption appliances that decrypt the traffic once and make decrypted traffic available to multiple stand-alone security protections. This improves the overall performance and simplifies the encryption key management, but could create an environment that is more complex to manage, maintain and audit. It also adds another potential point of failure to the infrastructure. Unfortunately, there are only a few vendors in this space, which limits the available choices.

One more direct way to limit the impact of traffic decryption while improving the overall security coverage is to minimize the amount of traffic to be decrypted. Blocking unwanted servers based on their reputation scores or on specific certificate information is an example of such a work-around. Alternatively, reputation can be used to not inspect "known good" destinations and sources. Most decryption features and products have yet to optimize decryption well and instead opt for a full or nearly full proxying, even for categories where administrators set up a decryption bypass. Organizations using ADCs do SSL termination for inbound traffic. Traffic inspection can be performed by the ADC, or another network security solution can be positioned on the network segment where the traffic is already decrypted.

In addition, content delivery networks (CDNs), vendors offering security cloud services for inbound Web traffic and cloud-based SWGs can decrypt the traffic off-premises. While this relieves the internal network from the burden of traffic decryption, delegating the decryption implies having to share the Web server's secret keys. It allows access to the decrypted data to the cloud service provider, which needs to ensure that it complies with the organization's requirements on privacy.

Recommendations:

- Leverage existing network security solutions to enforce outbound Web policy on SSL traffic, based on server reputation or the information available from the SSL certificate. Then, establish a prioritized list of the traffic profiles you need to decrypt.
- Ensure that network traffic will be decrypted only once. Then, decide whether you will decrypt with your existing network security appliances or with dedicated decryption appliances.
- Ensure that the impact of decrypting traffic based on today's traffic and future growth is reflected in network security budgets.

Legal Disclaimer

Gartner does not practice law. Therefore, the opinions and recommendations in this document should not be construed as legal advice. Gartner recommends that entities subject to legislation seek legal counsel from qualified sources.

Evidence

[1]Yahoo will switch to HTTPS by default. A. Peterson, B. Gellman and A. Soltani, "Yahoo to Make SSL Encryption the Default for Webmail Users. Finally." The Washington Post, The Switch blog, 14 October 2013.

Wikipedia plans to progressively switch to HTTPS by default. R. Lane, "The Future of HTTPS on Wikimedia Projects," Tech blog, Wikimedia Foundation, 1 August 2013.

[2]There is no independent organization that gives definitive statistics on global HTTPS usage. Therefore, Gartner has conducted secondary research to consolidate data from several sources, including reports from clients. The share of SSL traffic might vary greatly among different verticals, with financial institutions getting up to 40% of SSL traffic, whereas retailers get a lower than average share of SSL traffic.

[3]Zeus trojan downloads malware using HTTPS. B. Stone-Gross and R. Dickerson, "Upatre: Another Day Another Downloader," Dell SecureWorks, 4 October 2013.

Malware attached to a spam message about the Boston Marathon bombing uses SSL to communicate with its command and control server. N. Villeneuve, "Targeted Attack Campaign Hides Behind SSL Communication," TrendLabs Security Intelligence blog, Trend Micro, 25 April 2013.

Attackers using HTTPS in a drive-by attack. A. Makhnutin, "HTTPS Working for Malicious Users," Securelist blog, Kaspersky Lab, 8 October 2013.

Malware using public online services with HTTPS — Evernote and Google Docs. B. Donohue, "Cybercriminals Use Evernote as C&C," Threatpost blog, Kaspersky Lab Security News Service, 28 March 2013.

L. Constantin, "Malware Uses Google Docs as Proxy to Command and Control Server," Computerworld, 19 November 2012.

[4]"The Application Usage and Threat Report: An Analysis of Application Usage and Related Threats Within the Enterprise," Palo Alto Networks, February 2013. Page 16: "85 of the 356 applications that use SSL never use port 443, nor

do they use SSL defined ports (37 hop ports, 28 use port 80, 20 use other ports)."

[5]Recommendation to stop using RC4. Swiat, "Security Advisory 2868725: Recommendation to Disable RC4," Microsoft TechNet blogs, 12 November 2013.

Threats to SSL security. M. Green, "How Does NSA Break SSL?" A Few Thoughts on Cryptographic Engineering blog, 2 December 2103.

[6]J. W. Pirc, "SSL Performance Problems: Significant SSL Performance Loss Leaves Much Room for Improvement," NSS Labs, June 2013.

[7]D. Dulay, "Out With the Old: Stronger Certificates With Google Internet Authority G2," Google Online Security blog, 18 November 2013.

Note 1

Gartner's SSL Decryption Survey

During the second half of 2013, Gartner sent a survey to 56 major network security vendors providing enterprise firewalls, SWGs, UTM, IPSs, WAFs and dedicated SSL decryption appliances to understand how their clients were tackling traffic decryption, and 12 vendors responded. The study examined the technologies for traffic decryption and obtained market data about decryption technology usage.

A team of Gartner analysts who follow network security developed the survey and conducted several client inquiries about the current state of their decryption strategies. Both data sources contributed to the estimates provided in this research.

Note 2

Sample Laws Related to Cryptography, Employee Surveillance and Data Retention

Bert-Jaap Koops, "Crypto Law Survey."

U.S. — Electronic Communications Privacy Act of 1986.

U.S. — State laws related to Internet privacy, from the National Conference of State Legislatures.

Canada — The Personal Information Protection and Electronic Documents Act (PIPEDA), Office of the Privacy Commissioner of Canada, 1 April 2011.

Europe — Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Australia — Workplace Surveillance Act, 2005. Part 2, Section 10 requires 14 days' prior notification. Section 12 gives additional requirements for computer surveillance.

Note 3

Intercepting Encrypted Traffic

Decrypting SSL must be done in-line for outbound Web traffic, using an MITM approach. The appliance performing traffic decryption replaces the public Web server certificate with its own custom certificate. To avoid any warning on the endpoint, the client browser must trust the certificate authority that signs these ad hoc certificates. This implies that the network security appliance signs SSL certificates with a certificate authority already trusted in the enterprise, or deploys a certificate on every corporate endpoint, which adds to the burden of SSL decryption projects. A careful user who looks at the certificate will likely notice the interception.

For inbound traffic, this can be done in-line with an ADC or a WAF. This could also be done on a copy of the traffic, since the enterprise owns the server certificates and can provide them to the decryption solution. Working on a copy of the traffic avoids any impact on performance, but does not permit threats to be blocked. Security architects often choose SSL offloading in these situations, especially when an ADC or a WAF is present.

Technical implementations, such as certificate pinning, could prevent MITM interception. Some applications also use SSL encryption as a way to free them from the protocol standard. Once traffic decryption is in use, this often generates false alerts (false positives) and blocks "legitimate" traffic. For example, Microsoft Windows updates would need to be whitelisted.

Source: Gartner Research, G00258176, Jeremy D'Hoinne, Adam Hils, 9 December 2013

About Venafi

Venafi is the market leading cybersecurity company in Next-Generation Trust Protection (NGTP). As a Gartner-recognized Cool Vendor, Venafi delivered the first trust protection platform to secure cryptographic keys and digital certificates that every business and government depend on for secure communications, commerce, computing, and mobility. As part of an enterprise infrastructure protection strategy, Venafi solutions prevent attacks on trust with automated discovery and intelligent policy enforcement, detects and reports on anomalous activity and increased threats, and remediates errors and attacks by automatically replacing keys and certificates.