DECRYPTION: WHY, WHERE AND HOW

Why: The Case for Decryption

Internet traffic encrypted with Secure Sockets Layer or Transport Layer Security protocols – SSL and TLS, respectively – is on an explosive upturn. According to the Google® Transparency Report: "Desktop users load more than half of the pages they view over HTTPS and spend two-thirds of their time on HTTPS pages."[1]

Given the primary benefits of encryption – the private and secure exchange of information over the internet, and compliance with certain regulations, such as the Health Insurance Portability and Accountability Act and the Payment Card Industry Data Security Standard, or HIPAA and PCI DSS – the upward trend in SSL adoption is expected to continue. The next major revision of HTTP 1.1 is HTTP/2, and although the standard itself does not require encryption, most client implementations have stated they will only support HTTP/2 over TLS, which effectively makes encryption mandatory. Major browsers, including Chrome®, Firefox®, Safari® and Internet Explorer®, are in various stages of marking HTTP webpages "not secure."

Encryption is a great means for secure and private business information exchange, and it is necessary for compliance. However, encrypted traffic is essentially opaque data that leaves organizations blind to security threats contained inside. Unfortunately, criminals have learned to exploit this lack of visibility and identification to hide from security surveillance within encrypted traffic and deliver malware. Even legitimate websites that use SSL can be infected with malware. Moreover, attackers increasingly use SaaS applications to deliver malware. An attacker can place an infected file in a legitimate shared folder in an organization's sanctioned file storage application, such as Box or Dropbox®, and from there, the infected file can easily spread to users who sync their files with the folder.

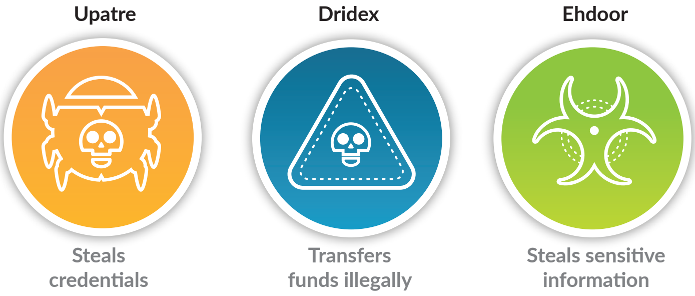

Figure 1: Examples of malware transferred over encrypted traffic based on Palo Alto Networks Unit 42 threat research

Without the ability to decrypt, classify, control and scan SSL-encrypted traffic, it's impossible for an organization to adequately protect its business and its valuable data from modern threats. This is where SSL decryption – the ability to decrypt, inspect and re-encrypt internet traffic before it is sent to its destination – comes into play. Decryption, one of the "10 Things Your Next Firewall Must Do," is required for several security-related actions, including threat prevention, advanced malware prevention, file blocking, data filtering and blocking of malicious webpages.

Where Should You Decrypt? The Options

Many technical options are available to decrypt traffic on your network, including web proxies, application delivery controllers, SSL visibility appliances and next-generation firewalls. Where it's best to decrypt SSL traffic depends on which option provides the greatest protection with the least management overhead – in other words, maximum security return on investment.

Web Proxies

A web proxy acts as a "middleman," decrypting and inspecting outbound traffic before re-encrypting it and sending it to its destination (see Figure 2). However, web proxies are limited to inspecting and securing web traffic, which includes HTTP and HTTPS. They are typically deployed on well-known web ports, such as 80 and 443. If an application uses non-web ports or protocols, web proxies can't see the traffic, defeating the purpose of gaining complete visibility and control over encrypted traffic on your network. It's like deploying airport security in only one major airport and leaving the rest exposed. Proxies also require you to modify your browser's proxy settings or use a proxy auto-config file, which adds more management overhead and another area to diagnose if users can't access the internet.

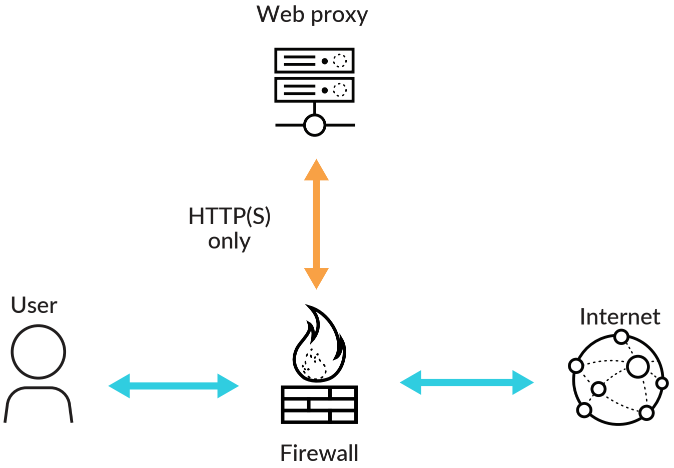

Figure 2: Decryption and re-encryption by a web proxy

[1] https://transparencyreport.google.com/https/overview?hl=en

Application Delivery Controllers

SSL offload is one of the functions performed by Application Delivery Controllers. An ADC deployment usually requires two separate boxes – one to decrypt traffic and one to re-encrypt.

The problem with ADC deployments is that traffic travels unencrypted between the ADC devices, meaning rogue IT personnel or anyone with access to the physical network connecting the devices has easy access to the data. An adversary can simply port mirror and run a packet capture to retrieve sensitive data in clear text. This undermines the promise of complete confidentiality that is one of the fundamental purposes of encryption and may also violate compliance laws in some industries and geographies.

SSL Visibility Appliances

SSL visibility appliances decrypt traffic and make it available to all other network security functions that need to inspect it, such as web proxies, data loss prevention systems and antivirus (see Figure 3).

The problem is that these devices increase capex and opex. In addition to the one-time cost, an SSL visibility appliance becomes yet another device in the network that needs to be managed, maintained and updated, with a configuration and rule base entirely different from other security devices. Instead, if one security device is used to decrypt traffic and broker it to all other complementary devices, there is no need to add SSL visibility appliances.

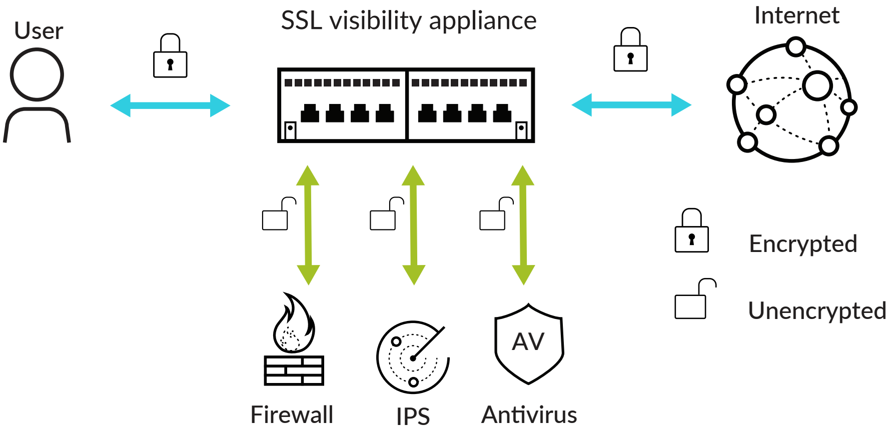

Figure 3: Decryption through an SSL visibility appliance

Where Should You Decrypt? The Recommendation

Organizations are replacing traditional legacy firewalls with next-generation firewalls at a fast clip. In fact, according to Gartner, "enterprise firewall" is now synonymous with NGFW.[2] NGFWs include security functions, such as application and user control, intrusion prevention systems, URL filtering, network antivirus, and advanced malware analysis. Customers are using firewall refresh opportunities to consolidate multiple security devices into an NGFW to take advantage of the cost savings, enhanced security and ease of managing a single device. In addition, reducing devices and consolidating security functions dramatically reduces the complexity and time consumption of troubleshooting since the network topology is far simpler.

Next-Generation Firewalls With and Without Decryption		
Use Cases Supported	**With Decryption**	**Without Decryption**
Identify size of the payload, bandwidth	✓	✓
Identify the source of the traffic – who and where inside the company	✓	✓
Identify source and destination IP addresses, port, and protocol	✓	✓
Identify the application used	✓	—
Identify the data type sent	✓	—
Identify if corporate usage policy was violated	✓	—
Stop transfer of specific file types (e.g., EXE, RAR)	✓	—
Stop loss of sensitive data	✓	—
Identify and stop threats inside an encrypted tunnel	✓	—

Figure 4: NGFWs with and without decryption

[2] "Magic Quadrant for Enterprise Network Firewalls," 10 July 2017 by Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur

NGFWs are the most suitable devices to decrypt traffic, providing several advantages:

1. Decrypted traffic is stored in memory and not sent to other devices. This preserves SSL's promise of confidentiality and meets compliance regulations.
2. NGFWs can see and decrypt traffic on all ports, providing visibility into all applications, users, content and threats.
3. By consolidating multiple functions into a single device, an NGFW provides enhanced security. For example, it can block known threats using vulnerability protection, antivirus and anti-spyware signatures, and by blocking malicious websites. It can also send new potential threats to the advanced malware analysis environment. If threats are identified, new protections can be delivered and distributed globally within minutes.
4. An NGFW can broker decrypted traffic to other complementary devices as appropriate, such as for long-term retention of logs in forensics appliances.
5. NGFWs provide an easy-to-use management interface that reduces complexity and opex. For example, you can combine applications, users, content, URLs, threat prevention and advanced malware analysis into a single rule.

NGFW Buying Criteria for Your Decryption Needs

Not all NGFWs are equal, and unfortunately, it can be difficult to distinguish between firewalls with similar claims. It is important to have clear guidelines for evaluating an NGFW prior to purchase. This will ensure the firewall can support a comprehensive breach prevention strategy, which includes SSL decryption.

Refer to the "Firewall Buyer's Guide" for a list of all business requirements your next firewall should address as well as advice on how to create an RFP and a functional test plan to assist in the vendor and product selection process.

Here are the criteria to compare the SSL decryption capabilities of NGFWs:

1. **Granularly choose what to decrypt:** Privacy concerns and regulations require that your NGFW can selectively decrypt traffic based on criteria flexible enough to meet your needs. These criteria can include user; URLs; URL categories, such as finance or health; externally hosted URL lists to comply with regulations; IP address-based source and destination; ports; and protocols. To catch potential malware, the firewall must also allow you to exclude applications from decryption when they are running on their default ports but continue to decrypt those same applications when they are detected on nonstandard ports.
2. **Exclude applications that may break upon decryption:** Application vendors sometimes use HTTP Public Key Pinning, also known as certificate pinning, to resist impersonation by attackers using wrongly issued or otherwise fraudulent certificates. When this technique is used, network security devices may break some applications upon decryption. Your NGFW must allow you to exclude such traffic easily by using hostname of the website or application in the exclusion rule. If the NGFW forces you to define exclusions based on distinguished and common names of certificates, it is too complex. To make it even easier, the NGFW should ship with predefined exclusions for well-known applications that break upon decryption.
3. **Enforce certificate status:** You may want to drop traffic for which the SSL certificate is expired, the server certificate issuer is untrusted or the certificate has been revoked. Your NGFW must allow you to accept or deny traffic that meets any combination of these criteria.
4. **Enforce cipher suites:** Cipher suites include key exchange algorithms, such as RSA, DHE and ECDHE; encryption algorithms, such as 3DES, RC4 and variants of AES; and authentication algorithms, such as MD5 and SHA variants. The NGFW must support multiple cipher suites and allow you to enforce those that meet your security requirements. You should be able to choose whether to allow or block traffic that does not meet your specified cipher suites.
5. **Enforce protocol version:** You may need to enforce the use of specific SSL/TLS versions, such as TLS 1.2. The NGFW must offer flexibility in enforcing specified protocol versions and blocking traffic that uses any weaker version.
6. **Integrate with hardware security modules:** An HSM is a physical device that manages digital keys, including secure storage and generation. It provides both logical and physical protection of these materials against unauthorized use and potential adversaries. Your NGFW must integrate with an HSM for storing private keys and master keys. Even if your organization does not currently require keys to be stored in an HSM, you may need this functionality in the future.
7. **Allow users to opt out of SSL decryption:** In some cases, you might need to alert users that the NGFW is decrypting certain web traffic and allow them to terminate sessions they do not want inspected. Your NGFW must allow SSL opt-out so users are notified that their session is about to be decrypted and can choose to proceed or terminate the session.
8. **Decrypt outbound and inbound traffic:** The NGFW must be able to decrypt traffic in both directions so you have the flexibility to deploy it in front of users or your web servers to decrypt outbound or inbound traffic, respectively.
9. **Decrypt SSH:** Most traffic on the internet is encrypted via SSL/TLS. However, Secure Shell, or SSH, can also be used to encrypt and tunnel traffic inside your network. For example, some internal data center applications may use SSH, which is allowed by policy. To prevent users from using SSH to evade your acceptable use or threat prevention policies, your NGFW must support decryption of SSH traffic that meets your criteria.

10. **Use hardware crypto acceleration:** SSL decryption is very resource-intensive. Your NGFW must use hardware crypto acceleration to maintain high performance while decrypting traffic.

11. **Share threat intelligence and stop threats everywhere based on shared threat intelligence:** There are cases when the traffic is not decrypted on the NGFW, due to privacy concerns or certificate pinning, for example. In these cases, if the NGFW is part of a platform that acts on threat intelligence gathered from the network, endpoint and cloud, you will still be able to stop threats, even if the traffic is not decrypted on the network. Let's say a threat passes through the network undetected in encrypted traffic and reaches the endpoint. The platform shares threat intelligence between the network, endpoint and the cloud, and advanced endpoint protection based on this shared intelligence blocks the threat before the attack succeeds. In addition, information about this threat is shared with the entire platform to make network and cloud security more intelligent. This is a distinct advantage that an NGFW acting alone cannot provide.

It is best if your NGFW vendor has plans to support the following forward-looking trends, which are likely to become critical:

- **HTTP/2:** This is a major revision of the HTTP network protocol used by the World Wide Web. It was developed from the earlier, experimental SPDY protocol, originally developed by Google. Although the standard itself does not require encryption, most client implementations have stated that they will only support HTTP/2 over TLS, which effectively makes encryption mandatory.
- **TLS 1.3:** Having been approved by the Internet Engineering Task Force, TLS 1.3 is expected to make all secure internet connections faster and safer. Highlights in TLS 1.3 include faster data delivery, removing non-AEAD encryption and non-PFS key exchange, and dropping renegotiation.

The Security Impact of HTTPS Interception

The University of Michigan, University of Illinois Urbana-Champaign and others published a 2017 study called "The Security Impact of HTTPS Interception" that examines the prevalence and impact of HTTPS interception by network security devices. The findings indicate that nearly all interceptions reduce connection security, and many introduce severe vulnerabilities.

This is of concern to network security administrators because the intention behind intercepting and decrypting HTTPS traffic is to gain visibility and control. The paper indicates several reasons why interceptions reduce connection security:

- The default configuration for many of these network security devices weakens security, for example, by using RC4-based ciphers.
- Many devices have broken certificate validation.
- The installation process for many devices is convoluted and crash-prone.
- Device configuration is confusing.

Therefore, it is critical to ensure that your NGFW:

- Does not enable RC4-based ciphers by default. The recommended best practice security policy is to avoid weak algorithms, such as MD5, RC4, SHA1 and 3DES.
- Blocks invalid certificates by default, including sessions with expired certificates, untrusted issuer certificates and unknown status certificates.
- Blocks sessions with unsupported versions. The recommended best practice security policy blocks use of vulnerable SSL/TLS versions, including TLS 1.0 and SSLv3.
- Uses Online Certificate Status Protocol and/or certificate revocation lists – OCSP and CRLs – to verify the revocation status of certificates.
- Does not store decrypted traffic on disk. The details must be only stored in memory, meeting security and regulatory requirements.

In summary, decrypting traffic alone can weaken security. However, given due diligence while buying an NGFW, and if you follow best practices, decryption will not only provide you the necessary visibility into all traffic, but also protect you from adversaries that hide threats in encrypted tunnels.

How to Enable SSL Decryption: People, Process and Tools

Enabling SSL decryption is not just about having the right technology in place. A triad of people, process and tools must align and work together toward the same goal.

People	**Several teams need to work together:** • Legal/Compliance team to decide what types of traffic can be decrypted. • Human Resources team to communicate the impact of decryption to everyone who uses your network, including employees, guests and contractors. In addition, computer usage policies, guest sign-in waivers and contractor usage policies must all be updated to stay compliant. • Security Governance team to manage public key infrastructure, or PKI. • IT team to install certificates on endpoints as well as manage design and sizing. • Server team to ensure decryption of inbound traffic destined to web servers.
Process	**Enabling SSL decryption involves multiple processes, such as:** • Performance analysis for design and sizing. • Testing for user experience impact and deployment issues as well as scenarios such as expired certificates and user opt-out. • Operations support for dealing with possible decryption-related issues. • Change control and phased deployment of decryption.
Tools	**Successful deployment and analysis of results requires tools for various functions, including:** • Certificate management. • Network performance analysis. • NGFW for decryption policy creation, exclusions, logging and reporting.

How to Enable SSL Decryption: Best Practices

With an agreement between teams and a handle on the appropriate processes and tools, you can begin decrypting traffic. Follow these best practices for optimum results and to avoid common pitfalls:

1. **Determine the sensitive traffic that must not be decrypted:** Best practice dictates that you decrypt all traffic except that belonging to sensitive categories, such as Health, Finance, Government, Military and Shopping.
2. **Add exclusions to bypass decryption for special circumstances:** You will need to bypass decryption in certain circumstances, such as for traffic that breaks upon decryption, specific users who need to bypass decryption for legal reasons, or partner websites that may be allowed to bypass strict certificate checks. Make sure you create such exclusions only when warranted and keep them to a minimum.
3. **Set up verification for certificate revocation status:** To verify the revocation status of certificates, the NGFW uses OCSP and/or CRLs. Make sure that certificates presented during SSL decryption are valid by configuring the firewall to perform CRL/OCSP checks.
4. **Configure strong cipher suites and SSL protocol versions:** Consult your security governance team to find out which cipher suites must be enforced and determine the minimum acceptable SSL/TLS protocol version. For example, your security team may want to use the DHE or ECDHE key exchange algorithms to enable perfect forward secrecy, or PFS, along with TLS 1.2 protocol. Alternatively, the team may want to block use of vulnerable SSL/TLS versions, such as TLS 1.0 and SSLv3, and avoid weak algorithms, such as MD5, RC4, SHA1 and 3DES. Enforce your security team's recommendations on your NGFW.
5. **Deploy the decryption certificate from your enterprise root certificate authority:** Deploy this certificate on your NGFW so that your end users do not see SSL certificate warning messages.
6. **Decrypt SSH in addition to SSL:** SSH is required for some applications, but can be misused, as mentioned earlier. For this reason, it is recommended that you allow SSH to be used only for applications and users that need it in addition to enabling SSH decryption.

To learn more, check out the following resources:

✓ SSL Decryption Webpage

✓ Best Practice Assessment: This complimentary assessment helps you to maximize the capabilities of your NGFW, like SSL decryption, to prevent successful cyberattacks.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com