Decryption: Why, Where, and How

Internet traffic encrypted with Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocols is on an explosive upturn. According to the Google Transparency Report, "Nearly 95% of traffic uses encryption depending on the platform."[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 (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS)—the trend in encrypted traffic is expected to continue. The major revision of HTTP 1.1 to HTTP/2, which offers significant performance improvements and an enhanced user experience compared to older protocols, effectively makes encryption mandatory as browsers support HTTP/2 over TLS. Major browsers, including Chrome®, Firefox®, Safari®, and Microsoft Edge®, now mark plaintext HTTP webpages as "not secure."[2]

1. "Google Transparency Report," Google, accessed May 12, 2020, https://transparencyreport.google.com/https/overview?hl=en.
2. "A milestone for Chrome security: marking HTTP as 'not secure'" Google, July 24, 2018, https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure.

Encryption is a great means for secure and private business information exchange, and it is necessary for compliance. Uninspected, encrypted traffic essentially leaves organizations blind to security risks contained inside. Unfortunately, attackers have learned to exploit this lack of visibility and identification to hide from security inspection within encrypted traffic and deliver malware. Even legitimate websites that use TLS can be exploited by attackers to host malware. Today, more than 70% of malware campaigns use some type of encryption to conceal malware delivery, command-and-control (C2) activity, or data exfiltration, enabling them to evade security measures.[3] See figure 2 for a look at current trends with TLS.

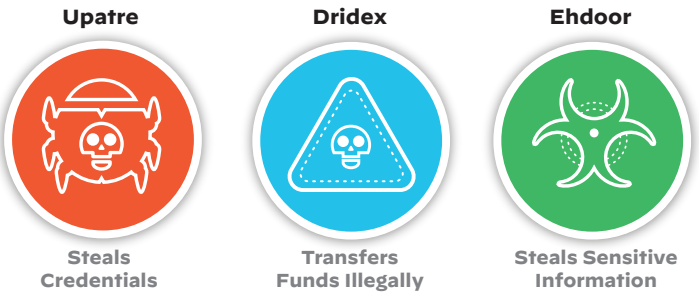

Figure 1: Examples of malware transferred over encrypted traffic based on Palo Alto Networks Unit 42 threat research

An attacker can upload files containing malware, which the user then downloads and executes, compromising the user's endpoint. Moreover, attackers increasingly use sanctioned software-as-a-service (SaaS) applications, such as Dropbox®,[4] to deliver malware. An attacker can place an infected file in a legitimate shared folder in an organization's sanctioned file sharing application, and from there, the infected file can easily spread to users who sync their files with the folder.

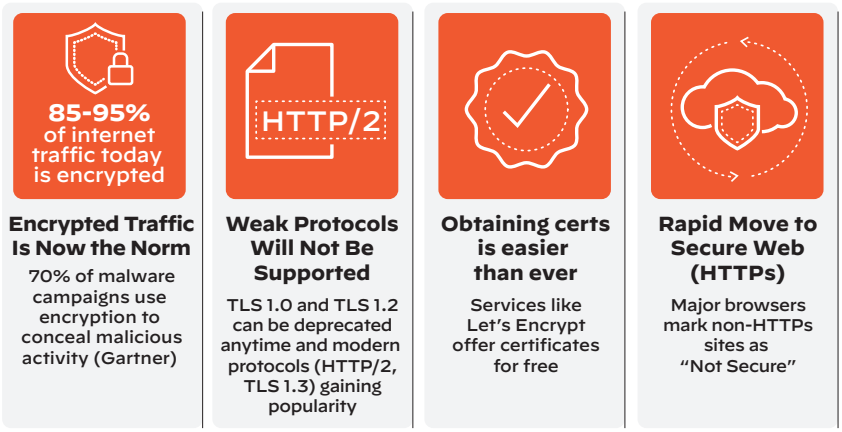

Figure 2: Massive risks within encrypted traffic

Without the ability to decrypt, classify, control, and scan TLS-encrypted traffic, it's impossible for an organization to adequately protect its business and its valuable data from modern threats. This is where TLS decryption—the ability to safely and securely decrypt, inspect, and re-encrypt internet traffic before it is sent to its destination—comes into play.

Phishing and data loss attacks have become highly prevalent, with about 70% of breaches today using stolen credentials. Decryption is required for several security-related actions, including preventing credential-based attacks, preventing sensitive content from leaving an organization, preventing advanced malware, and blocking both malicious URLs and risky files. Figure 3 summarizes the reasons to enable decryption.

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 and decryption appliances, and next-generation firewalls (NGFWs). Where it's best to decrypt TLS/SSL traffic depends on which option provides the greatest protection with the least management overhead—in other words, maximum security return on investment.

Figure 3: Reasons to deploy decryption in your environment

3. "Keeping Up With Encryption in 2020," Security Boulevard, April 6, 2020, https://securityboulevard.com/2020/04/keeping-up-with-encryption-in-2020.
4. "Cyberattackers are delivering malware by using links from whitelisted sites," TechRepublic, March 9, 2020, https://www.techrepublic.com/article/cyberattackers-are-delivering-malware-by-using-links-from-whitelisted-sites.

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 4). 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. For example, Office/Microsoft 365™ applications work across multiple ports besides 80/443.[5] Regular proxies would miss traffic on these other ports. Moreover, web proxies cannot access non-web 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 terminal 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.

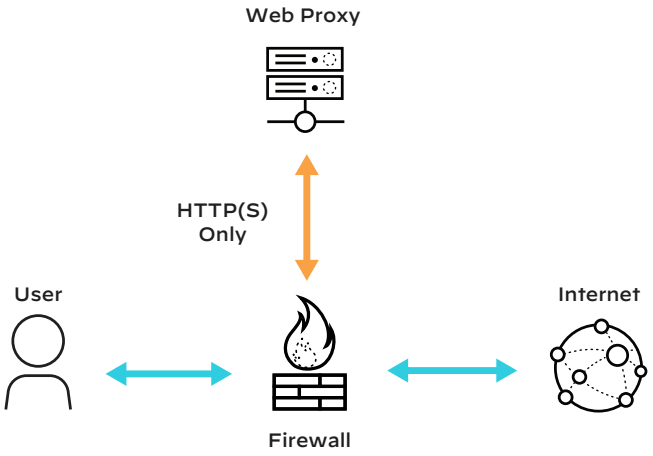

Figure 4: Decryption and re-encryption by a web proxy

Application Delivery Controllers

SSL offload is one of the functions performed by Application Delivery Controllers (ADCs). An ADC deployment usually requires two separate appliances: one to decrypt traffic and one to re-encrypt. Given the two-stage operation, the problem with ADC deployments is that, once decrypted, the traffic travels unencrypted between the ADC devices until it hits the encryption device. An adversary can simply sniff the traffic and retrieve sensitive data in cleartext or manipulate the traffic. This undermines one of the fundamental purposes of encryption—the promise of complete confidentiality—and may violate compliance laws in some industries and geographies.

SSL Visibility and Decryption 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 5).

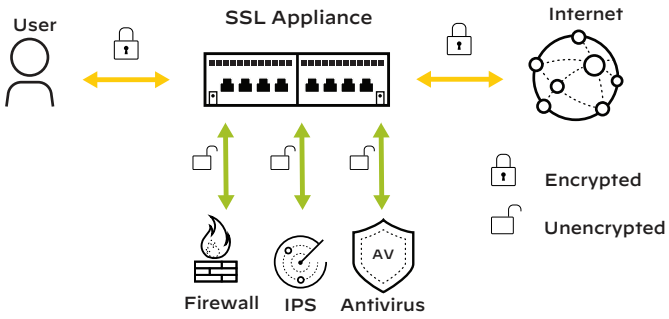

Figure 5: Decryption through an SSL visibility and decryption appliance

The Recommendation: NGFWs

According to Gartner, "enterprise firewall" is now synonymous with next-generation firewall.[6] Organizations 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.

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

- Decrypted traffic does not leave the NGFW, and inspection of traffic to prevent threats takes place within the firewall. This preserves TLS's promises of confidentiality and integrity.
- Full coverage of all web and non-web traffic, and the ability to see and decrypt TLS traffic, provides visibility into all applications, users, content, and threats. You can have application visibility, data visibility, and threat prevention for SaaS applications like Google Workspace™ with granular control over what data can be uploaded and downloaded.

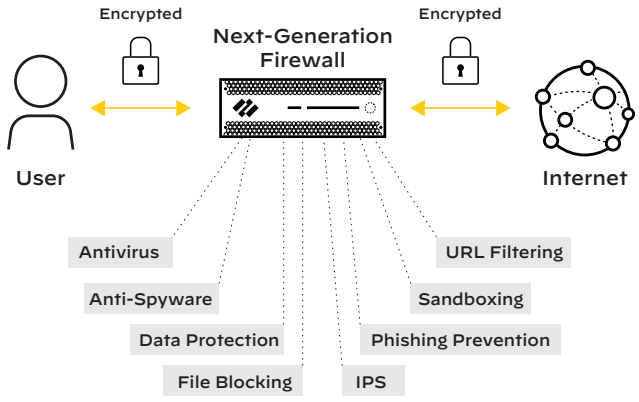

Figure 6: Decryption on an NGFW

Note: A "—" indicates limited or no support.

5. "Office 365 URLs and IP address ranges," Microsoft, April 28, 2020, https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges?redirectSourcePath=%252fen-us%252farticle%252fOffice-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2.
6. Jeremy D'Hoinne, Adam Hils, Rajpreet Kaur, "Magic Quadrant for Enterprise Network Firewalls," Gartner, July 10, 2017, https://www.gartner.com/en/documents/3757665.

Table 1: NGFWs 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 usage	✓	—
Identify the data 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	✓	—
See complete details of all encrypted connections	✓	—
Log all decryption sessions	✓	—
Get full visibility into TLS 1.3	✓	—
Get full visibility into HTTP/2	✓	—
Easily troubleshoot decryption issues	✓	—
Use URL categorization to comply with privacy regulations	✓	—

- A single device with multiple consolidated security functions provides enhanced security. For example, once you decrypt traffic and find malware, it blocks known threats and malicious websites using vulnerability protection, antivirus, and anti-spyware signatures. In addition, having fewer devices means simpler network topology and less time spent troubleshooting.
- An easy-to-use management interface reduces complexity and opex. For example, you can combine applications, users, content, URLs, threat prevention, and advanced malware analysis into a single policy to safely decrypt your traffic.
- An NGFW can also intelligently broker all traffic (TLS, decrypted TLS, and non-TLS) to third-party security tools, such as IPS, IDS, DLP, and forensic appliances.

Next-Gen Firewall 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 you purchase helps you achieve a comprehensive breach prevention strategy, which includes TLS decryption.

Refer to the "Next-Generation 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 TLS 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, device, IoT, workload, and URL Filtering to exclude applications such as finance or health, externally hosted URL lists to comply with regulations, IP address-based source and destination, ports, and protocols.

2. Exclude Apps That May Break upon Decryption

Application vendors sometimes use 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.

3. Enforce Certificate Status

You may want to drop traffic for which the TLS 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. Control 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 only allow 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, and you should be able to disable weak algorithms and cipher suites that leave you vulnerable to downgrade attacks, where hackers force connections to your server to use outdated protocols with known exploits. Otherwise, these techniques can leave your encrypted connections open to man-in-the-middle and other types of attacks.

5. Enforce Protocol Version

You may need to enforce the use of specific TLS/SSL versions, such as TLS 1.2, to leverage the security improvements over earlier versions, stay complaint with security standards, or remain active as browsers stop supporting old protocols. The NGFW must offer flexibility in enforcing specified protocol versions and blocking traffic that uses any weaker version.

6. Integrate with Hardware Security Models

The most secure solution for storing encryption keys is a hardware security module (HSM)—a physical device that manages digital keys. An HSM is a trust anchor. HSMs generate trusted certificates and keys and store them securely. The advantages are their high performance and ability to protect any content from unauthorized access. Your NGFW must integrate with an HSM for storing private keys and master keys.

7. Allow Users to Opt Out of TLS 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 TLS 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

To effectively decrypt all traffic, the NGFW must be able to decrypt in both directions, giving you the flexibility to deploy it in front of users or your web servers to decrypt outbound or inbound traffic, respectively. Otherwise, asymmetric decryption can be like listening to only half of a conversation and can cause incomplete SSL decryption.

9. Maintains Performance

TLS decryption can be resource-intensive. While your NGFW provides the throughput (i.e., performance) you need to secure your network, it must meet performance expectations even when decryption is turned on. With advances in NGFW performance capabilities, it is now much easier to meet these performance expectations.

10. Share Threat Intelligence and Stop Threats Based on Shared Intelligence

There are cases when the traffic is not decrypted on the NGFW, such as for privacy concerns or certificate pinning. 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 a NGFW acting alone cannot provide.

11. Easy Deployment

Deploying and implementing decryption is difficult, and enterprises often don't have the expertise or time to undertake decryption projects. Security teams spend considerable time trying to resolve issues and are under pressure to maintain business continuity. As a result, they may choose not to decrypt or give up midway. Your NGFW must make deploying decryption easy and offer full logging for visibility into the details of all encrypted connections to help you troubleshoot decryption-related issues and easily assess their security posture.

12. Support for Modern Protocols

It is best if your NGFW vendor supports the following forward-looking trends, which are gaining widespread adoption.

- **HTTP/2:** This is a major revision of the HTTP network protocol used by the World Wide Web. It improves page load times by 50% and significantly enhances user experience. Today, about half of domains use HTTP/2, and all major browsers support HTTP/2 only over TLS, which makes encryption mandatory.
- **TLS 1.3:** Having been approved by the Internet Engineering Task Force, TLS 1.3 makes 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. About one-fourth of all TLS traffic today is encrypted in TLS 1.3. Your NGFW must offer end-to-end TLS 1.3 support without downgrading to older, insecure protocols, keeping the security intact.

13. Network Packet Broker

Modern NGFWs can intelligently forward all types of traffic (e.g., TLS, decrypted TLS, and non-TLS) to third-party security tools from a single device, eliminating the need to buy and manage multiple appliances and decrypt traffic multiple times. This allows organizations to simply their networks, reduce operational complexity, optimize network performance, and maximize existing security tools' efficacy by selectively sending only the necessary traffic to a given tool.

Table 2: How to Enable TLS Decryption

People	**Several teams need to work together:** • Legal/Compliance team to inform 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 (PKI). • IT team to install trusted certificates on endpoints as well as manage design and sizing. • Server team to ensure decryption of inbound traffic destined to web servers.
Process	**Enabling TLS 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.

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," which 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 TLS/SSL versions, including TLS 1.0, TLS 1.1, and SSLv3.
- Uses Online Certificate Status Protocol (OCSP) and/or certificate revocation lists (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 a 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 TLS Decryption: People, Process, and Tools

Enabling TLS 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.

How to Enable TLS Decryption: Best Practices

With agreement between teams and a handle on the appropriate processes and tools, you can begin decrypting traffic. Follow these best practices:

1. Determine Sensitive Traffic That Must Not Be Decrypted

Best practices dictate that you decrypt all traffic except that belonging to sensitive categories, such as Health, Finance, Government, Military, and Shopping.

2. Add Exclusions to Situationally Bypass Decryption

You will need to bypass decryption in certain circumstances, such as for applications that break upon decryption, specific users who need to bypass decryption for legal reasons, or partner websites that may be allowed to bypass strict certificate checks. 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 TLS decryption are valid by configuring the firewall to perform CRL/OCSP checks.

4. Configure Strong Cipher Suites and TLS Protocol Versions

Consult your security governance team to find out which cipher suites must be enforced, and determine the minimum acceptable TLS/SSL protocol version. For example, your security team may want to use the DHE or ECDHE key exchange algorithms to enable perfect forward secrecy (PFS) along with TLS 1.2 protocol. Alternatively, the team may want to block use of vulnerable TLS/SSL versions, such as TLS 1.0, TLS 1.1, 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 TLS certificate warning messages.

To learn more, check out the following resources:

- ✓ Next Generation Firewall webpage
- ✓ Decryption on LIVEcommunity
- ✓ Next-Generation Firewall products
- ✓ Decryption Best Practices
- ✓ PAN-OS webpage
- ✓ Security Subscriptions: Learn how Palo Alto Networks subscriptions can convey additional benefits.
  - **URL Filtering**: Selectively decrypt based on URL to balance performance, security, and privacy requirements.
  - **IoT Security**: Specify which IoT devices to decrypt and write decryption policies with Device-ID™
  - **WildFire® malware prevention service**: Detect potential malware and unknown threats
  - **Threat Prevention**: Apply threat prevention controls including IPS, anti-malware, file-type controls, and DLP to decrypted traffic
- ✓ Best Practice Assessment: This complimentary assessment helps you to maximize the capabilities of your NGFW, such as TLS decryption, to prevent successful cyberattacks.

paloalto NETWORKS

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