SOLUTION BRIEF

Maximizing Security and Performance with Versa Networks SSL/TLS Proxy Solution

Introduction

TLS and SSL are protocols that provide secure communication over the internet. They are commonly used to encrypt sensitive data such as usernames, passwords, and credit card information, ensuring that they cannot be intercepted by malicious actors.

SSL was the first protocol developed to provide secure communication over the internet. It was widely adopted in the early days of the INTERNET and is still used today, although it has been superseded by the newer TLS protocol. TLS is the successor to SSL and provides enhanced security features, improved performance, and better compatibility with modern web standards.

Both TLS and SSL work by establishing an encrypted connection between a client and server. The encryption process ensures that any data transmitted between the two parties is protected from interception and manipulation. TLS and SSL also use digital certificates to verify the identity of the parties involved in the communication, providing an additional layer of security.

TLS and SSL are used in a variety of applications, including e-commerce, online banking, and secure email. They are also an essential component of many security protocols, such as HTTPS, which is used to secure web traffic. In fact, this set of protocols is used with more than 85% of INTERNET traffic today. With such a large adoption it is important to understand why SSL and TLS are required to secure Internet traffic but also why one needs to understand it.

This document will cover the following topics:

- The risks associated with SSL and TLS encryption.
- What is SSL/TLS proxy and how can you take advantage of it to enhance your security.
- Versa Networks Secure Access Architecture
- Legislation and End Users Rights Considerations

The risks associated with encryption

Although SSL/TLS secures network communications, the encryption that comes with it can create challenges for enterprises that need to inspect traffic to protect against cyber threats. Amongst those threats are:

1. **Access to non-corporate web sites and download of unauthorized content** from employees (games, streaming …). Although such activities usually do not harm the company assets, they reduce productivity and use enormous resources such as bandwidth and CPU.
2. **Ransomware attacks:** Cybercriminals can use SSL/TLS encryption to protect their ransomware communications, making it more difficult for security researchers and law enforcement to track and disrupt their operations.
3. **Crypto jacking:** Cybercriminals can also use encryption to protect their mining operations, allowing them to hijack victims' servers and use their processing power to mine cryptocurrencies.
4. **Data Loss Prevention:** Enterprise data is a significant asset – therefore protecting the Confidentiality, Integrity and Availability of Enterprise Data is very important to the success of any organization. If the data is transferred within encrypted sessions, it will be difficult to enforce Data Compliance and Data Governance policies and meet legal/regulatory requirements.

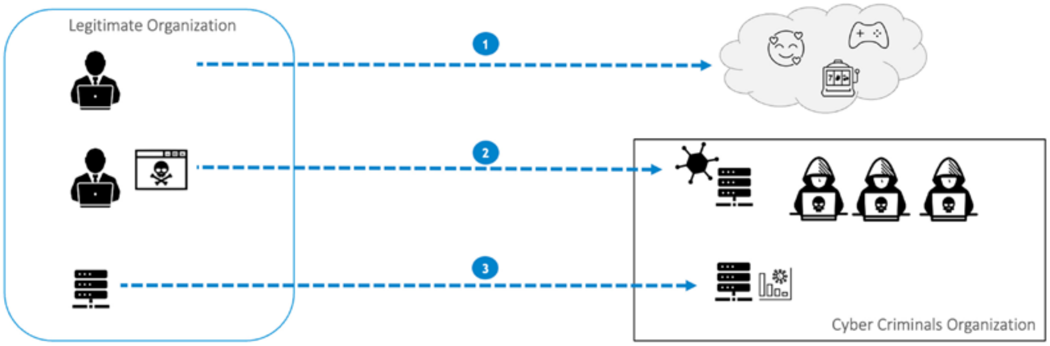


figure 1: Risks associated with Encryption

Additionally, expired, or untrusted certificates can pose several risks for users on the INTERNET. Those certificates are used by TLS/SSL to validate the identity of the website or web application to which it is issued. If the certificate is expired or untrusted, it may indicate that the website is not safe to use. Many users do not pay attention to the warning message caused by those certificates which often cause a threat for the organization.

It is also imperative that strong cryptographic keys and ciphers should be enforced to ensure strong security and confidentiality of the data being transferred. Weak cryptographic keys and/or ciphers lead to cryptanalysis attacks and potential data breaches that cause immense harm to the organizations.

What is SSL/TLS proxy

SSL proxy is a security technology that decrypts SSL/TLS traffic to enable inspection of network traffic for security threats. SSL proxy intercepts SSL/TLS traffic, decrypts it, and inspects the content for potential threats before forwarding it to the intended recipient. This allows enterprises to identify and block malicious traffic that may be hidden within encrypted communications. The SSL/TLS proxy can be deployed as an on-premises or cloud-based solution, and it can be implemented as a standalone product or as part of a comprehensive security solution. Enterprises can benefit from SSL/TLS proxy by improving network security using Inspections Services such as IPS (Intrusion Prevention Solution), CASB (Cloud Access Security Broker), DLP (Data Leak Prevention), IPS, Anti-Malware, and Net-Gen-Firewall. This helps reduce the risk of data breaches and enhance visibility and access control for network traffic, and also helps in meeting with compliance/regulatory requirements.

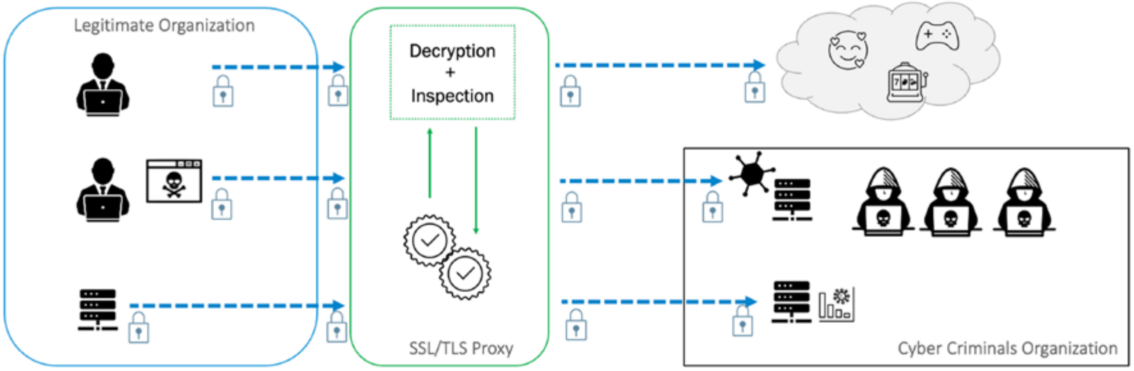


figure 2: SSL/TLS Proxy

Versa Networks Solution

The Versa SSL/TLS Proxy is a comprehensive solution that provides decryption and inspection capabilities. It enables the organization to gain visibility, enforce access control, detect and block data exfiltration, malware, viruses, and other cyber threats.

Currently, the Versa SSL/Proxy functions is available on:

- Versa Secure SD-WAN Appliances.
- Versa Secure Web Gateways (SWG) which is part of Versa Secure Internet Access.

This flexibility allows us to provide SSL/TLS Proxy for SD-WAN customers who need security at the branch but also for VSIA (Versa Secure Internet Access) customers requiring the same capabilities for their remote workers.

Both provides several key features and benefits:

- **Security:** Inspection of SSL/TLS traffic to provide comprehensive threat protection, including data loss prevention, advanced malware protection, and intrusion prevention.
- **Visibility**: The Versa operating system provides granular visibility into SSL/TLS traffic, which helps identify unauthorized applications, websites, and users.
- **Data Governance:** The decrypted traffic is inspected for any Data Exfiltration attempts, while also enforcing access control for confidential and sensitive data. The Data Loss Prevention (DLP) feature inspects all aspects of the decrypted traffic, including the headers, payload, normalized content and reconstructed files. Based the results of data scanning, DLP helps organizations gain visibility into the data flows, enforce access control and digital rights, and comply with Confidential/Privacy requirements.

- **Inspection:** The Versa solution can perform comprehensive inspection and analysis of the SSL/TLS connection and detect illegitimate & expired certificates as well as weak encryption & authentication algorithm. In addition, it can use an external Certificate Revocation List (CRL) or the Online Certificate Status Protocol (OCSP) protocol to verify if a server certificate was revoked. In some situations, this can help mitigate malicious activities even if you do not decrypt the traffic.

Additionally, the Versa SWG provides the following advantages:

- **Scalability:** The Versa SWG can scale up or down based on the organization's needs, ensuring that SSL proxy services are available when required.
- **Performance:** The Versa SWG uses hardware acceleration and cloud-native architectures to deliver high-performance SSL proxy services.

Versa Networks Solution Architecture

The Versa SSL/TLS Proxy solution (figure 3) is designed to deliver high-performance SSL/TLS decryption and inspection capabilities. The architecture includes the following components on both Versa Secure SD-WAN and Versa SWG:

- **SSL/TLS Proxy:** The SSL proxy intercepts SSL/TLS traffic and decrypts it for inspection. It can also inspect the certificate of the (Web) server and make sure it is legitimate and trusted.
- **Trust engine:** Using a ZTNA (Zero Trust Network Access) approach, the trust engine plays a crucial role in ensuring that only authorized users and devices can access the network resources, while blocking all other attempts.
- **Security Engine:** The security engine inspects decrypted traffic for potential threats, including data exfiltration, malware, viruses, and phishing attacks. In addition, it controls security policies to provide access to websites, applications, and services.
- **Reporting and Analytics:** The reporting and analytics module provides granular visibility into SSL/TLS traffic, including application usage, user behavior, and threat intelligence.

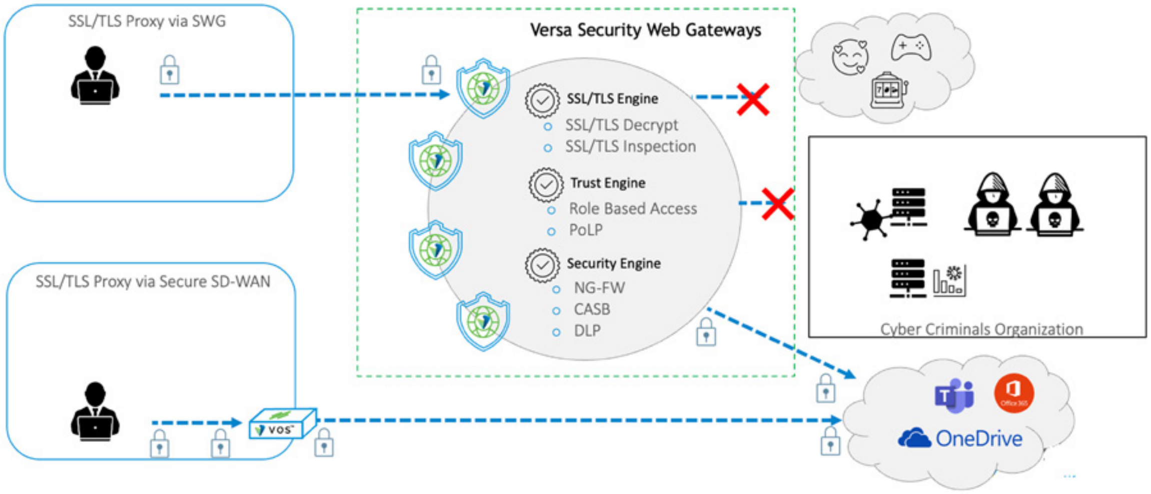


figure 3: Versa SSL/TLS Proxy Solution

Versa Networks Proxy Modes

There are predominantly two modes of deployment – Forward/Full Proxy and Reverse Proxy. Within each of these modes, there are additional modes of operation depending on the use case. This section describes the various modes of proxy operations. It is important to note that Versa Proxy solution supports all the modes of proxy operations that are described in this document. Versa supports TLS v1.2 and TLS v1.3 in all the proxy modes.

Forward/Full Proxy

The Forward/Full Proxy mode is also known as Man-In-The-Middle (MITM) Proxy, or Break-Inspect Proxy. Typically, Forward/Full Proxy is deployed closer to the client or browser, because the primary objective of the Forward/Full Proxy is to enforce security policies for the browsers (end-users), providing full visibility into end-user traffic, and protecting the endpoint browsers/devices from threats like malware, fishing, spyware, etc., In the Forward/Full Proxy modes, the proxy presents a spoofed certificate to the browser, in lieu of the certificate that the target website is using. The spoofed certificate allows the proxy to break the browser's communication with a target website into two logical sessions: The proxy will become the server for the browser, while at the same time the proxy can be the client to the target web/application server that the browser is trying to visit.

If the endpoint device is not configured with the Proxy's certificate, then the browser will display a warning to the end user that the certificate for the website cannot be trusted because it's the spoofed certificate by the Proxy. Often, configuration of the Proxy certificate on the endpoint devices is the biggest hurdle to deploying a Full/Forward Proxy. On all modern Operating Systems, the Trusted Certificate store is managed by Operating System instead of the browsers. The rollout of the Proxy certificate is typically orchestrated by Active Directory or Mobile Device Management (MDM) solution.

In some scenarios, the Forward/Full Proxy is ineffective, even if the Proxy certificate is deployed on the endpoint devices. While browsers tend to use the Operating Systems' Trusted Certificate store, certain Enterprise Browsers and Mobile/Desktop Applications use certificate pinning to prevent Forward/Full Proxy from decrypting the traffic. Additionally, certain protocols like TLS v1.3 and QUIC allow the TLS handshake itself to be encrypted, in which case the Forward/Full Proxy will be unable to present a spoofed certificate.

When the browser/client trusts the Proxy certificate, the Forward/Full proxy can be deployed in multiple different modes, depending on the use case.

Transparent Forward Proxy

In the Transparent Forward Proxy Mode, the Proxy will decrypt the incoming traffic, inspect the traffic, and if allowed, forwards the re-encrypted traffic to the destination. The browser or the Operating System does not need to be configured with explicit Proxy IP Address, which is why it is referred to as a Transparent Proxy. The Transparent Forward Proxy is able to transparently decrypt any browser traffic that is traversing through it.

While in the Forward Proxy mode, the semantics of the underlying TCP/IP session packets are mostly in-tact. The transparent forward proxy is not allocated with any IP Addresses. When the traffic reaches the destination website via the transparent forward Proxy, the source IP Address is the same as the original IP Address of the client/browser, with appropriate NAT policies applied to the browsers' IP Addresses. In the transparent forward Proxy mode, the packet buffers received on the network by the Proxy are re-used to construct the final re-encrypted payload, with the TCP/IP headers adjusted as applicable. Therefore, the transparent forward Proxy mode is the most efficient, in terms of memory utilization and performance. The trade-off is that since the transparent forward proxy is operating within the constraints of packets buffers received, the Proxy is not in full control of the communications towards the browser and the target website.

Transparent Full Proxy

In the transparent full proxy Mode, the Proxy splits the browsers' connections with the target website into two parts: the Proxy becomes the server to the browser and at the same time, the Proxy is a client to target website that is being accessed. The Proxy has full control over both sessions of the communication – therefore it has the maximum flexibility of determining the content that is sent/received towards each direction. However, because of maintaining two independent connections towards the browser and the target website, there is more overhead in terms of memory utilization and performance.

The browser or the Operating System does not need to be configured with explicit Proxy IP Address, which is why it is referred to as a Transparent Proxy. The Transparent Forward Proxy can transparently decrypt any browser traffic that is traversing through it.

In the Transparent Full Proxy mode, the Proxy is assigned explicit pool of IP Addresses for the outbound connections. When the traffic reaches the destination website via the transparent full Proxy, the source IP Address is the Proxy's IP Address, with appropriate NAT policies applied to the Proxy's IP Addresses. Hence the transparent full proxy mode is sometimes referred to as an Anonymizing Proxy. If the target website needs to have access to the browsers' original IP Address, the Proxy can be configured to send the X-Forwarded-For (XFF) Header with the browser's IP Address.

Explicit Full Proxy

In the explicit full proxy mode, the Proxy splits the browsers' connections with the target website into two parts: the Proxy becomes the server to the browser and at the same time, the Proxy is a client to target website that is being accessed. The Proxy has full control over both sessions of the communication – therefore it has the maximum flexibility of determining the content that is sent/ received towards each direction. However, because of maintaining two independent connections towards the browser and the target website, there is more overhead in terms of memory utilization and performance.

In the Explicit Full Proxy mode, the browser or the Operating System needs to be configured with explicit Proxy IP Address and port number, which is why it is referred to as an Explicit Proxy. The Explicit Full Proxy will not decrypt any browser traffic that is traversing through it. The Explicit Full Proxy can be configured with the decryption policies to decrypt or to not decrypt, based on the URL Category of the destination website. Typically, websites within the financial and health-care categories, and similar websites that are related to Personally Identifiable Information (PII), are not decrypted to comply with privacy policies. Instead, the browser will make an explicit request to the Explicit Proxy to reach any destination website. The Explicit Full Proxy makes a connection to the target website and proxies the data between the browser and website after the applicable security inspection and policy enforcement.

In the Explicit Full Proxy mode, the Proxy is assigned explicit pool of IP Addresses for the outbound connections. When the traffic reaches the destination website via the Full Proxy, the source IP Address is the Proxy's IP Address, with appropriate NAT policies applied to the Proxy's IP Addresses. Hence the Full Proxy mode is sometimes referred to as an Anonymizing Proxy. If the target website needs to have access to the browsers' original IP Address, the Proxy can be configured to send the X-Forwarded-For (XFF) Header with the browser's IP Address.

Reverse Proxy

The Reverse Proxy mode is typically deployed when the certificate of the target website/application is available to be configured on the Reverse Proxy. When the browser traffic is going through the Reverse Proxy, the Proxy presents the target website's certificate to the browser, while at the same time it establishes another connection to the target website. At this point, the Reverse Proxy can decrypt the traffic, perform security inspection and policy enforcement for the decrypted traffic, and forward the traffic along to the destination. The difference between Forward/Full Proxy and the Reverse Proxy, is that the Reverse Proxy presents the target website's original certificate to the browser, instead of a spoofed certificate, e.g., in the case of Forward/Full Proxy.

The Reverse Proxy can be deployed closer to the web server/application to protect the web server itself, or it can be deployed closer to the endpoint device for device/user protection.

Traditional Reverse Proxy

The Reverse Proxy splits the browser connection into two arms – it is a server to the browser, while at the same time, it is a client to the target web server/application. The content is written back and forth without any modifications to the payload, unless explicitly configured.

Application Reverse Proxy

The Application Reverse Proxy is deployed closer to the devices/users, typically to provide security to the endpoint browsers/ devices/users. The Application Reverse Proxy is configured with the web server/application's Server Certificate.

The Application Reverse Proxy rewrites the content – so that all communications to the target web server/application will go through the Application Reverse Proxy for security inspection. For example, if the response contains any links/URLs to the target website/application, they are rewritten in such a way, that all subsequent access to the links contained within the response will also reach the Application Reverse Proxy for security inspection.

Proxy Chaining

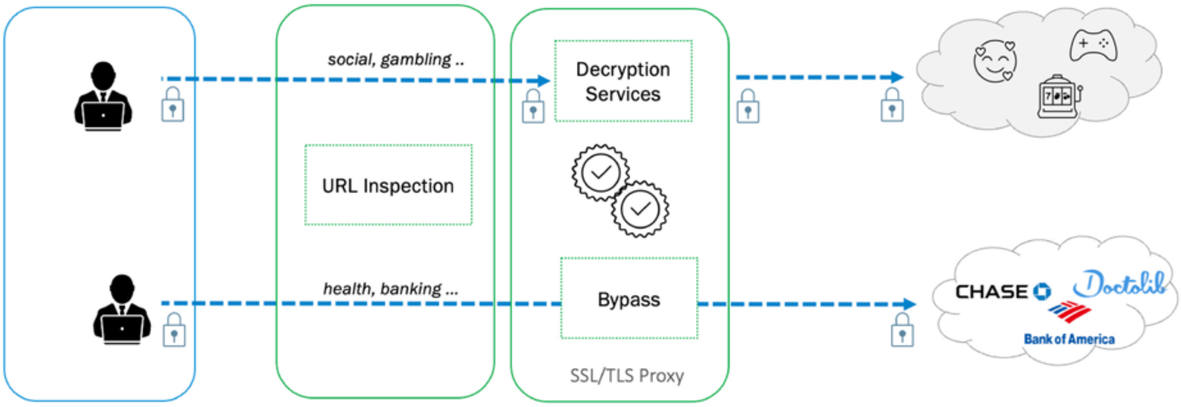
The Versa TLS Proxy solution supports proxy-chaining, where after applying the Versa Proxy processing, the traffic can be sent to another upstream Proxy instead of the destination website/application.

Legislation, End-Users Rights & Limitations

While SSL/TLS proxy is the perfect tool for modern enterprise, end user privacy must be kept in mind. The legislation regarding SSL/TLS decryption varies by country and region. In general, governments and regulatory entities have the authority to regulate and monitor internet traffic within their area to protect national security, prevent cybercrime, and enforce laws and regulations.

Similarly, enterprises might decide to enforce decrypt or no-decrypt action depending on whether the destination website pertains to processing Personally Identifiable Information (PII) or users' private data. Typically, financial and healthcare websites are not decrypted in enterprises. The Versa Secure Web Gateway offers Decryption Policies to match on the category of the destination websites and based on that enforce decrypt/no-decrypt actions.

Additionally, some applications offer services based on a website and mobile/desktop application, at the same time. Some mobile/desktop applications implement a feature called Certificate Pinning to prevent proxies from decrypting traffic exchanged by the application. The Certificate Pinning feature associates a specific Root-of-Trust certificate with the mobile/desktop application. The mobile/desktop applications will only accept certificate that is issued by the specific Root-of-Trust, and will reject any other certificates, including the certificates issued by the proxy, thereby preventing decryption of the traffic by a proxy. In such cases, such application traffic can be exempted/bypassed from decryption, by configuring the appropriate Decryption Policies on the Versa Secure Web Gateway.



In the European Union, the General Data Protection Regulation (GDPR) regulates the processing of personal data and imposes strict requirements on the interception and processing of encrypted traffic. The GDPR requires that any interception of encrypted traffic must be transparent, lawful, and proportionate to the legitimate purposes pursued by the interceptor.

In summary, the legislation regarding SSL decryption varies by authority and is subject to a range of legal frameworks, including privacy laws, national security laws, and data protection regulations. It is important for individuals and organizations to understand the legal requirements in their area and obtain appropriate legal advice before engaging in SSL/TLS decryption practices.

Conclusion

Versa Networks Solution provides a comprehensive and scalable SSL/TLS proxy solution that helps organizations protect against cyber threats and improve visibility. With its powerful features, Versa Secure SD-WAN or Versa Security Web Gateway which is part of versa Secure Private Internet access can be an effective solution for organizations looking to deploy SSL/TLS proxy services.

For more information on Versa Networks, please visit https://versa-networks.com, contact us at https://versa-networks/contact or follow Versa Networks on X (Twitter) @versanetworks

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com