NIST SPECIAL PUBLICATION 1800-37A

# Addressing Visibility Challenges with TLS 1.3 within the Enterprise

**Volume A:**
**Executive Summary**

**Murugiah Souppaya**
**Tim Polk***
Computer Security Division
Information Technology Laboratory

**William Barker**
Dakota Consulting
Silver Spring, Maryland

**John Kent**
The MITRE Corporation
McLean, Virginia

**Former NIST employee; all work for this publication was done while at NIST.*

January 2024

SECOND PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/addressing-visibility-challenges-tls-13

# Executive Summary

The Transport Layer Security (TLS) protocol is an essential building block for enterprise security. TLS is widely deployed to secure network traffic. The latest version, TLS 1.3, has been strengthened so that even if a TLS-enabled server is compromised, the contents of its previous TLS communications are still protected—better known as *forward secrecy*. As a result of the TLS 1.3 ephemeral key exchange approach used to achieve forward secrecy, the changes interfere with passive decryption techniques that are widely used by enterprises to achieve visibility into their own TLS 1.2 traffic. Many enterprises depend on that visibility to permit their authorized network security staff to implement controls needed to conform to cybersecurity, operational, and regulatory requirements (e.g., intrusion detection, malware detection, troubleshooting, and fraud monitoring). This forces enterprises who have a governance requirement driving these controls to choose between using the old TLS 1.2 protocol or adopting TLS 1.3 with some alternative method for internal traffic visibility.

In practice, as NIST described in Special Publication (SP) 800-207, there may be circumstances where network traffic cannot be deeply inspected. When network inspection devices are used on networks that service a diverse and dynamic set of users, devices, and network destinations, such as those used by the organization's staff for day-to-day work, appropriate compensating measures should be employed—for example, ensuring that the inspection device management interfaces are connected not to the network being monitored, but rather to a dedicated control plane network. Adding more key management processes can increase the attack surface available to adversaries. In cases where organizations segment their networks, move away from intranets, and permit access to enterprise services from any network, inspecting traffic in these environments may become less practical and less valuable over time unless provisions are made for policy controls that determine which traffic is inspected.

In other places, deep traffic inspection may be more valuable and can create less of an increase in attack surface. For example, deep traffic inspection could be more appropriate in application environments that guard sensitive data and have a small number of expected network clients and destinations that can be predicted in advance. In general, when decryption and inspection are performed, organizations should employ technologies such that user privileges and the set of traffic that is inspected are constrained by policy controls to only that which is necessary.

Network traffic that is not decrypted can and should still be analyzed using visible or logged metadata, machine learning techniques, and other heuristics for detecting anomalous activity. For instance, this is consistent with the Trusted Internet Connections (TIC) initiative, as updated in Office of Management and Budget (OMB) Memorandum M-19-26, which gives government agencies the flexibility to maintain appropriate visibility without needing to perform inline traffic decryption.

TLS 1.3 offers significant improvements over TLS 1.2. Vulnerable optional parts of the protocol (e.g., use of vulnerable RSA options) have been removed, it supports ciphers that are required to implement perfect forward secrecy (PFS), and the handshake process has been significantly shortened. Using TLS 1.2 is not recommended because it doesn't have the security and performance enhancements of TLS 1.3. Also, because the Internet Engineering Task Force (IETF) is deprecating TLS 1.2's protocol implementation, it will become obsolete over time.

This guide summarizes how the National Cybersecurity Center of Excellence (NCCoE) and its collaborators are using commercially available technology to build key management-based solutions for organizations that require TLS 1.3 visibility. As the project progresses, this preliminary draft will be updated, and additional volumes will be released for comment. The goal of the completed guide is to help readers determine whether the solutions are practical for use in their enterprise environments.

# 1 CHALLENGE

Enterprises that are required to perform security monitoring and analysis in their networks typically employ tools and architectural solutions to provide necessary visibility into their internal traffic. Most of these visibility solutions take advantage of a characteristic in TLS 1.2 that enables them to masquerade as the TLS server and decrypt past, present, and future TLS 1.2 traffic. The TLS 1.3 protocol prevents use of the TLS 1.2 visibility solutions on which these enterprises have relied to enable their network management and security staffs to perform monitoring and analytics necessary to detect, identify the nature of, respond to, and recover from intrusions and other anomalies.

The project demonstrates methods for providing the necessary visibility without recommending any change to the TLS 1.3 protocol (https://datatracker.ietf.org/doc/rfc8446). To find new solutions for visibility into TLS 1.3 traffic, the NCCoE identified a broad set of options. These include:

- endpoint mechanisms that establish visibility, such as enhanced logging;
- key-management mechanisms that defer forward secrecy until all copies of keying material needed to maintain current levels of network visibility are deleted;
- network architectures that inherently provide visibility, such as use of overlays, or through incorporation of middleboxes (https://doi.org/10.17487/rfc3234); and
- innovative tools that analyze network traffic without decryption.

In order to minimize the impact on network architectures and facilitate adoption of TLS 1.3, this project has focused on the second and third options: key-management and middlebox (break and inspect) mechanisms. Several challenges are associated with these mechanisms. Some of these challenges are shared by TLS 1.2 visibility solutions, while others are unique to TLS 1.3. Challenges include:

- **Secure management of servers' cryptographic keys**. Private and secret keys must be protected throughout the cryptographic lifecycle: creation, distribution, use, retention, and destruction. Unauthorized disclosure places all past, present, and future traffic encrypted under those keys at risk.
- **Management of recorded traffic**. This demonstration project assumes that recorded traffic is stored in encrypted form, not plaintext. To be useful, the enterprise must be able to identify the corresponding key material. However, recorded traffic remains at risk of compromise until the corresponding key material is destroyed. Any solution must allow the enterprise to recover plaintext traffic when required, while ensuring that traffic is not at risk of compromise indefinitely.
- **Managing expectations of privacy**. The security enhancements associated with TLS 1.3 may increase privacy expectations. Enterprises that rely on visibility for critical management and security controls should ensure that TLS 1.3 connections within that scope are accepted only by

informed users (for example, user awareness of monitoring for auditing and security forensics purposes).

In addition to the TLS-specific challenges, the NCCoE is considering the practical challenges of scalability, ease of deployment, and usability of the visibility solutions demonstrated.

**This preliminary practice guide can help your organization:**

- understand what types of key management-based solutions enterprises can use to achieve TLS 1.3 visibility
- determine whether key management-based solutions for TLS 1.3 visibility are practical for your environment
- understand the capabilities and limitations of middlebox solutions that decrypt traffic for inspection and forward re-encrypted traffic to enterprise servers

# 2 SOLUTION

The NCCoE is collaborating with technology providers to demonstrate an architecture for TLS 1.3 visibility. The demonstration architecture includes two server-based key-management solutions and a third that combines network architecture (e.g., middlebox) and key-management techniques. The solutions are intended only for enterprise data center environments and are server-based rather than client-based.

The solutions are expected to provide controlled enterprise visibility into encrypted TLS 1.3 traffic. This supports four specific scenarios identified by the NCCoE: operational troubleshooting, performance monitoring, threat triage, and cybersecurity forensics. Data requirements for performance monitoring and threat triage are largely real-time, while operational troubleshooting and cybersecurity forensics require access to historical data stored in encrypted form.

To achieve visibility through key management, the enterprise may apply one of two technical mechanisms for each enterprise server whose traffic is of interest. In the first option, a key distribution function would provision bounded lifetime Diffie-Hellman key pairs to TLS 1.3 servers within the enterprise for use in ephemeral key exchanges. In the second case, TLS 1.3 servers within the enterprise would provide copies of their symmetric traffic keys to a key distribution function. In both cases, compensating security management controls are necessary to limit access to the keys and data to authorized individuals in accordance with enterprise access policies.

The Diffie-Hellman keys and symmetric traffic keys are retained by the key distribution function until all corresponding encrypted traffic has been decrypted or is no longer available. Systems that are authorized to examine traffic would obtain the appropriate keys from the key distribution function. The solution would also incorporate components to retain traffic for retrospective applications, like troubleshooting and cybersecurity forensics. The stored traffic is retained in encrypted form until policy conditions (e.g., retention time or maximum storage) are met. Once retention is no longer required by the systems authorized to examine the traffic, the data is deleted.

Since TLS 1.3 is designed to achieve forward secrecy, the solution also assumes out-of-band notification of the visibility policy. This restricts the solution for use within a single enterprise.

Some aspect of analytics functions needing enterprise visibility into encrypted traffic may require combining network architecture and key-management techniques to achieve operationally necessary visibility. Necessary analytics functions may include identification of causes of network performance degradation or failures; key management-based communications failures; detection and identification of anomalous received data; identification of sources of anomalous data; and detection of traffic from unauthorized sources.

Therefore, the project's scope includes demonstration of an architecture that achieves visibility inside the data center through middlebox tools that break and inspect traffic. Middleboxes are used at the enterprise edge to achieve real-time visibility. In this demonstration project, we examine deployment within the enterprise and address access to historical data by leveraging key-management based solutions.

| Collaborators | |
|---|---|
| AppViewX | NETSCOUT |
| DigiCert | Not for Radio, LLC |
| F5 | Nubeva |
| JPMorgan Chase | Thales Trusted Cyber Technologies |
| Mira Security, Inc. | US Bank |

While the NCCoE is using a suite of commercial products to address this challenge, this guide does not endorse particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

# 3 HOW TO USE THIS GUIDE

This practice guide is being developed in five parts. Depending on your role in your organization, you might use this guide in different ways:

**Business decision makers**, such as chief information security, product security, and technology officers, can use this part of the guide, NIST SP 1800-37A: *Executive Summary*, to understand the project's challenges and outcomes, as well as our solution approach.

**Technology, security, and privacy program managers** who are concerned with how to identify, understand, assess, and mitigate risk can use NIST SP 1800-37B: *Approach, Architecture, and Security Characteristics*. It describes the architecture and different implementations. Also, the future NIST SP 1800-37E: *Risk and Compliance Management*, will map components of the TLS 1.3 visibility architecture to security characteristics in broadly applicable, well-known cybersecurity guidelines and practices.

**IT professionals** who want to implement an approach like this can make use of NIST SP 1800-37C: *How To Guide* currently under development. It will provide product installation, configuration, and integration instructions for building example implementations, allowing them to be replicated in whole or in part. They will also be able to use a future NIST SP 1800-37D: *Functional Demonstrations*, which will provide the use cases that have been defined to showcase TLS 1.3 visibility capabilities and the results of demonstrating these capabilities with each of the example implementations.

# 4 SHARE YOUR FEEDBACK

You can view or download the preliminary draft guide at the NCCoE TLS 1.3 Visibility project page. NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on designing and implementing the example solution and developing other parts of the content. As a preliminary draft, this volume will have at least one additional draft released for public comment before it is finalized.

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. Once the example implementation is developed, you can adopt this solution for your own organization. If you do, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and recommended practices for transforming the processes associated with implementing this guide.

To provide comments or join the TLS 1.3 Visibility community of interest, contact the NCCoE at applied-crypto-visibility@nist.gov.

---

# 5 COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.