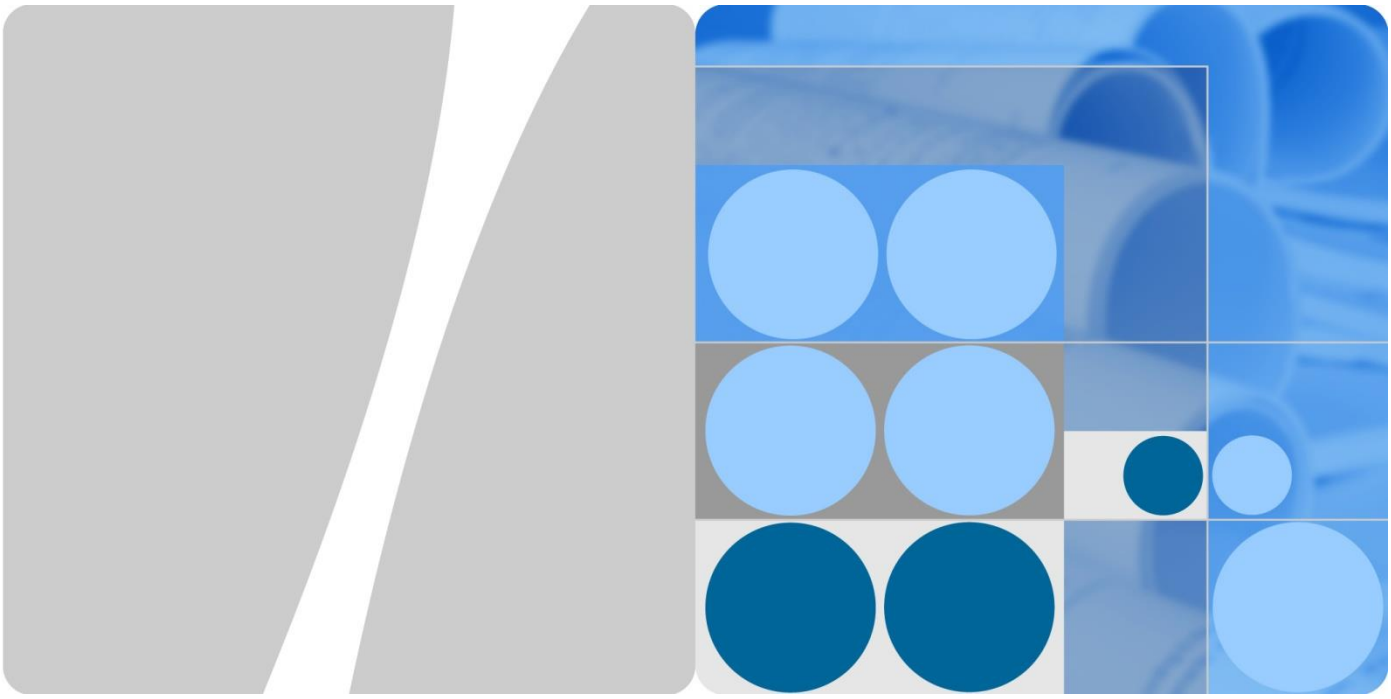


HUAWEI USG Series T-level Next-generation Firewall

Encrypted Traffic Detection Technical White Paper

Issue 1.0

Date 2017-2-31

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

Email: ask_FW_MKT@huawei.com

Call: 4008302118

Contents

HUAWEI USG Series T-level Next-generation Firewall

Encrypted Traffic Detection Technical White Paper

Keyword:

NGFW, SSL TLS

Abstract:

This document describes the principle and solution of the encrypted traffic detection technology for Huawei NGFW.

Abbreviation	Full Spelling
NGFW	Next-Generation Firewall
SSL	Secure Sockets Layer

1 Background

The Secure Sockets Layer (SSL) protocol is an important technology that is widely used to guarantee interaction security on the Internet. In normal cases, HTTP traffic is transmitted over the Internet in plaintext, which may be intercepted. To eliminate this risk, SSL can be used to encrypt HTTP traffic (namely, HTTPS) to guarantee information security during data transmission.

However, encrypted traffic also brings huge challenges to the security detection function of the FW. The FW at the intermediate location cannot analyze completely encrypted application data for whether threats, viruses, and attacks exist in the data and whether the data is transmitted in an authorized way. According to Gartner's data in 2013, 25% of Internet traffic is encrypted, and 50% of attacks are implemented through encrypted traffic.

Common FWs cannot decrypt encrypted data and therefore cannot detect data content or defend against attacks initiated through encrypted traffic. FWs of certain vendors may perform coarse-grained detection (such as domain name filtering) based on key information, such as certificate information, during the SSL handshake process. This technology, however, blocks all traffic of a certain website but cannot identify attack traffic hidden in trusted traffic, causing a high rate of false positives and negatives. The administrator faces a dilemma in deciding on the configuration.

The encrypted traffic detection technology of Huawei helps users cope with this issue. The encrypted traffic detection technology decrypts encrypted traffic and performs in-depth detection on the plaintext to prevent malicious attacks from entering the enterprise network or prevent enterprise confidential information from being disclosed. The category-specific refined and encrypted traffic detection configurations help the management plane perform traffic security configurations in a refined way based on network traffic features, ensuring security and user experience (performance). In addition, with the decryption and mirroring function, encrypted traffic can be handed over to the third-party device for audit and security detection so that encrypted traffic can be completely visualized.

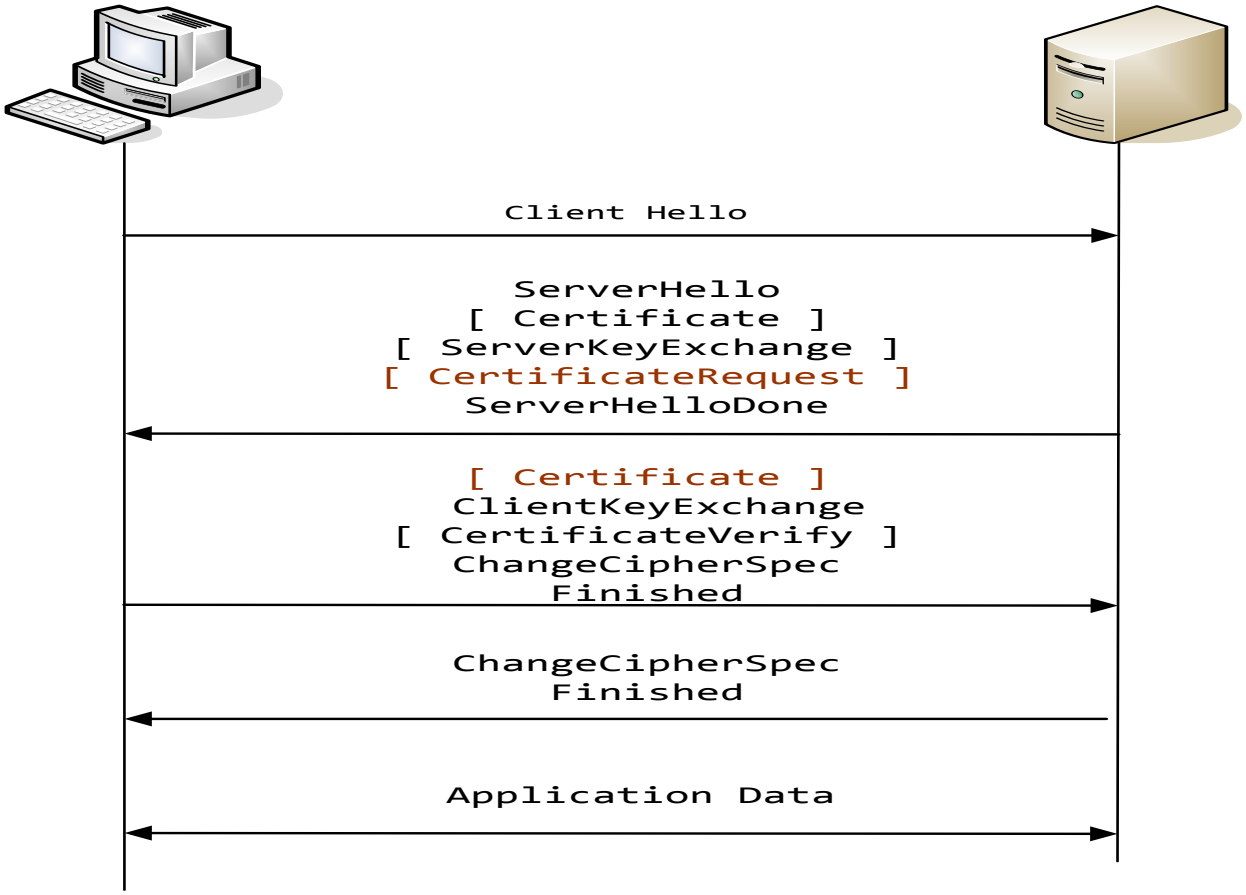
2 Concepts and Principles

2.1 SSL Concepts

Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are security protocols that guarantee the security and data integrity of Internet communications. During the handshake phase, SSL/TLS employs an asymmetric encryption mechanism to negotiate the algorithm set used for subsequent data transmission, ensuring that the data is trusted, reliable, and integrated.

The SSL client and SSL server use the digital certificate to authenticate each other during the handshake phase. The certificate, like the ID card to a person, is issued by a third-party trusted authority (certificate authority, namely, CA, in this case). With other public information released by the CA and standard verification method, all clients can verify whether the obtained peer certificates are trusted, so as to ensure that the entire connection interaction is trusted. Generally speaking, most traffic over the Internet involves the authentication of the server by the client. That is, the server needs to show its certificate to the client, whereas the client does not need to show its certificate to the server. For applications involving privacy, such as those in finance and healthcare sectors, it is possible that the server also requires the client show its certificate. This is called client authentication or bidirectional authentication.

Figure 2-1 Simplified SSL handshake process



1. The client sends a Client Hello message to a server that has the SSL service enabled. The message contains a list of algorithms and versions supported by the client.
2. The server selects an encryption algorithm and version (which are highly secure and deliver optimal performance) from the list sent by the client and sends the choice back to the client. Meanwhile, the server sends its own certificate, which usually contains the server name (Common name), certificate issuance authority, and corresponding public key, to the client. Certain servers may also require the client send its own certificate (for client authentication). On the live network, however, this step is usually not involved, except for specific bank applications.
3. After obtaining the server certificate, the client verifies whether the server is the one it attempts to access through the server name and locates the local CA certificate based on the issuance authority in the certificate to further verify whether the server certificate is indeed issued by this authority.
4. If the client verifies that the server certificate is legitimate and trusted, a master key is generated, encrypted with the public key in the server certificate, and then sent to the server. After the server receives this master key, it uses its own private key to decrypt the master key. This process is called asymmetric encryption. Only the server has the private key that can be used to decrypt the master key. This prevents the private key used for subsequent symmetric encryption from being obtained by a third party.
5. The client and server calculate parameters required in subsequent symmetric encryption based on the key. These parameters are keys for subsequent encryption between the client and server. After the server and client notify each other of the completion of the

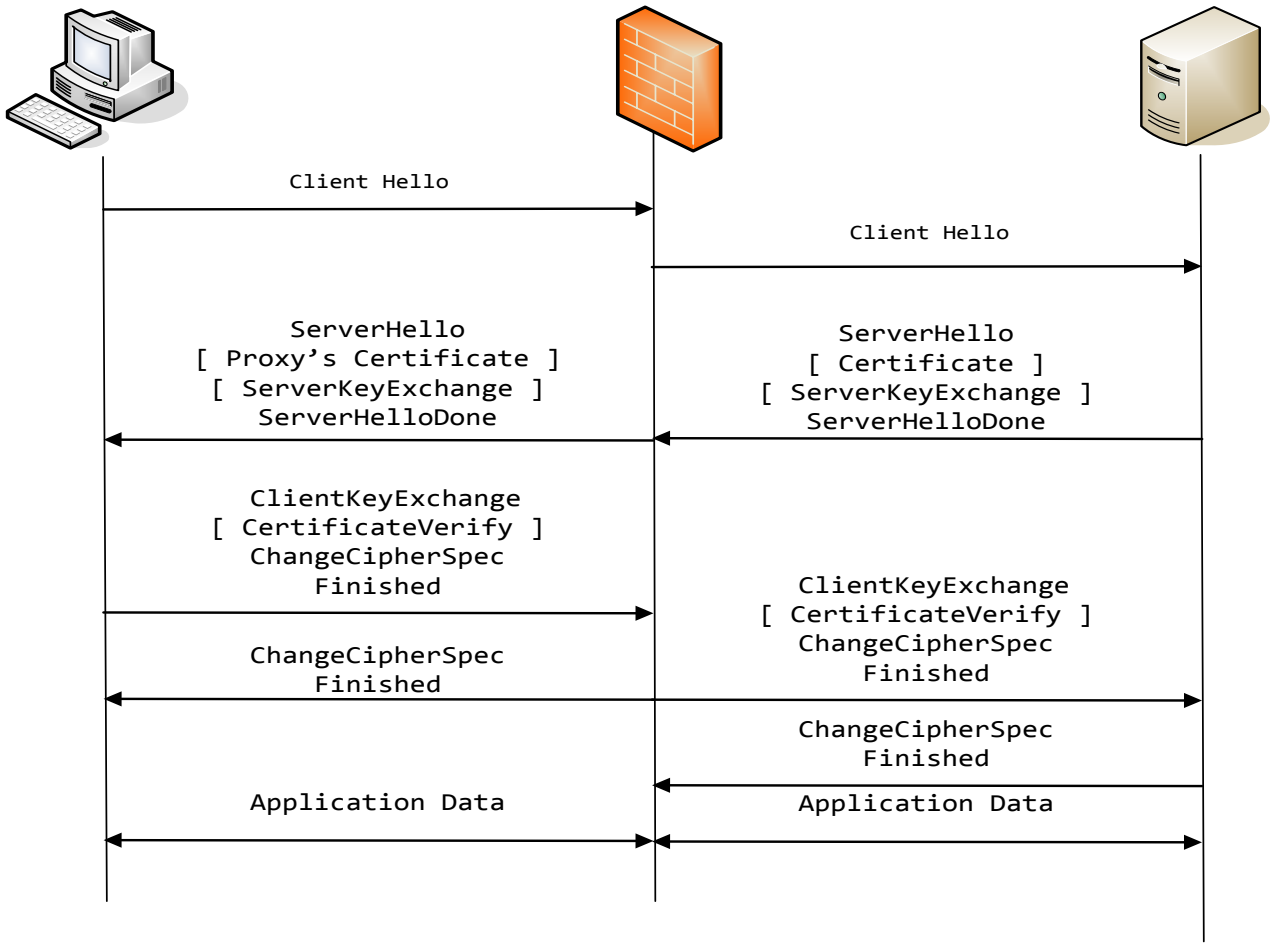
handshake phase, the negotiated keys are used for subsequent interaction of encrypted application data.

2.2 Principles of SSL Proxy

The SSL proxy uses the NGFW device as the man-in-the-middle. With the authorization of the administrator, the SSL proxy dynamically re-issues and replaces the certificate sent from the server to the client and impersonates the server to interact with the real client.

After receiving the client request, the man-in-the-middle proxies the client to establish a connection with the server and meanwhile acts as the server to establish a connection with the client. This actually turns SSL handshake into two completely independent processes. Therefore, the man-in-the-middle can obtain the complete content in the interaction with the client and server so as to process the content.

Figure 2-2 SSL proxy process



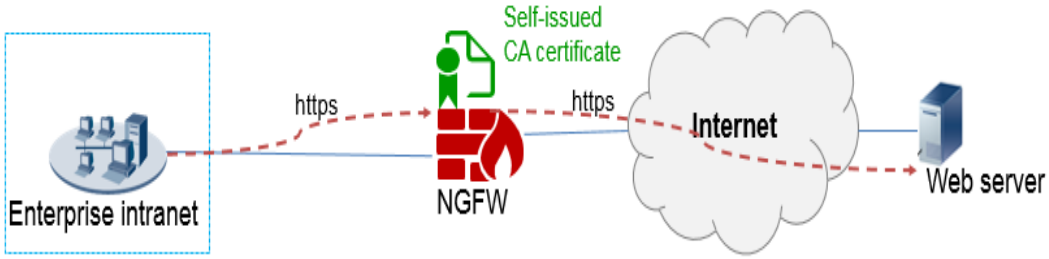
2.3 Principles of Encrypted Traffic Detection

The encrypted traffic detection feature decrypts encrypted traffic, performs security checks on the traffic, re-encrypts the traffic, and then forwards the traffic out in proxy mode. This mainly applies to two scenarios: scenario of detecting outbound encrypted traffic of the intranet client and scenario of detecting inbound encrypted traffic of the intranet server.

In the proxy process, two situations are possible as for the certificate sent from the proxy to the client based on the usage scenario: One is dynamic issuance using the CA certificate trusted by the client, and the other is the usage of the imported server certificate.

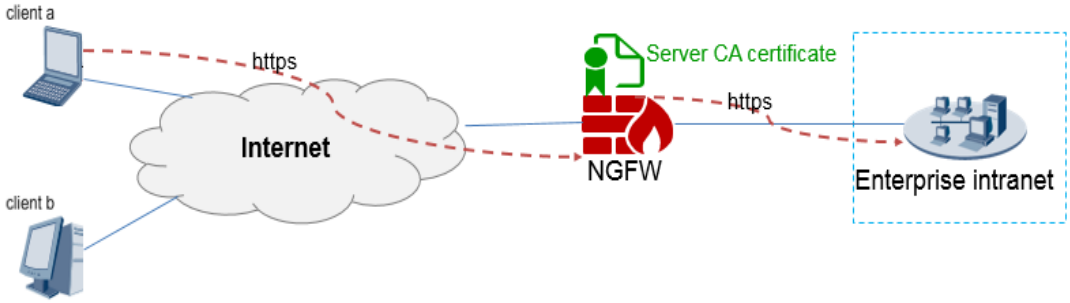
As for the scenario of outbound encrypted traffic detection, such as the scenario in which the enterprise intranet accesses a large number of external servers, the CA certificated trusted by the client (decryption certificate) shall be used for certificate re-issuance.

Figure 2-3 Outbound encrypted traffic detection



In inbound encrypted traffic detection scenarios, it is possible that the administrator directly imports the certificate and private key of the intranet server to the device.

Figure 2-4 Inbound encrypted traffic detection



2.3.2 Configuration of Category-Specific Detection

Category-specific detection applies to scenarios of outbound encrypted traffic detection. The URL category corresponding to the server is queried based on the plaintext information for the SSL handshake between the client and server. Based on the category information, how to process the traffic to this server (decrypt, directly block, or not decrypt) is determined.

SSL session negotiation and subsequent packet encryption and decryption are CPU-consuming. If the encrypted traffic detection function is enabled for all traffic, device resources are severely occupied. The configuration of the category-specific detection policy allows users to filter encrypted traffic initially from the granularity of domain name category

to exclude secure sites that can be trusted and sites that can be directly blocked. The helps reduce the resources consumed by the device for processing encrypted traffic.

2.3.3 Balance Between Performance and Security

This applies to scenarios of outbound encrypted traffic detection and inbound encrypted traffic detection.

After encrypted traffic detection is enabled, the SSL proxy establishes a connection with the client and another connection with the server. The administrator can configure the encryption algorithms and versions used by these two connections individually. SSL session negotiation and subsequent packet encryption and decryption are CPU-consuming. In addition, the CPU resources consumed increase with the security requirement. Therefore, the administrator can configure the encryption algorithms and versions individually for these two connections based on network features. For example, for a secure and trusted internal network, algorithms and versions of lower security are used; for a complicated external network exposed to lots of attacks, algorithms and versions of higher security are selected for a balance between performance and security.

2.3.4 Certificate Validity Check

This applies to scenarios of outbound encrypted traffic detection.

In most phishing attacks, a forged website that is extremely similar to the real website is sent to users to trick them into entering such key information as the user name and password. Technically, SSL sites can defend against such attacks, considering that the forged websites use certificates that are not trusted by the client browsers, such as Internet Explorer and Chrome, and the browsers display alarms on the untrusted certificates in the access to the forged websites. However, there are also some nonstandard websites with untrusted certificates on the live network, and phishing attackers forge the untrusted certificates of the encrypted websites to be almost the same as those of the real websites. Users may carelessly ignore alarms on the clients and choose to continue their access, falling into the traps of the attackers.

In the encrypted traffic detection function, server certificates can be verified on the device. For expired certificates and certificates that are issued by untrusted CAs (depending on the administrator to import third-party trusted CA certificates on the device), the device can directly block traffic based on the administrator configuration to protect internal users from attacks.

2.3.5 Plaintext Mirroring

This applies to scenarios of outbound encrypted traffic detection and inbound encrypted traffic detection.

The plaintext mirroring function sends decrypted plaintext data in RawPacket format to the third-party detection device through the interface. Certain enterprises require complete audit and backup of historical traffic data. This function helps satisfy this requirement by decrypting and mirroring encrypted traffic. Meanwhile, the security functions of the third-party detection device can be used to detect mirrored data to expand the functions and capabilities of the firewall.

2.3.6 Whitelist Exceptions

This applies to scenarios of outbound encrypted traffic detection.

The administrator can use the URL category and other conditions to specify on what traffic decrypted detection is performed and on what is not performed. In inbound encrypted traffic detection scenarios, the administrator can also choose not to import interval server certificates to prevent decrypted detection on the corresponding traffic. However, decrypted traffic detection is not performed on certain traffic by default. A list of such websites is called a whitelist exception.

On the live network, when certain applications access servers, in-depth and detailed detection and special verification are performed on obtained server certificates. For example, whether or not the public key in the server certificate is consistent with a locally preset public key is checked (public key pinning). If they are inconsistent, verification on the client fails, and the connection is terminated eventually.

In this scenario, the certificate and public key sent from the SSL proxy to the client are generated by the SSL proxy itself. Therefore, the client may terminate the connection. Therefore, the encrypted traffic detection function adds application sites of this type to whitelist exceptions by default so that proxy detection is not performed on them. The administrator can remove sites from or add similar sites to whitelist exceptions.

3 Typical Applications

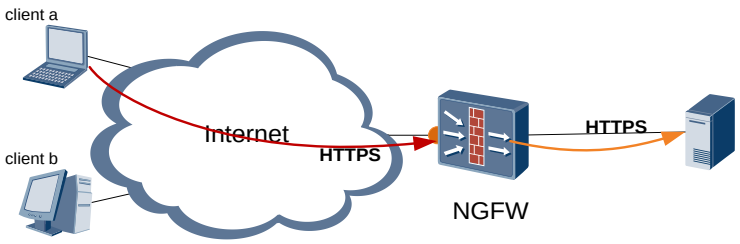
The encrypted traffic detection feature is a part of the content security component and controlled by the content security license. To use and configure this feature, the user must purchase the content security license and install the content security component.

This function employs the proxy mode and does not apply to scenarios where interactive traffic information of the two ends cannot be obtained, such as scenarios of off-line deployment, one-way traffic, active/active deployment, and inconsistent forward and reverse paths.

In a scenario where the client accepts only trusted certificates, decryption of traffic of this type is not supported by default. A typical application of this scenario is in the access to a website that employs the HTTP Strict Transport Security mechanism. The browser may block the access because of untrusted certificates. In this case, the client shall trust the decryption certificate as the CA certificate.

3.1 Inbound Encrypted Traffic Detection

Figure 3-1 Inbound encrypted traffic detection

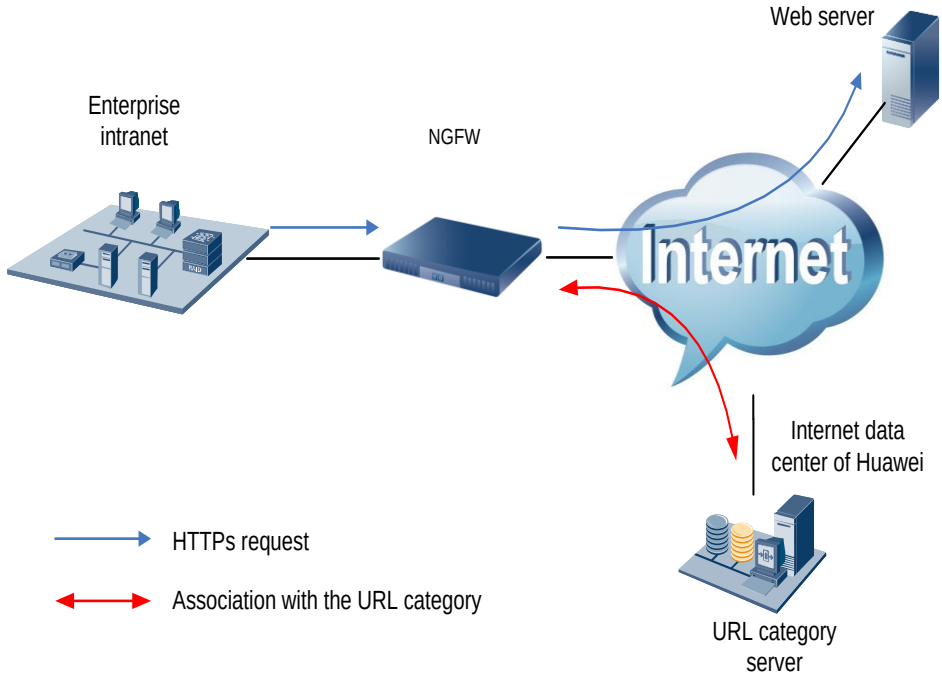


An HTTPS server is deployed on the enterprise network and provides HTTPS services externally. However, the server is exposed to various attacks from hackers and from extranet users due to various causes. The NGFW performs security detection on external encrypted traffic to protect the HTTPS server on the enterprise network.

In this scenario, the administrator shall import the certificate and private key of the internal server to the NGFW. In actual access, if the SSL proxy cannot find the certificate sent from the internal server, the SSL proxy does not perform proxy detection on encrypted traffic.

3.2 Outbound Encrypted Traffic Detection

Figure 3-2 Outbound encrypted traffic detection



Internal users may access external HTTPS servers through HTTPS. Sensitive information of the enterprise may be transferred out in encrypted mode, causing asset losses. In this case, the NGFW can decrypt encrypted traffic in the outbound direction through SSL proxy mode and performs security detection on the decrypted traffic.

In this scenario, a large number of external servers exist, and the administrator cannot obtain their certificates or private keys. Therefore, dynamic issuance by the SSL proxy is required. The certificates obtained by the clients on the enterprise network are dynamically issued by the SSL proxy. To prevent unnecessary certificate alarms and access failures caused by the alarms (such as HSTS sites), the administrator shall use CA certificates trusted by internal clients as SSL proxy decryption certificates or import SSL proxy decryption certificates to the list of CAs trusted by clients.

3.3 Carrier Network

On carrier networks, on one hand, the NGFW cannot obtain certificates or private key pairs of servers; on the other hand, the NGFW cannot install decryption certificates to the trusted lists of clients as CA certificates. In addition, carrier networks usually have high requirements on

performance but no fine-grained security detection requirements. Therefore, the encrypted traffic detection feature is not recommended.

This scenario involves most the complete isolation and filtering of websites of a category. Therefore, the URL filtering function is recommended to perform coarse-grained filtering of encrypted traffic. In this case, the NGFW uses the certificate and SNI information in the SSL handshake process to query categories and perform corresponding actions.