FORTINET Training Institute

FortiGate Administrator

Certificate Operations

FortiOS 7.4

Last Modified: 18 April 2025

Objectives

- Configure FortiGate for full SSL/SSH inspection
- Install private CA certificates on endpoints
- Troubleshoot certificate issues

Why Does FortiGate Use Digital Certificates?

- Inspection
  - SSL/SSH and HTTPS traffic inspection
  - Inbound or outbound traffic through FortiGate
  - Traffic to and from FortiGate
- Privacy
  - Ensure privacy for exchanges with other devices, such as FortiGuard
- Authentication
  - User authentication for network access
  - User authentication for VPN connection
  - As second-factor authentication for FortiGate administrator

FortiGate Uses SSL for Privacy

- SSL features:
  - Privacy of data
  - Identifies one or both parties using certificates
  - Uses symmetric and asymmetric (public key) cryptography
- Symmetric cryptography
  - Uses the same key to encrypt and decrypt data
  - Need safe way to exchange the single key
  - Faster than asymmetric cryptography
  - Used by FortiGate for exchange with other managed devices, for example, FortiManager
- Asymmetric cryptography
  - Uses two keys, one public and one private
  - Only the public key is shared with peers
  - Slower and more resource intensive than symmetric cryptography
  - Widely used, for example, HTTPS traffic

Using Certificates to Identify a Person or Device

- What is a digital certificate?
  - A digital identity produced and signed by a certificate authority (CA)
  - Analogy: passport or driver's license
- How does FortiGate use certificates to identify devices and people?
  - The **Subject** and **Subject Alternative Name** fields in the certificate identify the device or person associated with the certificate
- FortiGate uses the X.509v3 certificate standard

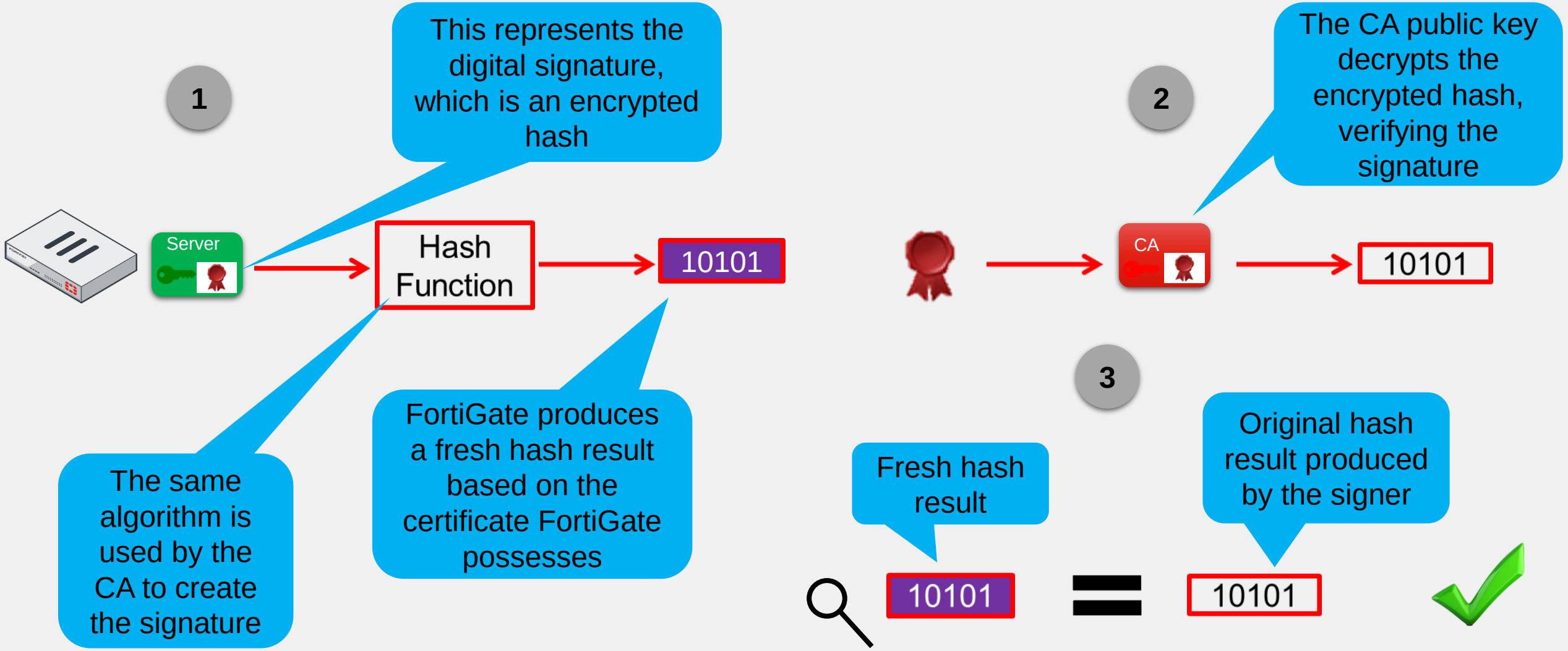
Field	Value
Version	V3
Serial number	0cacbf0403e86fc4ba3da5f26b...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Amazon RSA 2048 M02, Amaz...
Valid from	Sunday, 26 February 2023 02...
Valid to	Thursday, 28 March 2024 01:...
Subject	training.fortinet.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=c03152cd5a50c3827c7...
Subject Key Identifier	54c8bdc749bd966ac110f515d...
Subject Alternative Name	DNS Name=training.fortinet.c...
Enhanced Key Usage	Server Authentication (1.3.6....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc...
SCT List	v1, eecdd064d5db1acec55cb7...
Key Usage	Digital Signature, Key Encipher...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint	5a09781b2bc9d911f18c2d285...

How Does FortiGate Trust Certificates?

- FortiGate does the following checks against a certificate before trusting it and using it:
  - Revocation check
  - CA certificate possession
    - FortiGate uses the **Issuer** value to determine if FortiGate possesses the corresponding CA certificate
    - Without the corresponding CA certificate, FortiGate cannot trust the certificate
  - Validity dates
  - Digital signature validation
    - The verification of the digital signature on the certificate must pass

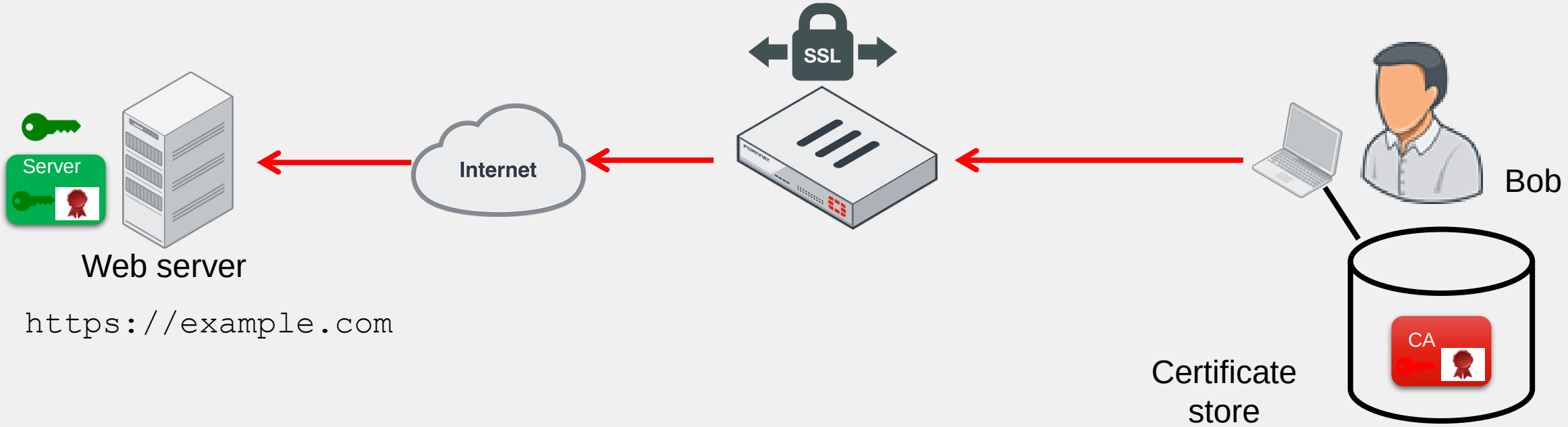
Field	Value
Version	V3
Serial number	0cacbf0403e86fc4ba3da5f26b...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Amazon RSA 2048 M02, Amaz...
Valid from	Sunday, 26 February 2023 02...
Valid to	Thursday, 28 March 2024 01:...
Subject	training.fortinet.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=c03152cd5a50c3827c7...
Subject Key Identifier	54c8bdc749bd966ac110f515d...
Subject Alternative Name	DNS Name=training.fortinet.c...
Enhanced Key Usage	Server Authentication (1.3.6....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc...
SCT List	v1, eecdd064d5db1acec55cb7...
Key Usage	Digital Signature, Key Encipher...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint	5a09781b2bc9d911f18c2d285...

FortiGate Verifies a Digital Signature



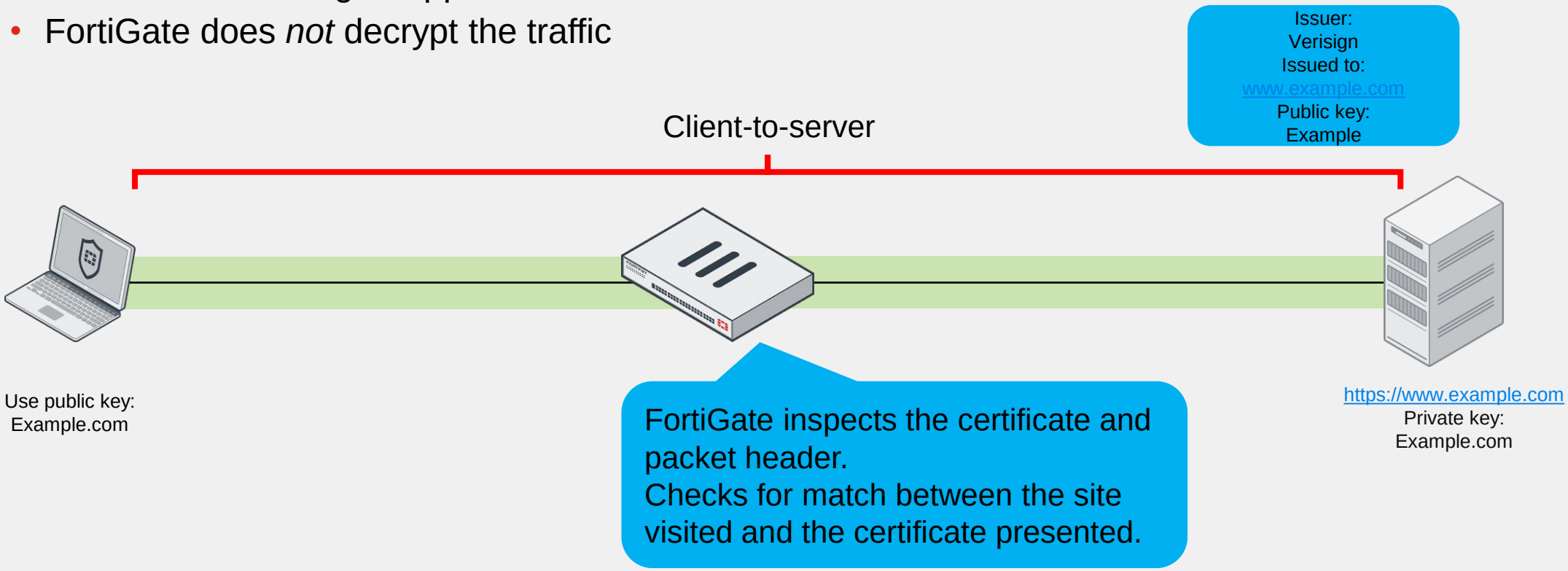
Encrypted Traffic With No SSL Inspection

- Cloaked by encryption, viruses can pass through network defenses unless you enable full SSL inspection



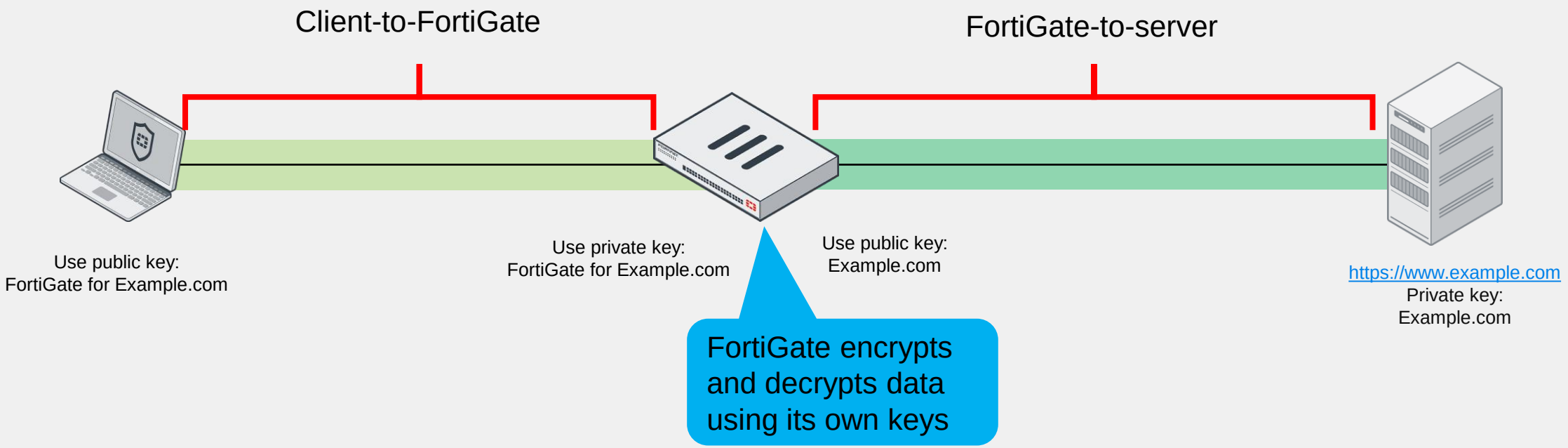
SSL Inspection Modes

- SSL certificate inspection
  - Relies on extracting the FQDN of the URL from either
    - TLS extension server name indication (SNI)
    - SSL certificate **Subject** or Subject Alternative Name (**SAN**) fields
  - Use for web filtering or application control
  - FortiGate does *not* decrypt the traffic



SSL Inspection Modes (Contd)

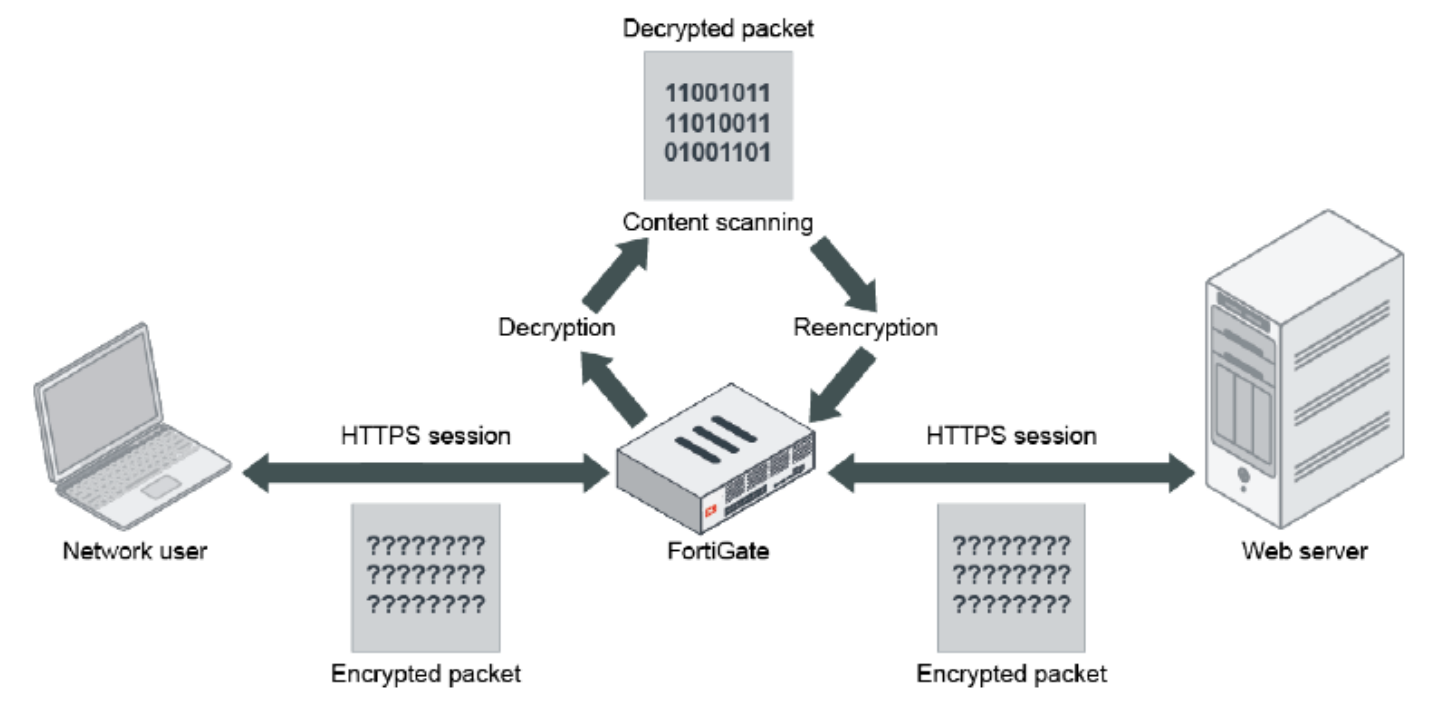
- Full SSL Inspection
  - FortiGate acts as a man-in-the middle proxy
  - Maintains two separate SSL sessions—client-to-FortiGate, and FortiGate-to-server
  - FortiGate encrypts and decrypts packets using its own keys
  - FortiGate can inspect the traffic



Full SSL Inspection

- Protect from attacks that use commonly used SSL-encrypted protocols
  - HTTPS
  - SMTPS
  - POP3S
  - IMAPS
  - FTPS

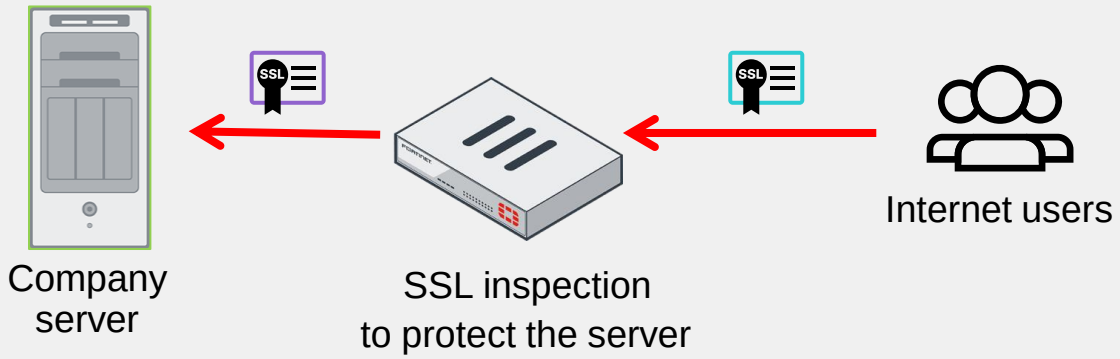
- FortiGate impersonates the recipient of the originating SSL session
  - Impersonates – decrypts
  - Inspects – blocks threats
  - Re-encrypts and sends to real recipient



Inbound or Outbound SSL/SSH Inspection

- SSL/SSH inspection for outbound traffic
  - Protecting internal users
  - Multiple clients connecting to multiple servers
    - External web servers
    - External mail servers
    - External FTPS servers

- SSL/SSH inspection for inbound traffic
  - Protecting a single company server
    - HTTPS server
    - Mail server
    - FTPS server
  - FortiGate use a server certificate
  - FortiGate as proxy server



* → arrow direction represents traffic initialization

SSL Inspection Profile Configuration

- Ready-to-use profiles for inspection of outbound encrypted sessions
  - SSL certificate inspection
  - SSL full inspection
- Customizable profile
  - Outbound deep inspection with options
- User-defined profile
  - Inbound traffic
  - Outbound traffic

Security Profiles > SSL/SSH Inspection

Name	Comments
SSL custom-deep-inspection	Customizable deep inspection profile.
SSL deep-inspection	Read-only deep inspection profile.
SSL no-inspection	Read-only profile that does no inspection.
SSL certificate-inspection	Read-only SSL handshake inspection profile.

Predefined profile for SSL full inspection

Predefined profile for certificate inspection

SSL Inspection Profile Configuration (Contd)

- Customized SSL/SSH inspection profile
  - Based on deep inspection profile
  - User defined

Security Profiles > SSL/SSH Inspection

Edit SSL/SSH Inspection Profile

Name: custom-deep-inspection

Comments: Customizable deep inspection profile. 37/255

Decrypt outbound traffic

SSL Inspection Options

Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers | Protecting SSL Server

Inspection method: SSL Certificate Inspection | Full SSL Inspection

CA certificate: Fortinet_CA_SSL | Download

Blocked certificates: Allow | Block | View Blocked Certificates

Untrusted SSL certificates: Allow | Block | Ignore | View Trusted CAs List

Server certificate SNI check: Enable | Strict | Disable

Enforce SSL cipher compliance

Enforce SSL negotiation compliance

RPC over HTTPS

Inspection mode

Refine action related to certificate analysis

Exempting Sites From SSL Inspection

- Why exempt?
  - Problems with traffic
  - Legal issues

Allowlist exemption as rated by FortiGuard web filtering as “reputable”

Exempt per web category

Exempt per address (FQDN, IP address, address range)

Security Profiles > SSL/SSH Inspection

Exempt from SSL Inspection

Reputable websites

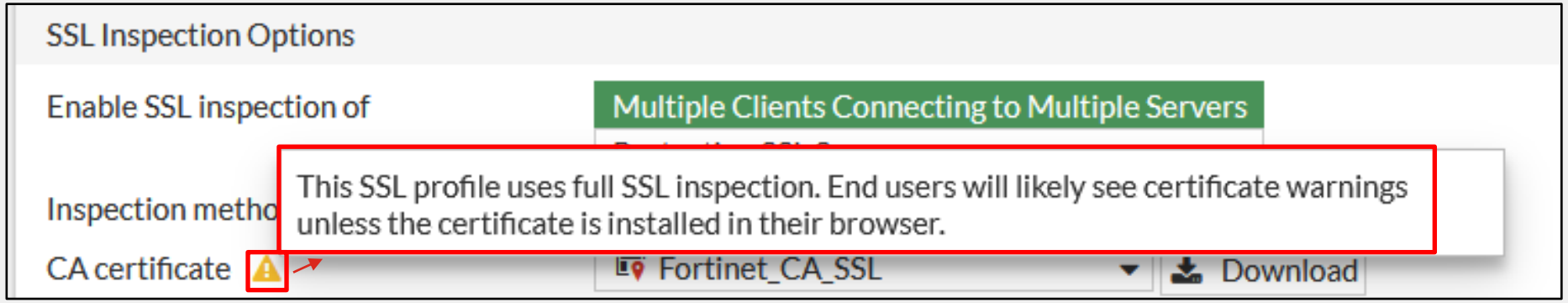
Web categories
- Finance and Banking
- Health and Wellness
- +

Addresses
- adobe
- apple
- fortinet
- google-drive
- google-play
- skype
- softwareupdate.vmware.com
- update.microsoft.com
- verisign
- +

Log SSL exemptions

FortiGate Self-Signed CA Certificates

- By default, FortiGate uses a self-signed encrypting SSL CA certificate
  - `Fortinet_CA_SSL`
  - Not listed with an approved CA, therefore, by default, not trusted



- To avoid warnings on user devices
  - Install CA certificate `Fortinet_CA_SSL` as trusted CA on user devices
  - Install a company CA certificate on FortiGate for SSL full inspection

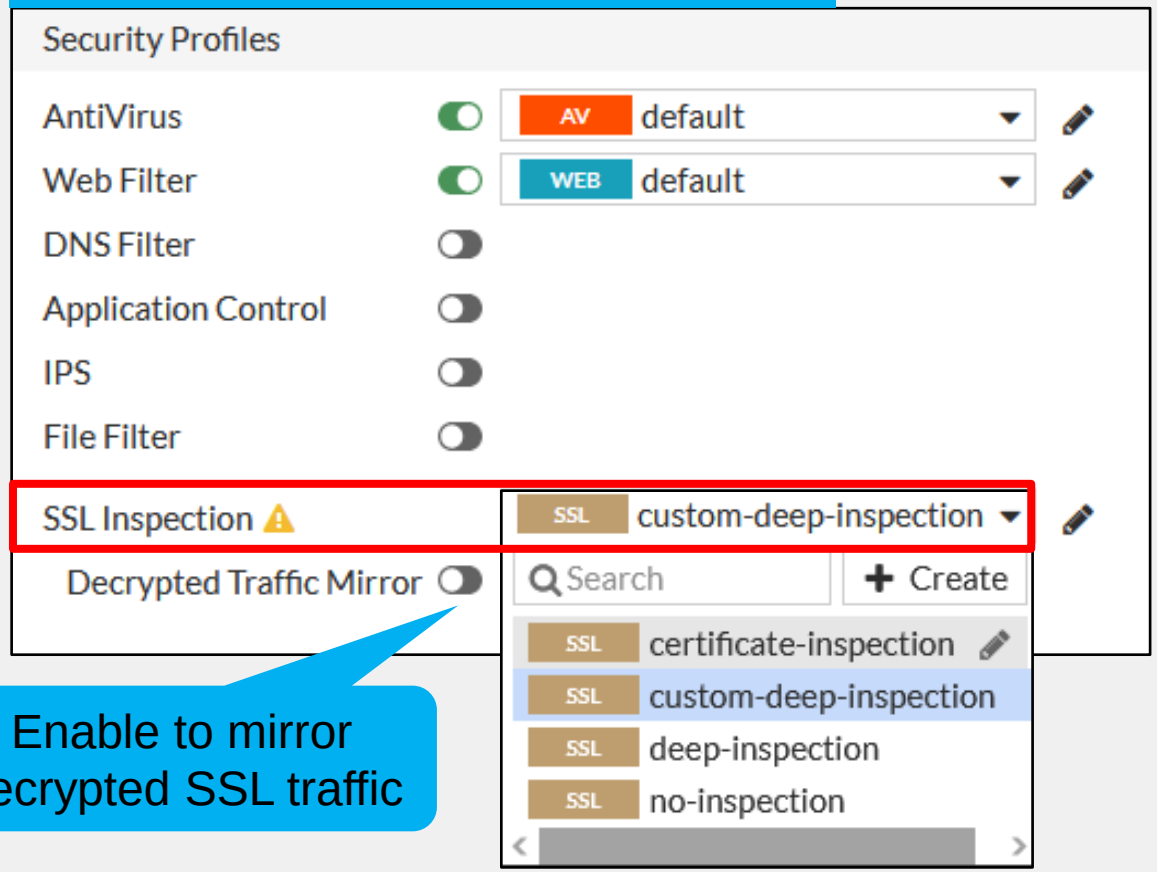
Full SSL Inspection—Certificate Requirements

- Full SSL inspection requires that FortiGate acts as a CA to generate an SSL private key and certificate
  - The CA certificate requires these two extensions to issue certificates:
    - cA=True
    - keyUsage=keyCertSign
- FortiGate can use:
  - Preloaded, self-signed `Fortinet_CA_SSL` certificate
  - A certificate issued by the company CA
- The root CA certificate must be imported into the client machines

Applying an SSL Inspection Profile to a Firewall Policy

- For SSL inspection
  - Define SSL inspection profile
  - Allow the traffic with a firewall policy
  - Apply security profiles
  - Apply SSL inspection
- Combine SSL inspection with security profiles
- With the **no-inspection** SSL profile there is no SSL or SSH traffic inspection
  - No web filtering
  - No application control

Policy & Objects > Firewall Policy

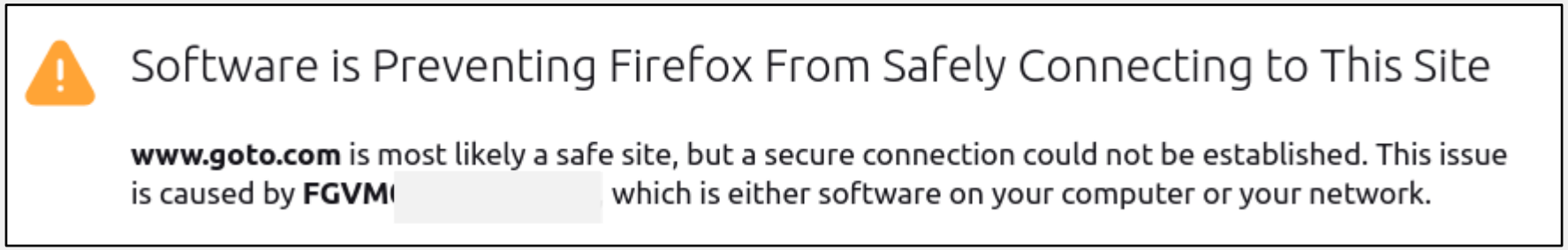


Enable to mirror decrypted SSL traffic

Select SSL inspection profiles

Certificate Warnings During Full SSL Inspection

- During full SSL inspection, browsers might display a warning because they do not trust the CA

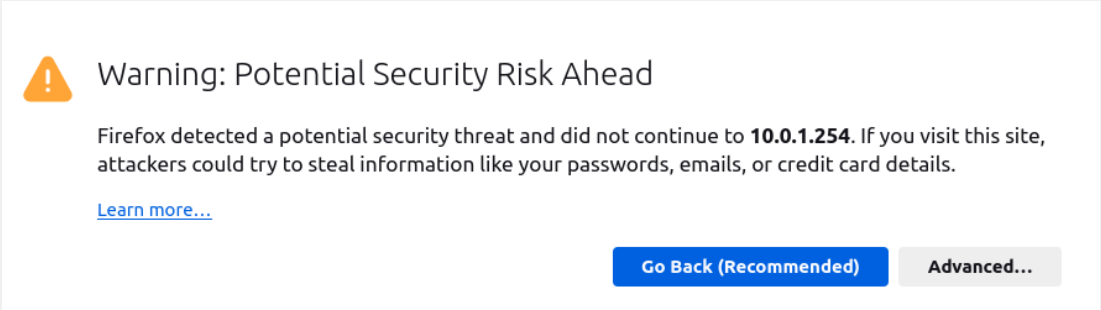


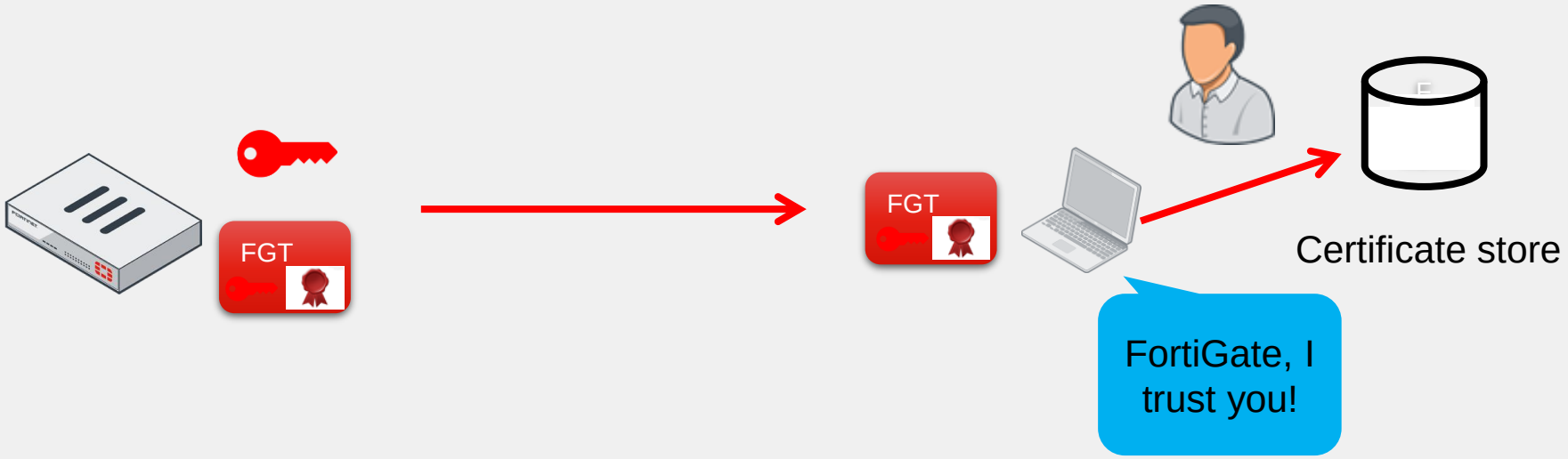
- To enable a smooth user experience, and prevent certificate warnings, do one of the following:
  - Use the `Fortinet_CA_SSL` certificate
    - And import the FortiGate CA root certificate into all the browsers
  - Use an SSL certificate issued by a private CA
    - This CA may already be available in the device browsers

- This is not a FortiGate limitation, but a consequence of how SSL and digital certificates work

Certificate Warnings on the FortiGate GUI

- By default, FortiGate uses a self-signed SSL certificate
  - Not listed with an approved CA, therefore, by default, not trusted
  - Used for HTTPS GUI access
- Available options to avoid those warnings:
  - Accept the warning at first connection
  - Use the `Fortinet_GUI_Server` certificate and import the `Fortinet_CA_SSL` certificate
  - Use a certificate signed by a recognized CA





FortiGate HTTPS Server Certificates

- Default settings: `self-sign`
  - Default
  - Triggers warning on first connection from browsers

System > Settings

Administration Settings

HTTP port: 80

Redirect to HTTPS

HTTPS port: 443

Port conflicts with the SSL-VPN port setting

HTTPS server certificate: self-sign

A default certificate is being used, which will not be able to verify the server's domain name (admins will see a warning). To avoid this warning, switch to the FortiGate's "Fortinet_GUI_Server" certificate or generate a trusted certificate using Let's Encrypt.

Create Certificate

- Alternative: `Fortinet_GUI_Server`
  - Pre-loaded on FortiGate
  - Signed by `Fortinet_CA_SSL`

System > Settings

Administration Settings

HTTP port: 80

Redirect to HTTPS

HTTPS port: 443

Port conflicts with the SSL-VPN port setting

HTTPS server certificate: Fortinet_GUI_Server

Download HTTPS CA certificate

For optimal security please generate a trusted certificate using Let's Encrypt.

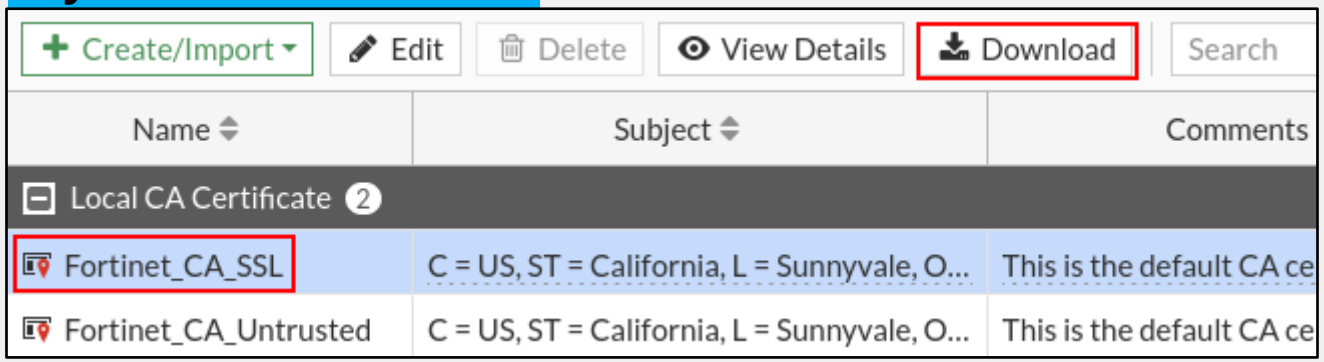
Create Certificate

Download the CA certificate and import into the browser

Download Private CA Certificates From FortiGate

- Download `Fortinet_CA_SSL` private CA certificate

System > Certificates

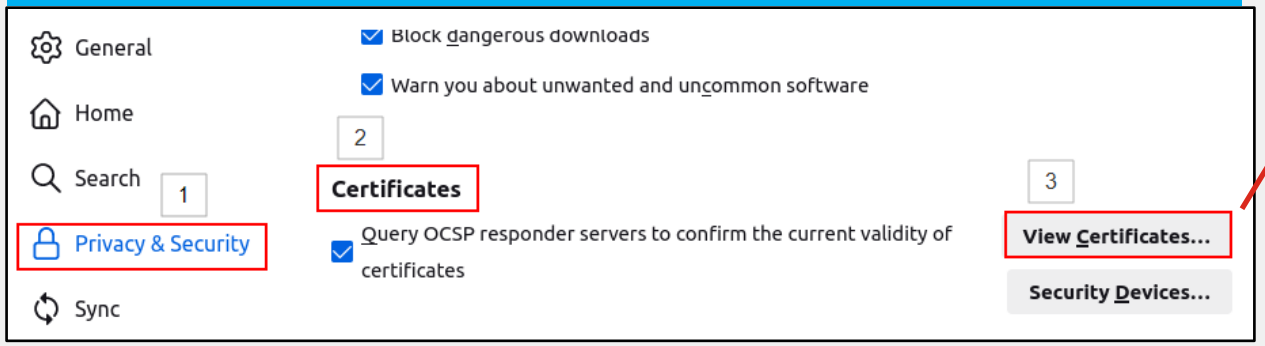


- Generate a file `Fortinet_CA_SSL.cer`
- Transfer to any computer that requires it

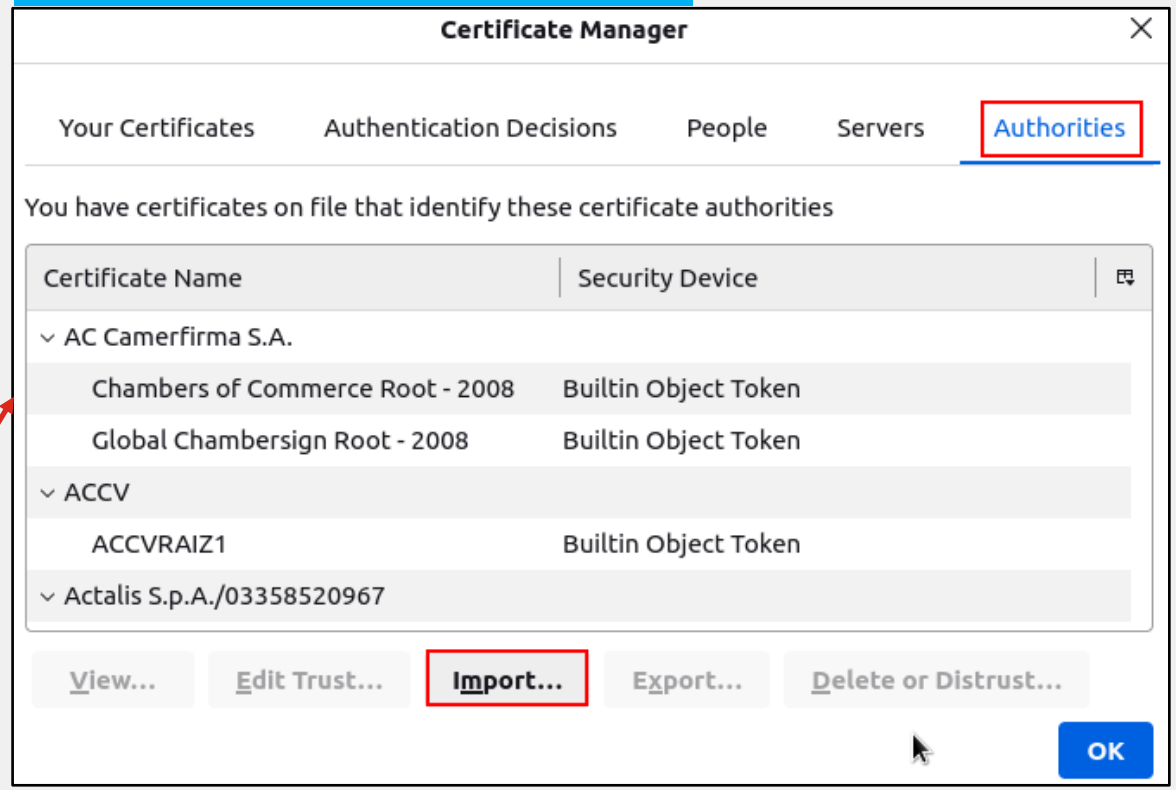
Import Private CA Certificates Into Endpoints

- Import `Fortinet_CA_SSL` private CA certificate into user device
  - Exact process depends on the operating system
  - Example for Linux and Firefox
    - Open the browser setting menu
    - Open the certificate store
    - Import the certificate as a CA authority

Firefox: **Settings** > **Privacy & Security** > **Certificates**



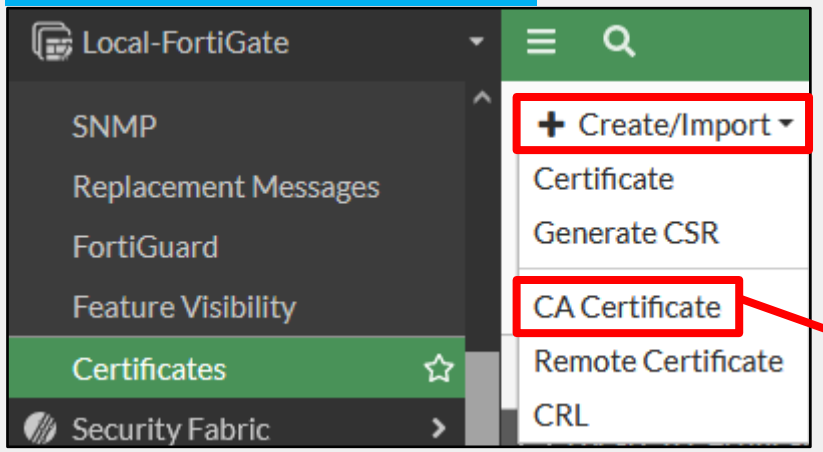
Firefox: **Certificate Manager**

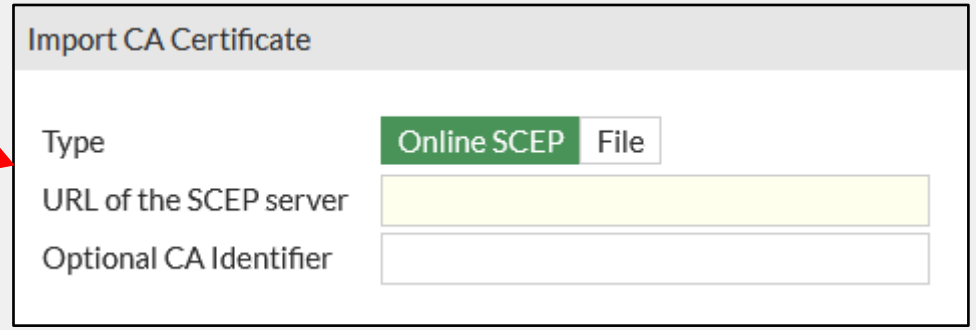


Import a CA Certificate on FortiGate

- Import company-owned private CA or CA signed by a certificate authority

System > Certificates

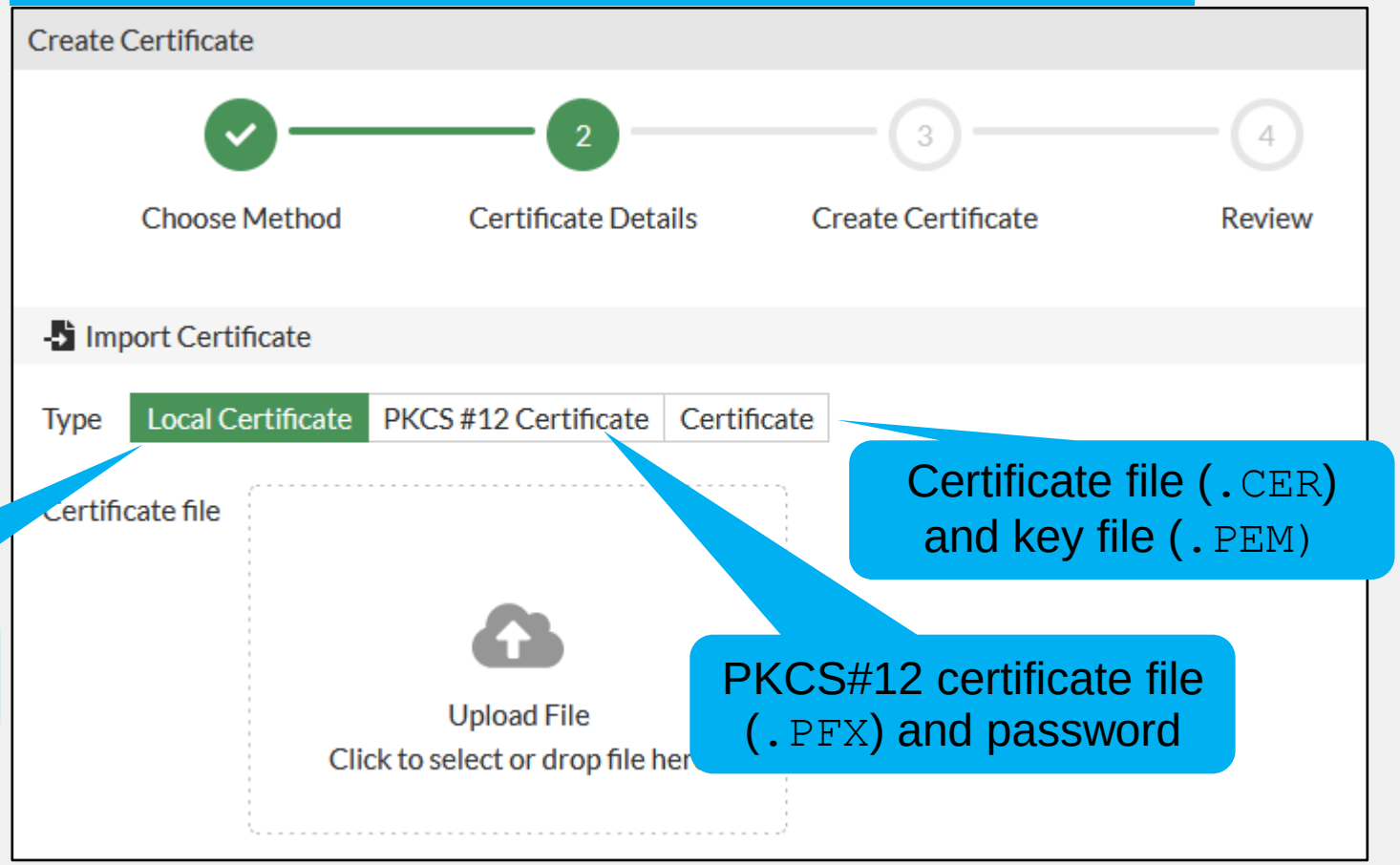




Import a Certificate on FortiGate

- Import private certificates
- Used for:
  - FortiGate GUI
  - SSL-VPN tunnels
- Import options:
  - Certificate after CSR request
  - Certificate and associated key file
  - PKCS#12 certificate

System > Certificates > Create/Import > Certificate



Certificate file (`.CER`) after CSR request

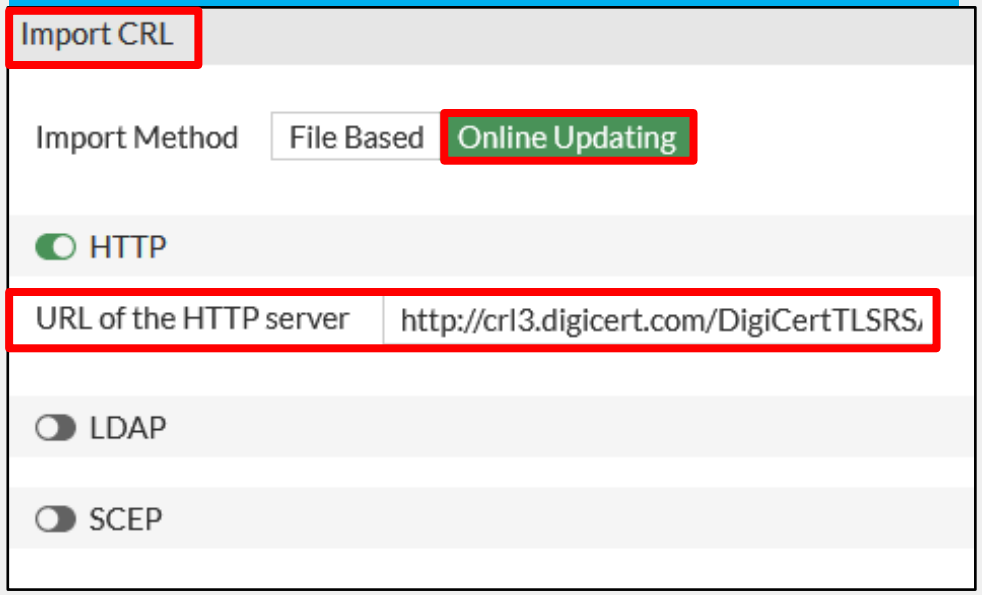
Certificate file (`.CER`) and key file (`.PEM`)

PKCS#12 certificate file (`.PFX`) and password

Import CRLs on FortiGate

- CRLs are lists of revoked certificates
- Published by CA administrator and updated periodically
- Import on FortiGate
  - Online updating
    - HTTP
    - LDAP
    - SCEP
  - File import

System > Certificates > Create/Import > CRL



System > Certificates

Name	Subject	Comments	Issuer	Expires	Status	Source
CRL 1						
CRL_1			DigiCert Inc		Valid	User
Local CA Certificate 2						
Fortinet_CA_SSL	C = US, ST = Califor...	This is the defaul...	Fortinet	2030/04/25 13:37:28	Valid	Factory
Fortinet_CA_Untrus...	C = US, ST = Califor...	This is the defaul...	Fortinet	2030/04/25 12:21:58	Valid	Factory

CRL section

FortiGate Certificate Store

- Central location for CA, Certificates, and CRL on FortiGate

System > Certificates

Name	Subject	Comments	Issuer	Expires	Status	Source
CRL 1						
CRL_1			DigiCert Inc		Valid	User
Local CA Certificate 3						
ACME-SSL-Cert	C = CA, O = ACME, OU = ACME-IIT, CN = ACME-SSL-...	Company signing CA	ACME	2024/09/27 06:21:00	Valid	User
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This is the default CA certificate ...	Fortinet	2030/04/25 13:37:28	Valid	Factory
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...	This is the default CA certificate ...	Fortinet	2030/04/25 12:21:58	Valid	Factory
Local Certificate 18						
FortiGate_ACME					Pending	User
Ana	C = CA, O = ACME, OU = ACME-Finance, CN = Ana, e...		ACME	2024/09/27 06:21:00	Valid	User
Local-FortiGate	C = CA, O = ACME, OU = ACME_IT, CN = ACME-FGT, ...		ACME	2024/09/27 06:04:00	Valid	User
Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, I...	This certificate is embedded in t...	DigiCert Inc	2024/06/06 16:59:59	Valid	Factory
Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Lt...	This is the default CA certificate ...	Fortinet	2025/08/28 10:57:01	Valid	Factory
Remote CA Certificate 5						
CA_Cert_1	C = CA, O = ACME, OU = ACME-IIT, CN = ACME-SSL-...		ACME	2024/09/27 06:21:00	Valid	User
Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA...		DigiCert Inc	2030/09/23 16:59:59	Valid	Factory
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, O...		Fortinet	2056/05/27 13:27:39	Valid	Factory

Loaded CRLs

Deep inspection signing CAs certificates

Pending CSR

User certificate

Company cert. for FortiGate

CA certificates

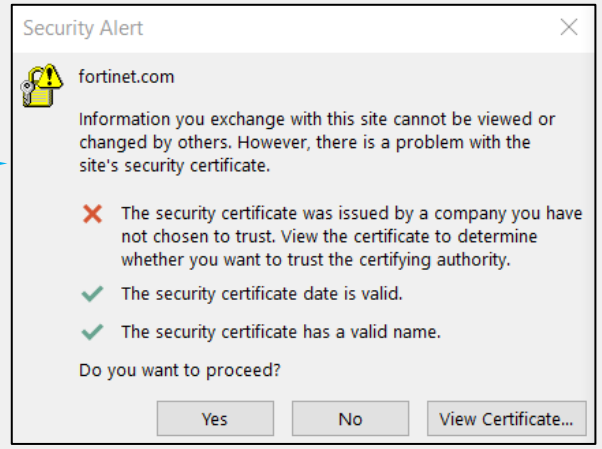
Imported CA certificates

FORTINET Training Institute

Applications and SSL Inspection

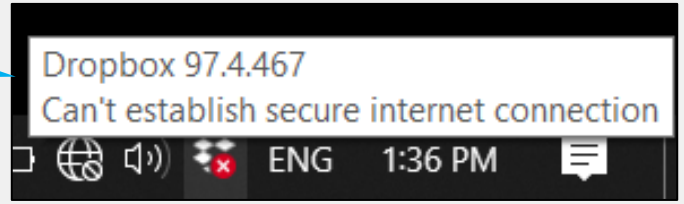
- Any SSL application might be impacted by SSL inspection (not just the browser)
  - The solution depends on the application security design
  - Consider other SSL-based protocols such as FTPS, SMTPS, and STARTTLS (not just HTTPS)
- Microsoft Outlook 365 for Windows error after enabling full SSL inspection:

Solution: Import the CA certificate into the Windows certificate store (FortiGate keeps inspecting SSL traffic)



- Dropbox for Windows error after enabling full SSL inspection:

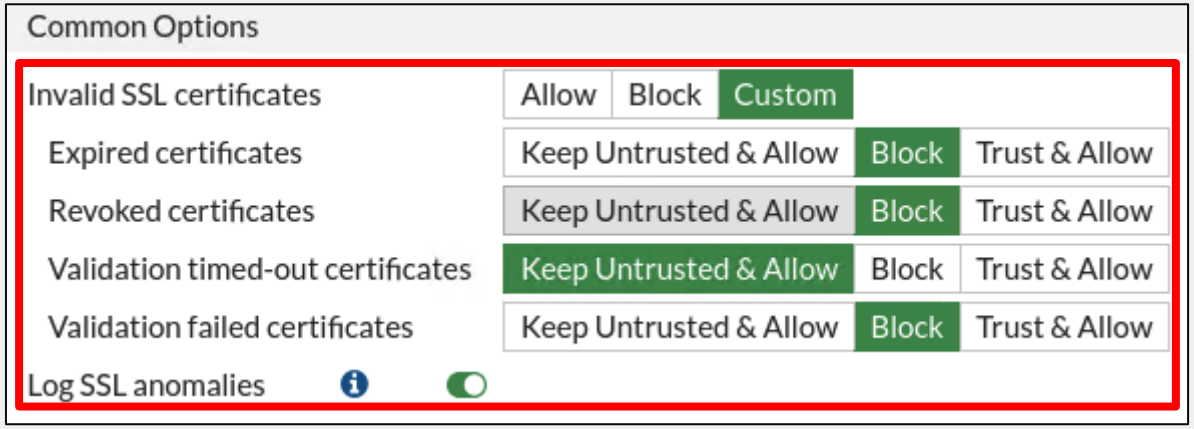
Solution: Exempt Dropbox domains from SSL inspection (FortiGate no longer inspects SSL traffic)



Invalid Certificates

- FortiGate can detect invalid certificates for a variety of reasons
  - Invalid certificates produce security warnings due to problems with the certificate details
- FortiGate can **Keep Untrusted & Allow**, **Block,** or **Trust & Allow** invalid certificates
- Selecting **Custom** allows the user to select the action for each reason

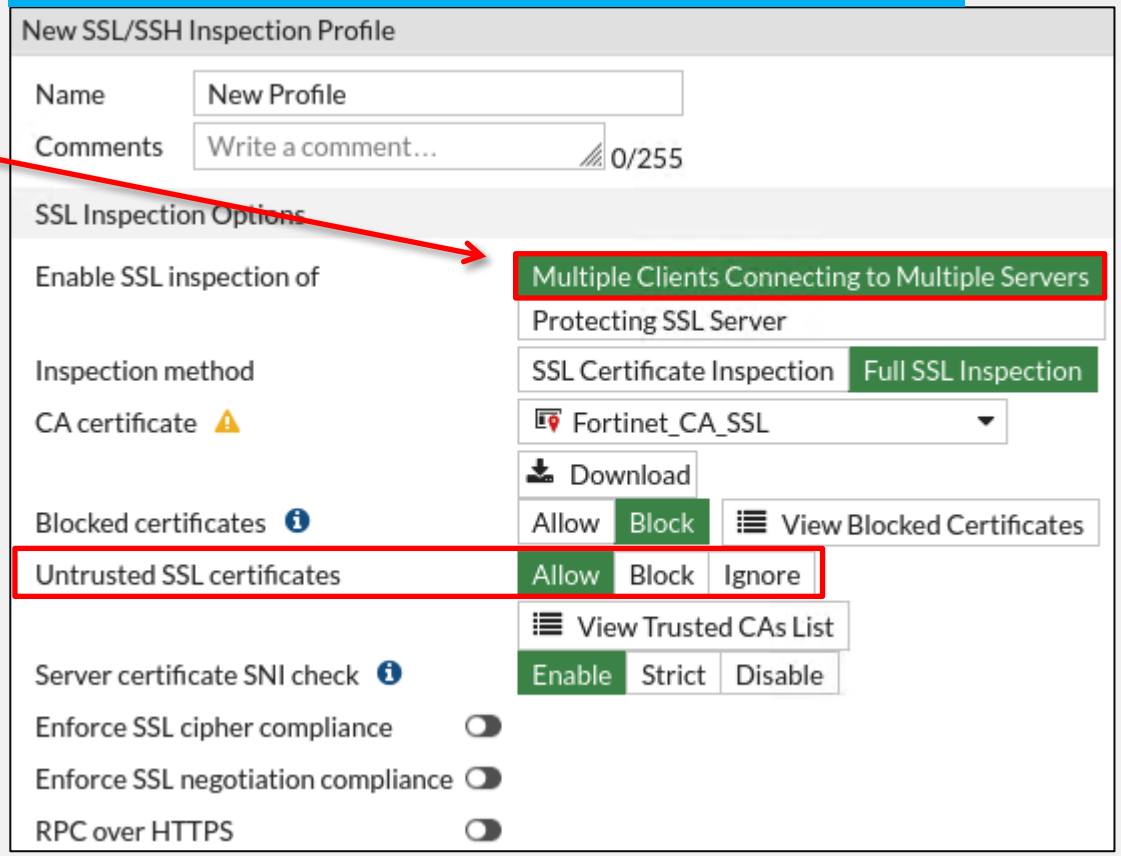
Security Profiles > SSL/SSH Inspection



Untrusted SSL Certificates Setting

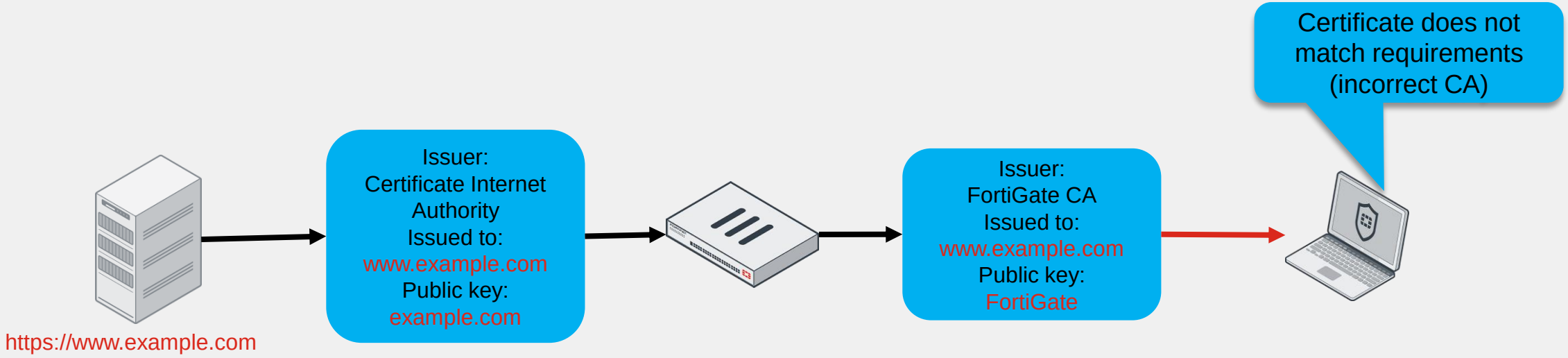
- Allow, block, or ignore untrusted certificates (only available if **Multiple Clients Connecting to Multiple Servers** is selected)
  - **Allow**: sends the browser an untrusted temporary certificate when the server certificate is untrusted
  - **Block**: blocks the connection when an untrusted server certificate is detected
  - **Ignore**: uses a trusted FortiGate certificate to replace the server certificate always, even when the server certificate is untrusted

Security Profiles > SSL/SSH Inspection



Full SSL Inspection and HSTS

- Some clients have specific requirements for SSL
  - HSTS: HTTPS Strict Transport Security
    - Example: Chrome requires a Google certificate when accessing any Google site
- HSTS common error message
  - “Privacy error: Your connection is not private” (NET::ERR_CERT_AUTHORITY_INVALID)



Visit Sites With HSTS Requirement

- Possible workarounds for sites with HSTS requirement
  - Exempt those websites from full SSL inspection
  - Use SSL certificate inspection instead
  - Adjust browser settings

Security Profiles > SSL/SSH Inspection

Wildcard FQDN definition to exclude *.example.com sites from SSL deep inspection

Policy & Objects > Firewall Policy

ID	Name	Destination	Security Profiles
2	Exempt_Deep_Inspection	Exception-Add	WEB default SSL certificate-inspection
1	Full_Access	all	WEB default SSL deep-inspection
0	Implicit Deny	all	

Carefully define exception policy to exclude only sites that require it from deep inspection

Knowledge Check

1. Which attribute or extension identifies the owner of a certificate?
   - ✓ A. The subject name in the certificate
   - B. The unique serial number in the certificate

2. Which configuration requires FortiGate to act as a CA for full SSL inspection?
   - ✓ A. Multiple clients connecting to multiple servers
   - B. Protecting the SSL server

3. Which inspection mode can protect your LAN devices from encrypted malware?
   - A. Certificate inspection
   - ✓ B. Deep inspection

Review

- ✓ Describe certificate inspection and full SSL inspection
- ✓ Configure FortiGate for full SSL inspection
- ✓ Identify obstacles to implementing full SSL inspection and possible remedies