SSL Inspection の証明書検査について

2010 年 7 月 13 日現在

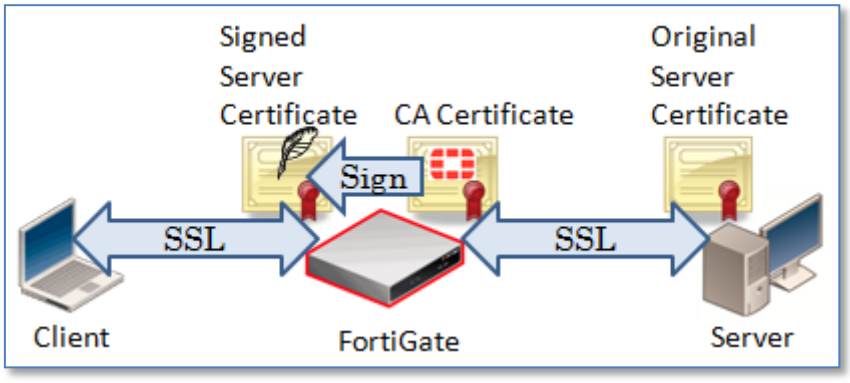
対象製品	FortiGate
対象 OS	FortiOS 4.0, 4.0MR1, 4.0MR2
項目	SSL Inspection

FortiGate 4.0 以上において Deep Scan 機能を有効にして SSL Inspection を行う際の、接続先サーバの証明書をどのように検査するのかと、その検査機構に関するトラブルシューティングについて説明します。

■ 基本的な動作説明

SSL Inspection を通じて SSL サイトへ接続すると、FortiGate がそのサーバとの SSL セッションを終端し、クライアントへその SSL セッションを中継します。

FortiGate はクライアントへ新たな SSL セッションを確立するために、サーバの証明書（Original Server Certificate）を FortiGate が持っている CA 証明書（Fortinet_CA 等の CA Certificate）で署名し、これ（Signed Server Certificate）をクライアントへ提供します。



■ 例）https://support.fortinet.com/ のオリジナルサーバ証明書（一部抜粋）

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1208893255 (0x480e3f47)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Entrust, Inc., OU=AND ADDITIONAL TERMS GOVERNING USE AND
RELIANCE, OU=CPS CONTAINS IMPORTANT LIMITATIONS OF WARRANTIES AND LIABILITY,
OU=www.entrust.net/CPS is incorporated by reference, OU=(c) 2008 Entrust, Inc.,
CN=Entrust Certification Authority - L1B
        Validity
            Not Before: Nov 26 20:51:26 2009 GMT
            Not After : Nov 23 21:17:27 2012 GMT
        Subject: C=CA, ST=British Columbia, L=Burnaby, O=Fortinet Technologies
Canada Inc., OU=Customer Support, CN=support.fortinet.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALS
```

■ 例）https://support.fortinet.com/ へ SSL Inspection を通じてアクセスし、FortiGate が署名したサーバ証明書（一部抜粋）

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4c:24:30:7e:00:00:00:00
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate
Authority, CN=FortiGate CA/emailAddress=support@fortinet.com
        Validity
            Not Before: Nov 26 20:51:26 2009 GMT
            Not After : Nov 23 21:17:27 2012 GMT
        Subject: C=CA, ST=British Columbia, L=Burnaby, O=Fortinet Technologies
Canada Inc., OU=Customer Support, CN=support.fortinet.com
```

■ 例）FortiGate にインストールされている、CA 証明書（一部抜粋）

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate
Authority, CN=support/emailAddress=support@fortinet.com
        Validity
            Not Before: Apr  9 01:25:49 2000 GMT
            Not After : May 24 01:25:49 2020 GMT
        Subject: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate
Authority, CN=support/emailAddress=support@fortinet.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
```

■ SSL Inspection による証明書検査について

FortiGate が接続先のサーバ証明書を受け取った際に、その内容を確認します。これは、diagnose によるデバッグで処理内容を一部確認することができます。

FortiGate では、証明書の有効期限が過ぎているものについては無効な証明書として扱います。

よく発生するエラーである Common Name とサイト名（URL）の不一致があっても、FortiGate はこれを気にしません。FortiGate に該当する CA 証明書を持っていなければ、外部 CA においての正当性確認を行ないません。FortiGate はこれらの照合結果を、無効な証明書として判断するための材料としては扱いません。

無効な証明書の正当性を無視して SSL セッションを確立したい場合は、allow-invalid-server-cert オプションを有効にしてください。

FortiOS 4.0 MR1 以下

```
config firewall profile
  edit <name>
    set <protocol> allow-invalid-server-cert
  next
end
```

FortiOS 4.0 MR2

```
config firewall profile-protocol-options
  edit <name>
    config <protocol>
      set <protocol> allow-invalid-server-cert
    end
  next
end
```

■ 参考資料

How to enable Deep Content Inspection
http://kb.fortinet.com/kb/documentLink.do?externalID=FD30586

Technical Note：Cannot browse secure web sites (HTTPS) with IE6 when AV deep scan is enabled on a FortiGate
http://kb.fortinet.com/kb/documentLink.do?externalID=FD32344

Technical Note：Importing the FortiGate SSL Proxy certificate in Internet Explorer 8 (IE8) for decryption on SSL Inspection
http://kb.fortinet.com/kb/documentLink.do?externalID=FD32404

-以上-

※このドキュメントの内容は作成時点のものであり、将来にわたって保証されるものではありません。また内容は予告なく変更される場合がございますのでご了承ください。