

El dispositivo Threatgrid no acepta el certificado CA

Contenido

[Introducción](#)

[Solución](#)

Introducción

Al agregar el contenido del archivo de certificado, el dispositivo Threatgrid no acepta el certificado y muestra un error que indica que se trata de "No es un certificado de CA de cliente/servidor" y que el error se ve como sigue:



Solución

Es posible que el certificado en cuestión no tenga las extensiones necesarias para ser aceptado por el dispositivo Threatgrid. Para que el certificado de CA sea aceptado por la red de amenazas, debe tener las extensiones de CA correctas. Para verificar esto:

Paso 1: Para verificar el certificado, puede ejecutar este comando openssl.

```
openssl x509 -in poke.fireamp.pem -text
```

Paso 2: El contenido como se ve aquí es:

```
Certificate: Data: Version: 1 (0x0) Serial Number: 0 (0x0) Signature Algorithm:
sha256WithRSAEncryption Issuer: C = IN, ST = KA, O = MYLAB, OU = MYLAB, CN = root.mylab.com
Validity Not Before: Jun 3 08:55:34 2020 GMT Not After : May 29 08:55:34 2040 GMT Subject: C =
IN, ST = KA, O = MYLAB, OU = MYLAB, CN = dispupd-master3.mylab.com Subject Public Key Info:
Public Key Algorithm: rsaEncryption RSA Public-Key: (2048 bit) Modulus:
00:9f:4c:cc:c1:0c:bb:88:b0:fb:c0:68:19:a2:36: e4:29:4d:ef:68:23:e2:69:0f:d6:b7:96:7e:f8:80:
7a:1f:76:97:42:a4:a0:a5:26:2f:b6:06:67:14:26: df:ab:50:c0:fc:ec:e4:02:7b:ca:86:cf:99:8e:43:
1d:d3:51:4b:0a:7e:ca:46:5a:9f:f2:68:ae:3d:c5: a1:ab:3b:bb:c3:83:c3:a1:61:83:1e:1e:d6:ab:13:
a3:b1:51:b0:15:f4:a1:11:89:e6:79:0f:ae:89:6b: 5b:ec:74:4d:75:00:60:59:06:49:f1:f5:7c:b8:70:
67:29:fc:fb:81:88:cd:cf:a9:6e:8f:b6:02:b1:58: 02:8c:41:73:9f:7c:fc:9b:37:b4:1f:bd:28:7b:ca:
90:5e:97:7f:4f:40:0e:be:e3:55:cc:dc:32:fb:5a: ef:c0:40:83:ab:20:c5:28:c1:ca:c5:54:b5:c3:87:
```

```
ec:79:be:6e:46:e5:44:56:fc:ab:9b:5f:f5:a3:8b: 06:e3:b3:29:09:bd:76:96:ba:22:09:85:c5:e2:50:
e2:d9:10:f2:58:42:be:99:be:5f:6c:eb:82:dc:3e: d0:d3:a5:b4:c6:d5:7a:e6:1a:e8:cc:dc:19:b9:c8:
0c:8c:8c:87:a5:d5:0d:d1:d4:1b:a6:14:4f:29:68: 82:cf Exponent: 65537 (0x10001) Signature
Algorithm: sha256WithRSAEncryption 4a:1f:00:60:fe:0b:0b:e0:02:f8:85:6e:ff:e6:73:92:7a:3f:
4c:46:89:36:84:51:f1:f8:73:9a:b6:6e:83:54:92:48:f4:df:
df:10:d8:c4:f2:36:38:fd:0e:1b:9c:ef:f7:91:c3:90:db:cc:
ec:84:a0:45:9b:35:85:d9:39:10:e6:01:e9:6c:ab:29:c7:0b:
57:12:b4:cb:bd:cf:ae:1c:3a:ff:a1:7d:b7:d4:b2:98:53:7b:
d9:25:11:40:72:1b:ce:90:dd:3e:c8:3c:9f:bf:5b:f5:78:d0:
be:66:b9:d2:ed:d3:c8:71:1d:75:b7:29:37:17:5f:e3:63:68:
51:1d:30:7b:1d:45:67:b2:71:61:59:39:26:19:aa:87:d7:f1:
07:b1:3b:68:b0:1a:5a:9f:61:e3:55:ae:31:80:dc:46:e5:4a:
46:f7:12:6b:1b:8f:b5:68:bf:00:56:66:6a:c6:b2:d9:7a:ea:
61:de:15:72:eb:3b:49:d1:55:bc:9d:6c:8b:05:36:82:f7:b8:
12:ac:c9:f0:e9:1c:8b:60:2d:cf:61:8b:4f:7c:3f:89:e0:05:
e4:58:a8:22:13:74:76:7a:86:20:b2:8c:ae:cc:68:28:56:63:
df:ac:85:29:5b:e4:2b:8e:98:36:75:71:6f:48:3a:af:4c:8f: 4e:57:c5:ce
```

Paso 3:Esto indica que las extensiones CA no están presentes. Estas son las extensiones esperadas que se verán en el certificado de CA.

```
X509v3 Basic Constraints: critical CA:TRUE
```

Paso 4: Asegúrese de que el certificado tenga estas extensiones disponibles y, de lo contrario, deberá solicitar al proveedor de certificados que comparta el certificado de CA con estas extensiones. Si ha creado su certificado con OpenSSL, estos comandos le ayudarán a generar el certificado de CA con extensiones correctas.

```
openssl genrsa -out rootCA.key 2048
```

```
openssl req \ -addext basicConstraints=critical,CA:TRUE\ -outform pem -out rootCA.pem \ -key
rootCA.key -new -x509 \ -days "1000"
```

Paso 5: A continuación se muestra un ejemplo de cómo es un certificado aceptable:

```
Certificate: Data: Version: 3 (0x2) Serial Number:
56:e4:2f:5a:f3:21:e2:17:43:13:cb:21:b3:30:16:cb:37:12:54:c6 Signature Algorithm:
sha256WithRSAEncryption Issuer: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd Validity
Not Before: Nov 17 08:50:01 2020 GMT Not After : Aug 14 08:50:01 2023 GMT Subject: C = AU, ST =
Some-State, O = Internet Widgits Pty Ltd Subject Public Key Info: Public Key Algorithm:
rsaEncryption RSA Public-Key: (2048 bit) Modulus: 00:cb:1a:3d:db:4f:5d:15:4f:e7:75:37:ae:ac:a4:
dc:de:9d:67:34:6d:ca:d4:9a:e4:26:73:d0:08:90: 0f:0d:bc:16:0f:9c:bb:7d:7e:e0:39:36:78:0f:19:
b0:c1:6a:20:33:96:f9:70:f0:7d:33:74:79:8a:a1: f8:aa:a4:81:50:dc:e7:5a:b7:4d:6a:4a:d6:aa:5a:
59:d7:58:05:1c:14:d3:03:01:c5:cd:ce:a5:bd:68: be:c2:31:e1:3a:75:58:f3:5f:fe:c2:38:4e:5f:df:
be:9b:ad:e5:a0:81:41:41:ff:45:90:3c:20:1c:5b: 35:0b:9e:8c:79:49:f6:da:c0:85:df:6f:b7:e3:2c:
e4:fc:2e:08:ff:97:f3:e0:10:ff:3f:79:92:c9:19: ee:96:46:2c:07:bc:b4:16:88:f3:0e:98:dd:4e:07:
e6:7c:34:9d:a9:71:5a:61:a3:ba:d5:d1:a1:0f:e9: e2:7d:45:71:36:6e:2d:57:ee:0b:1a:80:c3:e8:76:
29:ed:e2:25:94:0b:4f:9d:01:35:fa:b9:91:e4:1f: 00:17:54:46:d1:2d:62:a1:7c:a2:bd:e0:67:fc:43:
c0:55:e7:82:86:88:34:11:66:0b:85:1a:c5:c0:87: ce:eb:b8:47:6d:4b:24:cd:4a:ab:e1:90:5f:1f:89:
10:a1 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier:
5C:2D:62:32:41:0A:5C:EB:4C:CF:41:A9:FB:81:F9:C1:D9:05:03:3D X509v3 Authority Key Identifier:
keyid:5C:2D:62:32:41:0A:5C:EB:4C:CF:41:A9:FB:81:F9:C1:D9:05:03:3D X509v3 Basic Constraints:
critical CA:TRUE Signature Algorithm: sha256WithRSAEncryption
1c:a4:5d:2e:71:2d:3d:74:98:f4:0e:d1:39:7e:ae:bc:cf:fb:
6c:7a:19:e6:f5:1e:57:0a:93:91:03:4f:9d:02:fb:f9:b7:f4:
64:92:a2:aa:33:34:2d:5a:52:bc:7c:b6:b1:a0:59:d3:98:72:
dd:c6:d2:e5:8c:e0:8b:87:60:44:c8:2c:ad:20:3d:9f:83:b1:
53:e7:22:bc:85:64:fe:b3:11:90:fb:68:1f:ba:04:bd:1a:8f:
dd:02:5d:aa:42:9b:9c:7f:5e:95:63:5f:07:65:b9:0d:83:0c:
a4:f6:48:d4:74:fc:bc:93:9f:79:68:9b:30:d8:c0:e4:d2:d7:
```

42:aa:fb:43:ef:40:4a:17:9d:3a:6f:50:24:c1:52:74:15:07:
50:82:64:60:20:e1:ec:85:72:11:14:4e:bd:44:a2:74:92:db:
30:d2:32:98:a7:f3:c2:47:b4:f5:6c:60:6d:0e:50:87:75:c7:
a3:a4:5d:25:96:58:43:bb:2b:c4:6c:ea:f1:88:f4:b1:29:22:
0b:cd:03:64:b8:fb:65:cf:29:62:59:ec:b8:b8:33:09:58:cf:
f5:67:2e:f4:b4:7d:de:84:e3:05:84:b8:91:2c:a1:32:af:44:
fa:2d:3e:c3:01:72:c9:56:c9:f0:ce:5e:28:61:f1:79:56:68: 36:f3:bb:21