Fehler beim Lösen einer 516-Unstimmigkeit bei der CN des Upstream-Zertifikats

Inhalt

Einleitung

In diesem Dokument wird die Behebung eines Fehlers bei der CN für ein 516-Upstream-Zertifikat beschrieben.

Problem

Wenn der Umbrella Secure Web Gateway (SWG)-Proxy so konfiguriert ist, dass er HTTPS-Inspektionen durchführt, kann ein Benutzer eine Fehlerseite 516 Upstream Certificate CN Mismatch erhalten, wenn er mit einer HTTPS-URL zu einer Website navigiert.

Dieser Fehler weist nicht auf ein Problem mit dem Attribut "Common Name" (CN) im Feld "Subject" (Betreff) des Websitezertifikats hin. Stattdessen bezieht sich das Problem auf das DNS-Namensattribut in der SAN-Erweiterung (Subject Alternative Names) eines Zertifikats.

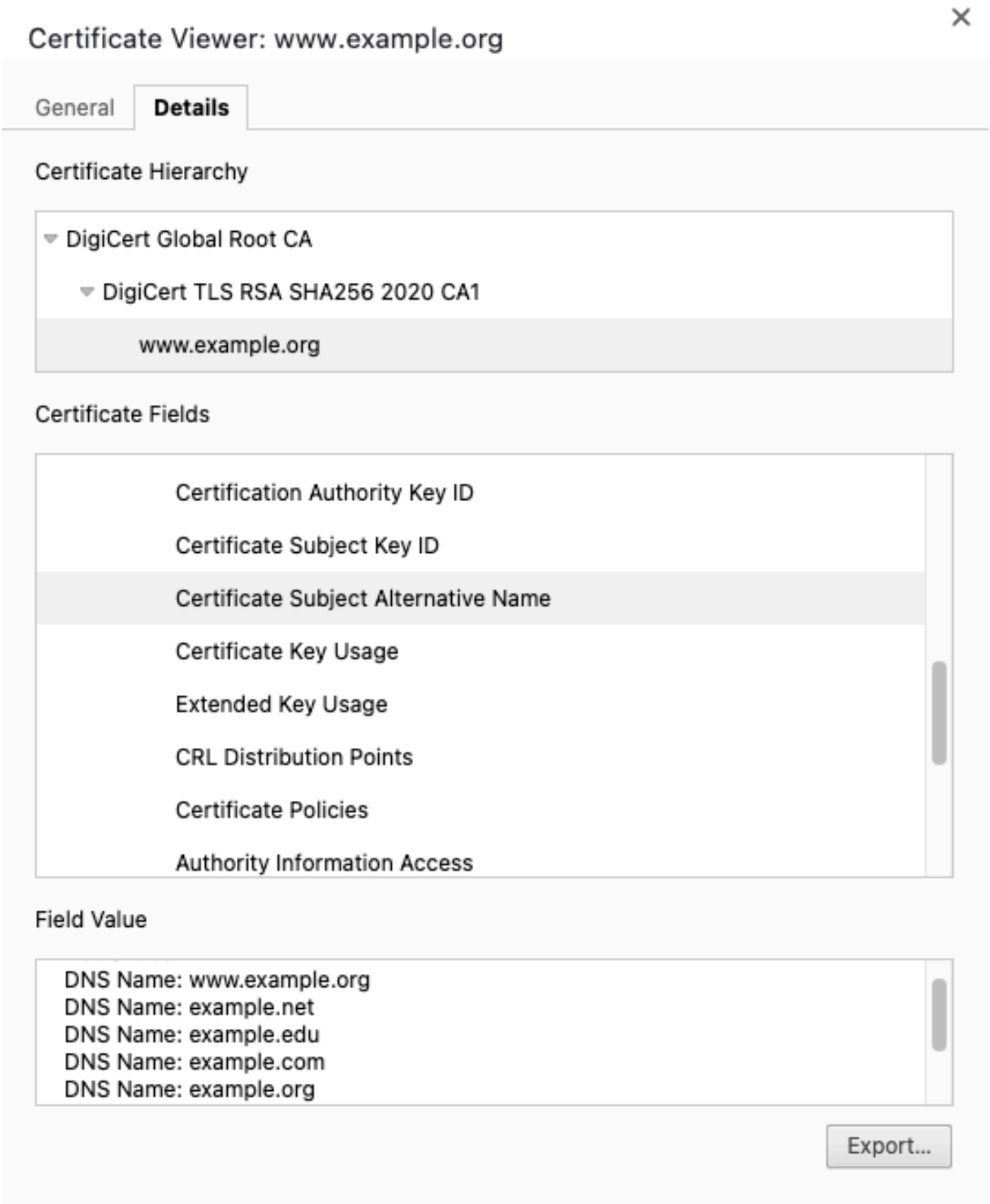
Wenn Sie nach der Durchsicht dieses Artikels den Grund für die 516-Fehlerseite nicht ermitteln können, wenden Sie sich an den technischen Support von Umbrella, und geben Sie die im Abschnitt Certificate Identity Errors (Fehler bei der Zertifikatsidentität) in diesem Dokument angegebenen Informationen an.

Mechanik der Zertifikatsidentität

Wenn eine HTTPS-URL angefordert wird, sendet ein Browser oder ein anderer Webclient den Domänennamen in der URL über die SNI-Erweiterung (Server Name Indication) in der Client Hello-Nachricht der TLS-Aushandlung an den Webserver. Der Server verwendet diesen SNI-Wert, um das Serverzertifikat auszuwählen, das an den Client zurückgegeben werden soll, da ein Server häufig mehrere Websites hostet und für einige oder alle Websites unterschiedliche Zertifikate besitzen kann.

Wenn das Serverzertifikat vom Web-Client empfangen wird, überprüft der Client, ob das Zertifikat

das richtige für die Anforderung ist, indem er den angeforderten Domänennamen mit den Domänennamen in den DNS-Namensattributen der Subject Alternative Names-Erweiterung des Zertifikats vergleicht. Dieses Image zeigt diese SANs in einem Serverzertifikat.



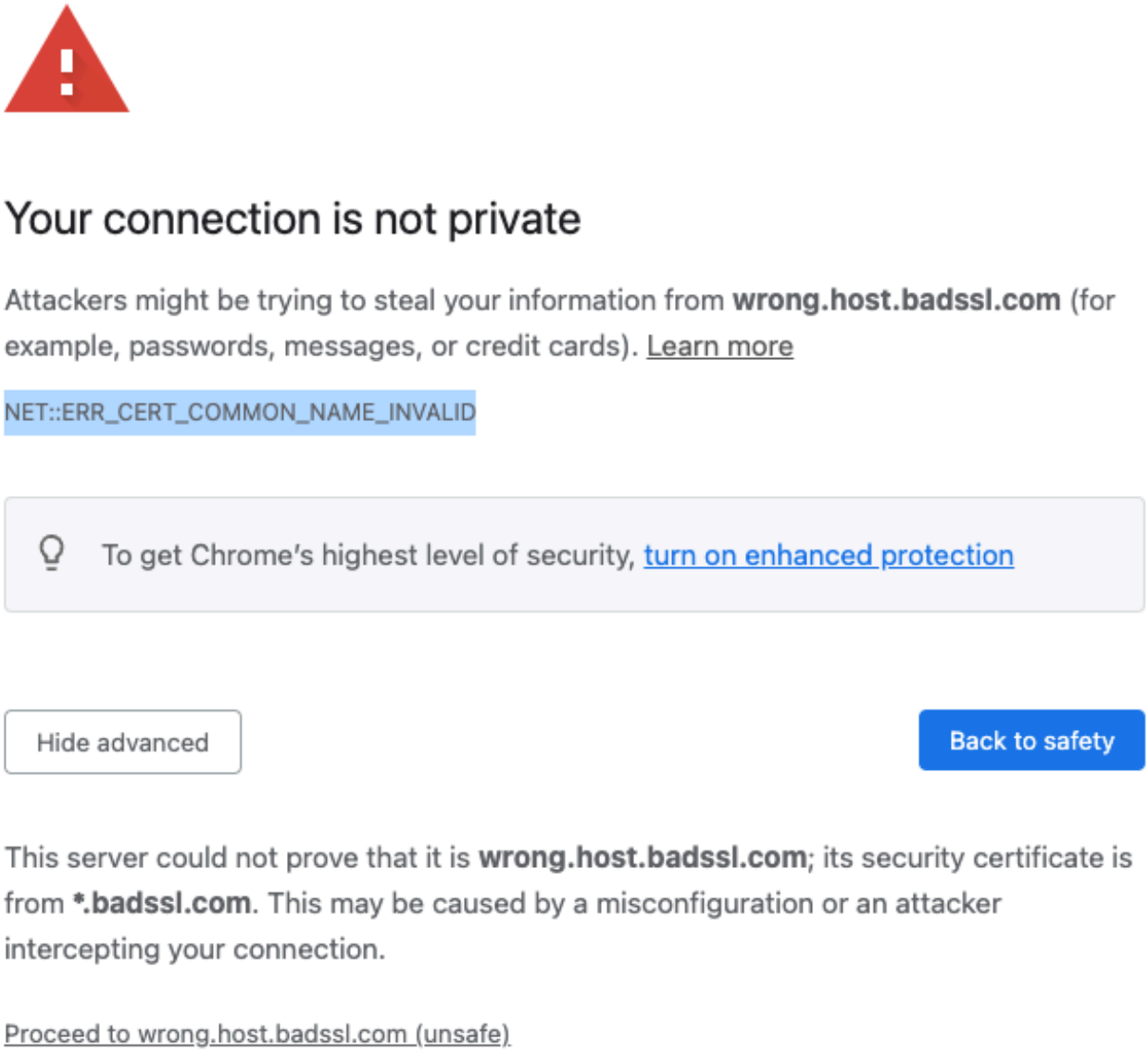
Dieser Webserver gibt dieses Zertifikat als Antwort auf Anforderungen mit diesen SNI-Werten sowie anderen Werten zurück, die nicht im Feld "Feldwert" angezeigt werden:

- www.example.org
- example.net
- example.edu
- example.com
- example.org

Beachten Sie, dass das SAN "example.com" nicht mit einem SNI von "www.example.com" übereinstimmt. Ein Platzhalter-SAN von "*.example.com" würde jedoch mit einem SNI von "www.example.com" oder einem anderen Domänennamen übereinstimmen, der ein einzelnes Label (eine Zeichenfolge ohne "") enthält. B. Zeichen) vor example.com, aber nicht mehrere Bezeichnungen. Beispiel: "www.hr.example.com" wird nicht von "*.example.com" abgeglichen, da "www.hr" aus zwei Labels besteht: "www" und "hr". Ein einzelner Platzhalter kann nur einem einzelnen Label entsprechen.

Fehler bei der Zertifikatsidentität

Wenn ein Web-Client ein Serverzertifikat empfängt und keiner der DNS-Namen des SAN mit dem SNI des Domänennamens in der angeforderten URL übereinstimmt, zeigt der Web-Client dem Benutzer in der Regel einen Fehler an. Dieses Bild zeigt, wie Chrome eine "NET::ERR_CERT_COMMON_NAME_INVALID"-Zwischenseite anzeigt.



16794294817428

Im Image lautete die angeforderte Site "https://wrong.host.badssl.com", die keinem der SANs entspricht. Das Zertifikat enthält einen SAN-DNS-Namen mit Platzhalter (*.badssl.com), dessen Platzhalter nur mit einem einzigen Label wie "host" übereinstimmen kann. Darüber hinaus enthält das Zertifikat keinen SAN-DNS-Namen mit dem genauen Wert "false.host.badssl.com" oder ein Platzhalter-SAN von "*.host.badssl.com", sodass der Benutzer mit diesem Fehler konfrontiert wird.

Um den Grund für eine nicht übereinstimmende Zertifikatsidentität zu ermitteln, überprüfen Sie die SAN-DNS-Namen des Zertifikats mithilfe der Zertifikatanzeigefunktion des Browsers, und vergleichen Sie sie mit dem Domänennamen in der angeforderten URL. Alternativ kann ein Tool wie der Qualys SSL-Servertest zur Diagnose eines Zertifikatidentitätsproblems verwendet werden.

Wenn der Grund für den 516-Fehler nach Verwendung der Informationen in diesem Abschnitt nicht ermittelt werden kann oder wenn die Lösungen und Problemumgehungen im nächsten

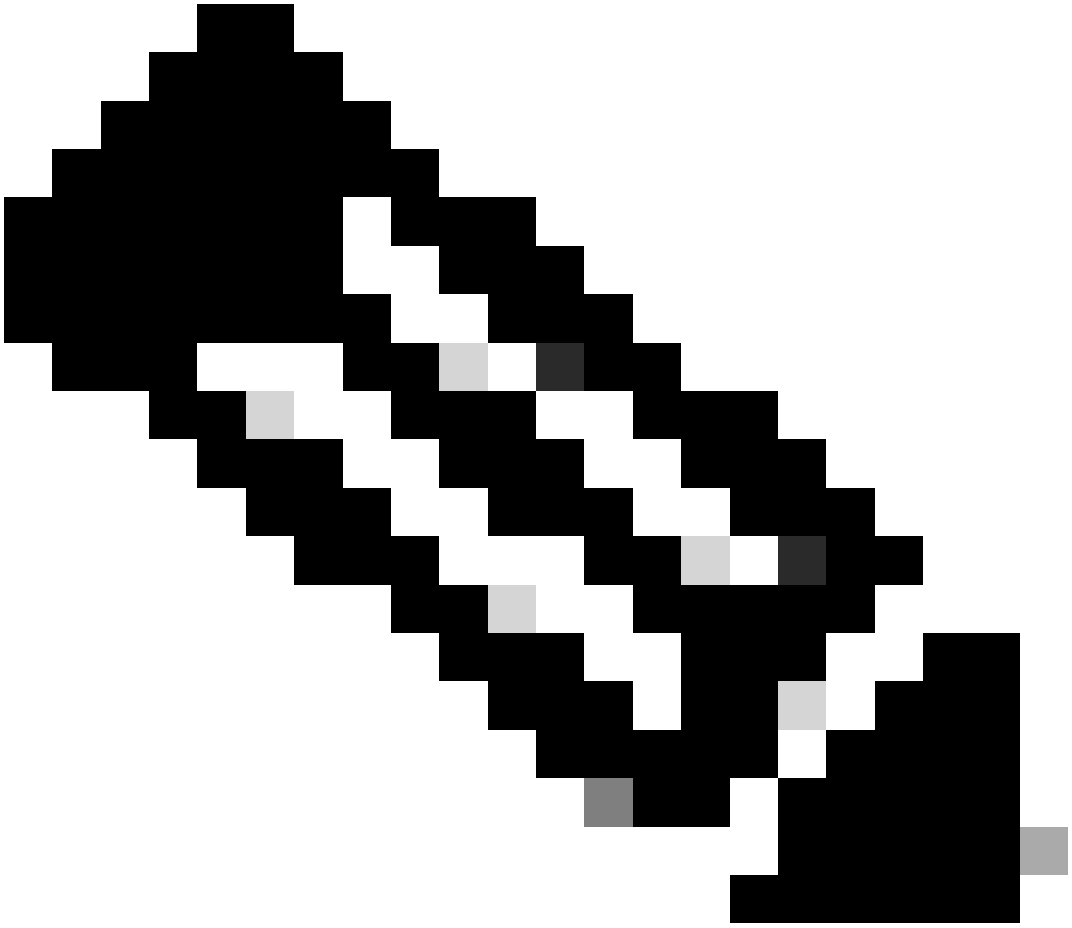
Abschnitt nicht angewendet werden können, öffnen Sie bitte ein Ticket beim technischen Support von Umbrella, und geben Sie Folgendes an:

1. ein Screenshot, der
    - die Adressleiste des Browsers, die die angeforderte URL anzeigt
    - die gesamte Fehlerseite zu 516 (siehe Abbildung im nächsten Abschnitt)
2. Der Text der URL, der aus der Adressleiste kopiert wird.

Auflösung

Um dieses Problem zu beheben, greifen Sie auf den Server mit einem Domänennamen zu, der mit einem der SAN-DNS-Namen im Zertifikat übereinstimmt. Dazu kann es erforderlich sein, dass der Administrator der Website dem DNS für die Zone einen passenden Domänennamen hinzufügt. Alternativ kann der Administrator das Zertifikat erneut ausstellen, um den Domänennamen der URL in einen der SAN-DNS-Namen aufzunehmen.

Als Problemumgehung kann der Domänenname der URL einer selektiven Entschlüsselungsliste für den Proxy des sicheren Webgateways oder einer Zielliste im intelligenten Proxy hinzugefügt werden. Wenden Sie die Liste auf die entsprechende Regelsatzeinstellung für die Webrichtlinie (sicheres Web-Gateway) oder die Zulassungsliste für die DNS-Richtlinie (intelligenter Proxy) an. Auf diese Weise wird verhindert, dass die Anfrage an die Website vom Proxy entschlüsselt wird, sodass der Proxy keine 516-Fehlerseite anzeigen kann.



Anmerkung: Die Verwendung des Secure Web Gateway-Proxys und des intelligenten Proxys wird nicht unterstützt. Pro Organisation kann nur eine Proxy-Technologie eingesetzt werden. Es wird empfohlen, dass Organisationen, die Abonnements für Secure Web Gateway haben, SWG verwenden und keinen Intelligent Proxy verwenden.

Common Name ist veraltet

Webclients haben ursprünglich den Domänennamen in der angeforderten URL dem Common Name (CN)-Attribut im Betreff-Feld des Zertifikats zugeordnet. Dieser Mechanismus ist in modernen Web-Clients veraltet. Domänen werden jetzt mit den DNS-Namen der Erweiterung Subject Alternative Name abgeglichen. Dennoch, Text von Fehlermeldungen oft weiterhin auf den veralteten Mechanismus, wie "NET::ERR_CERT_COMMON_NAME_INVALID" in Chrome.

Umbrella SWG zeigt eine 516-Fehlerseite mit diesem Text an, wenn der SWG-Proxy eine URL von einem Webserver anfordert und eine SAN-DNS-Namensungleichheit auftritt:

16794325789332

Cisco Umbrella plant, diesen Text zu einem späteren Zeitpunkt zu aktualisieren, um das aktuelle Verhalten besser widerzuspiegeln.

Zusätzliche Informationen

Siehe RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Abschnitt 4.1.2.6 für Informationen zum Zertifikatantragsteller und Abschnitt 4.2.1.6 für Informationen zum alternativen Antragstellernamen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.