Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

TLS-interceptie

Afwegingen en randvoorwaarden voor het inzetten van TLS-interceptie

Factsheet FS-2017-05 | versie 1.0 | 11 oktober 2017

TLS-interceptie maakt versleutelde verbindingen binnen het netwerk van een organisatie toegankelijk voor inspectie. Inzet van deze maatregel vergt vanwege bijkomende risico's een gedegen afweging en dient aan een aantal belangrijke randvoorwaarden te voldoen.

De reden voor het inzetten van TLS-interceptie is dat steeds meer internetdiensten en -verbindingen gebruik maken van versleuteling. Dit waarborgt de integriteit en vertrouwelijkheid van de verstuurde en ontvangen gegevens. Tegelijkertijd maakt dit het lastiger voor organisaties om het internetverkeer centraal in hun netwerk te inspecteren op kwaadaardige elementen en vertrouwelijke organisatiegegevens die via het internet de organisatie verlaten.

Achtergrond

Transport Layer Security-interceptie (TLS-interceptie) is het onderscheppen van versleutelde verbindingen om ze toegankelijk te maken voor inspectie.[1] Tussenstations die deze actie uitvoeren worden in deze factsheet als TLS-proxy aangeduid. TLS-interceptie kan ten aanzien van allerlei soorten TLS-verbindingen uitgevoerd worden, zoals HTTPS voor webverkeer en SMTP met STARTTLS voor e-mail. Organisaties passen TLS-interceptie meestal toe om binnen versleutelde verbindingen kwaadaardige elementen, zoals virussen en malware, en het weglekken van gegevens te detecteren en te blokkeren.[2]

Doelgroep

Chief Information Security Officers, privacy officers of functionarissen gegevensbescherming, informatiebeveiligers

Aan deze factsheet hebben bijgedragen

Autoriteit Persoonsgegevens, Belastingdienst, NBV, Achmea, Equens Worldline, Rabobank en De Volksbank N.V.

---

[1] Het gaat hierbij uiteraard alleen om onderschepping van versleutelde verbindingen die met behulp van het TLS-protocol tot stand zijn gebracht.
[2] Het voorkomen van weglekken van gegevens wordt ook wel Data Leakage Prevention (DLP) genoemd.

Het gebruik van versleutelde verbindingen, bijvoorbeeld met Transport Layer Security (TLS) of diens voorganger Secure Sockets Layer (SSL), neemt toe. Dit waarborgt de integriteit en vertrouwelijkheid van verstuurde en ontvangen gegevens van internetdiensten en geeft zekerheid over de identiteit van de server. TLS is daarmee een onmisbare maatregel om internetdiensten veilig aan te bieden, bijvoorbeeld webmail, internetbankieren en webshops. Een nadeel is dat versleutelde verbindingen opgezet door kwaadaardige software, zoals verbindingen tussen malware en een command-and-control-server[3], door de versleuteling niet langer kunnen worden ingezien. Dit bemoeilijkt detectie. Een bijkomende ontwikkeling is dat bonafide versleutelde diensten van bekende clouddiensten steeds vaker misbruikt worden voor malafide doeleinden, wat het uitsluitend blokkeren van (kwaadaardige) IP-adressen en URL's minder effectief maakt.[4]

TLS-proxy's kunnen (decentraal) op *endpoints* worden geïnstalleerd, zoals door sommige anti-virusscanners of firewalls wordt toegepast. Vaak worden ze echter op centrale plekken in een organisatienetwerk ingezet, zoals de verbinding met het internet. Alhoewel deze factsheet zich op de centraal ingerichte variant richt, gelden veel van de gesignaleerde risico's en aandachtspunten ook voor de decentrale varianten. TLS-proxy's die inkomend verkeer voor servers van de organisatie afhandelen (TLS-reverse-proxy's) vallen buiten scope van deze factsheet.

De belangrijkste feiten

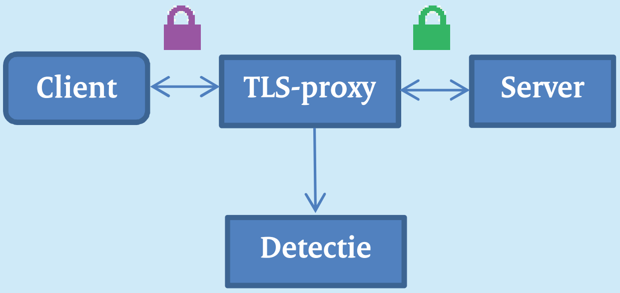
1. Bij TLS-interceptie positioneert een organisatie een TLS-proxy tussen de eigen clients en een server, om zo toegang tot de inhoud van de TLS-verbinding te krijgen.
2. Organisaties passen TLS-interceptie doorgaans toe op de verbinding met het internet om malware en het uitlekken van vertrouwelijke organisatiegegevens tegen te gaan.
3. Er is een aantal belangrijke randvoorwaarden voor het veilig en verantwoord implementeren van TLS-interceptie, waaronder een voorafgaande toetsing op privacyaspecten, een juiste configuratie en beveiliging van de proxy en het gecontroleerd uitrollen van certificaten.
4. TLS-interceptie dient niet afzonderlijk te worden ingevoerd, maar als integraal en afgewogen onderdeel van een bredere set van maatregelen ter implementatie van informatiebeveiligingsbeleid.

Hoe werkt TLS-interceptie?

TLS is een protocol voor het opzetten en gebruiken van een cryptografisch beveiligde verbinding tussen twee computersystemen, een client en een server. Hiermee wordt de vertrouwelijkheid en integriteit van de inhoud van de verbinding gewaarborgd en wordt de server geauthenticeerd, zodat de identiteit van de server niet vervalst kan worden.

In het geval van TLS-interceptie onderschept de TLS-proxy de aanvraag van de client om een versleutelde verbinding met de server te starten en doet de TLS-proxy zich voor als de betreffende server. Normaliter zal een client dit niet accepteren, want de identiteit van de server zal niet geauthenticeerd kunnen worden. Om de client de TLS-proxy toch te laten vertrouwen dient op de client het stamcertificaat (root CA) van de TLS-proxy geïnstalleerd te worden. De client vertrouwt vervolgens alle daarmee ondertekende certificaten. Voor elke server en bijhorende domeinnaam waar een client verbinding mee wil maken, maakt de TLS-proxy vervolgens een certificaat aan waarvan de naam overeenkomt met het opgevraagde domein en dat ondertekend wordt met het stamcertificaat (root CA) van de TLS-proxy.

De client accepteert zo het door de TLS-proxy ondertekende servercertificaat en zet een versleutelde verbinding op met de TLS-proxy. De TLS-proxy zet vervolgens een versleutelde verbinding op met de server en gaat het verkeer tussen de client en de server doorsturen. Doordat de TLS-proxy nu tussen de twee versleutelde verbindingen in zit, kan deze alle verkeer inzien en doorgeven aan het detectiesysteem.



Inzage gebeurt overigens uitsluitend op transportniveau. Indien een applicatie, bijvoorbeeld malware, op applicatieniveau ook nog afzonderlijk versleuteling toepast zal de TLS-proxy deze doorgaans niet ongedaan maken.

Wat zijn de risico's?

Informatiebeveiligingsrisico's

TLS-proxy's nemen de rol van het opzetten van veilige verbindingen met servers van clients over. Immers, in plaats van het systeem van de eindgebruiker gaat de de TLS-proxy een beveiligde verbinding met een server op het internet opzetten. De TLS-proxy zal daarom alle controles en waarborgen ten

---

[3] Computers die worden gebruikt voor de aansturing van een botnet.
[4] Cybersecuritybeeld Nederland 2016, p. 44, zie https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2016.html

aanzien van de authenticatie van de server, evenals de vertrouwelijkheid, integriteit en authenticatie van de verzonden en ontvangen gegevens, voor zijn rekening moeten nemen. De clientsoftware kan vervolgens voor deze aspecten alleen maar op de TLS-proxy vertrouwen, zonder dit zelf te kunnen verifiëren. Moderne browsers zijn vanwege het grote aantal dreigingen steeds strenger in het controleren van al deze aspecten, waarbij veel verschillende beveiligingsmechanismen worden gebruikt. Om hetzelfde beveiligingsniveau te handhaven moet de TLS-proxy de juiste controles uitvoeren. Tekortkomingen hierin kunnen ertoe leiden dat verbindingen van gebruikers en systemen van de organisatie worden gemanipuleerd of afgeluisterd.

TLS-interceptie kan ertoe leiden dat applicaties niet langer een verbinding met hun server kunnen maken, omdat zij alleen het specifieke certificaat van die server vertrouwen en niet een alternatief certificaat van de TLS-proxy. Deze maatregel wordt ook wel *certificate pinning* genoemd.[5] Ook authenticatie van de client met behulp van een clientcertificaat op de *endpoint* kan door TLS-interceptie bemoeilijkt of onmogelijk gemaakt worden. Wanneer applicaties encryptiealgoritmes of protocollen gebruiken die de TLS-proxy niet ondersteunt, kan dit tot verbindingsproblemen leiden. Dit is vooral een risico voor legacy-applicaties, maar het kan zich ook voordoen bij de introductie van nieuwe applicaties die gebruikmaken van nieuwe encryptiealgoritmes of protocollen.[6] Tevens zorgt TLS-interceptie ervoor dat clients niet langer kunnen zien dat een bepaalde website een *Extended Validation*-certificaat gebruikt.[7]

Ten slotte is er het risico dat de TLS-proxy gehackt wordt, aangezien het een zeer aantrekkelijk doelwit is. Als een aanvaller erin slaagt de TLS-proxy te compromitteren, krijgt hij toegang tot alle gegevens die er door stromen. Deze zijn in de TLS-proxy onversleuteld en kunnen daarom door de aanvaller ingezien en gewijzigd worden. Denk bijvoorbeeld aan vertrouwelijke gegevens als wachtwoorden en financiële gegevens. Ook kan de aanvaller met een buitgemaakt stamcertificaat van de TLS-proxy man-in-the-middle-aanvallen uitvoeren op clients die het certificaat vertrouwen.

Privacyrisico's

Voorafgaand aan het inzetten van TLS-interceptie door de organisatie is een toets op het voldoen aan de wettelijke vereisten met betrekking tot in elk geval de verwerking van persoonsgegevens aangewezen, gezien de mogelijke privacy-inbreuken.[8] Op de website van de Autoriteit Persoonsgegevens is meer informatie te vinden over het juridische kader met betrekking tot de verwerking van persoonsgegevens.[9] [10] [11]

Wat adviseert het NCSC?

Indien u mede op basis van de toets, genoemd in de vorige alinea, tot de conclusie komt dat het inzetten van een TLS-proxy mogelijk en ook opportuun is, dient u de technische vereisten voor de TLS-proxy helder te krijgen. Een belangrijk aspect is dat de TLS-proxy adequaat beveiligde verbindingen met de client en de server opzet. Deze factsheet sluit aan bij de NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (NCSC TLS-richtlijnen) voor de beschrijving van de beveiligingseigenschappen van veilige verbindingen.[12] De definities en uitwerking van **voldoende** en **goede** instellingen zijn te vinden in de NCSC TLS-richtlijnen.

In tabellen 1 en 2, aan het eind van deze factsheet, staan een aantal technische basisvereisten en *best practices* om de TLS-proxy aan te toetsen ten aanzien van het opzetten van veilige verbindingen. In tabel 1 ten aanzien van servers en in tabel 2 ten aanzien van clients. Basisvereisten zijn naar de huidige stand van de techniek de minimale vereisten waar een TLS-proxy aan zou moeten voldoen voor het opzetten van veilige verbindingen. De best practies geven een handreiking om gebruik te maken van recente en aanvullende beveiligingsmaatregelen. Uit internationaal onderzoek blijkt dat TLS-proxy's niet zonder meer aan de basisvereisten voldoen.[13] [14] Het is dan ook belangrijk om hierover zekerheid te krijgen, alvorens voor een product te kiezen.

---

[5] Veel mobiele apps, bijvoorbeeld voor internetbankieren, maken hier gebruik van.

[6] Een voorbeeld is het gebruik van TLS 1.3, dat nog niet door alle TLS-proxy's wordt ondersteund. Zie hierover: https://www.security.nl/posting/505600/Google+stopt+TLS-update+Chrome+56+wegens+problemen

[7] De populaire browsers zoals Firefox en Chrome ondersteunen alleen EV-certificaten van specifieke Certificate Authorities. De TLS-proxy kan deze niet zelf uitgeven, waardoor er geen EV-certificaat aan de client aangeboden kan worden.

[8] Voorts is het aangewezen van tevoren te bezien of ook overigens in juridische zin al dan niet sprake is van belemmeringen voor zover het gaat om het inzetten van TLS-interceptie.

[9] Het adres van de website is: https://www.autoriteitpersoonsgegevens.nl.

[10] Zie in het kader van de aankomende Algemene Verordening Gegevensbescherming: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving.

[11] Zie voor privacy in context van werkgever-werknemer: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/opinie-europese-privacytoezichthouders-over-privacyrechten-werknemers

[12] De TLS-richtlijnen zijn te vinden op: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

[13] Zakir Durumeric et al, 'The security impact of HTTPS interception', https://zakird.com/papers/https_interception.pdf

[14] Zie ook de waarschuwing van US-CERT: https://www.us-cert.gov/ncas/alerts/TA17-075A

Uitzonderingen op basis van risicomanagement

Maak als organisatie expliciete keuzes over hoe uw organisatie omgaat met het opzetten van verbindingen die naar de huidige maatstaven en volgens deze factsheet onvoldoende veilig zijn.[15] De TLS-proxy bepaalt immers de certificaatverificatie en de sterkte van de versleutelde verbinding voor alle TLS-verbindingen die door de proxy worden onderschept. In het algemeen kunt u het beste de NCSC TLS-richtlijnen en het voorbeeld van de moderne browsers volgen en op gelijk tempo onveilige verbindingsopties uitfaseren. Op basis van een risicoanalyse kan uw organisatie hierop een uitzondering maken, door een afweging te maken over de gewenste mate van compatibiliteit versus het risico voor gebruikers en de organisatie. Beperk waar mogelijk uitzonderingen tot specifieke servers of domeinnamen.

Denk tevens na over de zeggenschap en mogelijkheden die een inviduele gebruiker zou moeten hebben bij het al dan niet opzetten van een onveilige verbinding. Krijgt de gebruiker bijvoorbeeld een melding en kan deze doorklikken en zo de verbinding alsnog opzetten, of wordt er uitsluitend een melding gegeven dat de verbinding vanwege het beveiligingsbeleid niet tot stand kon worden gebracht. Meer zeggenschap voor individuele gebruikers kan het aantal hulpverzoeken van werknemers over niet werkende verbindingen verlagen, maar tegelijkertijd de risico's voor de organisatie vergroten. Terugkoppeling van foutmeldingen aan gebruikers is een aandachtspunt. Als een gebruiker via een webbrowser een TLS-verbinding opzet, kan via de webbrowser de nodige informatie aan de gebruiker verstrekt worden. Die mogelijkheid is er echter vaak niet voor mobiele apps.

Ten slotte kunt u op basis van risicomanagement besluiten om delen van het organisatienetwerk uit te zonderen van TLS-interceptie. Denk bijvoorbeeld aan het inrichten van een afgescheiden en geïsoleerd netwerksegment zonder TLS-interceptie voor privé-apparaten van werknemers.[16] Daarnaast kunnen bijvoorbeeld ook vertrouwde bestemmingen uitgezonderd worden op basis van bijvoorbeeld een domeinnaam of IP-adres, of categorieën van websites.[17]

Forward secrecy en out-of-band detectieoplossingen

De TLS-proxy en de client wisselen onderling sessiesleutels uit voor de versleuteling van de te versturen gegevens (bulkversleuteling). De sleuteluitwisseling kan op twee manieren plaatsvinden, een klassieke en een moderne. Op de klassieke manier genereert de client de sessiesleutel en versleutelt deze vervolgens met de publieke sleutel van de TLS-proxy. De TLS-proxy kan deze met zijn geheime sleutel ontsleutelen en gebruiken voor de bulkversleuteling. Sleuteluitwisseling met RSA vindt op deze wijze plaats. Met de geheime sleutel van de TLS-proxy kan op een later moment opgeslagen netwerkverkeer (inclusief sleuteluitwisseling) ontsleuteld worden. De moderne manier is het vastellen van de sessiesleutel volgens het Diffie-Hellman-protocol (DHE en ECDHE), waarbij de sessiesleutel door TLS-proxy en client wordt afgesproken maar deze nooit over het netwerk wordt verstuurd. Opgeslagen netwerkverkeer bevat daarom niet de sessiesleutels, die daardoor ook niet achteraf met de geheime sleutel van de TLS-proxy ontsleuteld kunnen worden (*forward secrecy*). Voor de combinatie van TLS-proxy en een out-of-band[18] detectieoplossing is dit een belangrijk verschil. In het geval van een verstuurde sessiesleutel kan de detectieoplossing met behulp van de geheime sleutel van de TLS-proxy het versleutelde verkeer ontsleutelen en inspecteren. Bij het gebruik van *forward secrecy* zal de TLS-proxy echter de detectieoplossing de individuele sessiesleutels of de volledige onversleutelde gegevensstroom moeten aanbieden om het verkeer te kunnen inspecteren.[19] Vanuit oogpunt van verbindingsbeveiliging heeft het gebruik van forward secrecy de voorkeur.

Waarborgen beveiliging TLS-proxy

Een TLS-proxy is een waardevol doelwit en moet in de meeste gevallen als 'kroonjuweel' van uw organisatie worden gezien. De TLS-proxy is immers in staat om het versleutelde TLS-verkeer dat door de proxy wordt geleid te ontsleutelen en zo bij de oorspronkelijke gegevens te komen. Wanneer een aanvaller erin slaagt om de TLS-proxy of de privésleutel van het stamcertificaat te compromitteren, kan deze kennisnemen van deze gegevensstromen en bovendien informatie wijzigen. Het is daarom belangrijk om de TLS-proxy zelf adequaat te beschermen. Dit betekent dat de TLS-proxy in het algemeen geen inkomende verbindingen vanaf het internet accepteert, de *management interface* van de TLS-proxy afgeschermd dient te zijn en omliggende firewalls en toegangsrechten restrictief zijn ingesteld. Daarnaast kan de TLS-proxy in een apart

---

[15] Denk aan publieke sleutels van onvoldoende lengte of een hashfunctie voor ondertekening van de fingerprint van het certificaat van onvoldoende sterkte.

[16] Denk aan een van bedrijfssystemen afgescheiden wifinetwerk waar werknemers voor privédoeleinden gebruik van mogen maken.

[17] Dit wordt ook wel *whitelisting* genoemd.

[18] De detectieoplossing zit in dat geval niet in de TLS-proxy ingebouwd.

[19] In TLS versie 1.3 wordt waarschijnlijk uitsluitend nog sleuteluitwisseling met *forward secrecy* ondersteund. https://www.ietf.org/mail-archive/web/tls/current/msg21278.html

netwerksegment geplaatst worden en gemonitord worden door een *intrusion detection* of *prevention system* en Security Information & Event Monitoring (SIEM). Tevens dient de verbinding met de *management interface* over een versleutelde verbinding te verlopen. Gebruik een uniek certificaat en geheime sleutel voor deze verbinding.[20] Sla daarnaast niet onnodig onderschept dataverkeer op. Houd ten slotte de software van de TLS-proxy voortdurend up-to-date, om zo kwetsbaarheden te verhelpen. Denk hierbij ook aan de cryptobibliotheken van de TLS-proxy, zoals OpenSSL of mbed TLS, die voorzien dienen te zijn van de laatste beveiligingsupdates. Zorg dat u hiervoor een ondersteuningscontract bij uw leverancier afsluit en begroot deze kosten voor de toekomst in, zodat u later niet met onvoorziene kosten wordt geconfronteerd.

Implementatie en integratie van TLS-proxy

Een TLS-proxy en bijhorende detectieoplossing zal het meeste nut opleveren wanneer deze goed geïntegreerd wordt binnen andere beveiligingsmaatregelen, zoals een Security Information & Event Monitoring (SIEM). Meer achtergrondinformatie daarover is te vinden in de Handreiking voor implementatie van detectie-oplossingen van het NCSC en de AIVD.[21] Het is daarnaast het overwegen waard om voor de detectieoplossing die gekoppeld is aan de TLS-proxy *signatures* van een andere leverancier te gebruiken dan die worden gebruikt voor de endpointsecurity, zoals lokale virusscanners. Zo worden eventuele lacunes in de signaturebestanden zoveel mogelijk ondervangen. Ten slotte dient de TLS-proxy over voldoende doorvoercapaciteit te beschikken om de verkeersstromen te verwerken. De benodigde capaciteit kan vastgesteld worden aan de hand van de maximale verbindingssnelheid van de internetverbinding of aan de hand van historische gegevens over het gebruik van de internetverbinding. Vanuit perspectief van toekomstvastheid is het aan te raden om daarbij enige marge aan te houden, want internetverbindingen worden steeds sneller, de hoeveelheid verkeer neemt toe en steeds meer internetdiensten maken gebruik van TLS.[22] Zorg in het geval van daadwerkelijke implementatie de eerste weken voor voldoende ondersteuning om onverwachte storingen op te kunnen lossen.

Handelingsperspectief

- Voer voorafgaand aan de inzet van TLS-interceptie een toets uit op het voldoen aan de wettelijke vereisten met betrekking tot in elk geval de verwerking van persoonsgegevens.
- Zet TLS-interceptie selectief en niet onnodig in.
- Toets de TLS-proxy aan de genoemde informatiebeveiligingseisen en configureer deze conform dit advies.
- Verifieer bij de leverancier van de TLS-proxy dat deze binnen korte tijd updates ter beschikking stelt wanneer er kwetsbaarheden in de TLS-proxy bekend zijn geworden.
- Bescherm de TLS-proxy zelf tegen aanvallen.
- Integreer de TLS-proxy binnen de bredere set van andere beveiligingsmaatregelen.
- Zorg voor voldoende capaciteit om onverwachte problemen die na implementatie optreden op te kunnen lossen.

Tot slot

TLS-interceptie kan enerzijds de informatiebeveiliging van een organisatie verbeteren door detectie mogelijk te maken van kwaadaardige elementen of vertrouwelijke organisatiegegevens die worden verstuurd via TLS-verbindingen. Anderzijds brengt het ook risico's voor informatiebeveiliging en privacy met zich mee. Het is aan te raden om TLS-interceptie niet als laaghangend fruit te zien, maar als een maatregel die het bredere palet van al genomen beveiligingsmaatregelen kan aanvullen. Maak een gedegen afweging over nut en noodzaak in de context van andere beveiligingsmaatregelen en zet TLS-interceptie selectief in. Voer van tevoren een toets uit op het voldoen aan de wettelijke vereisten met betrekking tot in elk geval de verwerking van persoonsgegevens. Investeer voldoende in het goed in kaart brengen en vervullen van randvoorwaarden op onder meer informatiebeveiligingstechnisch vlak.

---

[20] Het risico bestaat namelijk dat andere exemplaren van de TLS-proxy eenzelfde certificaat en geheime sleutel gebruiken. Een aanvaller kan het certificaat en de geheime sleutel dan extraheren uit dat andere exemplaar en deze vervolgens misbruiken om verbindingen met de *management interface* van uw TLS-proxy te onderscheppen.

[21] De handreiking is te vinden op: https://www.ncsc.nl/actueel/whitepapers/handreiking-voor-implementatie-van-detectie-oplossingen.html

[22] Zie voor statistieken: https://www.google.com/transparencyreport/https/metrics/?hl=en

Tabel 1 Technische vereisten aan TLS-proxy's voor het opzetten van veilige verbindingen met servers

Basisvereisten

- De TLS-proxy geeft bij het opzetten van verbindingen de voorkeur aan de nieuwste versie van TLS.[23]
- De TLS-proxy geeft de voorkeur aan het gebruik van *forward secrecy* bij het opzetten van versleutelde verbindingen.
- De TLS-proxy ondersteunt ciphersuites van **goede** of **voldoende** sterkte en volgt de voorkeur van de server bij het opzetten van een verbinding.
- TLS-renegotiation en TLS-compressie zijn conform de NCSC TLS-richtlijnen geconfigureerd.
- De TLS-proxy valideert servercertificaten in ieder geval ten aanzien van[24]:
    a. de geldigheid van het servercertificaat voor het aangeroepen domein (Subject Alternative Name en Common Name);[25]
    b. de geldigheidsduur van het servercertificaat;
    c. de status van het servercertificaat op basis van CRL of OCSP;[26]
    d. de geldigheid van de certificaatketen, waarbij het servercertificaat ondertekend is met een vertrouwd stamcertificaat (root CA) of tussencertificaat (intermediate CA);
    e. de beperkingen van certificaten, zoals aangegeven in de attributen. Voorbeelden zijn of het certificaat als servercertificaat gebruikt mag worden of dat de lengte van de keten van certificaten niet groter is dan één van de stam- of tussencertificaten toelaat;[27]
    f. de sterkte van de hashfunctie die gebruikt is voor het ondertekenen van de fingerprint, die van **goede** sterkte dient te zijn.[28]
- De publieke sleutel (RSA of ECDSA) van het certificaat, dient van **voldoende** of **goede** lengte te zijn.

Met een website als badssl.com kunt u in de praktijk testen of de TLS-proxy daadwerkelijk de nodige validaties uitvoert en welke ciphersuites worden ondersteund.

Best practices

- HTTP Strict Transport Security (HSTS) headers worden gerespecteerd en doorgestuurd naar de client.
- De TLS-proxy ondersteunt in hetzelfde tempo als moderne browsers de nieuwste certificaatcontroletechnieken:
    a. certificaatcontrole met behulp van HTTP Public Key Pinning (HPKP);[29]
    b. certificaatcontrole met behulp van DANE en TLSA.[30]
- De standaard vertrouwenslijst van de TLS-proxy voor stam- en tussencertificaten komt overeen met die van moderne webbrowsers, zoals Mozilla Firefox. De lijst wordt geregeld bijgewerkt.[31]

---

[23] Op het moment van schrijven van deze factsheet betreft dat TLS versie 1.2.

[24] Het servercertificaat is het certificaat van de server waar de TLS-proxy verbinding mee maakt, bijvoorbeeld van een website. De TLS-proxy dient bij validatiefouten de verbinding met de server te verbreken en het verzoek van de client naar de server niet meer door te sturen.

[25] Zie RFC 2818. Als een Subject Alternative Name bestaat moet deze worden gebruikt voor de validatie. Alleen als deze niet bestaat wordt de Common Name voor validatie gebruikt.

[26] Certificate Revocation List (CRL) en Online Certificate Status Protocol (OCSP) maken het mogelijk om te controleren of een certificaat ingetrokken is.

[27] Dit betreft controle op attributen van het certificaat conform RFC 5280 van de X.509 specificaties, zoals de *basic constraints*. Hiermee wordt aangegeven binnen welke grenzen een certificaat gebruikt mag worden. Denk aan waarvoor een certificaat gebruikt mag worden zoals servercertificaat, het ondertekenen van software, e-mailen, het tekenen als CA etc. Denk tevens aan de maximale lengte van de keten van certificaten.

[28] Moderne browser faseren ondersteuning voor het inmiddels als onveilig beschouwde SHA-1 voor certificaatondertekening uit. Het is aan te raden om daarbij aan te sluiten.

[29] De TLS-proxy zal HPKP alleen richting de internetserver kunnen ondersteunen. Met TLS-interceptie is HPKP-controle door de client niet meer mogelijk. Afhankelijk van de clientsoftware zal de HPKP-header door de TLS-proxy verwijderd moeten worden.

[30] Dit vereist dat de TLS-proxy ook DNSSEC ondersteunt en valideert.

[31] Zie voor deze lijst: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/

Tabel 2 Technische vereisten aan TLS-proxy voor het opzetten van veilige verbindingen met clients

Basisvereisten

- Indien de verbinding tussen TLS-proxy en server via TLS verloopt, dient ook de verbinding tussen TLS-proxy en client via TLS te verlopen.
- Gebruik geen standaard stamcertificaat (root CA) dat met de TLS-proxy meegeleverd wordt, want de bijhorende geheime sleutel is door derden makkelijk te achterhalen. Hiermee kunnen ze een man-in-the-middle-aanval uitvoeren op iedere client die het certificaat vertrouwt. Genereer daarom een nieuwe unieke privésleutel en certificaat. Sla de privésleutel veilig op.[32] Gebruik de privésleutel niet voor andere proxy's.
- Gebruik voor interceptie geen tussencertificaat van een leverancier die standaard door browsers wordt vertrouwd.[33]
- Zorg voor een zorgvuldig proces voor het installeren van het stamcertificaat (root CA) op de clients, zodat deze de TLS-proxy vertrouwen. Dit voorkomt dat gebruikers gewend raken aan het wegklikken van certificaatfouten om verbinding te kunnen maken, met alle risico's van dien.
- Persoonsgebonden clientcertificaten voor uitgaande verbindingen, geïnstalleerd op de TLS-proxy, kunnen alleen door geautoriseerde gebruikers worden gebruikt.
- De TLS-proxy ondersteunt en geeft bij het opzetten van verbindingen met clients de voorkeur aan cryptografische algoritmes van **goede** danwel **voldoende** sterkte voor:
    a. Certificaatverificatie
    b. Sleuteluitwisseling
    c. Bulkversleuteling, inclusief operatiemodus
    d. Hashing
- De publieke sleutel (RSA of ECDSA) van het certificaat is van **voldoende** of **goede** lengte.
- De hashfunctie die gebruikt is voor het ondertekenen van de fingerprint van het certificaat is van **goede** sterkte.[34]
- Het certificaat dat wordt gebruikt voor de interceptie is voorzien van de Subject Alternative Names uit het oorspronkelijke certificaat van de internetserver.
- TLS-renegotiation en TLS-compressie zijn conform de NCSC TLS-richtlijnen geconfigureerd.

Best practices

- Het certificaat dat wordt gebruikt voor de interceptie is voorzien van de organisatiedetails uit het originele certificaat van de internetserver.
- Maak voor de uitrol van het stamcertifaat op de clients gebruik van een al binnen de organisatie aanwezige PKI-omgeving.
- De TLS-proxy geeft de voorkeur aan het gebruik van *forward secrecy* bij het opzetten van versleutelde verbindingen met de client.

---

[32] Hiervoor kan bijvoorbeeld een Hardware Security Module (HSM) ingezet worden.

[33] Het gebruik van deze ongelimiteerde, voor elk domein bruikbare, tussencertificaten is niet toegestaan volgens de CA/B Forum Baseline Requirements. Als een dergelijk certificaat immers buiten uw interne netwerk komt, vormt dit een risico voor de informatiebeveiliging van andere organisaties en gebruikers. Er bestaat daarmee een grote kans dat browserfabrikanten dit betreffende tussencertificaat gaan blokkeren, waardoor de TLS-proxy onverwacht niet meer zal werken.

[34] Moderne browser faseren ondersteuning voor het inmiddels als onveilig beschouwde SHA-1 voor certificaatondertekening uit. Het is aan te raden om daarbij aan te sluiten.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2017-05 | versie 1.0 | 11 oktober 2017