

Begrijp Public Key Pinning en Certificaat Pinning in Paraplu

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[Compatibiliteit met Umbrella SWG](#)

[Andere toepassingen voor certificaatvastlegging](#)

Inleiding

Dit document beschrijft het pinnen van certificaten en het pinnen van publieke sleutels in Cisco Umbrella.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Certificaatpinning is een internetbeveiligingsmechanisme waarmee toepassingen zich kunnen verzetten tegen nabootsing van HTTPS-servers met behulp van verkeerd uitgegeven of anderszins frauduleuze digitale certificaten. Dit wordt gedaan door een server te koppelen aan een gedefinieerde set openbare sleutels, die de enige kunnen zijn die vertrouwd zijn voor verbindingen met die server. Er zijn twee technieken voor certificaatpinning:

- Public Key Pinning (PKP RFC7469) is een verouderd mechanisme voor het activeren van

certificaatpinning in webbrowsers. Vastgezette certificaten worden naar de browser verzonden met behulp van HTTP-headers.

- Statische certificaatvastlegging is wanneer een toepassing is gecodeerd om specifieke certificaten of certificaatautoriteiten te verwachten. Sommige desktop/mobiele applicaties gebruiken een statisch certificaat pinning mechanisme voor extra beveiliging.

Wanneer deze webapplicaties door Umbrella worden benaderd, komt de publieke sleutel die door Umbrella wordt verstrekt niet overeen met de sleutel die ervoor zorgt dat de applicatie de HTTPS-verbinding sluit. Certificaatpinning is meestal alleen van toepassing op desktop / mobiele applicaties omdat PKP-ondersteuning is verwijderd door moderne webbrowsers.

Compatibiliteit met Umbrella SWG

Umbrella omzeilt bekende URL's van SSL-decryptie om problemen met het vastzetten van certificaten in bepaalde omstandigheden op te lossen. Tabel 1 bevat toepassingen die wereldwijd zijn omzeild voor alle Umbrella-klanten. Tabel 1 bevat ook andere toepassingen waarvan bekend was dat ze op het moment van schrijven of schrijven gebruik maakten van certificaatpinning. Als u een van deze toepassingen gebruikt, kunt u overwegen om de methoden die later worden beschreven, om de opgegeven redenen, te gebruiken om de toepassing te omzeilen van HTTPS-inspectie. Tabel 2 bevat meer details voor de toepassingsservices die in tabel 1 worden behandeld.

Andere toepassingen voor certificaatvastlegging

Toepassingen kunnen worden omzeild op een per-klant (per-policy) basis om problemen met het vastzetten van certificaten op te lossen met behulp van Umbrella's [Selective Decryption](#)-functie. Deze uitzonderingen kunnen eenvoudig worden geïmplementeerd op basis van domein, applicatiennaam of categorie; Umbrella SWG bevat een grote bibliotheek met applicaties in onze app-database.

In de meeste gevallen ligt de beslissing of de toepassing moet worden omzeild bij de IT-beheerder. Het toevoegen van een decryptie uitzondering is een security trade-off omdat het voorkomt dat de veiligheid / file inspectie van de inhoud van het web. Dit is een individuele beslissing, afhankelijk van het type toepassing en de zakelijke behoefte. Als het probleem met het vastzetten van certificaten bijvoorbeeld alleen van invloed is op een mobiele/desktoptoepassing, kan de beheerder ervoor kiezen een uitzondering toe te voegen om de mobiele toepassing te laten werken of kan hij in plaats daarvan gebruikers vragen om de webversie van de toepassing te gebruiken.

Dit is een tabel met toepassingen die wereldwijd worden omzeild voor Umbrella-klanten en er is geen actie vereist of bekend om certificaatpinning te gebruiken op het moment van schrijven en niet standaard door Umbrella worden omzeild. Als u de toepassingen gebruikt die niet standaard worden omzeild, kunt u overwegen om de hierboven beschreven methoden te gebruiken om de toepassing te omzeilen van HTTPS-inspectie.

Tabel 1 - Toepassingen die certificaatvastpinnen kunnen gebruiken

Naam van toepassing	Cisco Umbrella Coverage
Adobe Services	Wereldwijd omzeild voor paraplu-kanten
Airbnb	Ondersteund door Application Control
Amazon Alexa	Ondersteund door Application Control
Amazon Drive	Ondersteund door Application Control
Amazon Kindle	Ondersteund door Application Control
Amazon Workspaces	Ondersteund door Application Control
amplitude	Wereldwijd omzeild voor paraplu-kanten
App Dynamics	Wereldwijd omzeild voor paraplu-kanten
Apple iMessage	Ondersteund door Application Control
Apple Mail	Ondersteund door Application Control
Apple Services (zie tabel 2 voor meer informatie)	Wereldwijd omzeild voor paraplu-kanten
Cisco Services (zie tabel 2 voor meer informatie)	Wereldwijd omzeild voor paraplu-kanten
Citrix Workspace	Ondersteund door Application Control
crashlytica	Wereldwijd omzeild voor paraplu-kanten
CrowdStrike Falcon	Ondersteund door Application Control
Diligent.com	Ondersteund door Application Control

onenigheid	Wereldwijd omzeild voor paraplu-kanten
DocuSign-overeenkomstcloud	Ondersteund door Application Control
DropBox	Ondersteund door Application Control
Druva Cloud Backup	Ondersteund door Application Control
Engyte Connect	Ondersteund door Application Control
Evernote	Ondersteund door Application Control
Facebook Messenger	Ondersteund door Application Control
Facebook	Ondersteund door Application Control
Filemail	Ondersteund door Application Control
vierkant	Ondersteund door Application Control
Giphy	Wereldwijd omzeild voor paraplu-kanten
GitHub	Ondersteund door Application Control
Google Drive	Ondersteund door Application Control
Google Play Store	Ondersteund door Application Control
Google Services (zie tabel 2 voor meer informatie)	Wereldwijd omzeild voor paraplu-kanten
Google Workspace	Ondersteund door Application Control
Ga naar vergadering	Ondersteund door Application Control
hype-machine	Ondersteund door Application Control

Instagram	Ondersteund door Application Control
LogMein Pro	Ondersteund door Application Control
Microsoft Defender voor Endpoint	Ondersteund door Application Control
Microsoft Intune	Ondersteund door Application Control
Microsoft Services (zie tabel 2 voor meer informatie)	Wereldwijd omzeild voor paraplu-kanten
Microsoft Xbox Live	Ondersteund door Application Control
Netflix	Ondersteund door Application Control
OpenDrive	Ondersteund door Application Control
PayPal	Ondersteund door Application Control
PingOne-identiteit	Ondersteund door Application Control
Rackspace-/cloudstationservices	Wereldwijd omzeild voor paraplu-kanten
Salesforce CRM	Ondersteund door Application Control
segment	Wereldwijd omzeild voor paraplu-kanten
signaalplatform-eenheid	Ondersteund door Application Control
Skype voor Bedrijven	Ondersteund door Application Control
Snapchat	Ondersteund door Application Control
geluidswolk	Ondersteund door Application Control

SpiderOak	Ondersteund door Application Control
Spotify	Ondersteund door Application Control
TeamViewer	Ondersteund door Application Control
TikTok	Ondersteund door Application Control
todoist	Ondersteund door Application Control
tjilpen	Ondersteund door Application Control
Vimeo	Ondersteund door Application Control
Workday HCM	Ondersteund door Application Control
Zoomvergaderingen	Wereldwijd omzeild voor paraplu-klanten

Tabel 2 – Details voor Diensten wereldwijd omzeild, zoals weergegeven in tabel 1

Apple Services	• Apple Captive Portal controleren • Apple iTunes en App Store • Aanvullende Apple-platformservices
Cisco Services	• Cisco Umbrella & OpenDNS Services • Cisco Webex- en Webex-teams • Cisco Cloud Email Security WebUI • AMP-eindpuntservice • Duo Security 2FA
Google Services	• Google Hangouts • Google Berichten op WEB • Aanvullende Google-platformservices
Microsoft Services	• Microsoft Network Connectivity Status Indicator • Windows Update • Windows-vertaalservice • Aanvullende Microsoft / Windows-platformservices

Zie Problemen oplossen met niet-browsertoepassingen of [neem contact op met Umbrella Support voor](#) extra hulp. Aanvragen kunnen worden overwogen voor toevoeging aan onze wereldwijde bypass-lijst nadat ze zijn beoordeeld door het Engineering-team.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.