2017

Beveiligingsbeleid van het Easy4IP systeem

V1.01

OSEC B.V.

Inhoud

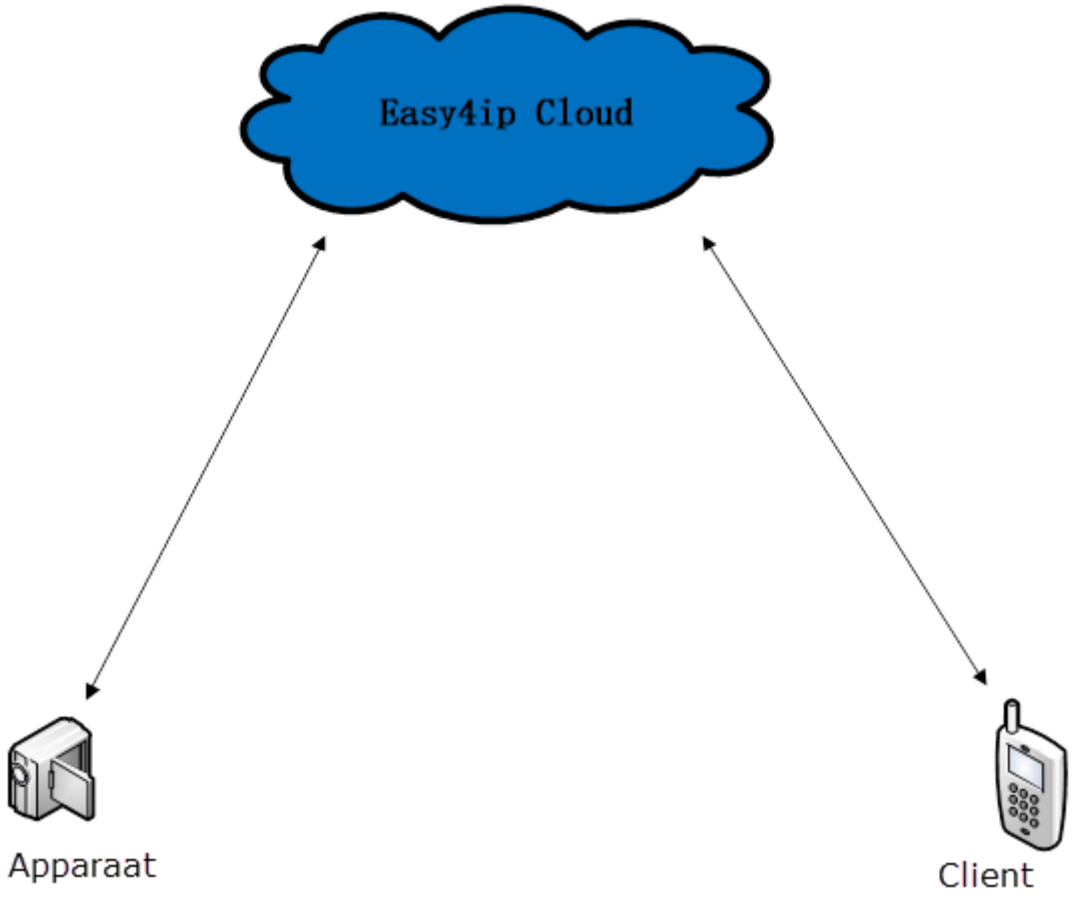
1. Introductie

Dit document beschrijft het beveiligingsbeleid binnen het Easy4IP systeem. Het wordt in de volgende onderdelen beschreven:

- beveiligingsbeleid van aanmeldingsprocedure
- beveiligingsbeleid van media transmissie
- validatie van apparaten
- beveiligingsbeleid van gebruikersinformatie
- beveiligingsbeleid van de servers

Dit document beschrijft de beveiligingsmaatregelen genomen door Dahua voor de P2P verbinding.. Naast deze maatregelen is het ook nog steeds noodzakelijk om te zorgen voor een goede wachtwoordbeveiliging in het apparaat zelf.

2. Beveiligingsbeleid van de aanmeldingsprocedure



Figuur 1 - Aanmeldingsprocedure

- verbinding tussen het apparaat en de easy4ip Cloud:
    - CA authenticatie van het domein
    - verbinding via https
    - WSSE(WS-security) authenticatie
- Verbinding tussen client en de easy4ip Cloud
    - CA authenticatie van het domein
    - verbinding via https
    - WSSE(WS-security) authenticatie

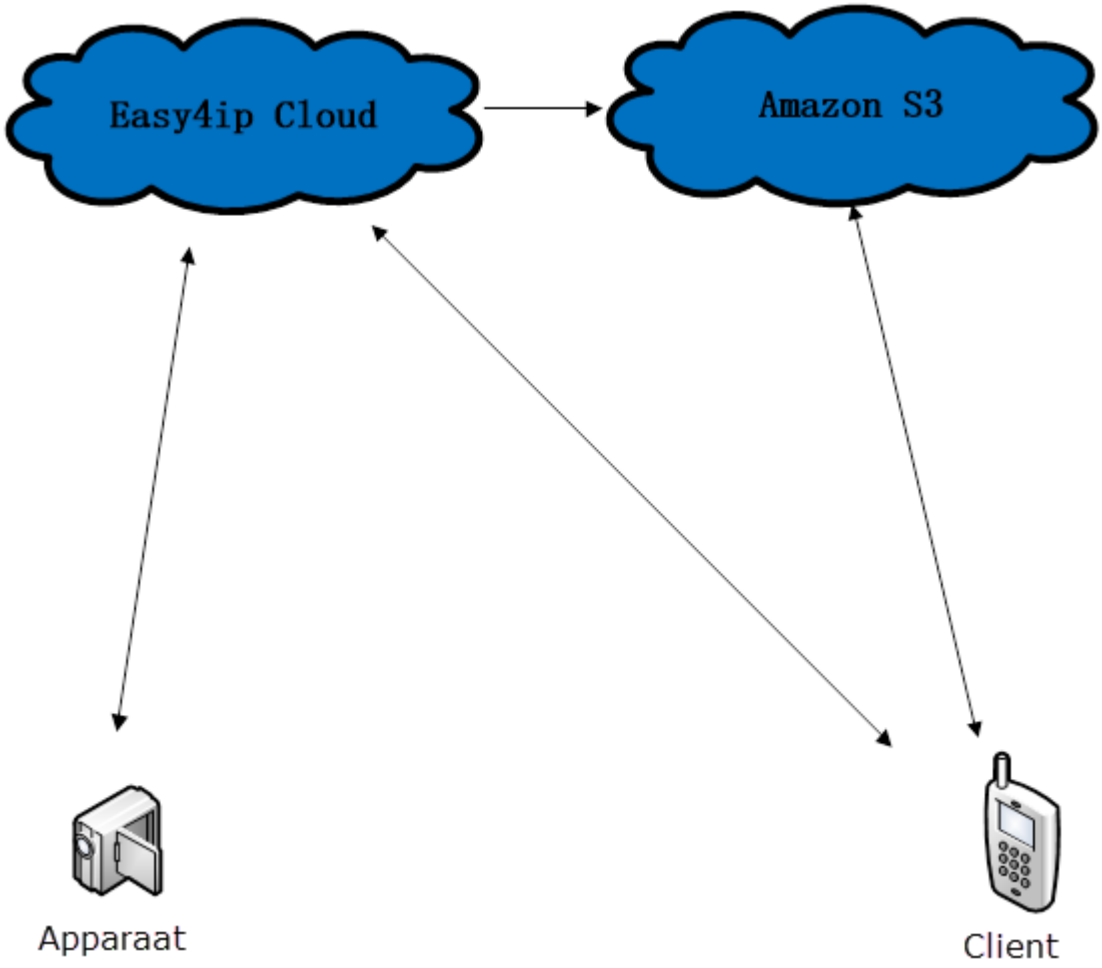
3. Beveiligingsbeleid van media transmissie

Er zijn drie belangrijke aspecten voor transmissie van media in het easy4ip systeem:

- Cloud storage
- Media forwarding
- P2P

Cloud storage refereert naar het opslaan van media of berichten in de Cloud. Media forwarding refereert aan de easy4ip stream van de apparaten naar de clients indien er live video wordt bekeken, of indien er opgenomen beelden worden bekeken.P2P refereert aan de peer-to-peer communicatie tussen de apparaten en clients.

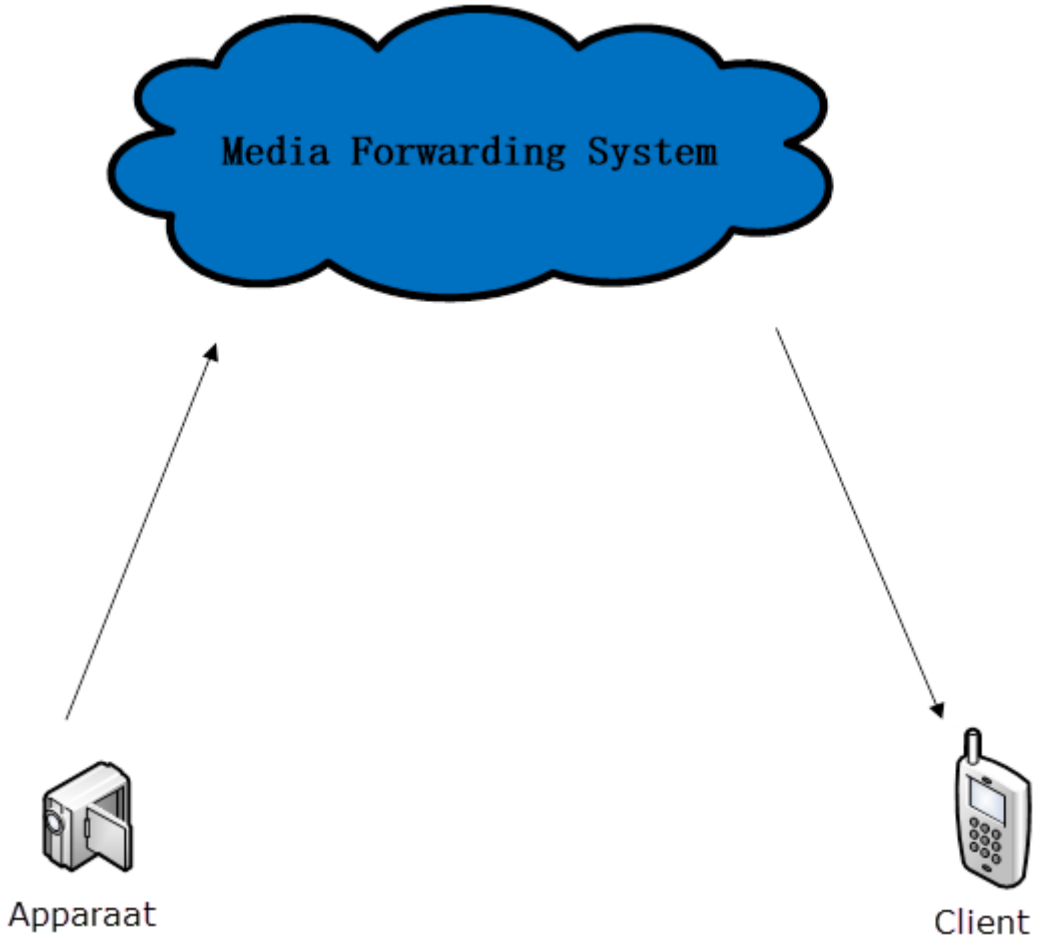
3.1 Cloud storage



Figuur 2 - Cloud storage

- verbinding tussen het apparaat en de easy4ip Cloud:
  - CA authenticatie van het domein
  - media is geëncrypteerd via een door de gebruiker gedefinieerde sleutel
  - verbinding via https
  - WSSE(WS-security) authenticatie
- verbinding tussen easy4ip Cloud en Amazon S3
  - CA authenticatie van het domein
  - media is geëncrypteerd via een door de gebruiker gedefinieerde sleutel
  - verbinding via https
- opslag tussen client en Amazon S3
  - verbinding via https
  - media is geëncrypteerd via een door de gebruiker gedefinieerde sleutel
  - tijdelijke URL met autorisatie en periodieke expiratie
- Verbinding tussen client en de easy4ip Cloud
  - CA authenticatie van het domein
  - verbinding via https
  - WSSE(WS-security) authenticatie
  - tijdelijke URL met autorisatie en periodieke expiratie

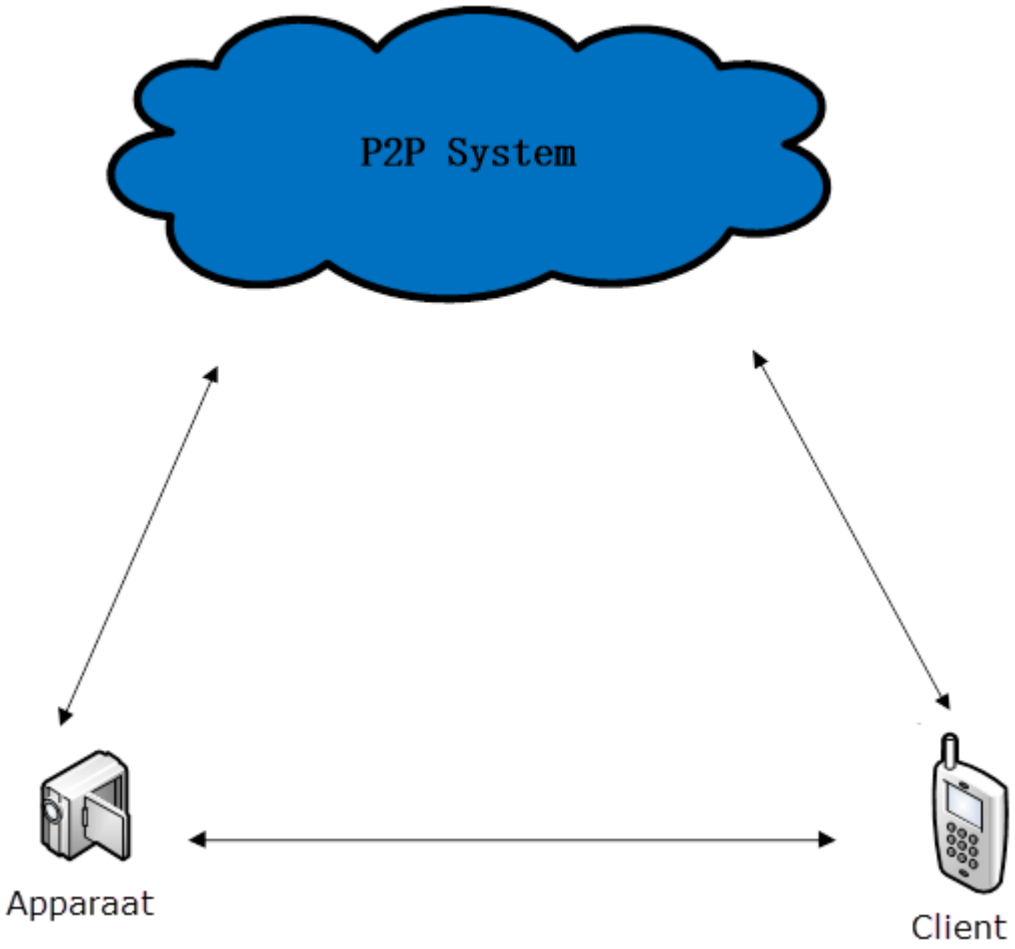
3.2 Media forwarding systeem



Figuur 3 - Media forwarding systeem

- **Verbinding tussen het apparaat en het Media forwarding systeem**
  - CA authenticatie van het domein
  - WSSE(WS-security) authenticatie
  - tijdelijke URL met autorisatie en periodieke expiratie
- **Verbinding tussen client en het Media forwarding systeem**
  - CA authenticatie van het domein
  - WSSE(WS-security) authenticatie
  - tijdelijke URL met autorisatie en periodieke expiratie

3.3 P2P systeem



Figuur 4 - P2P systeem

- CA authenticatie van het domein
- WSSE(WS-security) authenticatie
- Drie door gebruiker te selecteren transmissie modi

	Advantage	**Disadvantage**
passthrough	◆ Efficiënte transmissie ◆ Laag stroomverbruik apparaat en cliënt	Lage beveiligingsgraad
media is geëncrypteerd via een door de gebruiker gedefinieerde sleutel	◆ Efficiënte transmissie ◆ Hoge beveiligingsgraad	hogere belasting voor apparaat en client bij encryptie- en decryptie van media
TLS encryptie	◆ Zeer hoge beveiligingsgraad	Ongeveer 3 seconden vertraging zware belasting voor apparaat en client bij encryptie- en decryptie van media

4. Validatie van apparaat

- WSSE(WS-security) authenticatie

5. Beveiligingsbeleid voor gebruikersinformatie

- WSSE(WS-security) authenticatie
- Identificatie is gebaseerd op token met korte levenscyclus
- Gebruikers paswoord is niet in client opgeslagen – brute force zal geen invloed hebben
- Gebruikers paswoord is opgeslagen in easy4ip[cloud met behulp van MD5 encryptie

6. Beveiligingsbeleid servers

Het beveiligingsbeleid van de servers is gebaseerd op Amazon S3 en de web services

- Domein authenticatie met CA, voor beveiliging tegen domein hijacking en DNS cache vergiftiging
- Firewall filters
- Onregelmatigheidsdetectie netwerk verkeer
- Interactie tussen subsystemen gebaseerd op identificatie en validatie
- Alarm bij onregelmatigheden op netwerkniveau