Kryptolåda

Inledning

Detta dokument beskriver en kryptolåda som kan sättas med utsida mot det publika Internet (enligt Internetspecifikationen) och på sin insida erbjuda paketförmedling enligt Internetspecifikationen med trafikskydd och textskydd.

En kryptolåda ska givet en paketförmedlingstjänst enligt Internetspecifikationen kunna hitta andra kryptolådor för att upprätta relevanta koppel.

Avhängighet

Detta dokument är beroende av Internetspecifikation.

Begrepp

- **DoS-skydd:** Denial-of-service skydd från trafik som kommer från det publika Internet. En del av trafikskyddet.
- **Trafikskydd:** Ibland benämnt *signalskydd*, rör skydd av trafikflöden och behandlar bland annat störsändningar, falska meddelanden, och hoppande frekvenser / mottagaradresser.
- **Textskydd:** Ofta benämnt som kryptering, rör att skydda meddelandeinnehållet även om en antagonist kan läsa trafiken.

Arkitektur

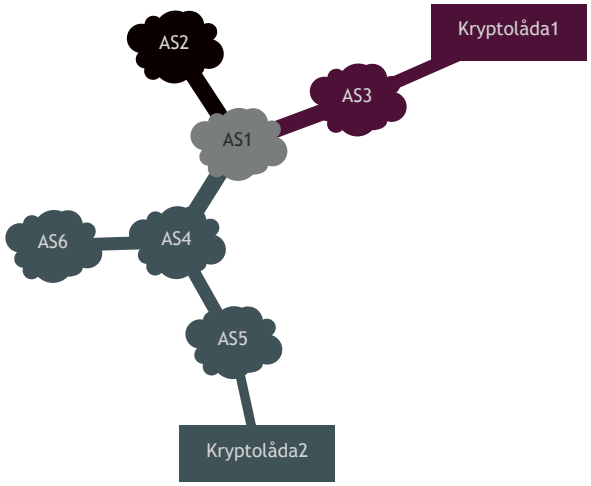
Övergripande hanterar arkitekturen för kryptolåda krypterad end-to-end trafik mellan två godtyckligt valda platser på Internet. Se arkitekturskiss för exempelritning av arkitekturen.

En kryptolåda kan både skicka och ta emot paket. Inkommande paket ska vara adresserade till kryptolådan

Tunnelidentiteter består av en kombination av:

- protokoll
- mottagaradress (IPv6)
- mottagarport

TODO: Vad är begärandet av en ny adress en del av? Använder vi bara prefix från In-



Figur 1: Arkitekturskiss

ternetspecifikationen och växlar mellan dem, eller ska vi lägga till hur man begär nya adresser via DHCP-PD eller en hel BGP-snurra?

TODO: Vem begär ny tunnelidentitet? Ska vi ha en kontrollenhet / annat som har ansvar att upprätthålla tunnlar osv.

TODO: Mesh, vilken del beslutar om hur vi bygger vårt mesh?

TODO: Kontrollplan?

DoS-skydd

Denial-of-service skyddet ska se till att kryptolådan ej kan sättas ur funktion genom designade trafikströmmar. Detta görs genom att kryptolådor ska klara av ett fullt trafikflöde enligt dess datalänklager.

TODO: Givet korrekt protokoll, port och adress så lämnar DoS över till trafikskydd?

- **Krav:**
  - DoS-skyddet **ska** filtrera bort all trafik som inte är adresserad till aktiv kryptografisk tunnel.
  - DoS-skyddet **ska** upprätthålla full tillgänglighet vid datalänkslagrets fulla trafikhastighet.

Trafikskydd

TODO: Vad gör trafikskyddet i den här lösningen?

- **Krav:**
  - Trafikskyddet **ska** meddela DoS-skyddet aktiva tunnelidentiteter.

Textskydd

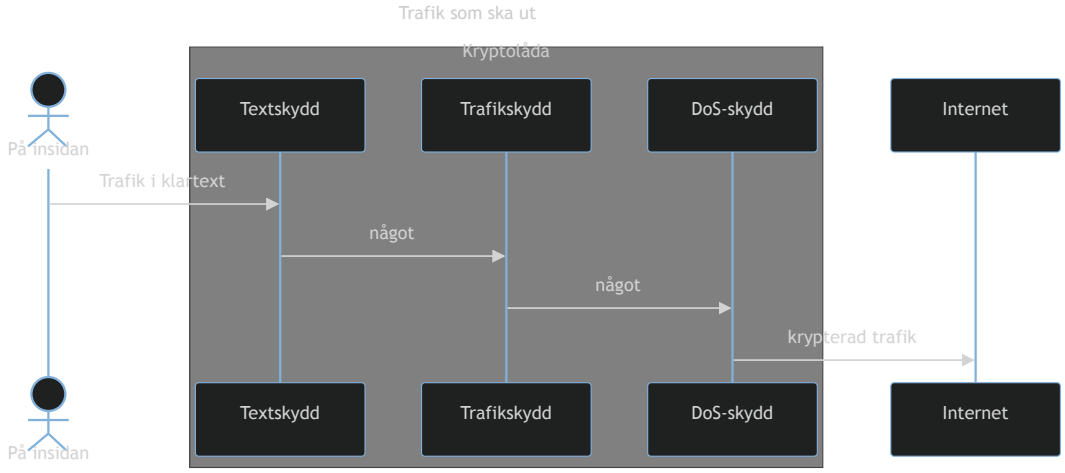
TODO: Hur mycket valfrihet ska finnas för textskyddet? Får användare välja vad som helst?

- **Krav:**
  - Textskyddet **ska** meddela trafikskyddet aktiva tunnelidentiteter.

Exempel

Från klient på insidan till trafik på utsidan

TODO: Reffa internetspecifikationen. På insidan så ska en klient inte se någon skillnad.



Figur 2: Trafik som går från klient

Trafik utifrån in till klient

TODO: Hur sker avskalning av skydd?

Verifikation

TODO: Ta fram mätbara krav på kryptolådan

Referensdesign

TODO: Ta fram referensdesign. Ev raspberry pi / liten referensdesign som man kan bygga och testa?

TODO: Hur hanterar vi kvantsaker? Ex nyckelutbyte över annan rutt än Internet?