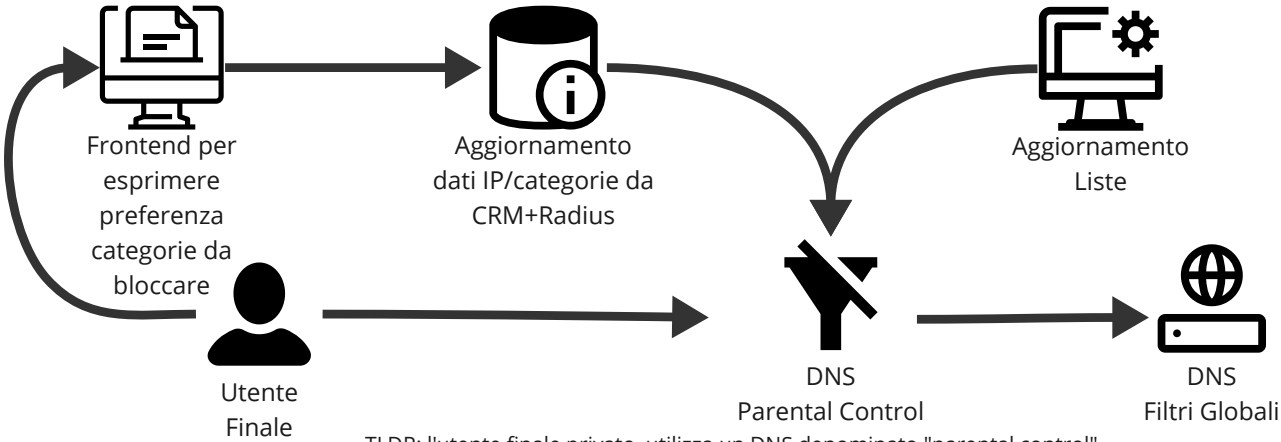
Architettura Parental control
9/23/CONS



TLDR: l'utente finale privato, utilizza un DNS denominato "parental control". Questo DNS è configurato in modo da avere conoscenza di ogni indirizzo IP assegnato alla clientela e per ogni cliente quali sono le classi di blocco da applicare. Se la richiesta non viene risolta localmente, viene forwardata agli attuali DNS dove sono applicati i filtri globali attualmente in essere (CNCPO, AAMS, AGCOM, etc)

Matteo Sgalaberni

DNS
Parental Control

DNS Resolver: unbound
Feature necessaria: Tags and Views
https://unbound.docs.nlnetlabs.nl/en/latest/topics/filtering/tags-views.html

Configurazione:
definizione dei tag da gestire
define-tag: "adulti gioco armi violenza odio mediche anonimizzatori sette"

Elenco IP e relative abilitazioni di blocco
access-control-tag: 10.0.1.1/32 "adulti gioco"
access-control-tag: 10.0.1.2/24 "armi violenza"
access-control-tag: 10.0.1.3/24 "adulti mediche"
access-control-tag: 10.0.1.4/24 "sette violenza"

> TLDR: in questo modo unbound applicherà ad ogni indirizzo IP un tipo di filtro diverso in base ai tag applicati, questa configurazione sarà creata da un sistema esterno di competenza dell'operatore e raccoglierà le info da Radius/CRM per capire le preferenze di categoria da bloccare espresse dal cliente per ogni accesso. Per ovviare al problema degli IP dinamici che cambiano nel tempo, la procedura di sincronizzazione potrebbe essere eseguita ogni X (15) minuti, rifare le configurazioni, fare un unbound-checkconf e reload.

Aggiornamento Liste

Aggiornamento Liste
Le liste da bloccare saranno aggiornate da un processo/sistema esterno che scriverà le zone locali di unbound

Configurazione di un dominio nel tag adulti:
local-zone: "adulti.it" redirect
local-data: "adulti.it A 127.0.0.1"
local-zone-tag: "adulti.it" "adulti"

TLDR: un processo/sistema esterno creato dall'operatore si occuperà di aggiornare le liste da una sorgente identificata e scrivere delle configurazioni che creino una lista di domini con un redirect ad un determinato IP di blocco e associato un relativo "tag", che è usato nella configurazione precedente.

DEMO

TLDR: POC fatto in docker della configurazione
Per replicarla, crea due file di conf Dockerfile e unbound_parentalcontro.conf in una directory vuota ed esegui i comandi in README
Nell'esempio il client 127.0.0.1 si troverà bloccato il dominio adulti.it nella categoria "adulti", il dominio "violenza.it" nella categoria "violenza" non sarà bloccato.

Demo Video su asciinema:
https://asciinema.org/a/599529

```
> cat README
#
docker build -t poc-pc .
docker run --rm --name poc-pc -d poc-pc
echo -e "\n✔️contenuto violenza.it aperto"
docker exec poc-pc host violenza.it 127.0.0.1
echo -e "\n🚫contenuto adulti.it bloccato"
docker exec poc-pc host adulti.it 127.0.0.1
docker stop poc-pc
```

```
> cat Dockerfile
FROM debian:bullseye

RUN apt -y update
RUN apt install -y unbound host procps
RUN /usr/sbin/unbound-anchor -4 || echo
COPY unbound_parental.conf /etc/unbound/unbound.conf.d/
CMD [ "unbound", "-d" ] %
```

```
> cat unbound_parental.conf
remote-control:
    control-interface: 0.0.0.0

server:
    interface: 0.0.0.0@53

    define-tag: "adulti gioco armi violenza odio mediche
anonimizzatori sette"

# Elenco IP e relative abilitazioni di blocco
    access-control-tag: 127.0.0.1/32 "adulti armi"

# Elenco domini bloccati per categoria adulti
    local-zone: "adulti.it" redirect
    local-data: "adulti.it A 127.0.0.1"
    local-zone-tag: "adulti.it" adulti

# Elenco domini bloccati per categoria violenza
    local-zone: "violenza.it" redirect
    local-data: "violenza.it A 127.0.0.1"
    local-zone-tag: "violenza.it" violenza
```

Considerazioni finali

Considerazioni finali

- il DNS ha configurazioni statiche e non dipende da database/sistemi esterni con tutti i vantaggi del caso come performance e resilienza a guasti, continua a funzionare anche se i sistemi esterni smettono di comunicare con lui;
- tutta la configurazione è stateless, è possibile replicare il DNS su N istanze indipendenti;
- sono da sviluppare dei **sistemi esterni** che interagiscono con questo sistema per eseguire le seguenti operazioni:
  - software che aggiorna le liste da una sorgente esterna e distribuisce le configurazioni sui vari unbound del parental control in campo
  - software che raccoglie l'elenco degli indirizzi IP associati ai clienti con le relative classi di inibizione da un proprio sistema
  - frontend per raccogliere le preferenze da parte del cliente finale sulle categorie di blocco da applicare per il proprio accesso

Tutto realizzabile e non complicatissimo in base alle risorse tecniche a disposizione. Rimane un unico grande dilemma.

Le liste dei domini da bloccare divisi per categoria da dove le prendiamo?

Se hai commenti o idee su come farla più semplice, robusta, diversa di così -> matteo@ehiweb.it / Telegram @sgalam

Matteo Sgalaberni
Ehiweb.it
28/07/2023