

Piracy e Parental

L'inizio per automatizzare i processi e monetizzare sui servizi

CHI SIAMO

Vayu è un'azienda di ingegneria di servizi per il mercato delle telecomunicazioni, che da oltre 10 anni mette a disposizione l'esperienza del proprio team di tecnici, ingegneri e manager, per innovare attraverso soluzioni specifiche costruite per operatori e service provider.

I NOSTRI VALORI



AFFIDABILITÀ



COMPETENZA



RAPPORTO UMANO



VISIONE STRATEGICA



NETWORK

ENGINEERING
& OPERATIONS

CONSULENZA

REGOLAMENTARE

SOFTWARE

UN ECOSISTEMA IN EVOLUZIONE

Dove ci eravamo lasciati

Wholesale Winery Tour - Campania 22 Marzo 2023

Servizi DNS - Obbligo vs Opportunità

<https://www.wholesaletours.it/2023/wwt/speakers/pdf/stefanoni.pdf>

Obbligo VS Opportunità

Obbligo:

- Inevitabile
- Costi
- Problemi

↓

il minimo indispensabile

Opportunità

- Qualità
- Controllo
- Servizi aggiuntivi

↓

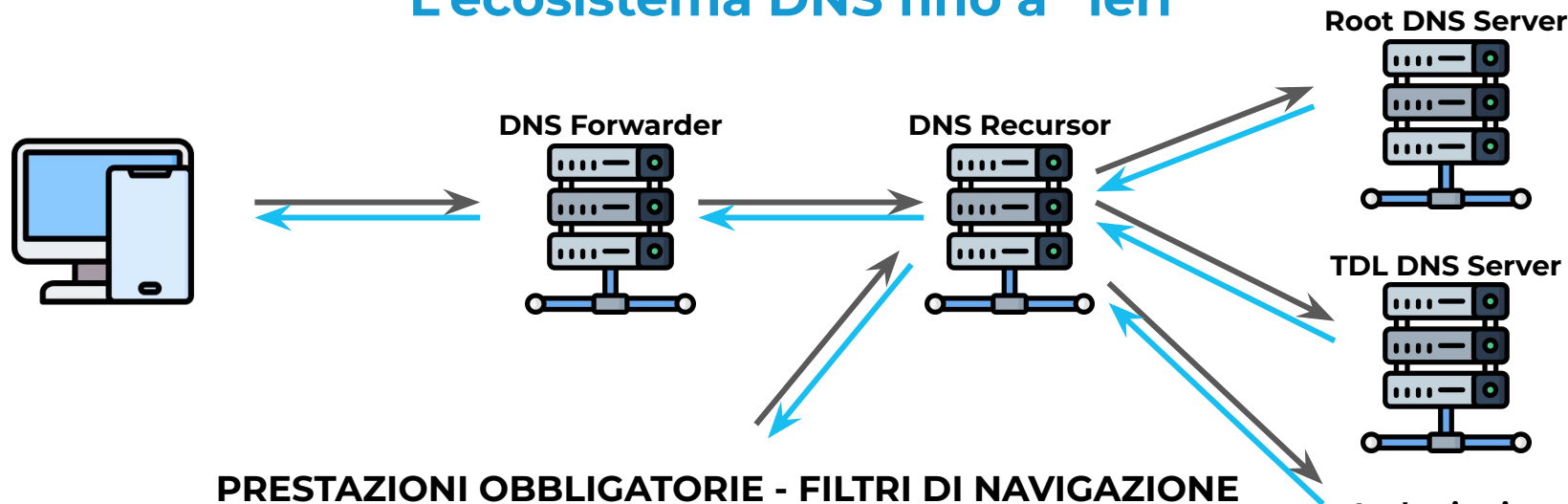
il meglio possibile

WHOLESALE WINERY FT Tour

Davide Stefanoni
SERVIZI DNS: obbligo VS opportunità

ITNOG

L'ecosistema DNS fino a "ieri"



PRESTAZIONI OBBLIGATORIE - FILTRI DI NAVIGAZIONE

CNCPO: Centro nazionale per il contrasto alla pedo-pornografia on-line

ADM: Agenzia delle dogane e dei monopoli

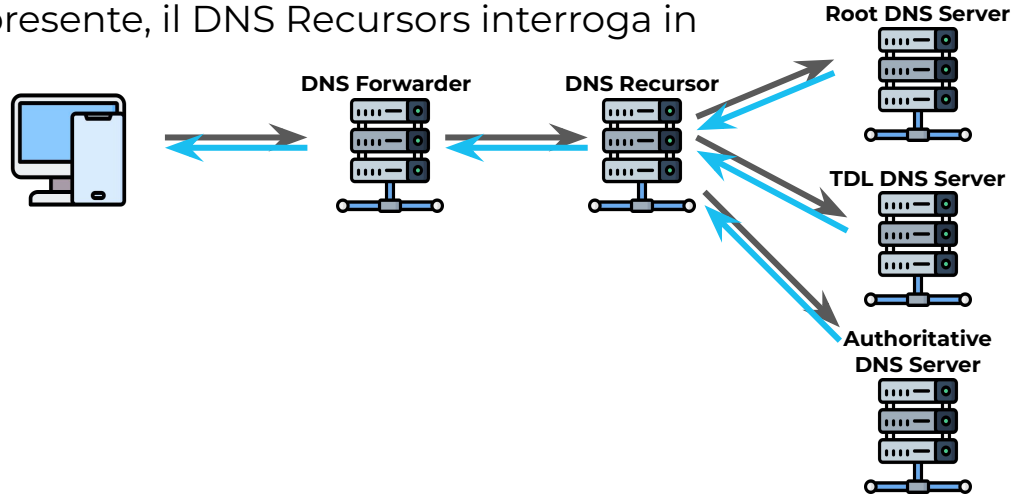
AGCOM: Autorità per le garanzie nelle comunicazioni

CONSOB: Commissione nazionale per le società e la borsa

Provvedimenti dell'**Autorità Giudiziaria**

Come funziona una Query DNS

- Il client invia una query DNS (direttamente al Recursor o ad un Forwarder intermedio)
- Il DNS Recursor funge da intermediario tra il client ed i nameserver DNS
- Viene interrogata prima la cache locale
- Sono verificati eventuali Filtri/Redirect legati a prestazioni obbligatorie
- Nel caso in cui la query non sia presente, il DNS Recursor interroga in ordine:
 - Root DNS Server
 - TLD DNS Server
 - Authoritative DNS Server
- La risposta viene inviata al client



ROOT DNS Server

- Esistono 13 root nameserver DNS a livello globale
- Sono noti a tutti i DNS Recursor e sono la prima fermata nella ricerca di un resolver ricorsivo per i record DNS
- Il Root DNS risponde indirizzando il Recursor a un TLD DNS Server, in base all'estensione del dominio (.com, .net, .org. ecc.)
- I Root Nameserver sono controllati da 12 organizzazioni indipendenti

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	170.247.170.2, 2801:1b8:10::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

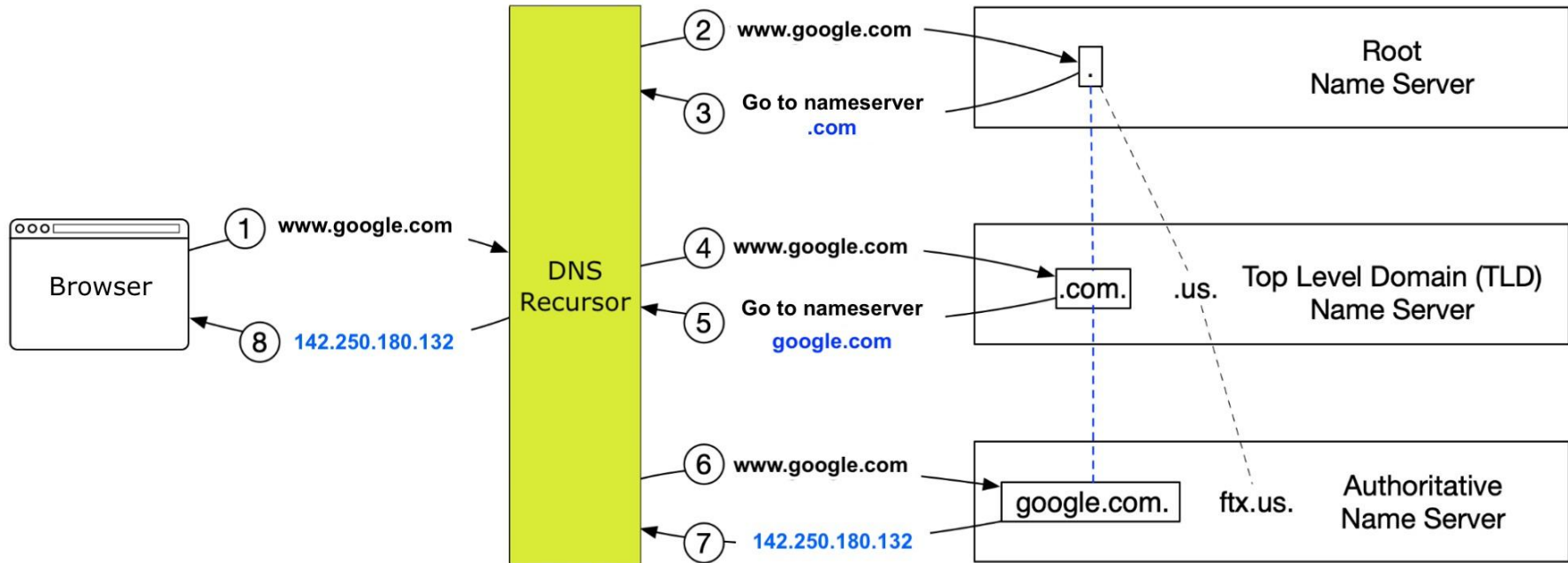
TLD DNS Server

- TLD Nameserver contengono le informazioni relative a tutti i domini di una specifica estensione di dominio
- .com TLD DNS Server contiene tutte le informazioni sui siti terminanti in *.com
- I TLD Server sono suddivisi in sei gruppi (generic, country code, generic restricted, infrastructure, sponsored, test), di cui i due principali sono:
 - Domini di primo livello generici: non specifici per Paese (.com, .org, .net, .edu, .gov)
 - Domini di primo livello con codice internazionale: includono tutti i domini di un Paese (.uk, .us, .it, ...)
- Il TLD DNS Server risponde alle richieste del DNS Recursor indirizzandolo sul DNS Autoritativo di uno specifico dominio

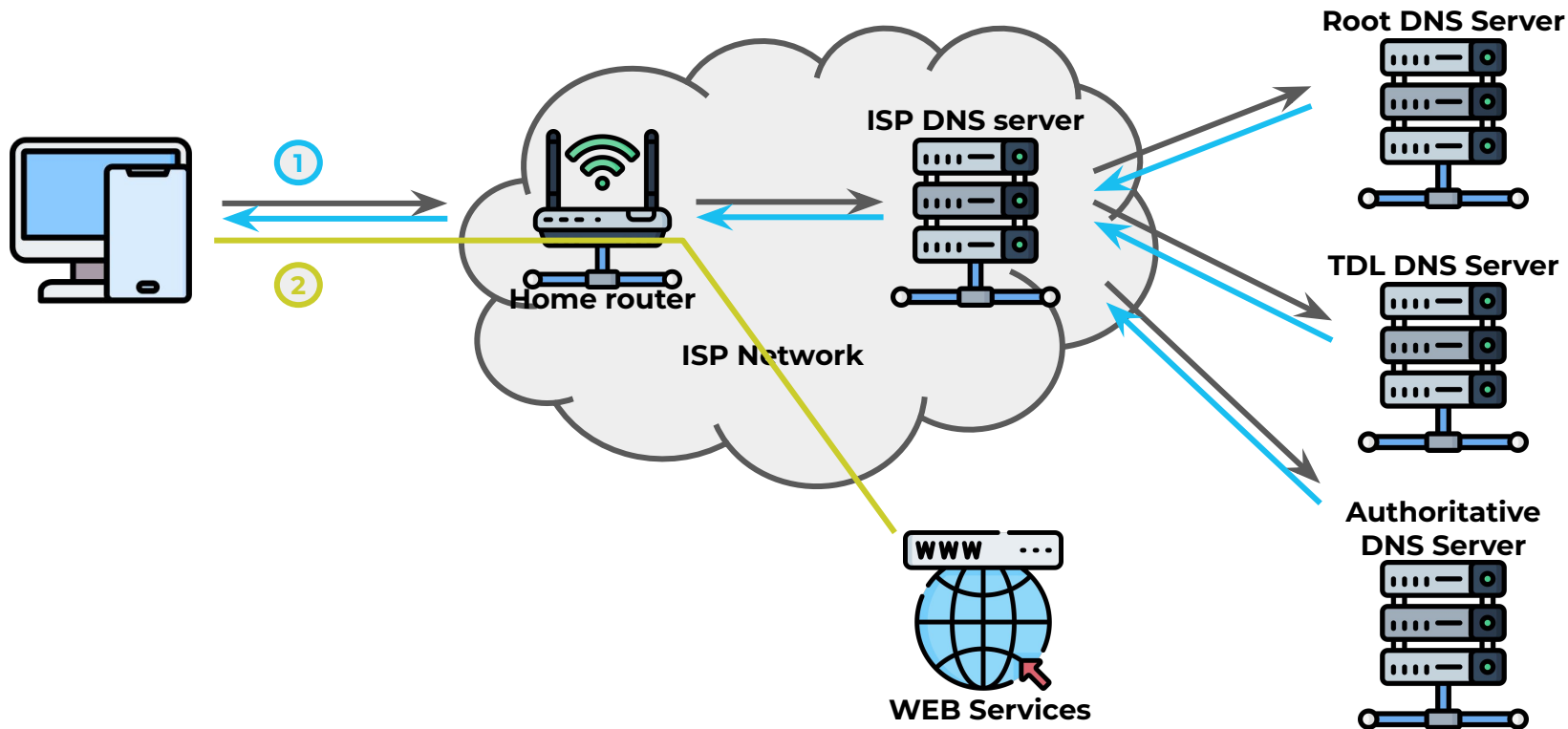
Authoritative DNS Server

- Il Nameserver autoritativo è di solito l'ultimo passo della query DNS
- Contiene informazioni specifiche sul nome di dominio richiesto (es. vayu.it)
- Può fornire due tipologie di risposte al DNS Recursor:
 - l'indirizzo IP del server trovato nel Record A
 - l'alias del dominio se vi è abbinato un Record CNAME : a quel punto il DNS Recursor dovrà eseguire una query DNS completamente nuova per ottenere il record abbinato all'alias

Come i DNS risolvono gli IP



L'esperienza del cliente



Perchè l'ISP dovrebbe utilizzare i propri DNS

Prestazioni:

- Si avvicinano i DNS ai clienti
- Utilizzo della Cache e riduzione dei tempi di risposta
- Non è un servizio che necessita di elevate risorse hardware
- Prodotti opensource disponibili
- Sicurezza e Privacy con Encryption attiva : DoH (DNS over HTTPS) e DoT (DNS over TLS)

Obbligo:

- Gestione delle richieste di reverse
- Ottemperanza alle richieste di Prestazioni Obbligatorie
- Conformità normativa

Opportunità:

- Creare record di reverse per ogni IP customer/infrastruttura
- Gestione diretta dei propri domini
- Creare dyndns per ip dinamici
- Pieno controllo sul servizio offerto
- Rete più sicura
- Offrire servizi a valore aggiunto

Prestazioni Obbligatorie e Conformità Normative nel mondo DNS

Filtri di Navigazione:

- Liste di blocco pubbliche/private
 - Provvedimenti e decreti di blocco
- | | |
|---|----------------------|
| ❖ | CNCPO |
| ❖ | ADM |
| ❖ | AGCOM |
| ❖ | CONSOB |
| ❖ | Autorità Giudiziaria |

Piracy Shield:

- Quadro normativo definito da AGCOM
- Piattaforma creata da AGCOM
- Ideata per l'oscuramento selettivo di FQDN (Fully Qualified Domain Name) ed IP "illegali"

Parental Control:

- Quadro normativo definito dall'art. 7-bis del DL 30 aprile 2020
- AGCOM con Delibera 9/23/CONS individua ed attualizza i requisiti minimi dei Sistemi di Controllo Parentale in capo agli Operatori
- Filtro di contenuti, sulla base di macrocategorie, "inappropriati per minori"

PIRACY SHIELD - Il quadro normativo

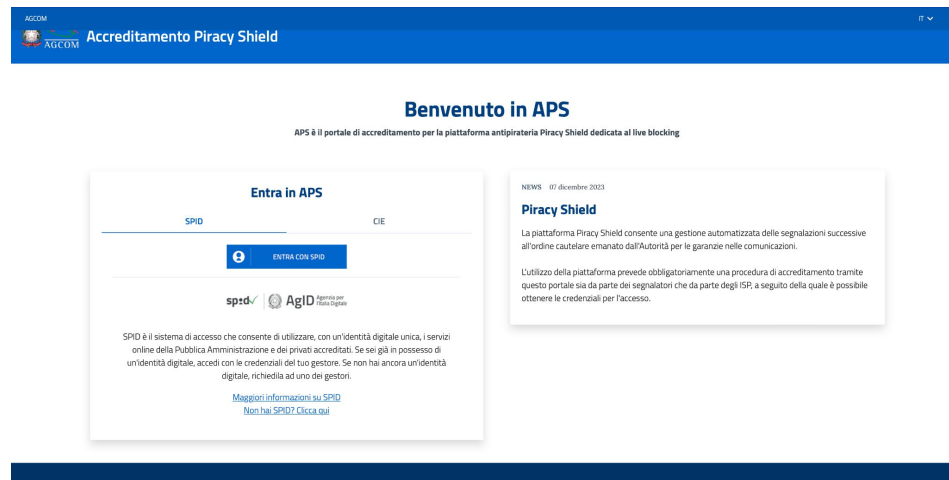
- Operativo dal 31 Gennaio 2024, con delibera 189/23/CONS introduce modifiche al Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70 di cui alla delibera n. 680/13/cons
- Requisiti Tecnici Operativi definiti nella delibera 321/23/CONS
- Obbligo per tutti gli ISP di implementare sulla propria rete dei sistemi di blocco per l'oscuramento selettivo dei contenuti digitali pubblicati nel sistema
- Il blocco deve avvenire entro 30 minuti dalla pubblicazione dei nuovi indirizzi
- Conferma dell'avvenuto blocco in risposta entro 30 minuti
- In caso di mancato rispetto delle disposizioni, gli ISP sono soggetti a sanzioni amministrative



PIRACY SHIELD - Il contesto tecnico-operativo degli ISP

Accreditamento

- L'utilizzo della piattaforma prevede obbligatoriamente una procedura di accreditamento sia da parte dei segnalatori che da parte degli ISP
- La procedura può essere eseguita tramite SPID direttamente sul sito AGCOM:
<https://aps.agcom.it/aps/login.htm>
- Si ricevono le credenziali per l'accesso al sistema (area web + IPSEC dedicata)
- Sono previste credenziali diverse per un ambiente di test e per l'ambiente di produzione



PIRACY SHIELD - Il contesto tecnico-operativo degli ISP

Segnalazione

- I titolari dei diritti, in qualità di segnalatori accreditati (es. Dazn, Lega Serie A, Lega Serie B, Mediaset, RTI), possono inviare al sistema Piracy Shield FQDN ed indirizzi IP che trasmettono contenuti in violazione al Diritto d'Autore.
- La piattaforma, “previa verifica”, provvede ad aggiornare la lista dei siti da oscurare e la invia agli operatori accreditati tramite ticket.

Ticket 2cef01cd64db499c90a4758f1a0739af

Status :  open

Timestamp : 📅 2024-04-07T20:29:24.963790+02:00

Acquisito : 📅 2024-04-07 20:33

IPv4

IPv6

FQDN

45.155.227.159 [ok]

45.135.236.111 [ok]

like55.xyz [ok]

akkuna.xyz [ok]

cheny22.xyz [ok]

PIRACY SHIELD - Il contesto tecnico-operativo degli ISP

Blocco

- Gli ISP sono tenuti ad *“eseguire i provvedimenti dell’Autorità senza alcun indugio e, comunque, entro il termine massimo di 30 minuti dalla notifica, disabilitando la risoluzione DNS dei nomi di dominio e l’instradamento del traffico di rete verso gli indirizzi IP o comunque adottando le misure tecnologiche e organizzative necessarie per rendere non fruibili da parte degli utilizzatori finali i contenuti diffusi abusivamente”*
- È inoltre richiesto che anche la conferma di avvenuto blocco sia inoltrata in risposta al ticket di segnalazione entro i 30 minuti



AVVISO

L'accesso al presente sito è stato disabilitato in esecuzione di un provvedimento adottato dall'Autorità per le garanzie nelle comunicazioni, ai sensi del regolamento in materia di tutela del diritto d'autore online approvato con delibera n. 680/13/CONS.

Per maggiori informazioni visiti il sito

www.agcom.it

PIRACY SHIELD - Flusso di lavorazione dei ticket

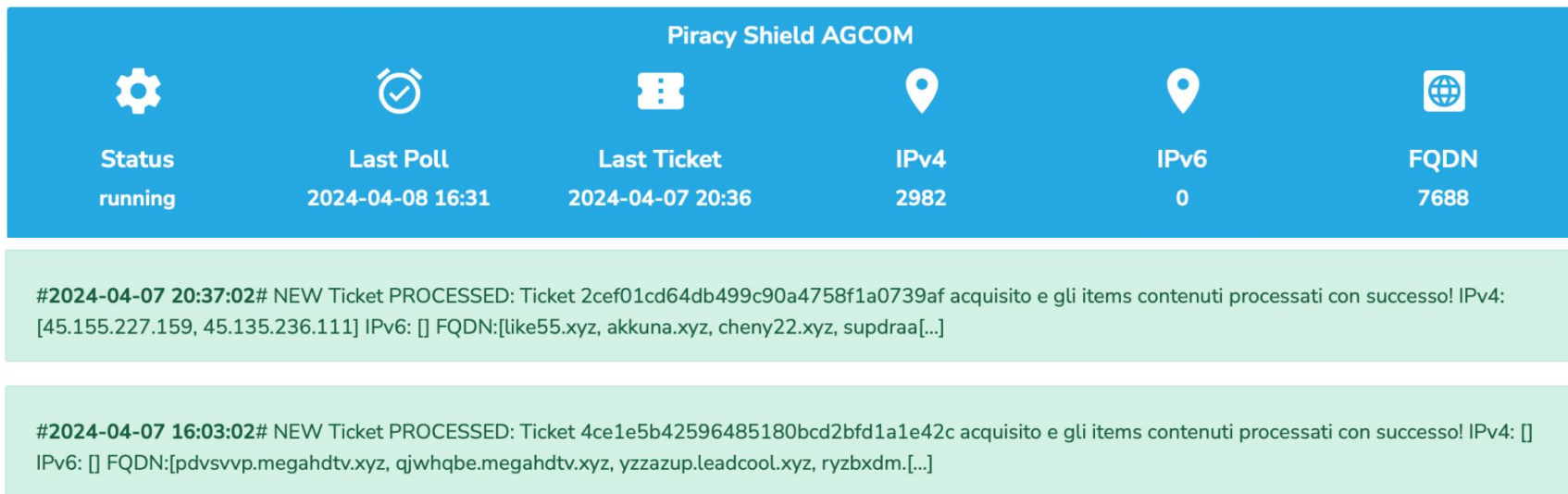
- Verifica continuativa della presenza di nuovi ticket
- Ogni nuovo ticket sarà in stato open per 30 minuti
- Gli elementi del ticket vanno processati in quei 30 minuti
 - applicazione filtri FQDN  inserimento blocchi su macchine DNS
 - inserimento blocchi IPv4 ed IPv6  inserimento blocchi su apparati Rete
- Va inviata conferma di ricezione e gestione entro 30 minuti
- Passati i 30 minuti il ticket passa in stato closed (avrò massimo 48 ore successive alla chiusura per aggiornare lo stato degli elementi)



Automazione dei processi tra Piracy e piattaforme ed apparati dell'ISP

Case Study: Interrogazione API e dashboard di controllo

- Login/Logout automatico
- Verifica e recupero dati del singolo ticket
- Verifica e recupero dati di tutti i ticket
- Impostare lo stato di processazione dei dati
- Monitoraggio dello stato della piattaforma Piracy
- Inserimento dati nella Whitelist dedicata all'ISP



Case Study: Applicazione Blocchi

Blocchi di tipo FQDN



Integrazione liste su DNS Recursor dell'ISP
Redirect automatico verso la pagina di
segnalazione indicata da AGCOM

Blocchi di tipo IP



Inserimento in rete delle rotte IPv4/IPv6 di
Blackhole
Blocco della raggiungibilità degli IP



ExaBGP

<https://pypi.org/project/exabgp/>

https://labs.ripe.net/author/thomas_mangin/exabgp-a-new-tool-to-interact-with-bgp/

Case Study: Route Injector via software

- ExaBGP è un'applicazione per integrare e controllare, su server e software, i processi BGP
- Semplice, flessibile ed adatto a differenti tipologie di utilizzo
- Permette l'inserimento in rete di rotte arbitrarie di tipo IPv4 ed IPv6, ma anche di FlowSpec

```
neighbor 192.168.150.1 {      # Remote neighbor to peer with
    router-id 192.168.250.1;    # Our local router-id
    local-address 192.168.250.1; # Our local update-source
    local-as 65000;             # Our local AS
    peer-as 65000;             # Peer AS
    family {
        ipv4 unicast;
        ipv6 unicast;
    }
    api {
        processes [announce-routes];
    }
}
```



Nel caso di Peer BGP Multipli
basta replicare la
configurazione.
Possono essere aggiunte
anche Community



Inietta la lista di IP
segnalati dal Piracy e li
annuncia sulle sessioni
attive

Case Study: Best Practice Router

- Filtri per le Network di “Bogon” : <https://ipgeolocation.io/resources/bogon.html>
- Filtro per la Default Route 0.0.0.0/0
- Utilizzo di una Community per poter manipolare e redistribuire le rotte in maniera semplice

Case Study: Best Practice Router

Juniper MX Configuration

```
set policy-options policy-statement in-piracy term discard-bogons from route-filter-list bogons
set policy-options policy-statement in-piracy term discard-bogons then reject
set policy-options policy-statement in-piracy term discard-default from route-filter-list default-route
set policy-options policy-statement in-piracy term discard-default then reject
set policy-options policy-statement in-piracy term accept-piracy from community piracy
set policy-options policy-statement in-piracy term accept-piracy then next-hop discard
set policy-options policy-statement in-piracy term accept-piracy then accept

set policy-options policy-statement out-piracy term discard-all then reject

set protocols bgp group PIRACY type internal
set protocols bgp group PIRACY peer-as 65000
set protocols bgp group PIRACY neighbor 192.168.250.1 description PIRACY
set protocols bgp group PIRACY neighbor 192.168.250.1 multihop
set protocols bgp group PIRACY neighbor 192.168.250.1 local-address 192.168.150.1
set protocols bgp group PIRACY neighbor 192.168.250.1 import in-piracy
set protocols bgp group PIRACY neighbor 192.168.250.1 export out-piracy
```

Case Study: Best Practice Router

Huawei NetEngine Configuration

```
route-policy in-piracy deny node 10
  if-match ip-prefix bogons
#
route-policy in-piracy deny node 10
  if-match ip-prefix default-route
#
route-policy in-piracy permit node 100
  if-match community-filter piracy whole-match
  apply ip-address next-hop blackhole
#
route-policy out-piracy deny node 100
#
```

```
bgp 65000
group PIRACY internal
peer PIRACY as-number 65000
peer 192.168.250.1 as-number 65000
peer 192.168.250.1 group PIRACY
#
ipv4-family unicast
peer PIRACY enable
peer PIRACY route-policy in-piracy import
peer PIRACY route-policy out-piracy export
peer 192.168.250.1 enable
peer 192.168.250.1 group PIRACY
#
#
```

Parental Control



Requisiti AGCOM

Delibera n. 9/23/CONS

Filtri di contenuti «inappropriati per minori» devono essere inclusi e attivati nelle offerte dedicate ai minori. Sulle altre offerte devono essere resi disponibili come attivabili da parte del titolare del contratto, in ogni caso devono essere totalmente gratuiti. Sono esclusi dall'ambito di applicazione i contratti di tipo business.

<https://www.agcom.it/documents/10179/29648921/Allegato+21-2-2023>

- Obbligo di fornitura
- Assistenza ai clienti
- Gratuità del servizio
- Pubblicità
- Pre-attivazione

Le linee guida: le scelte più semplici

- Gli operatori realizzano i sistemi di parental control mediante almeno una delle soluzioni tecniche:
 - i) basate su DNS o altro filtro a livello di rete dell'operatore
 - ii) filtraggio tramite applicativo installabile sui dispositivi del consumatore
- L'abilitazione alla configurazione, alla disattivazione o attivazione avviene tramite almeno uno dei seguenti metodi:
 1. codice PIN fornito all'atto dell'attivazione dell'utenza, comunicato in forma riservata, ad esempio tramite SMS
 2. SPID
 3. autenticazione nell'area riservata del sito web dell'operatore
 4. Tramite l'OTP che è inviato via SMS o e-mail
- Gli operatori devono comunicare all'Autorità le categorie utilizzate per i sistemi di Parental control e i soggetti terzi a cui è affidata la definizione e aggiornamento delle liste di nomi a dominio e siti oggetto di blocco

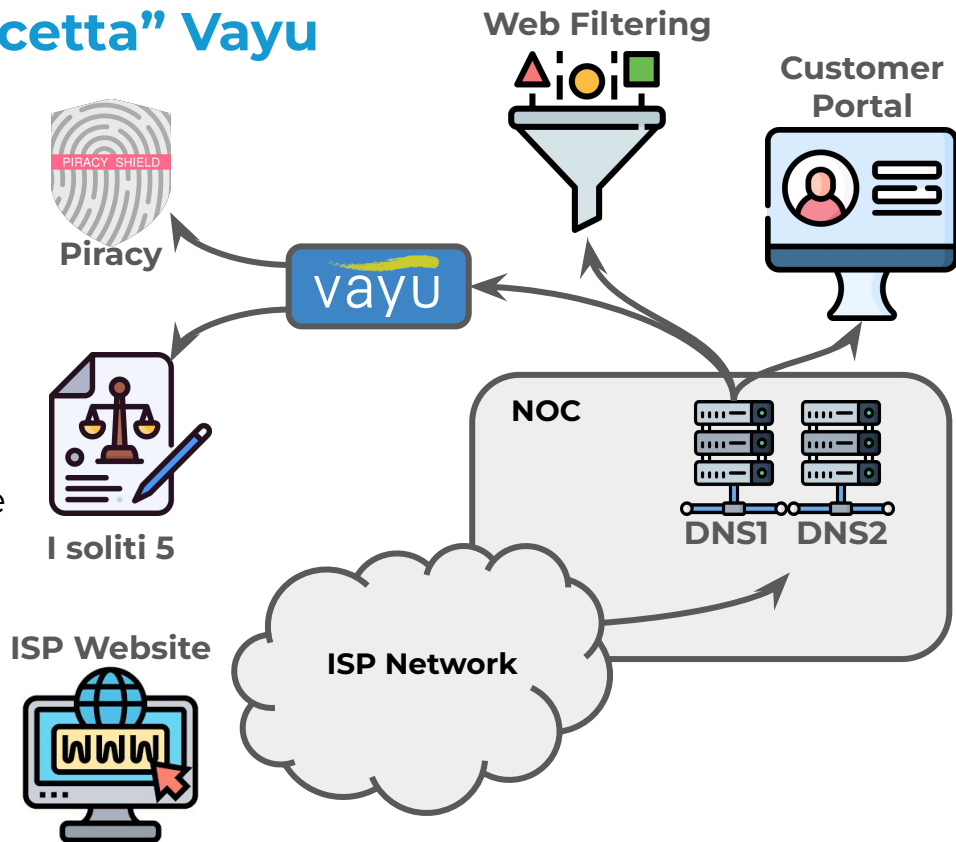
Categorie di Filtraggio

I contenuti oggetto di filtro dei SCP sono configurabili dal titolare del contratto, con la possibilità di personalizzare almeno le categorie di contenuti oggetto di filtro

- ❖ contenuti per adulti
- ❖ giochi d'azzardo / scommesse
- ❖ armi
- ❖ violenza
- ❖ odio e discriminazione
- ❖ droghe e informazioni pericolose alla salute
- ❖ anonymizer
- ❖ sette

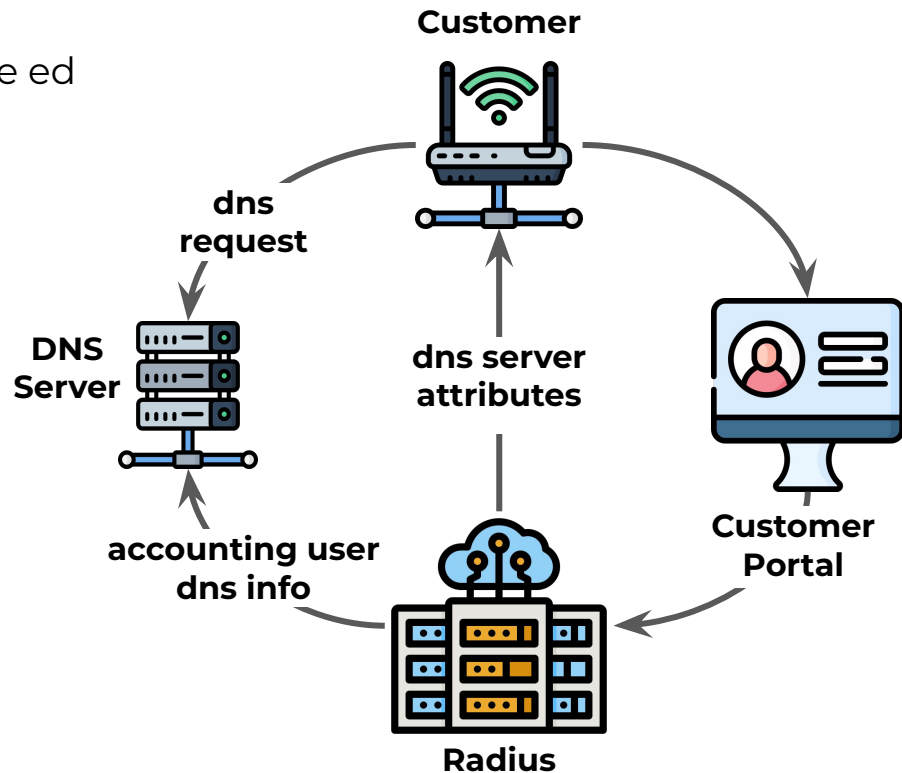
La “ricetta” Vayu

- **ISP Website** informativa tecnica e comunicazione ad AGCOM
- **DNS Server** ridondato con proxy cache
- **Vayu** sistema di gestione e monitoraggio liste di blocco regolamentari e Piracy
- **Sistema Web Filtering** gestione liste e categorie
- **Customer Portal** per assegnazione profili



Customer Portal

- Categorie di filtri organizzati in modo semplice ed intuitivo
 - Nessun filtro
 - Protezione Famiglia (tutti i filtri previsti da agcom)
 - Protezione Cybersecurity (malware, spam, phishing, botnet)
 - Filtri personalizzati
- Integrazione nativa con la piattaforma Radius dell'ISP



Customer Portal



SESSIONE
11.9 DAYS



CARICATO
4.90 MB



SCARICATO
41.09 MB



FTTH 10M/10M

VIA Cappuccini 45 - Tradate

codice: **TIM_FTTH_3**

Linea attiva - Connessione online

Servizio filtro web: Filtro personalizzato

MODIFICA



Dati supplementari

Campi di prova
prova1

Connessione

Consegna IPv4
Static

IPv4
172.16.3.17

Customer Portal



Modifica il servizio filtro web

Filtro Famiglia

Il filtro comprende le seguenti categorie

- ☐ - Contenuti per adulti
- ☐ - Armi/violenza/odio e discriminazione
- ☐ - Gioco d'azzardo e scommesse
- ☐ - Droghe e pratiche pericolose per la salute
- ☐ - Anonimizer
- ☐ - Siti pericolosi (Malware, Phishing etc...)

Filtro siti pericolosi

Il filtro comprende le seguenti categorie

- ☐ - Siti pericolosi (Malware, Phishing etc...)

Nessun Filtro

Nessun filtro è applicato alla navigazione

Filtro personalizzato

- ☒ Per utenti avanzati:
permette la selezione singola delle categorie

ANNULLA

PROSSIMA

Modifica il servizio filtro web

Seleziona le categorie di servizi web per **Filtro personalizzato**

- ☒ sesso e pornografia
- ☐ giochi d'azzardo
- ☒ armi
- ☒ violenza, odio e discriminazione
- ☐ droghe e informazioni pericolose alla salute
- ☐ anonymizer
- ☒ malware, phishing e spam

ANNULLA

ANTERIORE

SALVA

Come l'ISP può monetizzare sul servizio Parental?

- Aspetto fondamentale è la proposizione della soluzione sui mercati:
 - B2B
 - Enti e PA
- Non servono investimenti particolari o modifiche per estendere l'offerta
- Permette di remotizzare/centralizzare le funzioni di Web Filtering
- Indipendenza dal Router/Firewall Cliente
- Valorizzano la soluzione anche le categorie/funzioni non presenti nella delibera AGCOM:
 - Filtri di Cyber Security (malware and threat protection)
 - Alta IP Reputation
 - Categorie "avanzate"
 - Gestione di liste particolari e personalizzate
 - Gestione di timer e fasce orarie
- Sensibilizzare il cliente ed avvicinarlo alla soluzione (offerte di try & buy)

Grazie per l'attenzione

I nostri contatti
www.vayu.it
info@vayu.it
+39 0698373335

