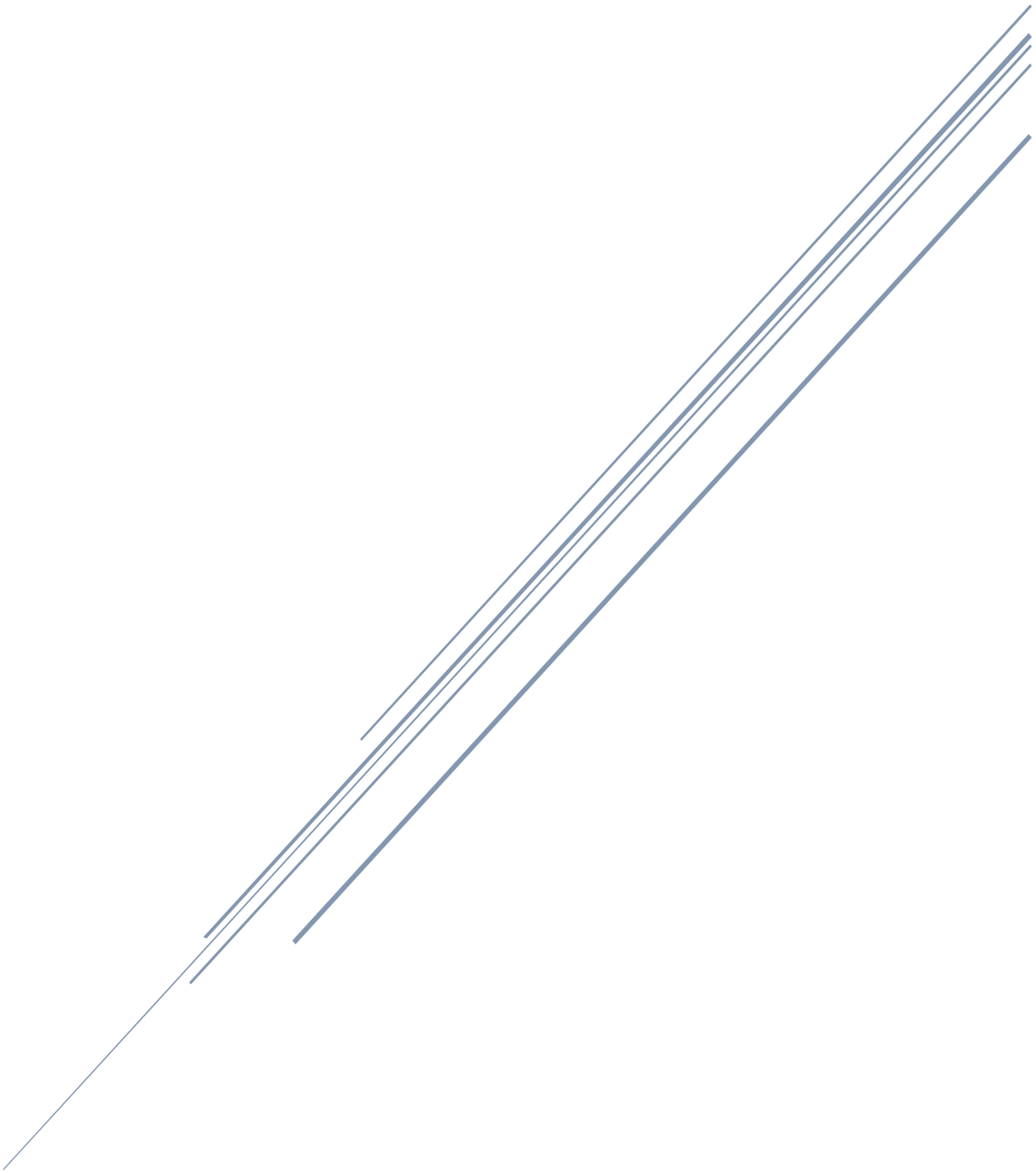
FASTAPN V 12.1.5

FlytLink Ltd



fastapn.com

Operation and Deployment Manual

Flytlink Ltd

admin@flytlink.com

UK Reg: 12452878

IFEC FASTAPN SERVICE

Operation and Deployment Manual

Date	Version	Name	Approval
Nov 15th 2015	Initial Draft v 1.1	W T Smith	CEO
Jan 22nd 2016	Final Rev 2.4	W T Smith	CEO
Feb 17th 2018	Final Rev 2.6	W T Smith	CEO
April 24th 2021	Final Rev 12.1.1	W T Smith	CEO
May 19th 2024	Final Rev 12.1.4	W T Smith	CEO
May 21st 2024	Amend Rev 12.1.5	W T Smith	CEO

Table of Contents

FastApn is a service owned and operated by
Flytlink Ltd, UK Reg 12452878, Concorde House, Brighton, United Kingdom
Tel UK: +44 (0)203 991 0033 - Tel USA: +1 720 598 8055

1 FastApn Description

1.1 High Level Overview

The FLYTLINK FastApn service has become the defined standard process for significantly improving data access speeds within networks and services that predominantly have high RTT's by design, such as ATG, LEO/MEO and GEO satellite links (within the airline (IFEC) industry), as well as service provisions that have to seriously manage bandwidth, specifically where quality issues occur due to free space, network latency and the loading of high numbers of concurrent users (contention). The latter normally occurs where the cost of provisioning a service is high, such as the aviation industry using satellite systems, hybrids and ATG networks, on both the ground and air segments,

The FastApn service can operate transparently with instantaneous activation, and fallback, additionally, the service enhances throughput and congestion management on all traffic protocols and via all ports, including VPN's, Exchange and Streaming, therefore they all enjoy the same acceleration, security, decongestion and protection processes, whilst providing the following benefits, with no system hardware or software modifications:

- Latency Reduction
- Congestion Reduction
- Deep Packet Filtering at source
- Full Client / System Controls

Resulting in:

- Decrease in Free Space & Network Latency
- Removal of all Adverts, Tracking, Telemetry and Unwanted Data
- Reduction in Bandwidth utilization
- Lower Operator Service Payments
- Increased Customer Satisfaction
- Enhanced Security

FastApn is a service owned and operated by
Flytlink Ltd, UK Reg 12452878, Concorde House, Brighton, United Kingdom
Tel UK: +44 (0)203 991 0033 - Tel USA: +1 720 598 8055

1.2 Transparent Services

The service can operate completely transparently, whether utilized as an end user service or fleetwide, there is no interaction required for a persistent redundant service, however, should a more hands on service be required, there are many statistical and configuration options that can be used in real time by accessing the FastApn service node assigned.

Each operator can have access to a BareMetal isolated server containing their unique FastApn system, which is not used for any other purpose or by any other users or operators, it's a fully operational endpoint system for the customer, thereby uniquely customizable right down to visual appearance and theming to suit corporate identities.

A comprehensive web-based dashboard is supplied and preconfigured for immediate operation and monitoring.

Figure 1: Top section example of the operator FastApn Dashboard

The service, with its incorporated processing modules, significantly reduces traffic, thereby reducing contention and bandwidth utilisation, leading to reduced costs and at the same time enhancing customer satisfaction.

It is configured to operate on all systems and networks with high RTT's, including ground segments, all without any interaction or any hardware or software modifications.

It's simply plug and play, but with the added option of adding access to the Web Administration GUI to track throughput, resource usage logs, and to apply real time configurations, request access controls and customisation, should this be required.

1.3 Statistical Analysis

The FastApn system records and monitors all traffic requests and produces graphical, selectable logs, top tables, audit controls and port access charts, as well as real-time viewing, without infringing or identifying users.

With this data, operators can easily determine what services and calls are bandwidth hungry and take immediate steps to reduce by blacklisting a rogue service or even a system.

The data can also be used for determining what passengers are using the IFEC service for, and therefore can build on marketing efforts to suit.

In the below example, graph colours represent system requests permitted and refused, mouse over refers and displays the actual traffic log for specific time bar.

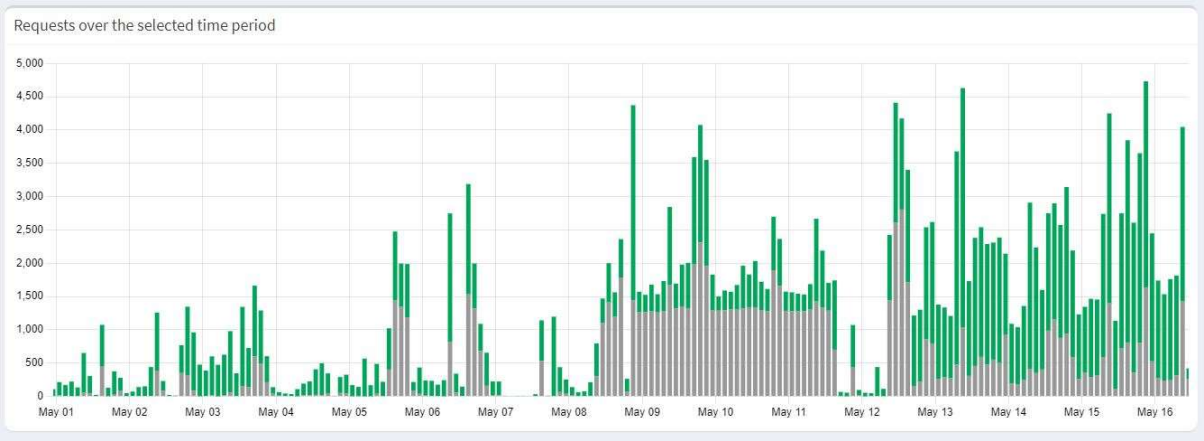


Figure 2: Definable time-based statistics, available in graphic format (shown) or selectable request logs

1.4 Group and Zone Management

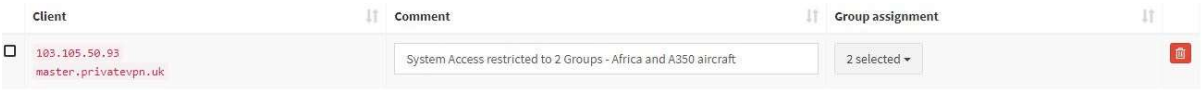
Within the system, the service has a Group and Zoning capability with unlimited group generation combinations, where operators can assign Data Request Controls to:

- Systems > aircraft / routers / networks / MAC's, IP's > Groups
- Domains > domain, URL's, partial, wildcards, Regex > Groups
- DPF Lists > defined lists, custom lists, status > Groups

1.4.1 Specific Data Request Access examples:

- Specific aircraft types
- Specific hardware types
- Territorial locations
- Operator bases
- Maintenance / VIP / Testing

Grouping combinations are unlimited, a combined grouping example would be to allow only certain content to be delivered to Ku equipped A350 aircraft flying to and from destinations within Africa, or for no content to be delivered to aircraft stationed in China.



1.1 Redundancy & Security

The simplicity of connection with the FastApn service is its unique attribute, a primary DNS IP change is all that is needed on any device, from a PED (Personal Device) right through to a corporate router heading an entire operation. All devices have the ability to change to a specific DNS on the fly, the redundancy element is already built in and all devices have a secondary option by default, so an unlikely a catastrophic FastApn service failure would have any impact on any segment of any connected network, whether airborne or ground based.

The service operation also includes the ability to specify upstream DNS servers, which can be any combination of customer owned devices and public DNS servers such as Cisco or Google, both with IPv4 and IPv6 capabilities, or the Unbound option can be put in place.

In addition, duplicate FastApn servers with fast failover can be provided if required, noting that this is a very rare optional requirement.

The service can also be connected and deployed using a proxy or can be used as the primary DHCP server for all connectivity.

1.2 Incorporated Modules

The FastApn service includes many time tested and validated modules in one transparent package for operators and end users alike, a full explanation of these functions can be found in section 4.0 of this document.

- DPF – Deep Packet Filtering
- DAL - Domain Access Lists
- Dynamic and Custom Flat file Blocklists
- DNS / PROXY / DHCP Service Access
- Pepsal's (performance Enhancing Proxy for Satellite Links)
- TCP Acceleration (Hybla / Fast Open / Reno + Proprietary)
- TCP Congestion Management
- SmartAVdns (Location Controls)
- Local DNS Configuration
- Telnet Statistical Access
- Web Based Administration and Configuration
- Long term Data Statistics
- System / Device Access Controls
- Group Management and Zoning
- FastApn System API

2 Service Utilization

2.1 Networks and Devices

The FastApn service can be used on all network types and devices, from individual PED's right through to corporate data segments whether transiting by Satellite, ATG, ATM, Mobile (3/4/5/6G), ADSL / SDL, either contended or at Committed Information Rates.

There is a choice to access by DNS, DHCP, VPN or Proxy settings in browsers, mobile devices, aircraft cabin routers, SDU's, SDR's, ACPU's, APN's, VPN's, ATG / EAN systems and systems using BGAN hardware, such as the Cobham Aviator and EMS based SDU's, these can either be the ground or air segments, or both. All service access methods provide all

enhancements on all ports without any software or hardware changes or modifications.

2.1.1 PED's – Personal Electronic Devices

Any connection capable device regardless of OS or manufacturer, examples include mobiles, tablets, laptops, PC's, gaming devices, all Linux OS and Windows OS variations

2.1.2 Local Networks / Aircraft Connections

Access Points / WAP's / Routers / Repeaters, or any device that is involved in the local connectivity of devices whether airborne or ground segments

2.1.3 Ground or Inflight Core Hardware

Core devices / ACPU's / SDU's / SD Gateways / Modems relative to any known or future services including ATG, 2Ku, Ka, BGAN, Iridium, EAN, OneWeb and SpaceX networks and key routing devices.

2.1.4 Aircraft / Zone / Custom Groups

Operator Group Management Controls for applying all FastApn services to a wide combination of scenarios including aircraft type, aircraft system types, planned destinations, restrictive or un restrictive zones, VIP's and pax segmentation. An unlimited number of Groups and combinations can be applied in real-time.

2.1.5 Aircraft Fleets / Core Network Access

Complete Zonal control of all the FastApn services over an entire aircraft fleet or ground segment including Entire Airlines, Fractional, VIP and Charter Organizations in flight and corporate sized ground network infrastructures with full redundancy and real time monitoring.

2.1.6 Primary Network Gateways

Normally ground based Networks that serve either internal company access and / or are specific to an airborne or satcom / IFEC redistribution network. DNS can be at any level within the network.

2.1.7 ISP Gateways

Company header and AS routers, ISP trunk routers, core devices.

3 FastApn Access Methods

3.1.1 DNS Access

Changes to the DNS servers used in any device, from personal devices (PED's) to corporate backend routers and airborne hardware and WAP's, is a very simple operation and the preferred and easiest choice for FastApn connectivity.

Every network connection in any device using TCP/IP will have a facility for this. It's likely that your hardware uses a default DNS server provided by the upstream provisioning network, and simply changing this to a different DNS IP provided by FastApn is all that is needed to enable the service. Only the primary DNS server IP needs changing, leaving the secondary default as a predefined backup. The operator can determine where the DNS IP change should be, and only one device change is needed – Levels:

- Personal Device (Owners Choice)
- WAP (Aircraft Wireless Access Point)
- ACPU / SDU (Aircraft Routing Devices)
- Ground < > Air Network Segments
- IFEC Connecting Gateways
- ISP / AS Gateways

For personal devices changes out of the realm of a provided service, such as In Flight Internet, can use our public FastApn nodes globally for continued use, so there is no need to change this back to an original DNS server, even when you are no longer aboard the aircraft or using a satellite / ATG or congested link, and it will continue to give you protection and acceleration, through any provider, wherever this may be located.

Note: Using the DNS method of system access does not route traffic through our systems, the operator existing backhaul infrastructure remains.

3.1.2 Proxy Access

The FastApn proxy service is a client individual BareMetal server that provides a gateway between pax / users and the internet, it is referred to as an "intermediary" because it goes between end-users and the services visited online.

The FastApn service can also be added to any device as a proxy, thereby effectively routing all traffic through an external gateway, where additional security, access lists and all the FastApn capabilities can be used, monitored and tracked, either by default OS software, or by third party software such as Proxifier or the built-in configuration or third-party plugins made for several browsers.

Nearly all devices have the ability to add a proxy, this includes most routers and inflight hardware, all Android and iPhone OS, and, right down to all PC Laptops, Macs and even browsers. Our proxy service runs on port :7478, and each client is issued with a unique ip for access. We also have global dynamic access via proxy on global.fastapn.com:7478 for persistent device use including small routers and BGAN systems, access of which is protected by a user / pass combination.

Note: Operators using the proxy method of system access do not need to make any DNS changes, as this is automatically called from within the proxy services, and it should be realised that access by proxy to the FastApn service routes all traffic as a backhaul provision to the internet.

3.1.3 VPN Access

Connection to FastApn by VPN is a popular choice for end user PED's and hardware / systems, due to its commonality in off the shelf devices, simple connection parameters and enhanced security. The VPN authentication can be by ACL (Access Lists (common for operators) or simple authentication clients.

FastApn can used many VPN protocols to connect:

- L2TPD
- L2TPD / IPSEC
- L2TPD / IKEv2
- PPTP
- OpenVPN
- Wire Guard

IPSec	L2TP	PPTP	SSL/TLS	OpenVPN	SSH	WireGuard
Secure	Secure	Fast	Widely used	Highly configrable	Allows port forwarding	Highly secure
Flexible	Widely available	Built-in client	Maintains data integrity	Open source	Supports key-based authentication	Open source
Widely supported	Easy to set up	Easy to set up	Required for compliance	Highly secure	Enables secure file transfer	Lightweight design

Figure 3: VPN Protocol types

Note: Operators using the VPN method of system access do not need to make any DNS changes, as this is automatically called from within the VPN service, and it should be realised that access by VPN to the FastApn service routes all traffic as a backhaul provision to the internet.

3.1.4 DHCP Access

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices. DHCP can be implemented on small local networks, as well as large enterprise networks.

DHCP assigns new IP addresses in each location when devices are moved from place to place, which means network administrators do not have to manually configure each device with a valid IP address or reconfigure the device with a new IP address if it moves to a new location on the network.

The FastApn service can also be accessed by DHCP, which means the service will automatically assign an IP and connect any number of users to the system and hence online. To enable this, the server would need to be placed within the network concerned (either manually or virtually), whether in airborne or ground segments, noting that only one DHCP server can be operational at the same time on the same network. The server has all the built-in capabilities to assign the main router and private IP blocks.

Operators using the DHCP method of system access do not need to make any DNS changes, as this is automatically part of the server when using DHCP.

Note: Using the DHCP method of system access will route traffic through our systems if accessed remotely, however, if the system server is placed within your own network, your existing internet backhaul infrastructure will remain.

4 FastApn Operating Principles

4.1 Technical Overview

The service utilises multiple common and proprietary techniques for managing TCP acceleration, Pepsal's, and DPF (Deep Packet Filtering), thereby boosting throughput, reducing latency and eliminating unwanted data at source, with the immediate effect of substantially reducing traffic congestion and contention, and subsequently, costs, while dramatically increasing customer satisfaction.

4.2 DPF (Deep Packet Filtering)

The DPF (Deep Packet Filter) segment of FastApn utilizes many dynamic methods to filter out, at source, unwanted data including, but not limited to the following table, noting that it's the customers decision to block specific sites, add whitelist specific sites, apply regex filtering, remove competition and apply filtering to specific locations, aircraft types and even systems through constructive grouping. In addition, the customer can even choose to utilize our hundreds of predefined blocklists without any complex interaction with the service, as well as block websites, social media, Apps and Games

4.2.1 Table of Custom Blocking DPF Lists & Domains

Advertising	Un Authorized Redirects
Analytics	Scams
Tracking	Malware
Telemetry	Suspicious Websites
AMP Hosts	Porn and 18+ sites
Malicious Websites	Hate and Junk
Phishing	Drugs
Ransomware	Firearms
Cryptojacking	Fake News
Abuse	Gambling
Fraud	Dating Services
Spam	Dead Domains
Piracy	Useless Websites

4.2.2 Table of Custom Apps, Ports, IP's and URL's

Crypto Pages	Youtube
Pinterest	Pixiv
Omegle	Gamebanana
Booth.pm	Patreon
Tik Tok	Facebook
Instagram	Snapchat
Twitter	Discord
Skype	Whatsapp
Spotify	Riot Games
League of Legends	Valorant
Shinden.pl	Myanime.list

4.3 Pepsal's – Performance Enhancing Proxy for Satellite Links

For high RTT's at the network level, Pepsal's use net filters to intercept connections that arrive from satellite or terrestrial high RTT links and "steals" the TCP SYN packet in the three-way handshake phase of a TCP connection, then pretends to be the other side of that connection, and

initiates a new connection to the real endpoint, using a user space application that directly copy's data between the two sockets, thereby substantially eliminating latency caused by repetitive TCP handshaking

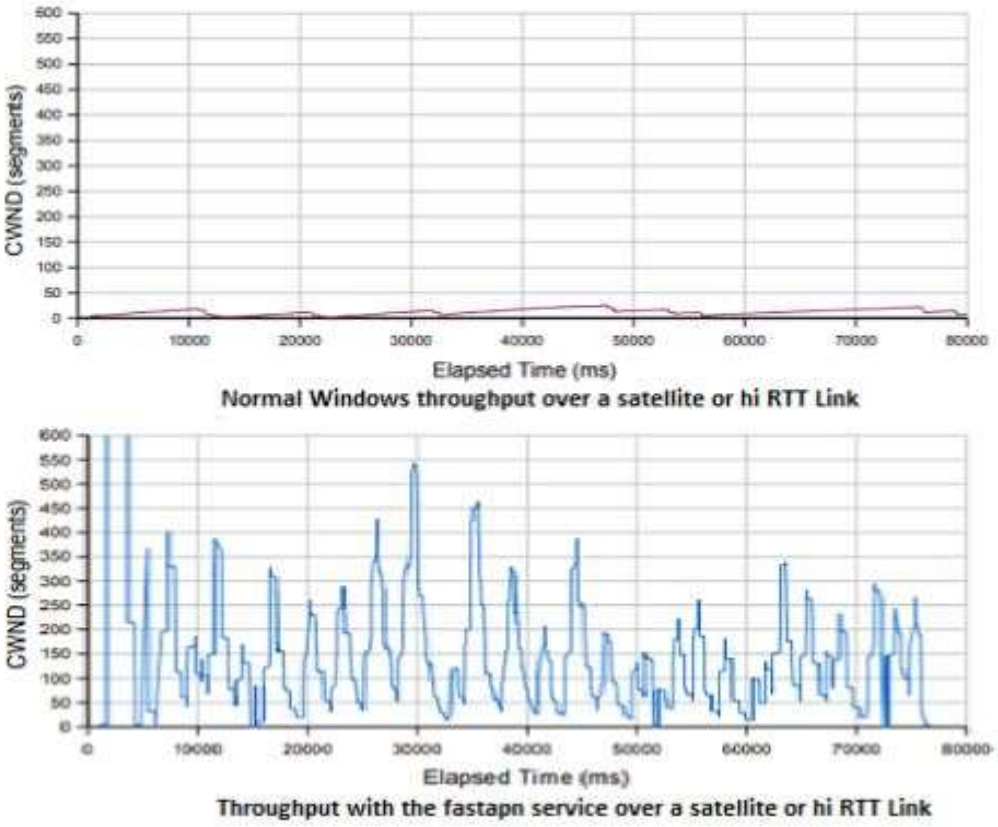


Figure 4: Difference before and after using the FastApn service on a high RTT link

4.4 DAL (Domain Access Lists)

Custom or predefined Domain blocklists can be selected readymade from FastApn, or compiled by the customer for specific grouping, service or even aircraft or system types, they are changeable on the fly and fully configurable. We currently hold in excess of 9 million dynamic domains that are proven to cause extra unwanted traffic or even contribute damage to services and systems. Within the DPF, these domains are blocked at source, i.e., at the DNS lookup level, thereby eliminating unwanted traffic.

4.5 Regular Expressions - Regex

A regular expression, or RegEx for short, is a pattern that can be used for building arbitrarily complex filter rules in *FastApn*. We implement the POSIX Extended Regular Expressions similar to the one used by the UNIX egrep (or grep -E) command. We amend the regex engine by approximate blocking (compare to agrep) and other special features like matching to specific query types only.

Our implementation is light and fast as each domain is only checked once for a match. When you request data, it will be checked against your RegEx. Any subsequent query to the same domain will not be checked again until you restart FastApn.

4.5.1 Hierarchy of regex filters

FastApn uses a specific hierarchy to ensure regex filters work as you expect them to. Whitelisting always has priority over blacklisting. There are two locations where regex filters are important:

1. On loading the blocking domains form the gravity database table, *FastApn* skips not only exactly whitelisted domains but also those that match enabled whitelist regex filters.
2. When a queried domain matches a blacklist regex filter, the query will *not* be blocked if the domain *also* matches an exact or a regex whitelist entry.

4.6 TCP Acceleration

We employ automatic Hybla, Westwood, Tahoe, Reno, proprietary and OILA Congestion Algorithms as part of the FastApn service. TCP Hybla and Hybla-i protocol addresses both the issues of satellite and high RTT links. Hybla-i combines TCP Hybla to solve the problem of high RTT's, and TCP Westwood to solve the high link error rates. These continuously calculate bandwidth used by the connection, algorithm is then used to set the

congestion window when packet loss occurs. Other Algorithms are automatically selected based on the connected network performance.

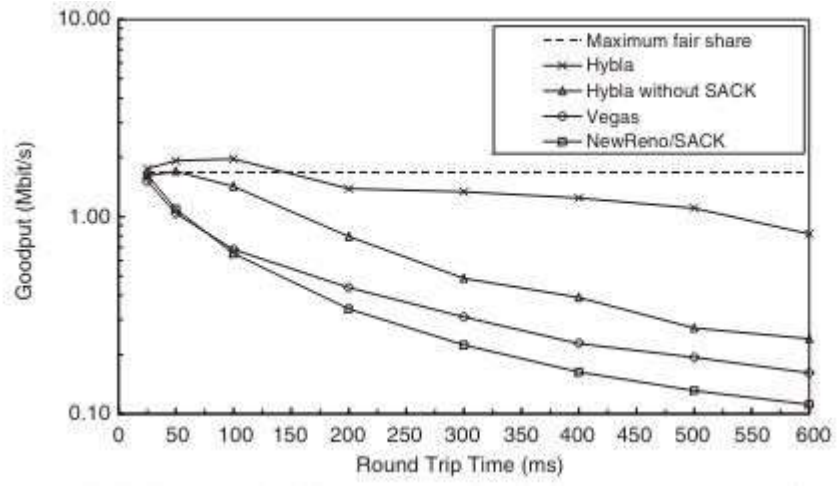


Figure 5: Performance of different TCP versions in the presence of congestion

4.7 SmartAVdns Option

SmartAVdns is a proprietary option that enables a location service with an additional level of bad traffic detection, and can place functionality is any global location, such as the carriers headquarters base country.

SmartAVdns works in the same way as normal DNS servers but with a redirection functionality. When you visit certain websites, the service reroutes your DNS requests to the FastApn SmartAVdns clusters and replaces the location data in your request with location information from its DNS server.

SmartAVdns doesn't assign a new IP address like a VPN does, but it changes how websites see your IP address. For example, you may be browsing in the UK, but connected to a German SmartAVdns server. Your DNS requests are redirected through German proxy servers rather than local ones before reaching the website's servers. This means the website thinks you're accessing the site from Germany.

4.8 Multipath Kernal

We deploy the Multipath MPTCP Kernal. Enabled Multipath TCP (MPTCP) is an effort towards enabling the simultaneous use of several IP-addresses/interfaces by a modification of TCP that presents a regular TCP interface to applications, while in fact spreading data across several sub flows. Benefits of this include better resource utilization, better throughput and smoother reaction to failures. MPTCP has broken the record for the fastest TCP connection ever – 51.8 Gbit/second with Multipath TCP was achieved.

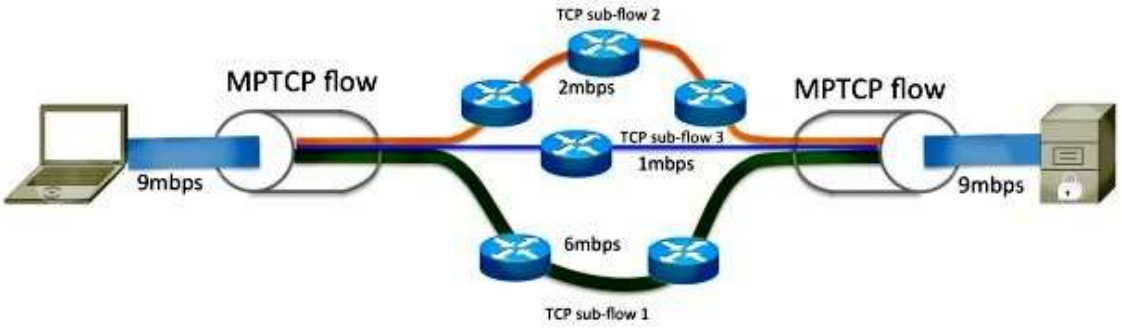


Figure 6: TCP Multipath flow within the FastApn Kernal

5 FastApn Web Administration GUI

5.1 System Remote Access Overview

For system users of any size, you can choose to have direct access into your FastApn management system, noting that the device is unique to you and not a shared resource, this also allows the ability for root user access in a shell, where you can choose to use the resource for any purpose reflecting your operation, as an example, an information portal promoting your services. The direct management system access is not available to PED's (Passengers / End Users), although pax will be accessing your resource only whilst on your network(s). We do have PA (Public Access Servers) for users that require persistent access across all networks globally.

5.2 Node Dashboard

The Dashboard presented on login depicts a real time view of your system operation, showing defined parameters such as Total Queries, Blocked Queries, Percentage

Blocked and the size of the dynamic DAL's. This is followed by a graphical presentation of queries and blocks over 24 hours, as well as client activity, split into system access, for example, aircraft types or locations dependent on IP or MAC.

Also shown ore the types of queries broken down into A, AAAA, SRV, PTR, TXT. SVCB, HTTP and HTTPS records and Upstream DNS servers where traffic lookups are made after being analyzed, . plus, blocked and cached lookups. In addition, Top Lists with counts are shown for Permitted domains, Blocked Domains, Clients and Blocked Clients.

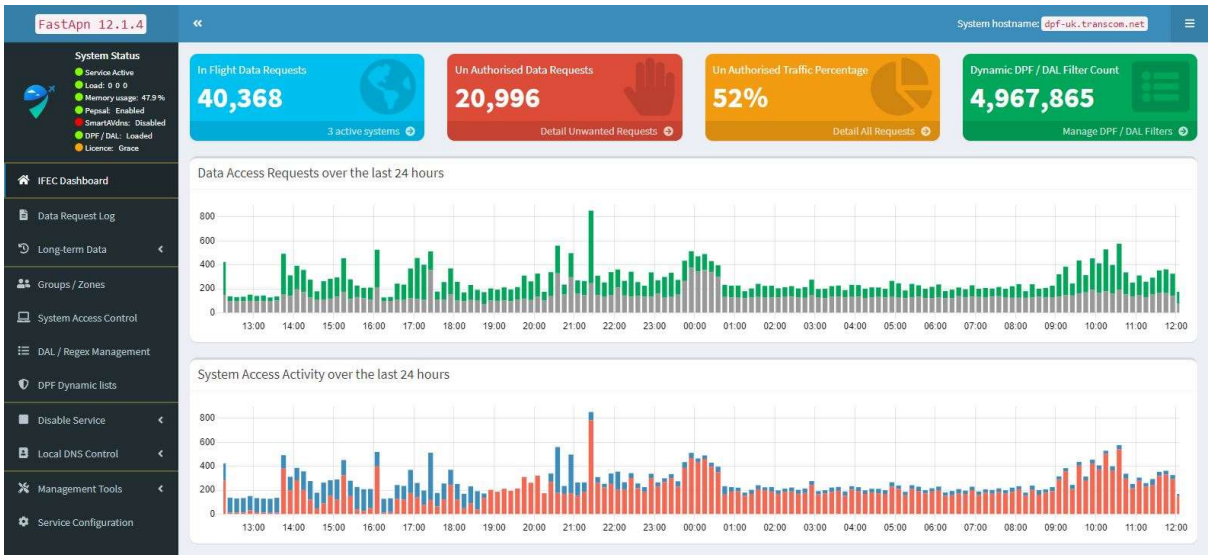


Figure 7: Main Dashboard view including side menu

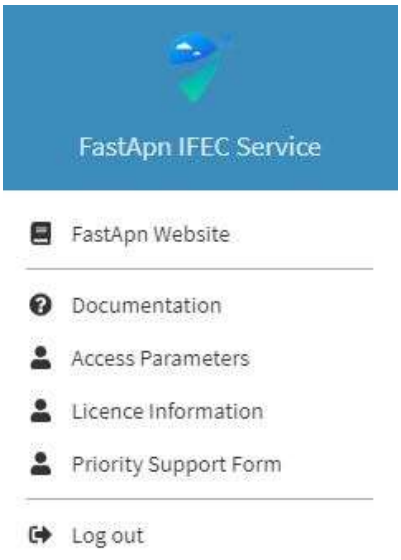


Figure 8: FastApn Information Menu

FastApn node information can be found from the dashboard main page, top right bars, detailing your unique and necessary parameters to configure any type of device, your license key and what it allows, and a support form that can be used for:

- reporting an issue
- making a change request (CR)
- configuration assistance
- DPF and DAL changes including Regex

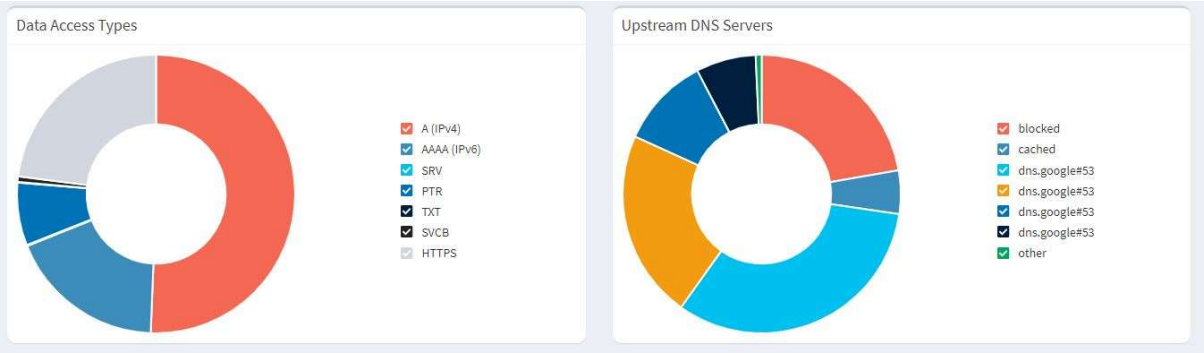


Figure 9: Pie chart showing Port access and Upstream DNS servers

Top Permitted Access

Domain	Hits	Frequency
www.linkedin.com	1221	
gateway.fe2.apple-dns.net	477	
lb._dns-sd._udp.0.7.168.192.in-addr.arpa	442	
lb._dns-sd._udp.126.147.237.10.in-addr.arpa	437	
lb._dns-sd._udp.atria1200.mesh	431	
lb._dns-sd._udp.6.0.0.192.in-addr.arpa	427	
gb-courier-4.push-apple.com.akadns.net	369	
logsink.devices.nest.com	345	
ntp-g7g.amazon.com	280	
fos5echocaptiveportal.com	274	

Top Un Authorised Access

Domain	Hits	Frequency
gs-loc.apple.com	1260	
eu-teams.events.data.microsoft.com	392	
app-measurement.com	369	
api.smoot.apple.com	355	
dns.google	292	
e.reddit.com	290	
d3p8zr0ffa9t17.cloudfront.net	284	
catalog.gamepass.com	277	
people-pa.googleapis.com	262	
firebaselogging-pa.googleapis.com	238	

Figure 10: Table of Permitted Access lookups and unauthorised Access

Top System Access (total)

Client	Requests	Frequency
05BBBC49.unconfigured.pool.telekom.hu	29635	
trvpn-uk.transcom.net	1002	
simon-vpn.transcom.net	561	
master.privatevpn.uk	338	

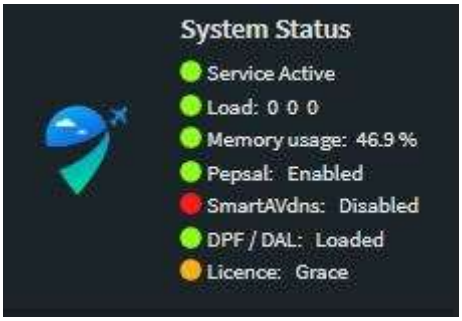
Top Un Authorised Access (blocked only)

Client	Requests	Frequency
05BBBC49.unconfigured.pool.telekom.hu	6440	
trvpn-uk.transcom.net	342	
simon-vpn.transcom.net	299	
master.privatevpn.uk	134	

Figure 11: Total system access and blocked access tables

5.3 Node Status

Dashboard top left shows your unique ID, Logo, Fleet or aircraft registration, followed by system status, Load counts (Unix style), Pepsal status and DPF / DAL operations, memory usage and license status.



5.4 Requested Data Log

The query log shows time and date stamped queries with DNS record type, originating domain, the client system that accessed the FastApn device, the status either showing forwarded approved lookups or blocked with details, a reply timing and process, i.e., IP or CNAME and a blacklist / whitelist switch

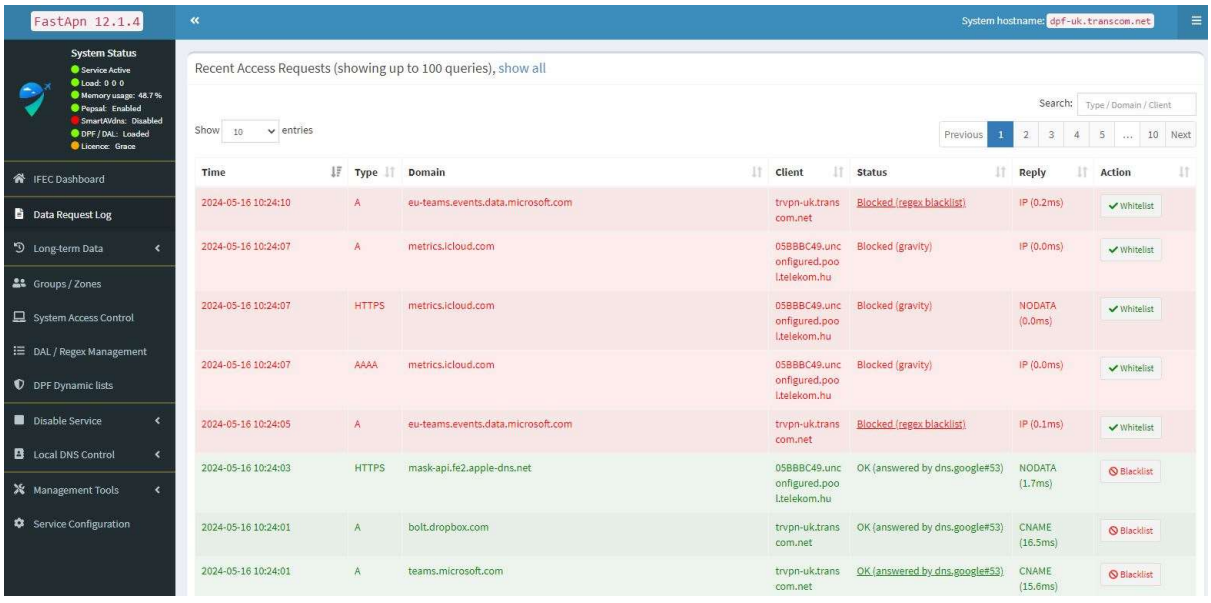


Figure 12: Data Request Log showing Permitted and Blocked Access

5.5 Long Term Data Statistics

Graphical Display

Searchable statistics with presets from today to all time plus a custom range

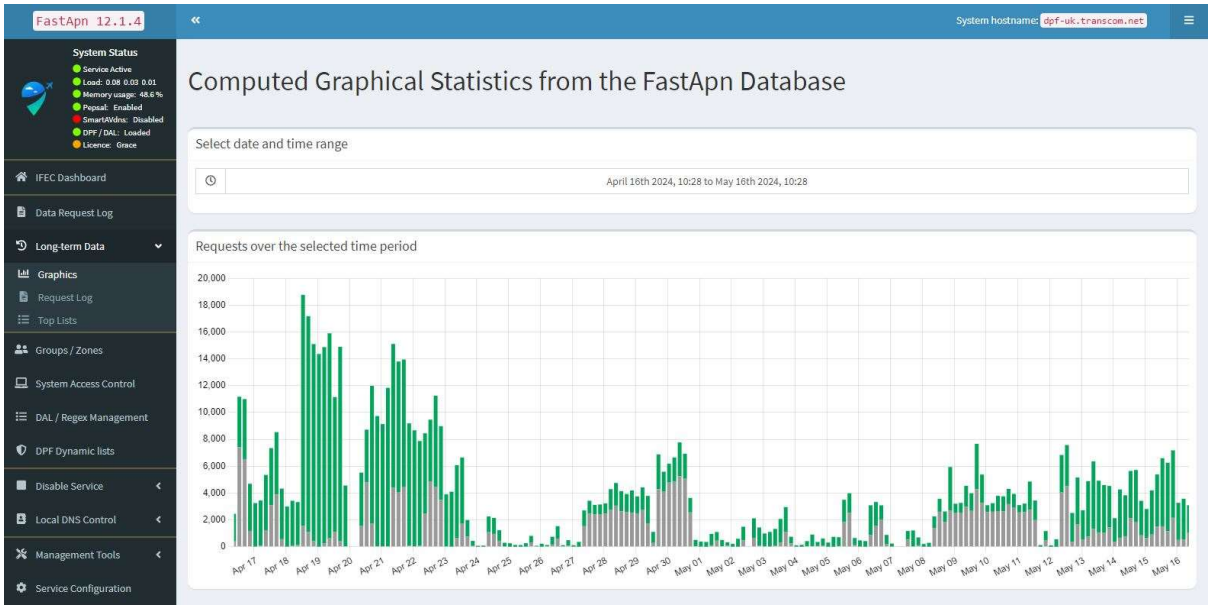


Figure 13: Long term statistical Data in graphical format

5.5.1 Query Log

Searchable statistics from the query log with 13 presets from permitted to Blocked by Regex with preset and custom times

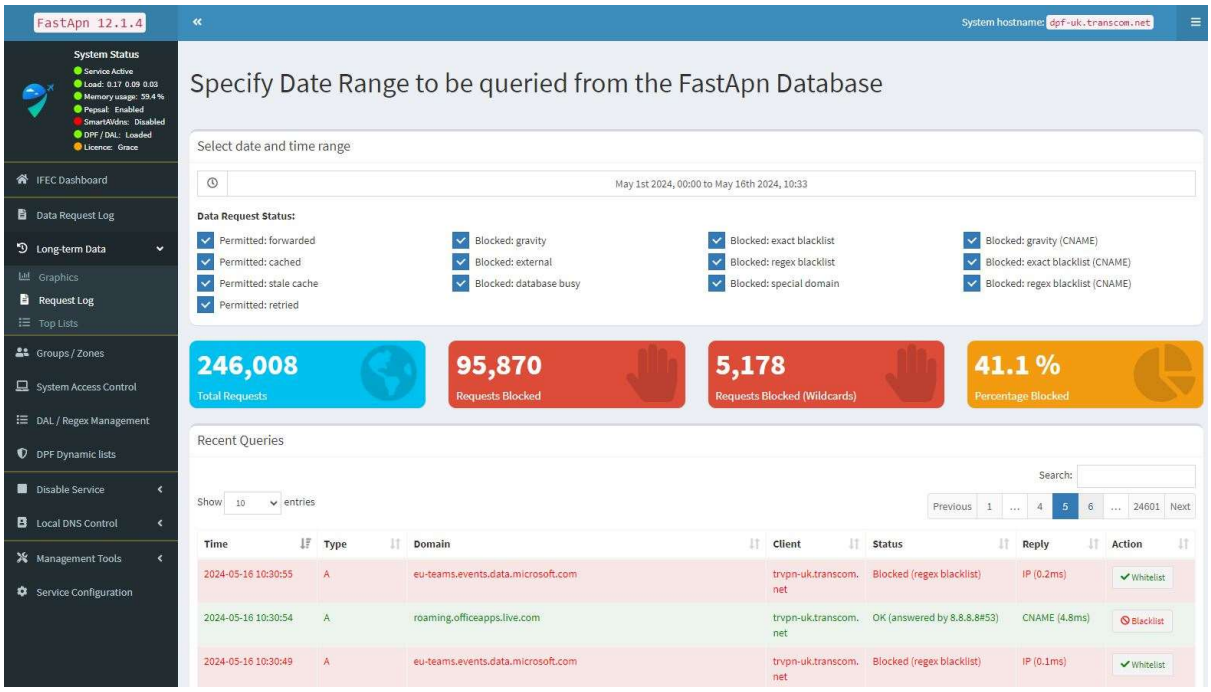


Figure 14: Selectable long term data access statistics

5.5.2 Top Lists

Searchable statistics with presets from today to all time plus a custom range showing top domains, top blocked and top client's systems.

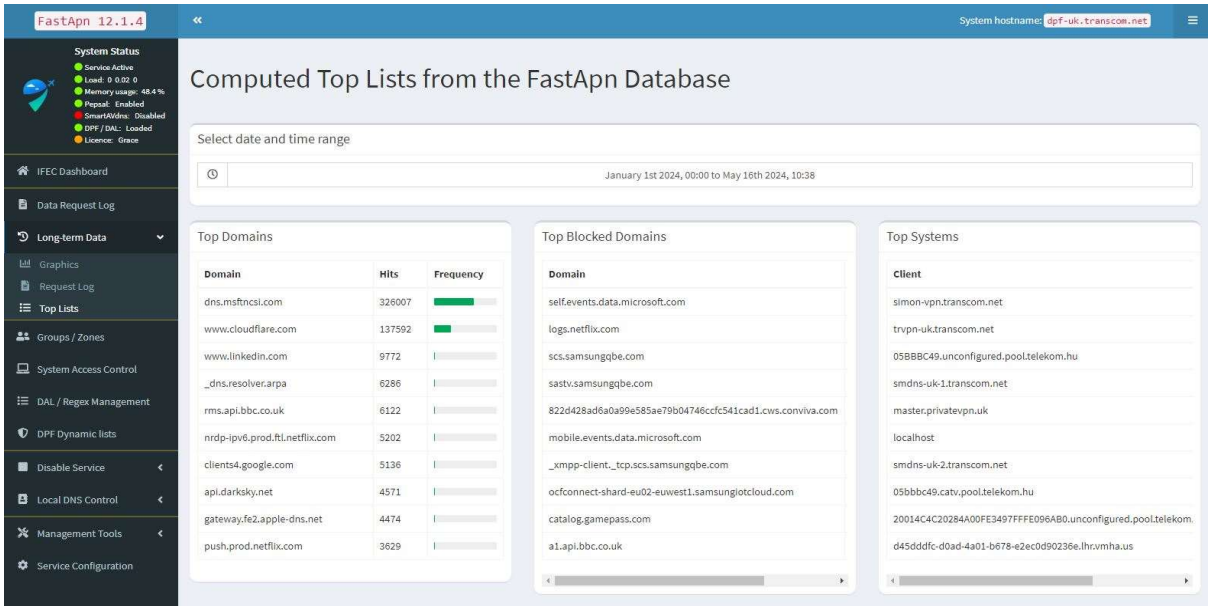


Figure 15: Long term top lists statistics for Permitted, Blocked and System Access

5.6 Node Group Management

Fully customizable Group management that can be anything from destination zones, aircraft types, equipment type, access devices and even services. DAL's and DPF's can be applied per group

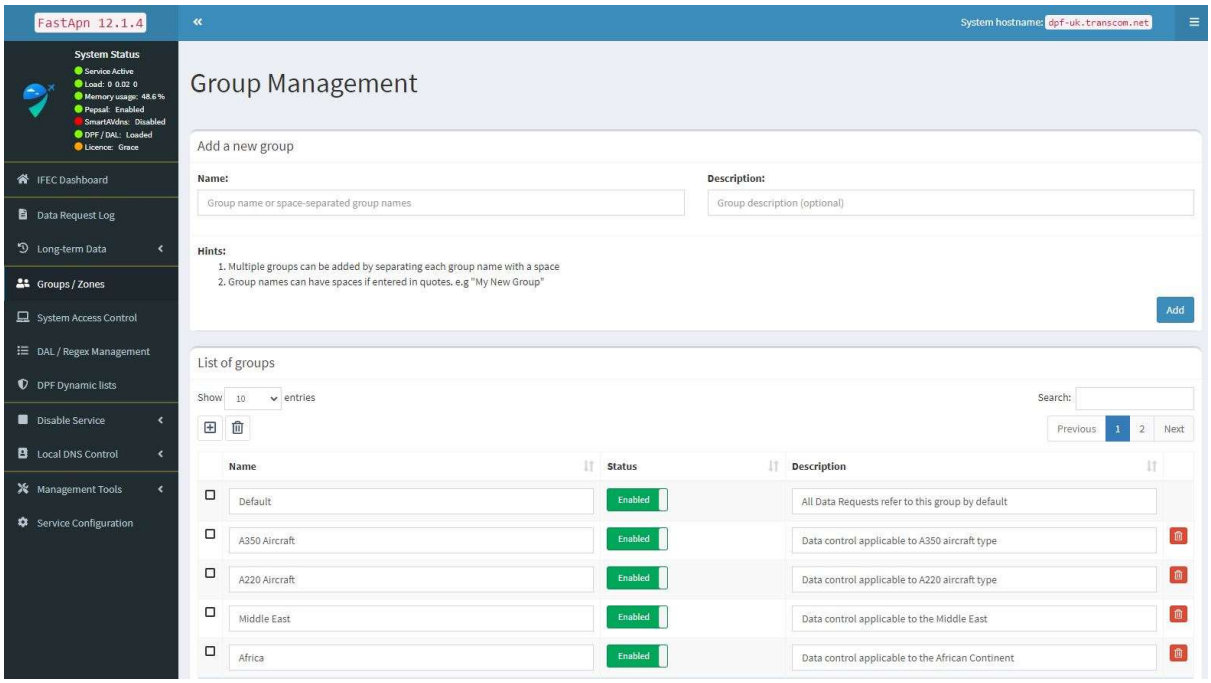


Figure 16: Group and Zone Generation

5.6.1 Group - System / Device Access

Systems may be described either by their IP addresses (IPv4 and IPv6 are supported), IP subnets (CIDR notation, like 192.168.2.0/24), their MAC addresses (like 12:34:56:78:9A:BC), by their hostnames (like localhost), or by the interface they are connected to (prefaced with a colon, like :eth0). Systems can be added to Groups for further processing, and node ACL (Access Control Lists) as well as firewalls can be configured.

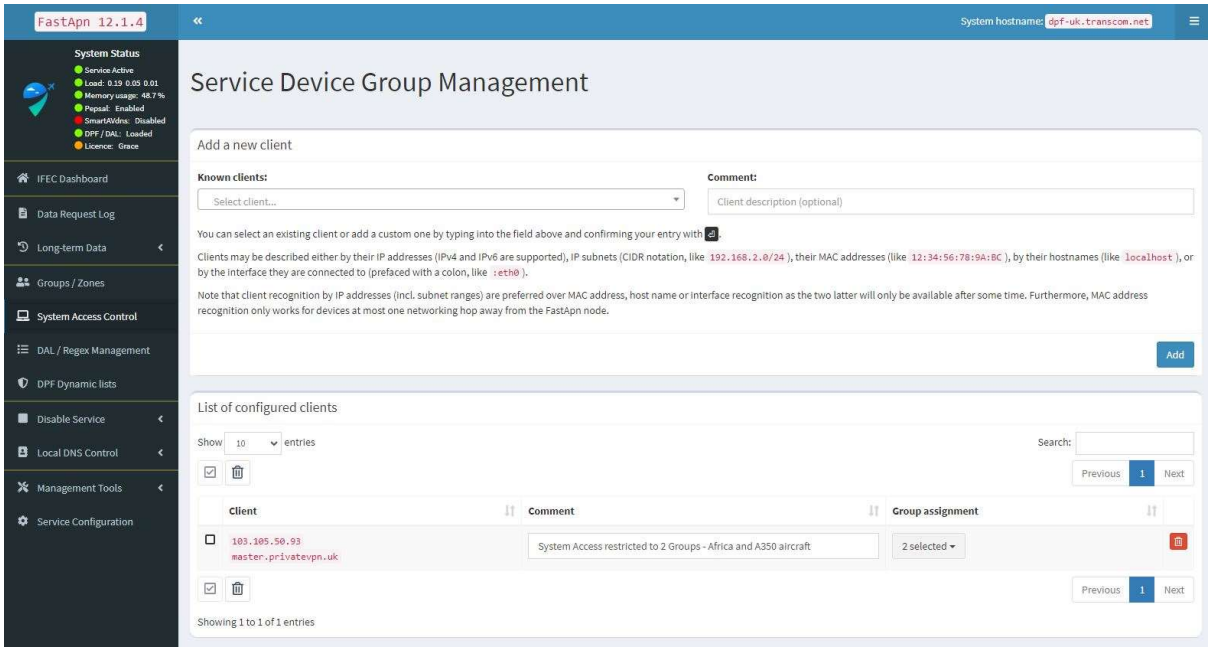


Figure 17: Group Assignment showing systems attached to Groups

5.6.2 Group - Direct Domain Management

Domains and all sub parts can be added here for the purpose of whitelisting or blacklisting, they can also be assigned to groups. Theres an automatic option to involve all subdomains, in which case the system will convert the entry into a standard Regex code. Domains can also be enabled / disabled and deleted.

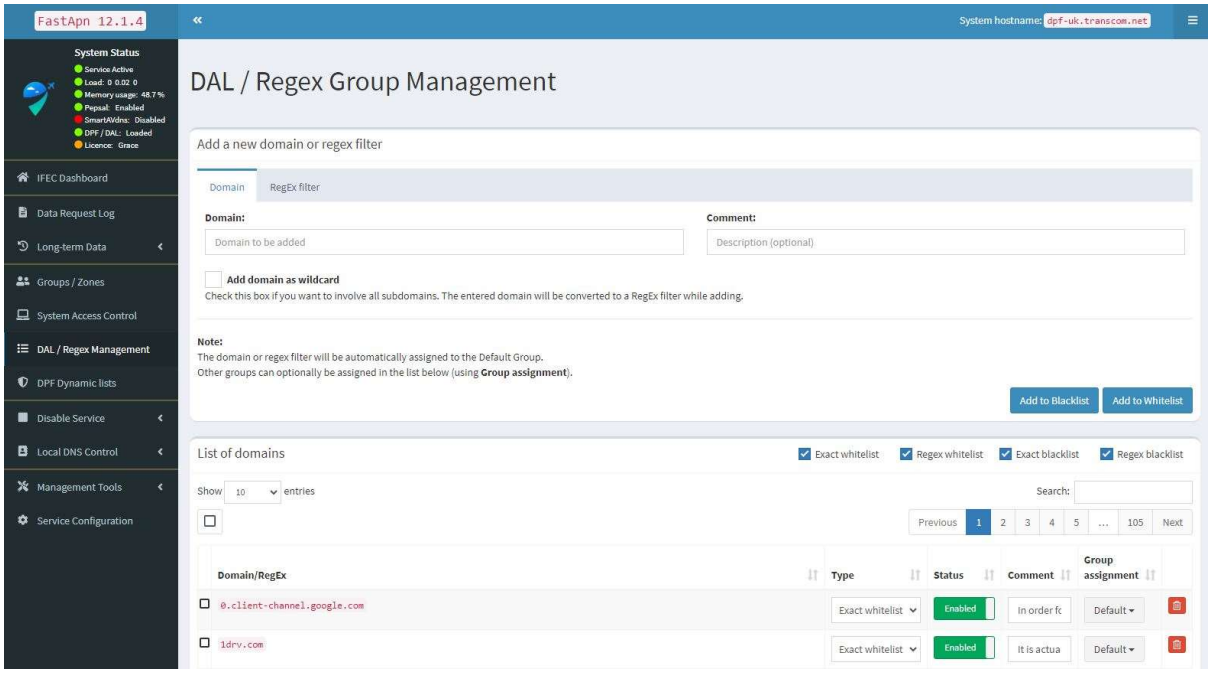


Figure 18: Group Assignment showing URL attachment to Groups

5.6.3 Group - DAL's and DPF Management

Within this section you will find listed all your blocklists, either predefined, and supplied by us, or your own lists, clicking on each will show the raw flat file format. From here, lists can be enabled / disabled and assigned to groups, as well as ability to delete the entire list. You can add as many lists as you wish through this interface. The example structure in the figure below is taken from our public nodes.

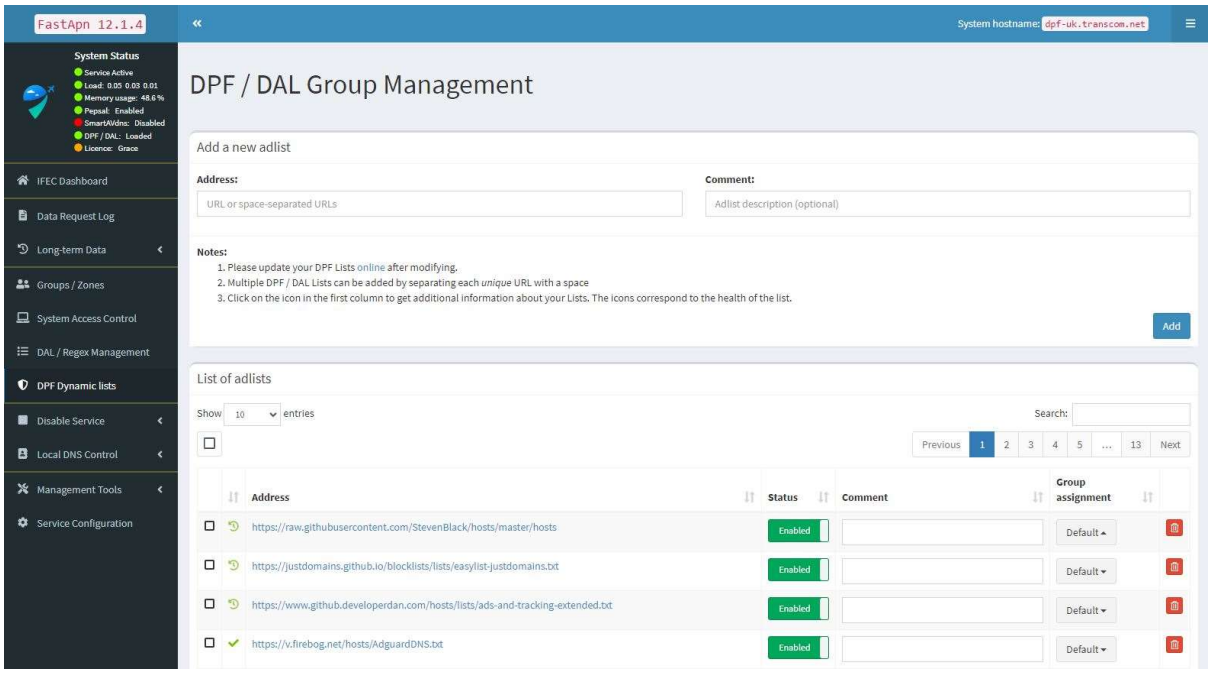
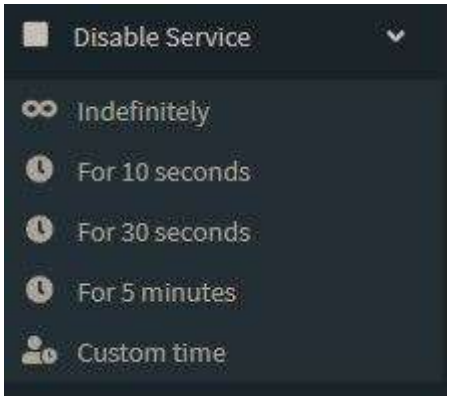


Figure 19: Deep Packet and Domain Block list example (taken from our public nodes)

5.7 Blocking Controls

From here, blocking and detection can be disabled from 10 seconds to indefinitely, or a custom time entered



5.8 Local DNS

5.8.1.1 DNS Records

Local DNS entries can be locally defined to prevent remote lookups, domains can be entered individually for by comma separated list, associated IP is required.

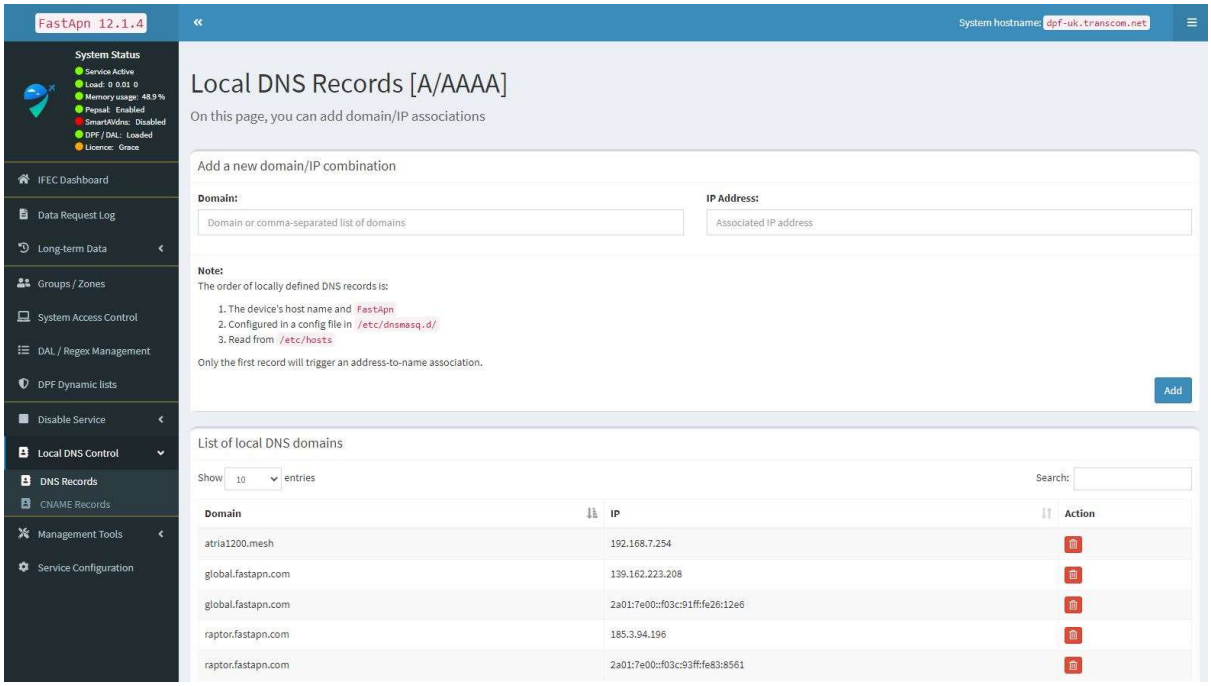


Figure 20: Local DNS configuration

5.8.1.2 CNAME Records

The target of a CNAME must be a domain that FastApn already has in its cache or is authoritative for. This is a universal limitation of CNAME records.

The reason for this is that FastApn will not send additional queries upstream when serving CNAME replies. As consequence, if you set a target that isn't already known, the reply to the client may be incomplete. FastApn just returns the information it knows at the time of the query. This results in certain limitations for CNAME targets, for instance, only active DHCP leases work as targets - mere DHCP leases aren't sufficient as they aren't (yet) valid DNS records.

Additionally, you can't CNAME external domains (bing.com to google.com) successfully as this could result in invalid SSL certificate errors when the target server does not serve content for the requested domain.

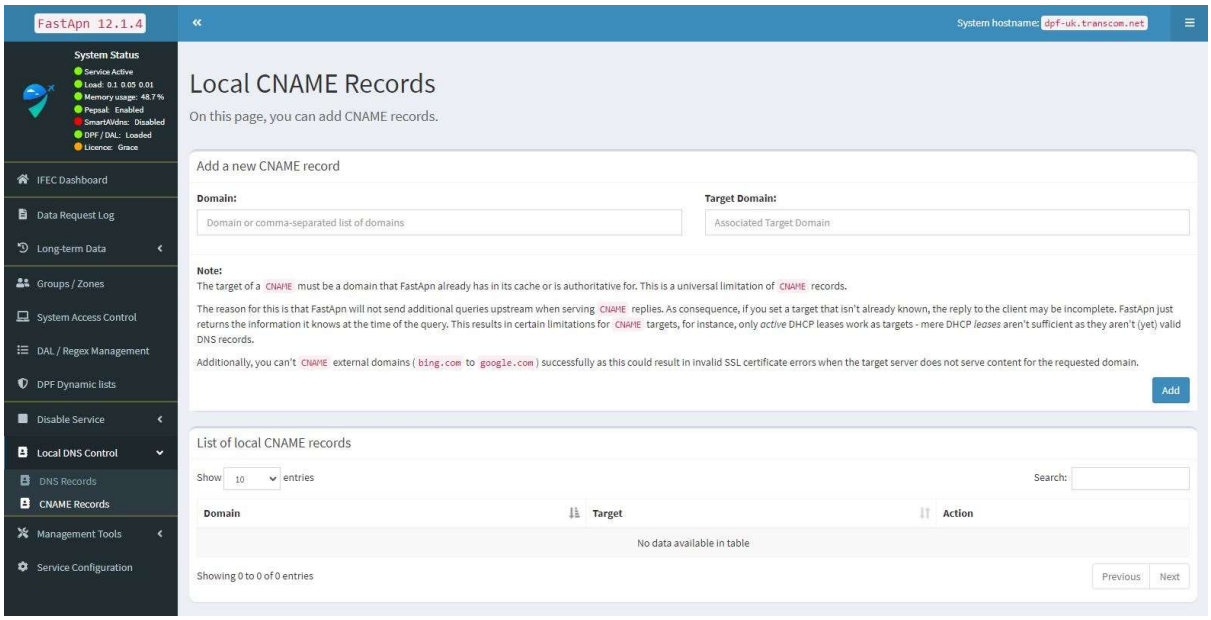


Figure 21: Adding CNAME records to the system

5.9 Management Tools

5.9.1 Dynamic List Updates

Online facility for manually triggering Data Access Blocking list updates, these are normally carried out automatically, but manual is available, and will show any real time issues with any lists format.

```
[i] Target: https://blocklist.sefinek.net/generated/0.0.0.0/forks/phishingArmy.phishing_army_blocklist_extended.txt
[√] Status: Retrieval successful
[√] Parsed 203516 exact domains and 0 ABP-style domains (ignored 0 non-domain entries)
[i] List has been updated

[i] Target: https://blocklist.sefinek.net/generated/0.0.0.0/forks/RPiList-Phishing.txt
[√] Status: Retrieval successful
[√] Parsed 264103 exact domains and 0 ABP-style domains (ignored 0 non-domain entries)
[i] List has been updated
```

Figure 22: DPF Blocklist update example

5.9.2 Blocklist Search

If a problem domain is listed in any number of lists, this search facility will advise, it's good for tracking problematic domains.

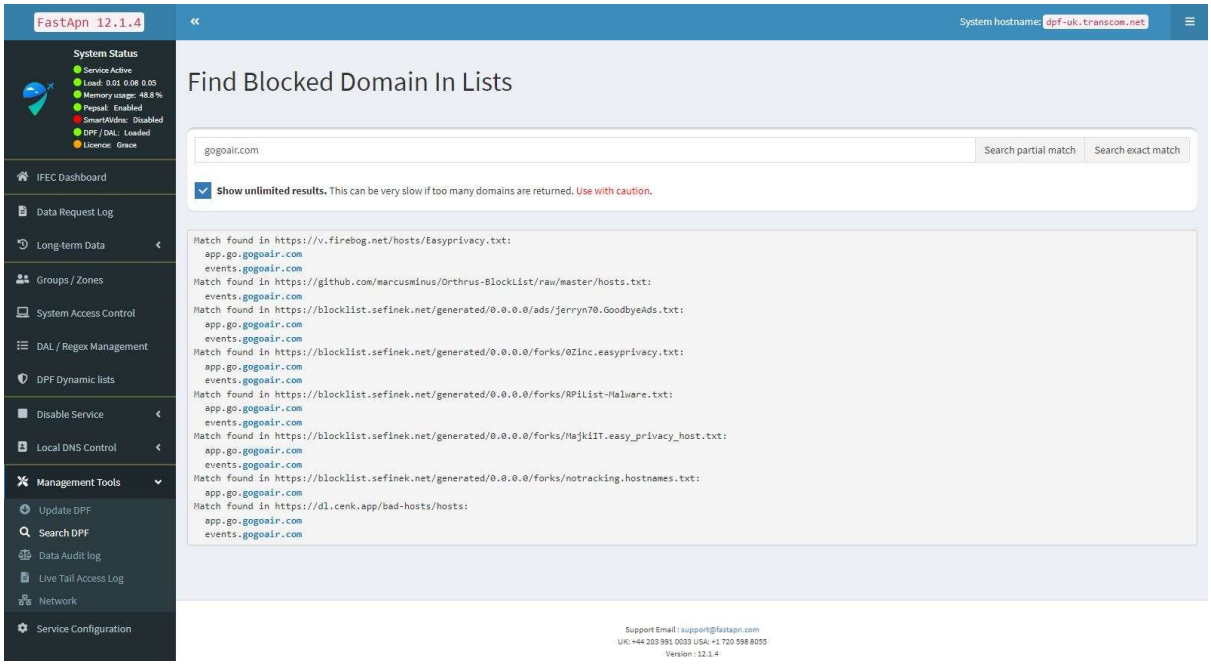


Figure 23: Blocklist search for specific Domains or part of

5.9.3 Audit Log

The running Audit log will allow you to backlist / whitelist and Audit high roller domains. The audit allows you to mark high counting domains as ‘aware’, and stop them from showing up in logs.

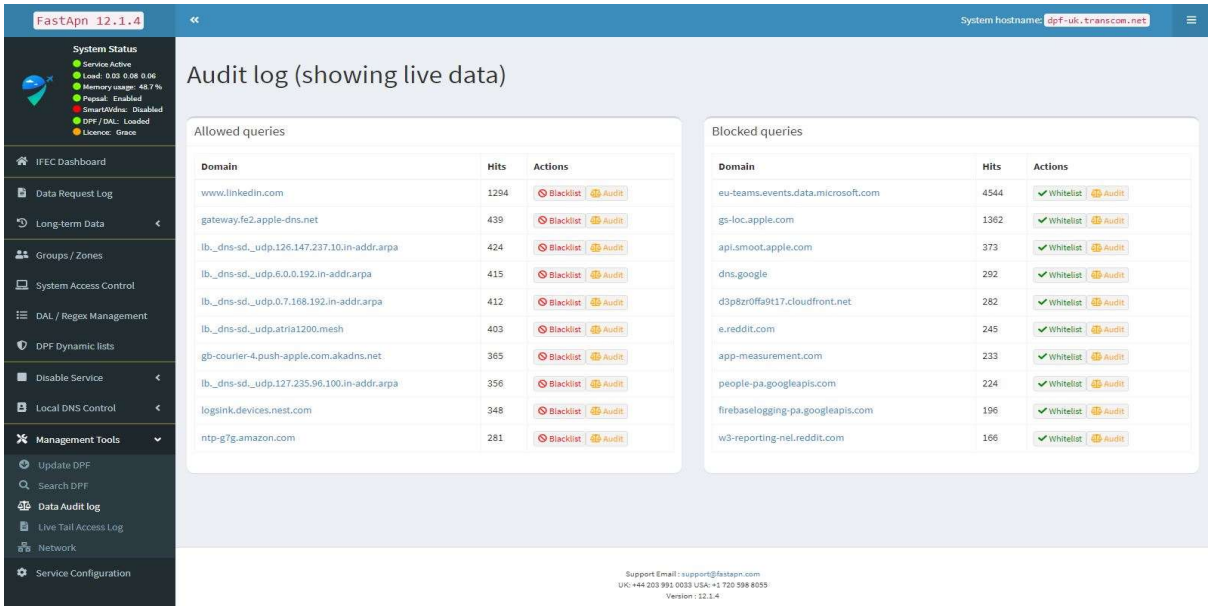


Figure 24: FastApn Audit Log live data tables

5.9.4 Tail Access Log (real time)

Since FastApn will log all Data Access Requests by default, use this command to watch the log in real-time, showing both valid and invalid requests.

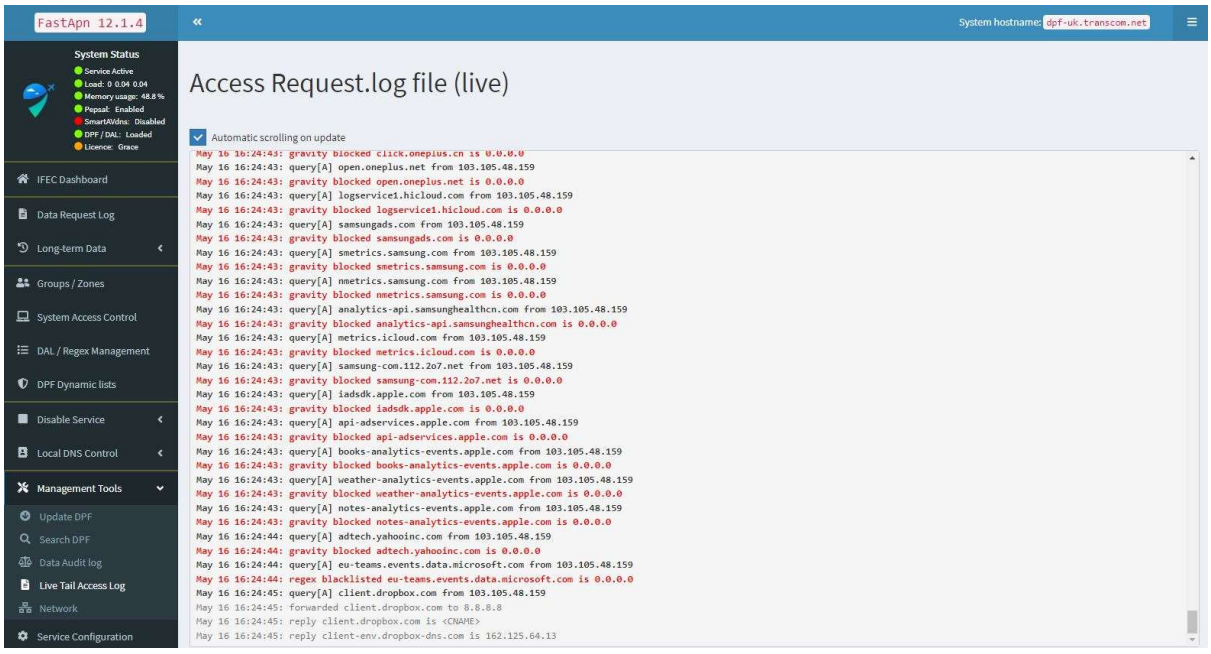


Figure 25: Live tail Data Access Log - Public Node sample shown

5.9.5 System Access Network

From here you can monitor and remove system access to your FastApn Node, this shows all IP's that have attempted or are authorized to use your system, including complex grouping and zoning. Also shown is the hardware address, Interface, Hostname, first seen, last request, number of requests and Action to take (i.e. delete)

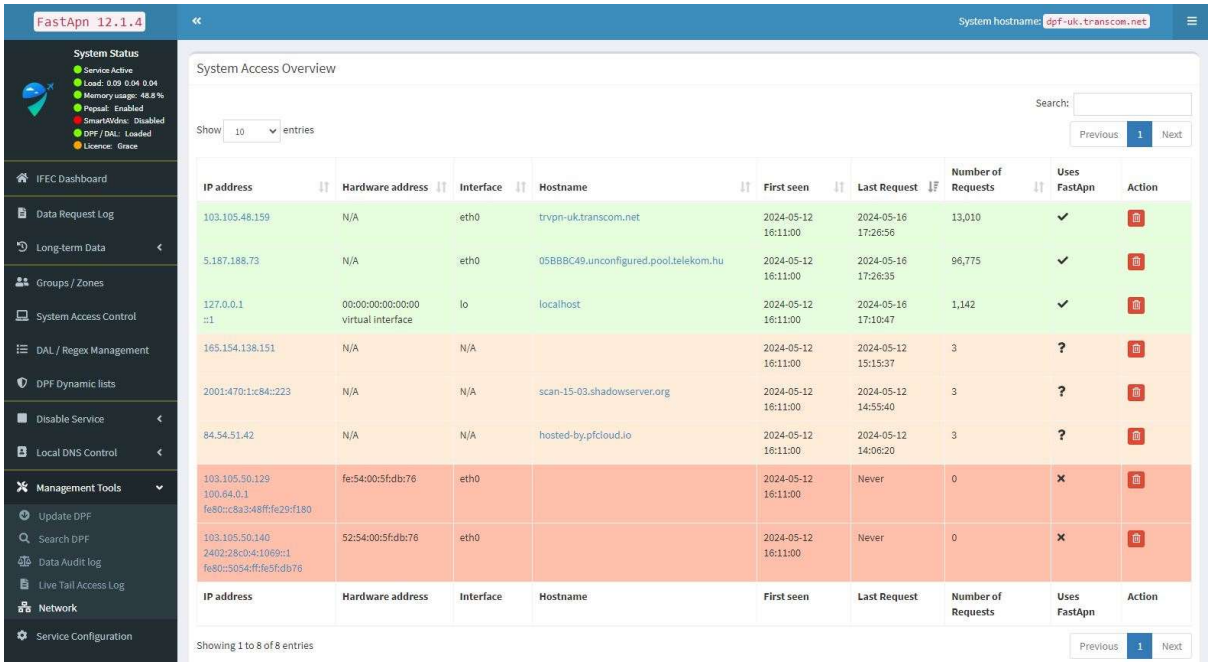


Figure 26: System Access to a FastApn Node

5.10 System Settings

5.10.1 Configuration Overview

The last sidebar menu item is for system configuration, noting that the default provided is adequately configured to utilize all of its modules and methodologies, there is little need to change any parameters, however, there may be options that your particular network would need.

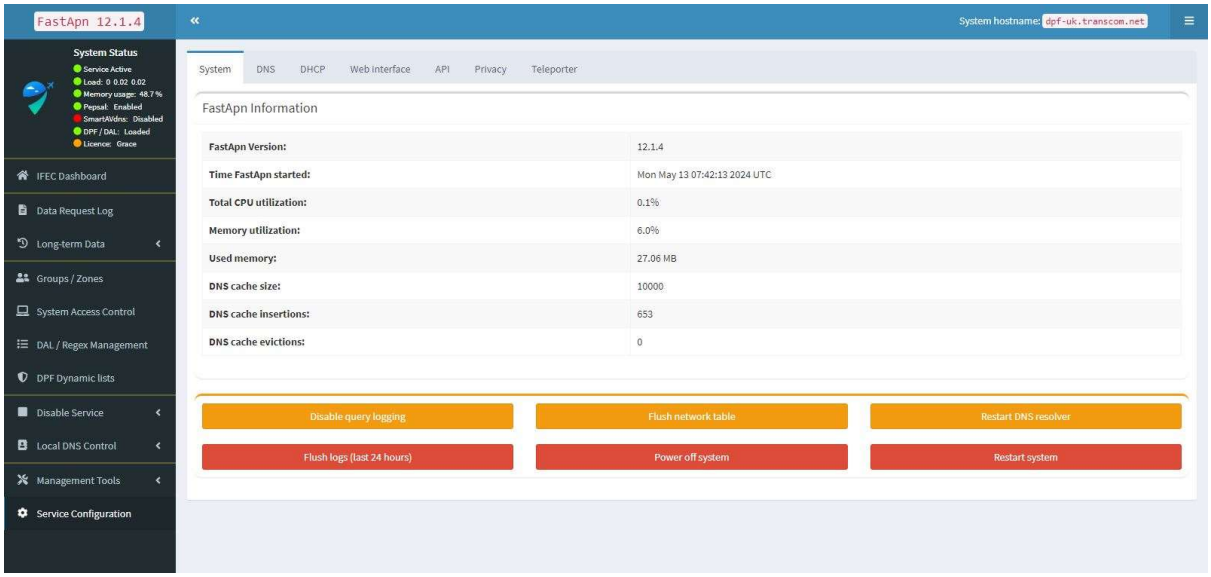


Figure 27: FastApn Node Configuration overview

5.10.2 System Information

Provides the running information and status of your node, including versioning, start time, CPU and memory load, DNS size, insertions and evictions.

There are also 6 operating options:

- Disable Logging
- Flush Network Table (Device Access)
- Restart DPF Resolver (DNS)
- Flush Logs
- Power the system off
- Restart the system

5.10.2.1 DNS Up Stream Configuration

From here you can choose your upstream DNS configuration, these are the DNS servers that will handle requests that have been checked for validity, and we have included 9 mainstream DNS providers:

- Google
- OpenDNS (Cisco)
- Level3
- Comodo
- DNS Watch with DNSSEC
- Quad9 (filtered DNSSEC)
- Quad9 (unfiltered no DNSSEC)
- Quad9 (filtered ECS, DNSSEC)
- Cloudfare (DNSSEC)
- Unbound option (self-recursion)

Note: ECS (Extended Client Subnet) defines a mechanism for recursive resolvers to send partial client IP address information to authoritative DNS name servers. Content Delivery Networks (CDNs) and latency-sensitive services use this to give geo-located responses when responding to name lookups coming through public DNS resolvers. *Note that ECS may result in reduced privacy.*

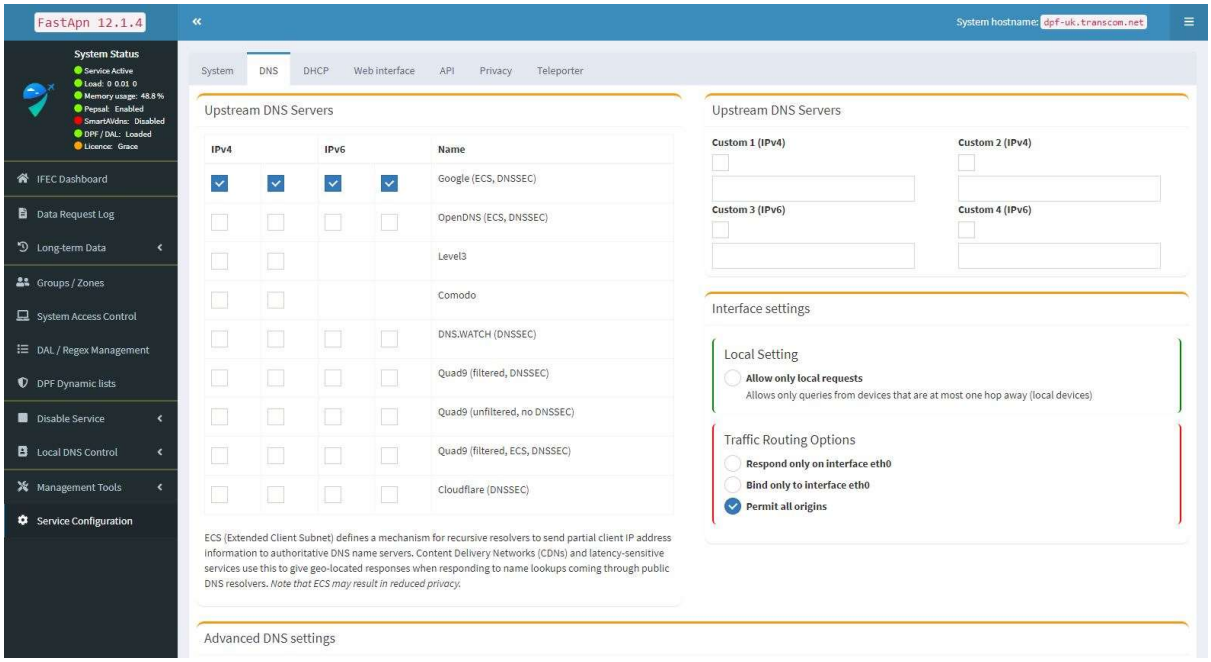


Figure 28: DNS Upstream Configuration - (Unbound Fully Recursive available)

5.10.2.2 Custom Upstream DNS

You can also choose to use your own set of DNS servers, there are four custom IP's that can be set, 2 for IPv4 and 2 for IPv6, please remember to allow recursion from the IP of your FastApn server. On request, you can also choose to use FastApn as your Unbound recursive DNS servers.

5.10.2.3 Traffic Routing Options

Within this section we also have configuration options that manage the interface, this is dependent on where your FastApn server reside. As example, if using as a DHCP server, you would only need local requests as the server would be within your network, however, for most scenarios, the permit all origins is set within the Traffic Routing options, and access is controlled simply by an Access Control List and simple firewall (i.e. UFW / IPTABLES), which we configure in advance

5.10.2.4 DNS Advanced Settings

Under Advanced Settings, there are options for forwarding, reverse lookups, DNSSEC, Rate Limiting and Conditional Forwarding, these options are rarely set unless it's an external network management decision

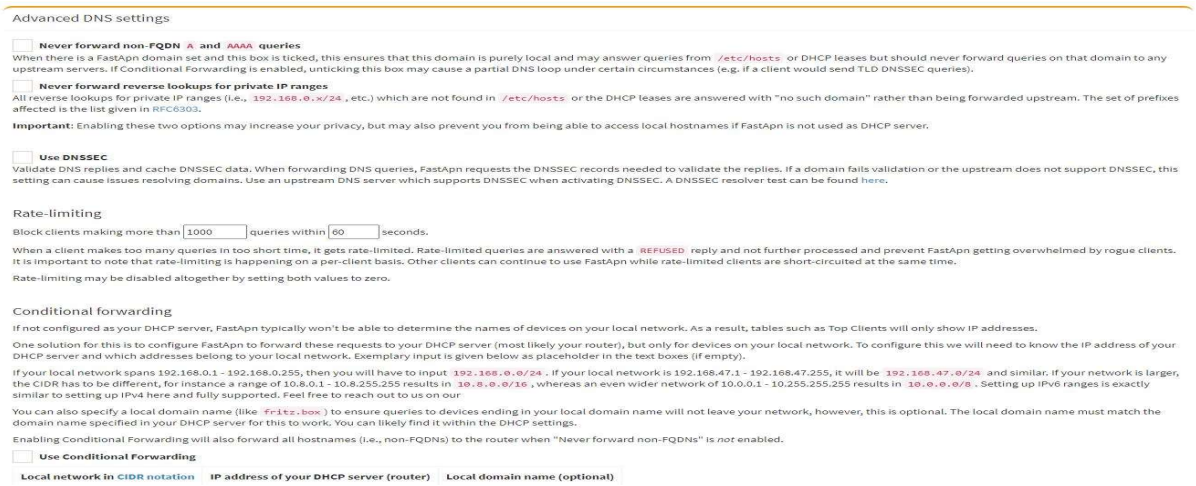


Figure 29: DNS Advanced Configuration

5.10.3 DHCP and Lease Settings

If you have chosen to host a FastApn node within your own network, here you will find all options fro managing the DHCP configuration, including the private address blocks, gateway addressing, lease times and options for SLAAC and IPv4 rapid commit.

Once activated, the system will show all active DHCP leases including MAC address, IP address and Hostname.

Should you wish to assign static addressing to MAC, this option is also available here, noting that specifying the MAC address is mandatory and only one entry per MAC address is allowed. If the IP address is omitted and a host name is given, the IP address will still be generated dynamically and the specified host name will be used.

If the host's name is omitted, only a static lease will be added.

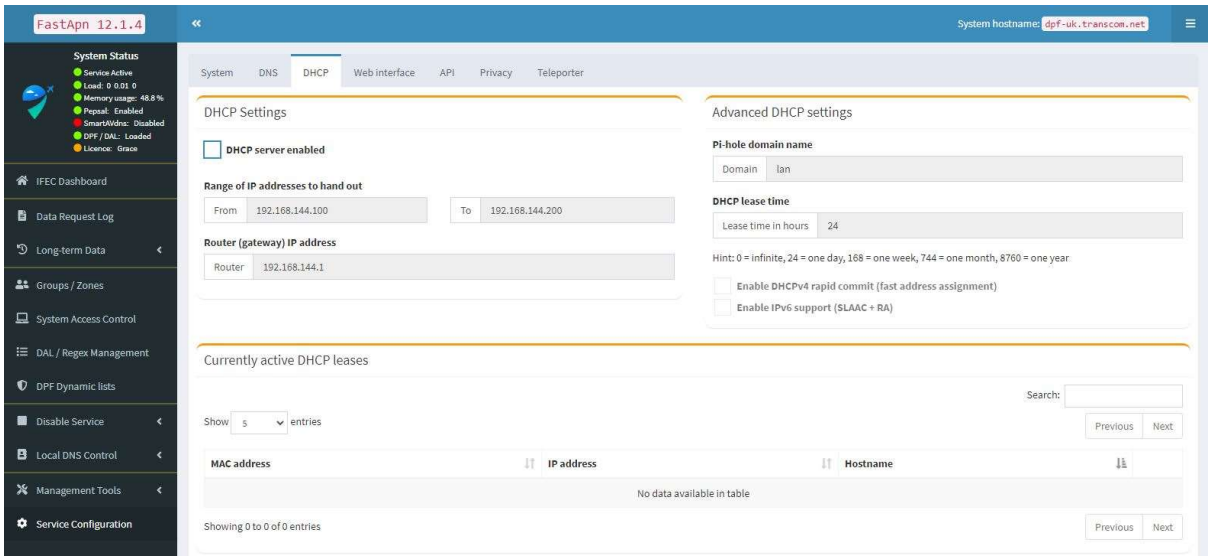


Figure 30: DHCP Configuration including active leases

5.10.4 Web Interface

Full administration and configuration is through the web interface, you will be assigned and node FQDN and can access the GUI on any web browser, which is also Bootstrap 5 compliant, so that it is fully usable on any mobile device.

There are six selectable themes to suit all tastes and environments and a boxed layout for very large screens.

Also, under the GUI settings we have Global for server temperature support, button styles (50), bar chart styles, query log colours and the option to hide non-fatal warnings from the logs.

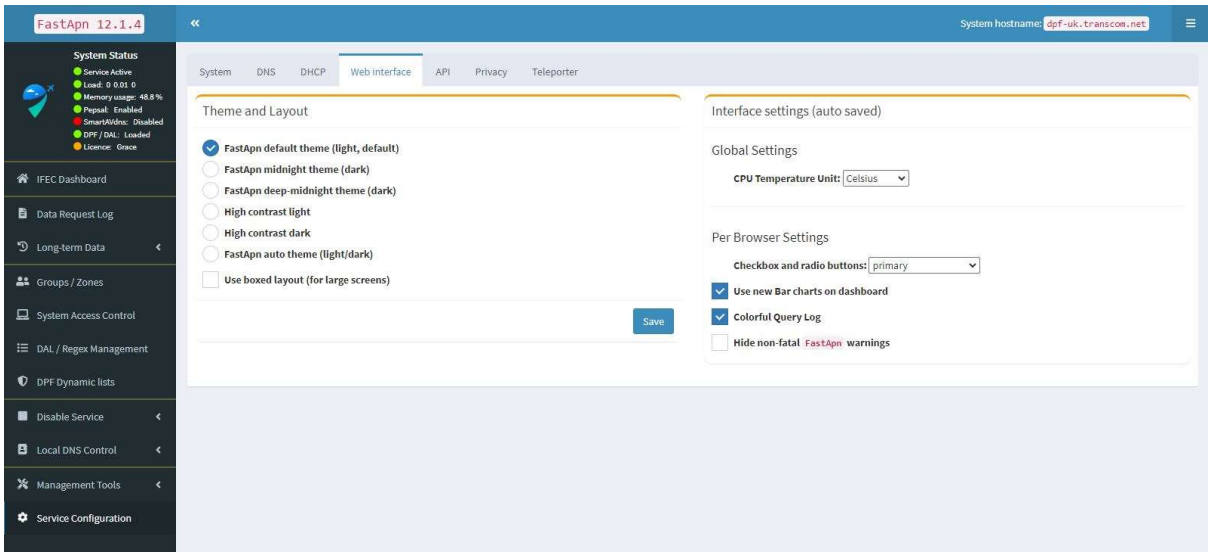


Figure 31: FastApn Web Administration GUI configuration

5.10.5 FastApn API

The service comes with a capable API, full description and parameters can be found in the Advanced section in this document. From the GUI you can use the GUI to enter domains that you do not wish to be shown in the many of the statistical logs and / or top lists, including system access by devices. This enables more clarity where some devices (like windows) have persistent ‘alive’ calls.

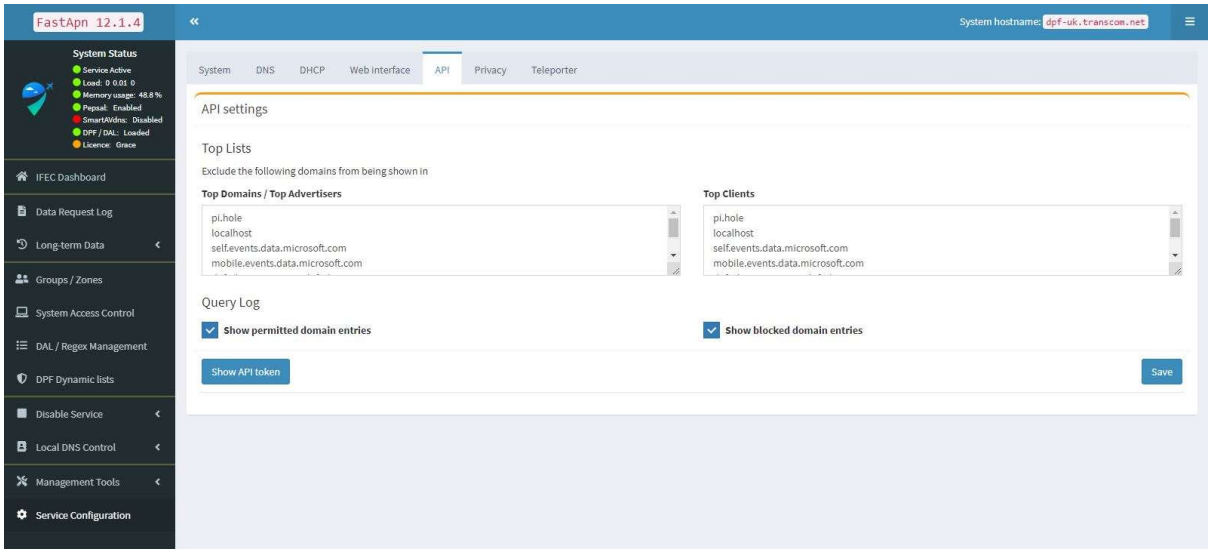


Figure 32: API Exclusions for known and unknown entities

5.10.6 Service Privacy

By default, the service records, logs and shows all activity, but you can choose to restrict this information in levels, right down to just anonymous statistics. This option may be required by some company policies.

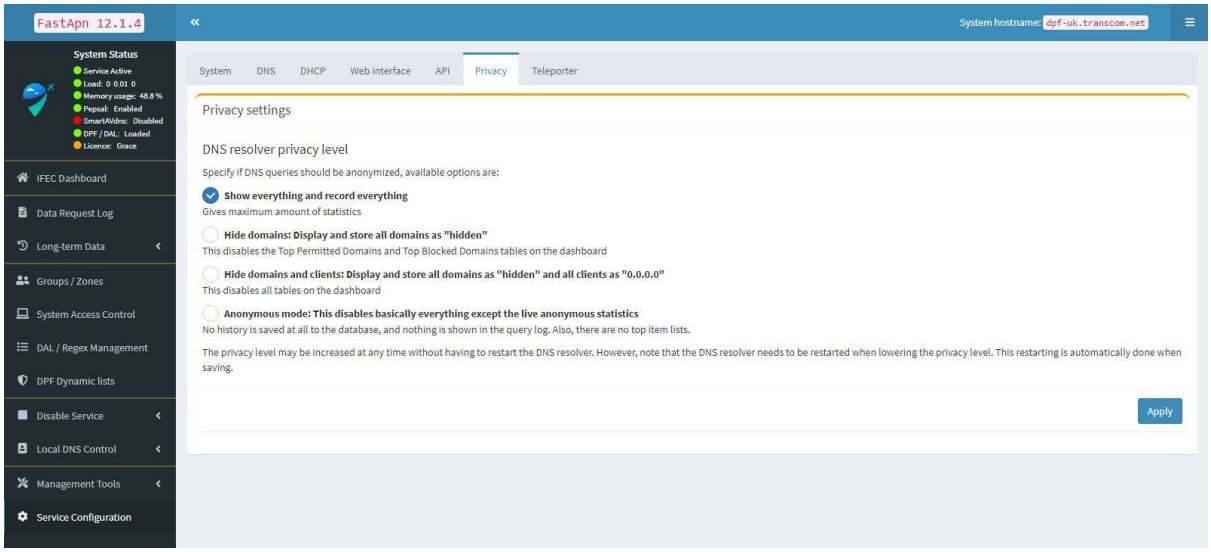


Figure 33: FastApn Node Privacy Settings

5.10.7 System Teleporter

The FastApn teleport allows you to backup and restore your node configuration, including 11 selectable options in relation to your dynamic and / or customized flat files and DNS records. Making it ideal for or adding duplicating FastApn nodes.

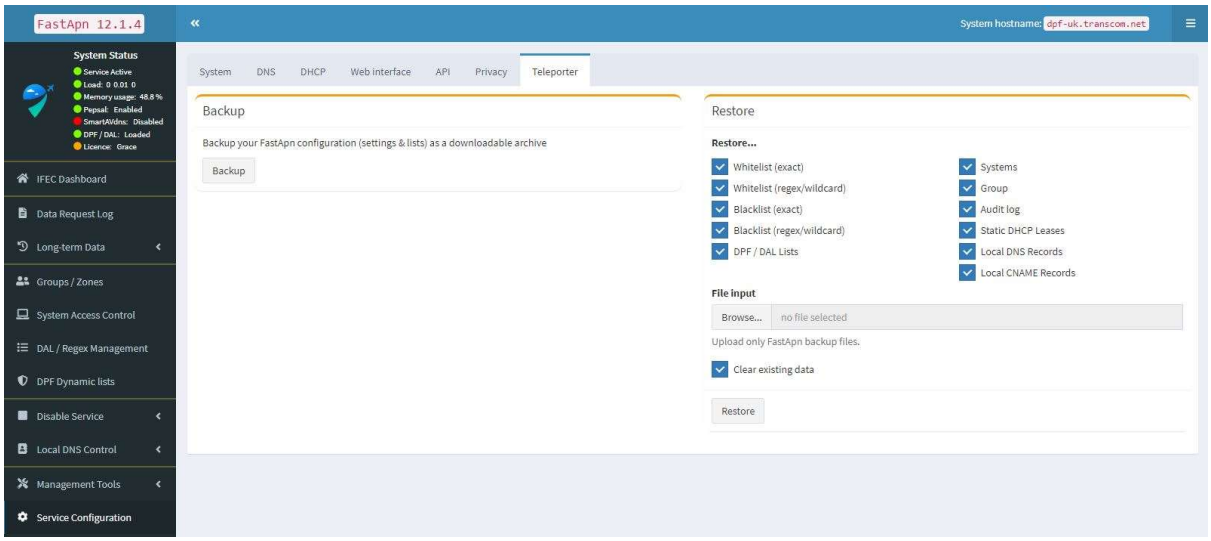


Figure 34: System and Backup Archiving and selectable Data Restoration

6 Service Activation

6.1 End User Devices (PED's)

As defined by the NIST, a PED is an electronic device having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to: pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders.

There are two areas of operation for PED's for In Flight Access, one being devices that are part of the aircraft on board equipment, such as provisioned iPads, and PED's that are carried by the PAX.

In the first option, the DNS setting for the FastApn service can be pre-configured, in the latter, it's the choice of the PED owner to configure the DNS to use the on-board service, or to use our public FastApn servers where access can be 24/7.

6.1.1 iPhone / iPad DNS

Note that where operators have chosen to configure the FastApn service further down the line, such as within WAP's, Cores or the associated ground network, there is of course no need to configure PED's.

1. Tap on Wi-Fi.
2. Tap on "i" next to the connected Wi-Fi name or any other Wi-Fi.
3. Tap on Configure DNS.
4. Tap on Manual → Add Server.
5. Next, type the issued FastApn DNS server IP (x.x.x.x)
6. Finally, tap on Save

6.1.2 Android DNS

Note that where operators have chosen to configure the FastApn service further down the line, such as within WAP's, Cores or the associated ground network, there is of course no need to configure PED's.

1. Tap settings
2. Network & Internet
3. Advanced
4. Private DNS
5. Enter your issued FastApn DNS hostname
6. Click Save

6.1.3 PC / Laptop DNS – Wi-Fi or Ethernet

Note that where operators have chosen to configure the FastApn service further down the line, such as within Waps, Cores or the associated ground network, there is of course no need to configure PED's.

1 Left click on your Network icon
2 Select Network and Internet settings
3 Click change adapter options
4 Double click on the Wifi or Ethernet interface
5 Select Properties
6 Double click on TCP/IPv4 to edit its properties
7 Click Use the following DNS server address
8 Enter the issued FastApn IP as the Preferred DNS server
9 Click OK to finish

6.1.4 MAC DNS – Any Network Profile

Note that where operators have chosen to configure the FastApn service further down the line, such as within WAP's, Cores or the associated ground network, there is of course no need to configure PED's.

1. Choose the Apple Menu
2. Select system preferences
3. Select Network
4. Click a Network profile (WLAN / LAN)
5. Click Advanced
6. Select DNS from the tabs
7. Click + to add a new DNS server
8. Enter the issued FastApn IP / hostname

6.1.5 FastApn Proxy Connectivity – PED's

The FastApn service can also be added to any device as a proxy, thereby effectively routing all traffic through an external gateway, where additional security, access lists

and all the FastApn capabilities can be used, monitored and tracked, either by default OS software, or by third party software such as Proxifier or the built-in configuration or third-party plugins made for several browsers.

6.1.5.1 Any Browser Proxy (all devices)

All browsers have the ability to enter a proxy configuration, normally found under the specific browser settings. In addition, you can use the same parameters in any proxy configuration service, program or application, on any device.

Chrome also has an excellent Extension called Switch Omega for configuring and selecting Proxy's to use on the fly.

Our Nodes are fully Dynamic, so they operate transparently in all segments such as EMEA, AMER, or APAC, depending where you currently are. This is also ideal for localising your device for streaming or another local requirement (UK or USA) using the optional SmartAVdns.

6.1.5.2 System Wide Proxy (PC / MAC)

Many OS including Windows 10, now have the ability to set a System Wide Proxy to divert all your device traffic though a proxy service. Simply head over to your Network and Internet settings, and select Proxy.

From here you have two choices, either enter the proxy information manually or use a script, we have provided both for you below.

6.1.5.3 Win / MAC Proxy with Portable USB

By far the most popular option for the FastApn service is a portable USB stick, simply carry it around or put the files on a micro-USB and leave it plugged in at all times, there are 4 profiles with automatic geo access to all nodes.

Note that using this method, ALL traffic from your device and applications will be accelerated and processed.

We recommend and supply Proxifier, it comes with a 30-day free trial. Get the USB version from Proxifier and unzip it onto any USB drive, then download the ready-made Profiles and unzip onto the same drive. To use, simply plug in the USB drive, open to view files and hit connect.

A small graph icon will appear by your clock on the task bar, right click to use the profile options as well as stats and graphs if needed

6.1.5.4 Win / MAC Proxy Installed (Proxifier)

Although it's not a necessity to run the FastApn service from installed software, it can be done with many off the shelf products. As with the portable device, we prefer Proxifier and maintain profiles for it, for ease of installation.

Note that using this method, ALL traffic from your device and applications will be accelerated.

Download the Proxifier version you require (links below) , and upload our readymade profiles into the Proxifier profile directory, profiles can also be imported via the application.

6.1.5.5 iPhone / Android Proxy (Internal)

The iPhone already contains an option for use with our service, and it's very easy to setup. Goto settings, Wi-Fi, and then select the 'i' symbol that is on the right-hand side of your Wi-Fi connection. Scroll down and select configure proxy, then select manual.

1. Tap on Wi-Fi Connection
2. Tap on "i" next to the connected Wi-Fi name or any other Wi-Fi.
3. Scroll down to the HTTP Proxy section and choose Configure Proxy.
4. Tap on Manual Configuration.

5. Provide proxy details – server and port
6. Provide Authentication as issued by FastApn when subscribed
7. Finally, tap on Save

Note that using this method, ALL traffic via wifi from your device and applications will be accelerated, but not for 4G, please use the application method below if you require 4G as well.

Our Nodes are fully Dynamic, so they operate transparently in all segments such as EMEA, AMER, or APAC, depending where you currently are. This is also ideal for localising your device for streaming or another local requirement (UK or USA).

6.1.5.6 iPhone / iPad Proxy with Application

As a free option, you can install a small application that is preconfigured, making it very easy for you to switch the FastApn service on and off without any configuration changes. The app link is below, and contains no advertising and is free of charge.

On initial setup, open the app, click '+' to add a new node, then enable, and under PAC URL, enter the URL below, press save, that's it. To use, simply click the app (a funnel icon) and enable the service. This application can also be used to switch between all of our nodes on the fly.

Note that using this method, ALL traffic from your device and applications will be accelerated, this includes 4G / 5G and Wi-Fi, and is one button selectable

6.1.6 FastApn VPN Connectivity – PED's

Devices classified as PED's (Personal Electronic Devices) , virtually all have the ability to use a VPN incorporated in their core software, this makes it extremely easy to connect to the FatApn service with the minimum of fuss, just add the VPN hostname as shown below, and service activation will be immediate.

6.1.6.1 iPhone / iPad VPN

8. Tap on Wi-Fi Connection
9. Tap on “i” next to the connected Wi-Fi name or any other Wi-Fi.
10. Scroll down to the HTTP Proxy section and choose Configure Proxy.
11. Tap on Manual Configuration.
12. Provide proxy details – server and port
13. Provide Authentication as issued by FastApn when subscribed
14. Finally, tap on Save

6.1.6.2 Android VPN

1. Go into your Android settings.
2. Click Network & Internet.
3. Click Advanced.
4. Select VPN.
5. Click the plus sign.
6. Enter in your FastApn provided information.
7. Click Save.

6.1.6.3 Mac VPN

1. On your Mac, choose the Apple menu
2. Select System Settings
3. Then click VPN in the sidebar. (You may need to scroll down.)
4. If you’re using an L2TP VPN and need to switch to a different configuration, click the Info ‘i’ button on the right, click the Configuration pop-up menu, choose a configuration, then click OK
5. Turn on the VPN service you want to connect to.

6.1.6.4 PC / Laptop VPN

1. Select Start > Settings > Network & internet > VPN > Add VPN.
2. Under Add a VPN connection, do the following: For VPN provider, choose Windows (built-in). In the Connection name box, enter a name you'll recognize (for example, My Personal VPN).
3. Fill in VPN details provided by FastApn
4. Select Save.

6.2 Routing Hardware

6.2.1 Device Overview

Local routing devices that connect two or more packet-switched networks or subnetworks, serving two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router. Devices include airborne equipment such as WAP's (Wireless Access Points) , general AP's (Access Points).

6.2.1.1 LAN Segments - DNS

To change the Primary or preferred DNS to FastApn on any routing device, simply identify the LAN settings in the menu and enter the issued FastApn IP address, noting that once completed, all devices connected to this LAN will automatically utilize the FastApn service, so there is no need to modify any PED.

6.2.1.2 WAN Segments – DNS

Alternatively, you can identify the WAN setting on any router, and follow the same procedure as the LAN, noting that all LAN's and all associated PEDS will be able to utilize the FastApn service, so there is no need to modify PED's or LAN segments

6.2.1.3 Core Hardware - DNS

Central processing devices including routers that summarily combine inputs to form a single trunk for transmission / reception, these include core routing services such as ACPU (2Ku system) and other central management devices

In some systems, there may be several routing devices in the network chain, so for maximum utilization, the device furthest back in the chain should be used, this is identified as Core Hardware, and can be the first Network device or router, such as the 2Ku ACPU or the Satcom Direct SDR

6.2.1.4 Ground Services - DNS

In the case of fleet management or ground-based segments controlling a large number of systems, the FastApn service DNS provisioning can be carried out on any routing device right back to the backhaul connectivity, thereby addressing every local and aircraft system, and therefore every LAN device and associated PED's

6.2.2 FastApn Proxy Connectivity – LAN / WAN / CORE / GROUND

Nearly all devices have the ability to add a proxy, this includes most routers and inflight hardware, all Android and iPhone OS, and, right down to all PC Laptops, Macs and even browsers. Our proxy service runs on port :7478, and each client is issued with a unique ip for access. We also have end user global dynamic access

via proxy for persistent device use including small routers and BGAN systems, access of which is protected by a user / pass combination.

Operators using the proxy method of system access do not need to make any DNS changes, as this is automatically called from within the proxy services

6.2.3 FastApn VPN Connectivity – LAN / WAN / CORE / GROUND

Many devices have the ability to add a VPN, this includes most routers and inflight hardware, all Android and iPhone OS, and, right down to all PC Laptops, Macs and even browsers. Our VPN access can be by any protocol and authentication by ACL's or common eser / pass combination.

We also have end user global dynamic access via VPN for persistent device use including small routers and BGAN systems, access of which is protected by a user / pass combination.

Operators using the VPN method of system access do not need to make any DNS changes, as this is automatically called from within the proxy services

6.2.4 FastApn DHCP Connectivity - LAN / WAN / CORE / GROUND

The FastApn service can also be accessed by DHCP, which means the service will automatically assign an IP and connect any number of users to the system and hence online. To enable this, the server would need to be placed within the network concerned (either manually or virtually), whether in airborne or ground segments, noting that only one DHCP server can be operational at the same time on the same network. The server has all the built-in capabilities to assign the main router and private IP blocks.

Operators using the DHCP method of system access do not need to make any DNS changes, as this is automatically part of the server when using DHCP.

7 Appendix A – Service Addressing

7.1 Authentication

Public node access always needs username and password authentication, where as operator BareMetal nodes can choose many authentication methods from user / pass, ACL to a Firewall. The Web GUI always requires a password unless the operator incorporates a node (as DHCP) within their own private network.

7.2 Access Format

global-px12.fastapn.com:7673

Public access for connection by proxy, cluster bank 12 on port 7673. Some devices will require this format whilst others will have a separate space for adding the port and user / pass authentication. Specific public location servers are also available and, in these instances, global will be replaced by the location name, i.e., dallas-px14.fastapn.com

global-vl09.fastapn.com

Public access for connection by VPN, the 'l' represents the VPN type (note lower case). VPN clients are built into all PED's and most routing devices and require only authentication by user / password. IPSEC will have a separate entry for the Tunnel Password.

- L = L2TPD
- S = L2TPD / IPSEC
- K = L2TPD / IKEv2
- P = PPTP
- O = OpenVPN
- W = Wire Guard

Global indicates that this connection is public (shared resource), where as a defined customer name denotes a private FastApn node, i.e.:

- luftdpf.fastapn.com
- fastapn-de.luftdpf.com

7.3 DNS Access

Hostname	<as issued>. fastapn.com	IPv4 and / or IPv6
IPv4	123.056.217.081	Example > Use issued IP4 address

7.4 Proxy Access

Hostname	<as-issued>. fastapn.com:7673	Port 7673 for Ground / IFEC Bypass
IPv4	123.056.217.081:**7673**	Example shown by IP
Hostname	<as-issued>.fastapn.com:7478	Port 7478 for Ground + IFEC
IPv4	123.056.217.081:**7478**	Example shown by IP
iPhone	https://<as-issued> fastapn.com/preset/<as-issued>**.pac**	

7.5 VPN Access

Hostname	<as-issued>.fastapn.com	IPv4 and / or IPv6
IPv4	123.056.217.081	Example > Use issued IP4 address
Tunnel	Password if used / required	Example, IPSEC

7.6 DHCP Access

If you are using the FastApn service by DHCP, you will have placed the server within your operating environment either directly or virtually, and configure the access address block within the server as required. DHCP will automatically issues any hosts connection with an IP. The client connected list can be seen within the FastApn server settings.

7.7 Web Admin GUI

Access to the Administrative Web GUI is by standard browser URL, an SSL certificate will have been installed using your dedicated IP and chosen hostname.

Web GUI	https://<as-issued>.fastapn.com/admin/
Domain Name	We can add a specific domain, A / AAAA records and CNAME

8 Appendix B – Test Access / Global Nodes

8.1 FastApn Test Access

We have deployed a global FastApn service for test and trial access, fully loaded with all the latest standard DPF and DAL files as well as Pepsal's and TCP Acceleration / Congestion Management modules.

The test systems can be accessed as follows:

DNS Hostname	dpf-uk.fastapn.com (request access)	
or…		
Proxy	gt-px.fastapn.com Port 7673/7478	Flight / Ground
VPN (L2TP/IPSEC)	gt.vp.fastapn.com	Flight / Ground
Username	**flight**	
Password	**linktest**	

Note: Test server access restricted by time per session by proxy, you will be prompted to re-enter login details every 10 minutes.

8.2 FastApn Public Nodes

For continuous access with a dedicated operator barebone system, you can choose to use our clusters of public nodes, where we maintain the latest dynamic blocking controls and system management. Access is by subscription services from daily to annually, and by device count and network mask.

The public systems can be accessed as follows:

DNS Hostname	dpf-uk.fastapn.com	(request access)
or		
Proxy	global-px12.fastapn.com Port 7478/7673	Flight / Ground
VPN (L2TP/IPSEC	global-vs09.fastapn.com	Flight / Ground
Proxy iPhone	https://fastapn.com/global.pac	
Username / Password	As issued when subscribed	
Public Access Pricing	Refer: Global Nodes FastApn Access	
Daily Fast Access	https://fastapn.com/access.html	

9 Appendix C System Pricing Matrix

9.1 Global Nodes FastApn Access

A global node is where we manage the FastApn access servers, these are good for all public, soho, corporate and aviation users, and specifically for those that do not wish to interact with the management of the system directly. In this scenario, configuration is simply down to the method you choose to connect with.

Clients / Systems	DNS	Proxy	VPN	DHCP	Unbound	GUI	Contract	GUI	Month £
/32 -1	✓	✓	✓	✗	✗	✗	✗	✗	£2 (DAY)
/32 -1	✓	✓	✓	✗	✗	✗	✗	✗	£5.49
/31 -2	✓	✓	✓	✗	✗	✗	✗	✗	£8.98
/30 -4	✓	✓	✓	✗	✗	✗	✗	✗	£13.96
/29-8	✓	✓	✓	✗	✗	✗	✓	✗	£27.92
/28-16	✓	✓	✓	✗	✗	✗	✓	✗	£55.84
/27-32	✓	✓	✓	✗	✗	✗	✓	✗	£116.68
/26-64	✓	✓	✓	✗	✗	✗	✓	✗	£223.36
/25-128	✓	✓	✗	✓	✗	✗	✓	✗	£446.72
/24-256	✓	✗	✗	✓	✗	✗	✓	✗	£893.44
Unlimited	✓	✗	✗	✗	✗	✗	✓	✗	£1786.88

Figure 35: APPENDIX C: Price and Service Matrix

We have global nodes in several locations and can also be chosen as the location for use by private nodes, these are:

Atlanta, GA	Toronto, CA	Stockholm, SE
Chicago, IL	Singapore, SG	Amsterdam, NL
Dallas, TX	Osaka, JP	Milan, IT
Freemont, CA	Tokyo, JP	London, UK
Los Angeles, CA	Chennai, IN	Paris, FR
Miami, FL	Mumbai, IN	Madrid, ES
Newark, NJ	Jakarta, ID	Frankfurt, DE
Seattle, WA		Sydney, AU
Washington, DC		Sao Paulo, BR

Figure 36: APPENDIX C: FastApn Global Node Locations

9.2 Private Node FastApn Access

A private node is where you have your own FastApn bare metal server with full authentication control and configuration management through the Web Administration GUI, this also includes full group and zoning, DNS management and DPF / DAL list controls, and choice of 25 primary access locations.

Subnet	/30	/29	/28	/27	/26	/25	/24	Unlimited
Hosts	4	8	16	32	64	128	256	U/L
DNS PROXY VPN DHCP SMDNS UNBOUND GUI ACL FIREWALL MD5 BLOW	✔	✔	✔	✔	✔	✔	✔	✔
Month £	£398.72	£473.16	£616.44	£744.12	£873.81	£1246	£1892	£2385
DAR / 1000 £	on req	on req	on req	on req	on req	on req	on req	on req

Figure 37: APPENDIX C: Private FastApn Nodes

9.3 External Optional Resources

In many scenarios, operators and corporates require supplementary services such as Portal displays and advertising platforms, we can incorporate all these into your FastApn facility, or provide as standalone options.

9.3.1 Private VPN

Any protocol VPN on a barebone server with unlimited backhaul > static IPv4 + IPv6

9.3.2 SmartAVdns

Isolated SmartAVdns for geo location services, 25 countries available

9.3.3 NGINX or Apache Host

Unlimited web space on a barebone server with full Shell Access and php preloaded

9.3.4 Mailcleaner DPF

Dual direction email filter with GUI and applicable to entire Domains (UL users)

9.3.5 VOIP Soft switch Access (IDD's)

Full SIP compliant in house VOIP Softswitch with Virtual, Vanity and toll Free IDD's

9.3.6 Domain Names

Provision of any domain name as ICANN Registrars with selectable DNS Access

10 Appendix D – Acronyms Used in this Document

DNS	Domain Name Server
Pepsal	Performance Enhancing Proxy for Satellite Links
DHCP	Dynamic Host Configuration Protocol
SmartAVdns	Smart Avionics DNS Server
Proxy	Intermediate Network
PED's	Personal Electronic Devices
LAN	Local Area Network
WAN	Wide Area Network
WAP's	Wireless Access Points
ACPU	Aircraft Control and Provisioning Unit (2Ku)
Router	Any Routing Device
ATG	Air To Ground
Avance	Gogo Air to Ground system (USA only)
EAN	European Air Network
Ku	Satellite Frequency Band 12 – 18 Ghz
Ka	Satellite Frequency band 26 – 40 Ghz
2Ku	Intelsat name for Ku system with two Antennae (Thinkom)
DPF	Deep Packet Filter
DAL	Domain Access lists
Flat file	Text file written in a basic text format
TCP	Transport Control Protocol
VPN	Virtual Private Network
IPSEC	Internet Protocol Security
PPTP	Point to Point Tunneling Protocol
IKEv2	Internet Key Exchange version 2
PAC	iPhone .pac file for fast proxy access
VOIP	Voice Over Internet Protocol (SIP)
IDD	International Direct Dial telephone numbers

11 Appendix E – Flat file DAL and DPF Lists

11.1 Flat file Format

A snip example of a flat file containing known dangerous domain names, noting that any DNS lookup of these domains will prevent traffic from passing to the requesting client due to the 0.0.0.0 response. The response can be customized in the Advance Configuration. The list can contain any number of domains.

Any custom list can be generated by following this exact format.

```
# Date: 14 May 2024 23:10:54 (UTC)
# Number of unique domains: 132,661
# ============================================================
0.0.0.0 ck.getcookiestxt.com
0.0.0.0 eu1.clevertap-prod.com
0.0.0.0 wizhumpgyros.com
0.0.0.0 coccyxwickimp.com
0.0.0.0 webmail-who-int.000webhostapp.com
0.0.0.0 010sec.com
0.0.0.0 01mspmd5yalky8.com
0.0.0.0 0byv9mgbn0.com
0.0.0.0 ns6.0pendns.org
0.0.0.0 dns.0pengl.com
0.0.0.0 12724.xyz
0.0.0.0 21736.xyz
0.0.0.0 www.analytics.247sports.com
0.0.0.0 2no.co
0.0.0.0 www.2no.co
0.0.0.0 logitechlogitechglobal.112.2o7.net
0.0.0.0 www.logitechlogitechglobal.112.2o7.net
0.0.0.0 2s11.com
0.0.0.0 30-day-change.com
0.0.0.0 www.30-day-change.com
0.0.0.0 mclean.f.360.cn
0.0.0.0 mvconf.f.360.cn
0.0.0.0 care.help.360.cn
0.0.0.0 eul.s.360.cn
0.0.0.0 g.s.360.cn
0.0.0.0 p.s.360.cn
0.0.0.0 aicleaner.shouji.360.cn
0.0.0.0 ssl.360antivirus.org
0.0.0.0 ad.360in.com
0.0.0.0 mclean.lato.cloud.360safe.com
0.0.0.0 mvconf.lato.cloud.360safe.com
0.0.0.0 mclean.cloud.360safe.com
0.0.0.0 mvconf.cloud.360safe.com
0.0.0.0 mclean.uk.cloud.360safe.com
0.0.0.0 mvconf.uk.cloud.360safe.com
0.0.0.0 3lift.org
0.0.0.0 448ff4fcfcd199a.com
0.0.0.0 44chan.me
-------snip------------
```

11.2 FastApn Provisioned Lists

Our global servers contain many hand-picked and compiled dynamic lists, currently totalling 6.4 million domains and several hundred regex defined black and white lists, representing an average traffic block of 62%, section snip below:

```
# Generic
# Date: 12 May 2024 23:10:54 (UTC)
# Number of unique domains: 132,661

# ads-and-tracking-extended.txt
# Released: 2023-11-17T01:05:24+00:00
# Count: 429286 domains

# AdguardDNS
# Admiral Generic
# Easylist Adblock plus
# Easyprivacy
# Prigent-Ads
# Prigent-Crypto
# Updated 15MAY24

# Blocklist Project Ads
# Total number of network filters: 154556
# Blocklist Project Crypto
# Total number of network filters: 23761
# Blocklist Project Fraud
# Total number of network filters: 196082
# Blocklist Project Tracking
# Total number of network filters: 155070

# Scam Blocklist
# Domains: 4883

# Master Telemetry
# Domains: 1686772

# NoPlay List App Scams / Tracking / Advertising
# Apps : 187
# Domains: 362442

# Googlevideo Scam tracking block

# hostsVN Telemetry
# Last modified: 15 May 2024 09:53 UTC+7
# Blocked: 20,074 domains

# WindowsSpyBlocker - Hosts spy rules

# Spotify Adverts

# Facebook Blocklist
# Twitter Blocklist

# GoodbyeAds
# Description: Blocks Ads.Trackers.Analytics.Malware.
# Entries: 2323182

--------snip-------------
```

11.2.1 FastApn Available Lists

We have an extended library of available DPF lists, which can be combined with your custom flat files to suit your business policies, locations, regulations and requirements, these can always be amended in real-time.

Lists can include domains, URL's, ports, subject matter and text

11.2.2 Unwanted Data

advertising, adware, spyware, malware, ransomware, pop ups, pop unders, JavaScript miners, bots, hackers, sniffers, cryptomining, analytics, cryptojacking, phishing, suspicious, device telemetry, targeted and privacy advertising, malvertising, AMP hosts, fraud, Scams

11.2.3 Apps

Pinterest, Omegle, Booth.pm, Tik Tok, Instagram, Twitter, Skype, Spotify Shinden.pl Youtube, Pixiv, Whatsapp, Facebook, Badu, Chatrooms, Forums, dating

11.2.4 Content

Crypto, Firearms, Porn, Religion, Gaming, Gambling, Violence, Hacking, Illegal Activities, Drugs, Hate, Extremists, Trash Articles, Malicious sites, Adult Content, News Sites, Paid Streaming Platforms

11.2.5 Privacy

telemetry, tracking, information mishandling, snooping, location tracking

11.2.6 Gaming

League of Legends Gamebanana Patreon Discord Riot Games Valorant Myanime.list