NETPROTECT

ESET NetProtect for Telco & ISP technical overview

Seamless network security for connected devices in mobile and fixed networks

Progress. Protected.

ESET NetProtect implements a DNS filtering solution for Telco & ISP companies, providing an additional level of security for users by filtering and reporting access to domains based on certain criteria including:

- ✓ ESET domain feeds (Anti-Malware, Anti-Phishing, Potentially Unwanted Content)
- ✓ Telco & ISP preferences, settings, Custom Whitelist / Blacklist
- ✓ End Customer's own Whitelist / Blacklist
- ✓ Web Content Filter, used to filter websites based on categories like Adult, Alcohol, Shopping...

Main Features

- ✓ **Anti-Malware Protection**
- ✓ **Anti-Phishing Protection**
- ✓ **Potentially Unwanted Content Protection**
- ✓ **Web Content Filter**
- ✓ **Whitelist/Blacklist**
- ✓ **Security Report**
- ✓ **Live events and statistics**
- ✓ **Customer Management Portal**
- ✓ **Telco/ISP Management Portal**

Protection Settings

Anti-Abuse Filter
A powerful feature that can be used to prevent abusive DNS traffic, which can harm DNS resolver performance or degrade the user's experience. The Anti-Abuse filter consists of a series of configurable DNS traffic rules that can be chained together to form advanced behavior based on DNS packet content and related metadata.

Off-Net applications for DNS filtering (Available for Android and iOS)
Protecting customers connecting outside of a Telco/ISP network (e.g public WiFi, coffee-shops, etc.).

WHAT YOU CAN GET WITH ESET NETPROTECT

High performance

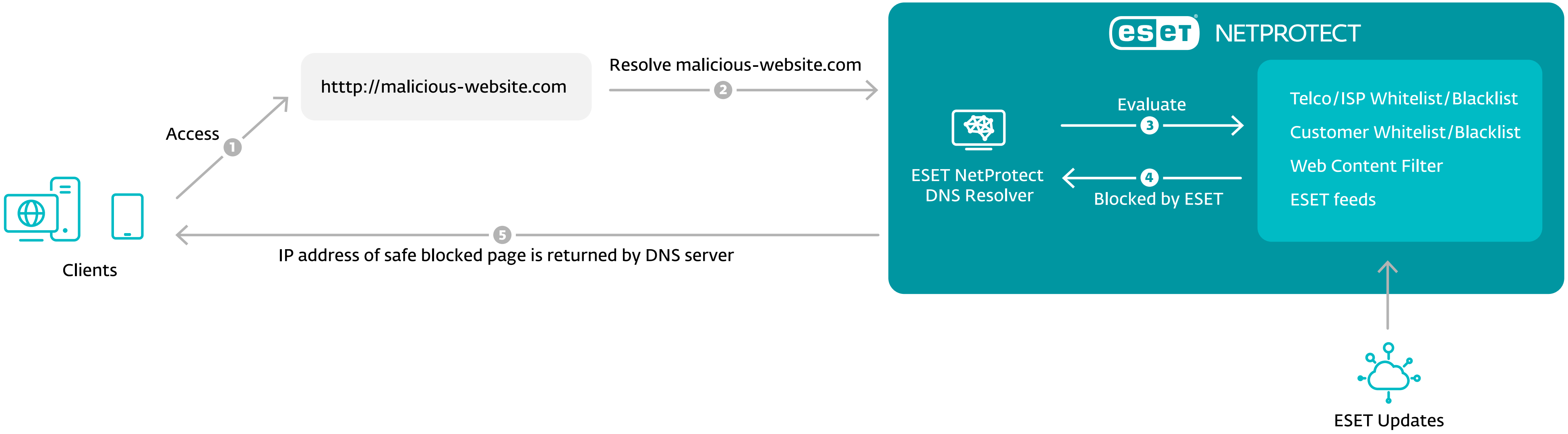
High availability

High scalability

Award-winning security

Other Features

- Solution using microservices built on a **Kubernetes** platform to achieve high performance, high availability and high scalability
- Secure **fully containerized** architecture isolated from underlying infrastructure and platform
- Real-Time solution monitoring, alerts and data analysis using industry-standard tools from **Elastic-ELK** (Elasticsearch, Logstash, Kibana)
- Easily deployable at any scale
- Ability to create custom modules (**microservices**) that can interact with our solution
- **Rich REST** and gRPC APIs to interact with our solution
- **Pause Protection** — optional ability to run in silent mode (malicious domains are only reported, not blocked)
- **ESET NetProtect supports SMTP** and Custom APIs for generating regular emails to customers with Security Reports.
- **Strong privacy focus** — Our solution does not require the customer's personal data and we can work in an anonymized environment



http://malicious-website.com
Access
1
Resolve malicious-website.com
2
eset NETPROTECT
ESET NetProtect DNS Resolver
Evaluate
3
4
Blocked by ESET
Telco/ISP Whitelist/Blacklist
Customer Whitelist/Blacklist
Web Content Filter
ESET feeds
Clients
5
IP address of safe blocked page is returned by DNS server
ESET Updates

Solution workflow with example

DNS (Domain Name System) is a distributed database used to convert human-readable domain names into IP addresses or to request another type of information. Examples of some well-known domains are github.com, youtube.com, tiktok.com,...

If, for example, a user wants to access http://malicious-site.com from his/her internet browser (considering this domain as malicious for this example):

- The browser asks a predefined DNS server to perform a conversion from malicious-site.com to an IP address
- The domain name is successfully translated into a valid IP address
- The browser then performs a request towards the resolved IP address
- The content of malicious-site.com is downloaded and displayed to the user

The same scenario with ESET NetProtect:

- The browser asks ESET NetProtect DNS Server to perform a conversion from malicious-site.com into an IP address
- Different feeds are evaluated to recognize domain reputation and populate user and Telco/ISP settings
- The IP address of the blocked page is returned
- The user is redirected to the safe website (blocked page) with a detailed explanation and the possibility to accept the risk and continue

ESET NetProtect performs validation of all the domains before they are accessed by the user or device, blocking and reporting access to domains known to be malicious or matching specific Telco/ISP or user criteria.

Integration and deployment

ESET NetProtect solution has been built using modern Kubernetes microservices architecture supporting all the major Kubernetes distributions and cloud solutions including Canonical microk8s, Red Hat OpenShift, Azure AKS, Azure ARO, Amazon EKS, Google Kubernetes Engine, and more.

The solution can be easily deployed at any scale in:

- On-Premises deployment
- Private cloud (virtualized enviroment)
- Public cloud

In typical deployments, each component runs in pairs on different physical nodes to achieve high availability, scalability, 0% downtime during component upgrade,...

Normally, ESET NetProtect is distributed as a HELM chart for straight-forward installation. There are many options to deploy our solution including ESET-assisted deployment.

Each Telco/ISP can have a different tech stack deployed and different preferences in certain areas. We are able to provide implementation support for them for seamless integration with their existing systems.

Below you can find components that may require customization:

- Integration with AAA (Authentication, Authorization, and Accounting) systems:
  - processing RADIUS accounting start/stop packets,
  - processing RADIUS accounting start/stop logs,
  - processing DIAMETER accounting start/stop logs,
  - integration with other AAA systems is possible,
- By default ISP/ Telco and Customer Management Portal are provided by ESET
  - Possible design customizations
  - Possibility to enable/disable UI features
- REST and gRPC APIs are provided by ESET enabling full interaction with our solution
  - Possibility to directly integrate the solution with Telco/ISP custom web portals, mobile applications and automation systems
- Off-net mobile applications are available
  - Possible design customizations
  - Possibility to enable/disable UI features

Possible configuration of DNS resolvers

There are multiple options for how to configure the recursive DNS resolving capabilities of our solution.

- By default, our solution ships with a recursive caching DNS resolver used to perform recursive DNS resolution
- A configuration where our solution forwards DNS queries to the Telco/ISP recursive DNS resolver/s is possible and should be considered

The Secure DNS resolver currently supports these DNS protocols (activation/ deactivation based on preference):

- DNS over UDP transport (UDP port 53)
- DNS over TCP transport (TCP port 53)
- DNS over TLS (TCP port 853)
- DNS over HTTP/2 (TCP port 443)

Hardware and software requirements

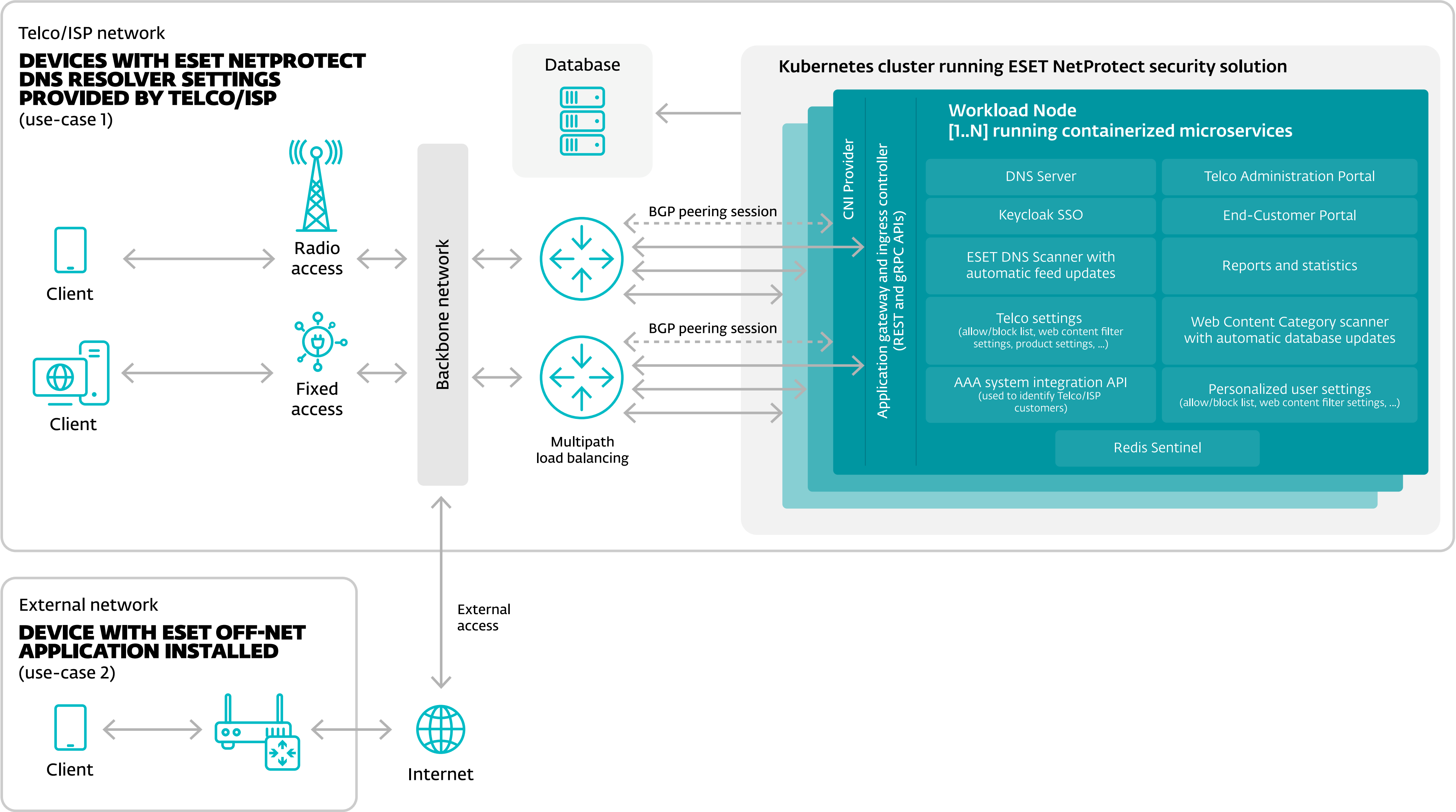
Minimal hardware requirements differ and are directly related to the expected DNS server load (e.g. DNS queries per second, type of DNS traffic).

Minimal technical requirements are based on:

- Expected number of DNS queries per second (from existing DNS server statistics if present)
- If there are no statistics about the number of DNS queries per second, we need the expected number of customers to calculate the average load

To achieve high availability, at least a 3-node Kubernetes cluster is required, although other setups are possible. If the customer desires to run our solution on-premises and does not have Kubernetes available, we can provide a complete setup (Kubernetes + ESET NetProtect).

eset NETPROTECT



Telco/ISP network

DEVICES WITH ESET NETPROTECT DNS RESOLVER SETTINGS PROVIDED BY TELCO/ISP

(use-case 1)

Client

Radio access

Client

Fixed access

Backbone network

Database

BGP peering session

BGP peering session

Multipath load balancing

Kubernetes cluster running ESET NetProtect security solution

CNI Provider

Application gateway and ingress controller (REST and gRPC APIs)

Workload Node [1..N] running containerized microservices

DNS Server	Telco Administration Portal
Keycloak SSO	End-Customer Portal
ESET DNS Scanner with automatic feed updates	Reports and statistics
Telco settings (allow/block list, web content filter settings, product settings, ...)	Web Content Category scanner with automatic database updates
AAA system integration API (used to identify Telco/ISP customers)	Personalized user settings (allow/block list, web content filter settings, ...)

Redis Sentinel

External access

External network

DEVICE WITH ESET OFF-NET APPLICATION INSTALLED

(use-case 2)

Client

Internet

Vocabulary

- **Anti-Malware Protection** — protects the user from accessing domains containing files categorized as malicious software, which, after installation, can provide remote access to an infected device, leak sensitive data from the device, harm the targeted device, or cause other damage to the device's owner
- **Anti-Phishing Protection** —protects your privacy and assets against attempts by fraudulent websites to acquire sensitive information such as usernames, passwords or banking details, or feed you fake news from seemingly reputable sources. Protects you from homoglyph attacks (replacing characters in links with ones that look similar but are actually different)
- **Potentially Unwanted Content Protection** —protects users against suspicious domains or websites hosting unwanted content
- **DNS (domain name system)** — a decentralized database used to convert human-readable domain names into IP addresses and other information
- **IP address** — a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication
- **Telco/ISP** — Telecommunication company providing internet connection services
- **Telco/ISP Management Portal** — web application intended for Telco/ISP to configure ESET NetProtect behavior
- **Customer Management Portal** — web application intended for the End-user (Telco/ISP customer) to configure ESET NetProtect behavior
- **Off-Net applications** — Android & iOS applications providing an additional level of security for users connected outside of the Telco/ISP network (public Wi-Fi)
- **Web Content Filter** — used to categorize domains so it is possible to block or allow certain domain categories. Example domain categories include: Adult, Alcohol, Shopping...
- **Domain feeds** — the source of domains belonging to a category/categories
- **Kubernetes or K8s** — open-source system for automating deployment, scaling, and management of containerized applications
- **Container** — the standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another
- **Microservices** — architectural and organizational approach to software development where software is composed of small independent services that communicate over well-defined APIs
- **HELM charts** — install and upgrade even the most complex Kubernetes application

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future.

www.eset.com