GreeNet's Traffic Detection Function and Policy Control Function

Solution Briefing

Table of Contents

1. Background

How to guarantee the user's quality of experience (QoE) is an urgent issue that Communication Service Providers (CSPs) needed to resolve. CSPs need to understand the service quality of different applications in the network, provide service guarantees for high-value applications, restrict low-value applications (like P2P), reduce the cost of building or leasing links, and improve user satisfaction. CSPs pay attention to provide differentiated services for different users. Through user-tiering services, they can ensure the QoE for key users, increase their stickiness, and ARPU.

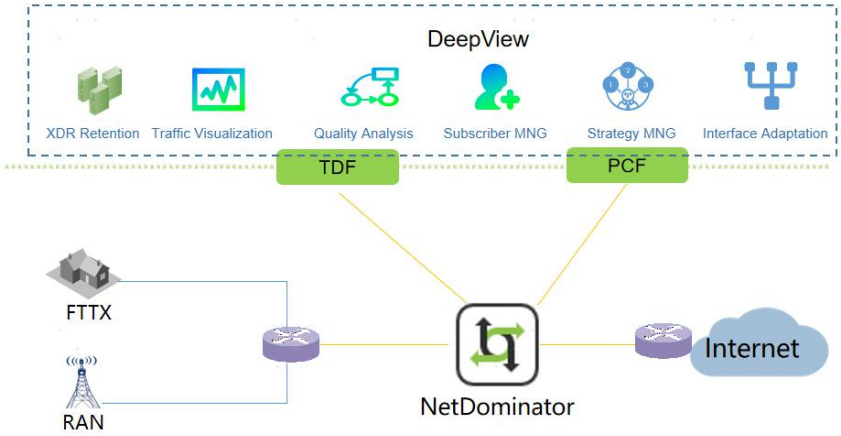
With the booming of subscribers number together with the devices scale, and the increasing number of Internet applications, network design has become more and more difficult. CSPs need to have deep insight for the traffic of the network, so as to spend less cost and construct more critical network infrastructures.

Increasing OPEX is the biggest concern of CSPs. They need to provide refined operation and customized services to improve revenue capabilities. GreeNet's Traffic Detection Function and Policy Control Function solution can bring profitable service that CSPs needed.

2. GreeNet's TDF/PCF Solution Overview

GreeNet provides the world leading solution for Traffic Detection Function and Policy Control Function (TDF/PCF) that help CSPs to have a full control of their network. The GreeNet TDF/PCF (GNT TDF/PCF) solution deploys NetDominator solution in the mobile network, integrating PCRF, PCEF, and TDF functions. The GNT TDF/PCF solution complies with 3GPP standards and can be deployed in 3G/LTE/5G mobile networks, and fixed-line networks as well. It supports Diameter Gx, Gy, Gz and Sd, Sy and also other interfaces that allow CSPs the capability with a closed-loop PCC and traffic analytics solutions.

Another core function of GNT TDF/PCF is GreeNet's DeepView Analytics Platform which provides the strategic management and smart GUI visual display.

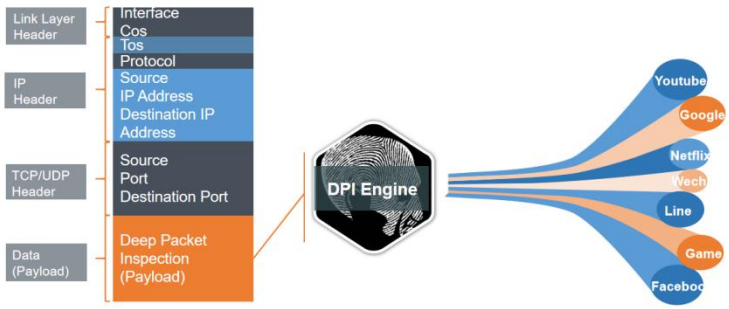


2.1 Comprehensive Traffic Management

a) Traffic Identification

GNT TDF/PCF solution is conveniently and effectively to monitor CSPs' operating conditions, both in real-time and long term. It analyzes the internal network traffic, identifies applications, and recognizes bandwidth distribution ratio of various applications and protocols. The GNT TDP/PCF's key capabilities are list as follows:

- Support up to 320Gbps throughput per 2RU box, enabling real-time network visibility and application control
- Empower with flexible DPI engine, supporting 4000 unique application signatures, and more than 1 million individual URL libraries
- Equip with centralized and intuitive policy interface, allowing quick and easy deployment of policies across multiple devices
- Allow to aggregate data record fields from different data records into one data record through custom field configuration

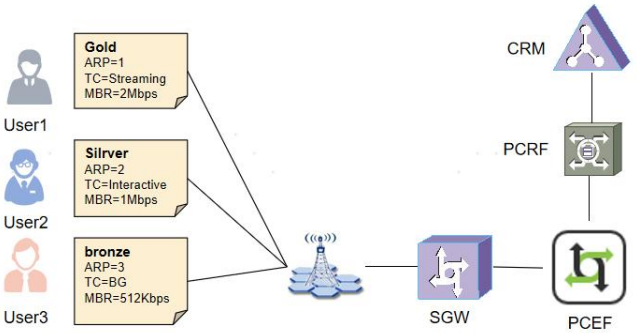


b) Traffic Visualization

NetDominator monitors the network traffic, identify traffic and report the results to the upper DeepView platform in the form of XDR records. DeepView will use big data analysis to intelligently analyze the historical trend of the network, network behavior characteristics, traffic flow direction information, application proportions, user traffic proportions, etc. DeepView also provides intuitive display for users with a graphical interface.

c) User Tiering

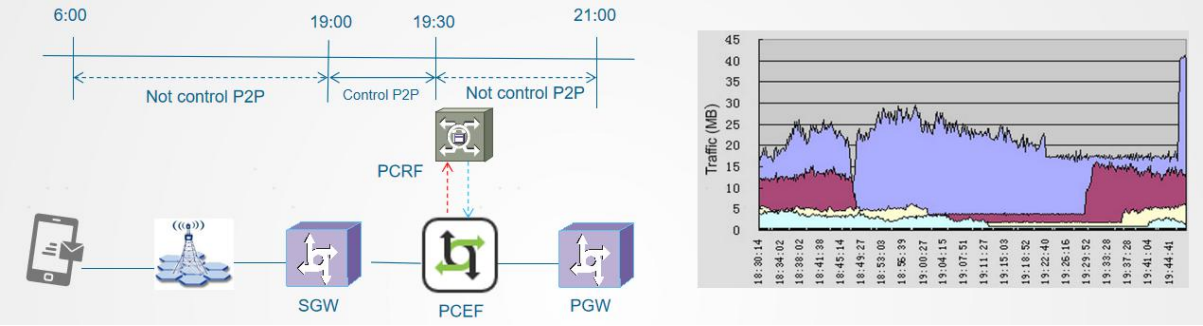
GNT TDF / PCF solution provides user-tiering services and provide different services for subscribers of different tiers. Through policy configuration, the service level of important users can be upgraded, and the expenditure to non-important users can be reduced.



APP Type	Gold user	Silver user	Bronze user
Web	256Kbps	64Kbps	32Kbps
Video	128Kbps	128Kbps	64Kbps
Download	64Kbps	32Kbps	16Kbps
IM	32Kbps	16Kbps	16Kbps

d) Traffic Control

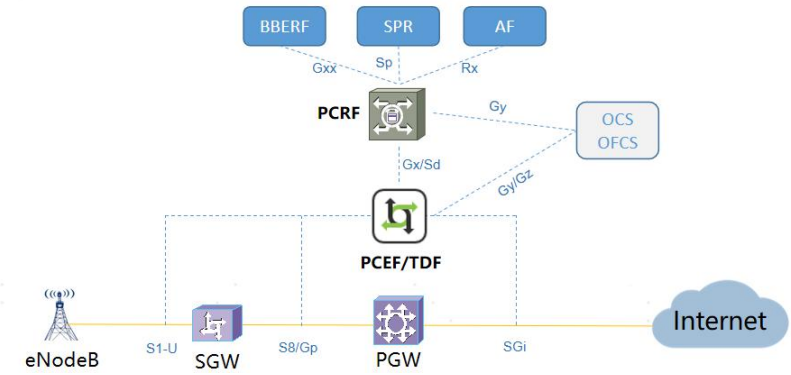
NetDominator effectively manages traffic for all users to confine the bandwidth of low-value applications like P2P and file downloading which maliciously abuse network. Through the traffic control, the bandwidth of low-value applications can be restricted, and the bandwidth of high-value applications would be guaranteed.



2.2 Rich Interface Support

The GNT TDF/PCF solution connects to the standard interface of the LTE mobile network based on the standard Diameter Gx, Gy, Gz and Sd, Sy, Sp interfaces. GNT TDF/PCF solution provides customer with a truly centralized integration strategy and policy charging function (PCF). It also provides deep packet inspection (DPI) and traffic detection function (TDF), traffic shaping, packet filtering and QoS functions, and implement policy decisions in the actual environment.

The GNT TDF/PCF solution adapts various access network and can be deployed across Cable network, WiFi, ISP, Fixed-line network, WiMAX, 3G, HSPA, LTE, 5G, etc.



2.3 Professional Security Protection

GNT TDF/PCF solution provides customer with professional security protection to protect users and their network infrastructures from various network threats and malicious traffic. Integrated with the world leading anti-DDoS and anti-malicious engines from Radware and Kaspersky respectively, GNT's TDF/PCF solution can identify and respond to threats in real time, allowing CSPs to implement subscriber-specific and network-specific policies for precise detection and attack traffic mitigation.

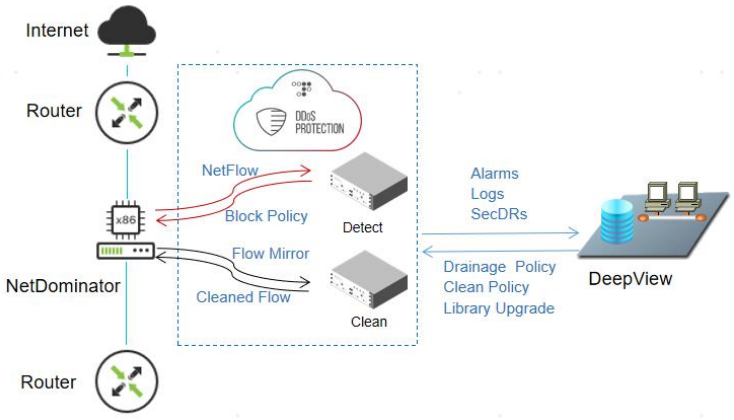
2.4 DDoS Mitigation

The GNT TDF/PCF solution integrates Radware's DDOS protection engine to provide CSPs with DDOS mitigation services, so that the CSPs' data center is always protected. Based on behavioral analysis algorithms, Radware's DDOS protection can be combined with GNT DPI function to provide the most effective DDOS mitigation solution against known and unknown attacks. The protection types can be included as follows:

- UDP flood attack
- TCP flood attack
- IGMP flood attack
- SYN flood attack
- ICMP flood attack

- Out-of-state flood attack
- HTTP flood attack
- SIP flood attack
- Network and port scanning
- DNS flood attack
- Brute force attack
- Malware spread

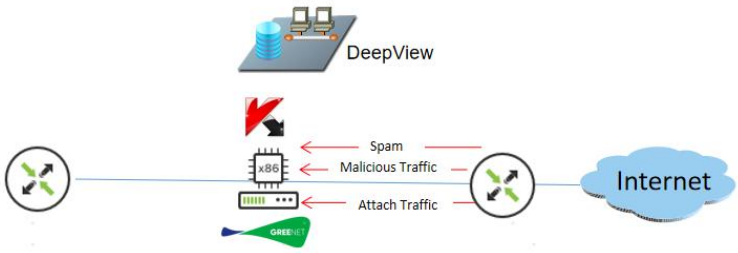
In addition, GNT also provides CSPs with additional cleaning center services. For the unknown attack traffic, the cleaning center provides a variety of DDoS traffic cleaning approaches, which can accurately identify normal traffic and clean all kinds of abnormal traffic, including traffic-based attacks, application layer attacks, scanning and snooping attacks and malformed packet attacks.



2.5 AntiVirus Protection & Threat Intelligence

GNT TDF/PCF solution also integrates with Kaspersky Anti-Virus SDK virus protection engine. The SDK offers the industry-leading protection against various known and unknown cyber threats. GreeNet and Kaspersky team up to provide highly reliable network security services with updated AV engines. With that, the solution always provides the latest detection technology and processing logic. Protection for CSPs includes:

- Block malicious URLs, phishing websites, adware, etc.
- Provide different types of known and unknown malware Rootkit, Bootkit and other
- Malware self-hiding tools
- Keylogger and/or screen grabber identity theft
- Botnet activity coordination
- Zero-day attack/unknown threat
- Drive-by download infection
- Help to implement anti-APT risk mitigation strategies



2.6 Overcome Routing Asymmetry

Multiple routing improve the network availability, but also bring challenges when implementing some network solutions. By using Asymmetric Routing capability, GNT TDF/PCF solution address the above-mentioned challenges. Through various methods including hash distribution, upload upstream traffic, flow tables to realize merging traffic of same source and same destination, GNT TDF/PCF allows CSPs to implement the Asymmetric solution in their network, and the complete traffic of the same subscriber can be analyzed and managed uniformly.

2.7 High Availability

The GNT TDF/PCF solution support the high availability up to 99.999%. The NetDominator supports 1+1 redundancy protection. It can work in both "active-active" or "active-standby"

modes. There is a heartbeat between redundancy servers to maintain the availability of the network service with HA detection. At the same time, NetDominator provides the Bypass unit that are installed inline. When the system detects an issue, the Bypass function kicks in to maintain an uninterrupted data flow that ensure that the services will not be affected.

DeepView supports cloud deployment and physical server deployment. Cloud deployment uses system cloning and recovery to provide backup. When the physical machine is deployed, it will provide system-level 1 + 1 hot standby, hard disk RAID and network card backup.

The following table details the different levels of redundancy:

NetDominator	Components	Redundancy
	System	1 Active + 1 Standby
	Hard disk	RAID 1, Hot-swappable
	Power supply	1 + 1 P/S, Hot-swappable
	Database	1 + 1, Replication
	Bypass	Optical detection+Heartbeat detection

DeepControl	Components	Redundancy
	System	1 Active + 1 Standby
	Hard disk	RAID 1, Hot-swappable
	Power supply	1 + 1 P/S, Hot-swappable
	Fiber Network Interface Card	N+1

3. Benefits

GNT TDF/PCF solution provides strong performance, security, HA and scalability. It integrates signaling analysis, network analysis, security protection, policy control and traffic management, increases revenue and reduces costs for CSPs.

Key features:

- Combines PCRF, PCEF and TDF, provide users with cost-effective solution, significantly reduce the time to market
- Highly detailed visual display of applications, subscribers and devices
- A single box supports millions of traffic control policies and supports more than 200G traffic processing capabilities
- Support identification, analysis, and management traffic under asymmetric conditions
- Multi-service platform combines network analytics, subscriber and application traffic management, all-inclusive DPI, DDoS mitigation and Web security functions

4. About GreeNet

GreeNet provides intelligent network service awareness solutions for enhancing customer satisfaction and monetization services for CSP customers. The company specializes in network service awareness, data and control plane analytics, and regulatory compliance's security solutions. Founded in 2003, GreeNet has 300 experienced in-house developers dedicated to developing innovative services and security solutions to meet market demands.

GreeNet has more than 250 deployments in 160 cities globally. The total bandwidth capacity installed by our customers is more than 400 Terabytes for various applications.

GreeNet's intelligent iNAS solution is developed with the industry's most advanced software-based DPI technologies. The solutions are used in the fixed, mobile, IoT, and any network access environment. It provides end-to-end IP network visibility, data analytics, network filtering, and network security solutions, including anti-Fraud, anti-Malware, DDoS Mitigation, and Parental Control.

For details, please visit www.greenet.co, contact one of our sales locations or email us at sales@greenet.co.