SANDVINE

Regulatory Traffic Management

Safety and security compliance for national networks

REGULATORY TRAFFIC MANAGEMENT DELIVERS:

Accurate Identification of All Traffic

Industry-leading traffic identification with frequent updates ensures current and accurate identification of all types of internet traffic and applications

Powerful Traffic Management

Multiple actions can be applied once traffic is identified to best suit the type of traffic and to comply with regulations and policies

Flexible Content Control

Content filtering can be customized to meet corporate, educational institutions, or public policies

Bypassing Technique Detection

Detects traffic tunneled through a VPN to bypass regulations

Carrier-Scale Deployments

Highly scalable and access-agnostic traffic management solution with ability to scale to carrier-scale deployments

MARKET OVERVIEW

Governmental telecom regulators and network operators are struggling to keep up with the ever-changing security and safety concerns introduced by content and applications that are counter to local regulations. Whether it is applications introducing safety concerns due to non-compliance with information retention regulations or URLs containing prohibited content, part of the challenge is constantly keeping up with the expanding internet.

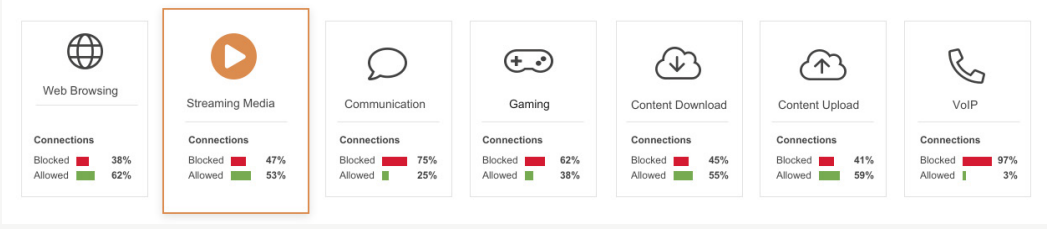
In most regions, some form of regulated content control occurs for safety or for social reasons. For example, content control for minors in public places and schools, where controversial topics and harmful content like religious propaganda, pornography, and drugs can be blocked or filtered. In many countries, laws and regulations allow for blocking, and even removal, of content like child pornography, violence, terrorism, and illegal gambling with substantial public support.

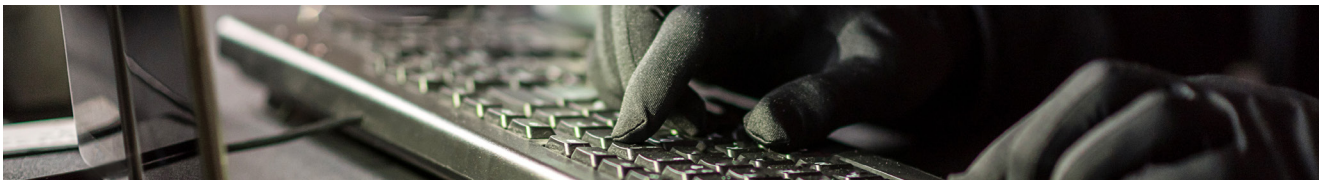
Aside from social reasons, some types of traffic can be direct threats to the availability of critical services, like voice or emergency services, for citizens provided by operators. Specific applications and/or traffic that are associated with, or known to be used as an attack vector for DDoS attacks, should be consistently monitored for threat indicators. When successful, these cyberattacks can have huge financial consequences for operators due to service disruption experienced by the public and the direct harm to national infrastructure.

With increasing connectivity comes more sophisticated cyberattacks and evasion techniques to bypass regulations. Therefore, regulators require a solution that can cover nationwide networks of all access types and operators need a solution that ensures full compliance, regardless of rapidly emerging applications.

Figure 1

Visualization of Application Categories





Drastically minimizes the threat and potential harm of DDoS-related traffic with surgical enforcement, even when net neutrality exists

SOLUTION OVERVIEW

This Regulatory Traffic Management solution leverages Sandvine's ANI Classification Engine, which boasts thousands of internet application signatures and URLs categorized by key types such as file sharing, VoIP, streaming media, and many more. Sandvine also supports customized, virtual services, giving operators the ability to define custom signatures with a variety of application attributes.

Advanced Traffic Classification Designed for Encryption

Sandvine's sophisticated traffic identification is the foundational technology driving this solution. With industry-leading capabilities to identify encrypted traffic and complex, polymorphic applications, the ANI Classification Engine is powered by machine learning and updated daily to maintain up-to-date signatures. Requiring an exact match to categorize traffic, the ANI Classification Engine keeps false positives to a minimum and the pitfalls of less sophisticated engines that rely on best match is avoided.

While regulations may trigger the use of circumvention tools, Sandvine's expertise in identifying tunneling (VPNs) and other masquerading techniques is leveraged to provide the most efficient compliance solution on the market.

Surgical Enforcement

Once traffic is identified, multiple actions can be taken on a per-flow basis. Traffic can be blocked or rejected, which will halt the specific traffic streams. A network operator can manage or block traffic from specific applications or entire groups of restricted applications. Traffic can also be rate-limited or session-limited, which is more effective for some types of applications (i.e., polymorphic applications that change behavior when blocked). Operators can also block or filter URLs to comply with regulations regarding potentially harmful content and information to protect citizens.

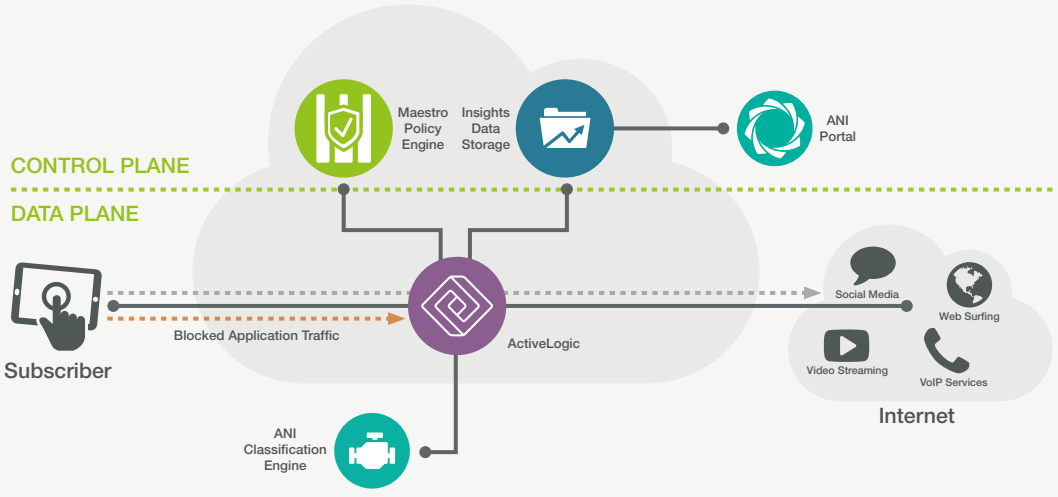
With the rapid introduction of malware, especially in mobile applications, the ability to block traffic by URL or application/application category increases a network operator's ability to secure and defend their networks from attacks.

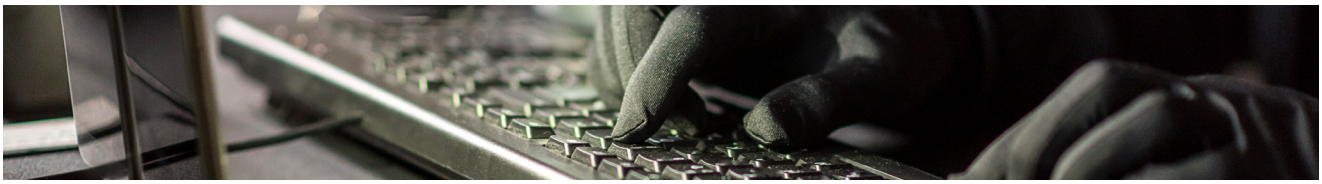
Traffic Analysis

Logging or analytics can be part of the regulatory requirement, and traffic can be monitored or re-marked and the flows passed, blocked, limited, dropped, etc., to provide a closed-loop analysis of the effectiveness of the regulatory compliance.

Figure 2

Sandvine sits on the network data plane to control traffic to and from the internet





Sandvine's Regulatory Traffic Management provides operators as well regulators with a sophisticated, flexible, and scalable solution designed to operate in today's complex networks, with the highest compliance-efficiency on the market.

ABOUT SANDVINE

Sandvine helps organizations run world-class networks with Active Network Intelligence, leveraging machine learning analytics and closed-loop automation to identify and adapt to network behavior in real-time. With Sandvine, organizations have the power of a highly automated platform from a single vendor that delivers a deep understanding of their network data to drive faster, better decisions. For more information, visit **sandvine.com** or follow Sandvine on Twitter at **@Sandvine.**

SANDVINE

USA
2055 Junction Avenue
Suite Number 105
San Jose,
CA, 95131
USA

EUROPE
Svärdfiskgatan 4
432 40 Varberg,
Halland
Sweden
T. +46 340.48 38 00

CANADA
408 Albert Street,
Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

ASIA
RMZ Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333