SANDVINE

Regulatory Traffic Blocking

Safety and Security Compliance for National Networks

KEY SYSTEM BENEFITS

- Frequent updates to Sandvine's industry-leading signature database ensures current and accurate identification of all types of Internet applications
- Performance scalability to Tbps per virtual or hardware cluster to drastically reduce the power and space footprint for carrier-scale deployments
- Supports virtual service definitions for local governmental regulatory compliance for custom application definitions
- Multi-use case deployments provide greater ROI than standalone deployments by adding Analytics, Traffic Optimization, Revenue Generation, Revenure Assurance, Network Security, or other Regulatory Compliance use cases

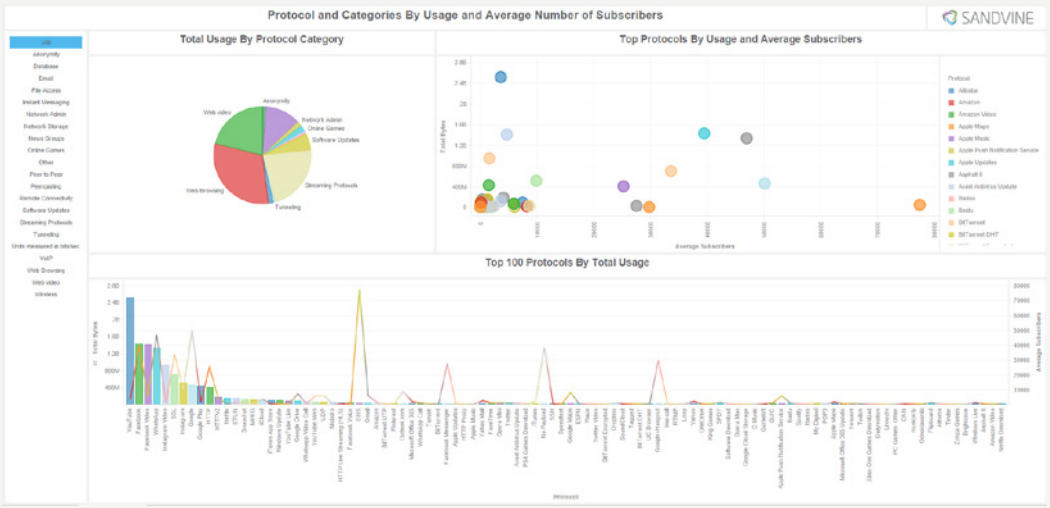
Governmental Telecom Regulators and Network Operators are racing to keep up with the ever changing security and safety concerns introduced by applications that do not comply with local regulations. Whether the applications introduce safety concerns due to non-compliance with law enforcement regulations, or are known attack vectors for DDOS attacks, maintaining up-to-date solutions for mitigating and blocking these applications is a severe challenge. When combined with the explosive bandwidth growth of the past few years, Regulators and Operators need higher performing, more flexible solutions to satisfy Regulatory Traffic Blocking use cases for Regulatory Compliance.

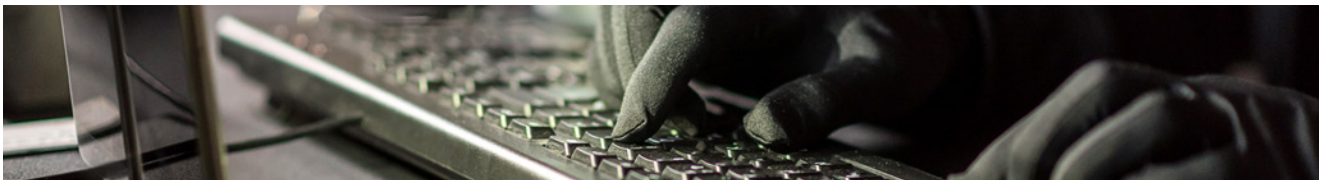
TRAFFIC BLOCKING FOR TELECOMMUNICATIONS REGULATORS AND TELECOM OPERATORS SOLUTION OVERVIEW

Sandvine's compliance solutions leverage our extensive application signature library of thousands of Internet applications categorized into categories like file sharing, VOIP, streaming media, and many more. Sandvine also supports customized virtual services, which give an operator the ability to define custom signatures using a variety of application attributes. Sandvine has a special focus on encrypted applications, with more than 50% of our signatures identifying encrypted traffic leveraging sophisticated hueristics and machine learning to stay current. Using Sandvine, a network operator can block or mitigate traffic from specific applications or entire groups of applications that are restricted by local laws. With the rapid introduction of malware, especially in mobile applications, this capability helps increase network operator's ability to secure and defend their networks from attacks.

Figure 1

SERVICES OVERVIEW FROM SANDVINE ANALYTICS





ACTIVE NETWORK INTELLIGENCE FOR REGULATORY COMPLIANCE

APPLICATION IDENTIFICATION: THE FOUNDATION OF NETWORK INTELLIGENCE

Sandvine's sophisticated application identification is the foundational technology that powers our regulatory traffic blocking solution. Sandvine's industry leading network intelligence engine is optimized to identify the most common Internet applications with minimal latency, while also supporting the "long-tail" of thousands of niche applications. Our engine requires an exact match to categorize traffic in order to minimize false positives, and avoid the pitfalls of less sophisticated solutions that rely on best match, which is increasingly challenged in the era of widespread encryption and polymorphic applications.

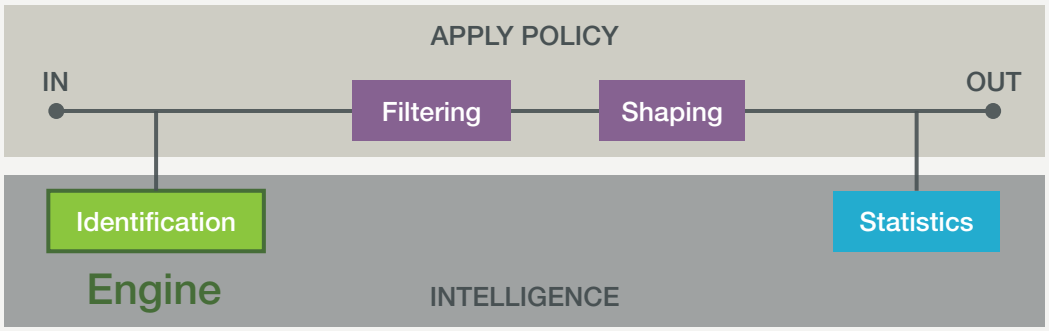
Once traffic is identified by the engine, it can take multiple actions on the flows in order to comply with regulations. Traffic can be blocked or rejected, which will halt the traffic streams. Traffic can be rate limited or session limited, which for some types of applications (namely polymorphic applications that change behavior when blocked) delivers better results. If logging or analytics is part of the regulatory requirement, traffic can be monitored or re-marked and the flows passed, blocked, limited, dropped, QoE, and many other metrics to provide a closed loop analysis of the effectiveness of the regulatory compliance.

REGULATORY TRAFFIC BLOCKING DEPLOYMENT

Sandvine solutions can be deployed anywhere in the network - on a virtual CPE, provider edge, core, or peering point. For regulatory compliance, Sandvine is traditionally placed in-line, enabling the solution to natively block traffic that is deemed to be non-compliant with the regulatory polices. When Sandvine is integrated with policy systems, more information is available as a selector for traffic blocking to further narrow the policy - for example if URL filtering for minors. This provides both operators and regulators more flexibility for regulatory enforcment.

Figure 2

ACTIVE NETWORK INTELLIGENCE FOR REGULATORY BLOCKING



v20180215

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
47448 Fremont Blvd,
Fremont,
CA 94538,
USA
T. +1 510.230.2777

EUROPE
Birger Svenssons Väg
28D
432 40 Varberg,
Sweden
T. +46 340.48 38 00

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

ASIA
Ardash Palm Retreat,
Bellandur, Bangalore,
Karnataka 560103,
India
T. +91 80677.43333