See. Control. Secure.

The Allot Regulatory Compliance Solution

Introduction

Regulatory compliance has become mission critical for national authorities and Communication Service Providers (CSPs) due to increased cyberthreats such as offensive, criminal or unethical on-line activities, and attacks on communications infrastructure. Regulations aimed at protecting the general population often require network operators to capture, analyze and retain records of application usage, block harmful content and sites and safeguard communication infrastructures against denial of service attacks.

Law enforcement and homeland security agencies rely on service providers to lawfully intercept, block and record dangerous traffic to help mitigate internal and external criminal and security threats.

To meet these requirements, service providers need a flexible, powerful and scalable solution that resolves current and future threats through adaptive machine learning of malicious behavior and dynamically expanding threat identification.

Solution

The Allot SmartRegulator solution is specifically designed to enable CSPs to meet national law enforcement and/or homeland security authority requirements. The solution is comprised of the following main components:

Security

- DDoS detection and mitigation of volumetric inbound and outbound based on advanced Network Behavior Anomaly Detection (NBAD) technology
- IoT Botnet activity detection and containment
- Detailed threat intelligence on attackers and their targets in the network
- High-precision blocking of illegal Anonymity and VPN applications utilizing machine learning algorithms
- Privacy by design ensuring confidentiality of personal data and restricting access to authorized users

Network Intelligence

- Industry leading DPI traffic awareness overcomes data encryption
- Automatic analysis and classification of application, user, session, device, location, content, type of interest and more
- Built-in support for thousands of applications and protocols - expandable through automatic updates or self-service interface
- Detailed extraction of Web traffic information and storage online usage records
- Unified front-end GUI integrates all data sets, and enables self-service analysis to produce meaningful intelligence such as user browsing behavior, destinations, and trends

Application and Content Filtering

- Precise, encryption agnostic URL classification and illegal URL filtering
- Supports global IWF blacklist as well as import of blacklist policies from national regulatory bodies
- Varied content management actions including block, redirect and disrupt (rate-limit) traffic to specified sites

Data Retention

- Scalable and reliable big data warehouse for long retention of high volume data records
- Built-in high availability
- Simple interface for ad-hoc retrieval of user online web log

Benefits

Allot offers a unique, unified solution based on massively scalable, in-line protection that inspects every packet and delivers the following key benefits:

- Granular, big data visibility into network, user and application behavior
- Blocking illegal content, such as pornography, violence, drugs, child abuse, fake and untruthful content and illegal applications
- Unlimited retention of detailed usage records
- Protection of network infrastructure against DDoS attacks

Flexible Deployment

The Allot Regulatory Compliance solution can be deployed in-line for active mitigation and filtering or as a passive probe to monitor live traffic. It applies to virtually any network type, including: ADSL, cable, mobile, etc. The solution presents a centralized management platform to deploy action policies across the entire network at a national scale and includes steering and chaining capabilities to easily integrate 3rd party products for enhanced solutions.

All Allot solutions support on-premise, cloud, hybrid, and virtual deployments.

High Performance and Scale

The Allot unified SmartRegulator solution can scale to inspect Terabits per second of data and store Petabytes of application and user data.

Track Record

Specific use cases have included:

- DDoS Detection and Mitigation (DDoS Secure) has been deployed at more than 70 service providers around the world, protecting against massive DDoS attacks that in some cases have tried to bring down government infrastructure and have exceeded 100Gbps.
- Smart monitoring solutions for proactive intelligence in countries across Asia to detect illegal and abusive online behavior based on usage profiles and to alert authorities about such suspicious activity.
- A nation-wide network intelligence solution covering more than 100 Million subscribers that selectively blocks the use of social networks to prevent their abuse by threat actors in a specific region of the country in one of the SAARC nations.
- A turn-key European regulatory project that collects and retains online usage data for varying time periods and provides a flexible user interface for on-demand queries based on law enforcement requirements.
- African, Asian and European projects that provide a dark web control solution at ISP locations country-wide. These projects cover more than 50 Million subscribers over multiple years with ongoing support via new signature development and other adaptations to changes in the online ecosystem.
- URL filtering and IP blacklisting to protect service provider reputation and comply with counter-terrorism regulatory requirements.