
allot
See. Control. Secure.
Use Cases
Transportation
Enterprise

INTRODUCTION

This document provides a selection of customer use cases applicable for the transportation sector. Each use case describes an individual challenge faced by transportation companies along with detailed descriptions of the products available that can be used to mitigate and manage those issues.

Allot's solutions empower you to increase productivity and protect your operations and users against ransomware, Denial-of-Service attacks, and Bot infection. By delivering full visibility and granular control over applications, users, and network utilization, the Allot Secure Service Gateway (SSG) enables you to remove risky applications from your network, control recreational traffic, and most importantly, ensure that your network runs according to your business priorities. In addition, Allot's solutions will reduce the total cost of ownership of your security investment by Allot leverages DPI technology to provide a clear and accurate view of network usage. Armed with this valuable insight, IT managers can dynamically control the delivery of critical applications to comply with SLAs, to protect network assets against attack, and to accelerate the Return on Investment (ROI) on their IT infrastructure.

Allot is a leading provider of intelligent IP service optimization solutions that help enterprises and data centers run more efficient networks that better satisfy their users.

Allot solutions are deployed worldwide in data centers and enterprise networks across a broad range of business sectors including e-commerce, education, energy, utilities, finance, government, healthcare, higher education, hospitality, media and telecom, retail stores, and transportation.

The use cases in this booklet are based on the key benefits that can be obtained directly by an enterprise or through managed services providers. Each case leverages both security and network intelligence capabilities for application, user and device behavior, and control for enterprises to:

- Understand how network resources are consumed before making infrastructure investments
- Define real-time traffic management policies that align performance to business priorities and adjust IP traffic flows dynamically when links are congested
- Define tiered traffic management policies based on individual levels of service for specific user profiles
- Reduce the enterprise attack surface and increase productivity by identifying and blocking risky applications such as anonymizers and peer-to-peer applications
- Control the use of unsanctioned IT applications such as cloud storage and social media
- Increase availability with real-time DDoS protection combined with traffic management to automatically remove DDoS attack traffic within seconds while maintaining maximum Quality of Experience (QoE) for all legitimate and business-critical network services
- Detect and neutralize web threats, phishing, ransomware, quarantine botnets, and malware-infected hosts

Key Benefits

- Prevent excessive, non-organizational use of a network
- Improve user productivity and satisfaction
- Optimize Internet-link performance

Acceptable Usage Management in Action

- Define acceptable usage tiers and quotas for non-organization-related traffic
- Assign user/department/facility to relevant tiers
- Automatically enforce acceptable usage in real time
- Block the use of inappropriate and risky applications and content on an organization's network

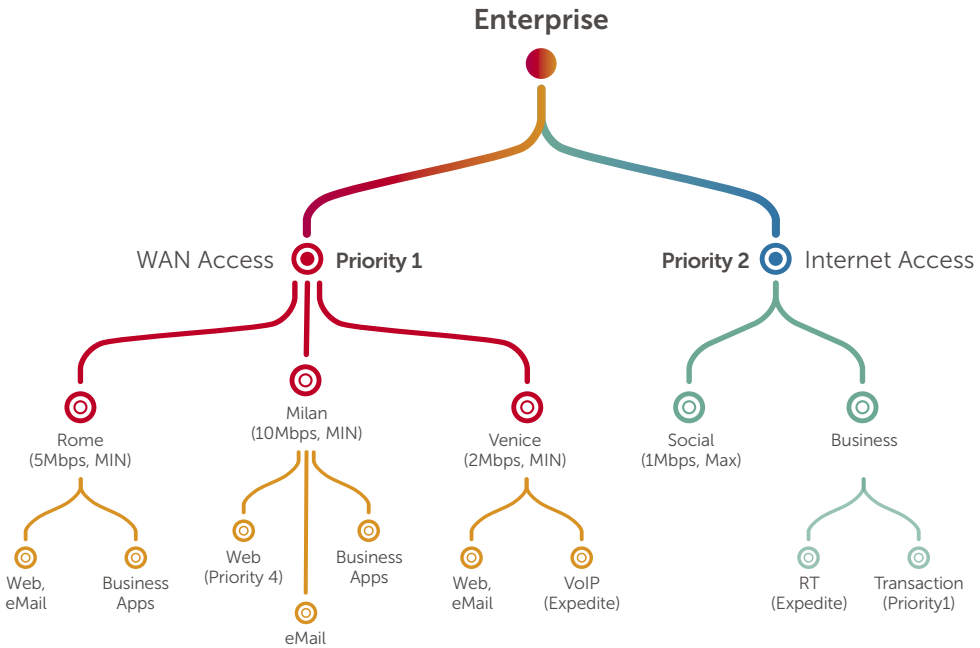
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

TRANSPORTATION
ACCEPTABLE USAGE MANAGEMENT

Internet connectivity is essential to the success of all business. Enterprises can manage this resource by establishing an acceptable usage policy that controls the utilization by individual facilities, departments, users, and applications. For example, management would be advised to block P2P downloads of shared content with applications such as BitTorrent because they consume bandwidth, may be used to export valuable corporate information, and invite malware into a network. In addition, the enterprise may limit access or assign quotas to social networks during business hours, and prioritize business applications over other Internet traffic. Through acceptable usage rules, enterprises can prevent individuals and applications from monopolizing Internet bandwidth, ensure quality of service for all users, and minimize non-business Internet activity to improve productivity and postpone costly infrastructure investments.

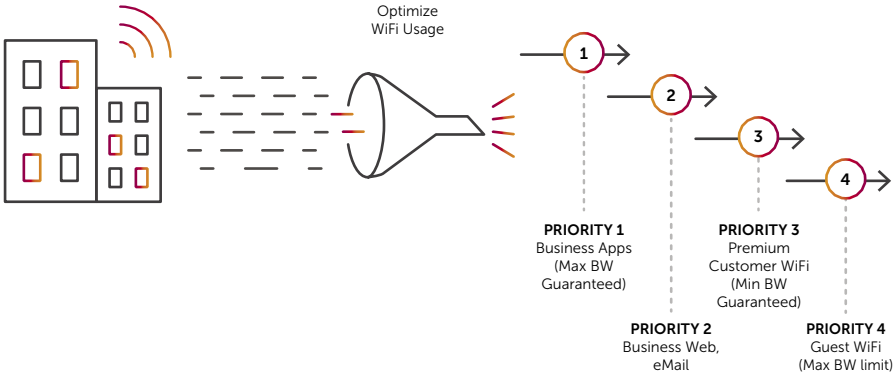
TRAFFIC MANAGEMENT & ACCEPTABLE USE POLICY



TRANSPORTATION
WI-FI OPTIMIZATION

A growing number of Wi-Fi service providers are the national media and telecom companies who offer Wi-Fi services to attract customers and enhance their in-house experience. This service can be easily monopolized by a few heavy users, and therefore requires fair usage management. For example, a media company cannot afford to enable its employees to download and stream high-definition movies during business hours. DPI-based solutions enable these enterprises to monitor Wi-Fi utilization in real time and enforce QoS based on dynamic network conditions.

WI-FI OPTIMIZATION



Key Benefits

- Prevent Wi-Fi network congestion
- Ensure Wi-Fi service availability to all users
- Enhance customer satisfaction

Wi-Fi Optimization in Action

- Map congestion conditions into fair usage policy rules
- Utilization threshold automatically triggers fair usage policy enforcement
- Rate-limit all users or only excessive users
- Automatically restore regular policy when congestion subsides

Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure

Key Benefits

- Match Wi-Fi service to diverse groups of customers and employees
- Increase revenue through tiered Wi-Fi packages as well as real-time and post-event upsell
- Improve resource utilization and planning through full visibility and tracking

Wi-Fi Service Tiers in Action

- Define tiers of services by user groups
- Apply traffic/bandwidth management policy at different tiers
- Enforce tiered Wi-Fi service plans and control congestion in real time
- Provide detailed usage reports to customers and management

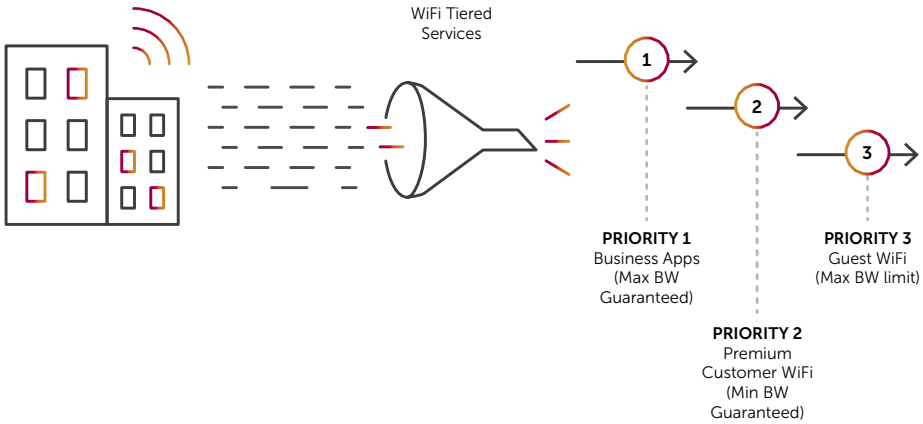
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics
- Allot Subscriber Management Platform

TRANSPORTATION
WI-FI SERVICE TIERS

Hotels, airports, convention centers, and public transportation often serve individual kinds of customer and employees; hotel guests, convention center attendees, exhibitors, and staff. The Wi-Fi connectivity requirements for these user groups are typically quite different and require multiple bandwidth management policies. For example, guest rooms may receive a fixed amount of Wi-Fi bandwidth with an option to pay-for-more, while convention and show floor areas allocate bandwidth according to a tiered pricing structure per event. Numerous show floor policies may be in use at an event, offering a range of Wi-Fi access speeds, with real-time upsells enabled by a central Command-and-Control office. At the same time, congestion thresholds are monitored, triggering peak usage policies that may limit Peer-to-Peer (P2P) traffic or individual connection establishment rates, ensuring sufficient bandwidth to meet Service Level Agreements (SLAs).

WIFI TIERED SERVICES

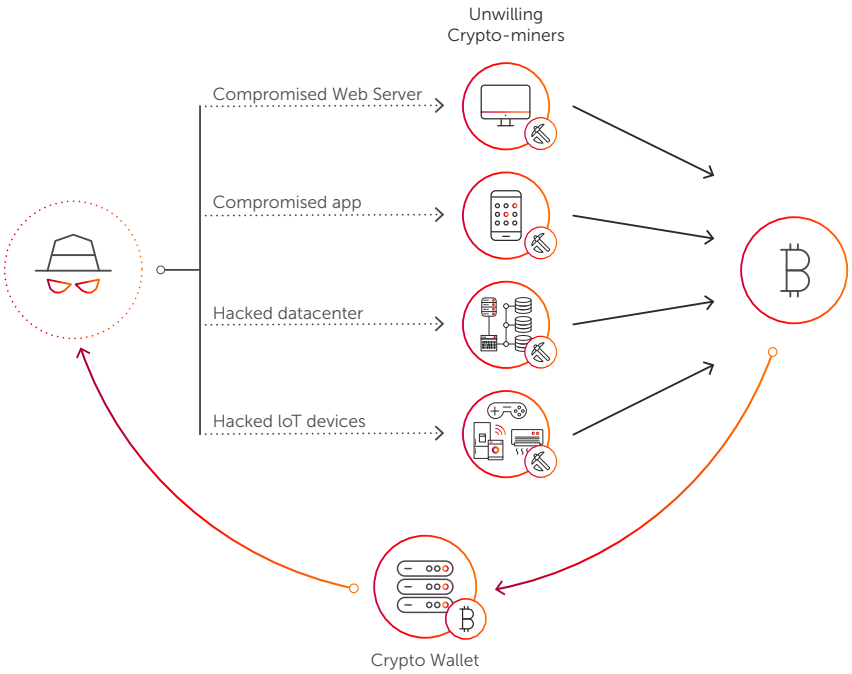


TRANSPORTATION

CRYPTOJACKING IDENTIFICATION AND MITIGATION

Cryptocurrency hijacking, or "cryptojacking" is one of the key threats Enterprise IT teams are facing today. Cryptomining requires massive amounts of computer processing resources, and cryptojackers are targeting CPU and GPU power located in companies and organizations as a means of mining for free. Network monitoring is certainly the best way to protect against cryptojacking. Cryptojackers must be able to communicate with their targeted servers, receive new hashes, calculate them, and return them to their own servers. Allot's NetworkSecure and Secure Service Gateway can identify this activity and protect valuable enterprise resources from cryptojacking attacks.

CRYPTO INFECTION ALERT



Key Benefits

- Isolate Coinhive libraries, which mines the Monero cryptocurrency
- Broad recognition and policy enforcement of cryptomining protocols & applications
- Prevent server resources from being hijacked and impairing business application performance
- Prevent valuable networking hardware from damage through overheating, and saving electricity consumption costs associated with cryptomining

Cryptojacking Identification and Mitigation in Action

- Identify and block Crypto malware
- Block access to web sites that inject Cryptomining software
- Identify and block Cryptomining protocols
- Identify and block P2P, VPNs, and other applications that enable Cryptojacking attacks

Powered by Allot Secure Service Gateway (SSG)

- Allot Web Security
- Allot Visibility & Control

FINAL WORD

The true business of your network is business processes. Bandwidth, throughput, latency, and other common communications metrics are all aspects of evaluating how well your network supports your internal and external processes to conduct business. And sometimes it is your network that is the business.

As demonstrated in the use cases contained in this booklet, Allot SSG provides added value to operations, planning, and your business. All our customers found immediate value the minute they turned on the lights in their networks and actually saw live application, user, and network behavior. In our experience, there is often a misalignment between the way companies think their business processes are working and the way they actually work.

Processes generally underperform for the following reasons:

- The flow of applications that compose the process is broken
- The network is experiencing congestion and other traffic or equipment malfunctions
- Security-related anomalies are impairing or causing denial of service

Network visibility and control solutions can highlight all of these issues in real time and provide the tools to fix them. Your IT team will be able to identify specific protocols and applications, either encrypted or not, and monitor and measure any static or dynamic policy element that you define.

Increased visibility will also provide IT with insights into how to increase network performance. For example, seeing which employees are using what applications and when, you can prioritize access and define traffic management policies that meet your business goals and user expectations and make fully informed decisions about the size and timing of future network investment.

For more information, visit: https://www.allot.com/enterprise