Use Cases

Local & National Government

Enterprise

INTRODUCTION

This document provides a selection of customer use cases applicable for the governmental sector. Each use case describes an individual challenge faced by governmental organizations 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

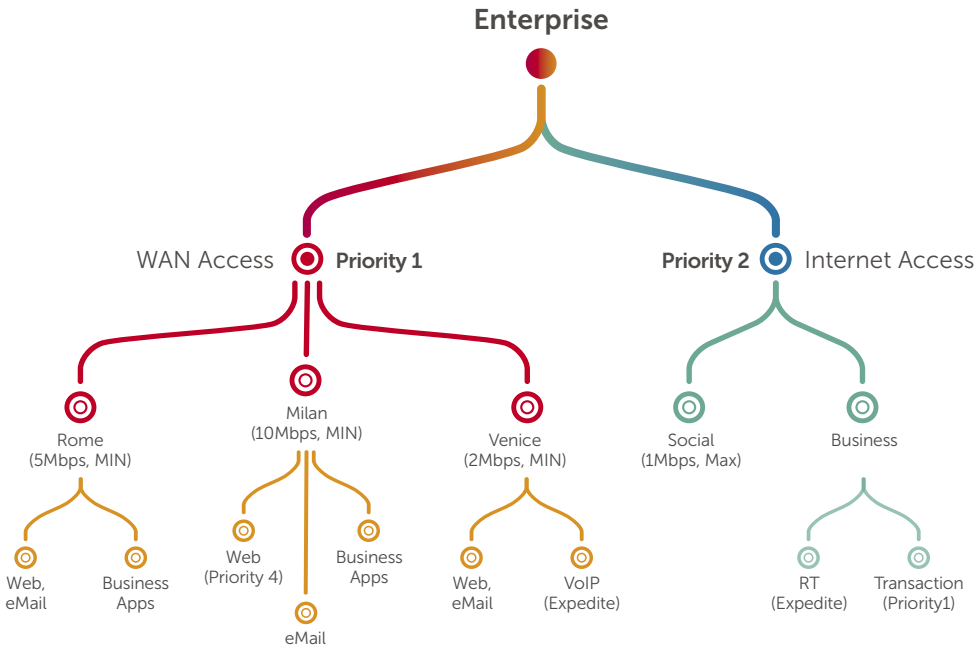
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

LOCAL & NATIONAL GOVERNMENT
ACCEPTABLE USAGE MANAGEMENT

Internet connectivity is essential to the success of all enterprises. Local and national government organizations 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 organization may limit access or assign quotas to social networks during business hours, and prioritize business applications over other Internet traffic. Through acceptable usage rules, governmental organizations 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



Patriotism is supporting your country all the time, and your government when it deserves it.

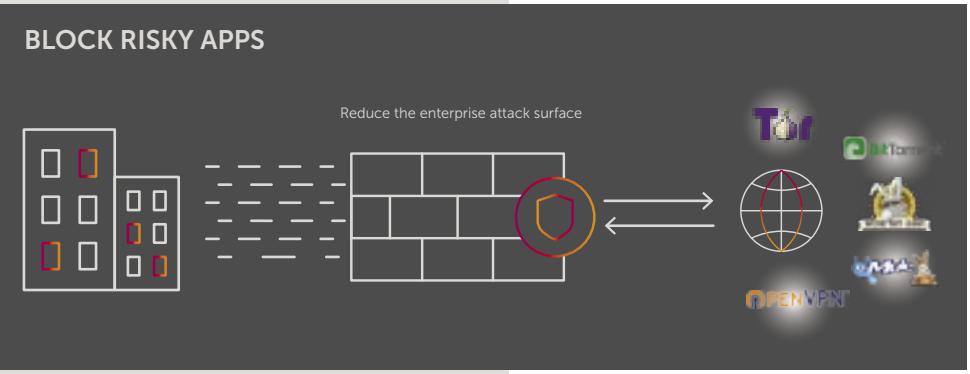
Mark Twain

Key Benefits

- Reduce the attack surface by blocking risky applications
- Identify and control the use of risky applications and unsanctioned IT applications, Virtual Private Networks (VPNs), and anonymizers
- Block traffic that circumvents security controls

Control Risky and Unsanctioned Applications in Action

- Detects and controls a range of anonymizers, peer-to-peer, and file-sharing applications
- Bi-weekly application recognition updates
- Blocks and limits user traffic that employs unsanctioned IT applications



Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

LOCAL & NATIONAL GOVERNMENT
CONTROL RISKY AND UNSANCTIONED APPLICATIONS

Heavy use of low priority or recreational applications and websites consumes considerable bandwidth and can congest and impair your network operations. Furthermore, some applications pose high levels of risk that extend beyond operational effectiveness, for example:

Peer-to-peer applications provide a backdoor to host data that can be accessed by anyone on the peer-to-peer network, and programs or content that is downloaded can include malware or violate copyrights.

Anonymizers/VPN tunnels are typically used to hide a user's identity and are in use by some to access illegal content or purchase illegal goods, such as drugs.

Although these applications can be used for the intended purpose of privacy, they are also used to hide illegal activities or they are exploited for cyberattacks. By nature, they are designed to bypass conventional security controls such as firewalls and Intrusion Detection System (IDS). They achieve concealment using encryption and obfuscation and identifying them is not a trivial effort.

Allot employs advanced mechanisms to detect encrypted applications that enable an enterprise to identify risk and/or malicious apps without having to decrypt them. These methods include the following and apply to encrypted HTTP and non-HTTP traffic:

- Traffic statistics
- Server Name Indicator (SNI) detection
- Machine learning algorithms
- Pattern detection
- Certificates analysis
- Secure Sockets Layer (SSL) extensions analysis
- Traffic heuristics

LOCAL & NATIONAL GOVERNMENT
INTERNET OF THINGS (IOT) INTELLIGENCE

IoT devices are typically designed for a specific purpose and typically they would use a limited set of protocols and applications when communicating with their back-end servers. This enables an organization to reduce the attack surface of IoT deployments by applying a policy that controls access to authorized servers and limits communication patterns to expected normal behavior. In addition, the SSG provides proactive defense of your network against IoT bots such as Reaper and Mirai with in line anti-malware and anti-bot capabilities and by identifying and quarantining malware-infected devices before they adversely affect the IoT deployment, network performance and integrity. Allot security solutions monitor connection establishment rates and other symptoms of anomalous user behavior, enabling organizations to surgically treat the root cause (that is, the malware-infected device) without having to resort to broader measures such as blocking entire subnets, links, or ports. Behavior-based anomaly detection enhances existing security layers with frontline mitigation of DDoS bots and other malware.

ALLOT SSG FOR IOT VISIBILITY, SECURITY & CONTROL

Key Benefits

- IoT sensor monitoring and security
- Anomaly alerts and reporting
- Prevention of bandwidth congestion and improvement of Quality of Experience (QoE) for correct sensor operation

Internet of Things (IoT) Intelligence in Action

- Apply access control and traffic policy to expected behavior of IoT deployments
- Detect anomalous behavior consistent with malware
- Identify malware (mass Domain Name Servers (DNS), spam bots, and port scanning)
- Measures sensor response time and allocates bandwidth for each sensor according to its defined operation
- Notify control services upon any anomalous activity

Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure
- Network Behavior Analysis Engine

Key Benefits

- Accommodate a wide range of employee workloads
- Align Internet access and resource allocation to organizational priorities
- Control cloud access costs

Managing Cloud Migration in Action

- Prioritize cloud applications and limit Internet traffic that is not organization-related
- Apply dynamic Quality-of-Experience-based congestion control
- Enforce priorities for specific applications and/or users
- Gain granular visibility on cloud application usage

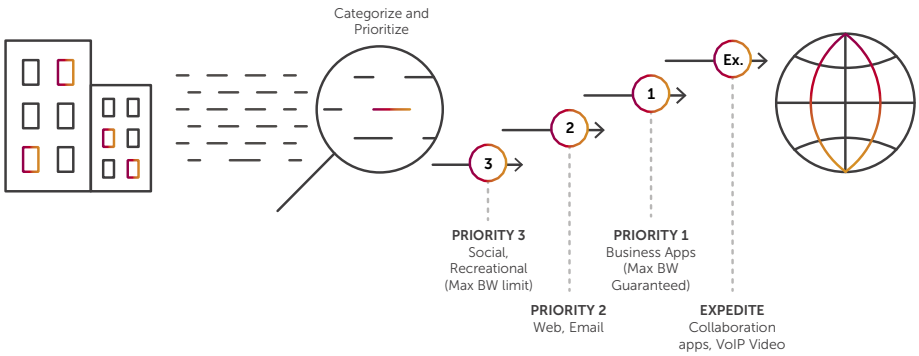
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

LOCAL & NATIONAL GOVERNMENT
MANAGING CLOUD MIGRATION

Many organizations are migrating applications from their private data centers to cloud-based applications. For example, exchange and collaboration servers are being replaced with Office 365 and on-premise CRM with Salesforce. The benefits of cloud migration are reduced cost, ubiquitous access, and zero maintenance and yet many organizations have received bill shock from unexpected usage and struggle to maintain a high level of user Quality of Experience (QoE). DPI-based traffic management and policy control solutions enable enterprises to monitor usage and behavior of cloud based applications and enforce priorities and committed data rates (Internet bandwidth) for business applications over personal content. QoE-based congestion control dynamically prioritizes Internet access based on organizational priorities by measuring multiple metrics and scoring the perceived QoE and end user would be receiving. With granular usage reporting, informed upgrades can be made when they are required to support the organization.

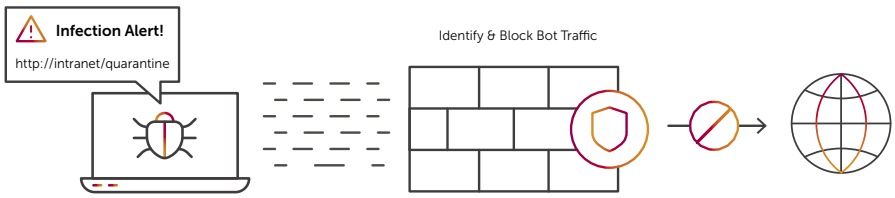
CLOUD MIGRATION, BUSINESS APP



LOCAL & NATIONAL GOVERNMENT
REAL-TIME BOT CONTAINMENT

Defend your network against malicious bots by neutralizing malware-infected hosts and spam activity before it adversely affects network performance and integrity. Prevent unintended spam and Internet Protocol (IP)- scanning traffic from eating up valuable bandwidth and quickly identify infected hosts that require cleanup. Allot security solutions monitor connection establishment rates and other symptoms of anomalous user behavior, enabling organizations to surgically treat the root cause (that is, the malware-infected host) without having to resort to broader measures such as blocking entire subnets, links, or ports. Behavior-based anomaly detection enhances existing security layers with frontline mitigation of bots and other malware.

INFECTION ALERT



Key Benefits

- Protect network integrity through the rapid treatment of bot infections
- Ensure organizational productivity by containing infected hosts
- Reduce help-desk time spent on problems resulting from malware

Real-time Bot Containment in Action

- Detect anomalous host behavior consistent with malware
- Identify malware through network behavior (mass-DNS, spam-bots, and port scanning)
- Block, limit, or quarantine user traffic within seconds
- Notify user and redirect to clean-up portal

Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure
- Host Behavior Analysis Engine

Key Benefits

- Protect data center availability and efficiency
- Ensure data center Service Level Agreements (SLAs) and minimize the risk of outages
- Gain visibility into attackers and their targets in your cloud

Real-time DDoS Attack Mitigation in Action

- In-line detection and mitigation in seconds, provides immediate remediation for short-lived attacks
- Detects traffic anomaly consistent with DDoS attacks including zero-day attacks—blocked memcached amplification attacks on first instance
- Creates custom signatures to precisely filter attack packets
- Mitigation applied automatically, or upon manual verification
- System issues detailed attack report and statistics

Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure
- Network Behavior Analysis Engine

LOCAL & NATIONAL GOVERNMENT
REAL-TIME DDOS ATTACK MITIGATION

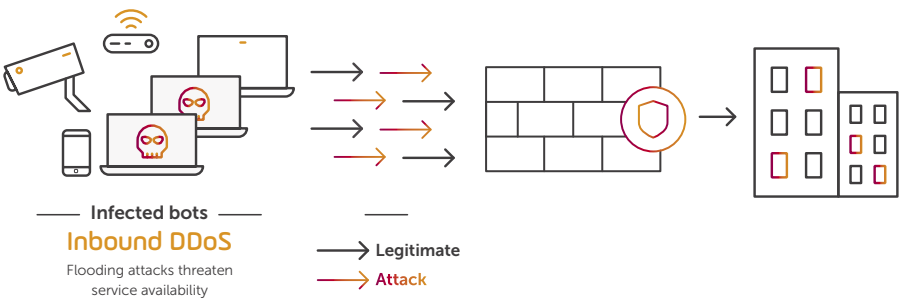
DDoS attacks are growing in intensity and sophistication every year such as memcached attacks and short-lived attacks that confound cloud-based DDoS mitigation solutions. Enterprise data centers are at the heart of modern day organizational operation and even minutes of downtime can result in significant revenue loss. By combining advanced traffic management with behavioral Distributed Denial of Service (DDoS) detection and mitigation, zero downtime can be achieved even under attack by maintaining critical business applications. In-line DoS/DDoS protection neutralizes flooding attacks within seconds of emergence by rapidly detecting, identifying, and filtering DDoS packets, while enabling legitimate traffic to flow unimpeded.

DDoS PROTECTION

In-line detection and mitigation blocks attacks in seconds

Protect perimeter devices; Firewalls, IPs and Load Balancers

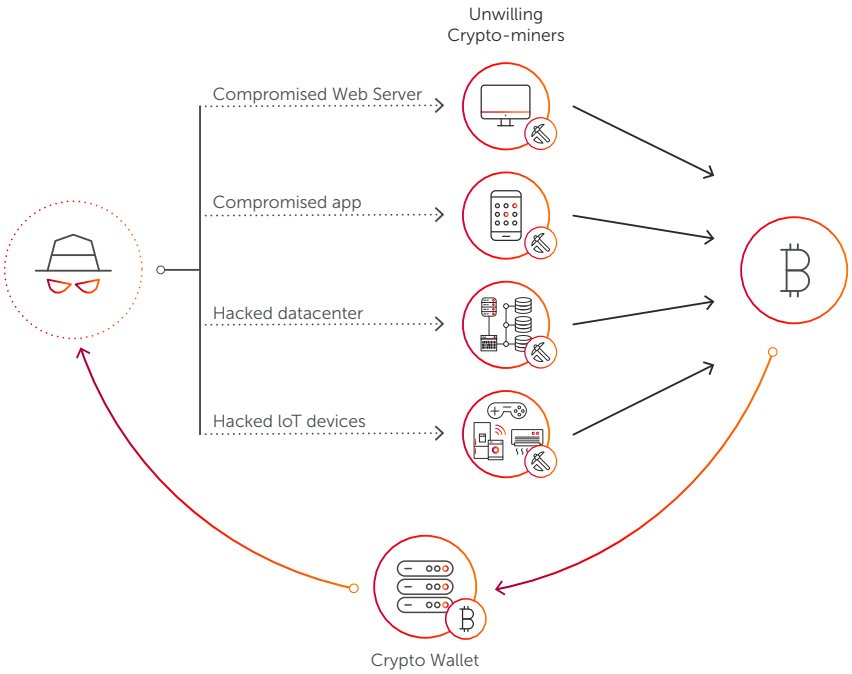
Assure service availability with dynamic congestion management and critical application prioritization



LOCAL & NATIONAL GOVERNMENT
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