allot

See. Control. Secure.

Use Cases

Enterprise

CONTENTS

INTRODUCTION

This document provides use cases by market sectors to enable you to align your network performance with your business priorities. It will help you to increase your 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 meets your business priorities. In addition, you can reduce the total cost of ownership of your security investment by leveraging both the built-in Secure Web Gateway function that protects your users against diverse types of web threats and Allot's behavioral engines that combat botnets and mitigate DDoS attacks.

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 leverages superior 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 Returns on Investment (ROI) on their IT infrastructure. Allot solutions are deployed worldwide in data centers and enterprise networks from all sectors, including e-commerce, education, energy, utilities, finance, government, healthcare, higher education, hospitality, media & 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. The cases leverage 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 adjusts 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

- Ensure availability and response time of critical applications
- Enhance user productivity and satisfaction
- Align network performance to business priorities
- Invest in infrastructure expansion when needed to meet business requirements

Business Application Prioritization in Action

- Analyze usage and performance of business applications and the Quality of Experience (QoE) that they deliver
- Define and enforce priority Quality of Service (QoS) for each application and propagate this across the network
- Enforce dynamic QoE-based congestion control aligned to business priorities
- Troubleshoot and act upon alerts as they occur

Powered by Allot Secure Service Gateway (SSG)

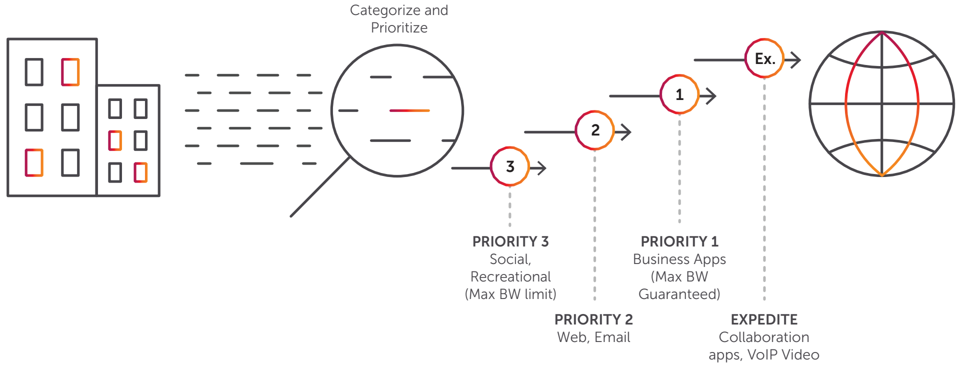
- Allot Gateway Manager
- Allot ClearSee Analytics

E-COMMERCE

BUSINESS APPLICATION PRIORITIZATION

Every enterprise relies on networked applications to conduct business successfully. In a connected world, corporate networks serve many applications ranging from recreational to business-critical. For the business to operate efficiently the IT team must ensure application availability and response time to all users and all access modes. Application control begins with understanding how critical applications are used, how they perform under different network conditions, and what are the factors that IT can control to ensure their delivery.

CLOUD MIGRATION, BUSINESS APP

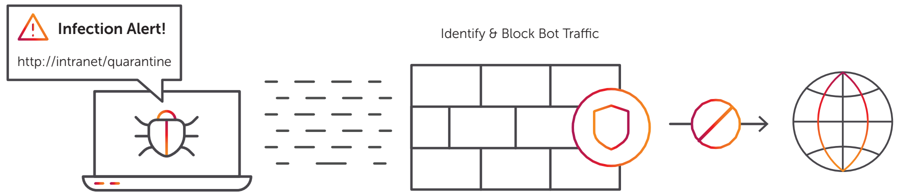

Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Business Apps (Max BW Guaranteed)
EXPEDITE
Collaboration apps, VoIP Video

Based on this analysis, each application receives a tailored QoS policy, which may define congestion thresholds along with some form of expedited forwarding (depending on delay sensitivity). It may also define guaranteed minimum bandwidth or separate data rates for inbound and outbound traffic. Altogether, these parameters ensure that business processes and users of Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Voice over Internet Protocol (VoIP), video conferencing, and other business applications can work more productively and with greater efficiency.

E-COMMERCE
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 enterprises 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 business 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

E-COMMERCE
REAL-TIME DDoS ATTACK MITIGATION

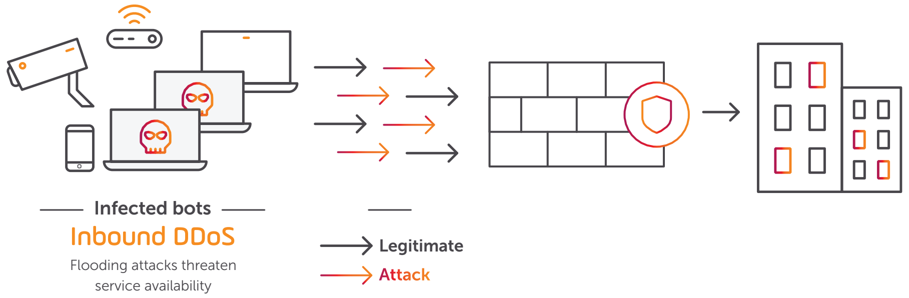
DDoS attacks are growing in intensity and sophistication every year such as memcached attacks and short-lived attacks that confound cloud-based DDoS mitigation solutions. Enterprise data centers are at the heart of modern day business operation and even minutes of downtime can result in significant revenue 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



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

Key Benefits

- Prevent excessive, non-business 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-business-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 a corporate network

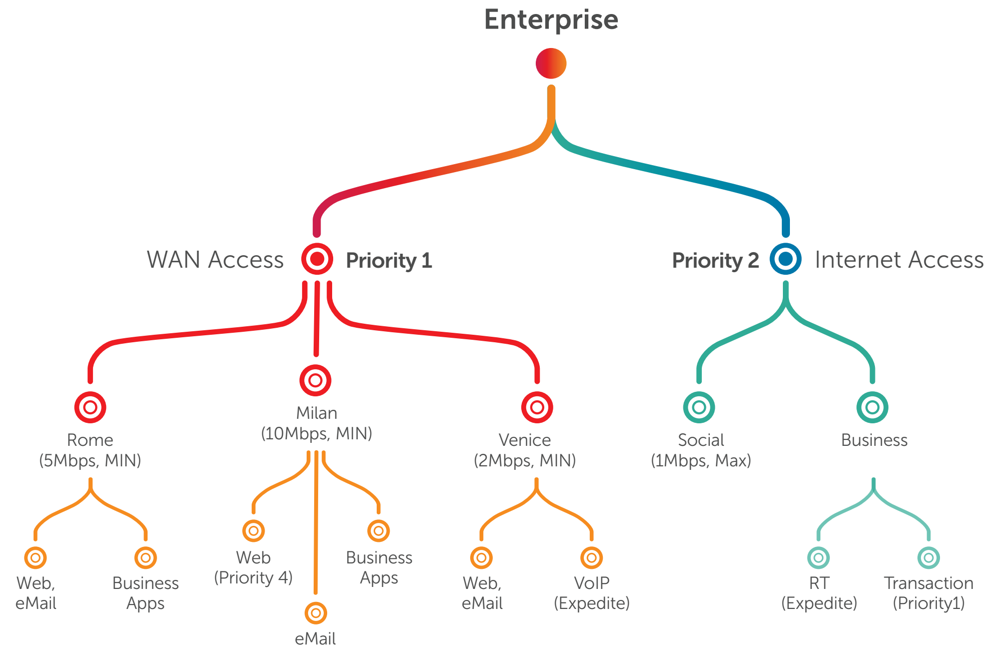
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

ENERGY & UTILITIES 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

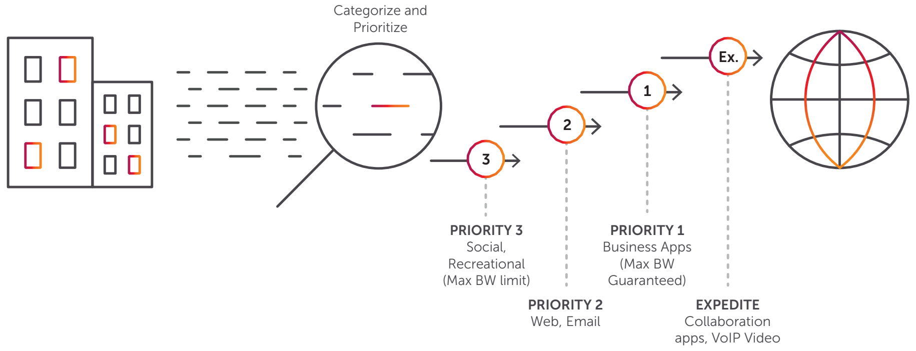


ENERGY & UTILITIES
BUSINESS APPLICATION PRIORITIZATION

Every enterprise relies on networked applications to conduct business successfully. In a connected world, corporate networks serve many applications ranging from recreational to business-critical. For the business to operate efficiently the IT team must ensure application availability and response time to all users and all access modes.

Application control begins with understanding how critical applications are used, how they perform under different network conditions, and what are the factors that IT can control to ensure their delivery. Based on this analysis, each application receives a tailored QoS policy, which may define congestion thresholds along with some form of expedited forwarding (depending on delay sensitivity). It may also define guaranteed minimum bandwidth or separate data rates for inbound and outbound traffic. Altogether, these parameters ensure that business processes and users of Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Voice over Internet Protocol (VoIP), video conferencing, and other business applications can work more productively and with greater efficiency.

CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Business Apps (Max BW Guaranteed)
EXPEDITE
Collaboration apps, VoIP Video

Key Benefits

- Ensure availability and response time of critical applications
- Enhance user productivity and satisfaction
- Align network performance to business priorities
- Invest in infrastructure expansion when needed to meet business requirements

Business Application Prioritization in Action

- Analyze usage and performance of business applications and the Quality of Experience (QoE) that they deliver
- Define and enforce priority Quality of Service (QoS) for each application and propagate this across the network
- Enforce dynamic QoE-based congestion control aligned to business priorities
- Troubleshoot and act upon alerts as they occur

Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

Key Benefits

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

Managing Cloud Migration in Action

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

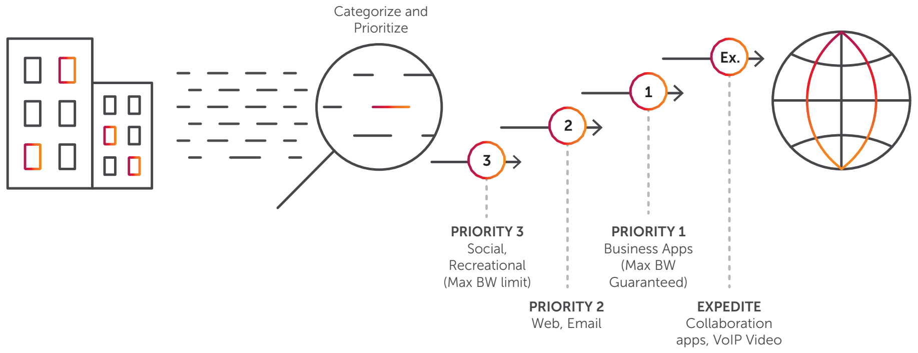
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

ENERGY & UTILITIES
MANAGING CLOUD MIGRATION

Many businesses 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 companies 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 business 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 business.

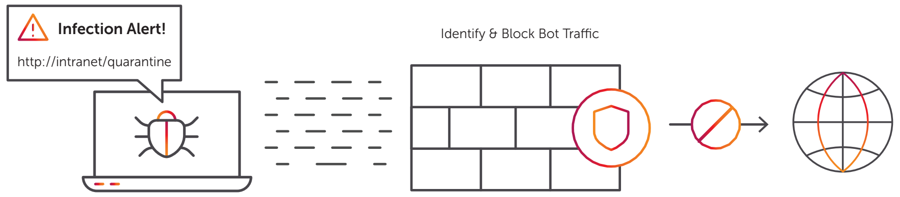
CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Business Apps (Max BW Guaranteed)
EXPEDITE
Collaboration apps, VoIP Video

ENERGY & UTILITIES
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 enterprises 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 business 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

ENERGY & UTILITIES
REAL-TIME DDoS ATTACK MITIGATION

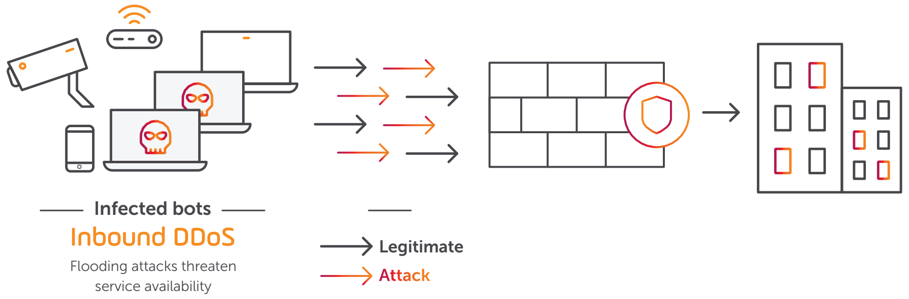
DDoS attacks are growing in intensity and sophistication every year such as memcached attacks and short-lived attacks that confound cloud-based DDoS mitigation solutions. Enterprise data centers are at the heart of modern day business operation and even minutes of downtime can result in significant revenue 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



ENERGY & UTILITIES
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:

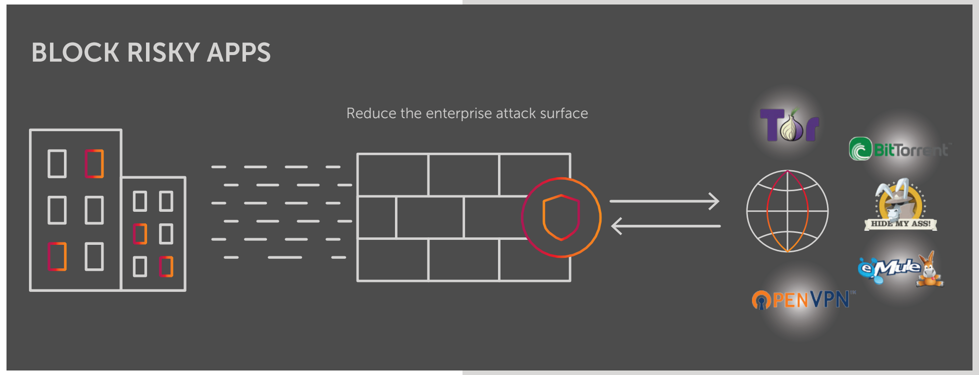
Peer-to-peer applications provide a backdoor to host data that can be accessed by anyone on the peer-to-peer network, and programs or content that is downloaded can include malware or violate copyrights.

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:

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



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

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 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

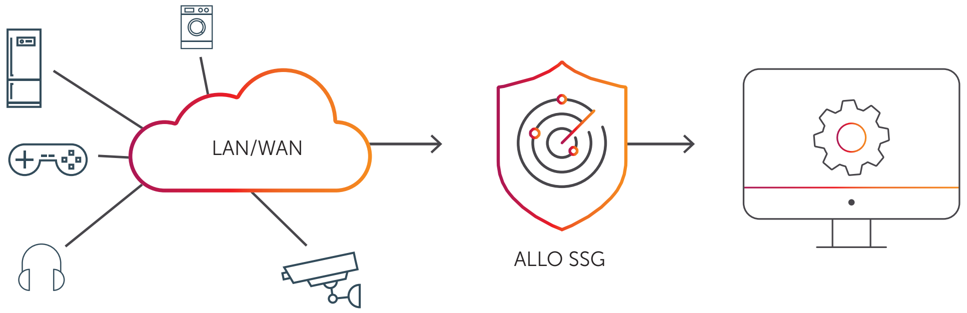
Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure
- Network Behavior Analysis Engine
- Host Behavior Analysis Engine
- ClearSee Analytics

ENERGY & UTILITIES
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 characteristic enables an enterprise 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 SSG FOR IOT VISIBILITY, SECURITY & CONTROL



Allot security solutions monitor connection establishment rates and other symptoms of anomalous user behavior, enabling enterprises 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.

Key Benefits

- Prevent excessive, non-business 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-business-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 a corporate network

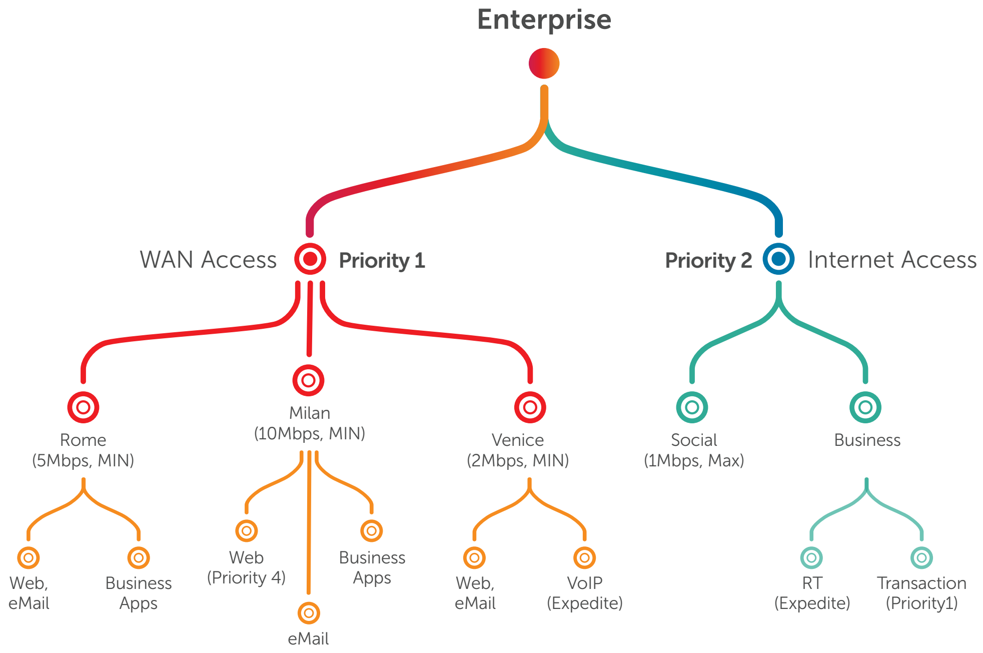
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

FINANCE
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

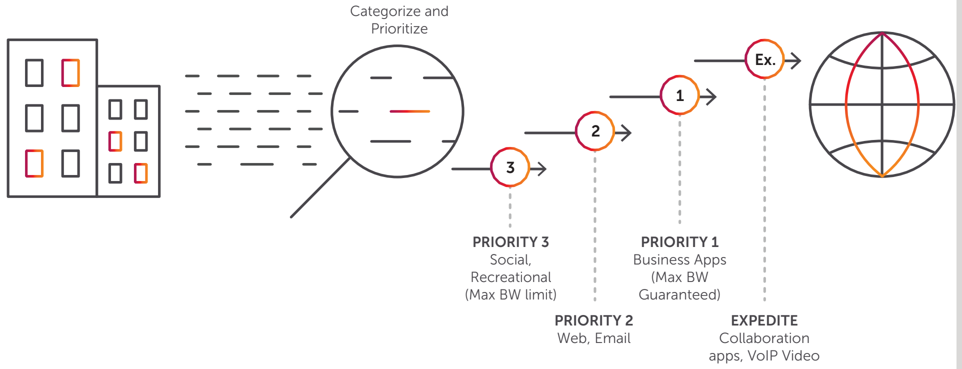


FINANCE
BUSINESS APPLICATION PRIORITIZATION

Every enterprise relies on networked applications to conduct business successfully. In a connected world, corporate networks serve many applications ranging from recreational to business-critical. For the business to operate efficiently the IT team must ensure application availability and response time to all users and all access modes.

Application control begins with understanding how critical applications are used, how they perform under different network conditions, and what are the factors that IT can control to ensure their delivery. Based on this analysis, each application receives a tailored QoS policy, which may define congestion thresholds along with some form of expedited forwarding (depending on delay sensitivity). It may also define guaranteed minimum bandwidth or separate data rates for inbound and outbound traffic. Altogether, these parameters ensure that business processes and users of Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Voice over Internet Protocol (VoIP), video conferencing, and other business applications can work more productively and with greater efficiency.

CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Business Apps (Max BW Guaranteed)
EXPEDITE
Collaboration apps, VoIP Video

Key Benefits

- Ensure availability and response time of critical applications
- Enhance user productivity and satisfaction
- Align network performance to business priorities
- Invest in infrastructure expansion when needed to meet business requirements

Business Application Prioritization in Action

- Analyze usage and performance of business applications and the Quality of Experience (QoE) that they deliver
- Define and enforce priority Quality of Service (QoS) for each application and propagate this across the network
- Enforce dynamic QoE-based congestion control aligned to business priorities
- Troubleshoot and act upon alerts as they occur

Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

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

FINANCE
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.

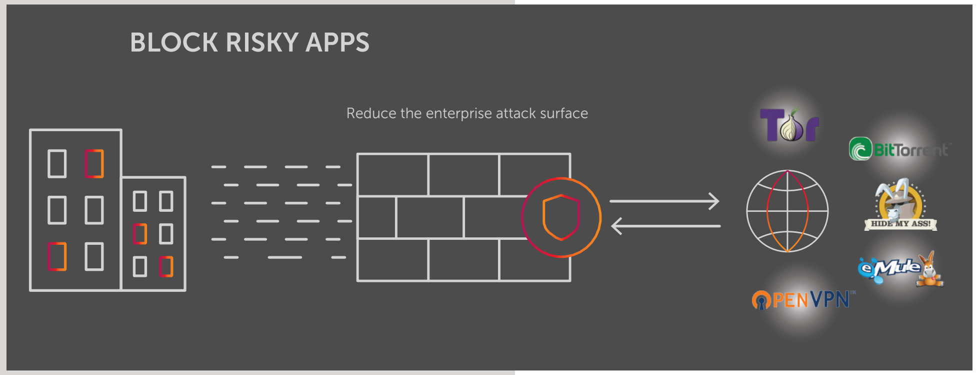
Anonymizers/VPN tunnels are typically used to hide a user's identity and are in use by some to access illegal content or purchase illegal goods, such as drugs.

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

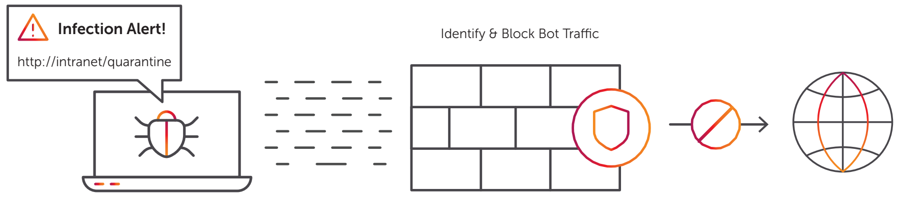
BLOCK RISKY APPS



FINANCE
MANAGING CLOUD MIGRATION

Many businesses 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 companies 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 business 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 business.

INFECTION ALERT!



Key Benefits

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

Managing Cloud Migration in Action

- Prioritize business cloud applications and limit Internet traffic that is not business-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

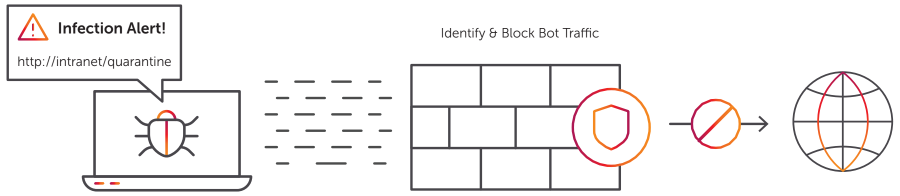
> Beware of little expenses.
> A small leak will sink a great ship.
>
> Benjamin Franklin

FINANCE

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 enterprises 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 business productivity by containing infected hosts
- Reduce help-desk time spent on problems resulting from malware
- Invest in infrastructure expansion when needed to meet business requirements

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

FINANCE

REAL-TIME DDOS ATTACK MITIGATION

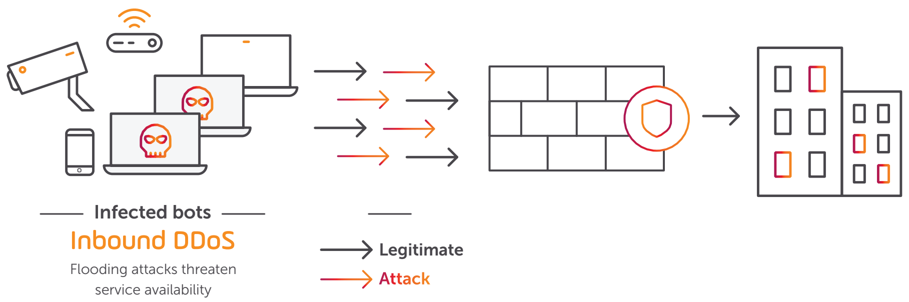
DDoS attacks are growing in intensity and sophistication every year such as memcached attacks and short-lived attacks that confound cloud-based DDoS mitigation solutions. Enterprise data centers are at the heart of modern day business operation and even minutes of downtime can result in significant revenue 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



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

Key Benefits

- Prevent excessive, non-business 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-business-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 a corporate network

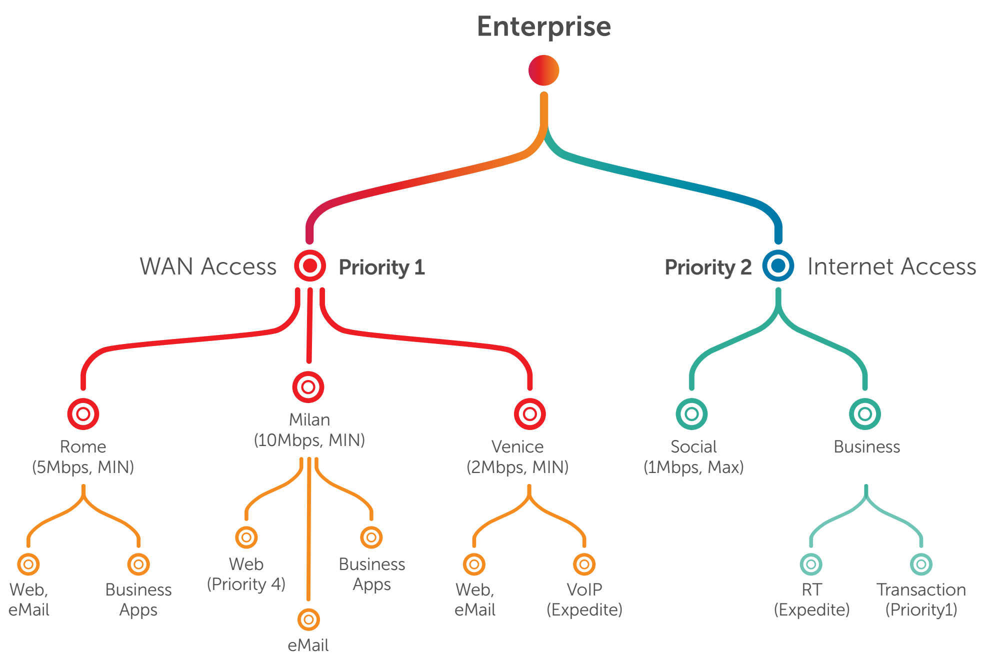
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

HEALTHCARE 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



HEALTHCARE

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:

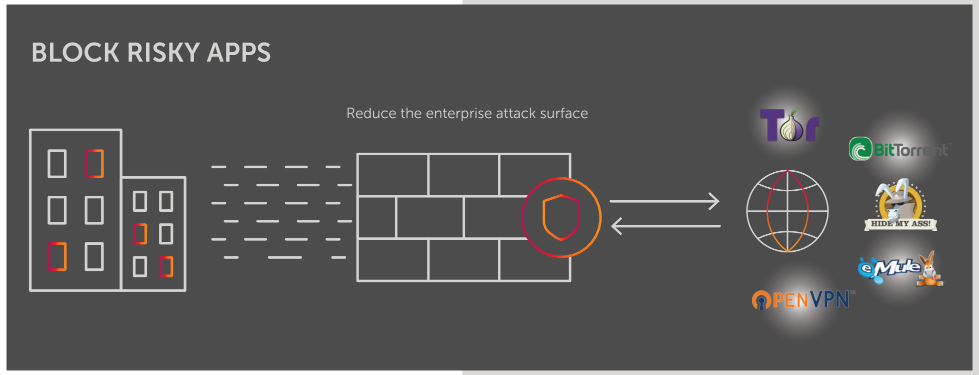
Peer-to-peer applications provide a backdoor to host data that can be accessed by anyone on the peer-to-peer network, and programs or content that is downloaded can include malware or violate copyrights.

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:

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



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 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

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)

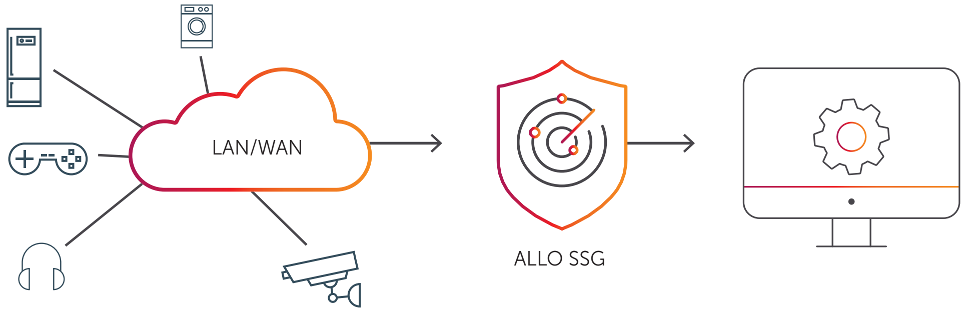
- Allot DDoS Secure
- Network Behavior Analysis Engine
- Host Behavior Analysis Engine
- ClearSee Analytics

HEALTHCARE

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 enterprise 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 enterprises 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

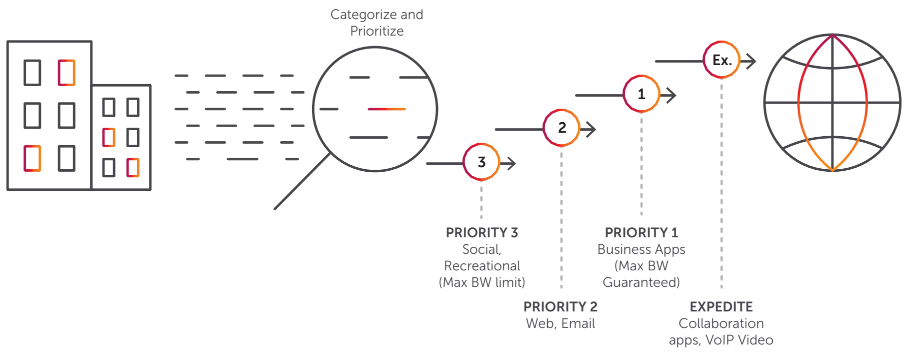


HEALTHCARE

MANAGING CLOUD MIGRATION

Many businesses 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 companies 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 business 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 business.

CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Business Apps (Max BW Guaranteed)
EXPEDITE
Collaboration apps, VoIP Video

Key Benefits

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

Managing Cloud Migration in Action

- Prioritize business cloud applications and limit Internet traffic that is not business-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)

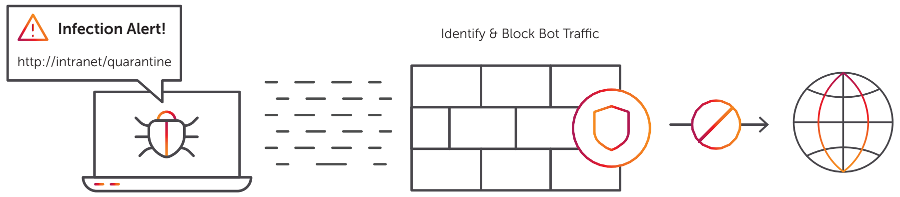
- • Allot Gateway Manager
- • Allot ClearSee Analytics

HEALTHCARE

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 enterprises 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 data center availability and efficiency
- Ens Protect network integrity through the rapid treatment of bot infections
- Ensure business productivity by containing infected hosts
- Reduce help-desk time spent on problems resulting from malware
- ure data center Service Level Agreements (SLAs) and minimize the risk of outages
- Gain visibility into attackers and their targets in your cloud

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

HEALTHCARE
REAL-TIME DDoS ATTACK MITIGATION

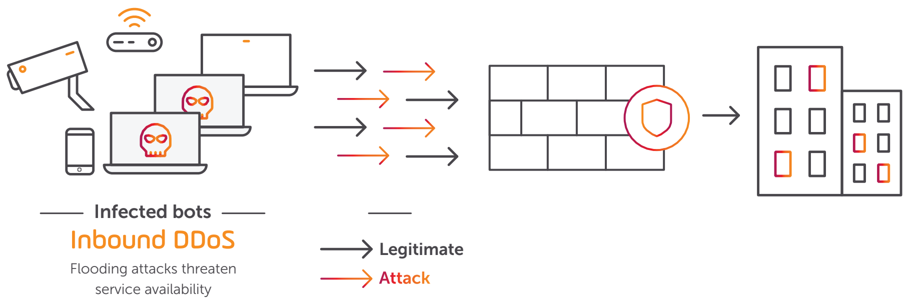
DDoS attacks are growing in intensity and sophistication every year such as memcached attacks and short-lived attacks that confound cloud-based DDoS mitigation solutions. Enterprise data centers are at the heart of modern day business operation and even minutes of downtime can result in significant revenue 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



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

HEALTHCARE
WI-FI OPTIMIZATION

A growing number of Wi-Fi service providers include medical organizations who offer in-department Wi-Fi service to provide Internet services to their clients to enhance their healthcare experience. This service can be easily monopolized by a few heavy users, and therefore requires fair usage management. For example, a hospital department cannot afford to allow the child of a patient to consume all the department's bandwidth watching HD videos while he waits for his parent to complete an out-patient visit. DPI-based solutions enable these enterprises to monitor Wi-Fi utilization in real time and enforce QoS based on dynamic network conditions.

Key Benefits

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

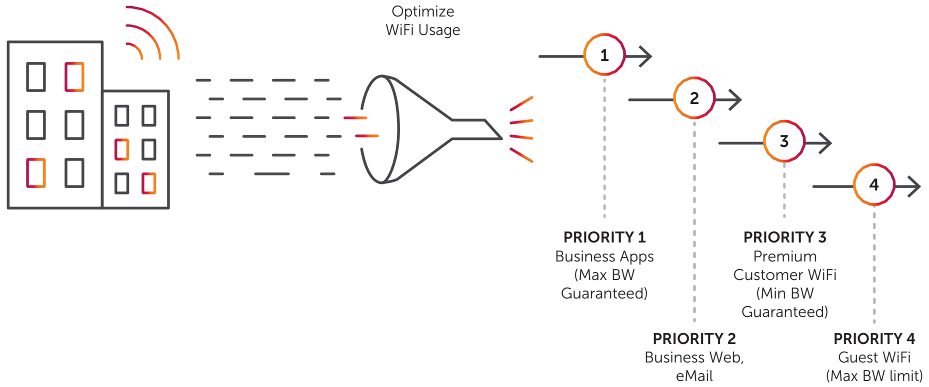
Wi-Fi Optimization in Action

- 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

WI-FI OPTIMIZATION

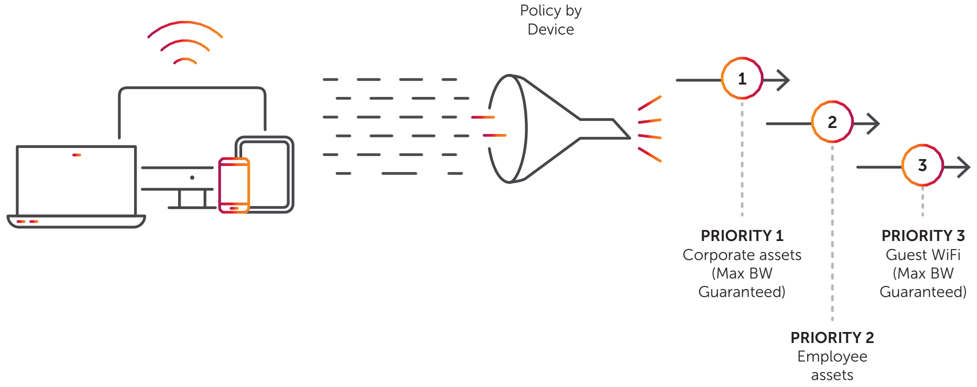

Optimize WiFi Usage
1
2
3
4
PRIORITY 1
Business Apps (Max BW Guaranteed)
PRIORITY 2
Business Web, eMail
PRIORITY 3
Premium Customer WiFi (Min BW Guaranteed)
PRIORITY 4
Guest WiFi (Max BW limit)

HIGHER EDUCATION

BRING YOUR OWN DEVICE (BYOD)

While many IT managers see Bring-Your-Own-Device (BYOD) as an inevitable disruption that opens the network to security risks, users see it as a great enabler of personal productivity and efficiency. Enterprises require the ability to enforce usage rules for personal devices once they are on the network. BYOD rules may include throttling heavy usage, allocating more bandwidth to employee devices over guest devices, and giving priority to business applications. Allot’s superior Deep Packet Inspection (DPI) technology provides device signatures in the same way that it provides application signatures, and it updates them regularly. This ensures timely and accurate identification of non-corporate devices and their traffic on the network.

BYOD


Policy by Device
1
2
3
PRIORITY 1
Corporate assets (Max BW Guaranteed)
PRIORITY 2
Employee assets
PRIORITY 3
Guest WiFi (Max BW Guaranteed)

Key Benefits

- Permit use of personal devices to enhance employee productivity
- Ensure personal devices do not compromise a network
- Strengthen network security measures

Bring Your Own Device in Action

- Map BYOD rules into Wi-Fi management policy
- Automatically detect traffic from personal devices
- Enforce BYOD rules in real time
- Review BYOD usage reports to evaluate and refine policy

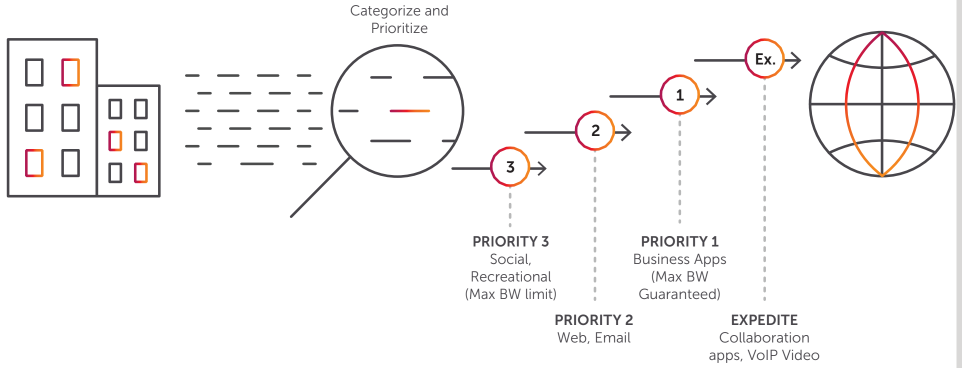
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

HIGHER EDUCATION
BUSINESS APPLICATION PRIORITIZATION

Every enterprise relies on networked applications to conduct educational activities successfully. In a connected world, computer networks serve many applications ranging from recreational to business-critical. For the educational establishment to operate efficiently, the IT team must ensure application availability and response time to all users and all access modes. Application control begins with understanding how critical applications are used, how they perform under different network conditions, and what are the factors that IT can control to ensure their delivery.

CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Business Apps (Max BW Guaranteed)
EXPEDITE
Collaboration apps, VoIP Video

Based on this analysis, each application receives a tailored QoS policy, which may define congestion thresholds along with some form of expedited forwarding (depending on delay sensitivity). It may also define guaranteed minimum bandwidth or separate data rates for inbound and outbound traffic. Altogether, these parameters ensure that teaching and training processes, human resource management, and financial and legal control systems can operate more productively and with greater efficiency.

Key Benefits

- Ensure availability and response time of critical applications
- Enhance user productivity and satisfaction
- Align network performance to business priorities
- Invest in infrastructure expansion when needed to meet educational requirements

Business Application Prioritization in Action

- Analyze usage and performance of business applications and the Quality of Experience (QoE) that they deliver
- Define and enforce priority Quality of Service (QoS) for each application and propagate this across the network
- Enforce dynamic QoE-based congestion control aligned to educational priorities
- Troubleshoot and act upon alerts as they occur

Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

Key Benefits

- Guarantee the performance of education-critical applications
- Reduce time and costs involved in troubleshooting a campus network
- Avoid costly Wide Area Network (WAN) upgrades

Campus Congestion Control in Action

- Monitor and analyze network usage
- Define fair-use policy for each campus, application, user, and time of day
- Enforce the policy based on congestion and other real-time triggers
- Troubleshoot and act upon alerts as they occur

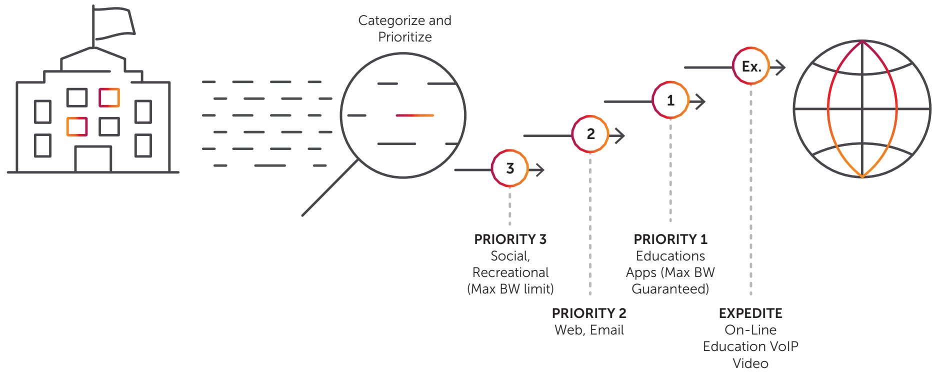
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager

HIGHER EDUCATION
CAMPUS CONGESTION CONTROL

Universities and colleges find themselves in the role of Internet Service Provider (ISP), delivering network and Internet services to students, faculties, administrators, and guests located on multiple campuses that are tied together in a WAN topology to a main campus hub. The ostensibly "free" and ubiquitous Internet connectivity can easily overload the campus WAN with recreational video/audio streaming, P2P downloads, social networking, and VoIP calling in addition to the demanding education applications it must support. DPI-based solutions successfully control WAN congestion by enforcing fair usage policy, which may include usage caps, limited data rates for recreational applications, assured forwarding for video lectures and remote learning, and busy-hour blocking of P2P. Campus networks have also found themselves indirect victim to DDoS attacks related to student on-line gaming activities and direct victims of malicious activity. With the combination of advanced traffic management with behavioral DDoS detection and mitigation, the SSG can protect the campus network and ensure minimal impact on education-critical applications.

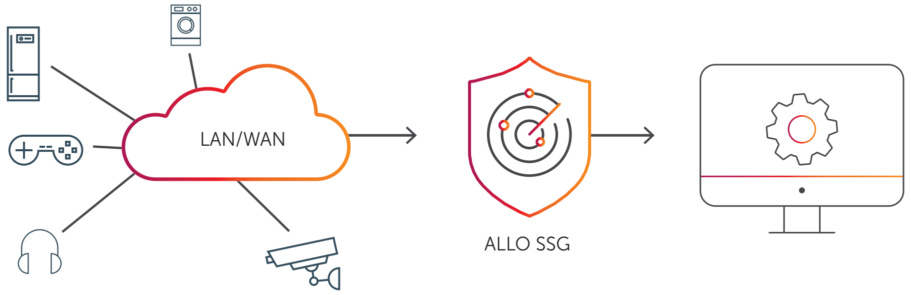
CLOUD MIGRATION, CAMPUS APP


Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Educations Apps (Max BW Guaranteed)
EXPEDITE
On-Line Education VoIP Video

HIGHER EDUCATION
INTERNET OF THINGS 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 enterprise 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 enterprises 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 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

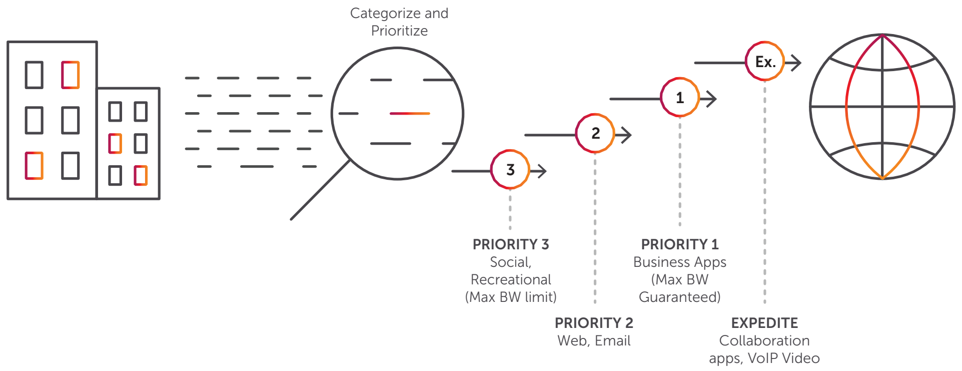
Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure
- Network Behavior Analysis Engine

HIGHER EDUCATION
MANAGING CLOUD MIGRATION

Many educational establishments 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 companies 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 educational organizations to monitor usage and behavior of cloud based applications and enforce priorities and committed data rates (Internet bandwidth) for educational applications over personal content. QoE-based congestion control dynamically prioritizes Internet access based on educational 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 educational organization.

CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
Ex.
1
2
3
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 1
Business Apps (Max BW Guaranteed)
PRIORITY 2
Web, Email
EXPEDITE
Collaboration apps, VoIP Video

Key Benefits

- Accommodate a wide range of student and educator workloads
- Align Internet access and resource allocation to educational priorities
- Control cloud access costs

Managing Cloud Migration in Action

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

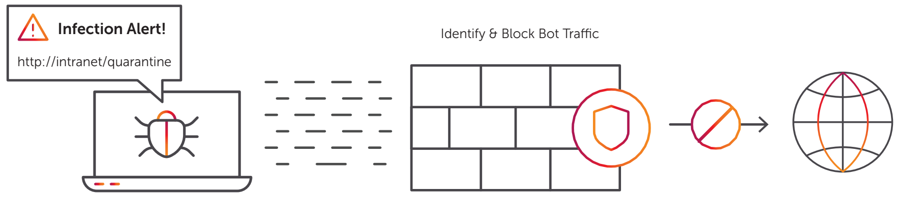
Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

HIGHER EDUCATION
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 enterprises 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 business 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

HIGHER EDUCATION
REAL-TIME DDoS ATTACK MITIGATION

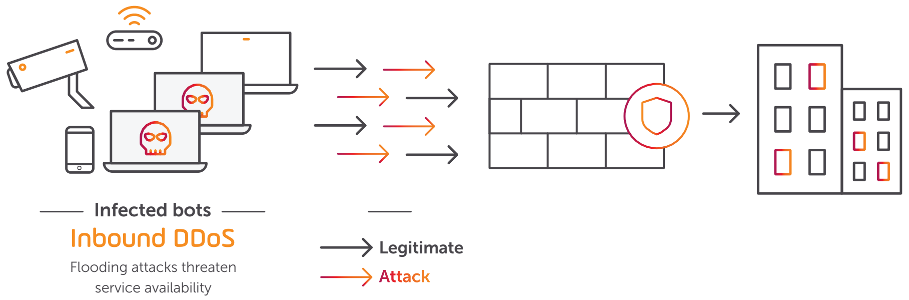
DDoS attacks are growing in intensity and sophistication every year such as memcached attacks and short-lived attacks that confound cloud-based DDoS mitigation solutions. Enterprise data centers are at the heart of modern day organization operation and even minutes of downtime can result in significant 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 organization 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



> Encouragement of higher education for our youth is critical to the success of our collective future.
>
> Charles B. Rangel

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

HIGHER EDUCATION
WI-FI OPTIMIZATION

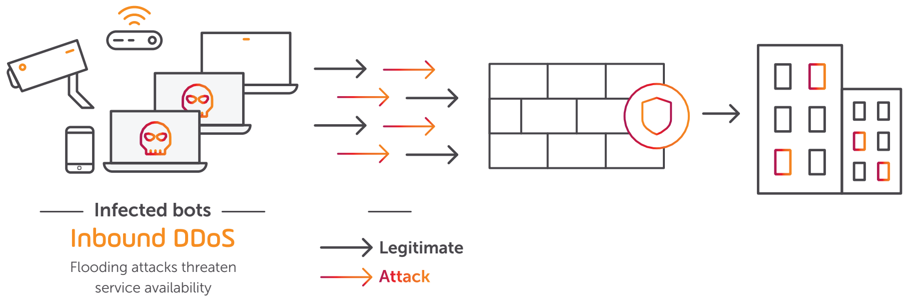
A growing number of Wi-Fi service providers include educational establishments who offer Wi-Fi service to provide Internet services to their staff and students to enhance their on-campus educational experience. This service can be easily monopolized by a few heavy users, and therefore requires fair usage management. For example, a higher education college cannot afford to allow its students to monopolize its Internet bandwidth by watching or downloading multiple high-definition videos during the study day. DPI-based solutions enable these establishments to monitor Wi-Fi utilization in real time and enforce QoS based on dynamic network conditions.

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



Key Benefits

- Permit use of personal devices to enhance employee productivity
- Ensure personal devices do not compromise a network
- Strengthen network security measures

Bring Your Own Device in Action

- Map BYOD rules into Wi-Fi management policy
- Automatically detect traffic from personal devices
- Enforce BYOD rules in real time
- Review BYOD usage reports to evaluate and refine policy

Powered by Allot Secure Service Gateway (SSG)

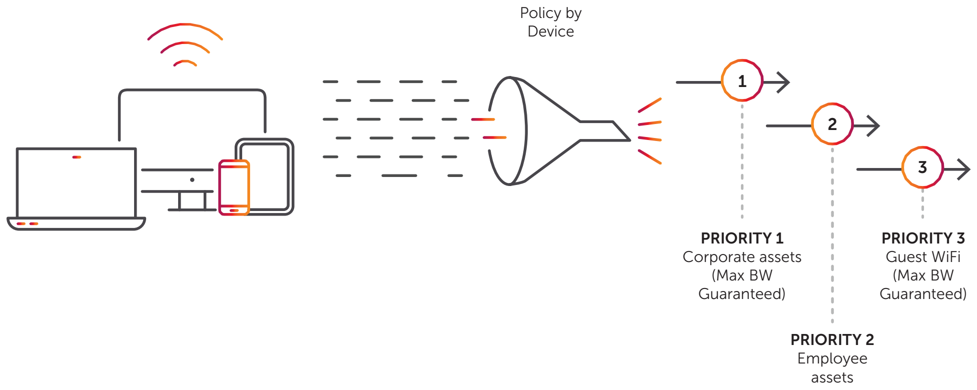
- Allot Gateway Manager
- Allot ClearSee Analytics

HOSPITALITY

BRING YOUR OWN DEVICE (BYOD)

While many IT managers see Bring-Your-Own-Device (BYOD) as an inevitable disruption that opens the network to security risks, users see it as a great enabler of personal productivity and efficiency. Hospitality organizations require the ability to enforce usage rules for personal devices once they are on the network. BYOD rules may include throttling heavy usage, allocating more bandwidth to employee devices over guest devices, and giving priority to business applications. Allot's superior Deep Packet Inspection (DPI) technology provides device signatures in the same way that it provides application signatures, and it updates them regularly. This ensures timely and accurate identification of non-corporate devices and their traffic on the network.

BYOD


Policy by Device
1
2
3
PRIORITY 1
Corporate assets (Max BW Guaranteed)
PRIORITY 2
Employee assets
PRIORITY 3
Guest WiFi (Max BW Guaranteed)

HOSPITALITY
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.

Key Benefits

- Protect network integrity through the rapid treatment of bot infections
- Ensure business 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

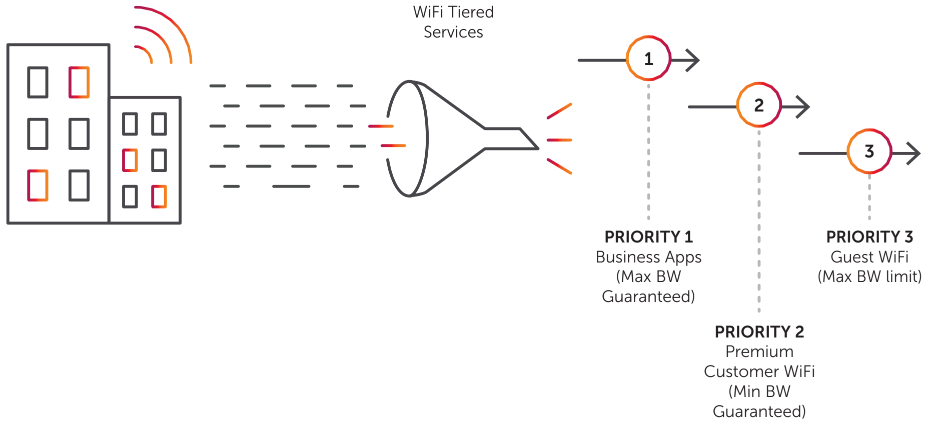
Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure
- Host Behavior Analysis Engine

HOSPITALITY
WI-FI SERVICE TIERS

Hotels, airports, convention centers, and public transportation often serve individual kinds of customer and employees, namely hotel guests, convention center attendees, exhibitors, and staff. The Wi-Fi connectivity requirements for these user groups are typically quite specific 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


WiFi Tiered Services
1
2
3
PRIORITY 1
Business Apps (Max BW Guaranteed)
PRIORITY 2
Premium Customer WiFi (Min BW Guaranteed)
PRIORITY 3
Guest WiFi (Max BW limit)

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

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

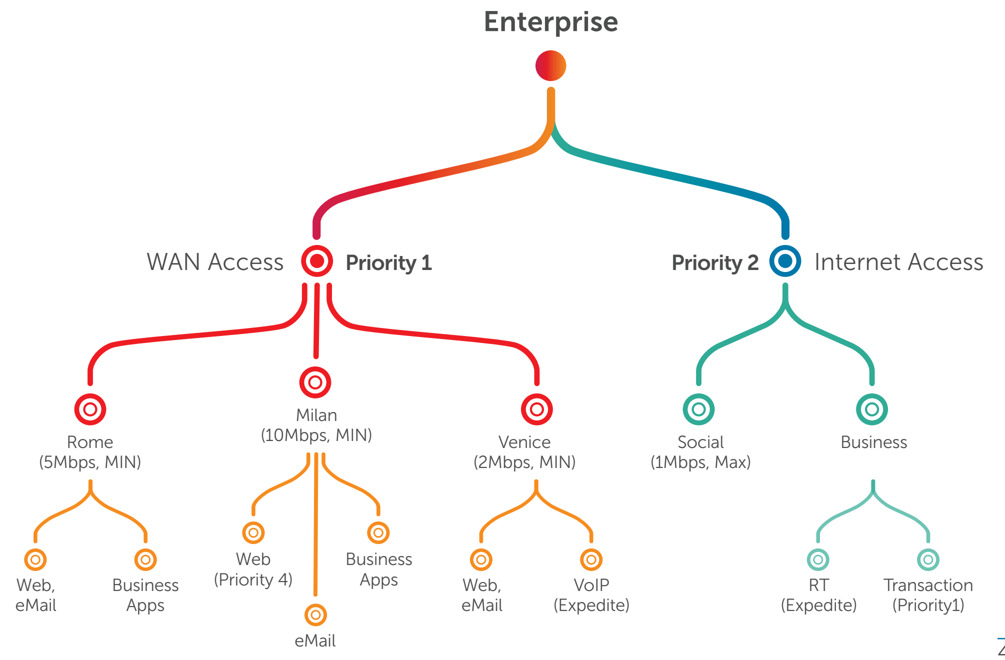
Powered by Allot Secure Service Gateway (SSG)

- 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

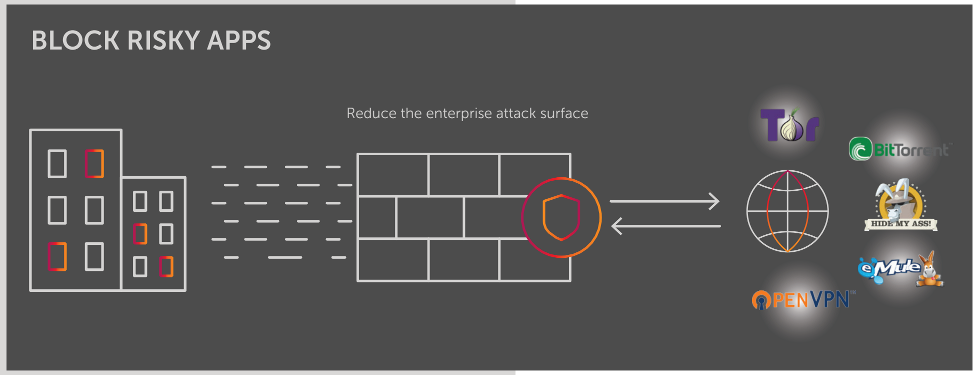
Heavy use of low priority or recreational applications and websites consumes considerable bandwidth and can congest and impair your network operations. Furthermore, some applications pose high levels of risk that extend beyond operational effectiveness, for example:

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:

BLOCK RISKY APPS

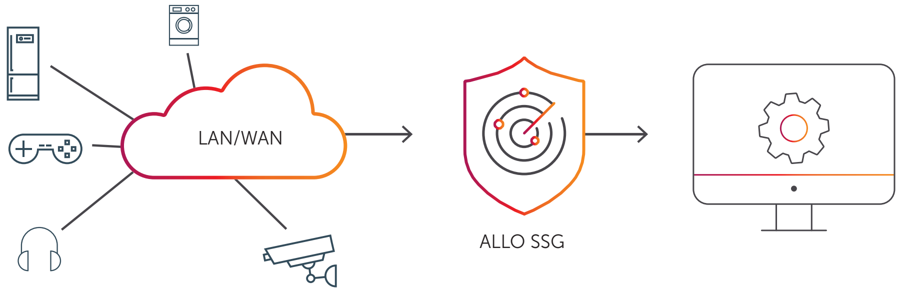


- Traffic statistics
- Server Name Indicator (SNI) detection
- Machine learning algorithms
- Pattern detection
- Certificates analysis
- Secure Sockets Layer (SSL) extensions analysis
- Traffic heuristics

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

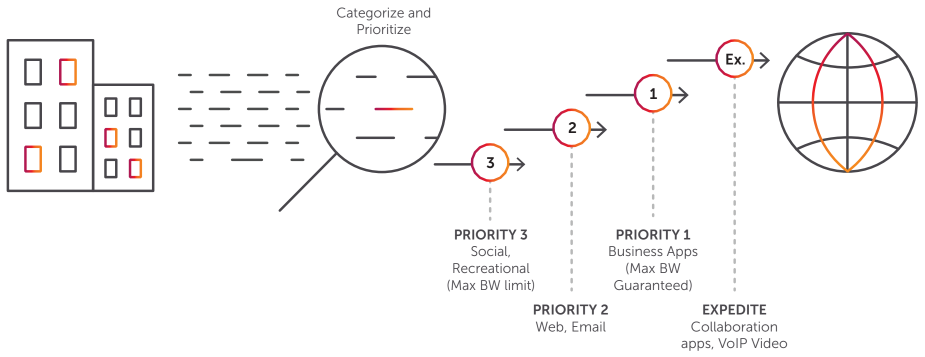
Powered by Allot Secure Service Gateway (SSG)

- 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.

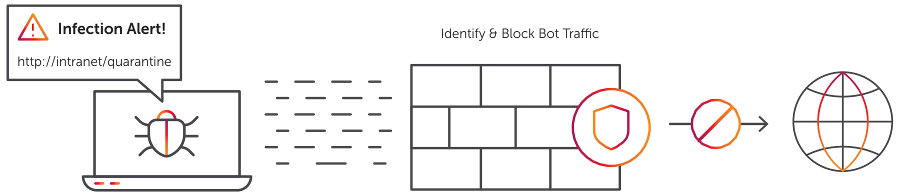
CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Business Apps (Max BW Guaranteed)
EXPEDITE
Collaboration apps, VoIP Video

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

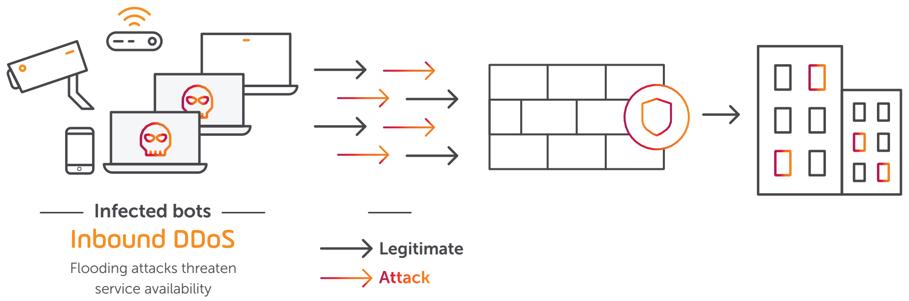
DDoS attacks are growing in intensity and sophistication every year such as memcached attacks and short-lived attacks that confound cloud-based DDoS mitigation solutions. Enterprise data centers are at the heart of modern day organizational operation and even minutes of downtime can result in significant 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



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)

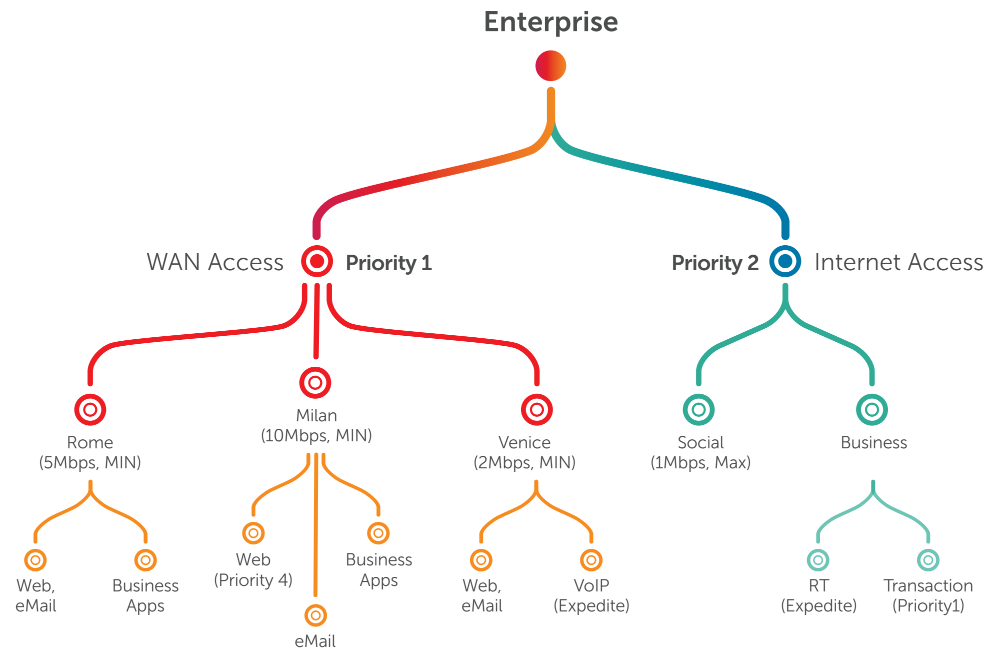
- Allot Gateway Manager
- Allot ClearSee Analytics

MEDIA & TELECOM

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

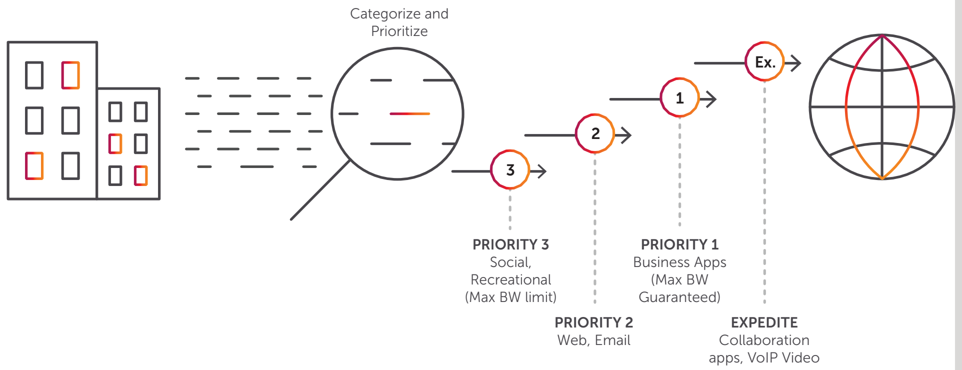


MEDIA & TELECOM

BUSINESS APPLICATION PRIORITIZATION

Every enterprise relies on networked applications to conduct business successfully. In a connected world, corporate networks serve many applications ranging from recreational to business-critical. For the business to operate efficiently the IT team must ensure application availability and response time to all users and all access modes. Application control begins with understanding how critical applications are used, how they perform under different network conditions, and what are the factors that IT can control to ensure their delivery.

CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 2
Web, Email
PRIORITY 1
Business Apps (Max BW Guaranteed)
EXPEDITE
Collaboration apps, VoIP Video

Based on this analysis, each application receives a tailored QoS policy, which may define congestion thresholds along with some form of expedited forwarding (depending on delay sensitivity). It may also define guaranteed minimum bandwidth or separate data rates for inbound and outbound traffic. Altogether, these parameters ensure that business processes and users of Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Voice over Internet Protocol (VoIP), video conferencing, and other business applications can work more productively and with greater efficiency.

Key Benefits

- Ensure availability and response time of critical applications
- Enhance user productivity and satisfaction
- Align network performance to business priorities
- Invest in infrastructure expansion when needed to meet business requirements

Business Application Prioritization in Action

- Analyze usage and performance of business applications and the Quality of Experience (QoE) that they deliver
- Define and enforce priority Quality of Service (QoS) for each application and propagate this across the network
- Enforce dynamic QoE-based congestion control aligned to business priorities
- Troubleshoot and act upon alerts as they occur

Powered by Allot Secure Service Gateway (SSG)

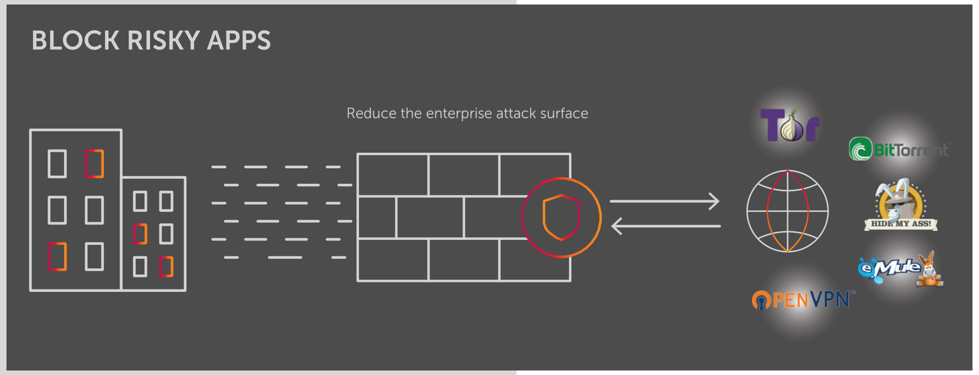
- Allot Gateway Manager
- Allot ClearSee Analytics

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


BLOCK RISKY APPS

Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

MEDIA & TELECOM

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:

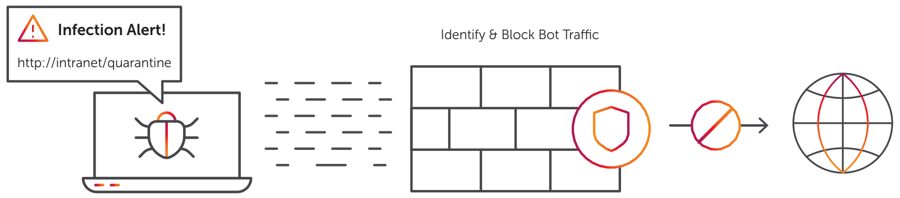
- Traffic statistics
- Server Name Indicator (SNI) detection
- Machine learning algorithms
- Pattern detection
- Certificates analysis
- Secure Sockets Layer (SSL) extensions analysis
- Traffic heuristics

MEDIA & TELECOM

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 enterprises 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 business 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)

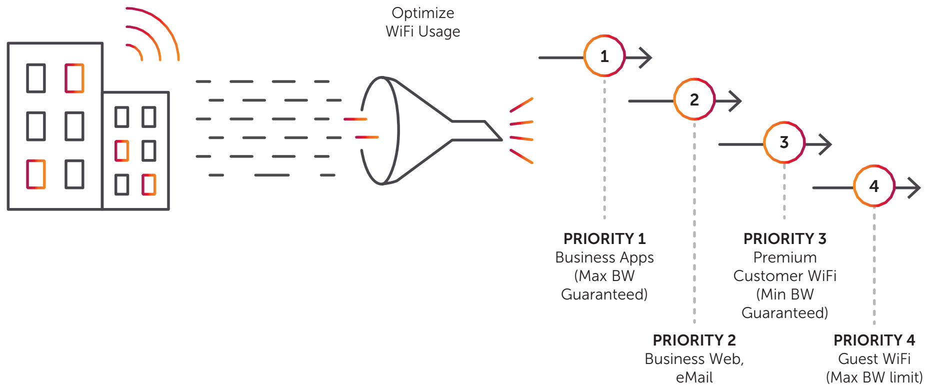
- Allot DDoS Secure
- Host Behavior Analysis Engine

MEDIA & TELECOM

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


Optimize WiFi Usage
1
2
3
4
PRIORITY 1 Business Apps (Max BW Guaranteed)
PRIORITY 2 Business Web, eMail
PRIORITY 3 Premium Customer WiFi (Min BW Guaranteed)
PRIORITY 4 Guest WiFi (Max BW limit)

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

- 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)

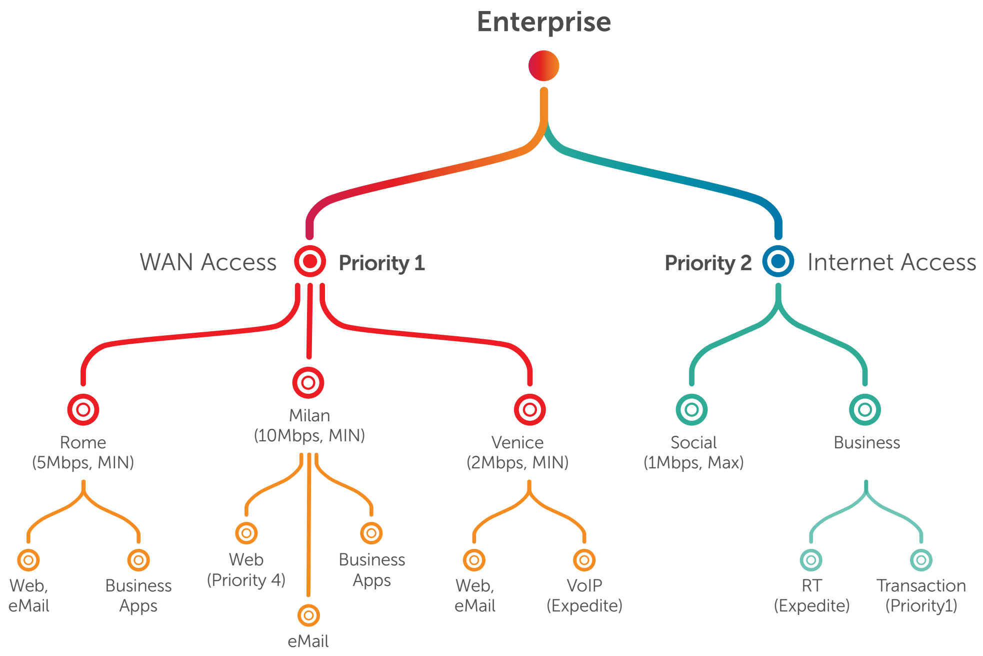
- Allot Gateway Manager
- Allot ClearSee Analytics

RETAIL STORES & RESTAURANT CHAINS

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

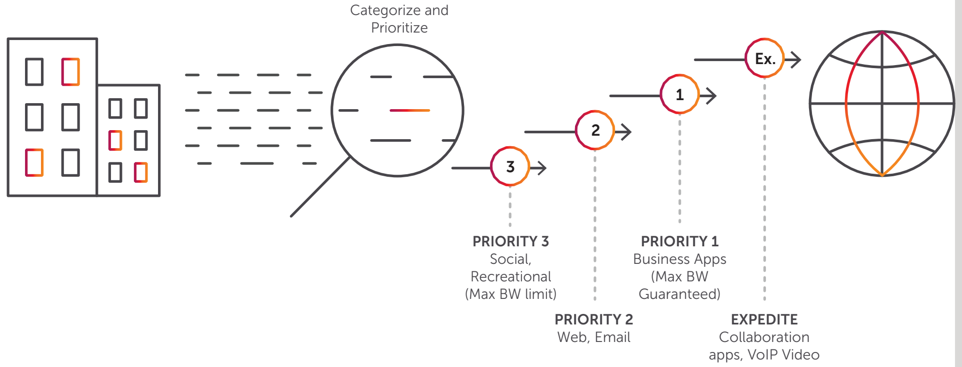


RETAIL STORES & RESTAURANT CHAINS

BUSINESS APPLICATION PRIORITIZATION

Every enterprise relies on networked applications to conduct business successfully. In a connected world, corporate networks serve many applications ranging from recreational to business-critical. For the business to operate efficiently the IT team must ensure application availability and response time to all users and all access modes. Application control begins with understanding how critical applications are used, how they perform under different network conditions, and what are the factors that IT can control to ensure their delivery. Based on this analysis, each application receives a tailored QoS policy, which may define congestion thresholds along with some form of expedited forwarding (depending on delay sensitivity). It may also define guaranteed minimum bandwidth or separate data rates for inbound and outbound traffic. Altogether, these parameters ensure that business processes and users of Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Voice over Internet Protocol (VoIP), video conferencing, and other business applications can work more productively and with greater efficiency.

CLOUD MIGRATION, BUSINESS APP


Categorize and Prioritize
3
2
1
Ex.
PRIORITY 3
Social, Recreational (Max BW limit)
PRIORITY 1
Business Apps (Max BW Guaranteed)
PRIORITY 2
Web, Email
EXPEDITE
Collaboration apps, VoIP Video

Key Benefits

- Ensure availability and response time of critical applications
- Enhance user productivity and satisfaction
- Align network performance to business priorities
- Invest in infrastructure expansion when needed to meet business requirements

Business Application Prioritization in Action

- Analyze usage and performance of business applications and the Quality of Experience (QoE) that they deliver
- Define and enforce priority Quality of Service (QoS) for each application and propagate this across the network
- Enforce dynamic QoE-based congestion control aligned to business priorities
- Troubleshoot and act upon alerts as they occur

Powered by Allot Secure Service Gateway (SSG)

- Allot Gateway Manager
- Allot ClearSee Analytics

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

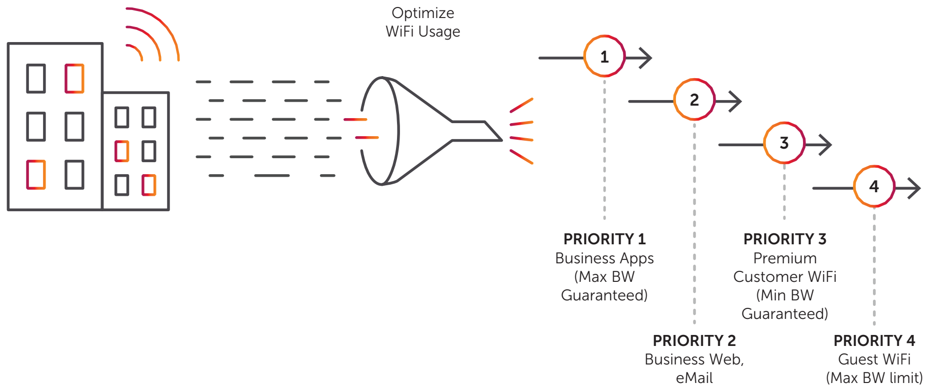
DDoS PROTECTION

RETAIL STORES & RESTAURANT CHAINS

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


Optimize WiFi Usage
1
2
3
4
PRIORITY 1
Business Apps (Max BW Guaranteed)
PRIORITY 3
Premium Customer WiFi (Min BW Guaranteed)
PRIORITY 2
Business Web, eMail
PRIORITY 4
Guest WiFi (Max BW limit)

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

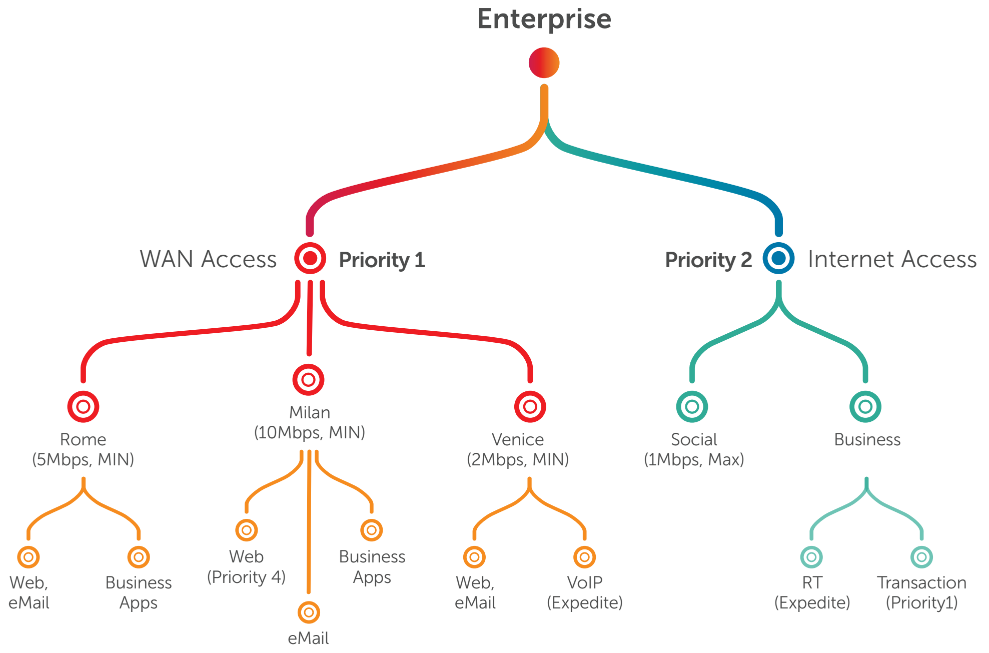
Powered by Allot Secure Service Gateway (SSG)

- 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.

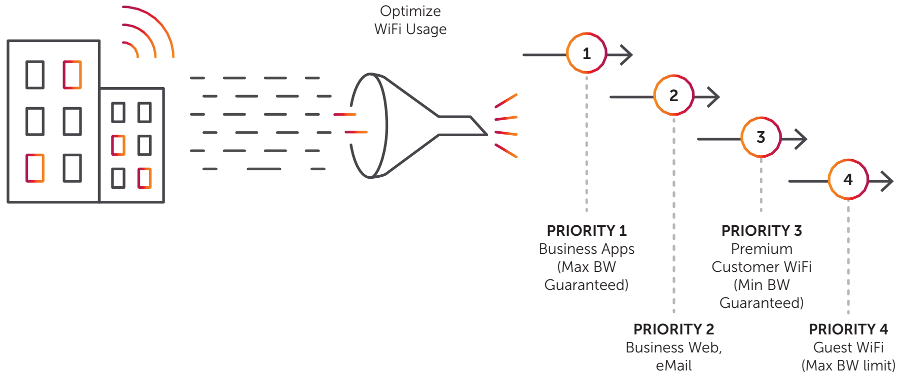
TRAFFIC MANAGEMENT & ACCEPTABLE USE POLICY



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

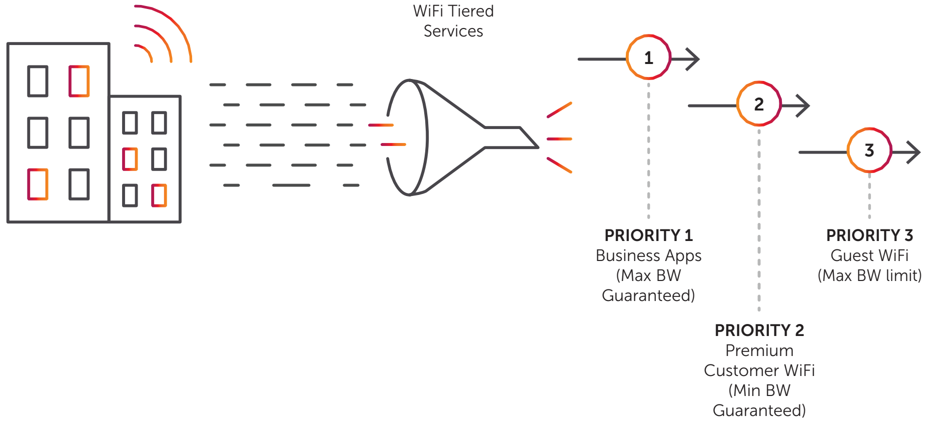
Powered by Allot Secure Service Gateway (SSG)

- Allot DDoS Secure

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



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

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.