allot
See. Control. Secure.

Allot IoT Defense—Solutions for Enterprises to Ensure IoT Service Continuity

Solution Brief

See. Control. Secure.

Contents

1 Allot IoT Defense—Solutions for Enterprises to Ensure IoT Service Continuity

IoT has found its way into many aspects of our lives and businesses including healthcare, energy, transportation safety and maintenance. These services, some defined as critical infrastructure at the national level, are also primary targets of malicious criminal and state sponsored activity. The need to secure IoT and ensure continuity of IoT-based services is a reality recently demonstrated when DDoS attacks left some housing in Finland without heating.

Vulnerable connected devices also pose a threat to the enterprise that deploys them. Verizon's Data Brief Digest 2017 describes such an event. A university experienced 5,000 devices making hundreds of Domain Name Service (DNS) look-ups, which slowed the institution's entire network and restricted access to many internet services. On a larger scale the sheer volume of devices has the capability to threaten telecommunications infrastructure as witnessed in the attack on access routers in Deutsche Telekom and the infamous DDoS attack on Dyn[1].

Allot IoT Defense (AID) enables enterprises to secure IoT deployments at the network layer that address two main concerns:

- IoT Service Protection
  To ensure service continuity of the IoT devices and protect them from attack as described below.
- IoT Infrastructure Protection
  To protect the IoT network and Enterprise network infrastructure that provides connectivity for the IoT and its IT systems.

[1] See Mirai case study below

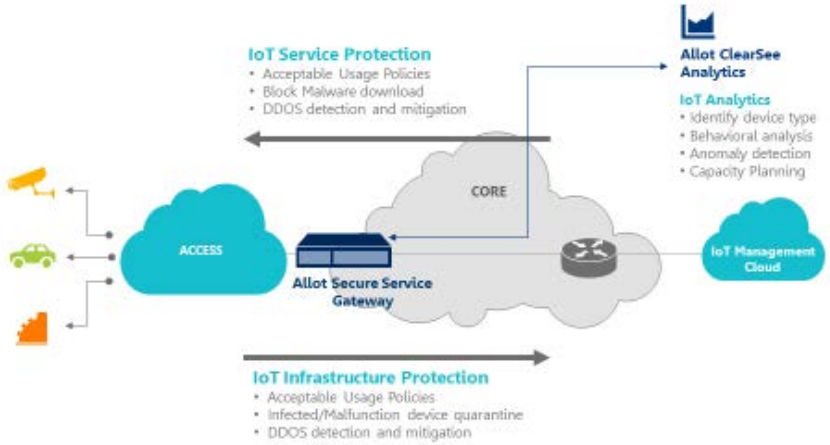


Figure 1: Allot IoT Defense

In addition, Allot IoT Defense provides powerful network analytics for visibility into IoT deployments for endpoint identification, communications patterns and trend analysis to support capacity planning and troubleshooting.

2 IoT Service Protection

IoT Service Protection is delivered at three levels in order to reduce its available attack surface and protect it from service disruption and infection. These are based on the following functions:

- Acceptable usage policies to prevent unapproved communication to the IoT devices
- Protect the IoT service against DDoS attacks
- Prevent download of malware to the IoT devices

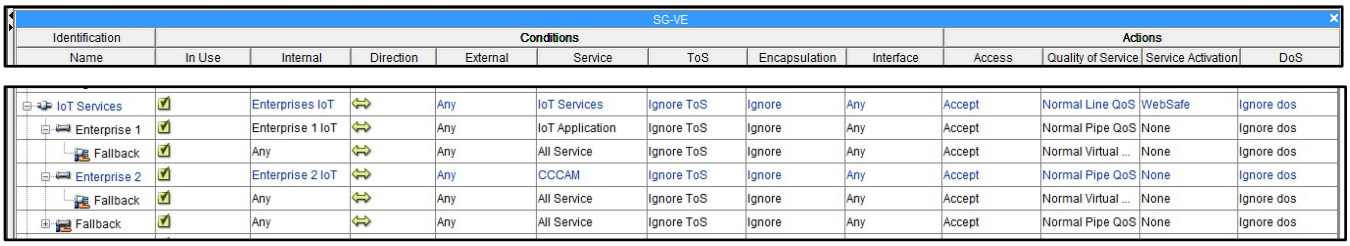
2.1 Acceptable Usage Policies (AUP)

IoT deployments typically serve a specific or a limited set of functions and they communicate directly with a limited set of management servers and services. The objective of the AUP is to police communications by source, application and behavior in order to reduce the attack surface of the device. Allot Secure Service Gateway enables the enterprise to define Acceptable Usage Policies that control access to the IoT devices and police the communication channel between the IoT device and authorized servers. The challenge is to provide granular access control and traffic policing on a large scale. Allot multiservice platforms, deployed globally in carrier networks, data centers and enterprise networks police millions of flows and have the scale and robustness required for the largest of IoT deployments.

The Acceptable Usage Policies can be defined in terms of:

- IP addresses / Domains of the servers authorized to communicate with the IoT devices
- Type of protocols and applications permitted for communication
- Time of day/ day of week for when the communication is allowed
- Number of new connections and amount of BW permitted for the communication

These policies are useful for reducing the attack surface and limiting the ability of attackers to take control over the IoT devices.



SG-VE

Identification	Conditions								Actions			
Name	In Use	Internal	Direction	External	Service	ToS	Encapsulation	Interface	Access	Quality of Service	Service Activation	DoS
IoT Services	☑	Enterprises IoT	⇔	Any	IoT Services	Ignore ToS	Ignore	Any	Accept	Normal Line QoS	WebSafe	Ignore dos
Enterprise 1	☑	Enterprise 1 IoT	⇔	Any	IoT Application	Ignore ToS	Ignore	Any	Accept	Normal Pipe QoS	None	Ignore dos
Fallback	☑	Any	⇔	Any	All Service	Ignore ToS	Ignore	Any	Accept	Normal Virtual ...	None	Ignore dos
Enterprise 2	☑	Enterprise 2 IoT	⇔	Any	CCCAM	Ignore ToS	Ignore	Any	Accept	Normal Pipe QoS	None	Ignore dos
Fallback	☑	Any	⇔	Any	All Service	Ignore ToS	Ignore	Any	Accept	Normal Virtual ...	None	Ignore dos
Fallback	☑	Any	⇔	Any	All Service	Ignore ToS	Ignore	Any	Accept	Normal Pipe QoS	None	Ignore dos

Figure 2: Allot's Policy Editor to Control IoT Traffic

2.2 Protect the IoT Service Against DDoS Attacks

As IoT based services permeate healthcare, energy and transportation, the effect of service disruption can have significant consequences as recently demonstrated. Tools like Shodan make it easy to identify IoT deployments that are limited in their capability to withstand an attack, owing to limited resources and lack of on-device protection.

Allot Secure Service Gateway DDoS protection provides advanced inline protection of DDoS attacks and can be effectively used to ensure continuity of an IoT Service. The challenge is to provide a fast response at massive scale. Allot multiservice platforms today protect national infrastructure in-line, protecting over 1TBps of aggregate traffic with detection and mitigation taking less than two minutes.

2.3 Prevent Download of Malware to IoT Devices

Mirai hit the headlines in 2016 as the source of some of the most devastating DDoS attacks seen until then. Mirai's code is publically available, the malware has been analyzed by numerous security experts and can be recognized by many commercially available anti-viruses, yet it continues to threaten IoT devices. This is because many of these devices are difficult or impossible to patch or there is no client software available to install and protect them. Mirai's infection process includes infiltration of an auxiliary bot on an IoT device, which later downloads the core malware.

Allot Secure Service Gateway provides network based Anti-Malware, utilizing the same technology with which Allot multiservice platforms protect mobile devices. The largest deployment involves close to nine million devices. Incoming traffic is inspected by the Secure Service Gateway, incorporating leading anti-virus engines, Kaspersky, Bit Defender and/or Sophos. Allot Secure Service Gateway is the only effective way to prevent infection of IoT devices, because it is network-based.

3 IoT Infrastructure Protection

The goal of IoT infrastructure protection is to ensure resilience of the enterprise infrastructure. As has been evident in cases of both service provider and enterprise networks, a compromised IoT deployment has the power to impact the very infrastructure it relies on for connectivity.

IoT infrastructure protection is delivered at three levels in order to reduce its available attack surface, identify and quarantine infected devices and protect the infrastructure from service disruption. These are based on the following functions:

- Acceptable Usages policies to prevent unapproved communication from the IoT devices
- Stop Outgoing DDoS by protecting the IoT infrastructure from internally sourced DDoS attacks that threaten external networks and services
- Identify and quarantine infected IoT devices

3.1 Acceptable Usage Policies

Similar to IoT Service Protection, Allot Secure Service Gateway enables the enterprise to define Acceptable Usage Policies that control communications from the IoT devices and police the communication channel between the IoT device and authorized servers. The Acceptable Usage Policies can be defined in terms of:

- IP addresses / Domains of the IoT devices and the management servers
- Type of protocols and applications allowed to be used for communication
- Time of day/ day of week when the communication is permitted
- Number of new connections / amount of BW permitted for the communication.

3.2 Stop Outgoing DDoS

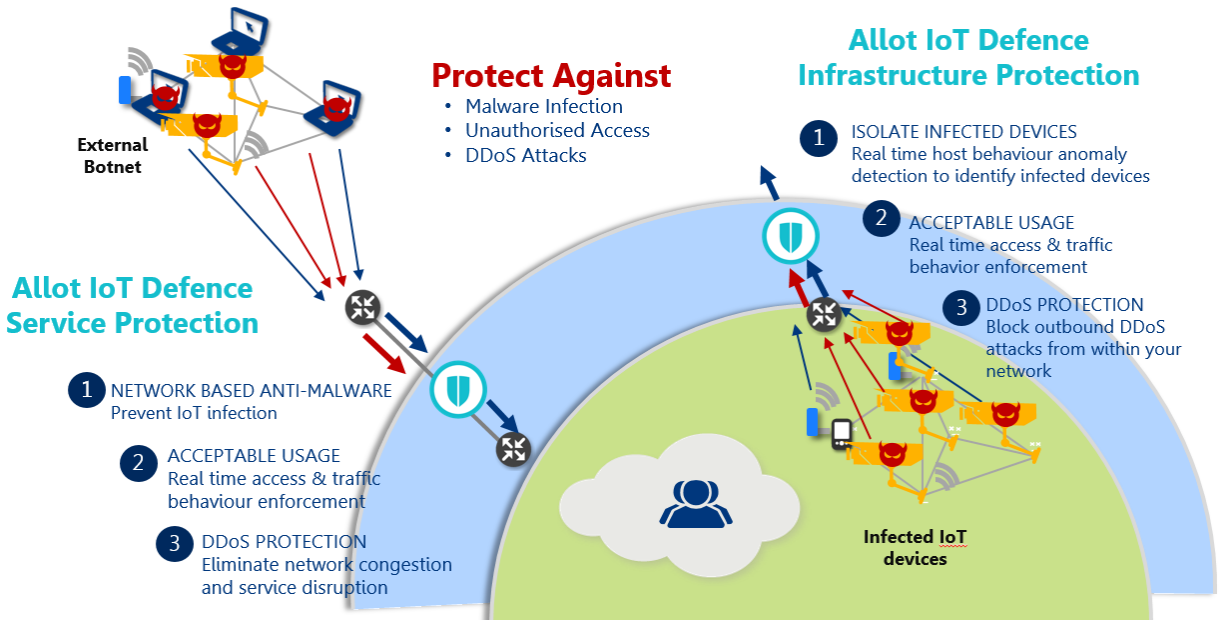
Large volumetric infections of IoT devices, typified by those recently triggered the highly damaging Mirai virus, impact not only the target of the attack, but also the network to which they are connected, and transit networks. The result is impaired service and quality of experience for users who share the same infrastructure. In addition to the crippling effect they can have on an enterprise network, the same enterprise could find itself liable for not adequately securing its network. Allot Secure Service Gateway DDoS protection provides advanced inline detection and mitigation against inbound and outbound DDoS attacks and can be effectively used to protect the internal infrastructure of an enterprise.

3.2.1 Infected IoT devices - Host Behavior Anomaly Detection (HBAD)

Allot Secure Service Gateway with Service Protector enabled also delivers Host Behavior Anomaly Detection (HBAD) to identify bot activities initiated from within the network. This allows quick identification of infected IoT devices and enables effective mitigation by limiting or quarantining those devices. For example HBAD can pinpoint abnormal activity such as port scanning that was identified in Mirai-style infected networks.

3.3 Visibility

Allot Secure Service Gateway delivers powerful analytics with Allot ClearSee Network Analytics. Analytics is a key component of IoT Defense, providing comprehensive visibility into IoT deployments. Utilizing HP Vertica and MicroStrategy BI, Allot ClearSee scales to provide real time and historical analytics that enable IT operations to identify devices, communications patterns, protocols and application usage and network utilization. These capabilities can be used for troubleshooting, trend analysis, planning and defining policies for the purpose of network optimization and behavior analysis and enforcement. Allot ClearSee can also serve as a data source, providing raw data or intelligent (correlated) data for third party SIEM solutions.



3.4 Summary

IoT Defense is based on the existing capability of Allot Secure Service Gateway and Allot multiservice platforms. They provide the three pillars: Visibility, Security and Control required to ensure service availability for IoT deployments and protect IoT infrastructure when and if things misbehave. We believe that this layered approach is the best way of dealing with the diversity and scale that characterizes IoT deployments.

Appendix A. When Things Misbehave – An Analysis of Mirai Threats

The Mirai botnet hit the headlines in 2016 following the massive DDoS attacks on Krebs and Dyn. The latter brought down parts of the internet on the US east coast using an army of hacked surveillance cameras that attacked the largest managed DNS infrastructure. A month later it infected home routers of German internet provider Deutsche Telekom, disconnecting nearly a million users from the internet for almost three days. The exploit code used to attack the routers was believed to be a modified version of Mirai.

While Mirai-infected bot attacks have mostly occurred in the U.S. and Europe, security researchers determined that over half a million IoT devices located in 164 countries worldwide were vulnerable to Mirai, so these botnet attacks were not limited to these regions. They are a global phenomenon.

During January 2017 Allot witnessed Mirai-like DDoS attacks in several service providers in Asia, all exhibiting similar characteristics. The Allot ServiceProtector inline DDoS protection system mitigated a slew of Mirai-like floods with relatively short hit-and-run cycles of massive traffic spikes to the target. These indicated powerful DDoS attacks, similar to other Mirai-powered DDoS attacks that required an effective real-time mitigation solution to block them.

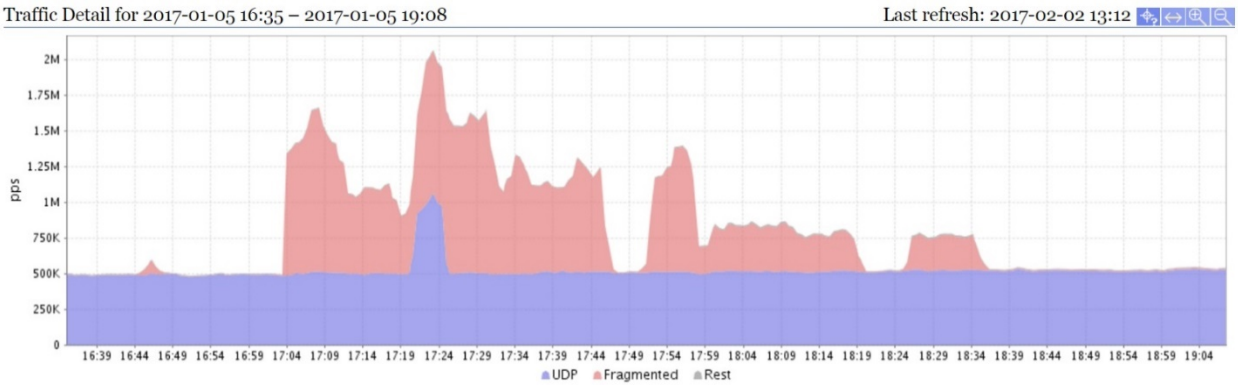


Figure 3- Surgical identification of the attack

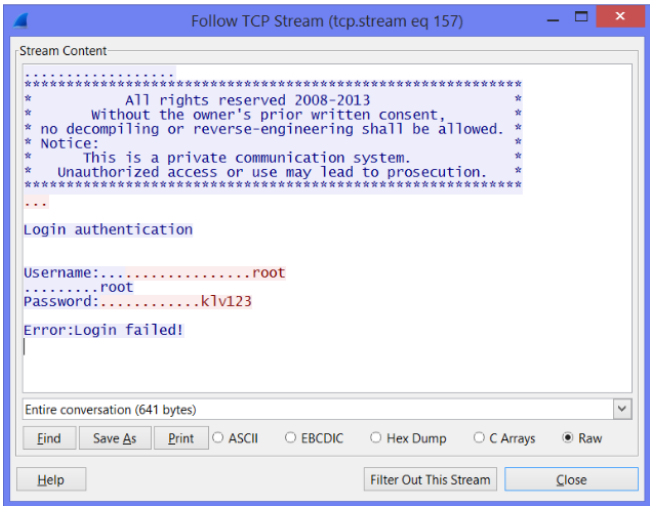


Figure 4: Taken from Mirai capture- attempting to login IoT Device

Mirai targets vulnerable devices with open management TCP ports such as 22, 23, 7547, 2323, etc. using a series of known passwords. Allot ServiceProtector inline sensors detected massive scan activity on all these ports. In addition, packet captures taken from the service providers' network indicated login attempts using different passwords from Mirai's list of common passwords.

After a vulnerable device is infected by Mirai, it becomes a remote controlled bot that can further spread the infection to other compromised devices and participate in a massive DDoS attack upon command. The attack on Deutsche Telekom took advantage of a vulnerability in the Eir D1000 modem that could enable a remote attacker to take control of an affected device using Transmission Control Protocol (TCP) port 7547. In our investigation, Allot ServiceProtector - Host Behavior Anomaly Detection (HBAD) identified significant HTTP scans on port 7547 as well as scans on port 23 generated by devices in the service providers' network; most probably scanning attempts to spread the bot infection to other external targets.

HBAD Events

Type (spread)	Target	Bit rate	Packet rate	Connection rate
Addr-Scan *(97.3%)*	*:7547/TCP	10.2K *(43.8%)*	17.5 *(44.2%)*	15.0 *(59.9%)*
Addr-Scan *(95.8%)*	*:23/TCP	12.1K *(52.0%)*	21.3 *(53.6%)*	9.52 *(38.2%)*
		22.2K *(95.8%)*	**38.8** *(97.8%)*	**24.5** *(98.1%)*

Since the release of the original Mirai source code on September 30, it has inspired many bad actors to exploit similar pools of IoT vulnerable devices and launch massive DDoS attacks. Such attacks proved that, if used on specific targets, they can cause a wide-scale outage by bringing down websites, services, or even internet infrastructure. It is hard to estimate the number of devices infected by Mirai and its copycats, or their distribution worldwide. Significantly, our investigation indicates that the family of Mirai-like botnets has not gone away. Anomaly-based DDoS protection such as Allot ServiceProtector provides a solution to the challenge presented by such malware. It can block the largest

incoming DDoS attacks generated by the scale of IoT bots. It stops the spread of bot infections and mitigate outbound DDoS attacks originating from such botnets.

P/N Dxxxxxx Rev.1

www.allot.com sales@allot.com

Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA - Tel: +1 781-939-9300; Fax: +1 781-939-9393; Toll free: +1 877-255-6826
Europe: NCI–Les Centres d'Affaires Village d'Entreprises, 'Green Side' 400 Avenue Roumanille, BP309 06906 Sophia Antipolis, Cedex France - Tel: +33 (0) 4-93-001160; Fax: +33 (0) 4-93-001165
Asia Pacific: 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104, Tel: +65 6749-0213; Fax: +65 6848-1015
Japan: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 - Tel: +81 (3) 5297 7668; Fax: +81 (3) 5297 7669
Middle East & Africa: 22 Hanagar Street, Industrial Zone B, Hod Hasharon, 4501317 Israel - Tel: 972 (9) 761-9200; Fax: 972 (9) 744-3626