Securing the Number One Attack Target on the Internet: IoT Devices

The IoT era

As networked communications continue to expand and grow in complexity, the network has increasingly moved to include more forms of communication. This has ushered in the era of the Internet of Things (IoT). No longer dependent upon person-to-person interaction, communications are made directly between simple devices, or between simple devices and complex systems. These connections between millions of IoT devices create demand for new services, unlocking new business opportunities to improve efficiency and quality of service. IoT technology is expected to spread exponentially across many industries, with growth estimated to surpass 20 billion connected devices by 2021.[1]

Within the Internet of Things, Communication Service Providers play an important role. This role can vary widely from, for example, a focus on offering IoT centric connectivity, like LoRA (long range) and LTE-M (Long Term Evolution (4G), category M1), to more advanced IoT services, including hosting IoT applications and offering IoT security services.

Security is the biggest challenge

For those Service Providers working within the IoT domain, the massive volume of newly connected "Things" introduces new challenges for security. While humans were historically considered the weakest link for security, IoT devices are providing stiff competition! IoT devices are now the number one attack target on the internet.[2] Without adequate safeguards, these connected devices are easily compromised for nefarious purposes. The Mirai botnet is a great example; at its peak, Mirai had more than a half billion compromised IoT devices, allowing the execution of attacks at an unprecedented scale.

Whether consumer or industrial IoT, security is perhaps the biggest challenge and barrier to more rapid global adoption. While security repercussions can be just costly "lessons learned" in the consumer IoT sector, the safety and legal implications can be colossal for industrial IoT. Hence, the critical requirements of safety, security, reliability, scalability, latency, performance, visibility, and adaptability become mandatory. F5 Networks can play a key role in the Service Provider network architecture, helping to enable advanced, IoT-specific security services.

[1] Gartner 2017: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[2] F5 Labs 2018, The Hunt for IoT: Multi-Purpose Attack Thingbots Threaten Internet Stability and Human Life https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot--multi-purpose-attack-thingbots-threaten-intern

F5 provides IoT security throughout the network

Interconnected networks of IoT devices include multiple points of vulnerability, each of which requires its own security solution. Most IoT security solutions focus on providing security within the device itself. Data centers create an additional point of vulnerability. Virtually all IoT devices communicate to applications via centralized or distributed data centers, creating a well-recognized need to protect these servers against attacks and data breaches.

Additionally, F5 recognizes the need to provide network-centric security, allowing end-to-end protection of interconnected networks of IoT devices. Limitations on computing power and low frequency of software updates mean that security on the end device is often limited. A network-based solution can address some of these limitations, as well as mitigate additional threats which target the IoT network infrastructure. Network-centric security is, therefore, a critical addition to the IoT ecosystem.

For many years F5 technology has provided cost-effective advanced services by means of deployment within Service Provider infrastructures. The same technology can be used by Service Providers to offer advanced security services for IoT-centric use cases, such as traffic management, RAN level security, and DDoS protection for cellular IoT. The F5 IoT Firewall is a key element of any effective IoT security solution, and, perhaps, the most important IoT security service that F5 can provide.

The IoT Firewall is a User-Plane firewall, deployed in the Service Provider's core network, that features key differences from traditional network firewalls to allow better efficacy when deployed within the IoT domain. The IoT Firewall provides device-aware, application-centric firewall policies. This allows Service Providers to offer IoT security services without the need to host the IoT application in their data centers, or directly manage the IoT application.

The primary security threats mitigated by the IoT Firewall are:

- **Network threats:** The F5 IoT Firewall prevents DDoS (Distributed Denial of Service) and application-layer attacks which may disrupt the integrity and availability of the Service Provider's network.
- **Device threats:** IoT Firewall ensures that devices are only connecting to 'safe' locations and prevents devices from connecting to unknown services. This reduces the chances of devices being compromised through malware and blocks malicious 'ThingBot' C&C (command and control) communication to stop devices from being exploited remotely.
- **Service abuse:** This capability prevents IoT devices from being used unexpectedly, which can result in revenue leakage for the Service Provider or the application owner (for example, stopping a connected car SIM from being used in another device to stream Netflix).

F5 IoT Firewall—an enhanced network-centric security service

The relationship between a Service Provider and their IoT customers can take a variety of different forms. In some cases, the Service Provider may act as a simple "pipe" provider—offering managed connectivity to IoT customers who choose to keep their IoT application in their own data centers (or in a Public Cloud). One strategic alternative to this model is for Service Providers to offer their IoT customers an enhanced network-centric security service that can be customized on demand directly by the customer and/or application owner.

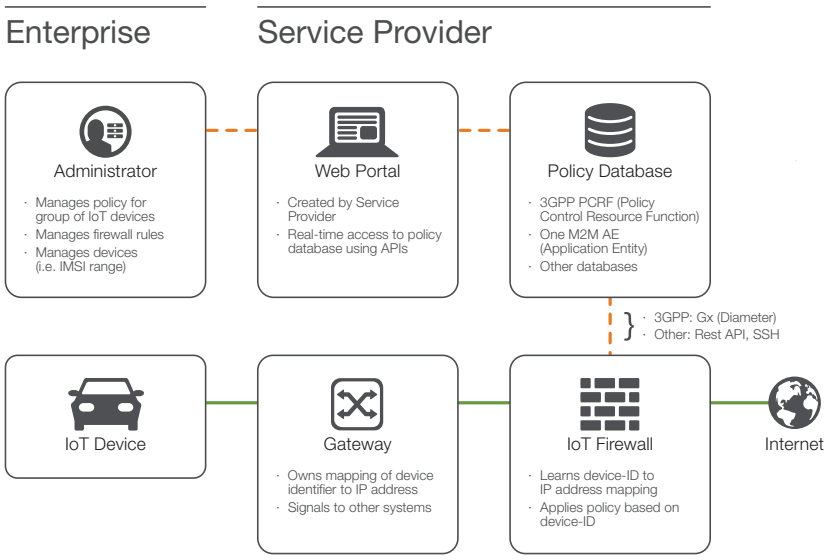

Figure 1: Typical Service Provider and Enterprise (customer) roles.

The diagram above details Service Provider and Enterprise (customer) roles. These roles are typically very well defined. In particular:

- The Service Provider provides the infrastructure, based on access termination (for example, a PGW), IoT network Firewall, Policy Control System, and, most importantly, an enterprise-facing Front-End Portal or REST API Interface.
- The Net/SecOps on the customer side uses this portal or API to define security policies that interact with the Gateway Service offered by the Service Provider.

A cost-effective solution

One of the biggest challenges for Service Providers is finding cost-effective ways to deliver these services. Without the right technology, it is challenging to tailor services for all customers requiring customized, IoT-centric implementations. Many providers choose to address this challenge by deploying a per-customer chain with a dedicated gateway node (for example, LTE P-GW) or a dedicated access point name (APN), a dedicated firewall instance, and a dedicated policy provisioning system. This approach is expensive and inflexible, and, therefore, not suited to supporting a mass roll-out of inexpensive IoT services.

The F5 IoT Firewall provides a flexible approach using a single instance that can be cost-effectively shared between different IoT customers. The single instance provides granular policy provisions for each customer and significantly simplifies deployment, lowering operational costs.

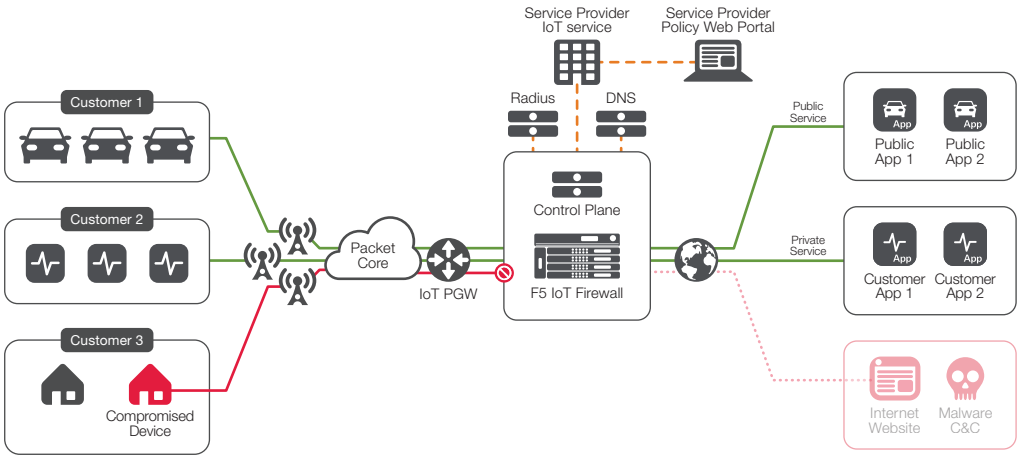

Figure 2: The IoT Firewall data plane serves as the enforcer of the security policy implemented by the customer, allowing the passage of explicitly permitted traffic, and blocking all other traffic. Customer 3 is passing infected traffic from an infected device. Green lines represent traffic that is allowed to pass, while the red line represents traffic that is blocked.

To achieve the required performance and scale, the F5 IoT Firewall efficiently provisions device-aware policies for millions of different devices using a common F5 appliance. This appliance may be physical or virtualized, which makes it particularly suited for Cloud/NFV deployments, as well as distributed architectures such as MEC (Multi-access Edge Computing).

This enables the Service Provider to:

- Support thousands of IoT customers, each with different security policy implementations
- Scale to millions of devices, increasing cost-effectiveness and business capacity

How it works

Positive security model

The F5 IoT Firewall security solution is based on a positive security concept. When an IoT service is provided by the Service Provider, only a pre-determined set of application servers can be contacted by the IoT devices connected to the SP network. All the rest of the traffic will be blocked, unless explicitly permitted by the IoT customer using the Web Portal, or the REST API interface, exposed by the Service Provider towards the customer.

The IoT customer can define security policies in two possible ways:

- Defining a list of destination IP address or IP Networks, destination ports, and destination protocols (UDP/TCP/other) which are permitted
- Defining a list of host names or domain names which are permitted

Functional components

In order to ensure the right policies are provisioned and implemented, the F5 IoT Firewall solution leverages two fundamental elements, both of which are needed to deliver the service:

- **IoT Firewall data plane:** The IoT Firewall data plane functions as the security policy enforcer, forwarding explicitly permitted traffic and blocking other traffic. Any traffic that is not explicitly permitted by a policy for the specific IoT customer will be dropped by the IoT Firewall data plane, as shown in Figure 2.
- **IoT Firewall control plane:** The control plane contains the security policies that will be applied to IoT devices when those devices are connected to the internet. These policies are defined on a per-customer basis. The control plane exposes an interface (typically xml, but any language can be used) which is accessed by the service portal. The service portal is typically developed and customized by the Service Provider. The IoT Firewall control plane typically contains two types of information:
  - A table listing IoT devices and the corresponding IoT Customer. This table may contain a very large number of devices. These device-to-IoT vendor mappings may take several forms, including:
    - A list of MSISDNs or IMSI devices
    - An IMSI range mapped to an IoT Vendor
    - A device connected to a specific APN belonging to a specific IoT service
    - Any distinctive element of the device which can be used to identify that device when it connects to the network
  - A table listing IoT customers' customized security policies, so that the IoT FW Control Plane can provision the correct policies to the data plane.

IoT Customer 1	Permit 192.168.5.0/24, Permit *.example.com
IoT Customer 2	Permit 10.100.0.0/23, Permit *.examplecar.com, www.carupgrade.com
...	
...	
IoT Customer n	Permit *.lightbulbupgradecustom.com

Table 1: Example of a table containing IoT Customer Policy

Workflow—enabling individualized customization

As described in the previous sections, the two elements (Control Plane and Data Plane/ Enforcer) represent the key components of the solution. Working together, they provide flexibility to allow customization on a per-customer level, while eliminating the need for customer-specific appliances, thereby reducing operational costs. When a new IoT customer is acquired by a Service Provider, all policy and provisioning information, as well as IoT device to customer mapping, is filed and stored in the Control Plane. This information may need to be updated over time as policies become more or less restrictive, IoT devices are added to or removed from the network, or as a result of changes to the application. A typical workflow might proceed as follows:

- When a new IoT device connects to the network, the Edge Device where the connection is terminated (which can be a vPGW in case of traditional mobile network) will send out an accounting message. This message will be intercepted by the IoT Firewall Control Plane as described in the picture below. This message is typically a Radius message, but, theoretically, any protocol can be used.
- The control plane extracts subscriber information from that message, including the IP address. Next, the control plane runs a lookup on the local information database to retrieve IoT customer information and corresponding policies.
- The IoT Firewall control plane sends the security policy to the IoT Firewall data plane. IoT devices are then provisioned by the IoT Firewall Data Plane as appropriate.
- The IoT Firewall data plane now has all the information needed to apply the right policies to the IoT device according to the definitions provided by the IoT Firewall control plane.

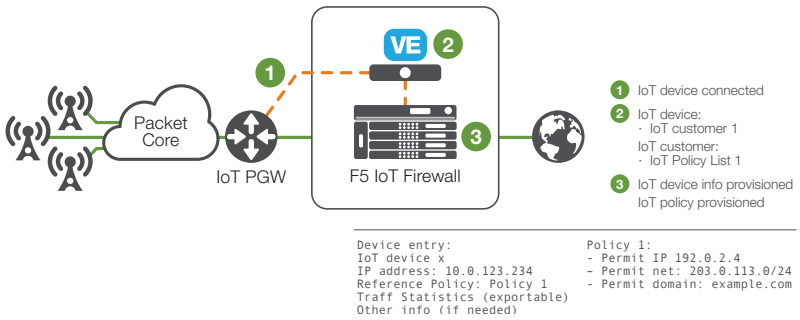

Figure 3: Typical workflow through the F5 IoT Firewall, including passage of information between the Control Plane and the Data Plane.

Addressing the IoT security risk

The F5 IoT Firewall is a critical component in any IoT network. It provides integrated, network-based security and traffic management capabilities, in combination with IoT device awareness. The IoT Firewall creates the ideal platform to provision new IoT security services, enabling Service Providers to cost-effectively introduce sophisticated IoT solutions within the existing infrastructure.

The rise of the era of the Internet of Things creates many opportunities; in order to take advantage of these opportunities, Service Providers must address the security risks created by network-based, device-to-device communications. F5's IoT Firewall allows Service Providers to ensure the security and resilience of their network, allowing them to provide ongoing, high-quality service in the face of new threats. By moving beyond basic connectivity services, Service Providers are also able to reduce operational costs and identify new opportunities to monetize new services demanded by IoT customers.

Learn more about F5 solutions for Service Providers at f5.com/solutions/service-providers.

©2019 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5.
DC0219 | OV-SP-306118756