WHITE PAPER

Securing the IoT Ecosystem with Fortinet

The potential impact of a successful cyberattack on an Internet-of-Things (IoT) ecosystem may result in failure of critical systems and industries and even physical danger to individuals and the environment. It is therefore important that IoT solution providers demonstrate a commitment to providing a service that is secure by design.

Managed service providers (MSPs), managed security service providers (MSSPs), and mobile network operators (MNOs) must embrace security as part of their IoT solutions and services in order to meet three main objectives:

1. Secure the entire IoT ecosystem to ensure service continuity
2. Deliver IoT security service-level agreements (SLAs) to encourage IoT services adoption and acceptance
3. Deliver revenue-generating IoT security services

Fortinet IoT Security Solutions

The Fortinet IoT solution consists of a number of best-practice security components that together provide comprehensive protection to an IoT ecosystem. Because the term IoT is in itself wide-ranging, any solution needs to be composed of a broad, integrated and automated feature set, which can be applied as needed for each individual use-case.

Fortinet IoT security capabilities are delivered via the most comprehensive range of network security products in the industry, interconnected, and integrated within the Fortinet Security Fabric to deliver a powerful platform for end-to-end IoT ecosystem security and security services.

Fortinet IoT security capabilities are delivered via the FortiGate next-generation firewall (NGFW) and FortiWeb application firewall. Both solutions comprise a range of physical and virtual offerings.

FortiGate Segmentation and Stateful Firewalling

In many cases, the traffic patterns of an IoT device are very predictable and a FortiGate stateful firewall can block any traffic that is addressed to nonauthorized destinations, as well as raising an alert to the fact that the device is behaving abnormally. In a typical IT environment, traffic to unauthorized destinations may be common due to many reasons, and typically such communications would simply be dropped. But in IoT and other machine-to-machine networks, such communications are usually a sign of misconfiguration or compromise. For this reason, specific negative rules should be configured with an appropriate action to ensure that an alert is generated, or automatic remediation is triggered.

FortiGate Intrusion Prevention

The FortiGate Intrusion Prevention Service is designed to detect and block a wide range of different IoT attacks, including:

- **Exploits**: This includes any attack on a vulnerability and will typically be used either to cause a denial-of-service (DoS) (by causing crashes or extra work within software) or local code execution that will often result in a second-stage attack such as transferring a malicious executable.
- **Scanning attacks**: These include looking for open Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports, or looking for known software or protocol versions. Usually the goal of reconnaissance attacks is to identify vulnerable targets, or to identify high-value targets.
- **Fuzzing attacks**: This is another method of finding vulnerabilities. It is usually done locally in a controlled environment, but can be used as a blunt-instrument attack on a live network. Examples include deliberate protocol anomalies or the use of extremely long fields, or invalid or unusual data. All of these techniques are designed to trigger programming errors. The goal is to find vulnerabilities, or simply to cause disruption.

These attack types and more are covered by the FortiGate intrusion prevention system (IPS) function, which contains more than 30,000 rules including an optional industrial package. Rule packages are automatically updated on a daily basis to ensure that protection is constantly up to date.

Fortinet IPS also has the ability to define rate-based rules, and since many IoT devices have a predictable packet rate, this can be used to detect unusual activity, possibly caused by malfunction or compromise, and remove such devices from the network.

There is a general trend in all areas of networking toward data encryption, and this is also true for IoT, where data is often of a private nature. Transport layer security (TLS) is most often used here, and IPS can perform TLS inspection to allow attacks to be detected over such secure links.

FortiGate Application and Protocol Control

The Application Control feature can be used to monitor or limit the protocols that can be used by the IoT device. Any unauthorized protocols can generate an alert and optionally be blocked. Application definitions include more than 4,000 application rules in 24 categories. All commonly used IoT protocols such as MQTT, AMQP, HTTP and CoAP are covered, and as for IPS, TLS inspection can be used with appropriate configuration. A wide range of industrial protocols is also available for Industrial Internet-of-Things (IIoT) solutions.

Antivirus

Fortinet has an industry-proven antivirus solution underpinned by FortiGuard Labs research and artificial intelligence (AI)-based processing. In conjunction with intrusion prevention, the vast majority of malicious files will never make it to their target.

Antivirus is important today mainly for the IoT infrastructure, such as the platform or web servers. But researchers anticipate that malware attacking the devices themselves—such as in the case of the Mirai IoT malware, perhaps the most famous current example—will become more prevalent in the years to come.

FortiGuard Labs has almost 20 years of experience defending against malware of all types, and despite the fact that device-targeted malware is rare today, the needed research is already underway to ensure that protection of the highest quality will be ready.

Anti-botnet

Any botnet activity, whether detected by destination address, domain, or protocol, can generate an alert and be blocked. Additionally, connections to other known bad destinations as detected by the FortiGuard Indicators of Compromise Service can generate a compromised alert. FortiGuard Labs maintains an updated list of known botnet destination address/port combinations that are checked against all outgoing sessions. Botnets that use fast-flux domains (in which a domain continually changes its IP address mapping) can be checked against the domain itself by intercepting and checking the Domain Name System (DNS) request. Finally, even if the destination address and domain are unknown, many botnets can be detected by their command-and-control protocol. By using these three methods in parallel, Fortinet ensures the best chance of detecting botnet-infected devices.

API Protection with FortiWeb

Application programming interfaces (APIs) are used in multiple areas in IoT networks. Generally speaking, the interactions between devices and IoT platforms are via APIs, usually involving protocols such as MQTT, HTTP, and CoAP, and using either JSON or XML as data encoding, with binary encodings such as CBOR used for high-compression, low-bandwidth environments. APIs are also used to communicate between applications and the IoT platform, usually using HTTP.

Fortinet has a very strong API protection function in FortiWeb, allowing a wide range of constraints to be defined, from simple rules such as maximum header and field lengths, all the way to schema validation and enforcement, focused on HTTP with JSON or XML.

In conjunction with FortiWeb, both generic attacks as well as those focused on attacking representational state transfer (REST) APIs and web front ends can be mitigated.

Automation

Fortinet has a comprehensive automation framework that allows a wide range of triggers to be linked to actions such as alerting, removing rogue devices from the network, or making API calls to other devices.

For example, any of the above detections can cause a device to be quarantined and blocked from further communications until the cause is established and remedial action is taken.

The Fortinet Security Fabric

With so many different IoT security challenges, a disparate set of independent point products inevitably introduces more challenges in terms of operational complexity.

The Fortinet Security Fabric was designed to overcome these challenges by integrating security components with the goal of ensuring that devices work in a consistent way, with sharing of threat intelligence, unified visibility and reporting, aggregated log processing and analysis, and single-pane-of-glass management. Fortinet IoT solutions form a part of the overall capabilities the Fortinet Security Fabric delivers to enterprises, MSPs, MSSPs, and MNOs.

Going Beyond: Integration with Technology Partners

Aptilo and Fortinet IoT Connectivity Control Service

The Fortinet Security Fabric also extends to a carefully selected set of third-party products that are part of the Fortinet Fabric-Ready program. Each of these partnerships has been developed to ensure a high-quality integration with the fabric for products, which bring real value to the overall solution.

Fortinet has been working with multiple technology partners to integrate their IoT solutions—complementing and enhancing the ability of communications service providers (CSPs) to deliver a broad set of innovative IoT services to their enterprise customers. This ecosystem of pre-integrated solutions provides rapid and effective onboarding of an ever-growing scope of integrated IoT services.

The Aptilo IoT Connectivity Control Service (IoT CCS) is an example of an IoT Security Fabric integration and the added value it provides to MNOs.

IoT CCS enables MNOs to meet some of the limitations presented by mobile packet cores (even enhanced ones) when trying to create flexible IoT services at scale, including:

- Complexity of offering private access point names (APNs) (virtual private network [VPN] connection) to businesses at scale
- Inability to offer IoT security services beyond APNs
- Automatic onboarding of new customers not possible
- Customers challenged to manage their own security and connectivity policies
- Impossible to set unique policies per customer, let alone per device
- Difficult to set up APNs to multiple stakeholders from the same device
- Difficult to bring global IoT connectivity without roaming and with policy-based traffic breakout

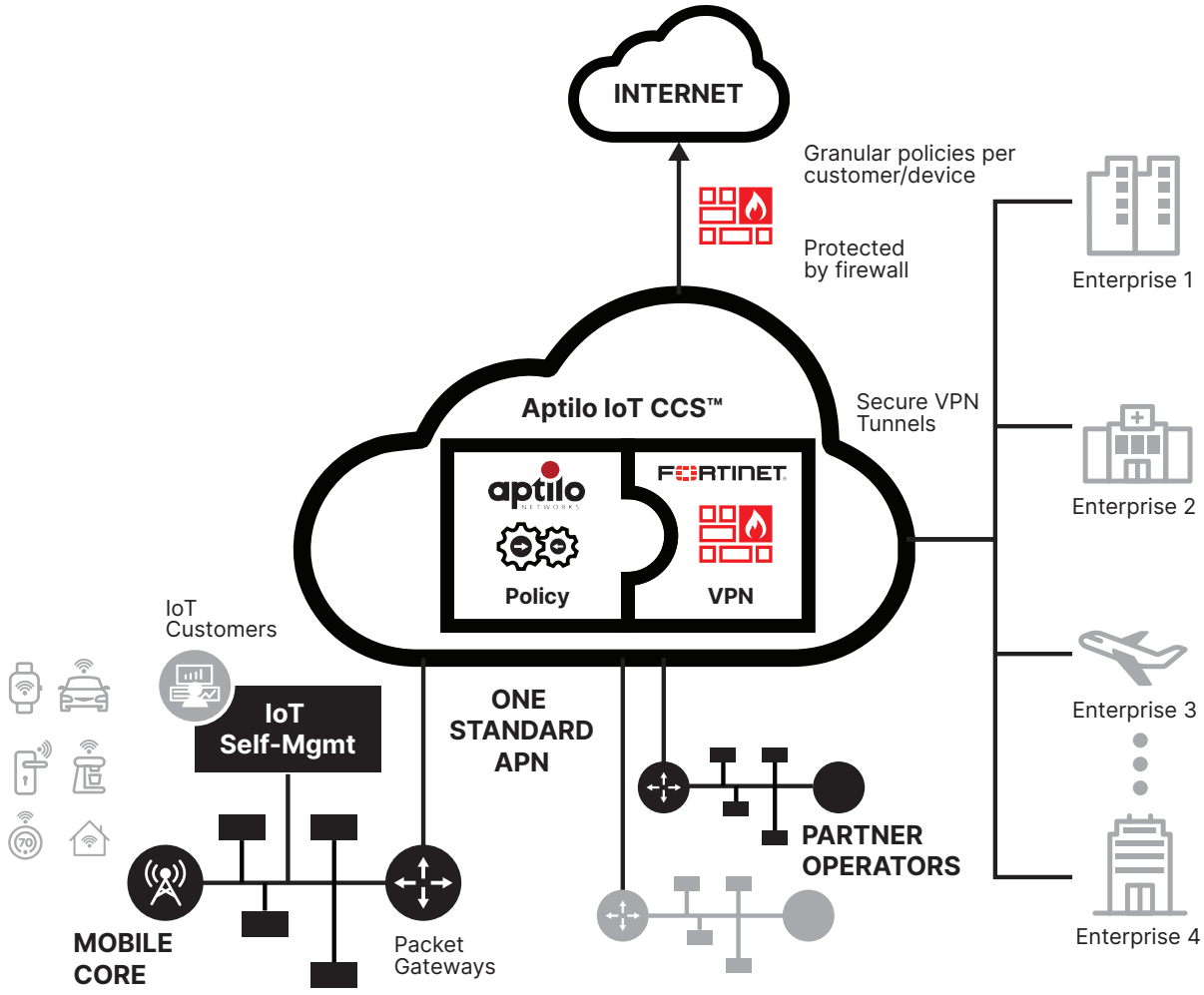
With the joint solution from Fortinet and Aptilo, mobile operators can leave their mobile core untouched and create IoT connectivity services previously considered out of reach. IoT CCS delivered as a service on Amazon AWS (OPEX) provides a flexible IoT connectivity control and security layer on top of any current and future mobile core. Mobile operators can deliver innovative IoT connectivity services in days rather than months, with a fraction of the alternative cost.

FortiGate, the family of Fortinet network firewalls, handles the security and traffic/data plane of the IoT CCS. Through FortiGate, IoT CCS gets policy enforcement at the edge, routing, VPN management, device traffic filtering, protection against distributed denial-of-service attacks (DDoS), limitation of the number of TCP connections, and more. Detection of anomalies is also part of the IoT CCS security layer.

IoT CCS multitenancy virtual APN removes the complexity of setting up individual private APNs for each business customer with only **one** standard APN to IoT CCS to serve all enterprises that are connected to the service. The VPNs are automatically provisioned via an API, making onboarding of new customers a breeze.

Using the same APN name, mobile operators can add international mobile operator partners to their IoT CCS service. Combined with their ability to instantly localize eSIM (eUICC) over the air, operators can offer a truly global and secure connectivity without roaming charges.

Through the IoT CCS multitenancy virtual APN, operators can offer a secure international connectivity with optional breakout for selected traffic at the nearest AWS point of presence, delivering optimized performance via the use of FortiGate software-defined wired-area network (SD-WAN) capabilities. This is a unique capability that is virtually impossible to obtain in the standard 3GPP core with home routing as the typical option.



Summary

IoT is changing the world we live in, and is bringing both massive opportunity and significant challenges in its wake. CSPs have an essential role in enabling and securing the IoT ecosystem for their customers.

Fortinet is ideally positioned to secure the diverse needs of IoT services and ecosystem, from enterprises to service providers. With carrier-grade performance, multitenancy, and flexible consumption models, Fortinet provides CSPs with an IoT security platform that safeguards IoT services and revenue while empowering customers to deliver on the promise of IoT.

May 31, 2021 1:59 PM

Macintosh HD:Users:spedersen:Desktop:wp-securing-the-iot-ecosystem-with-fortinet Folder:wp-securing-the-iot-ecosystem-with-fortinet

785701-A-0-EN