COMMSCOPE® RUCKUS®

White Paper

Ruckus IoT Security

December 2020

Table of Contents

© 2020 CommScope Inc. All rights reserved.

Intended Audience

This document provides an overview of the security behind IoT (Internet of Things) devices and protocols and the underlying security architecture of the Ruckus IoT (RIOT) suite. Some knowledge of the network protocols is recommended.

This document is written for and intended for use by technical engineers with background in Wi-Fi design and 802.11/wireless engineering principles. An understanding of IoT protocols such as IEEE 802.15.4, BLE, and Zigbee is recommended.

For more information on how to configure CommScope products, please refer to the appropriate CommScope user guide available on the CommScope support site. https://www.commscope.com/SupportCenter/.

© 2020 CommScope Inc. All rights reserved.

Overview

This document provides an overview of the security behind IoT (Internet of Things) devices and protocols and the underlying security architecture of the Ruckus IoT (RIOT) suite and is broken into the following main categories:

- State of IoT
- IoT-Designed Secure Architecture

Part One: State of IoT

The Internet of Things (IoT) landscape is varied and rapidly changing. Enterprises seeking to deploy IoT solutions come across challenges such as network investment, system integration, security, data analytics and several others. To encourage adoption, enterprise IoT solution vendors often develop vertically integrated, proprietary infrastructure silos that often address only a single problem, but that do not readily integrate with other silos and offer limited opportunity for infrastructure reuse. Each IoT system brings individual challenges and may use any number of network access technologies. When combined with other network vendors, IoT systems typically work in isolation from each other. The net result is that even successful IoT deployments require redundant network infrastructure, additional security apparatus, and extensive integration services. Low power radio-based systems (Bluetooth/BLE, Zigbee, etc.) require a radio hub or gateway device specific to the protocol it uses, and that device requires a network port and power.

More Layers of Complexity

As networks have evolved, they have added speed, functionality, and features, but have also added layers of complexity. An enterprise network twenty years ago was wired and probably flat. Managing and troubleshooting such a network involved following the packets. Securing it meant controlling access to ports and defining access to network resources. With the introduction of Wi-Fi, another layer of complexity was added. The packets were now in the air and so were the security risks. As a new technology focused primarily on access, the security aspects were an afterthought and had their share of growing pains. Anyone who has tried to secure a WEP network or managed a WPA/TKIP transition network understands pain.

IoT devices, both wired and wireless, bring yet another layer of complexity to networks. Whether these devices are integrated alongside the rest of the network devices or deployed as an overlay network, they pose a risk as they introduce a potential break-in point. This is especially true if they are part of an OT (operational technology) deployment and outside the purview of the IT enterprise system operator or if isolation best practices are not followed.

© 2020 CommScope Inc. All rights reserved.

Wi-Fi engineers have had to become experts on the wide variety of clients that access the network as each one brings its own challenges in terms of their behavior accessing and using the network. As Wi-Fi has become the dominant access mechanism, Wi-Fi engineers have also had to become experts in troubleshooting upper layer protocols and devices north of the access point since any problem a client device has is always blamed on the Wi-Fi. The level of complexity that IoT integration brings is further compounded by the plethora and variety of the devices using a variety of underlying protocols. IoT networks are a bouillabaisse soup that can include:

- IoT devices managed by the enterprise (both IP and non IP)
- BYOD devices such as home domain devices
- Mobile IoT devices, such as BLE tags

Best practices demand Wi-Fi systems be isolated, secured on dedicated VLANs, and may need careful examination of performance requirements. Wired IoT devices can be powered using PoE, but power budgets add new dimensions to network design and switch management. Unfortunately, even solving all that, each IoT system is usually logically isolated from every other one with proprietary management systems.

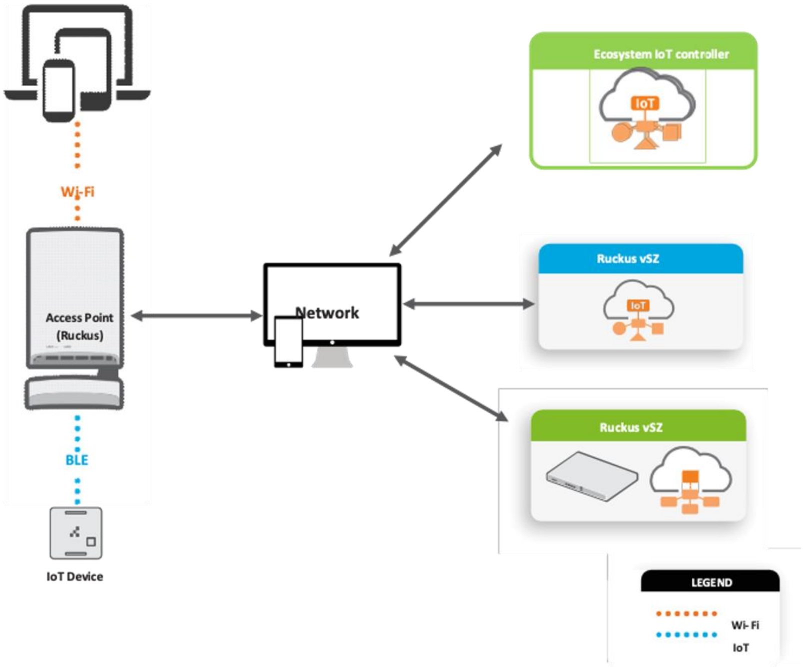

FIGURE 1: RUCKUS IOT ARCHITECTURE

© 2020 CommScope Inc. All rights reserved.

Growth of IoT Devices and Traffic[1]

IoT devices (things) from a security point of view are unique endpoints that can each autonomously connect and bidirectionally exchange data across the Internet. They represent the nearest and farthest edges of the network. Each IoT device can generate machine-state and/or surrounding environmental data that allows for monitoring, management, and analysis. These devices can be broadly categorized as video surveillance, household, medical, and industry uses.

The pace of the growth of the number of devices connected to the Internet continues, with one study from International Data Corporation estimating that by 2025, there will be 41.6 billion connected IoT devices: everything from machines, to sensors, and cameras. In the average enterprise, more than 30% of all network-connected endpoints are IoT devices (excluding mobile devices).

These devices will generate almost 80 zettabytes (ZB) of data in the year 2025. For reference, one gigabyte (1GB) is 1000 x 10^3 kilobytes. One zettabyte is 1000 x 10^7 kilobytes. The impact to networks doesn't only come from the amount of data generated. These varied devices each generated traffic with specific characteristics. Some devices, such as those seen in industrial and medical use, send machine health metrics, resulting in small, but bursty traffic, while other devices, such as video surveillance cameras being used to analyze large crowds, can generate large amounts of steady data.

The types of devices and their use cases are also expanding. Originally, industrial and automotive equipment were overwhelmingly represented followed by a strong growth in household devices (i.e. all things "smart home") and wearable devices. Increasingly, public safety concerns, the decrease in costs for cameras, and the higher bandwidth options, including Wi-Fi 6 and Wi-Fi 6e (6GHz) with low latency, high bandwidth, and increased channel capacity are growing in adoption rate.

Again, the amount of video traffic being generated is exploding. These are large, steady streams of traffic and it's not just the amount of traffic, it's the variety of devices generating it. It would not be unusual for a house to have a Ring doorbell, a few Nest cameras, outdoor security cameras, untold numbers of environmental control devices and home automation devices, not to mention the household appliances. All of these produced by different vendors and using up to a handful of different lower and upper layer protocols. The next highest category of traffic being generated by IoT devices is short, bursty, but exceptionally latency sensitive. These are the light switches, door locks, asset tracking, and the multitudes of medical equipment. The question then becomes, how do you have a network that can support both bursty and absolutely-has-to-get-there-without-delay traffic as well as steady high-volume traffic? The answer is—by design, not by accident.

In the example figures below each of the device types was designed and to be deployed and managed separately; considerations like CoG (cost of goods) take precedence over SecDevOps or security by design.

© 2020 CommScope Inc. All rights reserved.

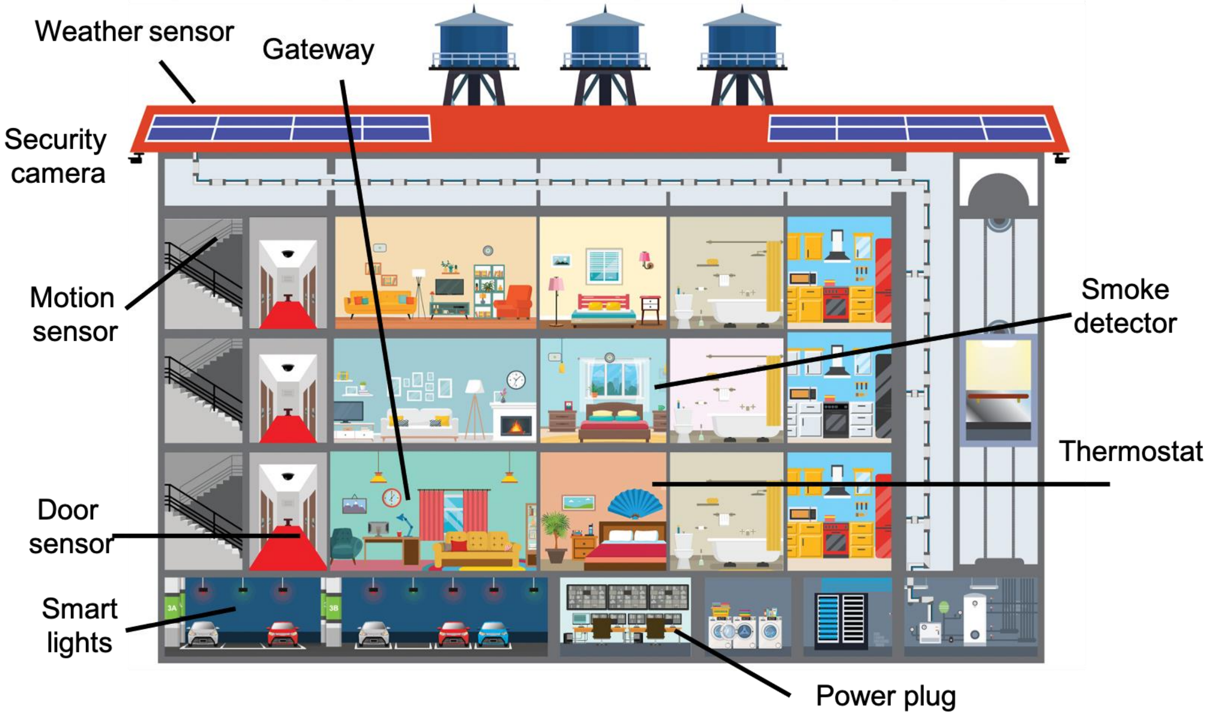

FIGURE 2: VARIETY OF IOT DEVICES IN THE HOME

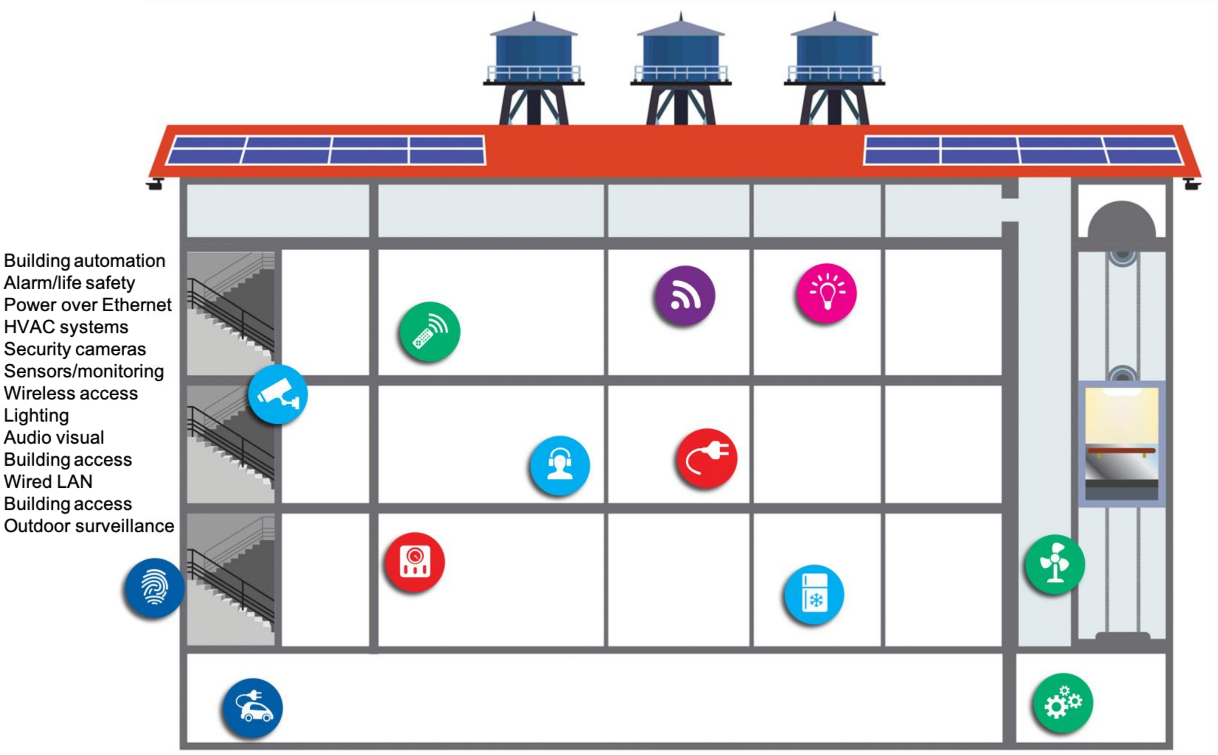

FIGURE 3: VARIETY OF IOT DEVICES IN THE ENTERPRISE

© 2020 CommScope Inc. All rights reserved.

Increasingly, IoT is becoming the fabric that will enable information exchange between people, processes, and “things” and, increasingly IoT devices are providing mission critical services. For example, connected entry systems, panic buttons, cameras and other surveillance sensors ensure safety across enterprise, MDU (multiple dwelling unit), and smart home deployments. There are industrial applications as well for physical safety, including sensors that guarantee required network conditions are being met for har real-time applications such as robotic controls and environment variables.

The data that is being shared from south to north end of the network (and back) has value for people, industries, and governments. Being able to scale to meet the needs created by this traffic is one thing; being responsible for managing the security vulnerabilities and privacy concerns all this creates is another. This cannot effectively be done as an afterthought, however, demanding the myriad of IoT vendors to design and develop devices with security at the forefront is not just a fool’s errand, effectively, that ship has sailed. Part Two: IoT-Designed Security Architecture will describe how to mitigate this and ensure that even a varied IoT/OT network can be designed, not just for performance, but for security as well.

Note: [1] https://www.idc.com/getdoc.jsp?containerId=prUS45213219

© 2020 CommScope Inc. All rights reserved.

State of IoT Security[2]

A recent Palo Alto study revealed an alarming trend. While the amount of IoT traffic and the number of IoT endpoints is dramatically increasing, the general security posture of IoT devices is declining. This leaves organizations vulnerable, not only to new IoT-specific malware but also to old attacks that the proliferation of IoT makes viable again.

It is not news that security professionals view IoT endpoints as "low hanging fruit back door" vulnerabilities into networks, but a Palo Alto report contains alarming numbers.

- 98% of all IoT device traffic is unencrypted.

  This exposes personal and confidential data on the network. Attackers who've successfully bypassed the first line of defense (most frequently via phishing attacks) and established command and control (C2) are able to listen to unencrypted network traffic, collect this information and then exploit that data for profit on the dark web.

- 57% of IoT devices are vulnerable to medium- or high-severity attacks.

  This makes IoT the low-hanging fruit for attackers. Because of the generally low patch level of IoT endpoints, the most frequent attacks are exploits using long-known vulnerabilities and password attacks using default device passwords. (See Note[3])

  - 83% of medical imaging devices run on unsupported operating systems.

  As a result of the Windows® 7 operating system reaching its end of life, this is a 56% since 2018. This general decline in security posture opens the door for new attacks, such as cryptojacking (which increased from 0% in 2017 to 5% in 2019) and brings back long-forgotten attacks such as Conficker, which IT teams have long been immune to.

  - 72% of healthcare VLANs mix IoT and IT assets.

  Healthcare organizations, in particular display poor network security hygiene. This allows malware to spread from users' computers to vulnerable IoT devices on the same network. There is a 41% rate of attacks exploiting device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses. This is a shift from IoT botnets conducting denial-of-service attacks to more sophisticated attacks targeting patient identities, corporate data, and monetary profit via ransomware.

Note[2]: https://unit42.paloaltonetworks.com/iot-threat-report-2020/

Note[3]: California's SB-327 IoT law took effect on January 1, 2020. It prohibits the use of default credentials.

© 2020 CommScope Inc. All rights reserved.

A number of high-profile, IoT-focused cyberattacks have forced enterprises to recognize that managing the risks introduced by IoT is necessary to protect their core business operations. This is hampered by the fact that organizations lack the tools to manage and secure their IoT devices. Enterprises manage their IT (information technology) and OT (operational technology) separately and each team has their own processes and tools. IT assets include computers, printers, and network equipment. OT assets include security cameras, door locks, HVAC sensors, etc.

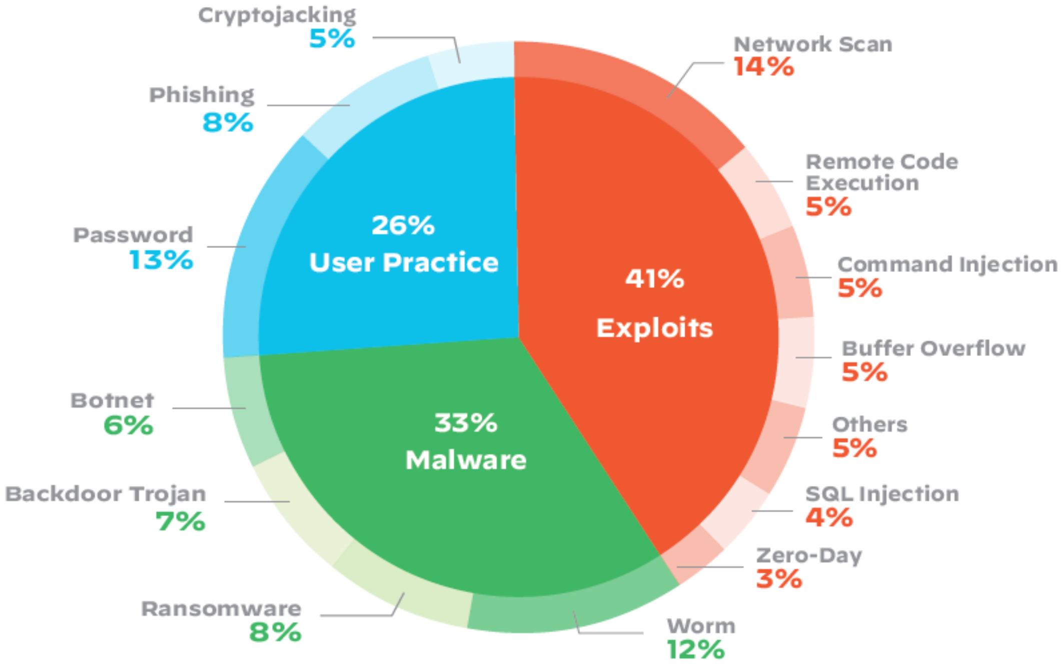

FIGURE 4: BREAKDOWN OF TOP IOT THREATS

© 2020 CommScope Inc. All rights reserved.

High Profile Attacks[4]

IoT hacking can be extremely effective, producing DDoS attacks that can cripple our infrastructure, systems, and way of life.

- Mirai Botnet: Service provider Dyn suffered the largest DDoS attack (to date) using hundreds of thousands of IoT devices (and IoT botnet) in October 2016. As a result, large portions of the Internet went down, including Twitter, the Guardian, Netflix, Reddit, and CNN. The malware used to create the botnet, Mirai, infected computers, which then continually searched the Internet for vulnerable IoT devices. Using known default usernames and passwords, Mirai gained access to the IoT endpoints, such as cameras and DVR players, and infected them. (https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet)
- St. Jude pacemakers: A year later, a vulnerability in devices like pacemakers and defibrillators that are used to monitor and control patients' heart functions and prevent heart attacks was exposed. Bad actors could take over control by hacking the app that transmits information to the implanted device. Once in, they could deplete the battery or administer incorrect pacing or shocks, according to the FDC. (https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/)

  The TRENDnet Webcam Hack: Cameras used for home security and baby monitoring had flawed software that allowed anyone with the camera's IP address to access the video and even audio. The mobile apps for the cameras stored consumers' login information in clear, readable text, in violation of basic security practices that dictate IP addresses should be secured and login credentials should be encrypted. (www.technewsworld.com/story/78891.html)

  Jeep Hack:In 2015, a team of researchers exploited a firmware update vulnerability to hijack and remotely control the vehicle over a Sprint cellular network. They were able to make the Jeep speed up, slow down, and veer it off the road. (https://securityintelligence.com/eight-crazy-hacks-the-worst-and-weirdest-data-breaches-of-2015/)
- Ring cameras: Using known user names and passwords, hackers accessed the camera and speaker system
- Philips Hue bulbs, Yale locks, many more…

Note[4]: **https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/**

© 2020 CommScope Inc. All rights reserved.

Attack Surface

The attack surface of a network is the aggregation of all the different vectors (attack points) where an authorized user can exfiltrate data, insert data, or change values within the network. The goal of network security is the keep the attack surface as small as possible. The proliferation of IoT devices in networks makes this challenging. IoT attack surface areas:

- **Devices:** Devices are often the initial source of an attack. Vulnerabilities can exist in a device's memory, firmware, physical interface, web interface, and network services. Any unsecure default settings, outdated components, and unsecure update mechanisms can be exploited by attackers.
- **Communication channels:** Attacks can also originate from the channels that connect IoT devices to each other. Protocols (see more below) used in IoT systems can have security issues that can affect the entire network. IoT systems are also susceptible to known network attacks such as denial of service (DoS) and spoofing.
- **Applications and software:** Vulnerabilities in web applications and related software for IoT devices can lead to network compromises. Web applications can, for example, be exploited to steal user credentials or push malicious firmware updates.

Securing the Surface

The development life cycle between software development and IT operations is referred to as DevOps, a cross-functional mode of working that uses the following categories to define key aspects of the development and delivery process:

- Coding
- Building
- Testing
- Packaging
- Releasing
- Configuring
- Monitoring

© 2020 CommScope Inc. All rights reserved.

What is notable is that security is not mentioned, which many industry experts have critically referred to as making security an “afterthought”. Breaking away from the traditional centralized security team model allows a delivery team to factor in the correct security controls into their DevOps model.

This augmentation is referred to as DevSecOps. At its foundation is the stance that security must be designed-in from the initial architecture phase. This is vital to controlling and minimizing the attack surface. Additional considerations include:

- Physical hardware access
- MQTT links
- REST API interface
- Any component communicating with Internet-based services and apps
- Allowing default usernames and passwords
- IoT protocol security gaps (not following the spec or best practices or not updating to newer versions of firmware)
- Secure data separation between clients

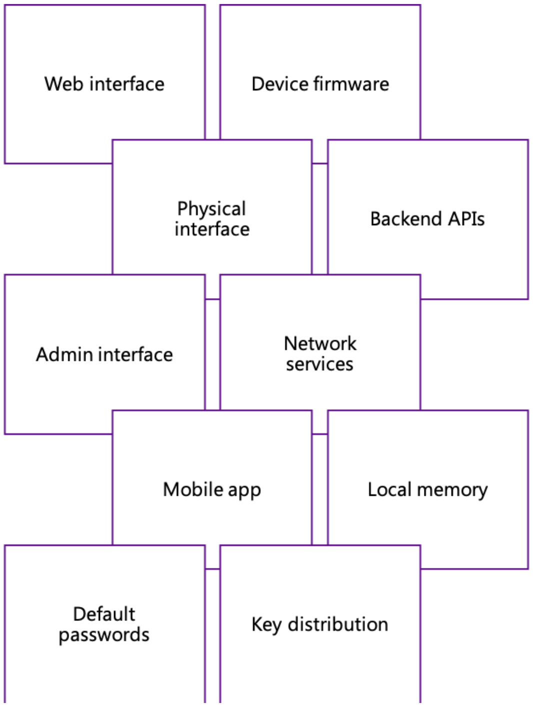

FIGURE 5: ATTACK SURFACE

© 2020 CommScope Inc. All rights reserved.

Protocols

Zigbee

The Zigbee protocol uses the 802.15.4 standard and operates in the 2.4 GHz frequency range with 250 kbps. The maximum number of nodes in the network is 1024 with a range up to 200 meters. Zigbee can use 128-bit AES encryption.

Zigbee has gone through several releases and rebranding that can be confusing to parse. ZigBee was ratified as draft 1.0 in 2004 and had numerous updates between 2005 and 2012. ZigBee Pro was ratified in 2007 and had a major update in 2015. The update made changes to the application and network layers, changes to security and clarification on the use of the 802.15.4 at the MAC and PHY layer. It was finally rebranded to Zigbee in 2018.

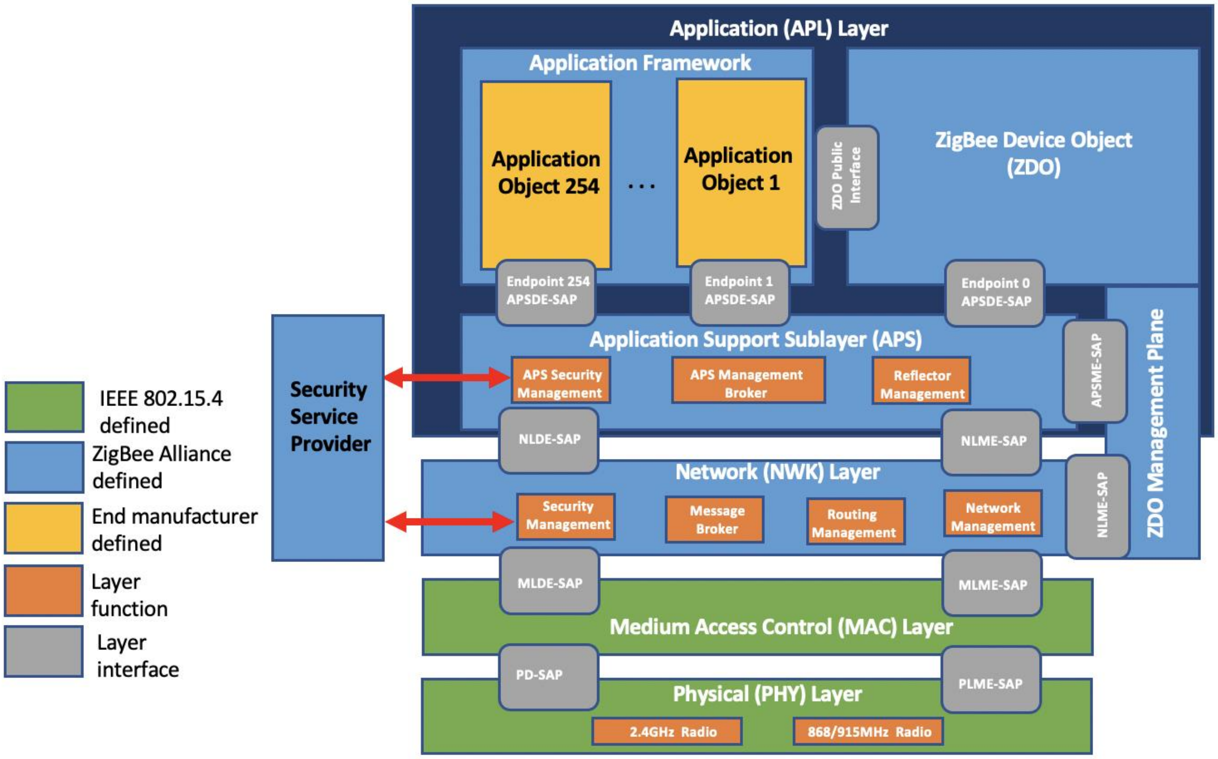

FIGURE 6: ZIGBEE PROTOCOL STACK

Securing Zigbee

Zigbee 3.0 with install code-based provisioning was established as the previous versions of Zigbee used a well-known key for bootstrapping the link security.

Zigbee supports centralized and distributed security modes. ACLs allow for pre-configured nodes to join the network.

Frame counters are used to prevent sending the same message multiple times. Receivers will use the frame counters to reject messages they have already processed. This process assists in preventing replay attacks.

Zigbee supports both link keys and network keys. The link keys are used between pairs. The network key is used at the network layer by all devices in the network.

© 2020 CommScope Inc. All rights reserved.

BLE

Bluetooth works in the 2.4 GHz ISM band and uses frequency hopping. With a data rate up to 3 Mbps and maximum range of 100m. Each application type which can use Bluetooth has its own profile.

Bluetooth has been around even longer than Zigbee and has also gone through several evolutions. Bluetooth Low Energy (BLE) is the fourth iteration and introduced a feature that reduced power consumption when communicating with low data rate devices like sensors. Bluetooth 5.x was first introduced in 2016 and brought optimization for IoT with higher bandwidth and longer range. All versions of Bluetooth are backwards compatible.

Early Security Issues

BLE “just works pairing” is considered insecure for several settings as it uses ephemeral keys based ECDH driven key exchange and hence does not provide protection against MITM attacks.

BLE Encryption

When encrypted and authenticated, all Data Physical Channel PDUs with a non-zero length Payload, all CIS Data PDUs, and all Broadcast Isochronous PDUs with a non- zero length Payload (in each case except those with an empty payload) shall be encrypted and authenticated. Authentication is performed by appending a MIC field to the Payload. Bluetooth supports AES-128 encryption.

The full security algorithms supported by BLE are:

- AES-CCM 128-bit encryption
- HMAC-SHA256 authentication
- ECDH or HMAC-SHA256 key generation

The standard specifies a link key used for authentication and it is a 128-bit key shared between the devices authenticating. The encryption key is derived from the link key, a random number, and a 96-bit Ciphering OFfset number (COF). The encryption key can be from 8 bits to 128 bits to accommodate for government regulations that may not allow for 128-bit encryption. The link key is 128-bits in all deployments as governments do not typically constrain authentication strength as they do encryption strength.

© 2020 CommScope Inc. All rights reserved.

Part Two: Ruckus IoT-Designed Secure Architecture

To address many of the issues described in the previous section, RUCKUS has developed a suite of products that can be deployed as an IoT access network that consolidates multiple physical-layer networks into a single converged network. This common network simplifies IoT endpoint onboarding, establishes uniform security protocols, and converges IoT endpoint management and policy setting.

The RUCKUS IoT Suite simplifies the creation of IoT access networks through the reuse of LAN and WLAN infrastructure, which shortens the time to deploy and reduces the cost of an IoT solution.

The following figure shows the various components that comprise the Ruckus IoT Suite.

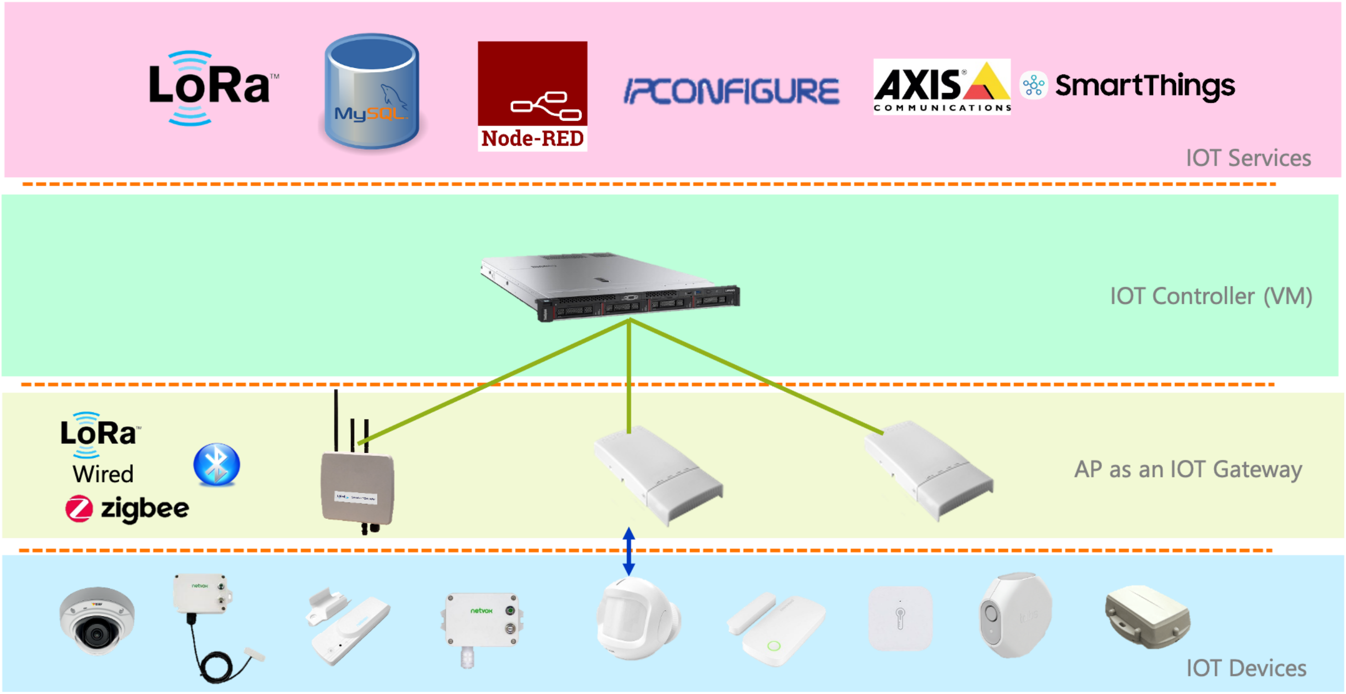

Figure 7: Security by Design

The Ruckus IoT Suite brings innovative features, including:

- A dedicated and secure IoT controller that provides a single pane view for management, control, and data traffic. This gives admins visibility of every IoT gateway or device in the organization from a single pane view.
- Enterprise grade authentication and authorization using a technology-independent centrally managed access filtering layer on top of the protocol-specific mechanism. This gives administrators full control to authorize or deny any IoT device access to the network and provides a policy enforcement point for IoT.

© 2020 CommScope Inc. All rights reserved.

- Forced default password change. This conforms with various regulatory requirements, such as SB-327 and to pass PCI security mode testing.
- PCI compliance (Payment Card Industry security)
- Secure, instantly patchable, auditable, and upgradable IoT hardware platform
- Physical hardware security for IoT dongles where used
- PEN tested solution

There are many ways in which IoT technology can aid across verticals. However, each IoT system brings individual challenges. When combined with other network vendors, IoT systems typically work in isolation from each other. Each requires a radio hub or gateway device specific to the protocol it uses, and that device requires a network port and power. It is better than wiring each IoT device, but every new cable run costs hundreds of dollars, at least. Then each IoT system is logically isolated from every other one with proprietary management systems.

For the physical layer, the Ruckus IoT Suite moves all gateway functions onto our IoT-ready APs by adding an IoT module. The snap in IoT module becomes the gateway for all IoT devices, and piggybacks power and network on the AP cable. No additional cable runs or switch closet ports.

For the logical layer, IoT devices are secured and unified by the Ruckus IoT Controller, a virtual machine. IoT devices use a lightweight message protocol called MQTT (think 'https for IoT'). Because all such traffic is encrypted and forwarded to the Ruckus IoT controller (acting as an MQTT broker), messages from different IoT systems can trigger functions on each other. For example, a door left open for too long can trigger an adjustment to the air conditioner, enabling green and sustainability initiatives.

Simply put, the Ruckus IoT Suite creates a single network for IT and OT.

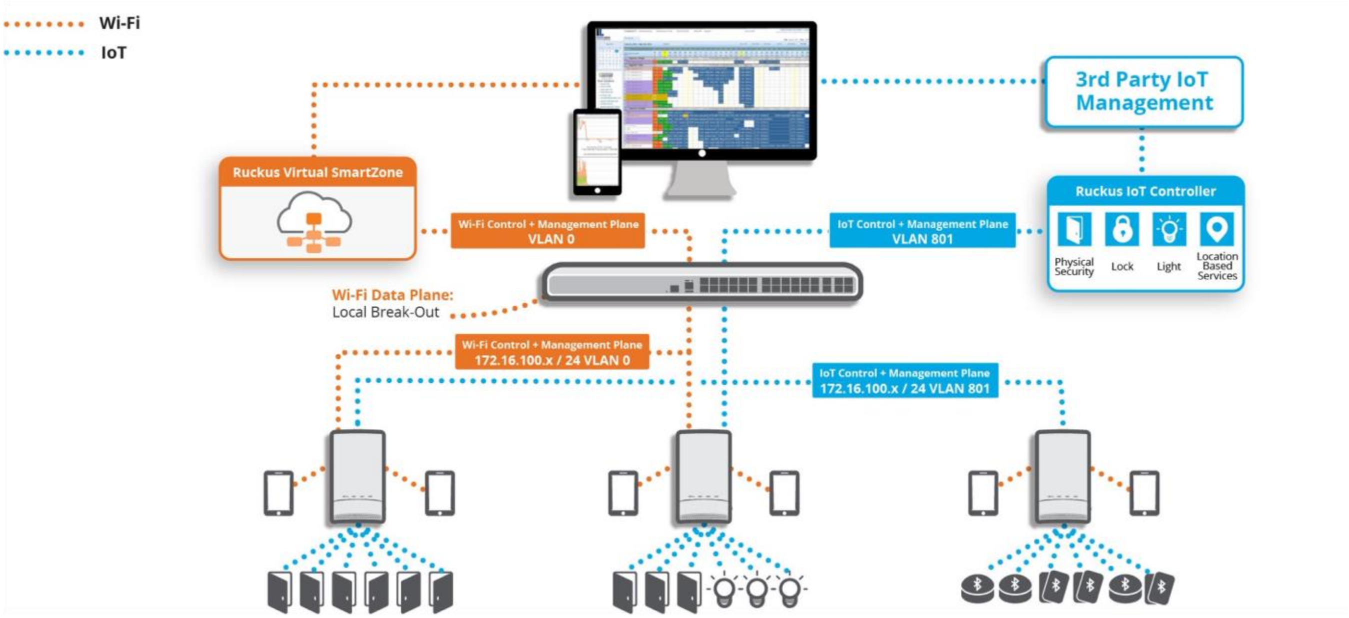
Wi-Fi
IoT
3rd Party IoT Management
Ruckus Virtual SmartZone
Ruckus IoT Controller
Physical Security
Lock
Light
Location Based Services
Wi-Fi Control + Management Plane VLAN 0
IoT Control + Management Plane VLAN 801
Wi-Fi Data Plane: Local Break-Out
Wi-Fi Control + Management Plane 172.16.100.x / 24 VLAN 0
IoT Control + Management Plane 172.16.100.x / 24 VLAN 801

FIGURE 8: TYPICAL RUCKUS IOT DEPLOYMENT

© 2020 CommScope Inc. All rights reserved.

The following components make up the Ruckus IoT Suite deployment:

- Ruckus IoT-ready access points
  - Ruckus 11ac (Wi-Fi5) access points with the Ruckus IoT module is used to establish multi-standards wireless access for Wi-Fi and non-Wi-Fi IoT endpoints
  - Ruckus 11ax (Wi-Fi6) access points natively support both Wi-Fi and non-Wi-Fi IoT endpoints
- Ruckus IoT Modules: Radio or radio-and-sensor devices that connect to an 11ac (Wi-Fi5) Ruckus IoT-ready AP to enable endpoint connectivity based on standards such as Bluetooth Low Energy (BLE), Zigbee, and LoRaWAN.
- Ruckus SmartZone Controller: A network controller that provides a management interface for the WLAN
- Ruckus IoT Controller: A virtual controller, deployed in tandem with a Ruckus SmartZone OS-based controller, that performs connectivity, device, and security management

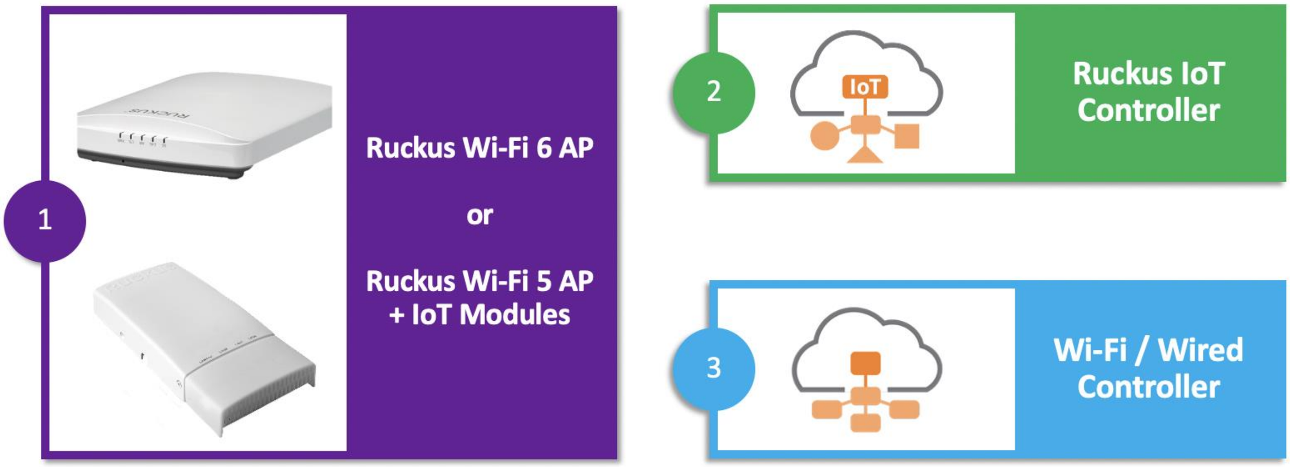

FIGURE 9: RUCKUS IOT SUITE COMPONENTS

© 2020 CommScope Inc. All rights reserved.

Architecture Analysis

End-to-end, the RUCKUS IoT Suite has been designed with a security-first and not as an afterthought.

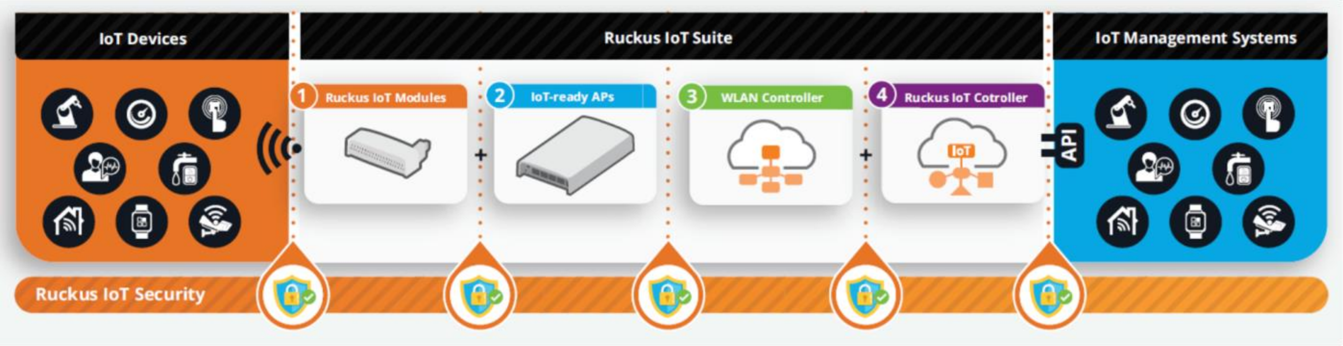

FIGURE 10: OVERVIEW OF RUCKUS IOT SUITE

Device to IoT Module

From IoT device to the RUCKUS IoT Module, security is ensured through:

- Authorized Access: Admin Login, RBAC, and IoT Device Policy Enforcement
- Secure Onboarding: MAC Whitelist, Pair Join, Device Fingerprinting
- Radio Transport Security (Zigbee, BLE)
- Application-level security (proprietary Zigbee, BLE payload)
- The most mature IoT chip in the industry with 100s of customers for the IoT stack

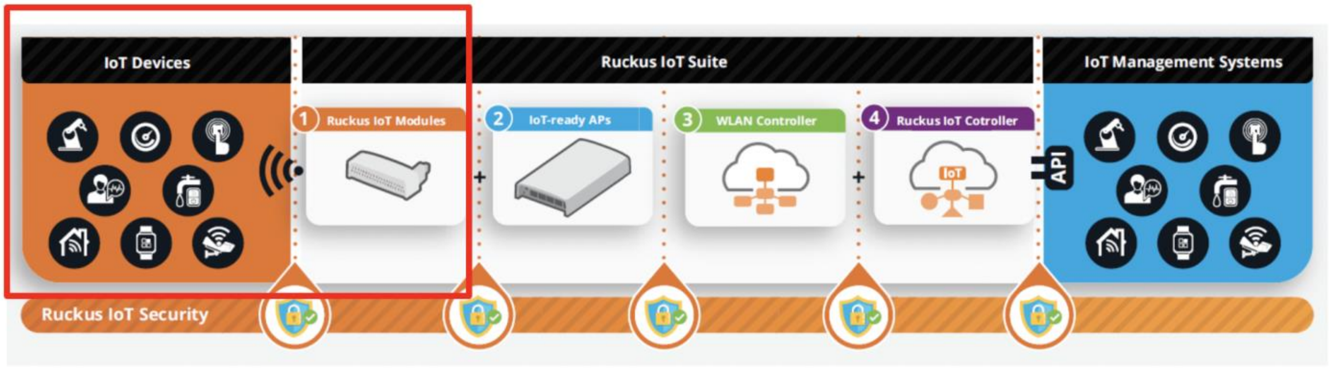

FIGURE 11: DEVICE TO IOT MODULE

Note: RUCKUS 11ax (Wi-Fi6) access points natively support IoT without the need for an attached IoT Module.

© 2020 CommScope Inc. All rights reserved.

Secure Enterprise IoT Onboarding

Onboarding an IoT device or RUCKUS access point requires admin login rights on the RUCKUS WLAN controller and some specific on-boarding actions.

The access points have the latest IoT protocol stacks and use enterprise-grade security sub-modes where available (E.g. Zigbee high security/enterprise mode or BLE passkey pairing). Device discovery is initiated by admin-approved access points, not by the IoT device.

Note: Zigbee 3.0 install codes are supported and the AP handles all Zigbee key management aspects. Legacy Zigbee is supported with additional patent pending link-layer security bootstrapping mechanisms. These initial key bootstrapping mechanisms have been co-designed between Ruckus and DormaKaba and also Salto.

The device discovery window is open for a limited time only and access points are always the coordinator of the network and can blacklist specific devices. Each device is authorized either by the IoT Controller admin manually authorizing each device by information discovered, or by bulk authorization using a csv-file uploaded to the IoT controller.

Secure Enterprise Onboarding Flow

- Turn on limited-time IoT discovery
- Present each device to IoT admin who can approve them manually or in bulk
- Allow each device to communicate by whitelisting it in the AP with its gateway

A global device table is maintained in the AP for authorized and unauthorized devices. Access points can ping each device every 30 seconds to ensure the connection is alive and secure.

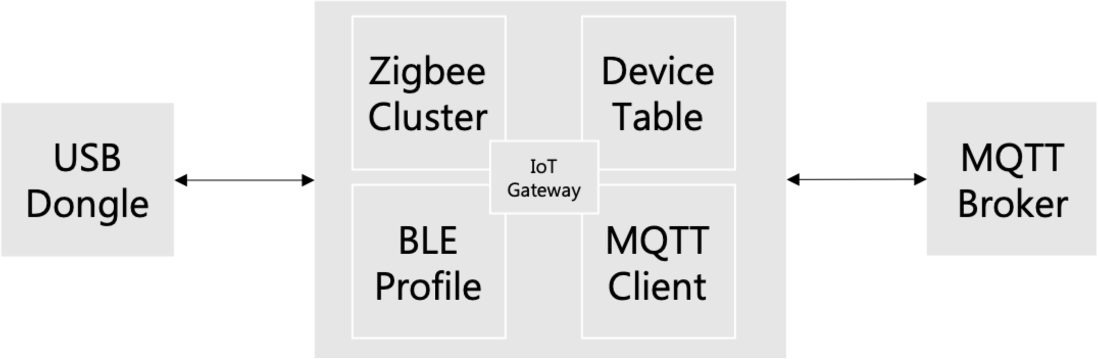

FIGURE 12: DEVICE CONNECTION TO THE NETWORK

© 2020 CommScope Inc. All rights reserved.

IoT Module to Access Point

Associating the IoT Module to the RUCKUS 11ac (Wi-Fi5) access point requires admin login rights and approval for the AP to in the IoT gateway and IP assignment after the USB plug-in. Physical security is accomplished with a security bracket and a sophisticated software-based hardware events framework provides physical intrusion detection using dongle-out event logic.

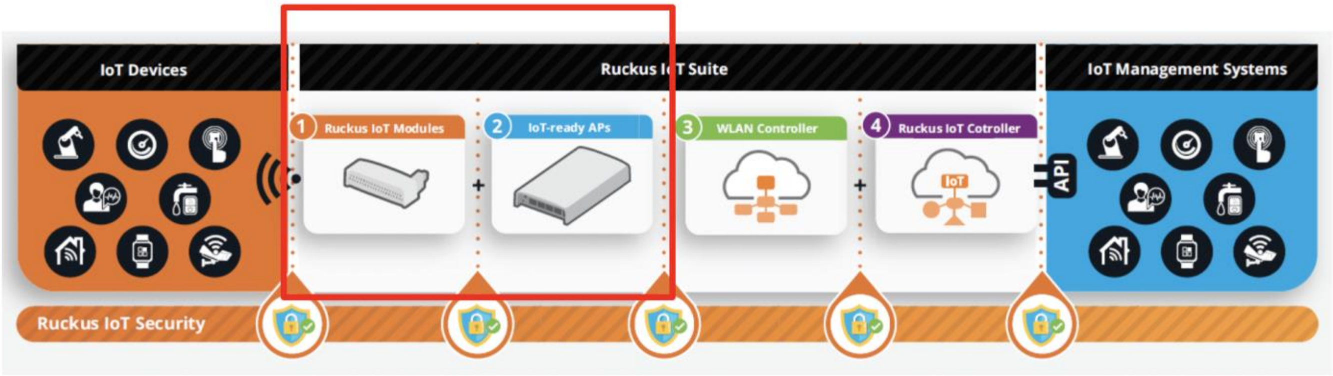

FIGURE 13: IOT MODULE TO ACCESS POINT

Note: RUCKUS 11ax (Wi-Fi6) access points natively support IoT without the need for an attached IoT Module.

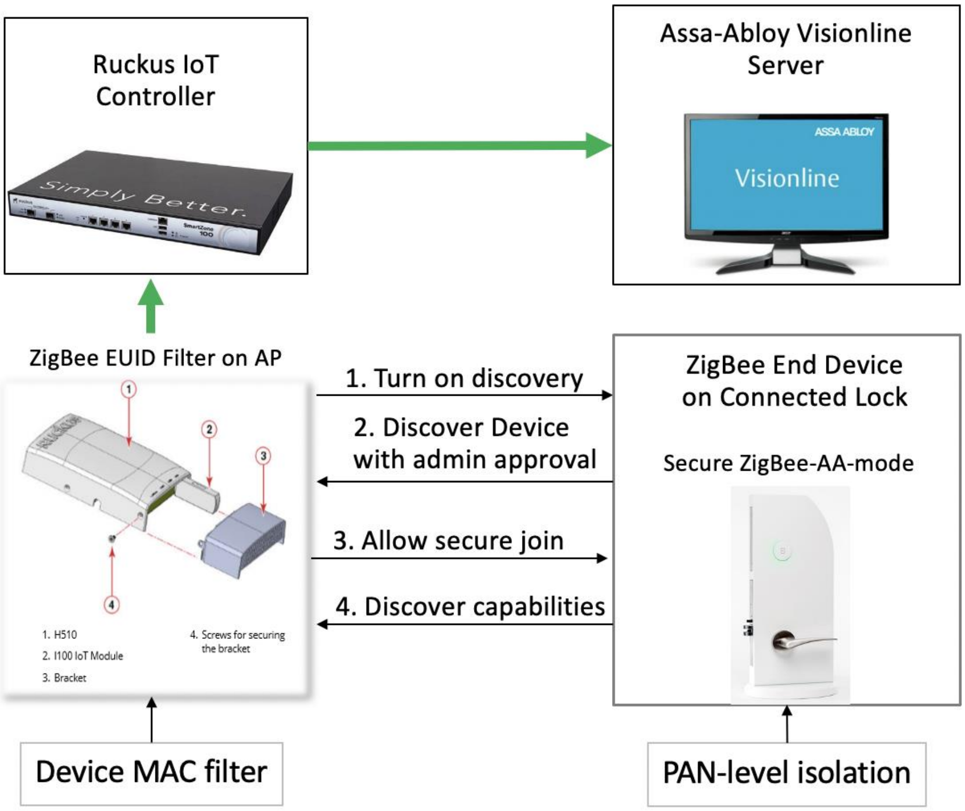

FIGURE 14: SECURE ONBOARDING

© 2020 CommScope Inc. All rights reserved.

Support for Assa Abloy Secure Mode over Zigbee

There is a special security mode for Assa-Abloy on the ZigBee 2.x and 3.0 stack. This was designed to support the Wingcard Elsafe solution for secure, low-energy, connected lock communication over the Ruckus Zigbee-AA mode. This turns off native Zigbee key management and replaces it with Assa-Abloy specific end-to-end security that is protected Assa-Abloy specific EUI64 encoded opaque messages between the locks and the Visionline server.

The RUCKUS infrastructure acts as a transparent transport. Secure MQTT is used between the AP and the RUCKUS IoT Controller and secure REST API from the RUCKUS IoT Controller to the on-premises Assa-Abloy Visionline Server.

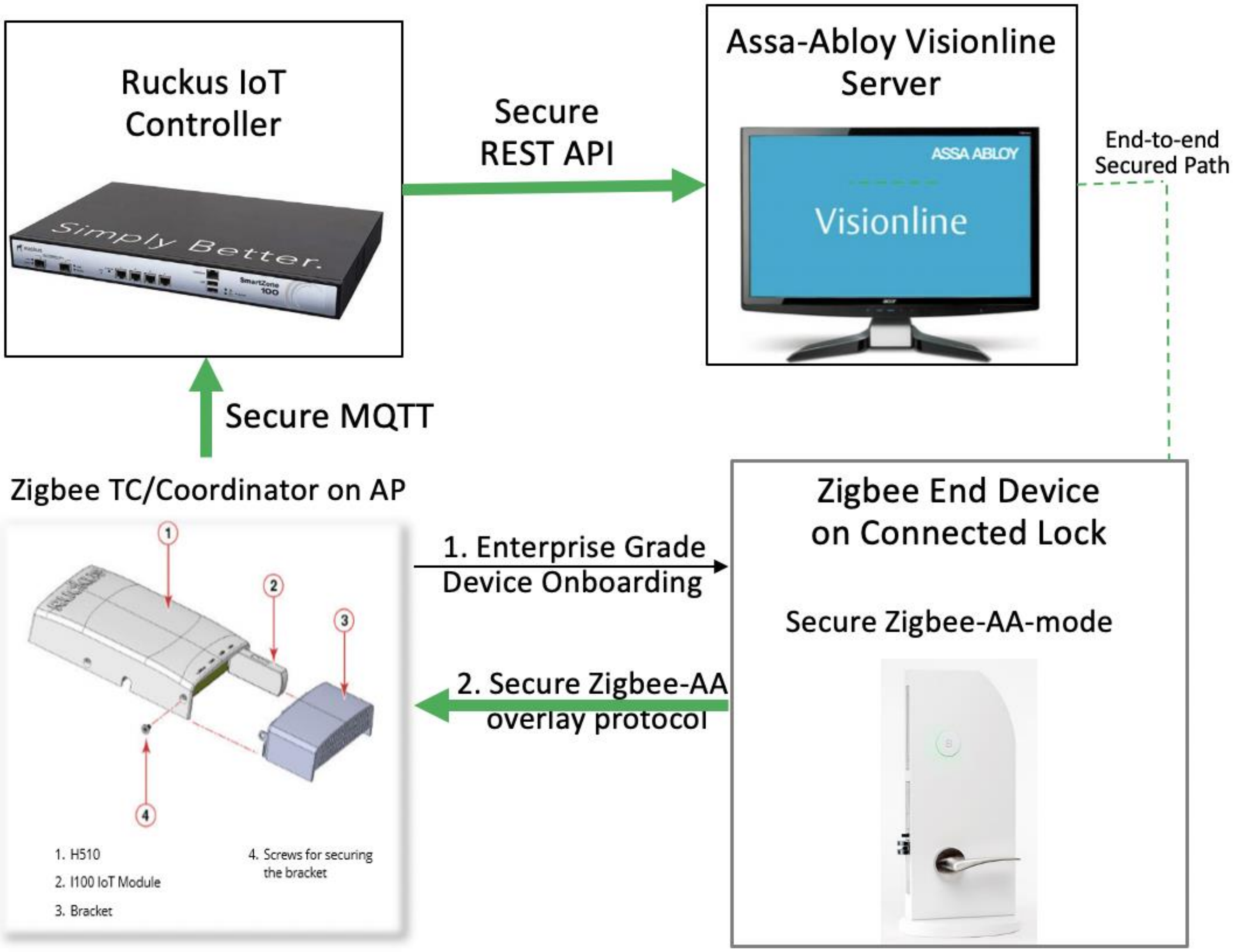
Ruckus IoT Controller
Simply Better.
SmartZone 100
Secure REST API
Assa-Abloy Visionline Server
ASSA ABLOY
Visionline
End-to-end Secured Path
Secure MQTT
Zigbee TC/Coordinator on AP
1
2
3
4
1. H510
2. I100 IoT Module
3. Bracket
4. Screws for securing the bracket
1. Enterprise Grade Device Onboarding
2. Secure Zigbee-AA overlay protocol
Zigbee End Device on Connected Lock
Secure Zigbee-AA-mode

FIGURE 15: VINGCARD SECURE ZIGBEE-AA MODE

© 2020 CommScope Inc. All rights reserved.

Access Point to IoT Controller

The RUCKUS IoT controller is a virtual machine that has north and south bound communication with all the APs or switches in the IoT network and 3rd party cloud or on-premise services. The link between the AP and IoT Controller is a secure MQTT link using TLS certificates, where the IoT controller is the server and AP is the client. TLS is the most secure industry standard cryptographic protocol to provide encrypted and private connections in a computer network.

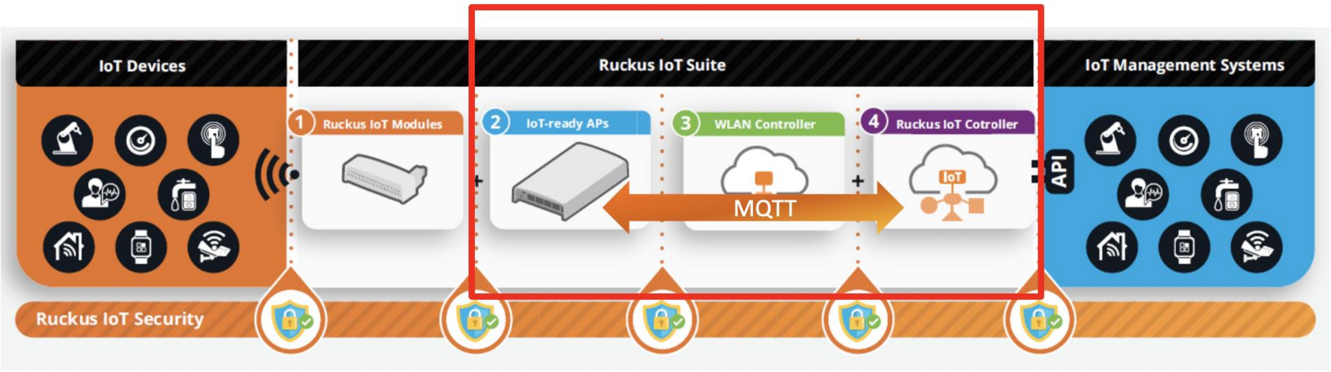

FIGURE 16: ACCESS POINT TO IOT CONTROLLER

Message integrity is provided by a secure envelope. Data sent between the RUCKUS access point and IoT Controller as encrypted MQTT over SSL with a high-security cipher suite and QoS 2. Mutual authentication of certificates using Ruckus certificate infrastructure with a Hardware Security Module (HSM). This confirms the identity of the communicating parties. The clocks on the IoT Controller and WLAN controller must be in synch with manually or with an NTP.

© 2020 CommScope Inc. All rights reserved.

Steps to secure AP to RUCKUS IoT Controller MQTTs

- MQTT client in the AP requests access to a protected resource (MQTT session)
- MQTT server presents certificate to the client
- Client verifies the server’s certificate
- If successful, client sends its certificate to the server
- Server verifies the client’s credentials
- If successful, server grants access to the protected resource requested by the client

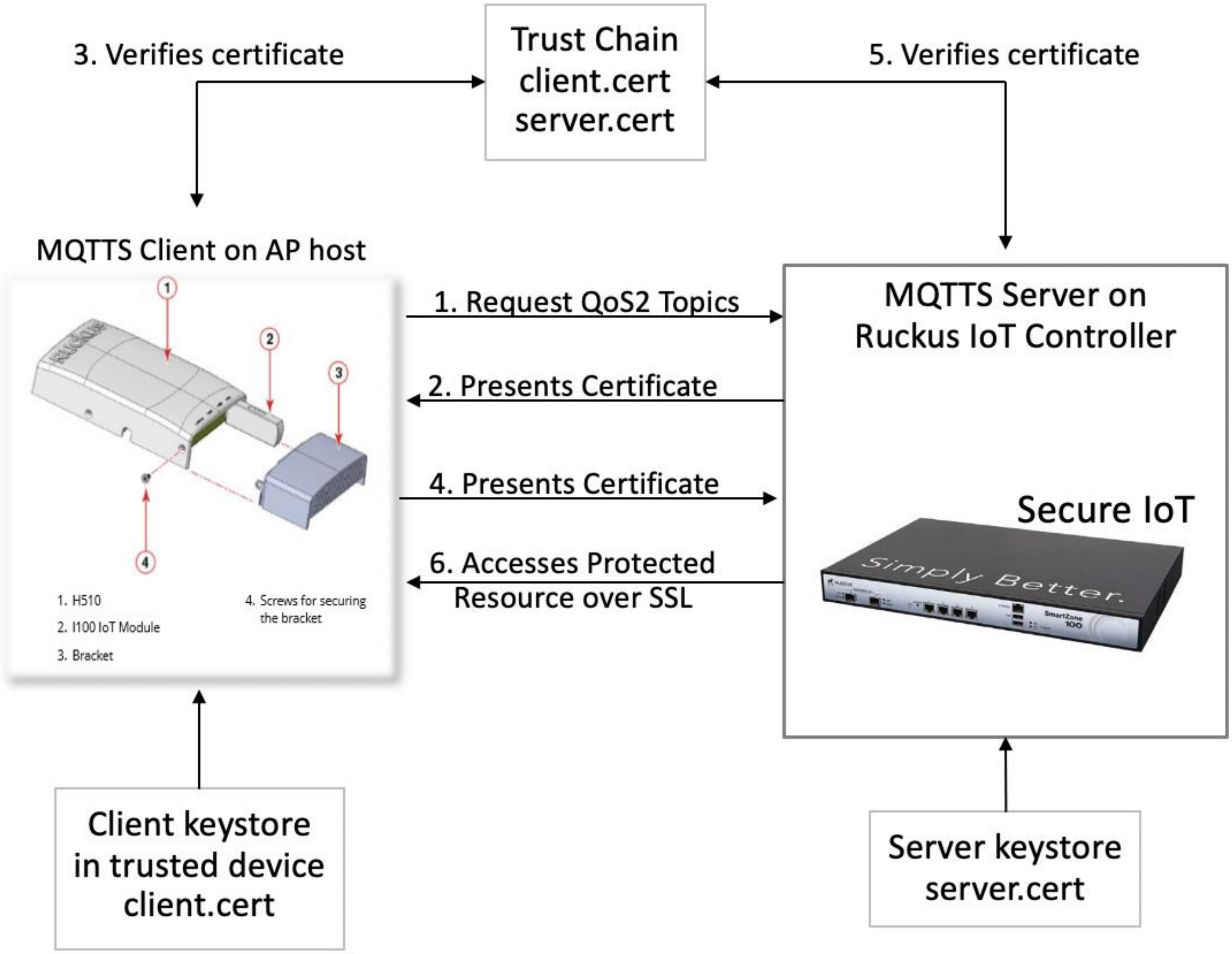

FIGURE 17: SECURE IOT CHANNEL OVER MQTT

© 2020 CommScope Inc. All rights reserved.

IoT Controller to 3rd Party Partner

Communication between the RUCKUS IoT Controller and 3rd party management systems uses authenticated HTTPS for every REST call and key rotation for a secure session management.

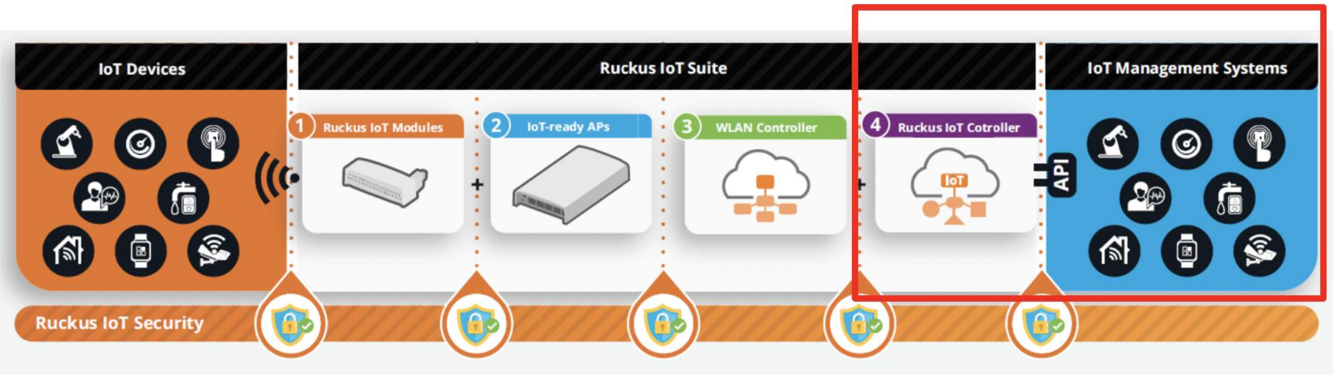

FIGURE 18: CONTROLLER TO 3RD PARTY PARTNER

Typically, the interface is REST API or MQTTS / HTTPS over TLS (SSL). Cloud services or on-premise servers from 3rd parties have varying levels of security implementation. Ruckus enforces secure authentication of all external connections using TLS/SSL. Secure authorization is ensured by using access and refresh tokens – every API call is checked. Any HTTP requests are redirected to HTTPS and there is a single pane of control for policy enforcement and visibility to all IoT APs and devices.

The database and other components in the IoT Controller are secured with their own unique credentials with no external access. Internal MQTT paths are inside a secure envelope with topics terminated inside the IoT Suite AP or IoT Controller providing protection from information leaks. All internal application ports (E.g. database, queues, etc.) are blocked from external access and access token refresh for inbound REST API calls is forced.

There is no device history stored in the IoT controller besides last known value for UI purposes with separate capability additions possible when combining the Ruckus IoT suite with other Ruckus products such as the vSZ, Cloud, and Analytics.

© 2020 CommScope Inc. All rights reserved.

IoT Network Interface

The network interface between the IoT Gateway and RUCKUS IoT Controller only uses secure MQTTS tunneling so as to minimize the surface for horizontal attacks.

VLAN Isolation

The network interface from the IoT gateways to the RUCKUS IoT Controller provides segmentation to IoT specific virtual LANs (VLANs) to further minimize horizontal attack surface. A Ruckus IoT deployment also supports simultaneous multiple VLAN groups with an offlink VLAN connecting these from the gateways to a common RUCKUS IoT Controller in larger deployments.

The IoT AP and Controller have a separate VLAN. This keeps non-IoT traffic separated (e.g. Wi-Fi traffic is on a different VLAN).

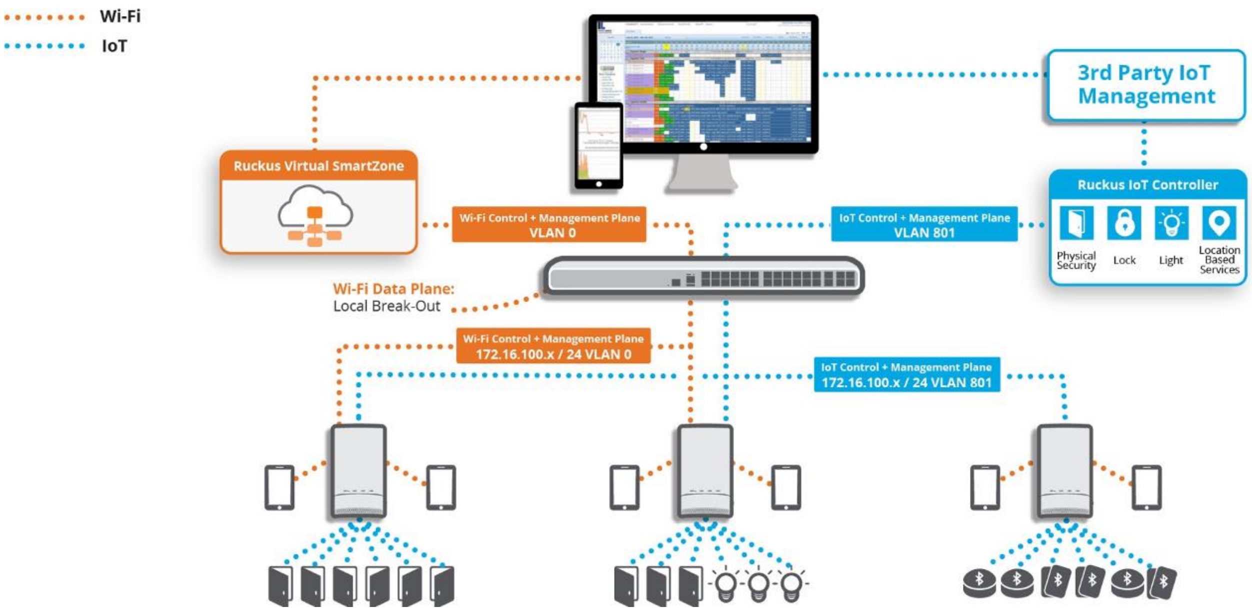
Wi-Fi
IoT
3rd Party IoT Management
Ruckus Virtual SmartZone
Ruckus IoT Controller
Physical Security
Lock
Light
Location Based Services
Wi-Fi Control + Management Plane VLAN 0
IoT Control + Management Plane VLAN 801
Wi-Fi Data Plane: Local Break-Out
Wi-Fi Control + Management Plane 172.16.100.x / 24 VLAN 0
IoT Control + Management Plane 172.16.100.x / 24 VLAN 801

FIGURE 19: NETWORK ISOLATION

IoT VLAN is a sub-option (22) of DHCP Option 43 and is designed to provide access points with a dedicated IoT VLAN. This allows other WLAN-specific interfaces and VLANs to remain independent of the IoT VLAN.

The IoT VLAN can be provisioned from DHCP, through the RUCKUS IoT Controller UI, or the AP CLI.

© 2020 CommScope Inc. All rights reserved.

Steps to Provision the IoT VLAN from DHCP

- Admin configures DHCP Option 43 sub-option 22 for IoT VLAN tag
- When the AP boots up it gets its DHCP and option 43 when defining its primary networking interface(s)
- If Sub-option 22 is present and valid, AP adds a VLAN interface, provisions address, and restarts IoT service on the new interface

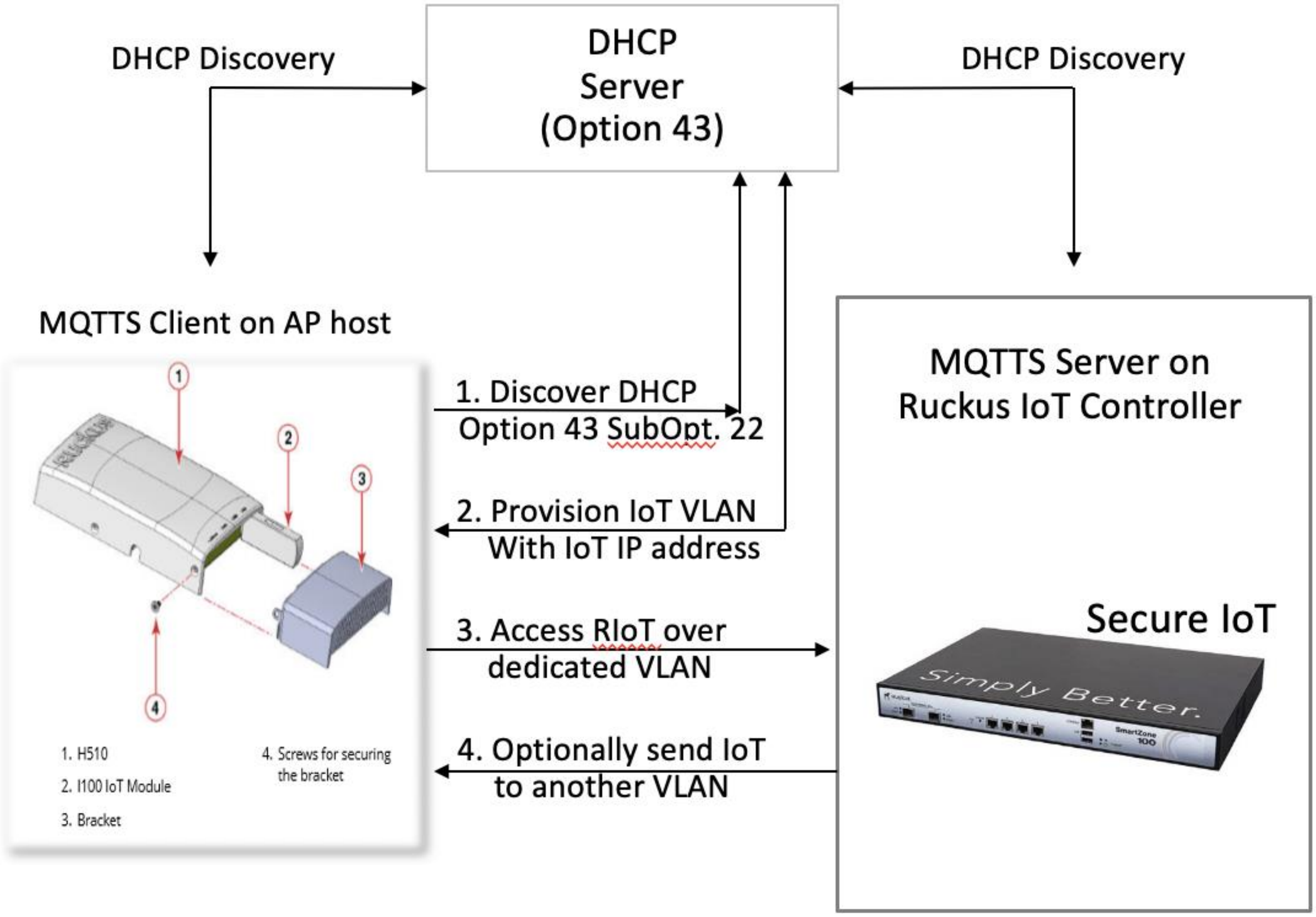
DHCP Discovery
DHCP
Server
(Option 43)
DHCP Discovery
MQTTS Client on AP host
1
2
3
4
1. H510
2. I100 IoT Module
3. Bracket
4. Screws for securing the bracket
1. Discover DHCP Option 43 SubOpt. 22
2. Provision IoT VLAN With IoT IP address
3. Access RIoT over dedicated VLAN
4. Optionally send IoT to another VLAN
MQTTS Server on Ruckus IoT Controller
Secure IoT
Simply Better.
SmartZone 100

FIGURE 20: PROVISIONING AN IOT VLAN FROM DHCP

© 2020 CommScope Inc. All rights reserved.

IoT Platform Security

The Ruckus IoT Controller uses a hardened OS which is platform- and network-pen-tested regularly.

SIRT Process

The Security Incidence Response Teams (SIRT) security processes at Ruckus continuously monitor any IoT, Wi-Fi, networking, or platform vulnerabilities found in the industry and, if necessary, update the product suites, including IoT, with security fixes and hot fixes as needed.

The RUCKUS IoT AP and WLAN controllers have been repeatedly pen-tested by core security teams over the past decade while the IoT team has focused on pen-testing the IoT Controller. The RUCKUS WLAN product lines have FIPS and Common Criteria conforming products to provide enterprise grade security.

Although the RUCKUS IoT product is newer, it is fully connected to the WLAN product security processes and there is an Incident Monitoring and Response process by cross-product-line so that SIRT also monitors IoT vulnerabilities and publishes advisories as needed.

Additionally, regular IoT penetration tests are performed and reports are uploaded to Jira. Bugs with the most critical severity-level are accepted from customer or internal team members from these penetration test reports. These are assigned to the respective sub-teams. Severity 3 and below are fixed with a lower priority unless otherwise requested by customers or Security Team.

© 2020 CommScope Inc. All rights reserved.

Pen Testing

Regular pen-testing with state-of-the-art tools is an integral part of the Ruckus product process and gives an additional layer of defense to avoid attack vectors in the product.

All IoT solution network elements regularly run through pen-testing, including:

- Network scans
  - Web App/REST app level scans
  - Full network-level pen-testing
- Platform scans
  - All platform software components are scanned
  - Special scans (E.g., database)

Highlights of scanning tools used:

- Two commercial pen-test tools: Commercial InsightVM and Nessus heavily used
- Several other scan tools used to provide maximum safety
- All exploit lists (CERT advisories, etc.) are monitored by us and Ruckus SIRT team

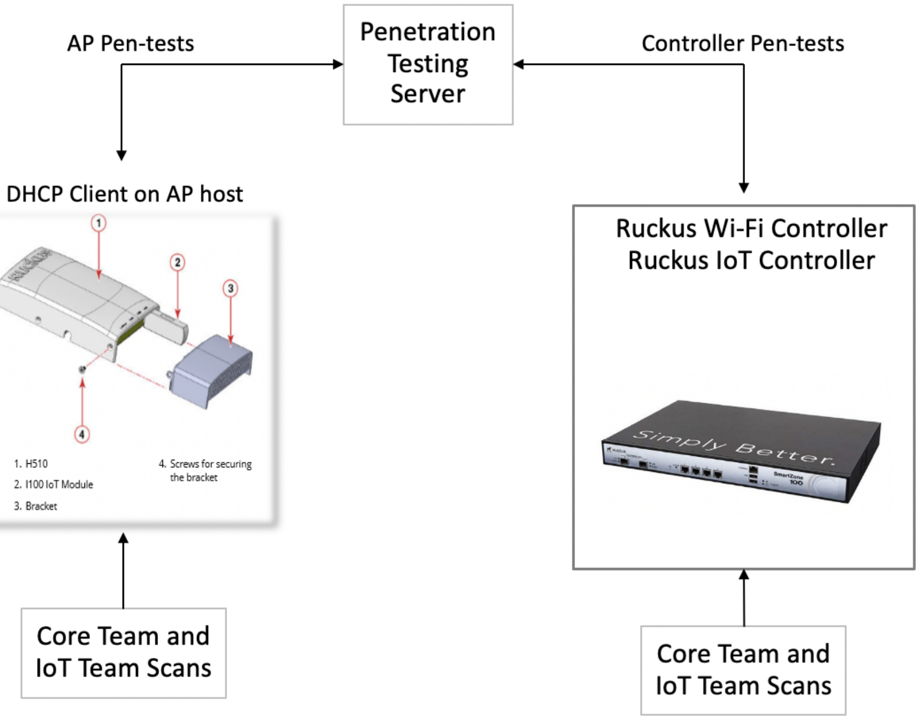

Figure 21: Routine Pen Testing Basics

© 2020 CommScope Inc. All rights reserved.

Appendix A: Message Queuing Telemetry Transport (MQTT)

MQTT is a lightweight, publish-subscribe network protocol that transports messages between devices usually over TCP/IP. MQTT was designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited.

The MQTT protocol defines two types of network entities: a message broker and a number of clients. An MQTT broker is a server that receives all messages from the clients and then routes the messages to the appropriate destination clients. An MQTT client is any device (from a micro controller up to a full-fledged server) that runs an MQTT library and connects to an MQTT broker over a network.

MQTT relies on the TCP protocol for data transmission. A variant, MQTT-SN, is used over other transports such as UDP or Bluetooth.

MQTT sends connection credentials in plain text format and does not include any measures for security or authentication. This can be provided by the underlying TCP transport using measures to protect the integrity of transferred information from interception or duplication.

The default encrypted MQTTS port is 8883. MQTT usage in the Ruckus IoT Suite has been carefully designed against MQTT information disclosure attacks.

© 2020 CommScope Inc. All rights reserved.

Ruckus solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- Ruckus Wi-Fi Access Points
- Ruckus ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

COMMSCOPE®

RUCKUS®

commscope.com

Visit our website or contact your local CommScope representative for more information.

© 2020 CommScope, Inc. All rights reserved.

Unless otherwise noted, all trademarks identified by ® or ™ are registered trademarks, respectively, of CommScope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to CommScope products or services. CommScope is committed to the highest standards of business integrity and environmental sustainability with a number of CommScope's facilities across the globe certified in accordance with international standards, including ISO9001, TL9000, ISO14001 and ISO45001. Further information regarding CommScope's commitment can be found at **www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability**.