Applying Security in 5G Service Architecture

Allen Yu
Security Strategy and Consultant
2018, 6, 22

Agenda

- 5G Services and Security
- Start Today with 5G Security
- 10 things to 5G for Secure Internet Gateway

5G User Cases

Transportation
Autonomous Vehicles
Automotive

IoT

Augmented Reality
Virtual Reality

Smart City
Traffic Management
Emergency Services

Manufacturing
Robotics

Tactile Internet

Health
Fitness & Healthcare

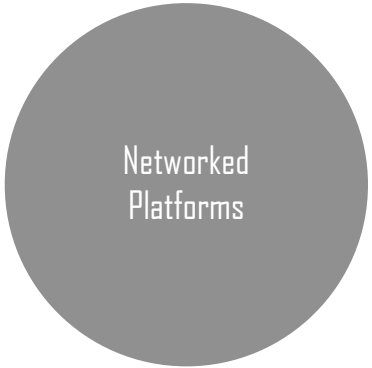
Smart Grid
Utilities

Government

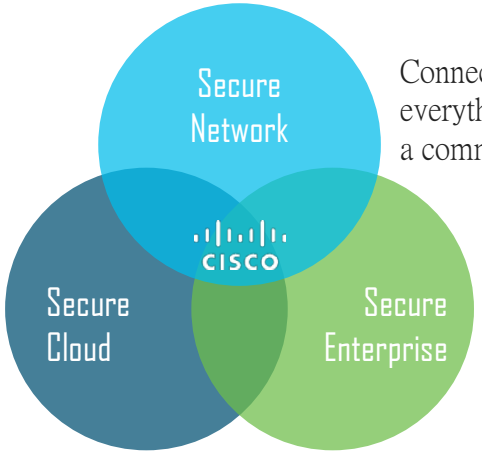
Smart Office

5G Security and Redefine Sec-Network

From: Connectivity → To: Experiences and Productivity



Scaled for subscriptions, devices and locations



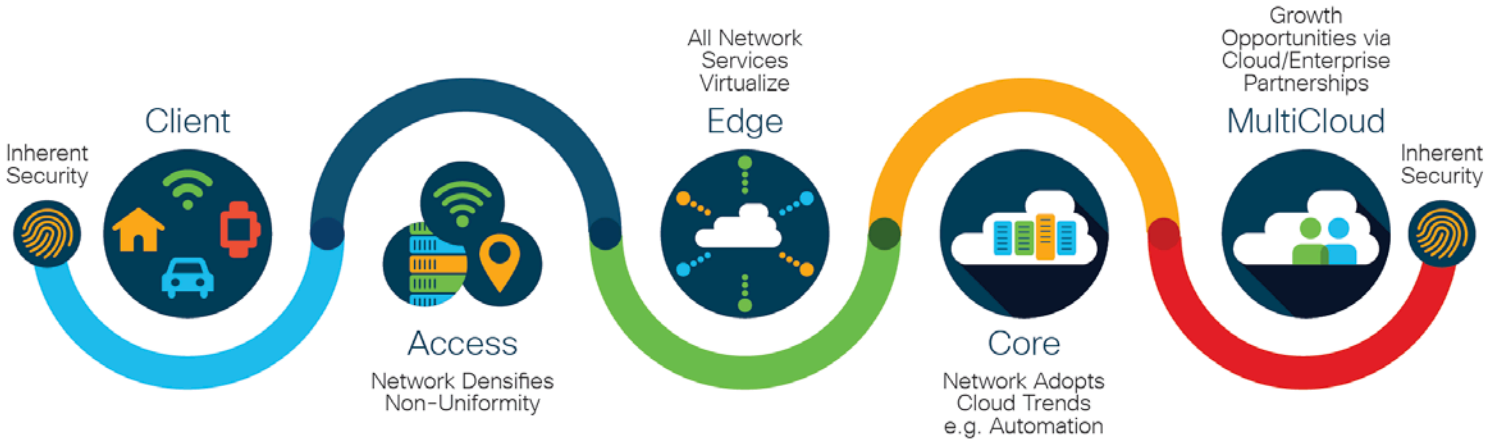
Connect everyone and everything on a common platform

Enable flexible business models

Deliver rapid time to revenue

Start Today with 5G Security

Security Innovation and Thought Leadership for 5G



5 Focus Areas for Security Innovation and Thought Leadership

- The architecture and trust boundaries detailing the threat surface (now and tomorrow) of 5G and IoT
  - Where the Enterprise meets the 5G slice
  - Where SP IT meets 5G
- Technology trends and architectures impacting how the 5G network is secured
- Visibility at Scale
- Threat and Dark Threat Analysis
- Comprehensive Threat Mitigation

5G Operational Security Requirements

Stop threats at the edge

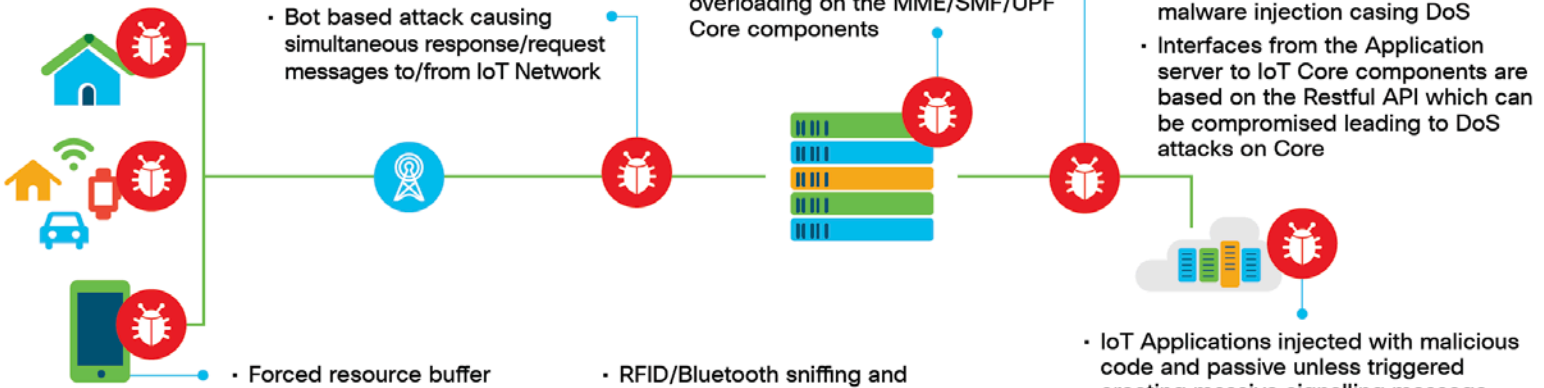
Protect users wherever they work

Control who gets onto your network

Simplify network segmentation

Find and contain problems fast

5G Architecture Threat Surface



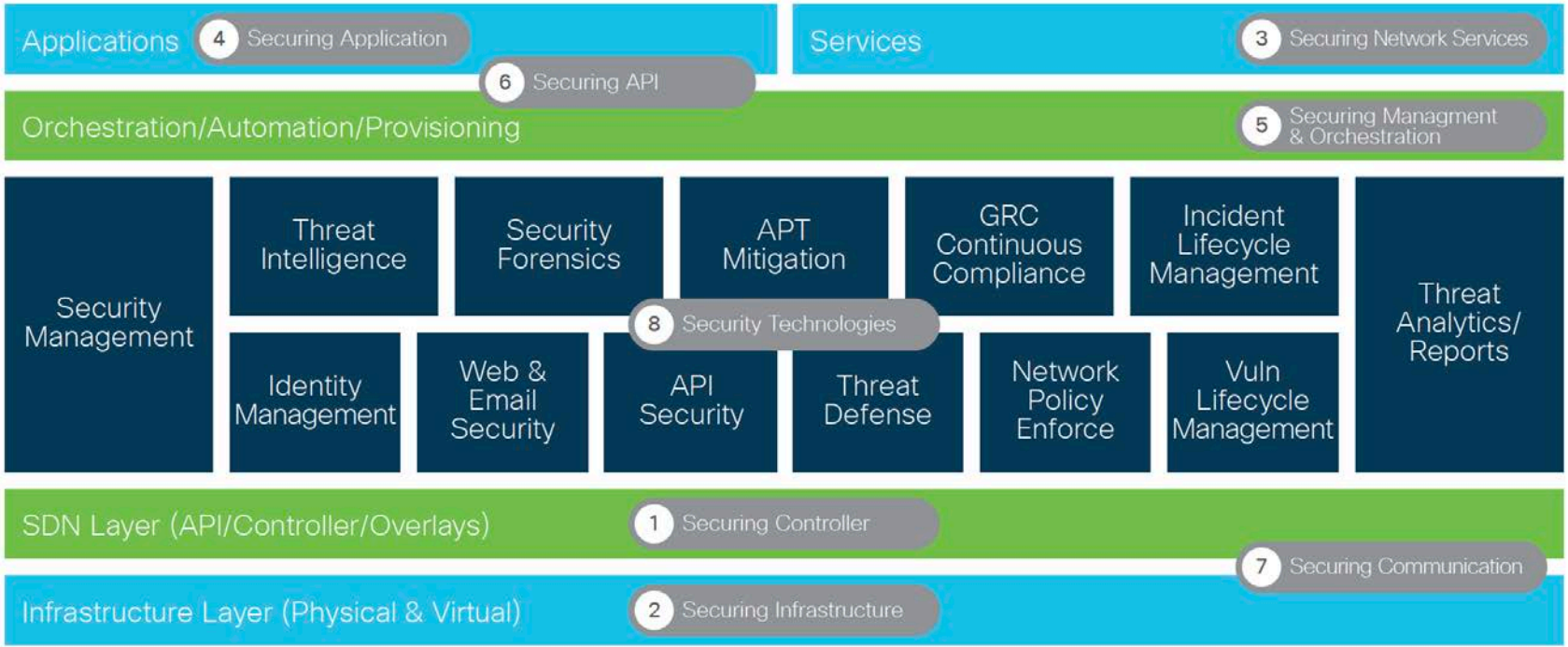
- Bot based attack causing simultaneous response/request messages to/from IoT Network
- Multiple new connection request (artificial) causing control plane resources to exhaust or cause overloading on the MME/SMF/UPF Core components
- Forced resource buffer overflows causing DoS
- Forced crash/Shutdown due to malware injection casing DoS
- Interfaces from the Application server to IoT Core components are based on the Restful API which can be compromised leading to DoS attacks on Core

- Forced resource buffer overflows causing DoS
- Forced crash/shutdown due to malware injection causing DoS
- Malicious code injection on driver which compromises HW causing DoS
- Compromised Protocol on IoT device causing malicious code injection on Primary device connected to IoT device
- Firmware OS hacking/code injection leading to compromised device

- RFID/Bluetooth sniffing and eavesdropping on the IoT device causing messages to be intercepted, modified and retransmitted with false information
- Spoofing another device on the network and collect (data silently)
- Malicious code injection leading to same device to be seen on multiple locations with separate IP address
- Multiplying the number of nodes (artificially causing increased signalling in both UL/DL

- IoT Applications injected with malicious code and passive unless triggered creating massive signalling message flows in IoT Network causing DoS
- Malicious Apps leading to Data Privacy leak

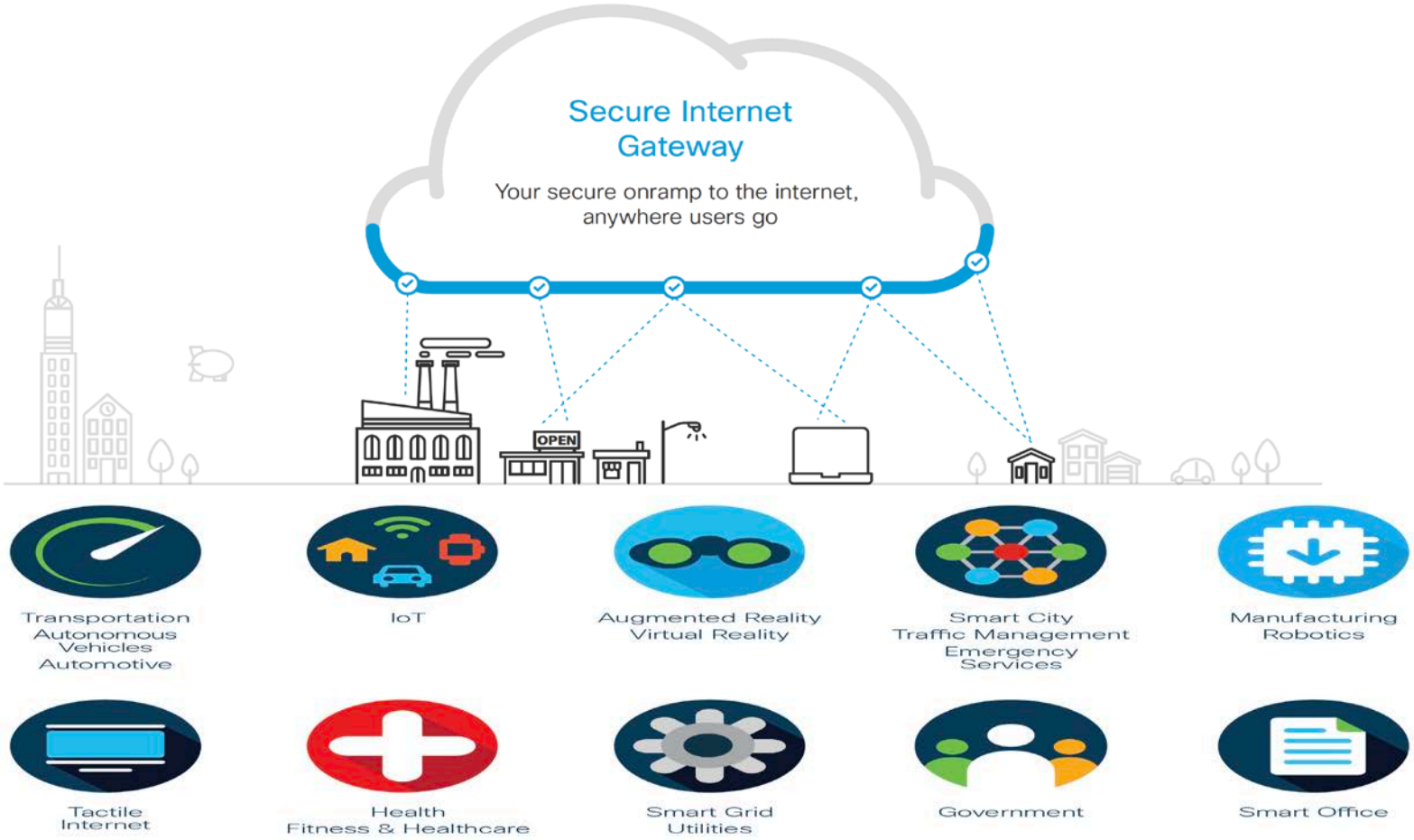
8 Step Process Used to Secure SDN/NFV



10 Things to 5G for SIA

Secure Internet Gateway

5G Secure Internet Gateway



Visibility and enforcement everywhere

1

A SIG must provide a complete view into internet activity, anywhere users are located. A SIG protects users no matter what network they connect to — even when they are off the VPN

Protects every device (managed or unmanaged) on your network — evenmobile phones and Internet of Things (IoT) devices. using integration a lightweight app extension to protect devices

Cloud-delivered Security Platform

2

The benefits and capabilities that a SIG provides can only be achieved when the platform is entirely built and delivered via the cloud. A SIG must also provide a comprehensive, yet simple way to get all traffic to the cloud platform for analysis

No hardware to deploy or software to maintain, and it can scale to meet the needs of any organization. a foundational component of how the internet works — as the main mechanism to get all internet requests to the cloud. also has tight integration with network to make it even easier. Additionally, with the app,

Protection Against Threats over All Ports and Protocols

3

With comprehensive coverage over every protocol and port, a SIG is able to protect against a broader range of attacks

By using DNS, stops threats over all ports and protocols — not just web ports 80 and 443 like a traditional web proxy. The DNS request becomes the very first point at which enforces security, by determining whether the domain or IP is legitimate or malicious.

Proxy-based Inspection of Web Traffic and Files

4

A SIG must have a cloud proxy to be able to more deeply inspect web traffic, especially for requests to risky sites. The proxy should be built using the latest technology and offer the ability to inspect files using antivirus (AV) engines and behavioral sandboxing

With the intelligent , only requests to risky domains (those hosting malicious and legitimate content) are proxied for deeper inspection — removing performance impacts felt by traditional proxies. proxy was built using a micro services architecture that automatically scales for better performance, and check files against AV engines and file reputation services

Open Platform to Integrate with Security Stack

5

A SIG must be built as an open platform that can integrate and share intelligence and event data with other systems. To better defend against today’ s threats, you need the ability to share information automatically between systems, and a SIG should be able to extend protection beyond the perimeter and help amplify investments you’ ve already made

Bidirectional API to easily integrate with existing systems including security appliances, intelligence platforms or feeds, and custom, in-house tools. Using API, you can send local intelligence into enforce it globally within minutes. You can also query our threat intelligence using the Investigate API and enrich security event data in your SIEM or other systems

Discovery and Control for SaaS Apps

6

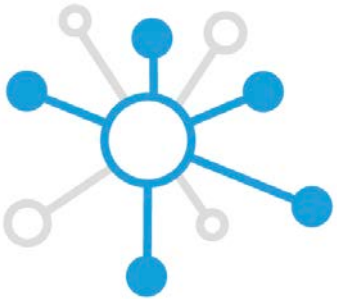
Cloud Access Security Brokers (CASB) solutions protect the usage of data and applications in the cloud. A SIG should work together with a CASB to provide more comprehensive visibility and control of SaaS apps

Provide visibility into and to control the use of sanctioned and unsanctioned SaaS apps. helps control data usage for sanctioned apps, and can uncover unsanctioned SaaS apps being used by employees and can be used to prevent access to those apps if needed. Together, protect your users, data, and infrastructure wherever they are.

Live Threat Intelligence

7

A SIG stays one step ahead of traditional security methods by uncovering attacks before they are executed. A SIG accomplishes this by using live threat intelligence derived from global internet activity that’ s analyzed in real-time, with updates enforced within minutes. Not only does a SIG enforce protection based on this intelligence, but it should also enable you to access the intelligence though a web-based console or API



Relationships between malware, URLs, domains, IPs, and networks across the internet. analyzes internet activity patterns from more than 120 billion DNS requests from 85 million users worldwide every day and automatically identifies infrastructure being staged for the next attack using a combination of statistical and machine learning models and human intelligence. Then, proactively blocks your users from these threats before a connection is ever made or a file is ever downloaded.

Easy to Deploy and Manage

8

A SIG must provide a comprehensive, yet simple way to get all traffic to the cloud platform for analysis. And it should be done without requiring complex deployments with VPNs, GRE or IPSec tunnels, and PAC files. Deployment should be simple and ongoing management should be minimal

Deploying quick and painless. It’ s as simple as changing a configuration on yournetwork to start pointing DNS to the Umbrella global network, so you can start protecting

Non-Intrusive to Users

9

A SIG keeps users protected without affecting how they get work done. Threats are blocked automatically without impacting connection speeds or device performance

Always on, always protecting, without action required from end users. They won’ texperience slow or broken connections with memory impacts on their devices. Infact, many even see performance improvements when accessing the internet.

Fast, Reliable Cloud Infrastructure

10

Not only do you need protection everywhere, but it also has to be reliable. A SIG must not only be built in the cloud, but on cloud infrastructure that provides rock solid and fast service

Exchange points around the world and has maintained 100% uptime since launching so requests are transparently sent to the fastest available with automated failover. And,has more than 500 peering partnerships with ISPs and CDNs that provide shortcuts between every network, which boosts internet connectivity.

Summary

- 5G security architecture consists of multi-layered protection with unparalleled visibility and threat mitigation
- Enhanced visibility to see more inside of the EPC and to quickly identify threats and errors
- Secures Network Slices – End-to-End
- Segmentation to reduce the attack surface and the impact of an attack
- Threat Protection to stop the breach across multiple points of the network
- World-class threat intelligence


CISCO