At-a-Glance

Scalable, intelligent, and adaptive threat-centric security for mobile service providers

Benefits

- Integrate best-in-class security services on a single platform
- Close gaps and improve efficiency with end-to-end automation
- Enhance agility with high scalability and performance across physical, virtual, and cloud infrastructures

Threat-Centric Security for Mobile Carrier Networks

Changes in Mobility Require a New Security Approach.

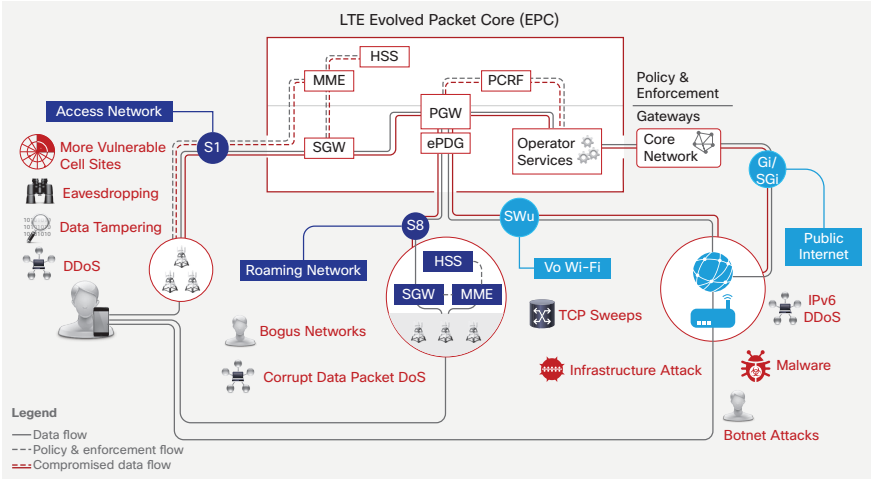
Recent advancements, like the all-IP evolved packet core, have also opened mobile networks, devices, and customers to a host of sophisticated threats. Earlier 2G and 3G networks were easier to secure.

Now, innovations including small cells, VoLTE, and VoWiFi, and the business imperative to provision and deliver services rapidly, necessitates securing critical interfaces such as:

- **Gi/SGi**, the third- and fourth-generation LTE interface to the Packet Data Network (PDN), from threats from subscribers and the public Internet
- **S1**, the LTE base station and core network interface, from the LTE backhaul traffic and access network
- **SWu**, the serving gateway to user equipment, from VoWiFi traffic to the evolved packet data gateway (ePDG)
- **S8:** the interface to other Mobile Service Provider networks

The new IP-based elements of your network are potentially vulnerable to all manner of IP-based attacks. Cyber adversaries are well organized and motivated to compromise mobile networks.

Figure 1. Highly Sophisticated and Well-Funded Threats are Putting Pressure at the Interface. If They Corrupt a Single Data Flow, They Can Access and Take Down Your Entire EPC.



Until now, a best-in-class approach to security services has been the industry standard for protecting mobile infrastructure. These manual methods, however, have proven to be insufficiently integrated and inefficient to provision. Ultimately, network performance, security, user experience, and time-to-market have been impeded.

Cisco threat-centric security for mobile service providers is available today on a physical platform and is slated for future virtual and cloud deployments. The physical hardware is carrier class and NEBS compliant.

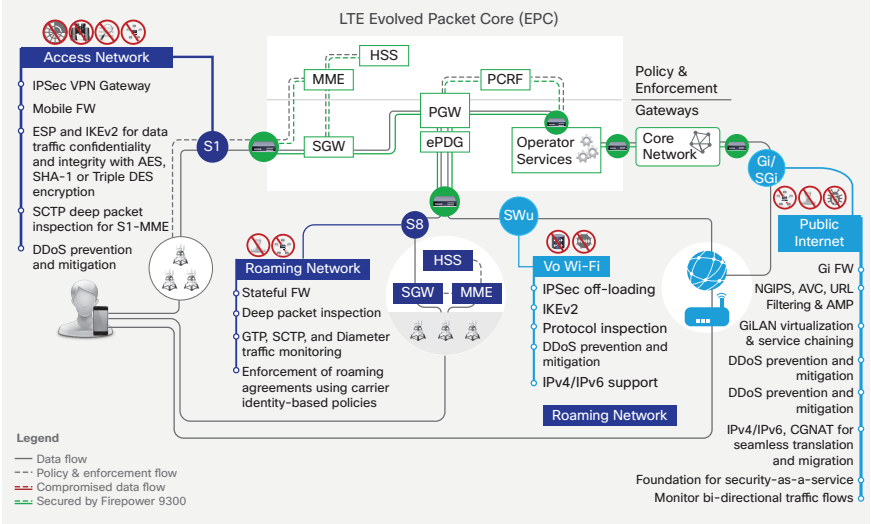
Firepower 9300

The first implementation of this new vision for mobile service providers is in hardware. The Cisco Firepower™ 9300 and Cisco Firepower 4100 series security appliances are threat-centric solutions that support superior threat defense, tight integration, end-to-end automation, and enhanced agility.

These appliances come with industry-leading next-generation firewall application control, next-generation IPS (NGIPS), and advanced malware protection (AMP) capabilities. They consolidate multiple security services on a single platform for improved threat visibility and security service orchestration, with lower latency. With Cisco's approach, service providers protect both themselves and their customers with scalable, intelligent, and adaptive threat-centric security.

A new approach to security is required to protect against these threats, one that helps protect data flows and workloads with a consistent security policy that follows workloads and flows across physical, virtualized, and cloud infrastructures. In response, Cisco delivers carrier-class advanced threat defense, plus tightly-integrated additional services, like DDoS mitigation, from our security partners.

Figure 2. Through the Strategic Placement of the Cisco Firepower Appliance, You Can Inspect Each Critical Data Flow and Secure All Physical or IP-Based Elements of Your EPC.



Adaptable Security for Any Scenario

The Cisco Firepower NGFWs are built to evolve with your network. They include a native security service stitching capability for traditional networks. They are software-defined networking (SDN) ready for orchestrating security services in next-generation networks.

The Firepower 9300 and 4100 Series include Cisco ASA stateful firewalling with:

- Comprehensive Layer 3 and 4 infrastructure protection
- Carrier-grade NAT and General Packet Radio Service (GPRS) Tunneling Protocol version 2 (GTPv2) inspection
- Stream Control Transmission Protocol (SCTP) and Diameter application inspection

The Firepower 9300 platform offers 10, 40, and 100 Gigabit Ethernet interfaces.

Next Steps

Contact your Cisco sales representative for more information. Find out more at Next-Generation Firewalls.

C45-737672-00 08/16