Cisco Security Gateway

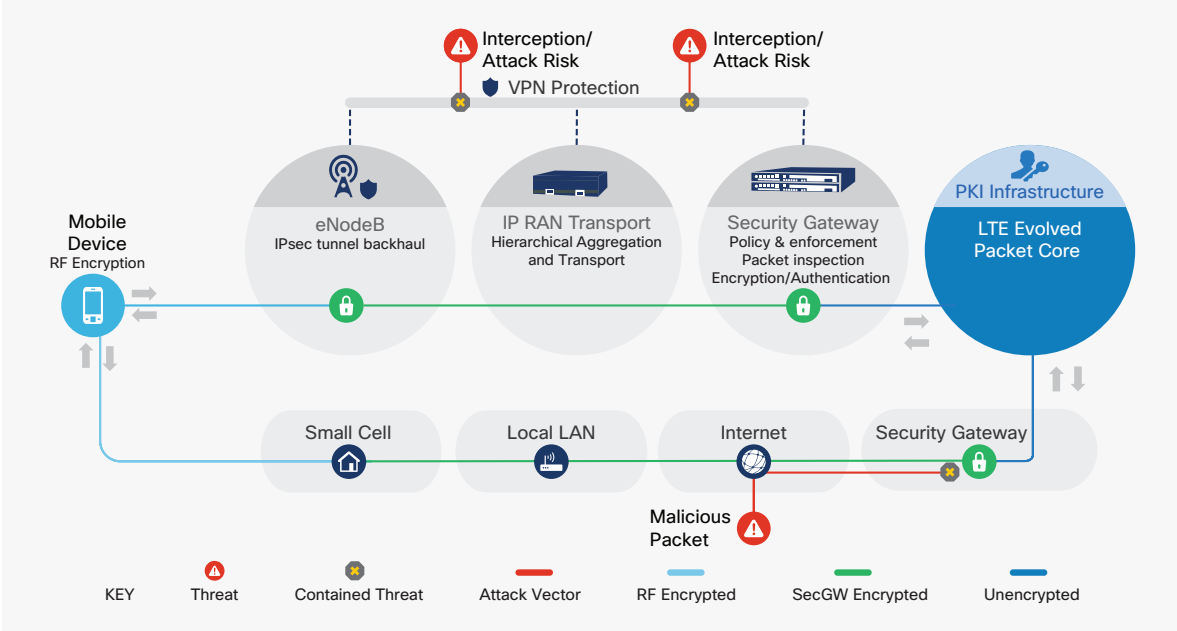
Evolving Networks Bring New Risks

With the evolution to 4G/LTE and 5G, mobile network architectures have become more IP-based. While we've seen data standards change in the past, the transition from 4G LTE to LTE-A and eventually 5G will dramatically escalate already lofty network requirements. At the same time, customers will continue to expect total geographic coverage, blazing fast transmission speeds, and absolute security when they use your network. Ubiquitous eNodeB equipment has delivered connectivity but also has significantly increased your attack surface.

In order to stay safe, your security solution must contain and block attacks that can disrupt the mobile network, provide end-to-end security and confidentiality for customers, keep up with the latest mobile technologies, and allow for management integration with existing systems to protect your investment.

On your macro network you run a risk of data interception at a few key areas. Unsecured backhaul is a primary vector for this risk, but your data has the potential to be pulled down at any stage in transmission between the mobile device and EPC.

The proliferation of cell towers presents an explosion in the number of staging points for an attack that could bring down your mobile network. To protect from this type of threat, you need a security gateway solution that authenticates and encrypts traffic from the eNodeB to protect the EPC and reduce the potential for network disruption.



Security Gateway minimizes the potential damage of interception by providing end-to-end encryption and secure IPsec tunnels. Security Gateway also makes sure that the eNodeB is authenticated against a centralized certificate authority and strengthens the perimeter between the radio access network (RAN) and the EPC.

Threats coming from cell sites are compartmentalized and contained inside your RAN network. We route this traffic through the Security Gateway for deep packet inspection and policy enforcement, effectively stopping threats in their tracks before they can attach to your infrastructure and potentially cause an outage.

What all of this means for you is that your customers and network get total, end-to-end protection from the most pressing attack and breach possibilities.

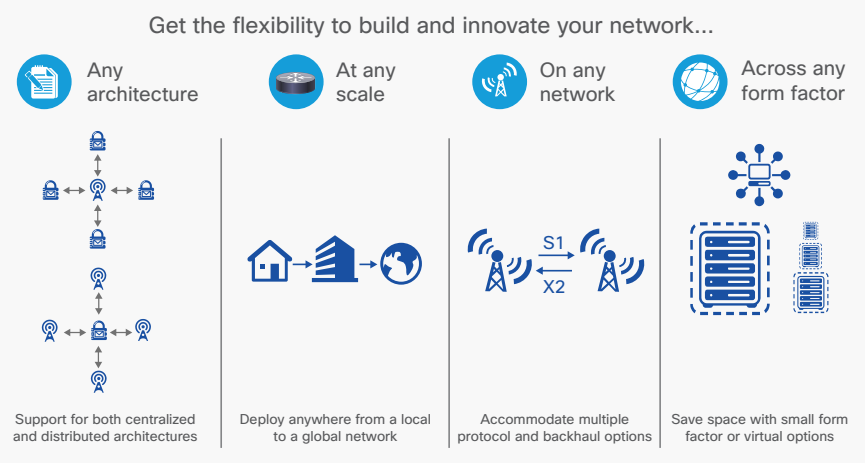
Partnership for Vodafone Hutchison Australia

Cisco and Ericsson are partnering to transform and virtualize an end-to-end telecom cloud infrastructure that includes both virtualized and physical security technologies such as the Adaptive Security Appliance and security gateway capabilities on Cisco Firepower to better prepare for new emerging services.

Cisco Security Gateway Solutions Offer

- Carrier-class performance with low latency
- Carrier-grade scalability and reliability
- Comprehensive security
- Supports multiple deployment options

When it comes to comprehensive security that adapts to changing threats and supports business agility, only Cisco delivers. Our scalable, intelligent, and adaptive threat-centric approach to security protects against the evolving threat landscape: one that enables the protections of data flows and workloads with consistent security policy in physical, virtualized, and cloud infrastructure that includes not only Cisco® carrier-class threat defense security services, but also tightly integrated additional services, like DDoS mitigation, from our security ecosystem partners.



Centralized Solutions

Cisco Security Gateway (SecGW) is based on the proven power of the Cisco Firepower Series so you get carrier-class throughput, latency, and scalability. Cisco Firepower 9300 and 4100 Series and ASAv all come with the same industry-leading carrier class firewall capabilities, so deployments are consistent either with physical on-premises hardware or virtually in the cloud.

Cisco Firepower SecGW consolidates multiple security services on a single platform for improved threat visibility and security service orchestration, including:

- ASA stateful firewalling with:
  - Comprehensive Layer 3–4 infrastructure protection
  - SCTP and diameter application inspection
  - Encryption of traffic between the eNodeB and LTE network core
- Management of security services with RESTful APIs
- DDoS mitigation
- Unique clustering technologies on Firepower; 5 Cisco Firepower 9300 chassis or up to 16 Cisco Firepower 4100 Series chassis for highly scalable performance

Distributed Solutions

The Cisco ASR 900 Series Aggregation Services Routers are the cornerstone of modern edge and carrier Ethernet networks. Programmable and scalable ASRs provide the highest single platform density, low power consumption, and virtualization capabilities. They optimize network performance and efficiency and reduce operational costs and complexity.

The Adaptive Security Virtual Appliance (ASAv) brings the power of ASA to the virtual domain. It runs the same software as the physical appliance to deliver proven security functionality. You can use it to flexibly move the SecGW across your network. You can expand, contract, or shift the location of these workloads over time and span physical and virtual infrastructures.

Cisco Security Gateway Solutions Portfolio

Firepower 9300

Firepower 4100 Series

ASR 900 Series

ASAv

End-to-End Protection

- End-to-end encryption and authentication
- Secure IPsec backhaul tunnels
- CMPv2, IKEv2

Simplified Deployment and Management

- SDN and NFV ready
- Diverse ecosystem partners
- Proven and rich UI
- Physical or virtual solutions

Reliability You Can Count On

- Grow with confidence
- Provide geo-redundancy and clustering
- Carrier-class availability

Today and Tomorrow

- Cisco paves the way for the adoption of 5G
- High-connectivity deployments with small cell and macro cell

Helpful Links

- Service Provider Security Solutions

C45-738562-00 02/17