Firepower Solutions for Mobile Service Providers
In this presentation, we will cover...

1. SP Mobile Market Trends
2. Cisco Mobile SP security solution
3. Mobile SP Security Use Cases
4. Firepower solution details and ordering
Mobile SP security
Market Trends
Mobile SPs are pursuing a host of opportunities

<table>
<thead>
<tr>
<th>Innovation</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensed Small Cells</td>
<td>Over the top (OTT) / Macro Cell connections to SP networks increase subscriber access</td>
</tr>
<tr>
<td>Voice-over (Vo) LTE</td>
<td></td>
</tr>
<tr>
<td>SP Wi-Fi</td>
<td></td>
</tr>
<tr>
<td>Vo Wi-Fi</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Innovation</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet of Everything (IoE)</td>
<td>More connected devices</td>
</tr>
<tr>
<td>Premium Mobile Broadband</td>
<td>Improved bandwidth interactions</td>
</tr>
<tr>
<td>Network as a Service</td>
<td>New line of business from excess capacity</td>
</tr>
<tr>
<td>Mobility Analytics</td>
<td>Visibility and monetization of customer usage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CAGR</th>
<th>$1.2T</th>
<th>4.9B</th>
</tr>
</thead>
<tbody>
<tr>
<td>57%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Cisco VNI Forecast
+Statista
$Gartner

*Cisco VNI Forecast

**Statista

§Gartner
Mobile SPs prioritize performance and innovation over security

**Paramount concern:** Maintain or improve subscriber experience
- Maximize performance
- Innovate services
- Scale with subscriber demand

**Security perception:** Necessary, but impedes agility, innovation and subscriber experience

**Cisco security enables performance, supports innovation, and scales to achieve business outcomes**
IP-based infrastructure brings new security challenges

- Increases vulnerabilities and expands the attack surface with the advent of LTE and IoE
- Opens SPs to experienced, sophisticated, and well-funded attackers
- Requires a new approach to Mobile SP security
### Which creates new risks

<table>
<thead>
<tr>
<th><strong>Trends</strong></th>
<th><strong>Risks</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Transition to all IP infrastructure (LTE)</td>
<td>Greater attack surface via IP connected devices</td>
</tr>
<tr>
<td>IPv4 NAT and increased IPv6 utilization</td>
<td>Complex and hard to defend network edges</td>
</tr>
<tr>
<td>Growth in microcell hotspots</td>
<td>Proliferation of less secure access points</td>
</tr>
<tr>
<td>Expanded use of stateful inline devices</td>
<td>Susceptible to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks</td>
</tr>
<tr>
<td>Virtualization of mobile network components</td>
<td>New edges and weak points</td>
</tr>
<tr>
<td>Growth of smart phones and applications</td>
<td>Greater attack surface</td>
</tr>
</tbody>
</table>
Increasing vulnerability at nearly every layer

Vulnerabilities:

- Application layer
- Transport layer
- Customer data
- Authentication, authorization, and accounting (AAA) protocols
- Data signaling gateways
- Mobile packet core
- Radio Access Network infrastructure (E-UTRAN)
Attack surface grows as networks improve

Types of Threats

- Data integrity
- Internal attacks
- DoS or DDoS
- Botnet attacks

Security solutions for 3G, LTE, and 5G
Securing network edges is critical

- Increase in connected devices and app complexity
- Growing number of IP addresses
- Migration from IPv4 to IPv6 protocol

- Subscribers increasingly access customer EPCs via other operators and untrusted networks

- Proliferation of microcells, cell stations, Evolved Node Bs (eNodeBs), or hotspots

- Subscribers using Mobile SPs networks for their own personal Wi-Fi hotspots

- Voice over Wi-Fi as a business imperative

Gi/SGi Interface
Internet

S8 Interface
Roaming

S1 Interface
OTT

SP Wi-Fi
OTT

SWu Interface
OTT

EPC

CISCO
Legacy security service chaining forces trade-offs

The standard siloed approach to security creates a cadre of network issues:

- Impeded performance
- Latency
- Varied platforms
- Inconsistent policies
- Increase CapEx / OpEx cost
- Reduced availability
Cisco SP architecture delivers security and performance

Cisco Services support Mobile SPs

Evolved Services Platform

Evolved Programmable Network

Applications

Service Broker

Orchestration Engine

Catalog of Virtual Functions

OPEN APIs

Service Profile

Compute

Storage

Network

Security

SMART SERVICE CAPABILITIES

Plan

Build

Manage
Cisco Mobile SP
Security Solution
Strategy
Consistency across physical, virtual & cloud

- Physical
- Virtual
- Cloud
Firepower 4100 Series

Introducing four new high-performance models

Performance and Density Optimization

- 10G and 40G interfaces
- Up to 60 Gbps throughput
- 1 RU form factor
- Low Latency

Multi-service Security

- Firepower Threat Defense integrated inspection for FW, NGIPS, AVC, URL, AMP
- Containerization for third-party security services

Unified Management

- Single management interface with Firepower Threat Defense
- Unified policy with inheritance
- Choice of management deployment options
Firepower 9300 Platform

High-speed, scalable security

**Benefits**
- Standards and interoperability
- Flexible Architecture

**Features**
- Template driven security
- Secure containerization for customer apps
- Restful/JSON API
- 3rd party orchestration / management

---

**Benefits**
- Integration of best-of-breed security
- Dynamic service stitching

**Features**
- ASA container
- Firepower Threat Defense container
  - NGIPS, AMP, URL, AVC
  - 3rd Party containers
  - Radware DDoS

---

**Benefits**
- Industry Leading Performance / RU
  - 600% Higher Performance
  - 30% higher port density

**Features**
- Compact, 3RU form factor
- 10G/40G I/O; 100G ready
- Terabit backplane
- Low latency, Intelligent fastpath
- NEBS ready

* Contact Cisco for services availability
Cisco transforms security service integration

---

Limited effectiveness
Increased latency
Slows network

Siloed

Data Packet

SSL Platform

DDoS Platform

WAF Platform

IPS Platform

SIEM Platform

Integrated

Data Packet

SSL Platform

DDoS

WAF

FW

NGIPS

AMP

Unified Platform

Maximum protection
Highly efficient
Scalable processing
Dynamic

---
SP Mobile Security
Use cases
Technology trends are driving use cases

- 3G-to-LTE
- IPv4-to-IPv6
- Hotspots
- Stateful devices
- Virtual
- Applications & smart phones

- Gi/SGi
- S1
- SWu
- SP Wi-Fi
- S8
- EPC
Protecting mobile SP revenue and enabling business continuity with the right protocol coverage, inspections, and performance:

- Security gateway (SecGW)
- SCTP stateful inspection
- Diameter inspection
- GTPv2 protocol for interoperator
- IPv6 capabilities
Protecting LTE backhaul traffic
Securing the S1 interface

Internet Protocol Security (IPSec) Tunnel

Firepower 9300
S1 Interface IPSec GW and FW

IPSec VPN Gateway
- Authentication between eNodeB and the packet core
- ESP and IKEv2 for data traffic confidentiality and integrity with AES, SHA-1 or Triple DES encryption
- SCTP deep packet inspection for the S1-MME control plane with the MME

Evolved Packet Core
- MME
- S-GW
- P-GW

Internet Protocol Security (IPSec) Tunnel
- Internet

eNodeB

Mobile FW
Protecting multiple interfaces
Securing Mobile SP Wi-Fi

- IPSec Tunnel
- Access Points
- Access Aggregation
- Wireless Controllers
- 3G/4G LTE Mobile Packet Core
- Internet

Firepower 9300 NAT FW
Firepower 9300 NAT FW

Stateful FW
Radius inspection
Authentication and authorization

Wireless Intrusion Detection System: DDoS prevention & mitigation (Radware), security penetration, client exclusion, rogue AP detection, etc.
Protecting against other networks
Securing the S8 Interface

Evolved Packet Core
- HSS
- MME
- S-GW
- P-GW

Firepower 9300
Roaming GW

Stateful FW
Deep packet inspection
GTP traffic monitoring
SCTP traffic monitoring
Diameter traffic monitoring
Enforcement of roaming agreements using carrier identity-based policies

Roaming Networks
Protecting against internet attacks
Securing the Gi/SGi Interface

Evolved Packet Core

S-GW

P-GW

Private IPV4 or IPV6

eNodeB

Firepower 9300
S/Gi Firewall (3G/4G/LTE)

Internet

IPv4/IPv6, CGNAT for seamless translation and migration

DDoS prevention & migration (Radware)

GiLAN virtualization & service chaining

NGIPS, AVC, URL Filtering & AMP

Gi FW

A foundation to deliver subscriber-managed security-as-a-service
Protecting the ePDG for VoWi-Fi environments

Securing the SWu interface

- IPv4/IPv6 support
- DDoS prevention & mitigation (Radware)
- Protocol inspection
- IKEv2
- IPSec off-loading

Evolved Packet Core

MME
S-GW
P-GW

Firepower 9300
SWu Firewall
Firepower solution details and ordering
Strong security for Mobile SPs

Mobile SP-centric ASA feature set:
- Comprehensive Layer 3-4 stateful infrastructure protection
- Carrier Grade NAT and GTPv2 inspection in ASA 9.5(1)
  - SCTP and Diameter application inspection in ASA 9.5(2) and beyond

Carrier-grade platform with 10GE/40GE and 100GE* interfaces

Service stitching for Cisco and 3rd party security applications*

Elastic stateful security scalability with clustering

High-performance platform for NGIPS

* Contact Cisco for services availability
Cisco NGFW Platforms

Firepower 4100 Series and Firepower 9300

Firepower Services on ASA 5500-X

Firepower Services on ASA 5585-X

All* Managed by Firepower Management Center

*5585-X management avail 2H ’16 (pre-commit date)
## Firewall & IPSEC Performance

<table>
<thead>
<tr>
<th></th>
<th>4110</th>
<th>4120</th>
<th>4140</th>
<th>SM-24</th>
<th>SM-36</th>
<th>SM-36x3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stateful inspection firewall throughput (maximum)</strong></td>
<td>20G</td>
<td>40G</td>
<td>60G</td>
<td>75G</td>
<td>80G</td>
<td>225G</td>
</tr>
<tr>
<td><strong>Stateful inspection firewall throughput (multiprotocol)</strong></td>
<td>10G</td>
<td>20G</td>
<td>30G</td>
<td>50G</td>
<td>60G</td>
<td>100G</td>
</tr>
<tr>
<td><strong>Concurrent firewall connections</strong></td>
<td>10M</td>
<td>15M</td>
<td>25M</td>
<td>55M</td>
<td>60M</td>
<td>70M</td>
</tr>
<tr>
<td><strong>New connections per second</strong></td>
<td>150K</td>
<td>250K</td>
<td>350K</td>
<td>0.6M</td>
<td>0.9M</td>
<td>2.5M</td>
</tr>
<tr>
<td><strong>Latency (UDP 64b, us)</strong></td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
<td>3.5</td>
</tr>
<tr>
<td><strong>IPSec 3DES/AES VPN Throughput – 450B Packets</strong></td>
<td>8G</td>
<td>10G</td>
<td>14G</td>
<td>15G</td>
<td>18G</td>
<td>54G*</td>
</tr>
</tbody>
</table>

*Using IPSEC Clustering (roadmapped)
9300 Pricing options to meet every Mobile SP’s needs

<table>
<thead>
<tr>
<th>Common Hardware</th>
<th>Optional Modules</th>
<th>Software Licenses</th>
<th>Subscription and Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Chassis(1)</td>
<td>• Security Modules(2)</td>
<td>• ASA Smart Licenses</td>
<td>• SMARTnet</td>
</tr>
<tr>
<td>• Supervisor(1)</td>
<td>• SM24</td>
<td>• ASA Standard</td>
<td>• Additional third party services*</td>
</tr>
<tr>
<td>• Fan(4)</td>
<td>• SM36</td>
<td>• Encryption</td>
<td></td>
</tr>
<tr>
<td>• Power Supply(2)</td>
<td>• Network Modules(2)</td>
<td>• 10 Sec. Contexts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 8x10G</td>
<td>• Radware Defense Pro DDoS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4x40G</td>
<td>• Unified image with NGFW, NGIPS, AMP*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1x100G*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Contact Cisco for availability
CISCO	TOMORROW starts here.
Appendix
**Firepower 9300 is the vanguard for a new platform-based security architecture**

<table>
<thead>
<tr>
<th>Management</th>
<th>Common Security Policy and Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Services and Applications</td>
<td>Cisco Security Applications</td>
</tr>
<tr>
<td>Security Services Platform</td>
<td></td>
</tr>
<tr>
<td>Infrastructure Element Layer</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Appliance</th>
<th>Virtual</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management APIs</td>
<td>Cisco ONE APIs</td>
<td>Platform APIs</td>
</tr>
<tr>
<td>Cloud Intelligence APIs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Cisco Networking Operating Systems (Enterprise, Data Center, Service Provider)**

- **Device API:** OnePK™, OpenFlow, CLI
- **ASIC Data Plane**
- **Route–Switch–Compute**
- **Software Data Plane**
The hardware supports carrier-grade performance*

<table>
<thead>
<tr>
<th></th>
<th>SM-36 (&quot;Extreme&quot;)</th>
<th>1 Chassis (3 clustered SM-36)</th>
<th>5 Chassis (15 clustered SM-36)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max FW Perf</td>
<td>80Gbps</td>
<td>240Gbps</td>
<td>1 Tbps</td>
</tr>
<tr>
<td>TCP FW Perf</td>
<td>60Gbps</td>
<td>145Gbps</td>
<td>725Gbps</td>
</tr>
<tr>
<td>Max VPN Perf</td>
<td>20Gbps (TBD)</td>
<td>60Gbps (TBD)</td>
<td>200+ Gbps (TBD)</td>
</tr>
<tr>
<td>Max Sessions</td>
<td>30M (60M future)</td>
<td>55M</td>
<td>225M</td>
</tr>
<tr>
<td>Max CPS</td>
<td>800K</td>
<td>1.2M</td>
<td>6M</td>
</tr>
<tr>
<td>10GE Ports (min/max)</td>
<td>N/A</td>
<td>8/24</td>
<td>40/120</td>
</tr>
<tr>
<td>40G Ports (min/max)</td>
<td>N/A</td>
<td>0/8</td>
<td>0/40</td>
</tr>
<tr>
<td>100G Ports (min/max)</td>
<td>N/A</td>
<td>0/4</td>
<td>0/20</td>
</tr>
</tbody>
</table>

*Performance numbers subject to change
More is needed from Mobile SP security solutions

Security solutions must address the following requirements:

- Transition to LTE and IP-based mobility
- LTE coexisting and communicating with 3GPP architecture (including seamless hand-off of UE between generations of architecture)
- Growth in number, type, and complexity of network-connected devices
- Rate of application growth and subsequent network traffic
- Future market changes which may impact bandwidth, latency, or device compatibility
- Long-term scalability in forwarding performance vectors such as:
  - Session capacitance and number of concurrent sessions
  - Effective throughput
  - Low latency
  - Reliable operation
Firepower 9300 delivers performance- and innovation-enabling security

Integrated security
- Best-of-breed security = Cisco + 3\textsuperscript{rd} party
- Security services on a consolidated platform
- Visibility and correlation across the EPC and every interface

End-to-end automation
- Dynamic service stitching
- Consistent security policies
- Restful APIs and 3\textsuperscript{rd} party tool integration

Enhanced agility
- Scales with subscriber demands
- Enables high-speed mobile network performance
- Dynamic provisioning across physical, virtual, and cloud