Secure Wi-Fi Offload for Untrusted Networks: Cisco ePDG Evolved Packet Data Gateway

Mobile subscribers want access to the Internet at home, work, hotspots, and everywhere in between. They also expect the same quality of experience and access to the same services regardless of access type. At the same time, we are in the midst of a mobile data surge that is placing strains on macro radio resources. These are some of the factors promoting expanded service offerings over multiple new unsecure, untrusted access networks, such as broadband DSL, fiber to the home, high-density events, or cable broadband networks, using technologies such as Wi-Fi. How do you cost-effectively and securely deliver the same intelligent services over untrusted networks that your customers enjoy today?

The Cisco® ePDG Evolved Packet Data Gateway, one component of Cisco's Small Cell Gateway, provides subscribers easy access as they transparently roam between external trusted networks and untrusted networks. The solution offers the highest possible level of security, market-leading IP Security/Internet Key Exchange Version 2 (IPsec/IKEv2) tunnel performance, integration of multiple network functions into a single platform for the lowest possible total cost of ownership, real-time integrated intelligence with policy enforcement, and voice-grade reliability. Cisco ePDG is tightly integrated into Cisco's Evolved Packet Core (EPC) solution, using the same hardware platforms (Cisco ASR 5000 and ASR 5500) and software as our existing functions, such as Cisco Packet Data Network (PDN) Gateway (PGW), Cisco Serving Gateway (SGW), Home Agent (HA), and Cisco high Rate Packet Data (HRPD) Serving Gateway (HSGW).

Cisco ePDG is a crucial component of a comprehensive solution that allows for integration of access of traffic that does not meet 3rd Generation Partnership Project (3GPP) standards into EPC, including a client as well as the access policy control framework. The access policy control framework is a very important element, providing you with the means to grant the user quality of experience while maintaining control over mobile devices. This framework extends the 3GPP-defined policy solution and provides exceptional Cisco value additions that allow optimal access and network selection as well as enhanced quality of service (QoS).

By using the same software found in Cisco's deployed EPC solution, you can provide the same service capabilities and consistency on the Wi-Fi network as is available on the macro network. This includes consistent QoS provided over the Wi-Fi network, supporting real-time low-latency applications, such as voice and video, with optimal user quality. The solution also addresses challenges such as mobile billing for Wi-Fi traffic as well as Lawful Intercept.

Cisco ePDG terminates and manages subscriber-initiated IPsec/IKEv2 tunnels. The IPsec tunnels are used to perform secure transfers of authentication information and subscriber data over the untrusted interfaces and backhauls. In addition, Cisco ePDG performs the following functions:

- Authentication and authorization of the subscriber equipment and data

- Implementing the S2b interface (currently based on Proxy Mobile IP v6 [PMIPv6], with GPRS Tunneling Protocol [GTP] on the roadmap) toward PGW to anchor the user session there
- Conveying assigned IP address (IPv4, IPV6, or IPv4v6) to the device

Cisco ePDG can be combined with Cisco PGW, SGW, or any other EPC function, offering the flexibility of a single chassis configuration.

The combined Cisco ePDG solution is also able to deliver real-time integrated subscriber, service, and application intelligence with QoS enforcement, firewall, NAT Travel and denial-of service (DoS) protection through Cisco In-Line Services. Uniting these functions in a single chassis also provides easy support for interaccess handovers that would otherwise be difficult to achieve.

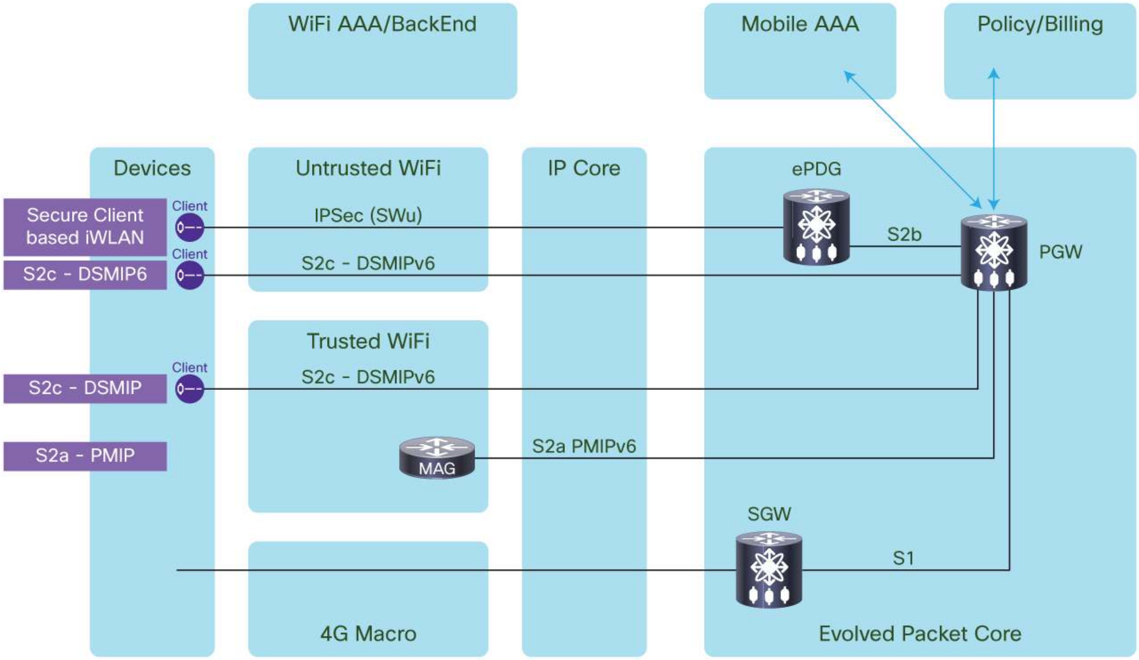
Target Architecture: Wi-Fi and 4G Integration

Figure 1 provides Cisco's view on supporting secure managed Wi-Fi through trusted and untrusted non-3GPP and 3GPP access, conformant to the methods specified in 3GPP TS 23.402. Cisco offers a complete, flexible, and standards-compliant solution for integration into the Evolved Packet Core from untrusted, non-3GPP access including Wi-Fi. Cisco's untrusted access solution is centered on the ePDG that follows the relevant sections of 3GPP 23.402 specifications while providing unique Cisco value additions.

Cisco ePDG supports the following respective logical interfaces compliant to relevant 3GPP specifications:

- SWu: logical interface toward user equipment (UE)
- SWn: interface toward non-3GPP network (Wi-Fi in this case)
- SWm: interface toward 3GPP AAA server
- S2b: interface toward PGW
- S2c: interface from untrusted access (future)

Figure 1. Cisco's Managed Wi-Fi EPC Architecture



Cisco ePDG Features and Benefits

Cisco ePDG is a software application on the Cisco ASR 5000 and ASR 5500, which are the same platforms that support other fourth-generation (4G) and third-generation (3G) nodes in the following:

- EPC: Mobility Management Entity (MME), Cisco SGW, and Cisco PGW
- Universal Mobile Telecommunications System (UMTS): Cisco Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN)
- Code Division Multiple Access (CDMA): Cisco Packet Data Serving Node (PDSN) and Home Agent (HA)

The Cisco ePDG software application is built on StarOS, the same software used for all other applications supported on the Cisco ASR 5000 and ASR 5500. This provides a high degree of flexibility for deployment plus a single hardware and software platform for ePDG, PGW, SGSN, GGSN, HA, HSGW, and PDSN. This flexibility allows Cisco ePDG to be deployed as a standalone chassis or co-located with any of the nodes provided by Cisco. For example, a single chassis can support an ePDG + PGW combination node or ePDG + PGW + SGW + MME. Note that the Cisco ASR 5000 can also be deployed as PDG/Tunnel Termination Gateway (TTG) and as Packet Data Interworking Function (PDIF). A vast set of services and capabilities are available on Cisco ePDG, delivering outstanding value. In addition, the same in-line services provided for other applications can optionally be enabled through Cisco ePDG.

This flexibility and service consistency allows Cisco to provide the same level of QoS over Wi-Fi networks as over macro networks. For example, voice traffic can be offloaded to the Wi-Fi network, providing a consistent voice over Long-Term Evolution (LTE) experience.

In addition, by using the Cisco ASR 5000 or ASR 5500 platforms, you will obtain the same level of redundancy, survivability, and availability for Wi-Fi services as for macro services. This includes both card -level and geographic redundancy.

Cisco ePDG supports IPSec/IKE v2 tunnel termination per RFC 4306, including: multiple child SA support; Network Address Translation (NAT) Traversal (RFC 3947), NAT Keepalive, and access control list (ACL); configurable dead peer detection (RFC 3706) timer support; Diffie-Hellman Groups 1, 2, 5, 14; and Denial of Service (DoS) protection, including thresholds for control plane attacks. For tunnel authentication and authorization, Cisco ePDG supports Extensible Authentication Protocol (EAP) and Key Agreement (AKA) authentication methods as mandated by 3GPP. The following encryption and authentication algorithms are supported:

- HMAC-MD5-96 (RFC 2403) NULL Encryption (RFC 2410)
- HMAC-SHA1-96 (RFC 2404)
- AES-128-CBC (RFC 3602)
- DES-CBC (RFC 2405)
- AES-256-CBC
- 3DES-CBC (RFC 2451)
- PRF_AES-128-XCBC

For UE-initiated connectivity, Cisco ePDG supports connectivity to more than a single PDN. Cisco ePDG supports UE connectivity to multiple access point names (APNs). The ePDG allows the UE to establish an SWu tunnel for each APN. The capability to support connection to multiple PDNs for a single APN is on the ePDG roadmap.

Untrusted Non-3GPP Access Networks

In the case of untrusted access networks, Cisco's ePDG supports the S2c interface, which provides a local anchor point to the user. From the deployment perspective, the Cisco ePDG can be deployed in a distributed configuration, hence providing a local network attachment point. The Cisco ePDG also supports Mobile Access Gateway (MAG) according to the PMIPv6 specification, RFC 5213 [8], and 3GPP TS 29.275 to support s2b interface toward PGW. Cisco also has plans to add GTP support to the ePDG in the future.

For IP address allocation, Cisco ePDG supports IPv4 and IPv6 addresses. The addresses for the end subscriber are allocated on the PGW and the Cisco ePDG transports these addresses to the end user. All existing address allocation methods supported on the PGW are also supported in this scenario. The address allocated by the PGW is used by the UE to gain connectivity to external PDNs.

Trusted Non-3GPP Access Networks

If you decide to also deploy Wi-Fi hotspots and hotzones in the mode of Trusted Wi-Fi infrastructure, consistent with the TS 23.402 model, Cisco's solution supports the S2a interface for trusted networks. In this context, the Cisco ASR 5000 can be deployed as Proxy-MIP Local Mobility Anchor (LMA), in conjunction with the PGW, which remains the subscriber's global anchor.

Associated with the Wi-Fi access network, the Cisco ASR 1000 can be deployed as a MAG, providing the function of local anchor point, and supporting the S2a interface towards the PGW on the Cisco ASR 5000.

Handover

For handover between non-3GPP and 3GPP access and the converse, the Cisco ePDG supports transparent handovers between 3GPP access and trusted and untrusted non-3GPP access or 3GPP access. The Cisco ePDG handover is supported regardless of whether the network uses PMIP-based S5 or GTP-based S5. Cisco EPC equipment supports interaccess handover at the network level. When Wi-Fi to LTE handover occurs, the session remains anchored on the same PGW and hence the session, including its previously allocated IP address, remains the same. This allows the device to retain the same IP address on interaccess handover.

Policy Control and Quality of Experience

Cisco considers policy control a very important aspect of any Wi-Fi offload solution. Therefore, in addition to the Policy and Charging Rules Function (PCRF) and policies applied at the network, Cisco is developing a solution based on Access Network Discovery and Selection Function (ANDSF), applying policies directly to the UE. These policies will control a device's access network selection and SSID selection, and will apply traffic routing policies, thus supporting a large number of use cases. For example, ANDSF allows the intelligent selection of LTE or Wi-Fi per application such as voice.

The adoption and success of Wi-Fi offload solutions to a large degree depends on the end-user experience that the solution delivers. End users will seek to preserve the quality of experience regardless of the access type. Quality of experience is typically defined as ease of connectivity, transparent authentication, and transparent services, while preserving the security of the macro cellular network. An essential component of the solution supporting the user's quality of experience is an interworking WLAN (iWLAN) client with the following requirements:

- No user action required to select access
- Transparent user authentication when attaching to different access types

- Policy-controlled access selection
- Operator control over traffic routing
- Session preservation on mobility
- New services enablement

Cisco's client strategy includes working with partners as well as delivering its own solution, starting with basic integration of Wi-Fi traffic into EPC with the ability to add more advanced functions such as policy control over time. Once established, the client footprint can be used as a delivery vehicle for additional services that require an end-to-end system.

Summary

In summary, Cisco ePDG is part of the complete Cisco packet core offering, as well as broader comprehensive Wi-Fi solutions that include access policy controls, treating Wi-Fi as an alternative access type while preserving end user experience, and providing significant value to mobile operators.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-707739-00 06/12