SECURING ULTRA-BROADBAND MOBILE ACCESS

DEPLOYING THE ALCATEL-LUCENT SECURITY GATEWAY TO ADDRESS THE CHALLENGES OF A FLATTER IP NETWORK ARCHITECTURE

APPLICATION NOTE

Alcatel·Lucent

ABSTRACT

Traffic volumes are increasing as are the number and type of radio access sites that operators need to support (such as macro cell, small cell, carrier Wi-Fi®). Today's flatter IP-based network architecture and the multitude of radio access sites could put the core network at risk. To mitigate this danger, service providers need to implement a security gateway at the edge of the network.

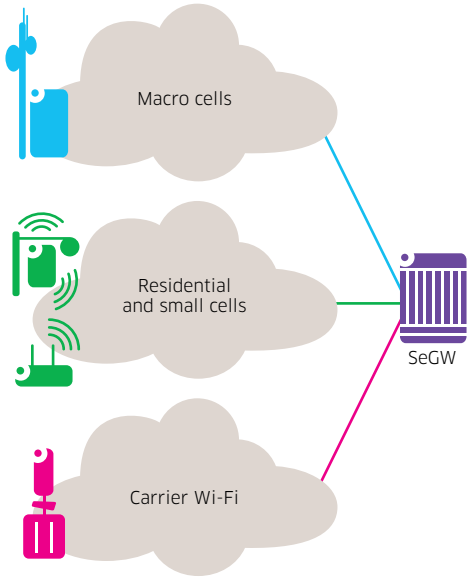
To minimize CAPEX and OPEX, Alcatel-Lucent believes the best solution is to use a common platform to act as the security gateway for all mobile technologies. The Alcatel-Lucent Security Gateway (SeGW) is implemented on the Alcatel-Lucent 7750 Service Router and 7450 Ethernet Service Switch. It inherits all the features and benefits of those well-established platforms, including high availability, and provides comprehensive, flexible security gateway features. The SeGW can be used in centralized and decentralized deployments, integrates seamlessly with third-party vendor equipment, and provides market-leading capacity to cope with the ever-increasing traffic volumes.

TABLE OF CONTENTS

WHAT IS DRIVING THE NEED FOR AN IP SECURITY GATEWAY?

Traffic growth is unprecedented, particularly the volume of mobile data and there is no sign that this growth will peak any time soon. The number of people reaching for smartphones and tablets continues to increase, as does their use of those devices to run bandwidth-hungry, often video-based apps. To support this growth and the demand for connectivity everywhere, the number of distributed cell/radio sites is also growing, moving beyond just macro cells. Innovations like carrier Wi-Fi®, small cells and residential cells are making it possible to bring wireless access closer to the user, which in turn increases the user's adoption of those bandwidth-hungry applications.

Figure 1. Demand for radio access is coming from multiple sources



With demand for connectivity coming from many different types of access devices, the Ultra-Broadband network must interoperate with equipment from many vendors, so reliance on standards is imperative.

Protecting the network

The evolution towards LTE yields an end-to-end flat IP network. This architecture is vulnerable to the kinds of threats known on fixed networks, plus some new ones that are specific to mobile networks, such as signaling storms. Also there is a massive — and growing — deployment of carrier Wi-Fi access infrastructures and small cells (such as metro, enterprise and residential cells) in metro areas, households and offices. Each of these sites creates an IP access point to the network that could potentially be used as an entry point by attackers/hackers.

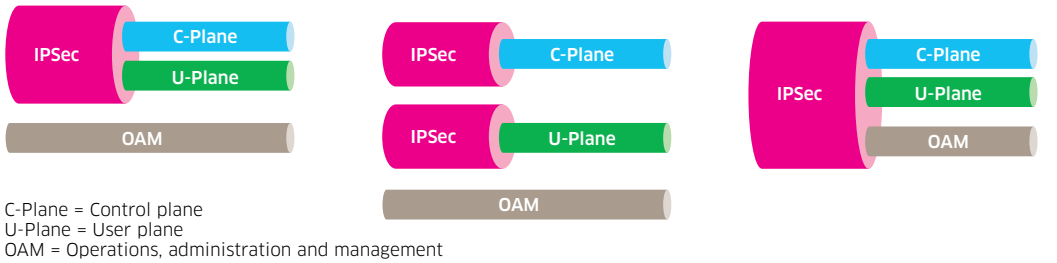
As a consequence, service providers need to protect their networks, but they must do this while simultaneously addressing the ongoing demand for speed and capacity. They need a solution that provides them with the ability to interoperate effectively with distributed cell radio sites, using a common security model. These highly distributed radio sites may be accessed over:

- Trusted networks
- Third-party and/or untrusted networks

With the need to secure a range of connections, there are different models service providers may choose to implement, depending on the level of trust. For trusted networks, IPSec may or may not be implemented. However, for untrusted networks, it is necessary to implement an increased layer of security, which can be applied to control plane, data plane, or management (OAM) traffic, or any combination thereof.

To address the new security challenges, the 3GPP standards body has introduced the concept of a security gateway through the 3GPP 33.210 and 3GPP 33.310 specifications. The concepts outlined are applicable to securing traffic from the range of radio access technologies. The security gateway offers IPSec and Certificate Management capabilities to provide access control through authentication, and traffic confidentiality and integrity through encryption. Authentication and encryption may be extended to the user plane, the control plane, and management traffic through multiple backhauling options as shown in Figure 2.

Figure 2. Examples of tunneling options for a 3GPP security gateway



C-Plane = Control plane
U-Plane = User plane
OAM = Operations, administration and management

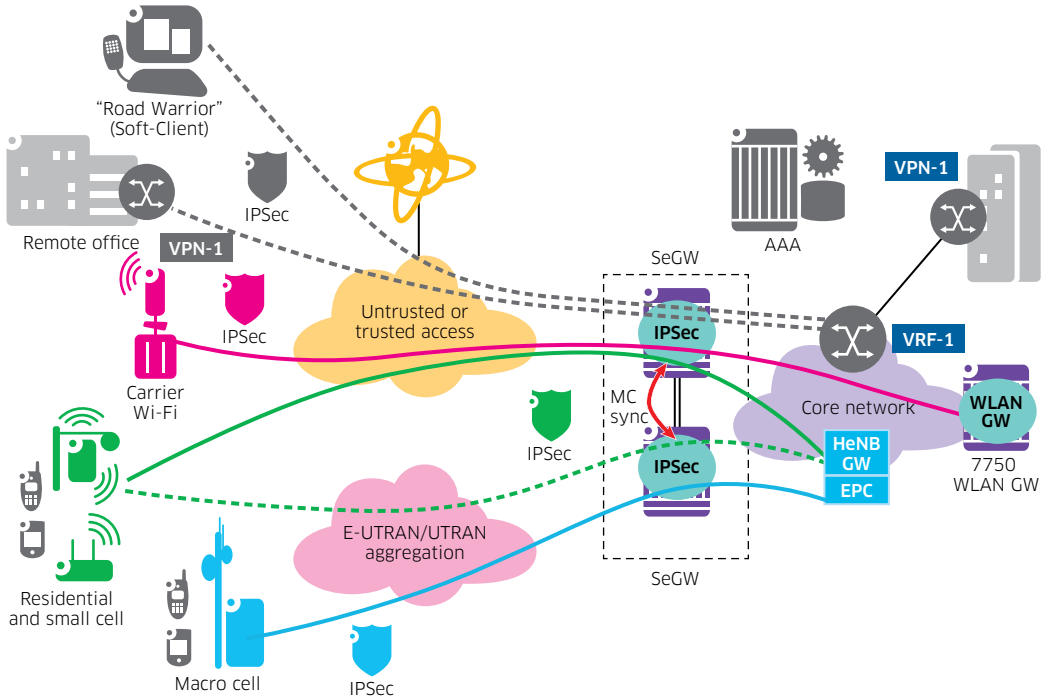
Given the diversity of access devices and the varying needs for security, Alcatel-Lucent believes the best solution for service providers is to use a common platform to act as the security gateway for all mobile technologies. This platform can be used across the range of radio access types (macro cell, small cell, residential cell and carrier Wi-Fi). It is more efficient in terms of both OPEX and CAPEX to have a single solution that can effectively address all the diverse requirements than to implement multiple single-purpose solutions. The Alcatel-Lucent Security Gateway (SeGW) is explicitly designed to serve this function and it conforms to the 3GPP standards.

ALCATEL-LUCENT SECURITY GATEWAY

The Alcatel-Lucent SeGW is delivered on the Alcatel-Lucent 7750 Service Router (SR) platform or the 7450 Ethernet Service Switch (ESS). Both are members of the industry-leading Alcatel-Lucent Service Router portfolio of next-generation carrier grade edge service router products. These platforms enable high-density service interfaces with low power consumption per bit transported. They provide the ability to support processing-intensive gateway services concurrently with other edge services, with no compromise between performance and advanced service delivery.

The 7750 SR and the 7450 ESS give service providers maximum networking flexibility with the ability to support multiple technologies and access options (Ethernet, Layer 2, MPLS, Layer 3) at speeds ranging from 100 Mb/s to 100 Gb/s. The platforms can be implemented in centralized or distributed deployment models and come in a number of form factors to suit different capacity requirements. To ensure high availability, they can be deployed in redundant configurations. For more information on these products, go to www.alcatel-lucent.com/7750sr and www.alcatel-lucent.com/7450ess.

Figure 3. Alcatel-Lucent SeGW solution overview



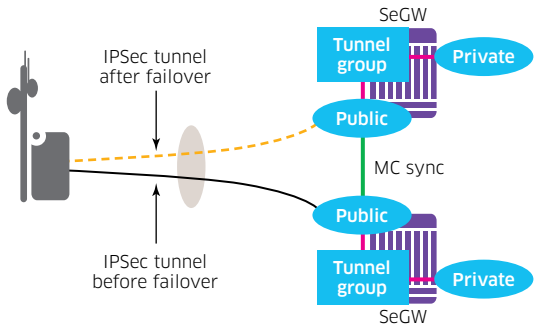
Alcatel-Lucent MS-ISA/MS-ISM

High density IPSec termination in Ultra-Broadband networks will require hundreds of gigabytes of IPSec throughput on the security gateway. The SeGW leverages its embedded service and application intelligence along with integrated services adapters and/or modules to support advanced application capabilities. The Multiservice Integrated Services Adapter (MS-ISA) and the Multiservice Integrated Service Module (MS-ISM) enable high-touch packet operations for deeper levels of integrated service capabilities, such as IPSec. They can terminate IPSec tunnels from the full range of radio access sites, including macro, small cell and carrier Wi-Fi.

The SeGW's flexible architecture makes it possible for operators to increase the number of MS-ISAs or MS-ISMs as IPSec traffic volumes increase. IPSec tunnel groups can be configured as required, with tunnel groups being load balanced across the available resources. Each SeGW can support multiple hundreds of gigabytes of IPSec throughput. The SeGW meets today's high availability requirements with:

- Intra-chassis resiliency (N:M sparing support, non-stateful)
- Multi-chassis stateful redundancy
- Non-stop routing and non-stop services
- Load balancing at the port, card, service and tunnel level
- Fast convergence across technologies, including BFD, MPLS, VRRP and BGP

Figure 4. SeGW provides multi-chassis redundancy



Stateful failover means that all the tunnel states are synchronized between the two chassis. Therefore IPSec inter-chassis failover is totally transparent to the IPSec peer (and there is no need to renegotiate tunnel).

The immediate benefit for operators is that they can deploy radio cells based on a single IPSec tunnel (per-service or for all services) instead of cumbersome, less scalable active/stand-by IPSec tunnels. They can do this while providing service hitless resiliency should there be a network/SeGW failure.

IPSec tunnels

Connectivity between the IPSec peer, such as the radio access site, and the SeGW is via one of three types of tunnels, depending on the application and/or the level of trust between the IPSec peer and the SeGW:

- LAN-to-LAN static tunnels
- LAN-to-LAN dynamic tunnels
- Remote access tunnels.

The security features attached to each tunnel type are described in Table 1.

Table 1. Alcatel-Lucent SeGW tunnel options

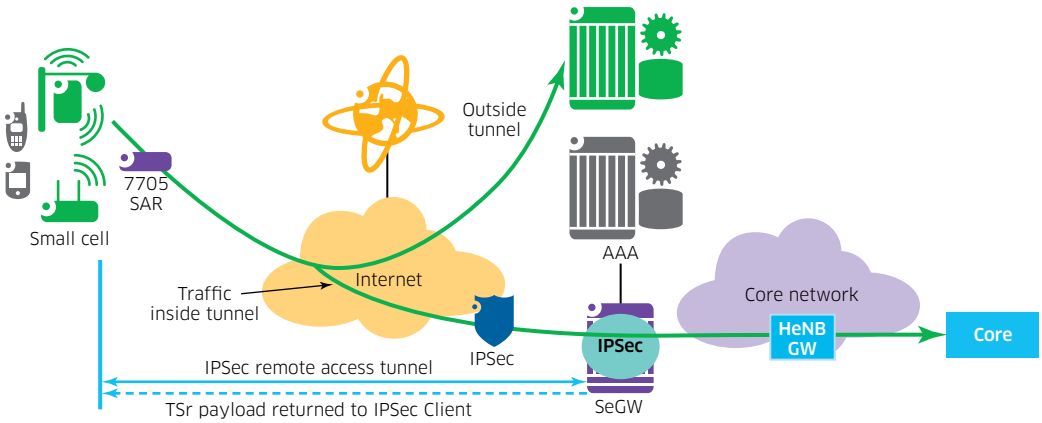
TUNNEL TYPE	SECURITY FEATURES	TYPICAL APPLICATION
LAN-to-LAN static tunnel	• Authenticated via PSK (Internet Key Exchange (IKE) v1/v2) or X.509 certificates (IKEv2) with explicit remote peer address • Per-tunnel configuration of IKE policy and transform • Explicit static route through the tunnel	• Gateway-to-gateway tunnels (e.g, inter-AS) • Limited mobile network deployments with Source IP address control • Limited scale business VPN
LAN-to-LAN dynamic tunnel	• Authenticated via PSK (IKEv1/v2) or X.509 certificates (IKEv2) with "any" remote peer address • Per-VPN configuration of IKE policy and transform • Dynamic routing through Reverse-Route-Injection (SA offer from client is converted to locally-installed routes to the IPSec tunnel)	• Macro mobile networks • Large business VPN
Remote access tunnels	• Authenticated via XAUTH with PSK + username/password (IKEv1); PSK, X.509 certificate or EAP (IKEv2) • RADIUS authorization • Dynamic binding to VPN (RADIUS) • Dynamic IP configuration of client through RADIUS	• Metro/residential, Carrier Wi-Fi mobile networks • "Road warrior" access to business VPN

The flexible manner in which the SeGW's tunneling solutions support 3GPP terminations enables much higher bandwidth per SeGW, compared to traditional IPSec applications.

There are also deployment scenarios where it is necessary to restrict the range of destinations an IPSec client, such as a small cell, can reach. Typically this traffic type is identified by lists of destination subnet/ranges.

The SeGW supports the creation of address range/subnet lists that can be returned to the IPSec client during the establishment of IKEv2 tunnels (Traffic Selector reduction (TSr)). As a result, any traffic received from the client/cell with an (inner) destination IP address out of the allowed ranges is discarded.

Figure 5. Traffic Selector reduction

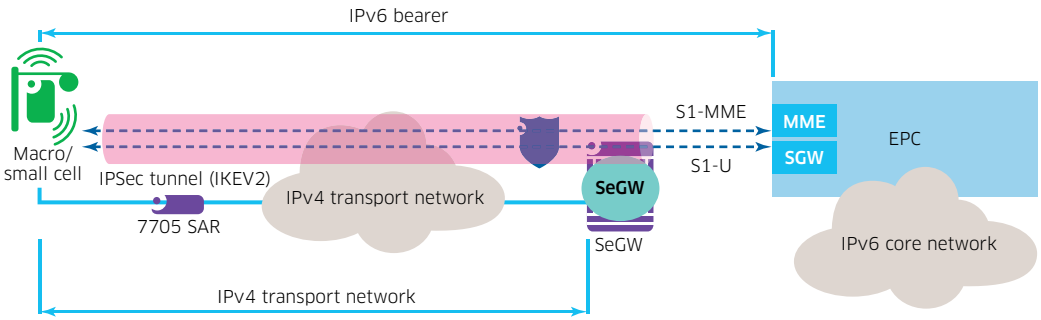


IPv6 over IPv4

The number of user equipment (UE) and other devices being deployed is increasing rapidly and IPv6 adoption is growing in response to the depletion of IPv4 addresses. As a result, many networks will need to evolve to IPv6 for bearer traffic between the UE/device and the appropriate Ultra-Broadband mobile core/gateway element. IPv6 can better support mobility plane evolution. However, this bearer traffic is often required to traverse IPv4 transport networks.

The SeGW addresses this requirement through the support of IPv6 over IPv4 IPSec tunnels. This enables the rollout of radio access points for IPv6 mobility plane traffic while using the existing IPv4-based transport services.

Figure 6. SeGW supports IPv6 over IPv4 tunnels



Certificate management

X.509 is an ITU-T standard for a public key infrastructure (PKI) that allows entities to build trust relationships between each other based on their mutual trust of a Certificate Authority (CA). In a simple deployment, the trusted CA issues a certificate, and “signs” certificates of the end entities that need to establish a secure connection between them. Entities trust each other’s certificates because they trust the issuing CA and can verify the CA’s signature by using the CA’s root certificate. In more complex scenarios, there could be a hierarchy of CAs, or a SeGW may have to check against multiple CAs for a given client. The Alcatel-Lucent SeGW supports all these scenarios.

Within this framework a public key certificate is provided to a client by a trusted CA to authenticate a user’s public key. The use of public key certificates is an important element of IPSec key management as it makes it possible to support large scale deployments.

Alcatel-Lucent provides a complete, seamlessly interworking solution for a PKI-based infrastructure when the SeGW is combined with the Alcatel-Lucent 9981 Certificate Management Server (CMS) that performs the CA/sub-CA functions. The SeGW can also be integrated into new or existing PKI infrastructures. Its certificate management functions are compliant with the above framework, and include support for the following:

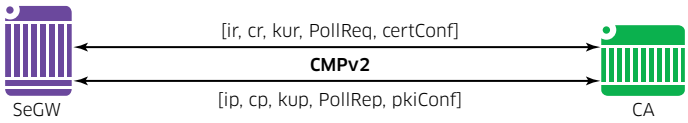
- X.509v3
- RSA/DSS key-pair generation
- CA profile management, with support of CA hierarchy and multiple trust-anchors
- Certificate enrollment using FTP/sFTP (PKCS #10) or Certificate Management Protocol CMPv2

- Certificate Revocation List (CRL) management and dynamic certificate status checking through Online Certificate Status Protocol (OCSP)
- Certificate/Key/CRL local storage and import/export support

Certificate Management Protocol

CMPv2 provides in-band communication between the SeGW (end entity) and the CA. This enables the SeGW to enroll and renew a certificate with the CA and ensures that certificates can be distributed in a simple and secure fashion.

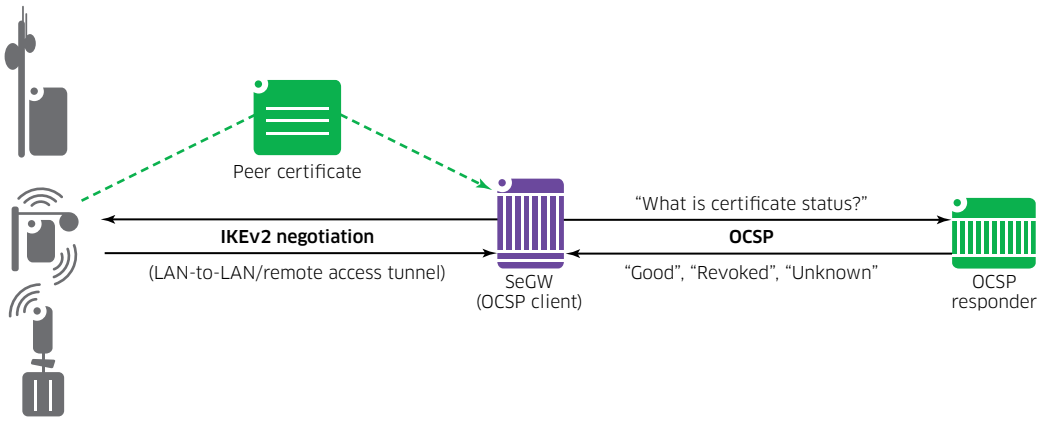
Figure 7. SeGW supports CMPv2



Online Certificate Status Protocol

The SeGW's support of OCSP allows the gateway to check the revocation status of a certificate in real time. This eliminates the need for periodic updates to the CRL, and removes the risk of relying on an outdated revocation status.

Figure 8. SeGW supports OCSP



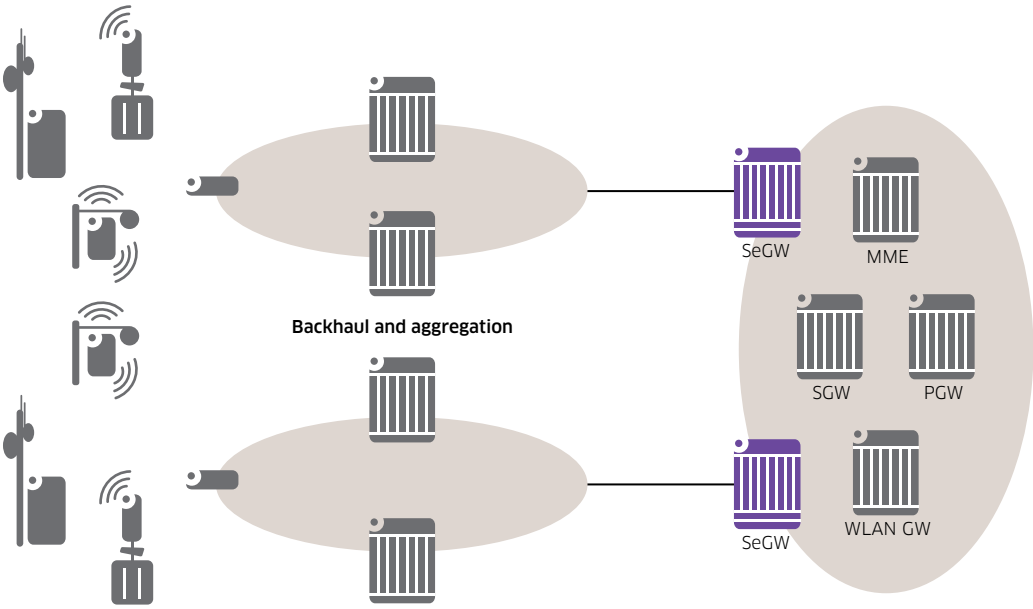
Support for centralized and distributed deployment scenarios

The 7750 SR and 7450 ESS can be put to many uses within a service provider network. They can be used in mobile backhaul networks, Metro Ethernet /aggregation networks, core and packet data networks. The IPSec SeGW is implemented in a way that enables the 7750 SR/7450 ESS to retain all of their functionalities. The SeGW function is simply an additional capability that can be enabled thanks to the hitless introduction of the MS-ISA/MS-ISM hardware modules. As a result, the SeGW function can be added to any 7750 SR/7450 ESS that is currently deployed in any of the network scenarios described above. Of course, the SeGW can also be deployed as a standalone system if required.

In mobile networks the SeGW can be cost-effectively deployed in either centralized or distributed scenarios. It can also be seamlessly integrated with any of the backhaul or core/packet data networks.

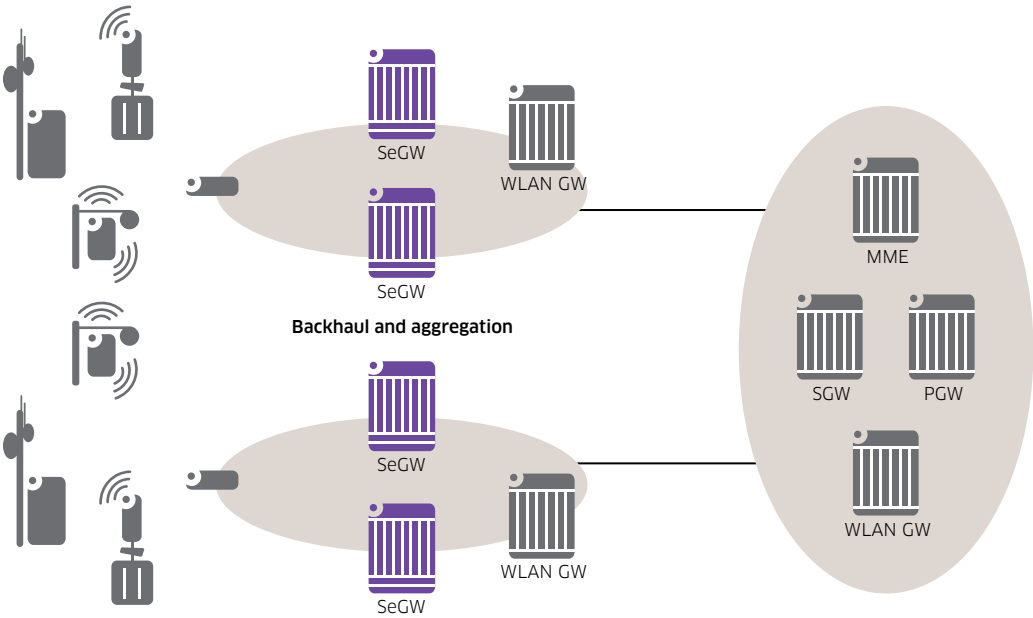
In centralized deployments (see Figure 9), hardware CAPEX and OPEX are lower because fewer SeGWs are deployed (only required at EPC node locations). 7750-SR or 7450 ESS or third-party routers are typically co-located with the Serving Gateway (SGW), MME/SGSN, and/or WLAN Gateway. The SeGWs can eventually substitute the EPC aggregation router/PE that terminates the IP/MPLS transport network, for further reduction in the total cost of ownership.

Figure 9. A centralized deployment model



In distributed deployments, performance may improve with better user traffic latency values as well as easier selection of mobile gateways and control elements. LTE X2 traffic between eNodeBs and the mobile core is backhauled to the SeGW to be routed between RAN elements, rather than through the network. Distributed deployments require more gateways, but as capacity and tunnel scale requirements are typically lower than in a centralized deployment, service providers can leverage an existing 7750 SR/7450 ESS base to deliver the SeGW function. See Figure 10.

Figure 10. A distributed deployment model



The flexible SeGW allows service providers to adopt a more distributed model for denser locations and a centralized model for lighter/broader deployments.

Prepared for the impact of small cells

As small cell (metro, enterprise, residential) and carrier Wi-Fi deployments get underway, additional capabilities are required to support their connectivity into the Ultra-Broadband backbone. The SeGW includes a range of features for supporting small cells:

- IKEv2 remote access tunnels can authenticate the small cell/Wi-Fi access point and authorize access using the IP address designation from RADIUS, based on PSK, X.509 certificates and/or Extensible Authentication Protocol (EAP) (specifically EAP-MD5, -SIM and -AKA)
- “Plug and Play “ procedures that allow automated rollout of radio cells through secured self-configuration across the network
- Support for Network Address Translation (NAT) traversal
- Application-level firewall rules through Application Assurance stateful IP session filters and Alcatel-Lucent Service Router Operating System (SR OS) ACLs
- Dynamic IKEv2 TSr
- Use of CMPv2, so certificates can be distributed between the SeGW and the CA in a simple and secure fashion
- Support for OCSP, which enables the SeGW to check the revocation status of a certificate in real time
- Support for IPv6 over IPv4
- Stateful inter-chassis redundancy

LEVERAGING THE ALCATEL-LUCENT ADVANTAGES

Implementing the security gateway on the Alcatel-Lucent 7750 SR or the 7450 ESS offers many advantages. These platforms provide a compact, high throughput security gateway solution that is ideally suited to handling the growing bandwidth demands of the Ultra-Broadband mobile access world: 2G, 3G, LTE, macro cell, small cell, carrier Wi-Fi and also VPN. The SeGW inherits all the 7750 SR’s and 7450 ESS’s high availability and resilience features. The SeGW can be easily added to an installed base of 7750 SR and 7450 ESS nodes or as part of a new install, maximizing the value of current or previous investments.

The 7750 SR and 7450 ESS platforms enables the SeGW to leverage the full range of Layer 2 and Layer 3 services and IP/MPLS networking capabilities to seamlessly interoperate with IP/MPLS-based networks, even when a network is based on third-party vendor equipment. Standard routing and MPLS protocols are used for seamless interoperability, and the same service model is leveraged wherever a 7750 SR/7450 ESS-based network is deployed.

Because the SeGW can be implemented on the 7750 SR, CAPEX and OPEX are further reduced by having a single node provide both security gateway and other edge functions such as WLAN Gateway, Broadband Network Gateway (BNG) or even mobile core gateways (SGW, PGW, GGSN).

The SeGW can be augmented with an application-level stateful firewall session filters using Application Assurance for enhanced protection of an operator's network across the range of deployment scenarios. This eliminates the need for external appliances.

With this flexibility, the SeGW functionality could be delivered in many different converged deployment scenarios, to meet an operator's requirements; including:

- Combined radio access security gateway and head-end backhaul aggregation router, in a centralized or distributed model
- Combined WLAN gateway and security gateway for fixed-mobile convergence
- Multiservice PE where security gateway and service PE are collapsed

The SeGW has been chosen by many operators worldwide for fixed and mobile applications and has been proven to interwork with all major fixed mobile equipment suppliers.

CONCLUSION

The SeGW addresses service providers' need to protect their networks while responding to the growing demand for speed and capacity coming from a variety of access devices. It enables their networks to interoperate effectively with the many access scenarios that are developing in response to widespread growth in mobile data and anticipates the capacity that will be required to address Ultra-Broadband mobile access. Built in accordance with industry, and 3GPP standards, the Alcatel-Lucent SeGW is an ideal solution to the security challenges service providers are facing.

ACRONYMS

AAA	Authentication, Authorization and Accounting
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
CA	Certificate Authority
CAPEX	Capital expenditure
CMP	Certificate Management Protocol
CMS	Alcatel-Lucent 9981 Certificate Management Server
CRL	Certificate Revocation List
EAP	Extensible Authentication Protocol
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESS	Alcatel-Lucent 7450 Ethernet Service Switch
E-UTRA(N)	Evolved Universal Terrestrial Radio Access (Network)
GGSN	GPRS Gateway Support node
GPRS	General Packet Radio Service
GW	Gateway
HeNB	Home eNodeB
IES	Internet Enhanced Services
IKE	Internet Key Exchange
IKE SA	IKE security association
IPSec	IP Security
MC	Multi-chassis
MME/GW	Mobility Management Entity/Gateway
MS-ISA	Multiservice Integrated Service Adaptor
MS-ISM	Multiservice Integrated Service Module
NAT	Network Address Translation
OAM	Operations, administration and management
OCSP	Online Certificate Status Protocol
OPEX	Operating expenditure
P	Provider
PDN	Packet Data Network
PDP	Packet Data Protocol
PE	Provider Edge
PGW	PDN Gateway
PS	packet switched
PSK	Pre-shared key
SA	Security Association
SAE	System Architecture Evolution
SAP	service access point
SAR	Alcatel-Lucent 7705 Service Aggregation Router
SeGW	Security Gateway
SGSN	Service GPRS Support Node
SGW	Serving Gateway
SR	Alcatel-Lucent 7750 Service Router
TSr	Traffic Selector reduction
UE	User equipment
VPN	Virtual Private Network
VPRN	Virtual Private Routed Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WLAN	Wireless LAN

Alcatel·Lucent