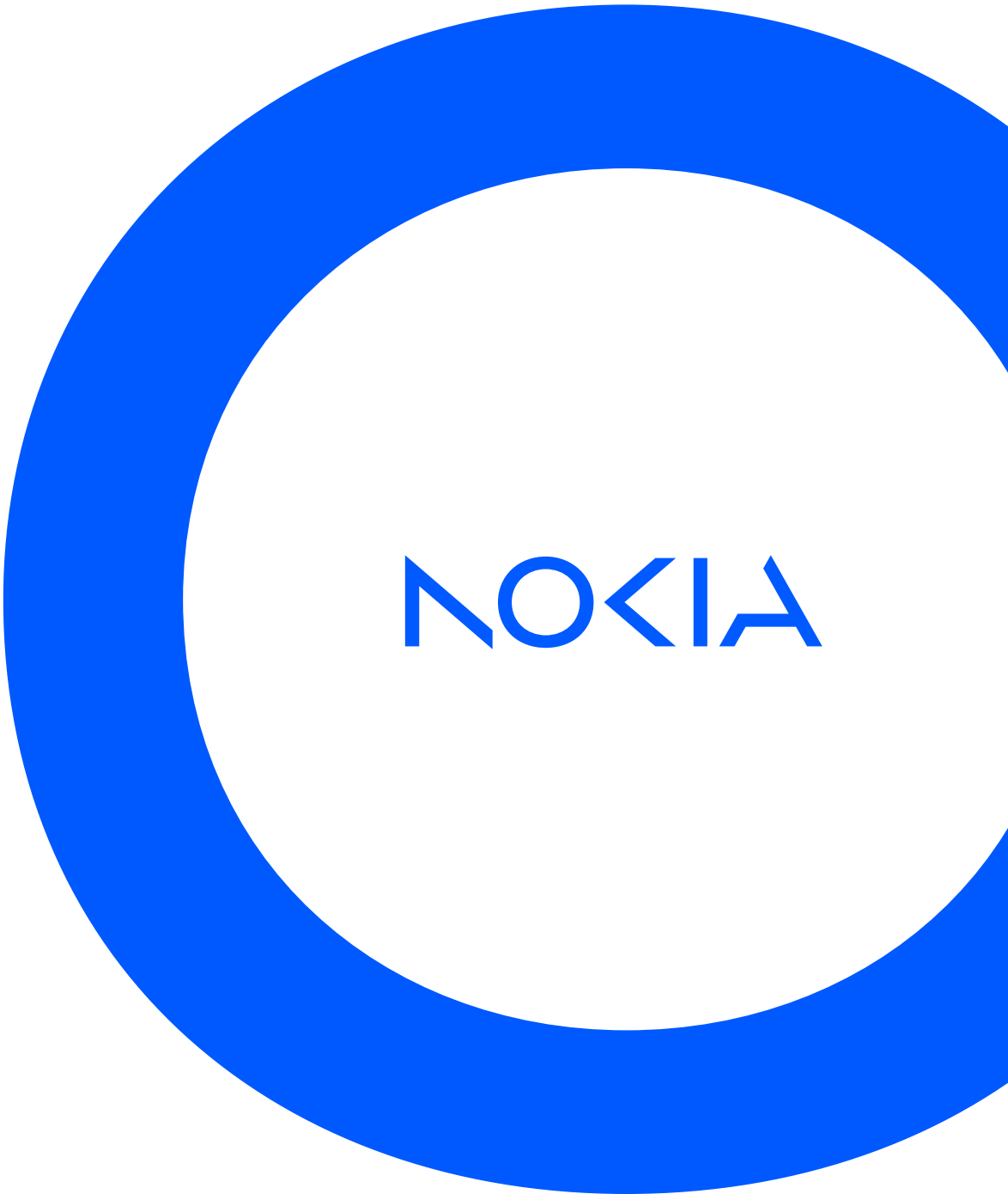
Network group encryption

Seamless encryption for mission-critical networks

Application note



Abstract

Security is a key consideration for any mission-critical communications network. The widespread adoption of IP/MPLS—from carrier to enterprise to mission-critical environments—for creating a converged network using a common networking paradigm, requires a comprehensive and universal security framework that does not impede the network's objectives and functions, or the ability to securely deliver critical services.

Today's encryption solutions have a selective security focus on specific environments and require tradeoffs between functionality and operational simplicity when extended beyond their original design. Nokia network group encryption (NGE) is a security solution that provides a ubiquitous, efficient and scalable encryption framework. By ensuring seamless, end-to-end security and confidentiality for all IP/MPLS traffic types and topologies, Nokia NGE meets the demands of modern and evolving wireline, wireless and converged mission-critical networks.

Contents

1 Encryption challenges for network operators

A Network operators worldwide recognize IP/MPLS as a key technology that extends its versatility to mission-critical applications by allowing various types of networks and services to be consolidated onto a single unified packet transport model. Often, when encryption is applied to mission-critical networks, compromises need to be made that break the homogeneity and uniformity of the network and diminish the benefits of convergence.

Existing solutions are often intrusive to the design or may require tradeoffs that create additional operational challenges. In some cases, the encryption solution requires new types of encapsulation and use of new topologies—that deviate from the original IP/MPLS network design. In other situations, current solutions cannot encrypt all types of traffic in a seamless manner or breaks the end-to-end integrity of encryption by introducing hop-by-hop encryp/decrypt requirements. Sometimes, the IP/MPLS control plane itself is not encrypted, and is left exposed to unauthorized inspection and even direct manipulation by third parties.

This paper discusses a new technique for encrypting and authenticating mission-critical IP/MPLS traffic. Nokia network group encryption (NGE) is a versatile, scalable, seamless and homogeneous group-based framework for ensuring and maintaining security, privacy and confidentiality—through encryption and authentication—for any type of traffic transported over an IP/MPLS network.

Nokia NGE is designed to leverage all the benefits associated with an IP/MPLS architecture without being intrusive or requiring compromises to security or network design, therefore increasing operational simplicity.

For all of these reasons, NGE is an important component of the Nokia security feature set [6] for securing mission-critical networks.

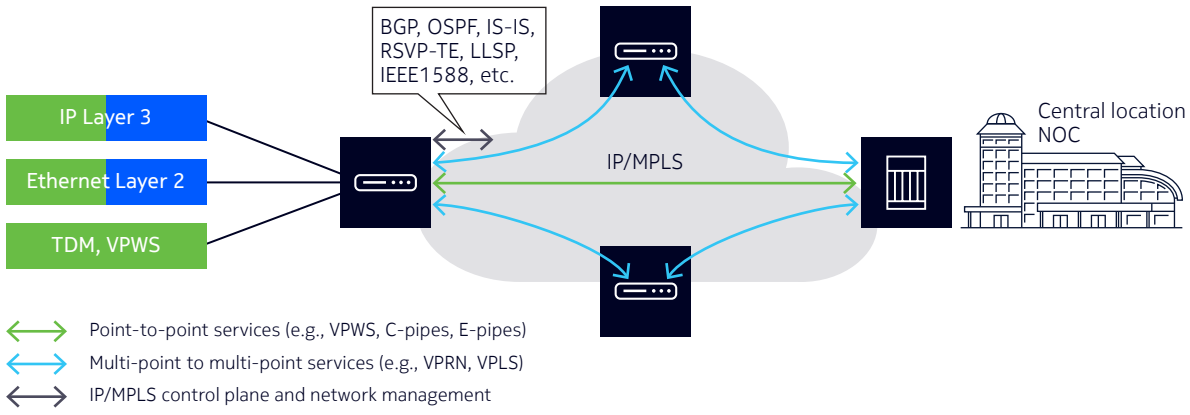
2 Nokia's approach

This section provides the background to the Nokia NGE solution and outlines Nokia's motivation for offering a new encryption framework and architecture.

2.1 Traffic types that need to be secured in IP/MPLS networks

To understand the challenges of encryption, it is important to know the rudimentary types of traffic found in most mission-critical IP/MPLS networks that needs to be secured. These are shown in Figure 1.

Figure 1. Three main traffic types that need encryption



Dedicated, point-to-point traffic is used to carry specific circuits or connections over designated tunnels, pipes or leased lines. This might include IP flows or non-IP based traffic such as teleprotection and SCADA circuits in power grids, dedicated circuits for transportation in train and track control, or other point-to-point mission-critical circuits. Dedicated, point-to-point traffic typically uses virtual leased line (VLL) or pseudowire-based MPLS services.

There is also traffic that is multi-point to multi-point or any-to-any in nature. Any-to-any critical traffic has many use cases: in smart grid automation, traffic surveillance, train monitoring and control systems, and in process message buses used in modern industrial control applications. This traffic typically leverages the capabilities of Layer 3 IP VPNs or Layer 2 virtual private LAN service (VPLS) technology that include multi-point to multi-point features. Encrypting this type of traffic typically requires a group-based approach to scale the network.

The third traffic type is IP/MPLS control plane traffic, the operational foundation of IP/MPLS networks and services. The control plane is used to establish and manage services, and it carries sensitive information such as topology, IP addressing and protocol details. Control plane traffic is often overlooked when securing mission-critical networks. However, the control plane is arguably one of the most important parts of a network to be secured.

Traditional encryption models cannot provide a complete encryption solution for all these traffic types concurrently without making compromises, introducing difficulties, or adding extra operational expense to the solution.

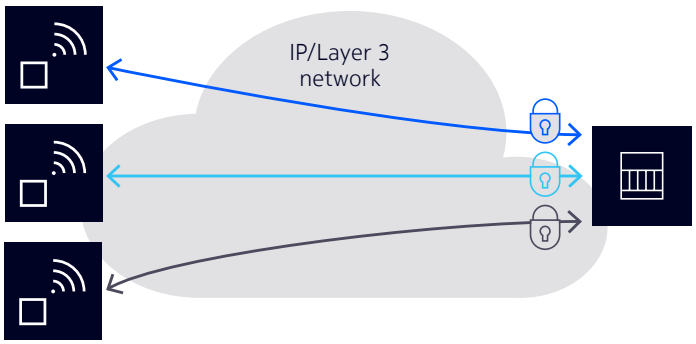
2.2 Shortcomings of traditional encryption methods

2.2.1 Point-to-point and group-based Layer 3 encryption

The traditional methods of adding encryption and authentication to secure traffic in an IP/MPLS network typically include techniques associated with the IP security (IPsec) suite of protocols and related technologies. IPsec was originally designed to secure point-to-point Layer 3 traffic (IPsec tunnels) over an insecure medium (see Figure 2), and did not initially target any-to-any communication for virtual private routed network (VPRN) services.

Because IPsec is designed for Layer 3 traffic, it does not adapt well to Layer 2 or other non-IP based legacy communications protocols. However, non-IP traffic increasingly requires any-to-any communication such as VPLS, which is similar to Layer 3 VPRNs.

Figure 2. Point-to-point encryption and control plane



To adapt IPsec for any-to-any communication, an operator must establish a mesh of point-to-point tunnels between participating nodes. Scaling issues and the operational complexity of this solution are well known and have inhibited this approach from being adopted at a large scale to solve any-to-any communication using a point-to-point encryption approach.

The Group Domain of Interpretation (GDOI) specifications [7], which leverage IPsec technology, have made it more feasible to transport any-to-any Layer 3 traffic. However, the fundamental point-to-point nature of the IPsec control plane still remains, and similar to IPsec, it does not adapt well for Layer 2 and other non-IP-based traffic.

Both IPsec and GDOI use the Internet Key Exchange (IKEv2) protocol [8] to distribute shared encryption keys between two end routers. When this control plane is operational, data is encrypted and traffic can flow. However, if the IKE control plane fails, encryption is halted. Moreover, the mission-critical traffic becomes severely impacted because the transport tunnels from IPsec or GDOI are no longer available.

Running a separate control plane beyond the existing IP/MPLS routing and signaling control plane adds additional complexity to network topologies and requires special considerations to guard against failures. In addition, when so many tunnels exist in a network where each tunnel requires an IKE session, growing these networks for any-to-any services becomes burdensome, raising concerns regarding IKE's ability to efficiently manage large numbers of tunnels.

As an example of IKE control plane issues for GDOI, IKE runs on a key server, typically another router in the network. The IKE control plane sessions need to be managed between a key server and group members (other routers in the network). Scaling up the IKE control plane to support large numbers of group members remains the biggest challenge because of the overhead added to router resources to support these IKE sessions. This overhead can quickly impose restrictions on a router's ability to efficiently manage and perform the required large-scale processing.

Also, requiring an IKE control plane for encryption that is separate from the control plane used to operate the underlying IP/MPLS network can lead to added risks of topology inconsistency. This could cause issues with routing reachability of key servers that are necessary to maintain IKE sessions, keep tunnels up, keep GDOI key synchronization intact, and maintain traffic flows. Finally, GDOI does not protect the IP/MPLS control plane as part of its security framework.

NGE does not use a separate control plane function to distribute and manage keys between peering nodes that need to send encrypted traffic. Therefore, there is no risk of a control plane malfunction that can stop mission-critical traffic from being encrypted or can drop the traffic altogether.

NGE is also designed without a bias for Layer 3 traffic or point-to-point tunneled traffic. Because its keys are group-based, NGE easily handles any-to-any communication of any type of traffic, including Layer 2 VPLS multipoint-to-multipoint services and machine-type communication (MTC) applications leveraging any-peer to any-peer communication. Finally, NGE is designed to protect the IP/MPLS control plane and management traffic as well as user traffic, ensuring that the control protocols user traffic relies on are not compromised.

2.2.2 Layer 2 security using MACsec

Media Access Control security (MACsec) is another encryption and authentication method that is being proposed to encrypt all types of traffic over an Ethernet link. While it effectively addresses security in Ethernet-only Layer 2 environments, there are two concerns that make it a questionable choice for an end-to-end security solution for mission-critical services based on IP/MPLS.

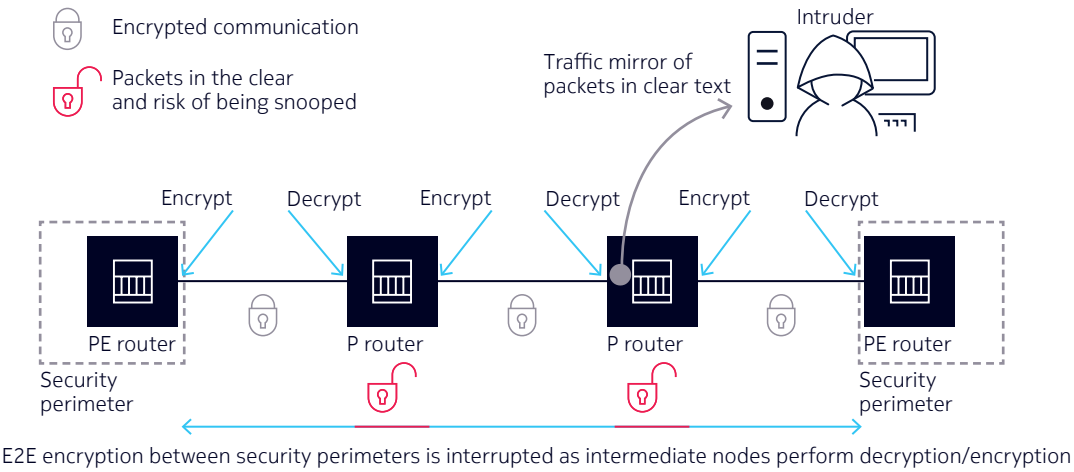
The first concern relates to using routing and forwarding information—IP/MPLS encapsulation in Layer 2 packets. To determine where packets need to be sent, MACsec needs to decrypt traffic, extract the forwarding information in IP/MPLS, and then re-encrypt the traffic.

For IP/MPLS networks this requirement may be imposed at each hop in the network because Layer 2.5 MPLS and Layer 3 IP header information must be accessed to determine next-hop paths and tunnels. This can present a potential security risk at each point where the packet is decrypted because port or service mirroring techniques could be used to duplicate clear text packets towards rogue and untrusted parties.

Multi-hop encryption and decryption also adds latency and introduces additional hardware and power costs because MACsec-capable hardware is required at each point in the network where MACsec decryption and re-encryption is occurring.

Figure 3 shows the main challenges to offering end-to-end IP/MPLS traffic protection using MACsec.

Figure 3. Challenges to offering end-to-end IP/MPLS protection with MACsec



The second concern is that it is not straightforward to carry MACsec traffic over wireless or wireline Layer 3 service provider networks. Because MACsec functions at Layer 2, operators that rely on Layer 3 carrier VPN services to interconnect sites (e.g., IP services over LTE networks) are left with a disjoint solution for two possible reasons: either another encapsulation layer is needed to put MACsec into Layer 3 packets or another Layer 3 security technology is needed to encrypt and protect these Layer 3 domains. To have a comprehensive security framework across the whole network, operators may need to "stitch" security across their Layer 2 and Layer 3 environments. This is cumbersome, complicated and adds unnecessary operational overhead when designing and planning networks.

NGE is designed to work over any type of Layer 2 and Layer 3 service provider network, including cellular networks that need to support growing and evolving MTC (M2M and Internet of Things [IoT]) devices and applications. NGE provides a consistent security framework for wireline, wireless and converged networks that uses a single, contiguous technology to provide a comprehensive and uniform end-to-end solution.

2.3 NGE design goals for mission-critical IP/MPLS networks

As larger numbers of smart applications are being deployed for critical infrastructures, it is necessary for mission-critical networks to leverage the benefits of IP/MPLS technology to its fullest. In doing so, security cannot create compromises or add additional burden that will reduce the usefulness and original intent of the network. NGE's flexibility to support different traffic types and any-to-any topologies while enabling security makes it an ideal choice to connect a wide variety of devices and equipment.

We have already seen that with traditional Layer 3 or Layer 2 approaches to encryption and authentication, there are limitations on the types of traffic that can be secured.

The benefits of MPLS' ability to carry different traffic types at either Layer 2 or Layer 3 have been proven through successful deployments worldwide. In some cases, it is the non-IP traffic carried over MPLS that is considered mission-critical. In others, modern mission-critical protocols leverage both Layer 2 and Layer 3 concurrently.

Nokia's approach to security is to capitalize on MPLS' ability to support the variety of traffic types by designing and optimizing a security framework that overlays encryption for MPLS payloads and results in encrypted traffic carried over an IP/MPLS network without altering the original traffic or creating additional encapsulations and overhead.

Nokia NGE performs encryption and authentication functions directly on the original traffic, and then packetizes it in the same MPLS frame that otherwise would have been used for unencrypted transport. With this approach, all original MPLS labels and functions are kept untouched so that MPLS services (e.g., VLL, VPLS and VPRN) are treated the same way as before the security function was added. Also, because NGE uses a group-based encryption approach, it provides any-to-any communication for encrypted and authenticated Layer 2 and Layer 3 traffic, including multicast traffic related to VPRNs, Internet enhanced services (IESs) and VPLS.

In a similar way, NGE can be applied directly to the IP/MPLS control plane without altering the network architectures that rely on that control plane. With NGE, key protocols such as OSPF, BGP, IS-IS, RSVP-TE, LDP and BFD can also be protected end to end.

As already mentioned, traditional encryption solutions face scaling, complexity, setup and control plane management issues. These sometimes result in less secure frameworks and have constraints to fully addressing all traffic types that need to be secured.

To address these shortcomings, Nokia has designed and developed NGE to:

- Overlay a flexible and efficient security framework on top of IP/MPLS to minimize the configuration and operational complexities associated with adding encryption to services. This is accomplished by leveraging existing network designs (e.g., for MPLS high availability, QoS, scalability and flexibility) and architectures. With this approach, encryption does not dictate the network design; instead, it is applied to the design.
- Maximize the types of traffic that can be secured with a comprehensive encryption solution, including legacy, Layer 2, Layer 3 and IP/MPLS control plane and network management traffic
- Maximize end-to-end integrity of traffic without breaking the security construct (which other techniques, such as multi-hop or tunnel-by-tunnel encryption/decryption, may do)
- Maximize the service uptime in mission-critical networks with non-stop encrypted services where traffic flows are ensured at all times—even during failures and recovery—by using restoration techniques that minimize the traffic and encryption impact of link outages or nodal (router) failures

- Minimize the additional/incremental control plane overhead traffic needed to operate functions enabling security, privacy and confidentiality while optimizing network resources for wireline, wireless and converged networks
- Minimize additional latency and eliminate potential performance bottlenecks that may be incurred with control plane-heavy encryption solutions while maximizing encrypted traffic throughput.

Table 1 provides a quick comparison of NGE and traditional Layer 3/ Layer 2 encryption approaches and techniques.

Table 1. Comparison of NGE and traditional L3 and L2 encryption techniques

Encryption approach/ technology	L3 point-to-point encryption tunnels (IPsec)	L3 group-based encryption (e.g., GDOI)	L2 MAC-based encryption	NGE
Applicability	Primarily for L3 IP services; does not support TDM/L2 services	Does not support TDM/L2 services	Supports L2 and L3 services but does not provide end-to-end protection and requires dedicated MACsec-capable hardware throughout	Wide variety of L2 and L3 services end to end
Scalability	Hard to scale for multi-point to multi-point	Key-server restrictions require additional technologies for spoke-to-spoke communications (e.g., DMVPN also needed)	Scales to the number of links in the network	Leverages network limits such as MPLS tunnels, router interfaces and VLL/VPRN/VPLS system limits
Encryption Control Plane	Requires maintenance of per-tunnel IKE sessions to maintain traffic flow	Requires maintenance of IKE sessions to key servers, where key server vulnerability impacts traffic	MACsec control plane required on each interface	No control plane in the network; keys are downloaded from the Nokia NSP via SSH sessions, but this is not required to maintain traffic flows; non-stop encryption
IP/MPLS Control Plane	Control plane traffic is exposed or needs tunneling	Control plane traffic is exposed	Control plane traffic can be protected but is exposed on each hop (e.g., T-LDP or BGP) in multi-hop sessions	Secured in all cases
Topology	Ill-suited for large mesh connectivity	Supports mesh connectivity	Supports point-to-point and mesh connectivity	Supports any topology: point-to-point, spoke and hub, or mesh
Robustness	IKE session management at risk when scaled or during network congestion	Key server becomes a single point of failure	Encryption/decryption performed at every hop, requiring increased security at every hop to protect from snooping/ hacking/packet mirroring	Optimized to ensure continuity of encrypted services
Recoverability	Re-establish security control plane for each tunnel to far-end routers	Key server-dependent (typically a router)	Re-establish security control plane for a link or each link connected to a router	Quick restoration of security framework ensured through distributed architecture

3 NGE solution functional overview

This section discusses:

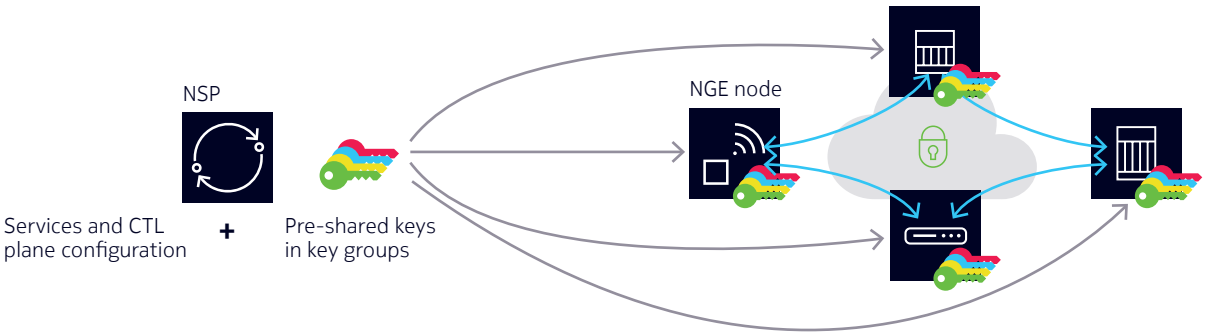
- NGE components: Building blocks that comprise the Nokia NGE solution
- NGE MPLS services packet formats and encryption algorithms
- An example that illustrates how the Nokia NGE solution is used in practice.

3.1 NGE components

As shown in Figure 4, the NGE solution encompasses five components:

- Nokia Network Services Platform (NSP): Acts as the key manager and provides service management for network-wide encrypted services
- Nokia 7705 Service Aggregation Routers (SARs) and the Nokia Virtualized Service Router (VSR): Routing elements capable of performing NGE. In subsequent text, these elements are jointly referred to as NGE nodes.
- Key groups: Predefined groups of key holders assigned to specific services or interfaces, and enabling network partitioning of security
- Encrypted IP/MPLS services: IP/MPLS services that require security and end-to-end encryption
- NGE domains: Network domains where Layer 3 user and control plane traffic plus select Layer 2 control plane traffic requires end-to-end encryption in the domain.

Figure 4. NGE solution components



3.1.1 Nokia NSP

The main component of the NGE solution is the Nokia NSP, which provides two main functions to enable NGE:

- Management of services and control plane functions that require encryption and authentication, and management of the nodes in security domains
- Encryption key management for all NGE nodes, including provisioning relevant keys used to perform traffic-level encryption and authentication.

NGE uses symmetric pre-shared keys to perform encryption and authentication. These are stored in key groups and managed by the NSP. The NSP ensures that all nodes participating in an encrypted service or allocated to an NGE domain have the key groups configured and synchronized. Only those key groups that are relevant to particular nodes are provided access to (downloaded with) the key groups and sensitive keying information.

Operational actions performed by the NSP include:

- Deploying keys to new nodes where/when new encrypted services are required
- Performing re-keying of the network at regular intervals
- Deleting keys from nodes that no longer need those keys.

3.1.2 NGE nodes

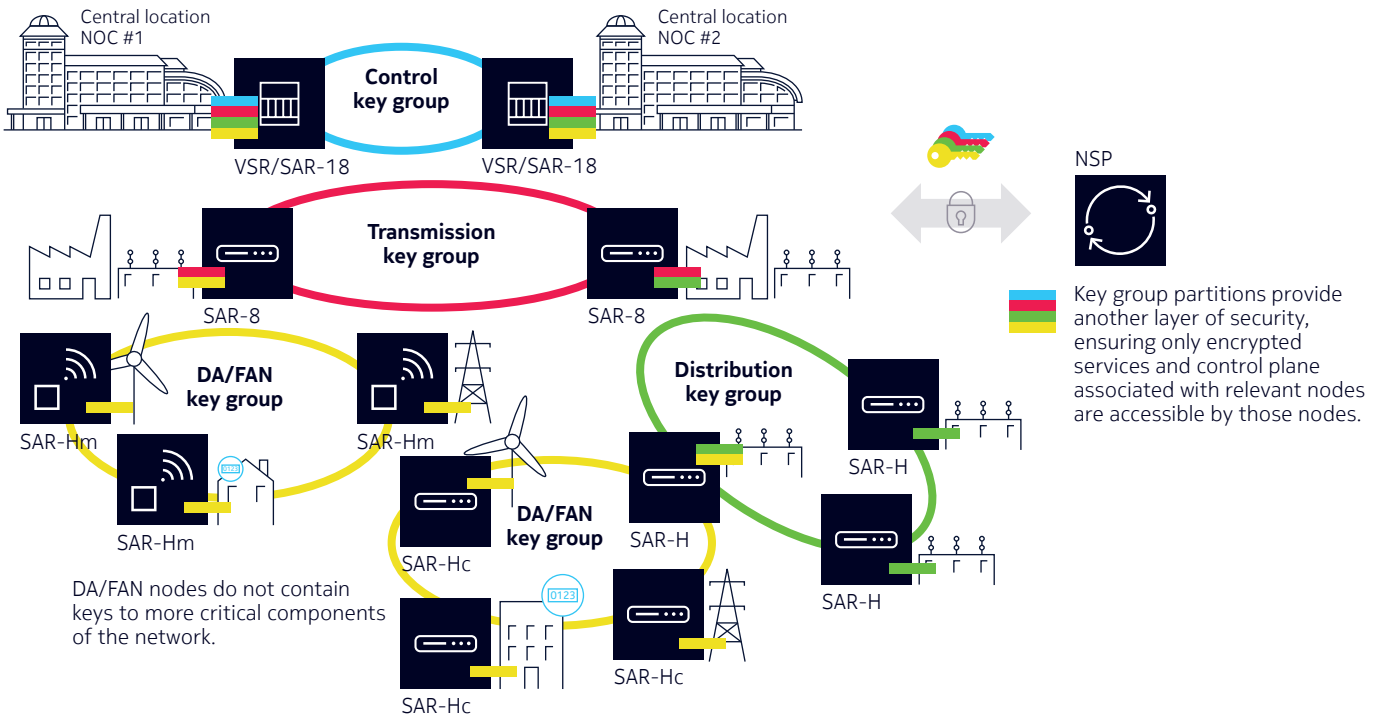
NGE network nodes perform the NGE encryption/authentication function for the IP/MPLS services and related control plane. From Nokia's industry-leading IP/MPLS portfolio, the Nokia 7705 SAR family and the Nokia VSR perform the enhanced encryption functions and act as NGE nodes.

3.1.3 Key groups

NGE allows segmentation of its security framework to provide a tiered approach to managing keys in the network. This is accomplished through key groups. Classes or sets of different MPLS services are configured for NGE and allocated to specific key groups, which define specific security policies for those services. For example, in a power utility smart grid network there may be different levels of services with different levels of criticality.

Figure 5 shows an example of key group partitioning.

Figure 5. NGE key groups enabling encryption partitioning



In the Figure 5 scenario, distribution automation (DA) and field area networks (FANs) are less critical than transmission or distribution substation network equipment. Due to the differences in criticality of infrastructure, it would be ideal to ensure that nodes at risk do not contain more critical information than is necessary. Encryption keys for sensitive portions of the network should not be available where nodes are at risk.

NGE enables operators to partition encryption keys between different security domains in a network. For example, if an attacker attempts to gain access to the network from a DA or FAN location that may be prone to attack because added physical security measures may be impractical or cost-prohibitive, the attacker will not be able to gain sensitive key information for other parts of the network. Thanks to key group domains and partitioning, the security perimeter is greatly reduced, and an attacker will have a very limited scope for any potential attacks.

3.1.4 Encrypted IP/MPLS services

The fourth component of the NGE solution is the IP/MPLS services that can be encrypted. Encryption of these services is accomplished by assigning key groups to service distribution points (SDPs) or directly to VPRNs.

SDPs provide transport of services over LSP, BGP or GRE tunnels. Any service that is configured to use an NGE-enabled SDP and associated tunnels will have its traffic encrypted before entering the tunnel, and decrypted when exiting the tunnel. The types of service that leverage SDPs for transport include VLLs (e.g., E-pipes and C-pipes), VPLS using spoke and mesh SDPs, and VPRNs that might utilize dedicated SDPs for transport.

Nokia VPRN services can automatically bind VPRN services traffic to transport tunnels (LSP, BGP and GRE). This automatic binding is leveraged by NGE to provide simple enablement of NGE on the VPRN. A key group that is assigned to a VPRN causes all traffic in the VPRN to be encrypted, regardless of tunnel type or destination.

With full visibility of IP/MPLS-based services and the nodes participating, the NSP manages the encryption key groups used to enable encryption on these services, and downloads them as appropriate to the correct NGE-enabled nodes.

3.1.5 NGE domains

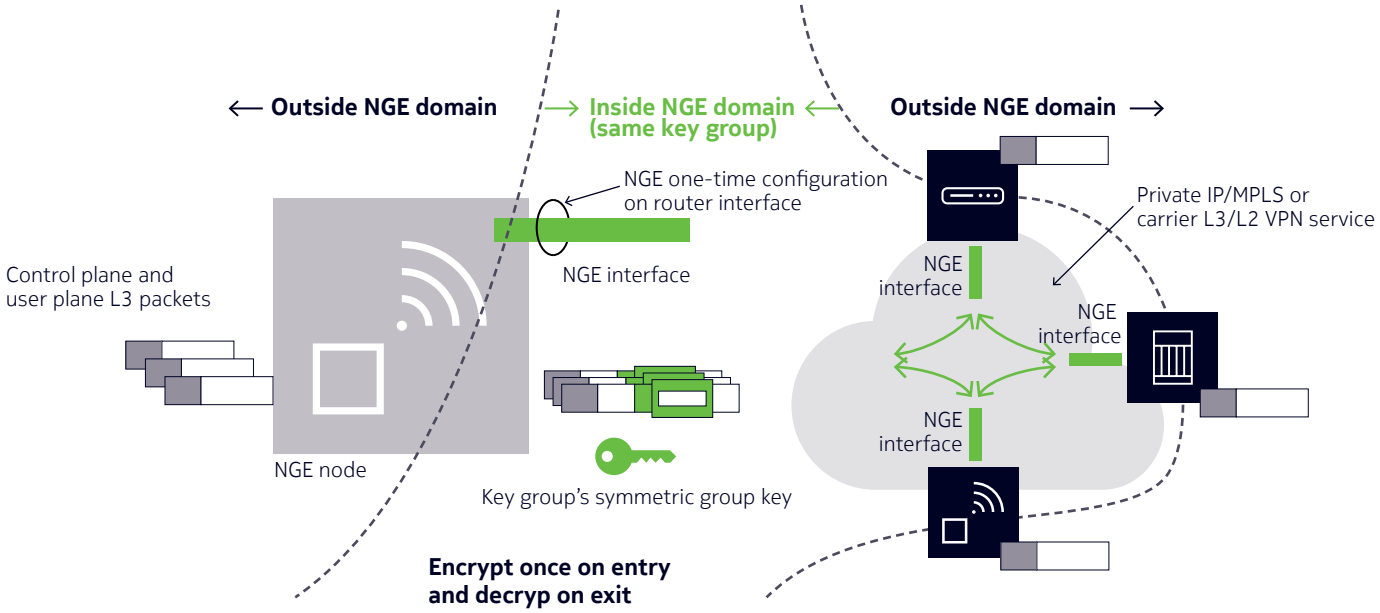
NGE domains are groups of nodes and router interfaces forming a network that use a single key group, to create a security domain (see Figure 6). NGE domains are created when enabling router interface encryption on router interfaces that need to participate in the NGE domain. The NSP assists operators in managing the nodes and interfaces that participate in the NGE domain.

Traffic is encrypted when entering the NGE domain (using the key group configured on the router interface) and is decrypted when exiting the NGE domain.

Traffic may traverse multiple hops before exiting the NGE domain, but decryption occurs only on the final node when the traffic exits the NGE domain.

NGE domains are an important tool for isolating and securing control plane traffic across third-party networks such as wireless carriers, Layer 3 IP VPN providers and Layer 2 service providers.

Figure 6. NGE domain



3.2 NGE MPLS services packet formats

NGE is designed to maintain the seamless nature of MPLS-based services without imposing additional restrictions when security is added to MPLS payloads.

To this end, the NGE MPLS services packet format minimizes the visibility of the encryption and authentication by performing this function only on the payload of the MPLS packet while keeping all MPLS labels intact.

This approach allows any intermediate nodes that are performing P-router, label switched router (LSR), area border router (ABR), or autonomous system border router (ASBR) functionality to continue forwarding packets as originally intended by these seamless MPLS-based services.

When NGE is added, there is no impact to any of the QoS, high-availability or MPLS tunneling functions and requirements originally placed on the network.

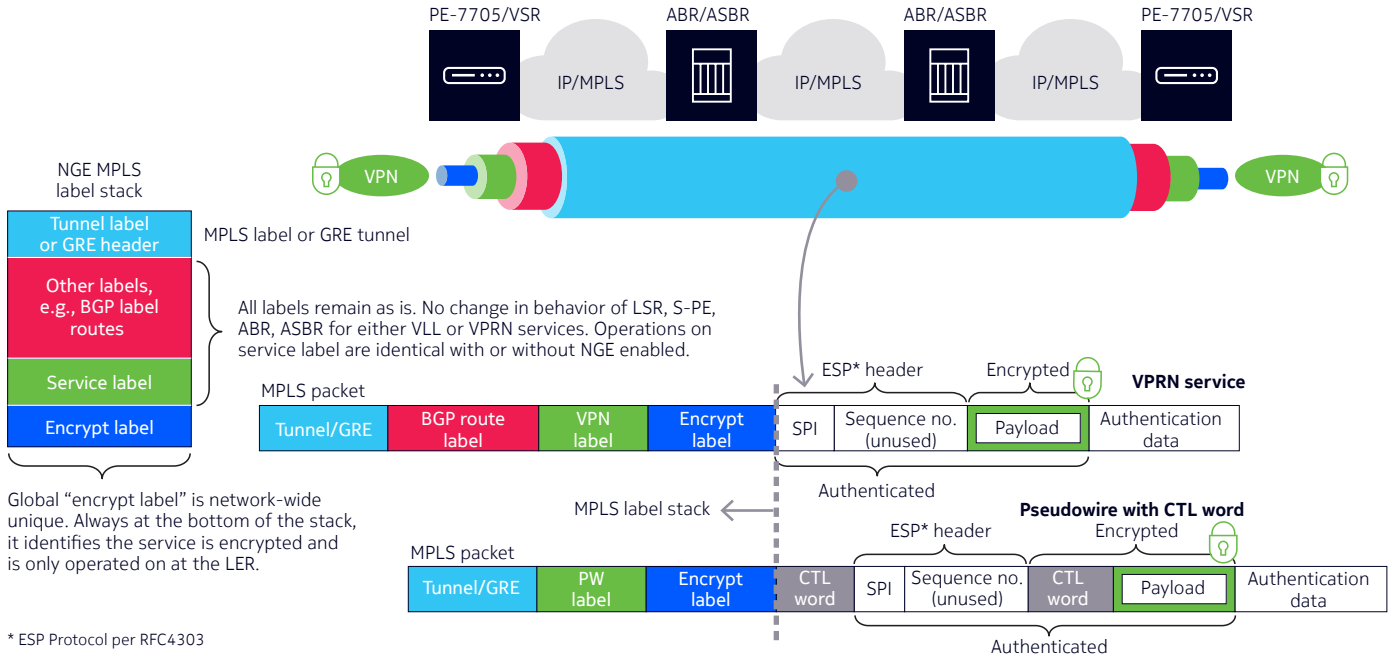
Figure 7 shows the NGE MPLS services packet format. The original tunnel, BGP tunnel and service labels are kept as defined in non-NGE-based MPLS packets.

NGE packets include a global encrypt label that is added after the service label.

This allows NGE nodes to:

- Quickly identify packets that have an NGE encrypted payload
- Keep statistics for encrypted packets and unencrypted packets
- Help with debugging and other operations, administration and maintenance (OAM) functions.

Figure 7. NGE services encryption packet format examples



3.3 NGE encryption algorithms

NGE uses the Encapsulating Security Payload (ESP) format defined in IETF RFC 4303 [4] to encrypt and authenticate MPLS payloads. NGE minimizes the added packet overhead associated with traditional encryption solutions: there is no additional IP header added to the payloads. For VPRN- or VPLS-based services that do not use a control (CTL) word, the payload is encapsulated by the ESP header as needed. For VLL or pseudowire-based services that use a CTL word, the CTL word is left in place for those pseudowire switching points that rely on the CTL word to be in its original position.

To avoid any potential attacks against VLL or pseudowire services using the CTL word, the CTL word is also copied into the secured portion of the payload. When the destination label edge router (LER) decrypts the payload, it checks the CTL word against the original CTL word to ensure it was not altered.

NGE uses symmetric ciphers with the same key used for encryption and decryption. NGE supports the Cipher Block Chaining (CBC) encryption mode and the following block ciphers:

- AES128 with a 128-bit key uses 128-bit size blocks
- AES256 with a 256-bit key uses 256-bit size blocks.

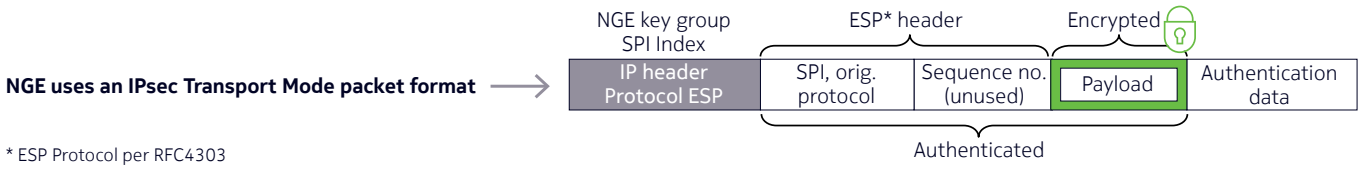
For authentication, the following algorithms are available:

- HMAC-SHA-256
- HMAC-SHA-512.

3.4 NGE domain packet formats

When creating NGE domains where NGE is then applied to Layer 3 user and control plane packets, NGE reuses a standard IPsec transport mode packet format (see Figure 8).

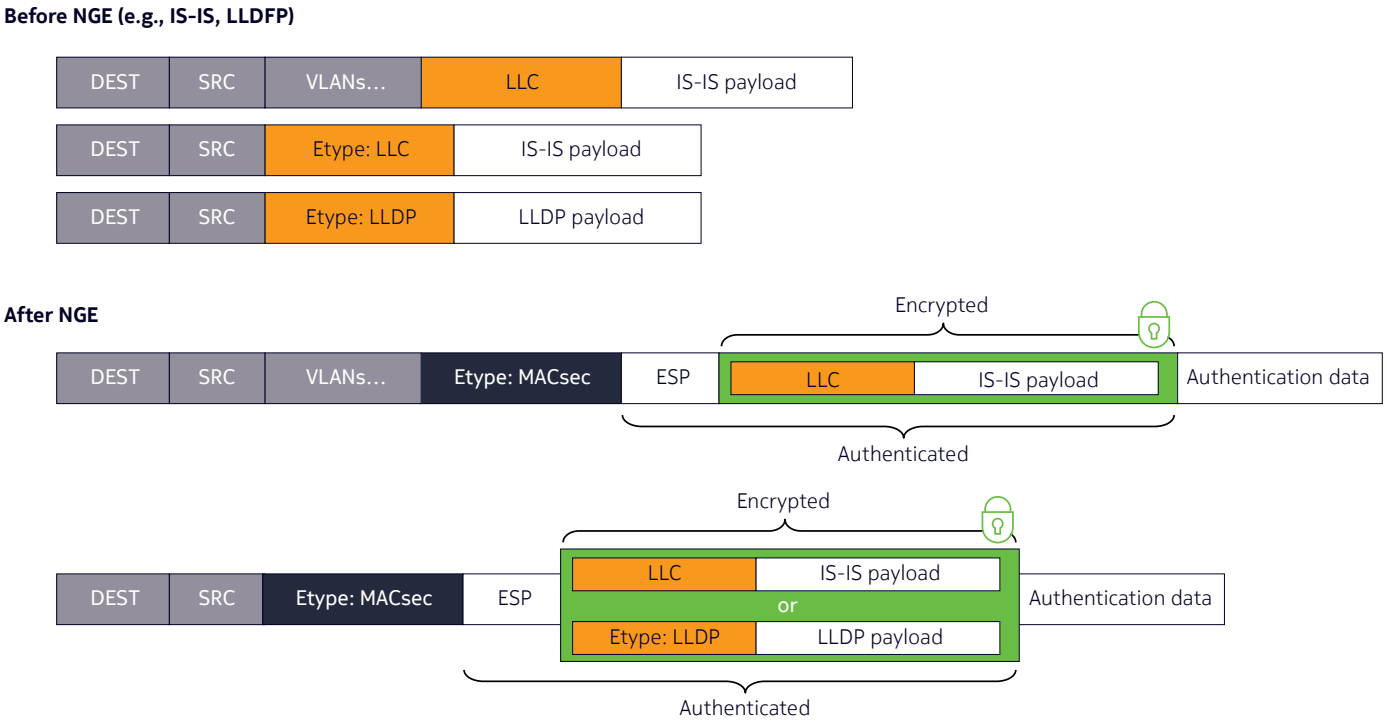
Figure 8. NGE domain Layer 3 packet format



NGE can also be enabled to protect the Layer 2 protocols IS-IS and LLDP. These protocols carry sensitive information about a network's topology, and NGE ensures they are not visible for inspection by attackers who might attempt to packet sniff the network. NGE again reuses the ESP protocol defined in RFC 4303 to encrypt the contents of the IS-IS and LLDP packets.

The packet format is shown in Figure 9.

Figure 9. NGE domain Layer 2 packet format

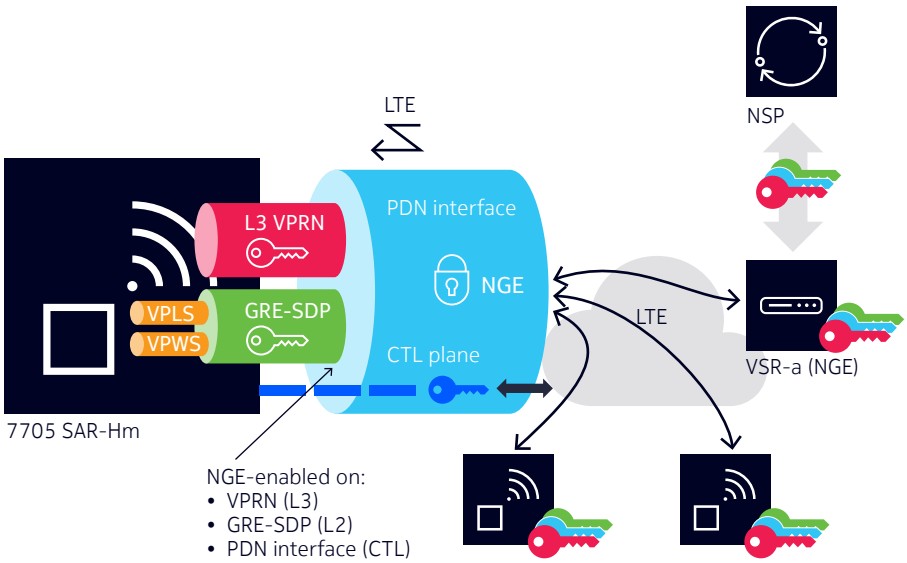


3.5 Example of the NGE solution in practice

A common use case of NGE is to protect traffic over a variety of network types. From private IP/MPLS, to Layer 2 or Layer 3 carrier VPN services, to LTE wireless networks, NGE is designed to provide comprehensive security across each type.

Figure 10 shows an example of NGE providing protection over a wireless service provider.

Figure 10. Application of NGE MPLS services and control plane encryption



In this example, NGE is applied to the various services and control plane traffic types on the 7705 SAR-Hm, an LTE/3G-capable IP/MPLS router to extend mission-critical services over wireless, and the Nokia VSR Appliance (VSR-A) head-end node. NGE is enabled on the three main traffic types to provide end-to-end security across the wireless provider's network.

As shown, NGE is enabled using a green key group on a GRE-SDP to protect VLL and VPLS Layer-2 based services that transit the network using that SDP. The GRE-SDP or multiple SDPs could be destined towards:

- Other 7705 SAR-Hm nodes reachable over wireless to provide M2M and IoT connectivity
- The VSR head-end node, to terminate services on it
- Other 7705 SAR, 7750 Service Router (SR) and VSR nodes past the VSR head-end node.

In Figure 10, NGE is also enabled on the VPRN by configuring a pink key group for the VPRN. All nodes participating in the pink VPRN can send any-to-any traffic between themselves without the need to configure a mesh of tunnels between them. Traffic can again travel between wireless nodes for IoT applications or back to the head-end node that also participates in the VPRN.

Finally, in the Figure 10 example, NGE is enabled on the wireless interface (packet data network [PDN] interface or router interface) by configuring a blue key group on the wireless interface. This creates an NGE domain over wireless for all 7705 SAR-Hm nodes that need to establish a control plane between themselves or to the head-end node and exchange routes or provide IP/MPLS signaling and control. All control plane traffic, such as BGP, BFD, T-LDP, etc., is NGE encrypted when exiting the wireless interface and must be NGE encrypted when received on the same interface.

Figure 11 shows the packet format and flows that might be expected in such a network.

Figure 11. Protocol stack of NGE MPLS services and control plane encryption

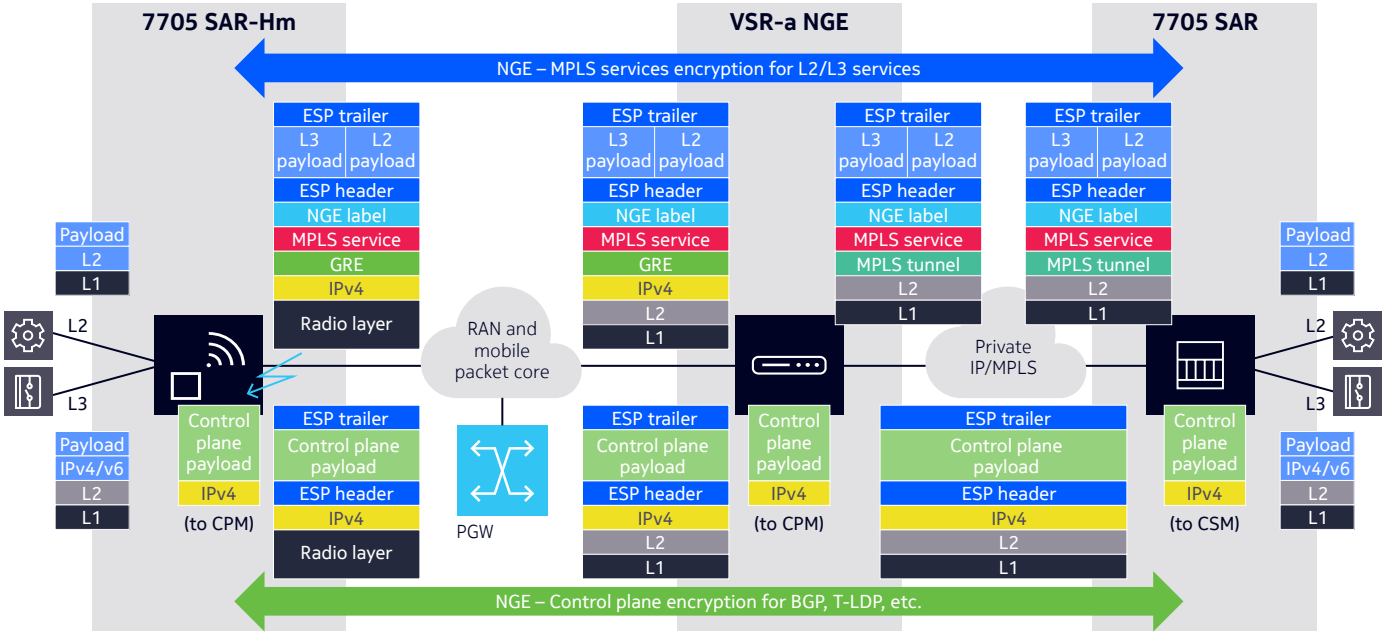


Figure 11 shows Layer 3 GRE-MPLS-based services in the wireless domain while providing a seamless transition to a private IP/MPLS network that uses LSP tunnels to continue carrying the NGE encrypted traffic for a complete end-to-end security solution.

4 NGE in-depth view

This section is divided into three main areas:

- Encryption key management
- IP/MPLS services encryption
- NGE domains.

4.1 Encryption key management

Nokia NGE encryption key management consists of:

- Nokia NSP service, control and key management
- Nodal key management.

4.1.1 Nokia NSP service, control and key management

The NSP provides three main functions when using NGE: network services configuration, IP/MPLS control plane configuration, and NGE key management. With full knowledge of which nodes are providing which services and control plane, the NSP easily determines which nodes require which keys to be used for a specific security domain.

Pre-shared keys are generated internally on the NSP using a strong random number generator with high entropy. When downloading the encryption keys to the nodes, the NSP opens a new secure shell (SSH) session to each node and installs the keys.

The NSP uses a default user ID or an operator-defined user ID that is specifically assigned for NGE key group updates. Activities by either ID can be tracked through regular user accounting and logging methods for security audit purposes, which may be a requirement driven by internal processes or external regulations such as NERC-CIP [3] audits.

The SSH sessions protect the keys during transport using a strong AES256 encryption algorithm, and the nodes store the NGE keys internally in a secure manner.

The NSP computes a simple CRC32 checksum for each key in use. To ensure that each node in the network has the correct set of keys, the NSP polls the nodes for the CRC checksums. When all the nodes report the correct checksum, the NSP knows that all the nodes are synchronized with the correct keys.

The NSP ensures that newly generated keys do not have CRC32 collisions with the previous keys used. If a collision is detected, the NSP skips to new key values that do not collide with the previous CRC32 values.

An advantage of using SSH for NGE key download is that it provides an extra layer of security in addition to NGE-secured transport tunnels. A new SSH session is opened on every key update. The pre-shared keys are downloaded over an in-band communications channel; for example, through a dedicated management VPRN service configured to use NGE. This way, the key download process can have two layers of security: the SSH session itself and the NGE-encrypted services carrying the SSH session.

This approach presents a significant challenge to a potential attacker, who needs to be able to decode the NGE tunnel and the SSH session at the same time. The added burden of decoding the SSH session before the next re-keying interval in a short time makes this task impossible without access to extraordinary compute resources.

Using in-band management in the described manner is not mandatory but is an option for additional security during key download.

After an NGE domain is secured, the NSP can use the encryption in this security domain for key updates. This greatly reduces the concerns associated with man-in-the-middle types of attacks.

After NGE is enabled, at no point can certificates or any other sensitive information that is normally transmitted as clear text (for example, when handshaking of the SSH session occurs) be intercepted by a man-in-the-middle because all certificates and other sensitive information will be hidden in encrypted NGE packets.

Even after a network outage, NGE is designed to maintain its encrypted services and SSH is constantly protected with an additional level of security.

4.1.2 Nodal key management

When the NSP downloads keys to a node, they are stored securely in permanent storage on the node. It is essential for NGE to maintain the operation of encrypted services during any type of network outage. Mission-critical traffic relies on the high availability of the network used to carry it. However, it is essential to prevent security-related control plane traffic from disrupting user traffic (encrypted or unencrypted) even though security is vital.

In traditional encryption solutions, when a network outage occurs, the security control plane needs to be re-established by re-handshaking and re-configuring itself to key servers that may be overburdened during network fluctuations. These added strains can delay the restoration of mission-critical traffic.

Also, for traditional approaches that rely on control plane connectivity to a key server, in case of lost connectivity to a key server, the traffic is immediately impacted and may be lost until connectivity to the key server is re-established. This is not the case with NGE—because NGE was designed to maximize both service availability and the efficiency of its security operation.

Because keys are securely stored on the node, at no time is there any risk that the traffic in the NGE domain will be impacted. If a network outage occurs, the nodes can immediately start using the locally stored keys to maintain traffic uptime in the secured domain. If connectivity to the NSP is lost, there is no impact to the keys that are already in the network because no control plane is running between the NSP and the nodes. NGE was designed to optimally balance the continuous requirement for security while maximizing mission-critical traffic uptime. Once the connectivity to NSP is re-established, the NSP will engage in a re-keying procedure.

4.1.3 NGE re-key procedure and operation

The NSP provides a network-wide re-keying procedure either per key group or for all key groups at the same time. The network operator has a choice: each key group can have its own re-keying interval or one global re-keying interval can be defined for all key groups.

As is typical with security functions, the NSP uses a standard “make-before-break” approach to the re-keying procedure. The steps are as follows.

Step 1: The NSP generates a new set of keys internally using a strong random number generator and ensures that the associated CRC checksums are unique (different from the previous keys used). The NSP then opens a new SSH session to each node and downloads the new keys to all nodes in the key group domain.

Step 2: After the domain-wide key update is finished, the NSP verifies the update by comparing the checksum in each node to the checksum stored in the NSP itself.

Step 3: The NSP instructs each node to start using the new key for outbound traffic. While this process is taking place, nodes are able to decrypt messages using either the old or new key. As a result, even though not every node switches at exactly the same moment, there is no traffic loss during the transition from the old key to the new one.

Step 4: The NSP confirms that all nodes are now using the new key. After all the nodes in the key group are confirmed to have activated the new key, the NSP deletes the old keys in all nodes in the domain.

4.2 IP/MPLS services encryption

NGE provides the ability to encrypt MPLS services using encryption key groups applied to services constructs. Operators can use the NSP to apply key groups to enable:

- SDP encryption
- VPRN encryption.

By applying key groups to SDPs and VPRNs, the list of encrypted services that is supported by NGE includes:

- VLLs: E-pipes and C-pipes
- VPRN services and IES using Layer 3 spoke-SDP termination
- VPLS using spoke and mesh SDPs
- Routed VPLS into a VPRN or IES
- MP-BGP-based VPRNs.

For services that use SDPs, tunnels can be either MPLS LSPs (RSVP-TE or LDP static LSP), BGP or GRE tunnels.

For VPRN services that use MP-BGP, the auto-bind feature is supported using LDP, GRE, RSVP-TE or MPLS (LDP or RSVP-TE).

As mentioned in Section 3.2, “NGE MPLS services packet formats”, NGE adds a global encryption label to the label stack for encrypting MPLS services and is used to identify NGE packets that are encrypted. The global encryption label is added to the bottom of the stack. This allows LSR, ABRs/ASBRs and other routing elements to forward NGE packets without the need understand NGE or to even know that the content of NGE MPLS packets is encrypted.

When a destination provider edge (PE) such as the Nokia 7705 SAR—which needs to have full visibility at the service layer—receives NGE packets, it will check whether an encryption label was employed. If so, it will then decrypt the packets as required.

4.2.1 Service distribution point encryption (VLLs, VPLS, VPRNs)

Nokia IP/MPLS routers use SDPs to make configuration and management of MPLS-based services easy and flexible. SDPs are associated with tunneling MPLS LSPs, including static LSPs, LDP LSPs and RSVP-TE LSPs.

In addition to MPLS-based tunneling, GRE-based tunnels can also be configured as SDPs for transport of MPLS-based services over Layer 3 IP networks.

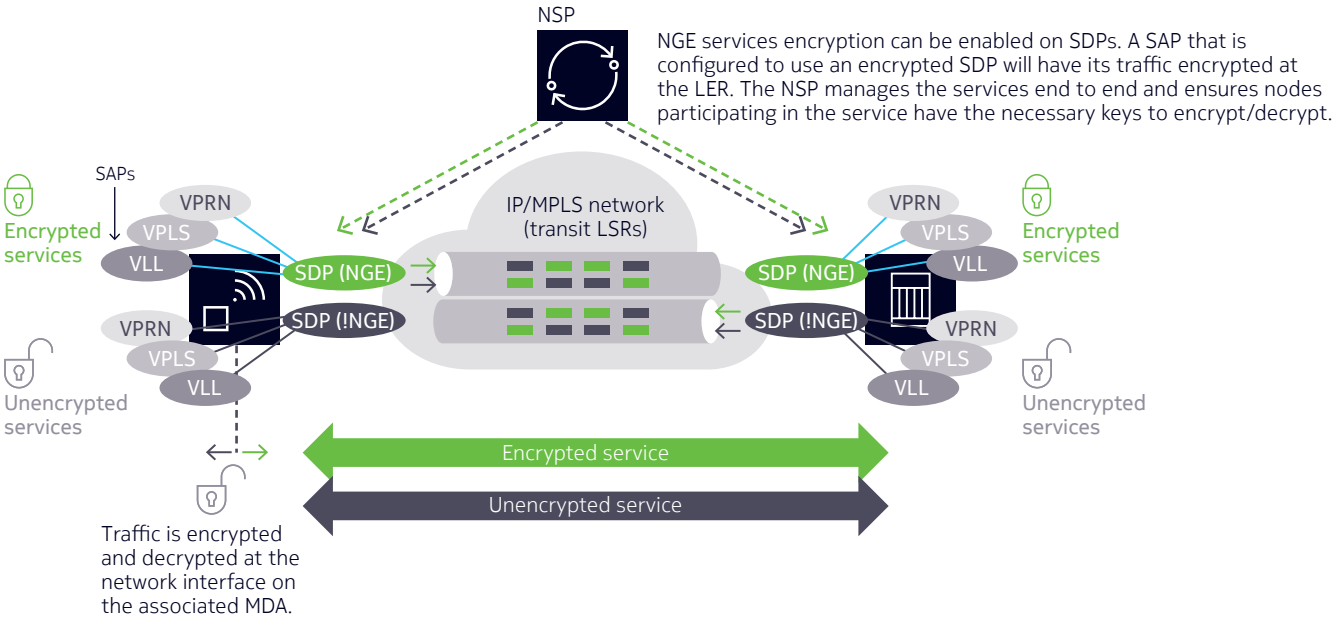
Multiple SDPs can share the same LSP. The purpose of defining SDPs is to aggregate a set of access-level services to be carried across the IP/MPLS network using LSPs configured on the SDP. These access-facing services are defined as service access points (SAPs), and they are mapped to SDPs to provide the transport between two PE routers.

NGE is configurable on the SDPs themselves by setting the key group security domain that the SDP is to be associated with. After the SDP has been configured with a key group value, any SAPs that are configured for that SDP will have traffic encrypted and authenticated using the keys and algorithms configured for that key group. The NSP ensures that both routers associated to a particular SDP have the key group information that enables NGE for the SDP. Figure 12 illustrates this process.

In the figure, the green SDP has been configured with NGE because a key group is configured on the SDP. Any VPRN-, VPLS- or VLL-based service that is associated with the light-blue SDP will have its traffic encrypted over the transport LSPs for the green SDP.

Both encrypted and unencrypted traffic can share the same LSPs. In Figure 12, the gray SDP is not configured with an NGE key group. As a result, any VPRN-, VPLS- or VLL-based services that are configured with the dark-gray SDP would not be encrypted.

Figure 12. SDP encryption



This way, transport LSPs can carry both encrypted and unencrypted services, possibly optimizing hardware dedicated for encryption to only traffic that requires the additional security. This capability adds a great deal of flexibility to the types of services that can be encrypted using NGE while minimizing the maintenance of the MPLS network because the LSPs and tunnels used for transport are not impacted or modified when enabling or disabling NGE.

The types of services and traffic that use SDP encryption include:

- VPRNs or IESs that use spoke SDPs
- VPLS-based services that use spoke or mesh SDPs
- Ethernet pseudowires (E-pipes) and constant-bit-rate pseudowires (C-pipes) such as serial links
- E1/T1 circuits
- G.703 co-directional
- C37.94
- FXS/FXO
- E&M
- Other legacy interfaces.

4.2.2 VPRN encryption

NGE supports any-to-any group-based encryption for VPRN-based services. VPRNs can also use SDPs to provide connectivity of services between PE routers, as already discussed.

This section focuses on how NGE can be enabled on the VPRN service directly where the Nokia Service Router Operating System (SR-OS) auto-bind feature is used to select transport LSPs to carry the encrypted traffic.

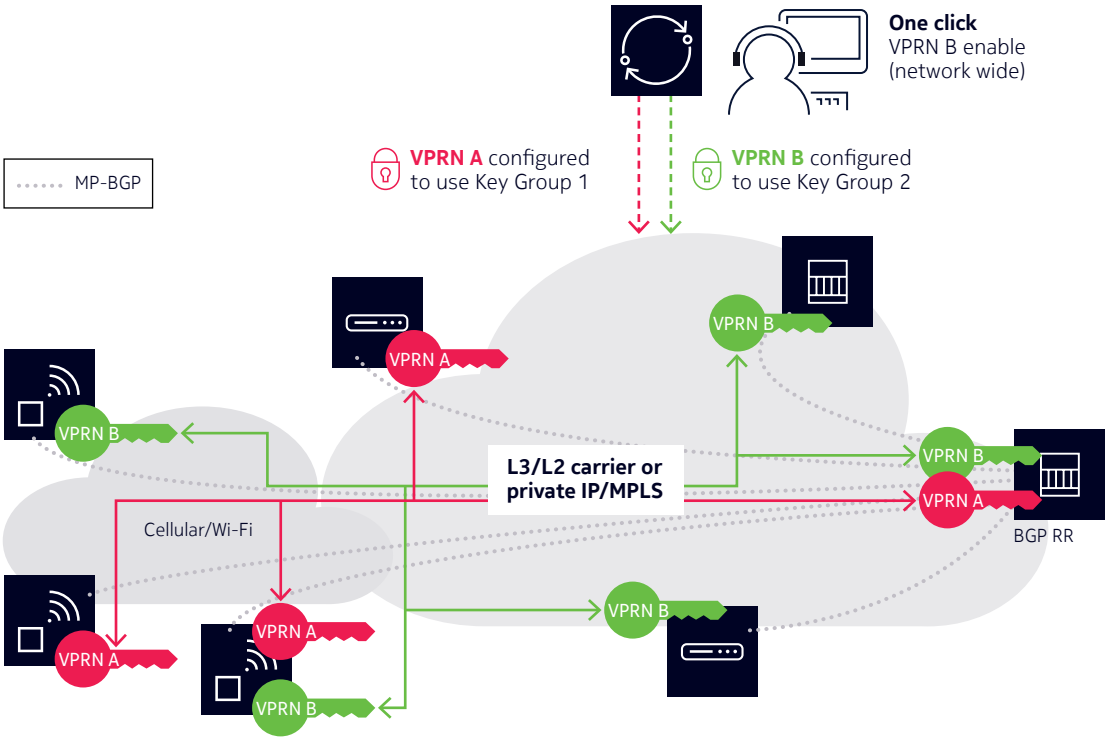
Nokia routers use a convenient method of binding Layer 3 VPRN services to LSPs or GRE tunnels based on the reachability of other routers in the VPRN as advertised in MP-BGP. Typically, nodes participating in a VPRN establish BGP sessions to an RR to learn routes to other nodes in the VPRN. Any node can reach any other node using multi-point to multi-point communication.

NGE can be directly applied to the VPRN service in a single operation to enable all VPRN traffic to be encrypted. The operator simply assigns a specific key group for that VPRN on the NSP. The key group information needed to enable NGE is then downloaded to all nodes in the VRPN.

After all the key groups have been downloaded and verified, each node is capable of encrypting and decrypting traffic in the VPRN by using the keys in the associated key group. The NSP then proceeds to enable NGE on each node as required until all nodes in the VPRN have been NGE-enabled for the VPRN.

Figure 13 shows an example of VPRN encryption over a wireless network using cellular or WLAN that includes NGE nodes connected to a Layer 2 or Layer 3 service provider or a private IP/MPLS network. There is no need to establish PE-to-PE security tunnels or meshes of security tunnels because the NSP downloads the group keys to the nodes participating in the VPRN after the operator enables NGE with one click on the VPRN. The VPRN traffic is never impacted when enabling or disabling encryption on the VPRN.

Figure 13. VPRN encryption



VPRNs can also be configured to use Layer 3 spoke SDPs. A Layer 3 spoke SDP is used to specifically assign MPLS tunnels to VPRN services without having the system choose the tunnels automatically, as is the case when using the auto-binding function. Using layer 3 spoke SDPs to assign MPLS tunnels to VRPRN services is convenient for connecting other routers that are not NGE-capable or NGE-aware to the VPRN. Doing this allows interworking and extending services in the same VPRN outside of the NGE domain.

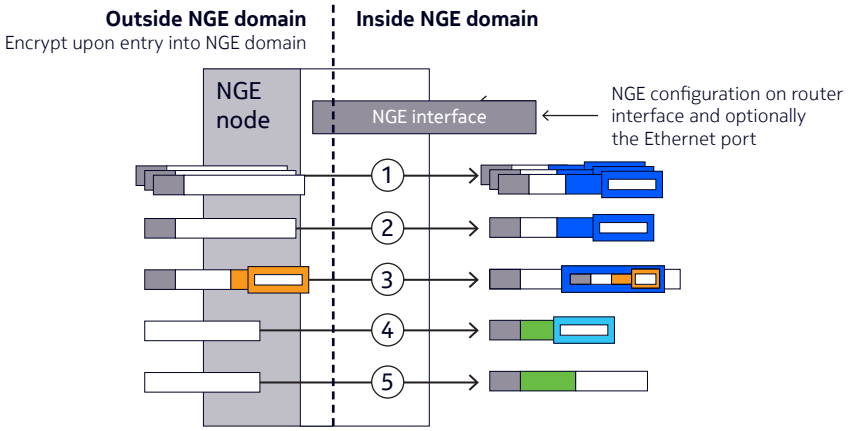
Using Layer 3 spoke SDP configuration in combination with auto-binding extends the flexibility of NGE. In addition, NGE provides simple rules for how to configure a combination of encrypted and unencrypted service in the same VPRN.

4.3 NGE domains

As summarized in Section 3.1, “NGE components”, NGE domains are created when a group of nodes and their router interfaces form a network that uses a single key group to create a security domain. NGE domains are created by enabling router interface encryption on router interfaces that need to participate in the NGE domain. The associated Ethernet ports where router interface encryption is enabled may also optionally be NGE-enabled to protect the sensitive Layer 2 protocols, IS-IS and LLDP.

The NSP assists operators in managing both router interface Layer 3 encryption and Layer 2 Ethernet port encryption when forming NGE domains. When operators add router interfaces to an NGE domain, they are automatically enabled with NGE using the NGE domain’s key group and are considered to be inside that NGE domain. Router interfaces that are not added to an NGE domain are considered to be outside the NGE domain (see Figure 14).

Figure 14. Traversing an NGE domain



In the figure, traffic is encrypted when entering the NGE domain using the key group configured on the router interface, and is decrypted when exiting the NGE domain. Traffic may traverse multiple hops before exiting the NGE domain, yet decryption occurs only on the final node when the traffic exits the NGE domain.

Various traffic types are supported and encrypted when entering the NGE domain, as shown by the following items on the NGE node in the figure.

Item 1. Self-generated packets: These packets include all types of control plane and management packets, including OSPF, BGP, LDP, SNMPv3, SSH, ICMP, RSVP-TE and 1588.

Item 2. User Layer 3 packets: Any Layer 3 user packets that are routed into the NGE domain from an interface outside of the NGE domain are encrypted.

Item3. IPsec packets: IPsec packets are NGE encrypted when entering the NGE domain to ensure that the IPsec packet’s security association information does not conflict with the NGE domain.

GRE-MPLS based service traffic consists of Layer 3 packets. Router interface NGE is not applied to these types of packets. Instead, they use service-level NGE for encryption to avoid double-encrypting these packets and impacting throughput and latencies. The two types of GRE-SDP packets that can enter the NGE domain are shown by items 4 and 5 in the figure.

Item 4. GRE-SDP MPLS packets (SDP or VPRN) with service-level NGE enabled: These encrypted packets use the key group that is configured on the service. The services key group can be different from the key group configured on the router interface where the GRE-MPLS packet enters the NGE domain.

Item 5. GRE-MPLS packets (SDP or VPRN) with NGE disabled: These packets are not encrypted and can traverse the NGE domain in clear text. If these packets require encryption, SDP or VPRN encryption must be enabled.

Creating an NGE domain from the NSP requires the operator to determine the type of NGE domain being managed. This will indicate whether NGE gateway nodes are required to manage the NGE domain.

The two types of NGE domains are:

- Private IP/MPLS network NGE domain
- Private over intermediary network NGE domain.

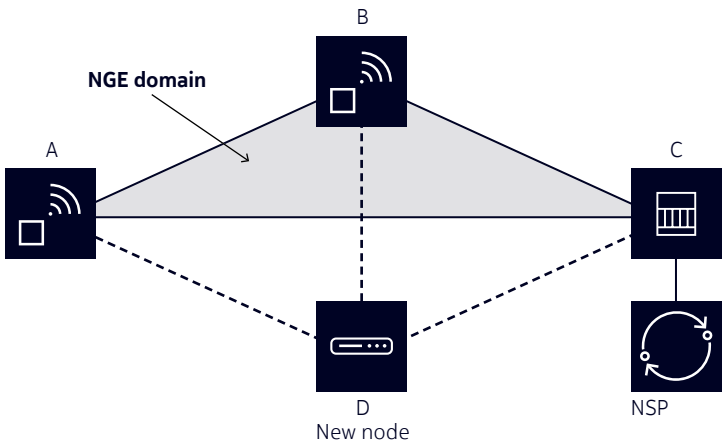
4.3.1 Private IP/MPLS network NGE domain

In a private IP/MPLS network NGE domain (see Figure 15), all interfaces are owned by the operator and there is no intermediary service provider needed to interconnect nodes. Each interface is a point-to-point private link between private nodes. When a new node is added to this type of NGE domain (Node D in Figure 15), the links that connect the existing nodes in the NGE domain (Node A, Node B and Node C) must be enabled with NGE router interface encryption for the new node to join the NGE domain.

Links from the new node to the existing nodes are enabled one at a time. The NSP provides tools that simplify adding nodes to the NGE domain and enabling NGE on their associated interfaces.

In this type of NGE domain, each interface is a direct link between two nodes and is not used to communicate with multiple nodes over a broadcast medium offered by an intermediary network. Also, there are no NGE gateway nodes required between the NSP and new nodes entering the NGE domain.

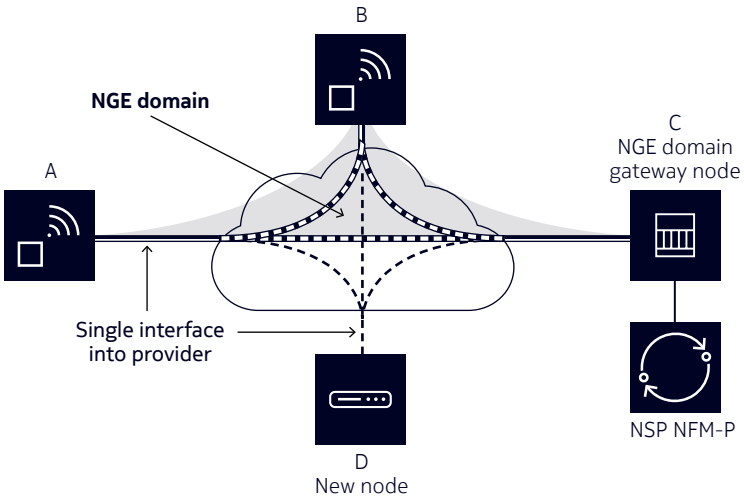
Figure 15. Private IP/MPLS network NGE domain



4.3.2 Private over intermediary network NGE domain

The second type of NGE domain is a private IP/MPLS network that traverses an intermediary network NGE domain, in which the intermediary network is used to interconnect nodes in the NGE domain using a multi-point to multi-point service (see Figure 16). The intermediary network is typically a service provider network that provides a private IP VPN service or a private VPLS used to interconnect a private network that does not mimic point-to-point links.

Figure 16. Private over intermediary network NGE domain



Private over intermediary network NGE domains have nodes with links that connect to a service provider network where a single link can communicate with multiple nodes over a Layer 3 service such as a VPRN or a Layer 2 service such as VPLS.

In Figure 16, Node A has NGE enabled on its interface with the service provider and uses that single interface to communicate with Nodes B and Node C, and eventually with Node D when it has been added to the NGE domain. This type of NGE domain requires the recognition of NGE gateway nodes that allow the NSP to reach new nodes that enter the domain. Node C is designated as a gateway node.

When Node D is added to the NGE domain, it must first have the NGE domain key group downloaded to it from the NSP. The NSP creates what is known as an NGE exception access control list (ACL) on the gateway node, C, to allow specific communication with Node D using SNMPv3 and SSH through the NGE domain. IP exception ACLs allow for specific encryption control on router interfaces that have NGE enabled.

After the key group is downloaded, the NSP enables router interface encryption on Node D's interface with the service provider. Node D is now able to participate in the NGE domain. The NSP also automatically removes the IP exception ACL from Node C when Node D enters the NGE domain.

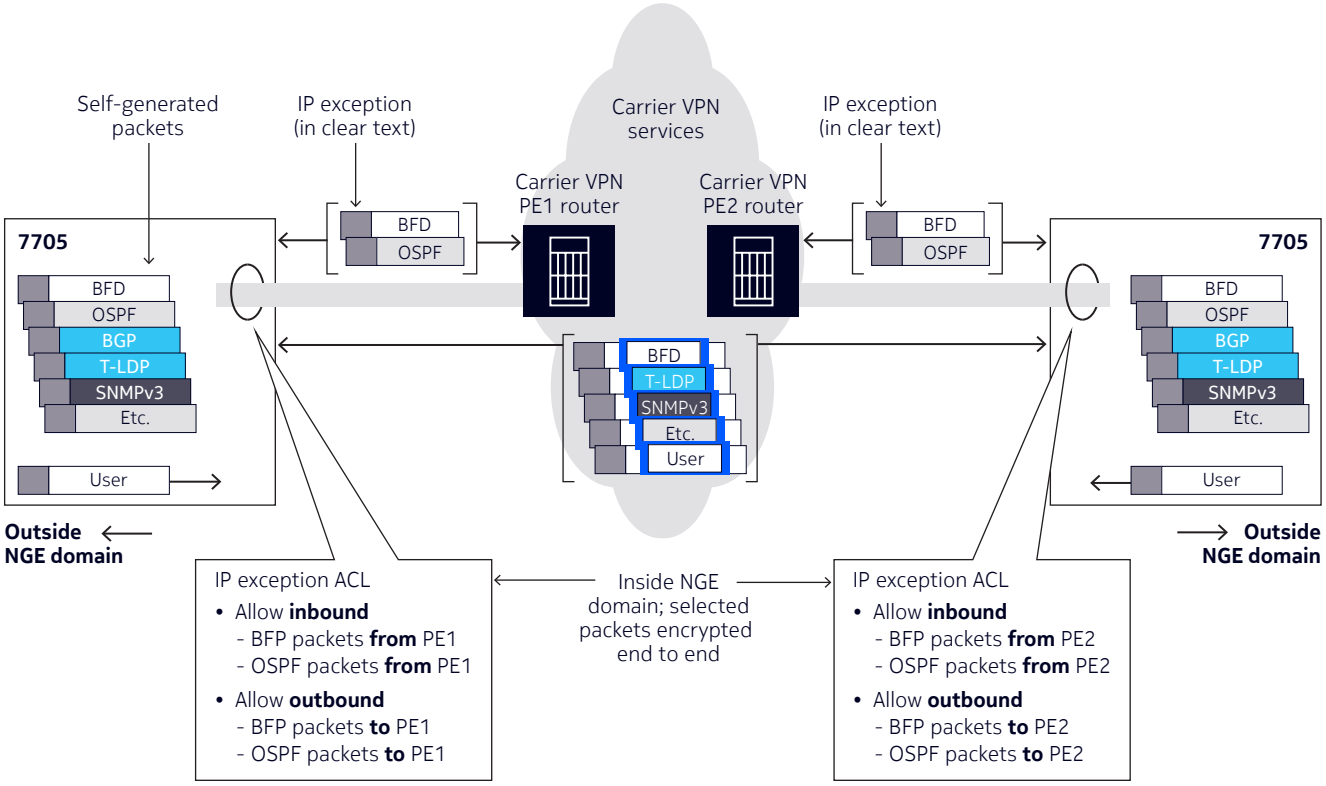
The next section describes the concept of IP exception ACLs used in NGE domains.

4.3.3 NGE domain exception ACLs

In some cases, Layer 3 packets may need to cross the NGE domain in clear text even though the NGE domain has been established; for example, when an NGE-enabled node needs to peer with a non-NGE-capable node to exchange routing information. This can be accomplished by using a router interface NGE exception filter applied on the router interface for the required direction, inbound or outbound.

This concept is illustrated in Figure 17.

Figure 17. NGE IP exception ACLs



IP exception ACLs are convenient if specific traffic flows to neighbor peering routers that are not NGE enabled need to be sent without encryption. For example, it may be necessary to peer with a service provider router to exchange routes using OSPF and provide a BFD function, yet all other protocol information between the private NGE nodes must be secured. In this case, OSPF and BFD to the peering router can be NGE-disabled using an exception ACL while all other traffic is protected.

NGE provides a simple yet flexible way for operators to choose which packet flows require NGE and which do not. The NSP assists the operator in managing the IP exception ACLs, where they are applied, and when they are enabled or disabled.

5 NGE benefits

Nokia NGE, with its next-generation techniques for encryption and authentication of a wide variety of MPLS-based services and associated control and management planes, provides significant benefits to users in the areas of simplicity, flexibility, robustness and performance.

5.1 Simplicity

NGE's service plane- and control plane-aware encryption is simple to configure and operate thanks to the NSP's inherent network-wide visibility of services and control plane. NGE's ability to seamlessly introduce a security overlay onto existing MPLS network architectures and designs allows operators to

maintain operations and maintenance functions such as resiliency, QoS and OAM while adding security to their networks. With this overlay approach to encryption, networks remain scalable, highly available and functionally equivalent without the compromises that other solutions impose.

Core routers can switch and route NGE packets seamlessly, maintaining interoperability at locations where they are deployed as LSRs, ABRs/ASBRs and pseudowire switching PE points. This results in a powerful end-to-end security framework that can be applied across the entire IP/MPLS network.

NGE is a highly scalable solution that avoids large meshed tunnel configurations and complex topologies. It reuses the MPLS network planning and resource allocations associated with the IP/MPLS user and control planes, and can adapt to many diverse types of network topologies and architectures.

The positive business impact on operational savings is directly driven by NGE's simplicity and overlay approach, freeing network planners to focus on maximizing services first, without restrictions or compromises caused by security.

5.2 Flexibility

NGE provides the flexibility to choose the IP/MPLS services and control plane items that require security. NGE does not impose any bias towards the types of traffic that can be encrypted: all network traffic types that an operator may find a good candidate to be protected in their IP/MPLS network can be protected and secured with NGE. The overall security framework can be tailored to address the security requirements of the network.

NGE provides the means to secure traffic in private IP MPLS networks or when traffic is crossing third-party service provider networks. NGE provides an end-to-end, multi-point to multi-point solution over these third-party service providers that includes cellular/wireless providers supporting MTC (M2M and IoT) applications, Layer 3 IP VPN providers, and Layer 2 VPLS or VLL service providers.

NGE provides additional functionality to create security partitions using key groups, allowing a hierarchical and tiered approach to a security architecture. For NGE domains, an operator can selectively choose traffic flows to be encrypted using IP exception ACLs on a per-flow basis.

5.3 Robustness

NGE robustness was designed and built into the solution. At the heart of NGE, the NSP delivers highly robust key management with hitless re-keying procedures and hitless encryption enable/disable operations for both services and control plane encryption.

Because key management and synchronization is performed centrally, no additional requirements related to key management functions are imposed on routers. As a result, there is minimal control plane overhead and maintenance required for network-wide encryption. There is also no risk to traffic based on an encryption control plane failure. During network outages or disruptions that cause reachability to the NSP to falter, traffic is never dropped, and encryption functions never halt.

NGE nodes will always forward their encrypted mission-critical traffic, without exception.

5.4 Performance

NGE provides high performance and comprehensive encryption solutions for all types of Layer 2 and Layer 3 services—without requiring conversion to IP and without adding extra overhead that potentially can increase latency (which is the usual case with IP encapsulation). All services are encrypted in MPLS packets without the need for further modification. For Layer 3 services, there is complete Layer 3 privacy because all IP headers are hidden from explicit inspection in the MPLS payload.

For control plane encryption in NGE domains using router interface level encryption, packets reuse IPsec transport mode, which does not add extra overhead and complexity to packets, thereby optimizing this aspect of the NGE solution.

NGE packets are encrypted and decrypted only once—at their origin and at their destination. This ensures low end-to-end latency and high throughput. Bandwidth consumption related to encryption overhead is lower than with tradition encryption because packet overhead for NGE is lower than with traditional approaches. (For example, NGE uses a 4-byte encryption label rather than an additional IPsec tunnel and GRE headers.) Lower overhead can save considerable bandwidth on constant bit rate services that have small packet sizes, including TDM pseudowires, teleprotection and services using SCADA-related protocols.

6 Conclusion

Cyber security is a growing concern for our society at large and for network operators in particular. Operators need to be proactive in evaluating their security risks, and then formulate their security policy and plan accordingly.

Nokia NGE is an innovative security tool that provides comprehensive protection for both IP and non-IP traffic seamlessly at the MPLS and IP layer with minimal key management overhead and complexity. It is an ideal solution for operators who are looking for an advanced security solution not available with traditional methods to help secure their mission-critical networks.

To learn more about Nokia Network Group Encryption, visit the Cyber Security for Power Utilities web page.

7 Acronyms

ABR	area border router
ACL	access control list
ASBR	autonomous system border router
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
CCTV	closed circuit television
CBC	Cipher Block Chaining
CPE	customer premises equipment
CPM	Converged IP Messaging
CSM	Control Switch Module
CTL	Control
DA	distribution automation
DMVPN	dynamic multipoint VPN
E&M	ear and mouth (signaling)
ESP	Encapsulating Security Payload
FAN	field area network

FXO	Foreign eXchange Office
FXS	Foreign eXchange Subscriber
GDOI	Group Domain of Interpretation
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
IED	intelligent electronic device
IES	internet enhanced service
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IoT	Internet of Things
IP	Internet Protocol
IPsec	IP security
IS-IS	Intermediate System-to-Intermediate System
LAN	local area network
LDP	Label Distribution Protocol
LER	label edge router
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LMR	land mobile radio system
LSP	label switched path
LSR	label switched router
LTE	long term evolution
M2M	machine-to-machine
MACsec	Media Access Control security
MDA	7750 Service Router Media Dependent Adapter
MP-BGP	Multiprotocol BGP
MPLS	Multiprotocol Label Switching
MTC	machine type communication
NFM-P	Network Functions Manager for Packet
NGE	network group encryption
NOC	Network Operations Center
NSP	Nokia Network Services Platform

OAM	operations, administration and maintenance
OSPF	Open Shortest Path First
PDN	packet data network
PGW	Packet Data Network Gateway
QoS	Quality of Service
RAN	radio access network
RSVP-TE	Resource Reservation Protocol – Traffic Engineering
RTU	remote terminal unit
SAP	service access point
SAR	Nokia 7705 Service Aggregation Router
SCADA	supervisory control and data acquisition
SDP	service distribution point
SNAP	Standard Network Access Protocol
SNMP	Simple Network Management Protocol
SPI	security parameter index
SSH	Secure Shell Protocol
TDM	time division multiplexing
T-LDP	targeted LDP
VLAN	virtual local area network
VLL	virtual leased line
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network
VPWS	virtual private wireless service
VSR	Nokia Virtualized Service Router
VSR-a	Nokia VSR Appliance
WLAN	wireless LAN

8 References

1. IEEE 802.1AE: IEEE Standard for Local and Metropolitan Access Networks: Media Access Control (MAC) Security. 2006. findstds/standard/802.1AE-2006.html
2. IETF. RFC 5996. Internet Key Exchange Protocol Version 2 (IKEv2). September 2010. http://www.ietf.org/rfc/rfc5996.txt
3. IETF. RFC 4302. IP Authentication Header. December 2005. http://www.ietf. org/rfc/rfc4302.txt
4. IETF. RFC 4303. IP Encapsulating Security Payload (ESP). December 2005. http://www.ietf.org/rfc/rfc4303.txt
5. IETF. RFC 6407. The Group Domain of Interpretation. October 2011. http://www. ietf.org/rfc/rfc6407.txt
6. Nokia Mission-Critical Communications Networks Solution for Power Utilities: Attaining NERC CIP Version 5 Reliability Standards Compliance (application note). July 2016. https://resources.ext.nokia.com/asset/181741
7. Nokia 7705 Service Aggregation Router: Security Overview for Power Utilities (application note). 2016. https://resources.ext.nokia.com/asset/184431
8. Nokia 7705 Service Aggregation Router: Security overview for mission-critical networks (application note). 2016. https://resources.ext.nokia.com/asset/174129

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: (March) CID187584