TECHNOLOGY WHITE PAPER

Alcatel-Lucent network group encryption

Seamless encryption for mission-critical networks

As mission-critical communications networks adopt IP/MPLS, security is a key consideration. Legacy services that have not yet been fully converted to IP must still be supported on a converged network. Also, some of the more modern mission-critical protocols are not IP-based. To ensure that communications are secured and confidentiality is maintained, Alcatel-Lucent network group encryption provides the essential seamless encryption to protect mission-critical networks.

Alcatel·Lucent

Table of contents

1 Introduction / 1

2 NGE overview / 1

2.1 Motivation / 2

2.2 NGE components / 5

2.3 Bits and bytes / 7

3 NGE key management / 8

3.1 Alcatel-Lucent 5620 SAM service and key management / 8

3.2 Nodal key management / 9

3.3 NGE network re-keying procedure / 10

4 Encrypted services / 11

4.1 Service distribution point encryption / 11

4.2 VPRN-level encryption / 13

5 NGE benefits / 14

5.1 Flexibility / 14

5.2 Robustness / 14

5.3 Performance / 14

6 Conclusion / 15

7 Acronyms / 15

8 References / 15

1 Introduction

Network operators worldwide recognize IP/Multiprotocol Label Switching (MPLS) as a key technology that supports mission-critical applications by merging various types of networks and services onto a single unified infrastructure. They understand that when offering services over a single or converged network, the end-to-end network must be scalable, flexible, provide high availability and properly prioritize traffic and services based on application requirements and Quality of Service (QoS) objectives.

As a result of the early adoption and success of IP/MPLS in carrier networks, the technology's importance is now being adopted by vertical markets with mission-critical networks, including utilities, oil and gas, mining, transportation, all levels of government, defense and enterprises.

In many cases the variety and types of network traffic require the "MP" portion of MPLS to live up to its name because legacy services that have not yet been fully converted to IP must still be supported on a converged network. Also, some of the more modern mission-critical protocols, such as Generic Object Oriented Substation Event (GOOSE) messaging, use a pure Layer 2 construct that does not always rely on an IP layer for transport. MPLS, however, is still capable of carrying such traffic. The mission-critical networks that often operate the communications of critical industrial and public infrastructures are experiencing a great deal of scrutiny from regulatory bodies to ensure that communications are secured from malicious attacks and confidentiality is maintained.

This paper discusses a new technique for encrypting and authenticating mission-critical MPLS traffic. Alcatel-Lucent network group encryption (NGE) provides a powerful, highly flexible and scalable group-based method of adding privacy and confidentiality (encryption and authentication) to any type of traffic transported over an MPLS network.

Alcatel-Lucent is a market leader in IP/MPLS technology, with a portfolio of products that offer a complete solution to implement end-to-end seamless MPLS networks. As part of that solution, a variety of security functions and features are available to secure network traffic and infrastructure. NGE provides a powerful, highly versatile and scalable group-based method of encryption and authentication that can be applied to any traffic type carried over IP/MPLS networks. It is an important component of the Alcatel-Lucent security feature set[1] for securing mission-critical networks.

2 NGE overview

To provide an overview of NGE this section is divided into three main areas:

- Motivation: The drivers to use a new technical approach for group-based encryption solutions over IP/MPLS networks
- Components: The building blocks that comprise the Alcatel-Lucent NGE solution
- Bits and bytes: The constructs that make up an NGE formatted message

The following sections discuss each of these areas.

1 For details, see *Alcatel-Lucent Mission-Critical Communications Networks Solution for Power Utilities: Attaining NERC CIP Version 5 Reliability Standards Compliance* (http://resources.alcatel-lucent.com/asset/181741), Alcatel-Lucent 7705 Service Aggregation Router Security Overview for Power Utilities (http://resources.alcatel-lucent.com/asset/184431), and Alcatel-Lucent 7705 Service Aggregation Router Security Overview for Mission-Critical Network (http://resources.alcatel-lucent.com/asset/174129).

2.1 Motivation

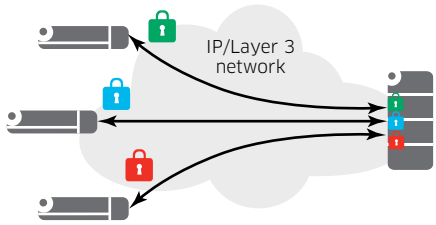
The drivers to use a new technical approach for encryption over IP/MPLS networks are the shortcomings of traditional encryption and authentication methods and the flexibility that NGE provides.

2.1.1 Shortcomings of traditional encryption methods

The traditional methods of adding encryption and authentication to 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 for point-to-point communication tunnels over an insecure medium (see Figure 1). It was not initially designed for any-to-any communications. However, it has nonetheless been adopted for any-to-any communications, for example by setting up meshes of point-to-point links to achieve the same result.

The newer Group Domain of Interpretation (GDOI) specifications[2] have made transporting Layer 3 services in an any-to-any network feasible. However, there is still the fundamental point-to-point nature of IPSec's control plane.

Figure 1. IPSec point-to-point connectivity and control plane



Both IPSec and GDOI use the Internet Key Exchange (IKEv2) protocol[3], originally defined in 1998, to efficiently distribute shared encryption keys between two routers. This has worked well for securing these point-to-point links. However, when creating meshes of links for any-to-any connectivity, concerns exist about the ability of IKE to manage these meshes of tunnels and links.

When implementing GDOI, IKE runs on a key server which is typically another router in the network. The IKE control plane sessions need to be managed between key servers and group members (other routers). Scaling the IKE control plane up to support large numbers of group members remains the biggest challenge since the overhead added to router resources for these IKE sessions can quickly become restrictive. Also when trying to scale networks for encryption, Public Key Infrastructure (PKI) and Pre-shared Key (PSK) handshake bottlenecks can arise that might impact recovery from network outages. Finally, having a control plane for encryption that is separate from the control plane used to operate an IP/MPLS network can lead to added risk of topology inconsistency. This could lead to issues with routing reachability of key servers, necessary to maintain IKE sessions in order to keep up tunnels and GDOI key synchronization.

These scaling, setup and control plane management issues of encryption plus some of the service constraints that current network encryption solutions impose on the network motivate network operators to search for alternatives.

2 IETF. RFC 6407: *The Group Domain of Interpretation*, October 2011. http://www.ietf.org/rfc/rfc6407.txt
3 IETF. RFC 5996: *Internet Key Exchange Protocol Version 2 (IKEv2)*, September 2010, http://www.ietf.org/rfc/rfc5996.txt

Alcatel-Lucent has introduced NGE to help address these concerns by:

- Minimizing the additional control plane running in the network that is needed to operate secure privacy and confidentiality functions using encryption and authentication techniques
- Minimizing the configuration and operational complexity associated with adding encryption to services
- Maximizing the uptime of services using encryption and authentication without the additional worry that link outages or nodal (router) failures will cause traffic failure
- Minimizing latency and performance bottlenecks incurred with encryption while maximizing throughput

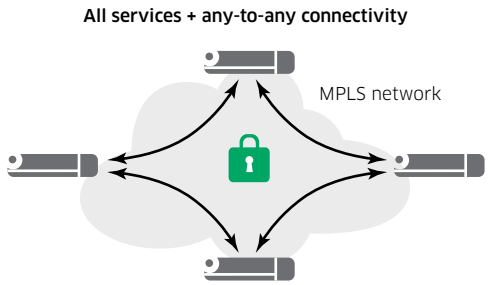
2.1.2 Flexibility of NGE

As more smart applications are being deployed in critical infrastructures, it is necessary for mission-critical networks to facilitate more meshed or "any-to-any" topologies while securing the connectivity among a wide variety of devices and equipment. NGE operating at the MPLS layer makes use of the existing meshed label switched path (LSP) to encrypt (see Figure 2).

With traditional approaches to encryption and authentication there is often limitations on the type of traffic that can be secured. The benefits of MPLS's ability to carry different traffic types at either Layer 2, Layer 3 have been proven through successful deployments worldwide. It is often the non-Layer 3 traffic carried over MPLS that is considered mission-critical. These devices might not have been upgraded to IP or will remain at Layer-2 to support such protocols.

The mains issue with using traditional approaches is that non-IP traffic needs to first be converted to IP or encapsulated in IP and then encrypted using IPSec. The converted traffic to IPSec can then be carried over MPLS tunnels. This process adds another layer of overhead, complexity and latency, as opposed to keeping the traffic in its more natural form over MPLS.

Figure 2. NGE flexibility



NGE extends the types of traffic that can be carried over an IP/MPLS network without altering the original traffic. In mission-critical networks this traffic often relies on virtual leased lines (VLLs) or pseudowire MPLS services to encapsulate the raw bit stream into MPLS packets. 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. The intent is to keep all original MPLS labels and functions untouched so that the VLL or pseudowire service is treated the same as before the security function was added.

Other types of services, such as Layer 2 Virtual Private LAN Service (VPLS) or Layer 2 Ethernet pseudowires (such as Ethernet port or VLAN-based pseudowires), can also be encrypted directly into MPLS tunnels using NGE without the additional management and packet overhead of converting this traffic to IP.

NGE can also provide any-to-any encryption and authentication for Layer 3 traffic, including Virtual Private Routed Networks (VPRNs) and Internet enhanced services (IESs) that use MPLS for transport. In these cases, MPLS tunnels are pre-established using either the Label Distribution Protocol (LDP) or Resource Reservation Protocol - traffic engineering (RSVP-TE) or are statically configured. Enabling NGE on these tunnels or enabling NGE directly onto the VPRN service itself allows for end-to-end and any-to-any Layer 3 services to be secured.

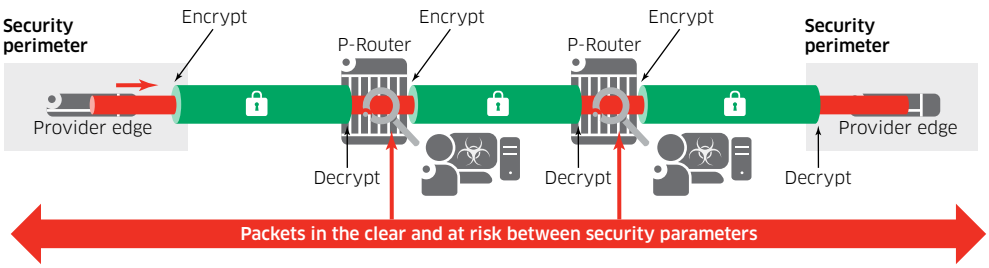
Sometimes Media Access Control security (MACsec[4]), another traditional encryption and authentication method, is proposed for encrypting all the various types of traffic over an Ethernet link. There are two main issues with MACsec that make it a questionable choice for end-to-end security of services.

The first issue is that traffic needs to be decrypted after every hop to determine where packets are routed and then the traffic needs to be re-encrypted. This presents a security risk at each hop of the network where the packet is decrypted, adds latency to encrypt and decrypt each hop, and adds hardware costs because encryption/decryption hardware is needed for each hop.

The second issue is that it is not possible to carry MACsec traffic over service provider networks (either Layer 2 or Layer 3) because MACsec is not typically offered as a service. Also, Layer 2/Layer 3 service providers would need access to VLAN or IP header information to properly provide such services, and those headers are hidden by MACsec.

Figure 3 shows the main MACsec challenges to offering end-to-end traffic protection.

Figure 3. MACsec challenges to offering end-to-end traffic protection



NGE does not have any per-hop encryption/decryption requirements because traffic is encrypted once during network ingress and decrypted once during network egress. Also, NGE can be enabled across any Layer 2 or Layer 3 service provider network to provide end-to-end security of any traffic needing the carrier services for transport.

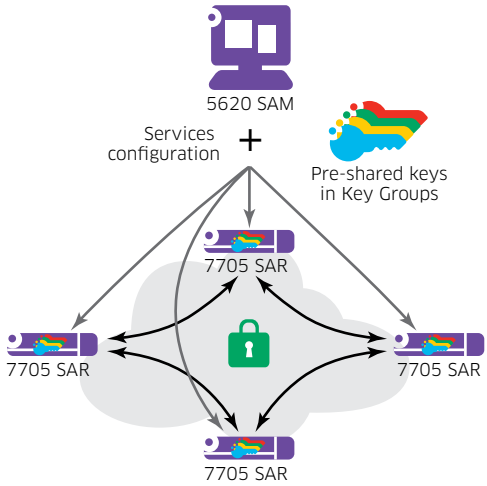
4 IEEE 802.1AE: *IEEE Standard for Local and Metropolitan Access Networks: Media Access Control MAC)* Security, 2006. https://standards.ieee.org/findstds/standard/802.1AE-2006.html

2.2 NGE components

As shown in Figure 4, NGE has four components:

- Alcatel-Lucent 5620 Service Aware Manager (SAM): Acts as the key and service manager for network-wide encrypted services
- Alcatel-Lucent 7705 Service Aggregation Routers (SARs): Routing elements capable of performing NGE-based service encryption
- Key groups: Holders of keys assigned to services, enabling security services network partitioning
- MPLS services: Services that require end-to-end encryption

Figure 4. Components that enable the NGE security solution



2.2.1 Alcatel-Lucent 5620 SAM

The main component of the NGE solution is the Alcatel-Lucent 5620 Service Aware Manager (SAM), which provides two main functions to enable NGE. The first is managing the services on the nodes within security domains that require encryption and authentication. The second is to act as the key manager for all nodes and provide the relevant keys in key groups that are used to perform encryption and authentication.

NGE uses symmetric pre-shared keys to perform encryption on the nodes. The 5620 SAM ensures that all nodes in a key group remain synchronized with the correct pre-shared keys and that only those key groups that are relevant to a particular node are downloaded with the sensitive keys.

Operational actions performed by the 5620 SAM include deploying keys to new nodes where new encrypted services are required, performing re-keying of the network at regular intervals, and deleting keys from nodes that no longer need those keys if services are removed from the key group domain.

2.2.2 Alcatel-Lucent 7705 SARs

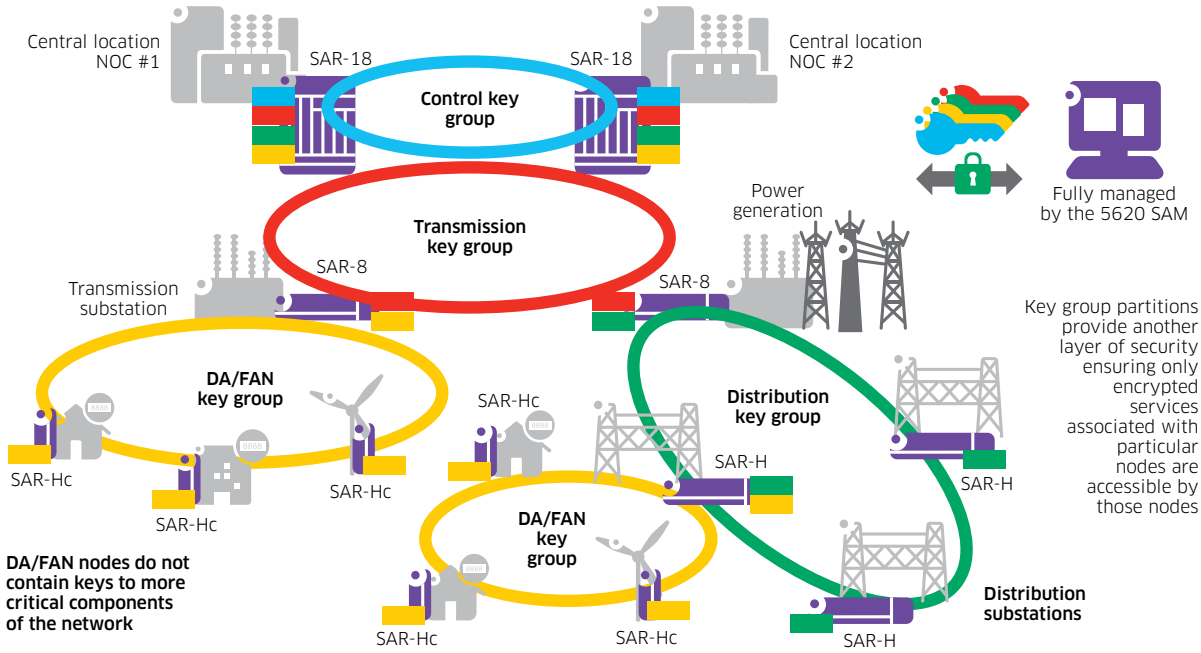
The second component is the nodes themselves that will perform the encryption authentication function for the MPLS services. The 7705 Service Aggregation Router (SAR) family is available from Alcatel-Lucent to perform the NGE enhanced encryption functions.

2.2.3 Key groups

Key groups enable NGE to provide a tiered approach to managing keys in the network. This is accomplished through key groups by configuring MPLS services to use a specific key group depending on the security policies of those services. For example, in a power utility smart grid network there may be different levels of criticality that need to be considered.

Figure 5 shows an example of key group partitioning.

Figure 5. NGE key groups enabling encryption partitioning



Distribution automation (DA) and field area networks (FANs) may be considered 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, which 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. The attacker is limited in scope of any attempted attack thanks to key group domains and partitioning.

2.2.4 MPLS services requiring encryption

The fourth component of NGE is the MPLS services that need encryption. These can range from TDM-based services that use pseudowire or VLL services, to Layer 2 VPLS or Ethernet VLL-based services, to Layer 3 services that leverage VPRN or IES functions over MPLS for any-to-any services. With knowledge of where these MPLS-based services are configured, the 5620 SAM manages the keys, downloading them to NGE-enabled nodes with MPLS-based services that require the additional security.

2.3 Bits and bytes

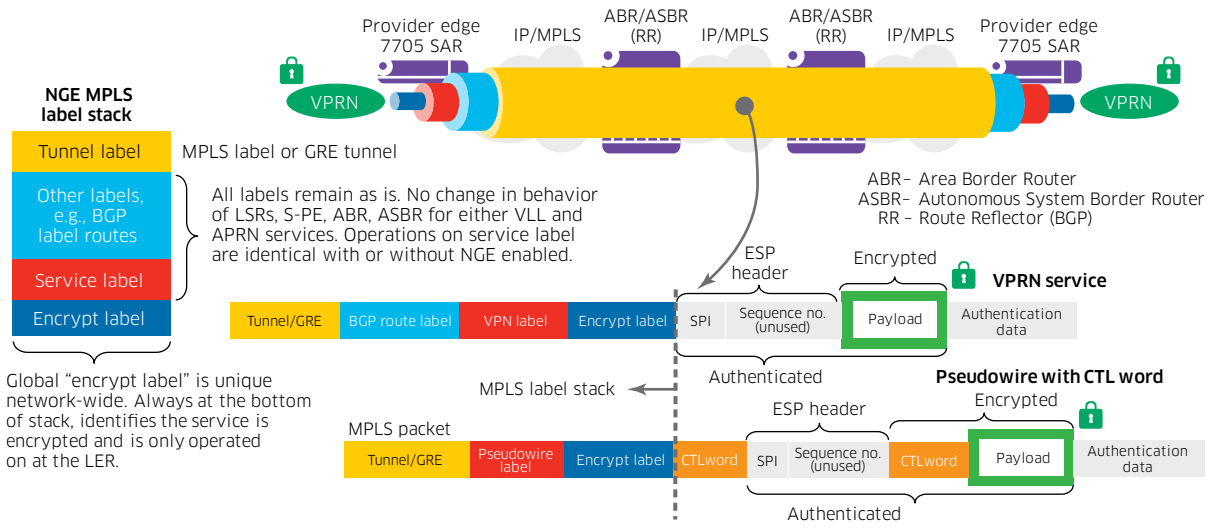
A main goal of NGE is to maintain the seamless nature of MPLS-based services without imposing restrictions when adding security to MPLS payloads. To this end, the format of an NGE-based packet attempts to minimize the visibility of the encryption and authentication by performing this function on only the payload of the MPLS packet while keeping all MPLS labels intact. This allows any intermediate nodes that are performing P-router, label switched router (LSR), area border router (ABR), autonomous system border router (ASBR) or route reflector 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 5 shows the NGE packet format. The original tunnel, Border Gateway Protocol (BGP) 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 nodes to:

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

Figure 6. NGE packet format examples



NGE uses the Encapsulating Security Payload (ESP) format defined in IETF RFC 4303[5] to encrypt and authenticate MPLS payloads. Because there is no IP header added to the payloads, NGE minimizes the added packet overhead associated with traditional encryption solutions. For VPRN- or VPLS-based services that do not use a 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 final label-edge router (LER) decrypts the payload, it checks the CTL word against the original CTL word to ensure it was not altered.

5 IETF. RFC 4303. IP *Encapsulating Security Payload (ESP)*. December 2005. http://www.ietf.org/rfc/rfc4303.txt

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 NGE key management

NGE key management consists of 5620 SAM service and key management and nodal key management.

3.1 Alcatel-Lucent 5620 SAM service and key management

The 5620 SAM provides the two main functions when using NGE in a network: service configuration and key management. With knowledge of which nodes are providing which services, the 5620 SAM can easily determine which nodes require which keys to be used in a security domain.

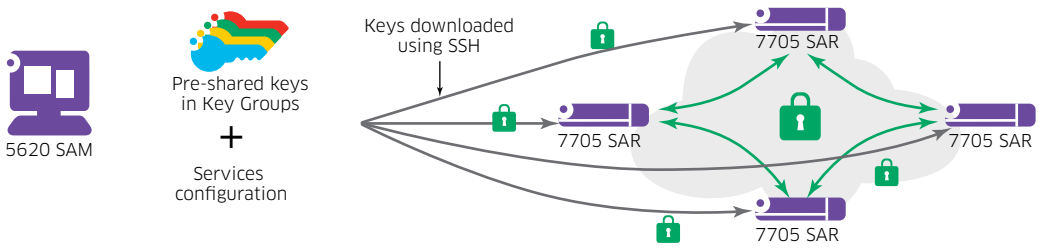
Pre-shared keys are generated internally on the 5620 SAM using a strong random number generator that is provided by the operating system of the 5620 SAM. When downloading keys to nodes, the 5620 SAM opens a new secure shell (SSH) session to each node and installs the keys (see Figure 7). The 5620 SAM uses a default user ID or an operator-defined user ID specifically assigned for key updates. Activities by either ID can be tracked through normal user accounting and logging methods for security audit purposes if needed by internal processes or external regulations such as NERC-CIP[6] 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 5620 SAM computes a simple CRC-32 checksum for each key in use. To ensure each node in the network has the correct set of keys, the 5620 SAM polls the nodes for the CRC checksum. If all the nodes match the checksum value the 5620 SAM knows all the nodes are synchronized with the correct keys.

The 5620 SAM ensures that newly generated keys do not have CRC-32 collisions with the previous keys used. If a collision is detected, the 5620 SAM skips to new key values that do not collide with the previous CRC-32 values.

Figure 7. 5620 SAM key deployment using SSH



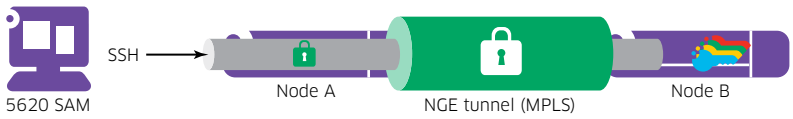
6 *Version 5 CIP Cyber Security Standards* is a suite of CIP standards published by NERC.

A main advantage of using SSH for NGE key download is that it provides an additional layer of security on top of the existing NGE transport tunnels. As shown in Figure 8, a new SSH session is opened on every key update. The PSKs are downloaded over an in-band communications channel, perhaps through a dedicated management VPRN service configured with NGE. Key download would have two layers of security: the SSH session itself and the NGE-encrypted services carrying the SSH session.

An attacker would already be challenged by decoding the NGE tunnel. The added burden of decoding the SSH session before the next re-keying interval is nearly impossible in a short period of time without extraordinary compute resources.

Using in-band management in this way is not mandatory but is an option for additional security during key download.

Figure 8. Key download over an NGE secured MPLS tunnel using SSH



After an NGE domain is secured, the 5620 SAM can use 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 are certificates or other sensitive information that are normally transmitted in clear text (for example, when handshaking of the SSH session occurs) able to be intercepted by a man-in-the-middle because the certificate and other sensitive information is hidden in NGE. Even after a network outage, NGE is designed to maintain its encrypted services and SSH is constantly protected with an additional level of security.

3.2 Nodal key management

When the 5620 SAM downloads keys to a node, they are stored securely in permanent storage on the node. A main goal of NGE is to maintain services in the encrypted domain during any type of network outage. Because mission-critical traffic relies on the high availability of the network used to carry such traffic, it is important not to have security functions disrupt this traffic even though security is still vital for the traffic itself.

In traditional encryption solutions, when network outages occur, the security control plane needs to re-establish, re-handshake and re-configure itself to key servers that may be overburdened during network fluctuations. These added strains can delay the restoration of important mission-critical traffic. Also, if traditional approaches rely on a control plane function to a key server and that key server loses connectivity, the traffic is immediately impacted and can be dropped until connectivity to the key server is re-established. This is not the case for NGE because it is designed to maximize availability while also maximizing its security function.

Figure 9 illustrates this basic concept. Because the keys are securely stored on the node, at no point in 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 5620 SAM is lost, there is no impact to the keys that are already in the network because no control plane is running between the 5620 SAM and the nodes.

The longer the 5620 SAM is not communicating with the nodes to perform re-keying procedures, the more stale the keys can become in the network. There is a tradeoff between having some level of security and maximizing mission-critical traffic uptime. The NGE solution attempts to maximize both, securing the traffic while avoiding traffic interruptions.

Figure 9. Non-stop encrypted services using NGE

3.3 NGE network re-keying procedure

The 5620 SAM provides a network-wide re-keying procedure on a per-key-group basis or for all key groups at the same time. Each key group can have its own re-keying interval or all key groups can be re-keyed using one global re-key interval. This choice is up to the network operator.

As is typical with security functions, the 5620 SAM uses a standard "make-before-break" approach to the re-keying procedure. The steps are as follows:

Step 1: The 5620 SAM first generates a new set of keys internally using a strong random number generator and ensures that the associated CRC checksums are unique from the previous keys used. The 5620 SAM then opens a new SSH session to each node and downloads the new keys to all nodes in the key group domain.

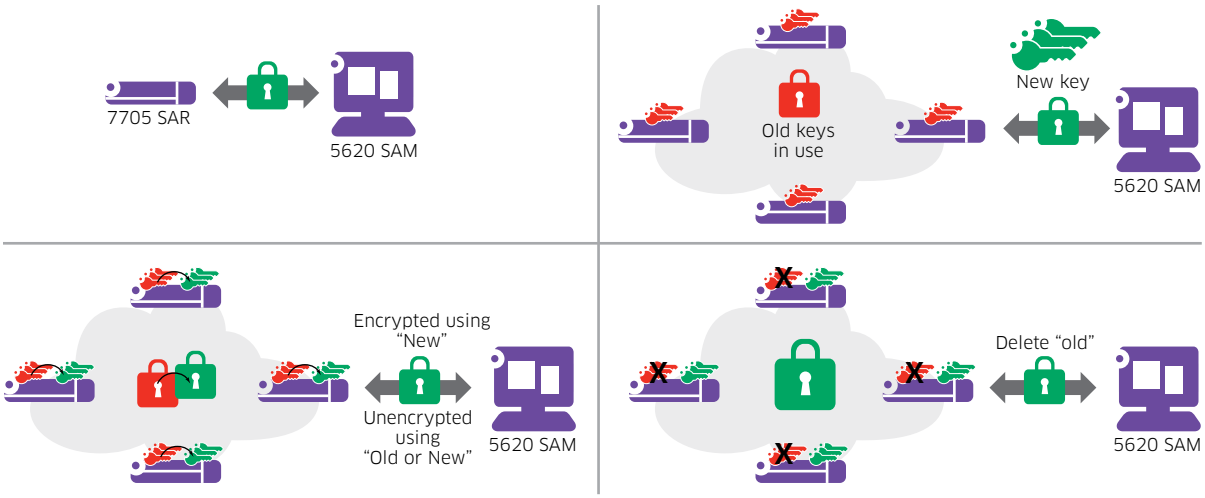
Step 2: After the domain-wide key update is finished, the 5620 SAM verifies the update by comparing the checksum in each node to the checksum stored in the 5620 SAM itself.

Step 3: The 5620 SAM 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 5620 SAM 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 5620 SAM deletes the old keys in all nodes in the domain.

The re-keying procedure is illustrated in Figure 10.

Figure 10. Non-stop encrypted services using NGE



4 Encrypted services

NGE provides two main modes of operation for encrypting MPLS-based services: Service Distribution Point (SDP) encryption and VPRN-level encryption.

4.1 Service distribution point encryption

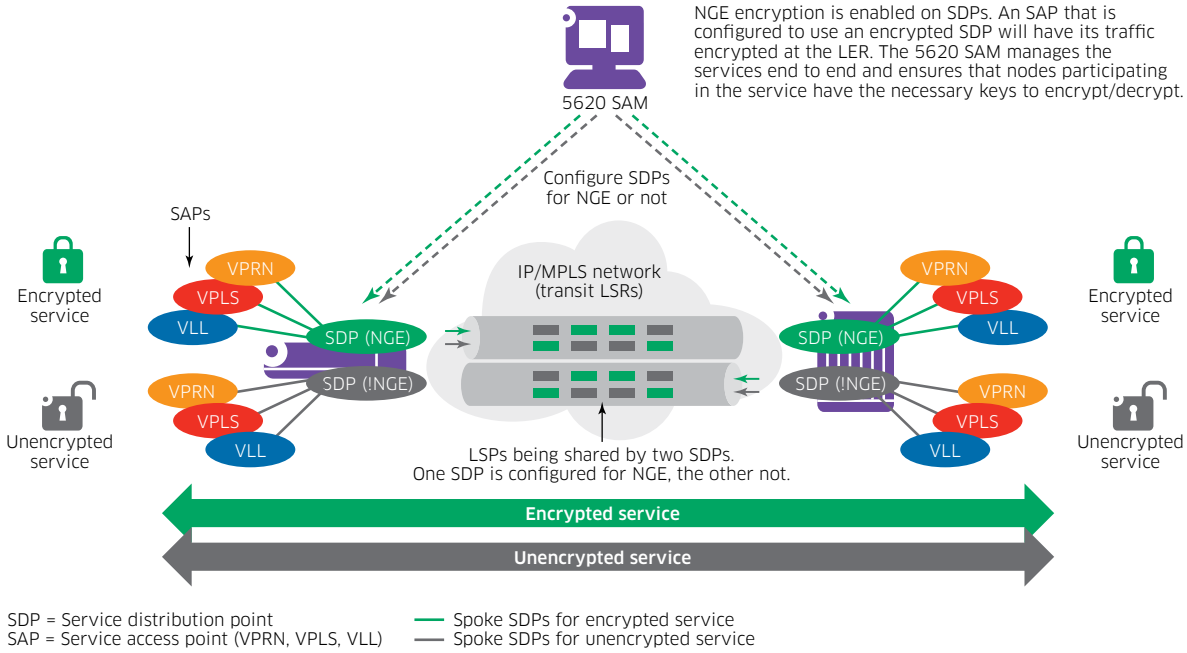
Alcatel-Lucent IP/MPLS routers use SDPs to make configuration and management of MPLS-based services easy and flexible. SDPs are associated with tunneling MPLS label switched paths (LSPs), including static LSPs, LDP LSPs and (RSVP-TE) LSPs.

In addition to MPLS-based tunneling, generic routing encapsulation (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 5620 SAM ensures that both routers associated to a particular SDP have the key group information that enables NGE for the SDP. Figure 11 illustrates this process.

Figure 11. Flexible service encryption of MPLS-based traffic over SDPs



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 green SDP will have its traffic encrypted over the transport LSPs for the green SDP.

Both encrypted and un-encrypted traffic can share the same LSPs. In Figure 11, 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 gray SDP would not be encrypted. In 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 include MPLS-based 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

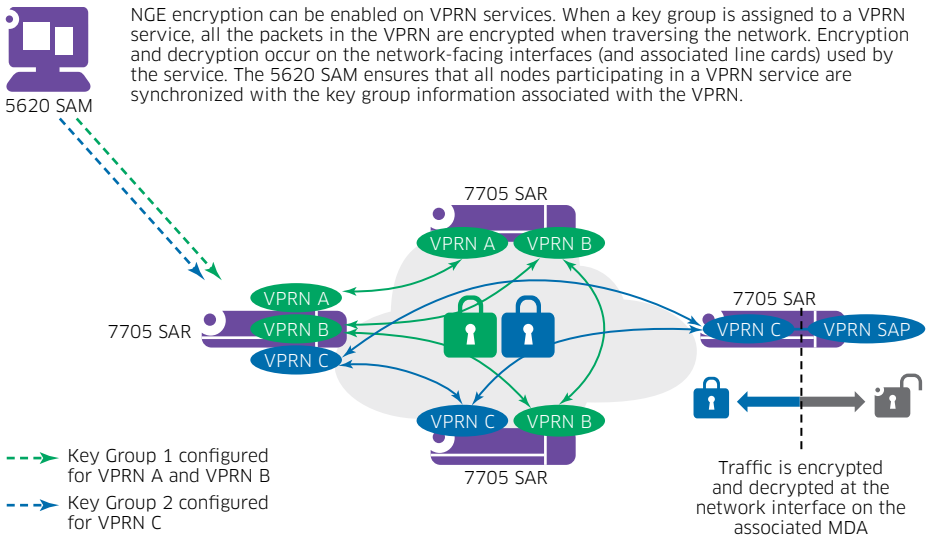
4.2 VPRN-level encryption

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. While the previous section discussed how NGE could be enabled for SDPs, this section focuses on Multiprotocol – Border Gateway Protocol (MP-BGP-) based VPRNs where services are "auto-bound" to transport LSPs.

The Alcatel-Lucent 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 advertised in MP-BGP. To encrypt the traffic in a VPRN using NGE, the 5620 SAM simply configures a particular key group for the VPRN. All nodes in the VPRN are then downloaded with the key group information needed to enable NGE. After all the key groups have been downloaded and verified, each node is capable of encrypting and decrypting traffic in the VPRN using the keys in the associated key group. The 5620 SAM then enables NGE on each node as required until all nodes in the VPRN have been NGE-enabled for the VPRN.

As shown in Figure 12, the same key group can be used for multiple VPRNs. In this example, VPRN A and VPRN B are using Key Group 1, and VPRN C is using Key Group 2. There is no need to establish provider edge-to-provider edge security tunnels or meshes of security tunnels because the group keys are downloaded to the nodes participating in the VPRN and can safely encrypt traffic sent to any other node in the VPRN.

Figure 12. MPLS-based VPRN service-level 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. This 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 to outside the NGE domain. Because this combination of auto-binding and L3 spoke SDP configuration is possible for added flexibility, NGE provides simple rules for how to configure this combination of encrypted and unencrypted service in the same VPRN.

5 NGE benefits

The next-generation techniques of encrypting and authenticating MPLS-based services using NGE provide some clearly identifiable benefits: flexibility, robustness and performance.

5.1 Flexibility

The service-aware encryption that NGE provides is simple to configure and manage, and maintains end-to-end MPLS network operations and maintenance functions such as resiliency, QoS and OAM. Core routers can switch and route NGE packets seamlessly, maintaining interoperability at router locations operating as LSRs, ABRs, ASBRs and pseudowire switching provider edge points because the NGE MPLS packets are transparent to them. The end result is seamless security encryption for MPLS networks.

NGE is a highly scalable solution that avoids large meshed tunnel configurations and complex topologies. NGE simply reuses the MPLS network planning and resource allocations associated with the MPLS user plane.

5.2 Robustness

As the main NGE component, the 5620 SAM provides comprehensive service-aware management of encrypted services and highly robust key management with hitless re-keying procedures. No additional stress is placed on routers because only the 5620 SAM manages key synchronization and updates. As a result, there is minimal control plane overhead and maintenance required for network-wide encryption.

NGE also provides a powerful and robust way to create security encryption domains using key groups.

Finally, NGE provides high availability and recovery of security functions of mission-critical data traffic in the event of network outages or failures.

5.3 Performance

NGE provides high performance and comprehensive encryption solutions for all types of Layer 2 and Layer 3 services without needing to convert traffic to IP or add the extra overhead and potential latency associated with IP encapsulation. All services are encrypted in MPLS packets without the need for further modification. For Layer 3 services, there is also complete Layer 3 privacy because all IP headers are hidden from inspection.

NGE packets are encrypted and decrypted only once as they traverse the network. The packets also have 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 VLL constant bit rate services that have small packet sizes, including TDM pseudowires, teleprotection and services using SCADA-related protocols.

6 Conclusion

Cybersecurity 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. Alcatel-Lucent NGE is an innovative security tool that provides comprehensive protection for both IP and non-IP traffic seamlessly at the MPLS 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.

7 Acronyms

ABR	area border router
ASBR	autonomous system border router
BGP	Border Gateway Protocol
CTL	Control
ESP	Encapsulating Security Payload
FAN	Flexible Access Network
GDOI	Group Domain of Interpretation
GRE	generic routing encapsulation
IES	Internet enhanced service
IKE	Internet Key Exchange
IP	Internet protocol
IPSec	IP Security
LDP	Label Distribution Protocol
LER	label edge router
LSP	label switched path
LSR	label switched router
MACsec	Media Access Control security
MPLS	Multiprotocol Label Switching
NGE	network group encryption
OAM	operations, administration and maintenance
RSVP-TE	Resource Reservation Protocol
SAP	service access point
SCADA	supervisory control and data acquisition
SDP	service distribution point
SSH	Secure Shell protocol
TDM	time division multiplexing
VLAN	virtual local area network
VLL	virtual leased line
VPLS	virtual private LAN service
VPRN	virtual private routed network

8 References

1. *Alcatel-Lucent Mission-Critical Communications Networks Solution for Power Utilities: Attaining NERC CIP Version 5 Reliability Standards Compliance*. October 2014. MKT2014107732EN_Attaining_NERC_CIP_Compliance_AppNote.pdf; http://resources.alcatel-lucent.com/asset/181741
2. *Alcatel-Lucent 7705 Service Aggregation Router Security Overview for Power Utilities*. January 2015. MKT2015019613EN_7705_SAR_Security_for_Utilities_AppNote.pdf; http://resources.alcatel-lucent.com/asset/184431
3. *Alcatel-Lucent 7705 Service Aggregation Router: Security overview for mission-critical networks*. http://resources.alcatel-lucent.com/asset/174129
4. IEEE 802.1AE: *IEEE Standard for Local and Metropolitan Access Networks: Media Access Control MAC) Security*. 2006. https://standards.ieee.org/findstds/standard/802.1AE-2006.html
5. IETF. RFC 5996. *Internet Key Exchange Protocol Version 2 (IKEv2)*. September 2010. http://www.ietf.org/rfc/rfc5996.txt
6. IETF. RFC 4302. I*P Authentication Header.* December 2005. http://www.ietf.org/rfc/rfc4302.txt
7. IETF. RFC 4303. *IP Encapsulating Security Payload (ESP)*. December 2005. http://www.ietf.org/rfc/rfc4303.txt
8. IETF. RFC 6407. *The Group Domain of Interpretation*. October 2011. http://www.ietf.org/rfc/rfc6407.txt

Alcatel·Lucent