TECHNOLOGY WHITE PAPER

Alcatel Vision for Secured Next Generation Networks

Planning and rollout of NGN services and infrastructure are gaining significant global momentum, led by VoIP and Video services. Operators are moving from customer trials to commercial rollouts. Security is an essential part of successful NGN rollout. Alcatel's customers are asking for our expertise and strategy on this very important set of requirements. It is the purpose of this paper to explain Alcatel's vision for securing NGN solutions. To achieve this, it will explain the most important parts of the security framework that Alcatel has designed as a basis for its NGN solutions. This paper addresses mid-technical managers in charge of security at operators deploying Next Generation Network solutions. It focuses on DSL-based fixed access NGN. Its purpose is to illustrate Alcatel's understanding of security issues in NGN and give an overview of Alcatel's generic security solution. The security of the NGN solutions will be discussed, i.e., security solutions that improve the ability of the NGN solutions to resist accidental events or malicious actions that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted data and the related services. Considerations of attacks and their mitigation cover the network layer up to the application layer. It is assumed that the reader has a basic knowledge of telecommunications security, as it is not an objective of this paper to provide a tutorial on generic security.

ALCATEL

Alcatel Vision for Secured Next Generation Networks

Introduction 1

The need for security in NGNs 1

Technological changes 1

Regulatory changes 1

Organizational changes 1

General constraints and objectives in securing NGNs 2

Most probable risks with NGNs 2

Threat analysis of the NGN multimedia architecture 2

Prioritizing security requirements: an operator's perspective 3

Alcatel NGN secured solution 3

Security principles 4

A first step towards security: the VPN security scenario 4

NGN Class5 and multimedia architecture, secured solution 5

Security zones 6

Front-end security 6

Security technologies 7

Intrusion detection and prevention 7

Firewall and NAT traversal issues and solutions 8

Conclusion 8

References 8

Abbreviations 8

Biography 9

Alcatel Vision for Secured Next Generation Networks

Introduction

The market is witnessing constant growth in the deployment of VoIP and multimedia solutions, and thereby an increasing demand for Next Generation Network (NGN) infrastructure. As confirmed by analyst reports (e.g., see [1]), VoIP and multimedia solutions are now growing and gaining in maturity, and as operators are moving from customer trials to commercial rollouts, there is an increased demand for secured solutions. But is this gain in interest for security in the telecom market fully justified? The straight answer to this question is 'yes.' Alcatel believes that the trend towards more and more security in telecommunications solutions will continue until security becomes an integral part of any such solution.

Just as criminality regularly outpaces criminal legislation, malicious attacks regularly outpace today's security countermeasures. This is because many popular applications have been deployed before any security was even envisaged, especially with IP-based networks. To reverse this inefficient approach, security must be taken into account from the early stages of any telecom system's design up to and including its deployment and operation.

This paper first justifies the need for security in NGN. It then lists constraints inherent in the NGN infrastructure that needs to be secured and the objectives to be reached when securing this infrastructure. Next, it describes the most probable security risks the NGN infrastructure is exposed to and gives an overview of its threat analysis. The paper then details Alcatel's NGN security framework and illustrates the most important elements of a secured solution. This includes key security principles as well as detailed security solutions that need to be applied at each step of the infrastructure's design. It concludes with future perspectives on the NGN security market.

The need for security in NGNs

There are three fundamental reasons why the security of telecom solutions requires significantly more resources on NGNs than on the traditional Public Switched Telephone Network (PSTN). These reasons are technological, regulatory, and organizational.

Technological changes

The technology is moving from a closed to an open environment. Also, PSTN is an infrastructure dedicated to voice, while the NGN infrastructure is shared for voice, data, and multimedia services, and possibly provisioned by multiple access and service providers. In the future, NGN solutions may also evolve to support additional services such as consolidation of public Internet services and high-speed Internet access.

PSTN is characterized by closed technologies. The ITU-T has defined SS7, a global telecom standard that defines the procedures and protocols by which PSTN network elements exchange information over a digital signaling network in order to handle wireless and wireline call setup, routing, and control. Such networks are closed and largely isolated from other network services. Also, fewer people are familiar with SS7 than, for example, SIP. PSTN mainly uses out-of-band signaling, which has the advantage of inherently providing some level of protection against threats from end-users. Consumer devices are closed (black boxes) and do not offer easy opportunities to misuse the network services. In the network, specific proprietary software applications are used. Thanks to the closed nature of the overall architecture, operators have kept full control over all service interfaces.

On the other hand, the next generation networks have a very open architecture to increase flexibility, and run end-to-end on a common technology, IP-based protocols, to increase inter-operability. There has also been much vulgarization on IP technologies that did not exist for PSTN suites. The NGN network infrastructure is open towards, or shared by, various types of service, such as voice, multimedia, and data, including the global Internet, and the services provisioned by multiple stakeholders. Signaling and control flows are carried in-band[1] jointly with end-user data traffic. NGN products also use generic hardware and software platforms. End-user devices are moving towards open platforms such as PC's. Finally, open interfaces are developed to support third-party application service providers.

Regulatory changes

Governments around the world are taking initiatives that put an increased responsibility onto operators and service providers for ensuring that critical infrastructures, of which voice/multimedia networks are a key part, are well protected against all kinds of threats. This is without taking into account classical legal requirements that already apply to PSTN and that are today highlighted with the evolution towards packet-based network services (e.g., the requirement for lawful interception that can impact the overall security architecture deployed, the obligation to support emergency calls, etc.). All those are clearly mastered in the PSTN context and now bring new challenges in deploying commercial NGNs.

In 2002, the OECD published ICT security guidelines that recommend, among other things, that security be a fundamental element of all products, services, systems, and networks and an integral part of system design and architecture.

In Europe, the EU directive on data protection requires operators and service providers to ensure that their infrastructure and service are adequately protected, and requires them to provide their customers with secured services. Furthermore, customers must be informed of any risk they face due to security breaches in the provided services.

Organizational changes

Fundamental changes in the telecom market situation have also led to security questions. The relatively high turn-over of employees, both at vendors and operators, has raised the risk of employee misbehavior. Because operators and carriers no longer form a small club of big (national) players where everyone knows each other, trust relationships are harder to build and maintain. Such aspects also have an impact on the

[1] This refers to the naked NGN infrastructure with no security measures yet (e.g., VPN infrastructure). Note that VPNs provide a virtual separation (as opposed to physical), and packets remain mixed at layer 3.

overall level of security of the deployed NGN services. This in fact increases the risk of internal attacks, which should now be considered as seriously as any type of external attack.

General constraints and objectives in securing NGNs

When deploying secured NGNs, NGN operators have the following objectives, and must take into account the following constraints:

- Minimize the additional cost of the secured solution by identifying the optimum security solution that will avoid prohibitive cost (the basic principle of security solution cost versus cost of risk being mitigated).
- Deploy a secured solution that is generic enough to be applied to most of the NGN applications and service scenarios with minimal impact on the architecture and the positioning of components and network elements.
- Ensure that the security solutions have been implemented and can be deployed and operated in a coordinated way so as to avoid inter-operability problems that would create security gaps.
- Ensure that voice and multimedia traffic QoS constraints are taken into account. Voice has specific constraints in terms of quality of service delivery (guaranteed bandwidth) and real-time performance (delay and jitter on the voice stream, but also timely delivery of the signaling). In the multimedia context, media such as video have constraints as well, such as limited tolerance to packet loss. Any security measure, in particular any encryption mechanism, must cope with these constraints. Security measures such as encryption will impact the consumed bandwidth and required processing power in the nodes of the VoIP network. The real-time requirements will result in a limited number of security gateways that can be placed on the end-to-end stream without excessively impacting delay and jitter.
- The voice service also has constraints such as 99.999 availability and legal requirements such as a lawful interception infrastructure and guaranteed emergency service provisioning, usually required to obtain an operating license. The business continuity constraint significantly impacts traditional networks by increasing their complexity. Such requirements are usually not imposed on data traffic, and the legal requirements are yet to be defined for VoIP. Today's VoIP infrastructures often foresee mechanisms to fall back on traditional systems in case of failure so as to maintain access to services such as emergency service.
- Finally, ease of use is critical to end-user acceptance of the security solutions. This includes ease of updating security with the latest technology with minimum impact on the rest of the infrastructure.

Most probable risks with NGNs

For carriers to manage the threats the NGN infrastructure is exposed to, it is of utmost importance to clearly identify the key risks and threats. This can be done by a threat analysis as illustrated in the next section. Also, as was explained earlier, key security risks related to the very nature of the NGN architecture can already be identified. Examples of such sources of additional risk are:

- The large number of external connectivity points with peer operators, with third-party applications and service providers (e.g., via OSA/Parlay gateways), and with the public Internet.
- The sharing of a core network infrastructure among several NGN service providers[2,3].
- Because no physical access is required, user traffic can possibly be more easily eavesdropped and manipulated on NGN architectures than in PSTN environments, for example, by remote access with intrusion and the installation of spyware on user devices or network nodes.

Besides the NGN infrastructure itself, new customer equipment, due to its openness and multi-application usage, can become a source of malicious flows (denial of service attacks), viruses, and so forth, targeting both the operator's systems and other customers (including spam). Operators have a role to play in providing their customers with the service of controlling and filtering user traffic to prevent user-to-user attacks (virus and worm removal and spam suppression).

As end-users now have the ability to manipulate their equipment, risks also include service theft and billing fraud due to third-parties (whether the operator's own customers or not) masquerading as legitimate customers. Fraud also includes malicious third parties luring customers to expensive 9xx numbers.

Also, while this paper focuses on DSL fixed access, it must be recognized that additional risks are introduced by the numerous heterogeneous technologies accessing the NGN infrastructure (wired, wireless Bluetooth, WiFi IEEE 802.11x), especially if the security technologies do not interoperate fully.

Finally, the interconnection between PSTN and NGN environments inherently brings more risks to the PSTN infrastructure itself, such as attacking the (unprepared) SS7 network by intruding on a signaling gateway. While this is possible, it is not very likely, since it would require breaking several levels of security measures.

Threat analysis of the NGN multimedia architecture

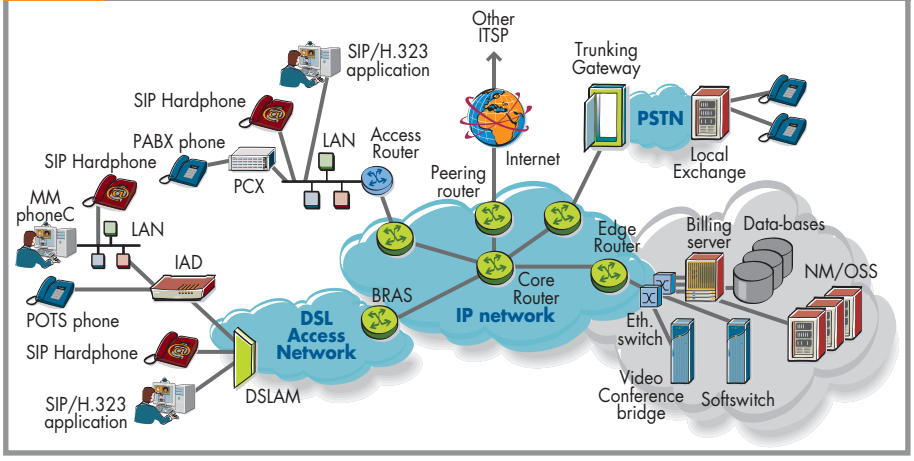
An overview of the architecture supporting the NGN Class 4/5, IP Centrex, video conferencing, and multimedia applications is illustrated in Figure 1, which depicts the main network elements involved in these applications. Performing a

[2] In the case of induced overload, it is the role of security to prevent it. It is the role of the QoS infrastructure to apply QoS techniques such as bandwidth management and load balancing to prevent an overloaded network using part of a shared infrastructure from having any QoS impact on the other networks.

[3] It is also necessary to differentiate induced overloads from those caused by legitimate traffic bursts by measuring traffic parameters and using, for example, statistics and pattern analysis to differentiate both cases. This is done in efficient Intrusion Detection Systems (IDS), allowing appropriate action to be taken.

threat analysis on such an architecture consists in a systematic and exhaustive study of all architecture domains and sites, network elements, interfaces, and flows between them, and an identification of all the threats on these elements and flows. The result consists in a list of threats on network elements and on signaling, application, control, and management traffic.

Fig. 1 NGN Class 5 and multimedia architecture



To illustrate Alcatel's understanding of security issues in NGNs and give an overview of its generic security solution, this paper first explains the threats to which the NGN infrastructure is exposed and from there the Alcatel NGN secured solution can be deduced. An exhaustive enumeration of all the threats identified in the analysis is not reproduced here for the sake of brevity. Most of the threats can be categorized as, for example, denial of service, eavesdropping, unauthorized access, etc. See ETSI TIPHON ([2]) for a typical example of categorization.

Threats constitute a risk to the security objectives as defined by ETSI TIPHON (see [2]): confidentiality, integrity, accountability, and availability. TIPHON also studied the correspondence between threats and security objectives (see [3] for more details).

Additionally, protocol-specific threats are also identified. For example, specific threats to SIP include SIP REGISTER, INVITE, and BYE flooding, unsolicited CANCEL and BYE, etc. Specific threats to MGCP and MEGACO/H.248 are, for example, denial of service by resource exhaustion using Add/CreateConnection, unsolicited or flood of Modify/ModifyConnection to affect the delivered QoS, etc.

A comprehensive NGN threat analysis is an essential basis for the design of the Alcatel NGN secured solution. This solution is described in the next section on secured solutions.

Finally, new threats are bound to be identified in the future and new vulnerabilities revealed. A sound design of the secured solution must allow sufficient flexibility to cope with the dynamic aspects of security within a continuous security process. Vulnerability is handled by Alcatel's Product Security Incident Response Team (PSIRT). This process handles vulnerabilities both within Alcatel-made software and within third-party software components integrated into Alcatel products.

Prioritizing security requirements: an operator's perspective

When prioritizing the security requirements, there is also the public operator's perspective. Public operators evaluate the risks according to their customers and specific businesses. They consequently identify those risks that need to be suppressed/mitigated with higher priority. Though there are possible discrepancies between operators, there is a common set of security requirements of interest to the vast majority of them.

Firstly, while emergency services and lawful interception are not security features as such, operators are legally required to provision them, so they will have to be provisioned in a reliable and secured fashion.

Secondly, it is key for each vendor to have a view of the global secured architecture solution.

Thirdly, based on operator requirements, market analysis, and the result of Alcatel's own work on threat analysis, the following security topics appear to have a high priority:

- Mitigation of (Distributed) Denial of Service – (D)DoS – attacks from end-users;
- Authentication solutions (administration and end-users);
- Intrusion detection (IDS) and intrusion prevention (IPS)[4];
- Mitigation of internal attacks;
- Security testing[5] and network element hardening[6];
- Vulnerability management process;
- Logging and auditing tools;
- Standards to be supported.

This list is not exhaustive. But in addition, consideration must also be given to the process aspects of security, such as swift distribution of security patches, personnel security screening and training, etc. Finally, the priority of security requirements also depends on the business in which the operator is involved.

Alcatel NGN secured solution

Designing secured solutions requires that the telecom manufacturer be able to extract a security vision out of the

[4] While masquerading is covered by adequate authentication, IDS/IPS refers to network-based attacks that can be detected or effective intrusions after authentication failed to fill its role.
[5] Security testing consists in using standard and proprietary tools for systematic and exhaustive testing of systems against known vulnerabilities.
[6] System hardening must be at the basis of any security solution. It consists of disabling all unnecessary features and services (e.g., closing unused ports and disabling unused applications), applying patches or purchasing the latest software releases (thus removing previously detected vulnerabilities), and having a secured patch management process (patch release and distribution).

complex world of NGN security. Also, the development and implementation of this vision requires absolute discipline. Security rules must be adopted and applied at each step of the solution conception.

Security principles

Alcatel follows these principles when designing secured solutions:

- Secure the operator's own infrastructure: threats can originate from anywhere - from customers, insiders, interconnected operators, or remote parties that connect on the NGN infrastructure via an Internet access.
- Ensure that the operator does not become a source of security holes and weaknesses towards interconnected domains such as operators and service providers.
- Allow the operator to provide its customers with a secured service: consumers usually expect the same quality of service with NGN-based voice/multimedia services that they were used to with PSTN, even in spite of their lack of interest in security procedures.
- As a secured solution relies heavily on individual network elements being themselves secured, Alcatel has also defined a general policy for the design and development of secured products. Product design and development phases ensure that appropriate security mechanisms are integrated into the product to mitigate security breaches and risks. This is achieved by ensuring that the product works securely and safely, that its day-to-day management is secured, and that any network or application service of which the product is part is also secured. This policy sets a common baseline for the security level of all Alcatel products.
- It must not be assumed that customers' equipment will behave in a friendly way.
- External borders (public Internet, peer NGN operators, third-party application service providers) must be protected with strong filtering mechanisms such as firewalls.
- Key management systems and control/signal servers are extremely sensitive elements that require strong protection with firewalls.
- As per Alcatel product design security policy, management traffic between management stations and network elements must be secured, at least with traffic authentication/integrity. Management security also includes the protection of remote carrier-site upgrades of xDSL modem firmware.
- As per Alcatel product design security policy, basic security mechanisms must be implemented individually within each network element (mainly[7] for control and management planes).
- The infrastructure must be segmented in such a way that servers accessible by end-user originated traffic are clearly separated from highly sensitive servers, themselves isolated from the OSS.
- The success of a security solution implies considering security as a process of continuously monitoring network security to cater for the evolution of threats and maintain optimum knowledge of the technology to mitigate them.

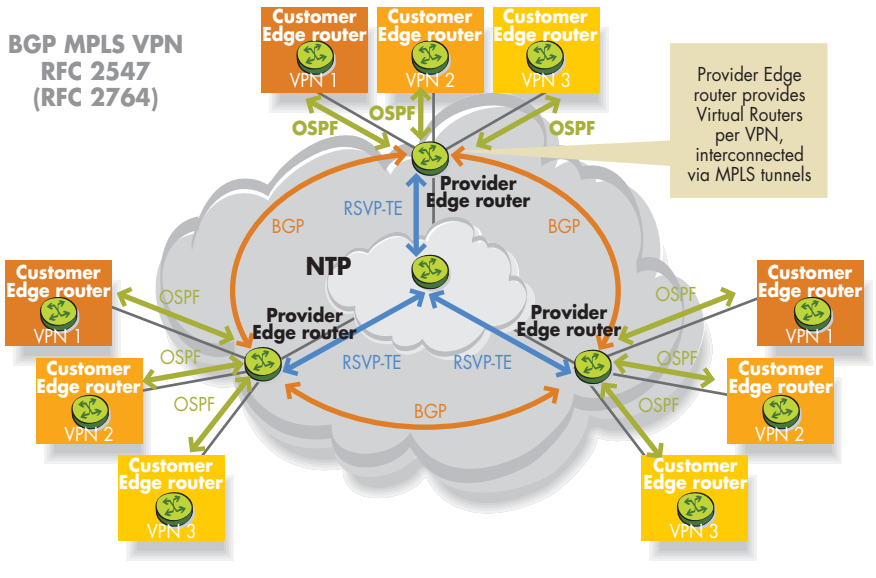
A first step towards security: the VPN security scenario

The main objective is to achieve a degree of security comparable to TDM technologies. When the voice/multimedia operator, called multimedia Application Service Provider (ASP), is a large and well-established operator, it often operates its own Network Access infrastructure and the IP backbone infrastructure. In other words, it also plays the roles of Network Access Provider (NAP) and Transport Network Provider (TNP). In this case, the operator can deploy its own VPN technology end-to-end through the NGN infrastructure. In a first instance, this scenario, called the "VPN security scenario", can be considered to be (relatively) inherently secured.

The Virtual Private Network (VPN) based solution enables a strict end-to-end separation of the data and the voice to be guaranteed. This prevents the data service from impacting the quality and security of the delivery of the voice service, by guaranteeing that respective signaling and media traffic remain strictly segregated, end-to-end.

[7] The general policy also covers the data/media plane, but the focus is on control and management aspects.

Fig. 2 MPLS VPN in the IP backbone



To implement this VPN-based security, the following configuration rules can be applied:

- The data VCs and voice (VoIP) VCs can be transported on separate VPs;
- The data and voice VPs can be collected on separate ATM interfaces that can be either on the same or on separate BAS elements;
- When VPs are collected on the same BAS, strict internal segregation is maintained by using virtual routers (VR) with separate routing tables;
- The segregation continues in the IP backbone with MPLS VPNs (BGP/MPLS VPN according to IETF RFC 2547 and RFC 2764[8]), see Figure 2, and in the ASP network also with separate LANs/VLANs and VRs in the routers.

This approach offers the following security guarantees:

- Attacks in the data VPNs will not affect the voice/multimedia ASP;
- The attacks in the signaling of the voice VPNs will be mitigated by the strict security features of the voice/multimedia ASP domains.

Several conditions need to be met for the VPN-based security to be considered sufficiently trustworthy:

- The network infrastructure cannot be compromised. This implies a secured network management:
  - In the case where SNMP is used for configuration management, this is achieved by using the additional security features specified in SNMP v3;
  - There must be no easy or unsecured access to network elements such as with FTP or telnet. This implies replacing FTP, remote login, and telnet with SSH[9];
  - For management application signaling exchanges on top of CORBA/TCP, specific protection with TLS, using mutual network element authentication, and with signaling encryption is recommended.
- For all operating personnel, all administrative access requires login and password and must be authenticated, access controlled, monitored, and logged[10].

The assumptions made in the VPN security scenario allow the security requirements to be "relaxed". The VPN infrastructure allows the elimination of some of the threats inherent in user access, such as eavesdropping on signaling or on content of communication, masquerading as a node, or modification of signaling or content of communication.

However, this scenario does not exclude the possibility of attacks from the residential or enterprise customers: the CPE can never be really trusted. CPE can be a SIP or H.323 IP phone, or a PC, or other equipment connected using an RGW or an IAD that will convert the SIP or H.323 signaling onto MGCP or Megaco/H.248. These four protocols can consequently be used for flooding attacks. The threats that cannot be eliminated by the VPN infrastructure and must consequently be mitigated additionally are:

- User identity theft (user masquerading), possibly leading to Theft of Service (ToS);
- Use of IP address spoofing for performing various attacks (intrusion, flooding);
- (D)DoS attacks by flooding or malformed/unsolicited messages;
- Unauthorized access (intrusion attacks);

The mitigation of these threats is explained next. Additionally, administrator identity theft leads to internal attacks. Finally, if the core network infrastructure (the IP backbone) is shared or not fully-owned by the NGN service operator, protection of communications between network elements that cross this shared and not fully trusted IP backbone infrastructure must be considered (e.g., IPsec-based tunnels, secure RTP, and so forth).

NGN Class5 and multimedia architecture, secured solution

Beyond the VPN security scenario, the entire architecture of the NGN VoIP and multimedia solution must adopt a secured design:

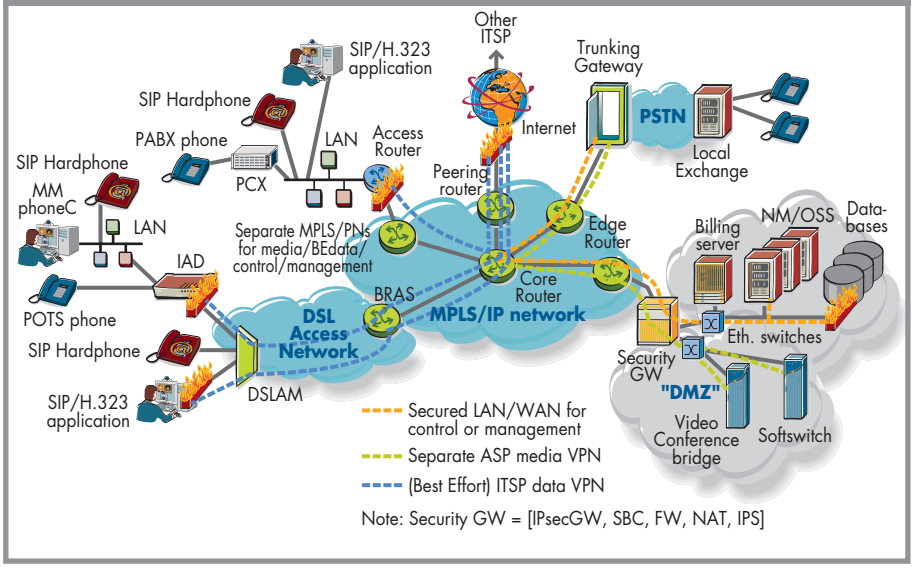
- Take security into account while defining the network architecture: position resources, servers, and security elements in a way that inherently provides a first step towards security. The secured architecture is based on two major principles:
  - Security zones, see details below;
  - Front-end-based security, i.e., a security solution based on implementation of security measures in the border elements, see details below;
- Positioning the security measures across the network in a way that relates to the threats they are countering, i.e., positioning the security measures such that they can operate most efficiently.

While the selection of security technologies is mainly a function of the requirements, it must also be done in a cost-effective way. The cost of the security solution should be lower than the cost of the risks it mitigates[11]. Also, needs for inter-operability with neighboring domains might influence the choice of the security solution.

[8] IETF RFC2764 describes a useful framework for VPNs running across IP backbones.
[9] SSH provides a secured alternative to remote login (telnet, rsh), file transfer (ftp), TCP/IP, and X11 port forwarding, with a security level equivalent to SSL/TLS.
[10] Administrative security rules also contribute to mitigating internal attacks, now to be considered as likely as external ones.
[11] ROI is quite difficult to estimate and depends how the operator evaluates the risk. There is a part of subjectivity, so this requires high operator expertise together with the secured solution manufacturer's help.

Figure 3 gives an overview of the NGN class 5 and multimedia architecture with security measures in place. The figure is there for illustration purposes and does not claim to be exhaustive. The secured solution will strongly depend on the configuration of the deployed NGN architecture and can imply additional security features (not shown) such as filtering and rate limiting in edge routers, IDS in the access, etc. Details are explained below.

Fig. 3 NGN Class 5 and multimedia architecture with an overview of security



Security zones

This architectural principle consists in splitting the operator infrastructure into separate zones such that:

- The security zones are protected from each other;
- It is difficult for an intruder to move from one zone to another;
- A zone groups network elements that require similar security strength;
- Sensitive servers (e.g., data storage) are separated from more exposed elements;
- Security solutions can be deployed in a customized fashion on a per zone basis.

It is therefore recommended that the different layers of the architecture depicted in Figure 1, i.e., advanced services layer, management layer, control layer, and media layer, be deployed in the form of separate security zones. This produces the (media) servers zones, the services and applications zones, the management zones, the access network zones, the sensitive (data) servers zones, and finally the demilitarized zones (DMZ, in which all servers exposed to the Internet, and therefore vulnerable, are placed). Each zone category can be implemented multiple times depending on the needs, i.e., separated for functional, security, or administrative reasons. The separation in security zones should not be confused with the security enforced between different administrative domains[12], as security zones are defined within a single administrative domain.

To prevent a proliferation of firewall infrastructure and optimize its cost and performance, the firewall infrastructure can be part centralized and part distributed, according to four schemes, which can be combined:

- Deploying firewall functions within a network element (e.g., firewall software);
- Deploying a firewall in front of a single network element;
- Deploying a firewall at the border of an administrative domain or a zone containing several network elements that need protection;
- Deploying a firewall as a centralized element between two or more security zones in order to control the signaling and control traffic exchanged between them.

The firewall configuration to be adopted will substantially depend on the operator's network configuration and on the size and position of the various network elements to be protected. For example, fewer large elements might reduce the flexibility in designing more separate zones.

Front-end security

The front-end security approach mainly consists in deploying security measures at the borders of the operator domains or security zones. Such security measures apply to media/transport, control, service/application, and management planes separately. The security functions deployed at the domain border can include termination of security tunnels, mitigation of intrusion or DoS attacks, but also functions such as user authentication.

The front-end-based security provides the following advantages:

- It allows attacks to be stopped before they penetrate a domain or zone;
- Letting the domain border take an active part in the user authentication function allows the border element (proxy element) to identify whether an authentication is successful or not. This has the advantage of preventing unauthenticated user signaling traffic from penetrating more deeply into the domain. See, for example, the role of the proxy-CSCF in 3GPP IMS (see [4]).

[12] An administrative domain is a distinct physical or logical area that is managed by a single administrative entity, such as a single network operator, an Internet access provider (IAP), an application service provider (ASP), and so forth.

- Security measures deployed inside a domain or zone can be different from the ones deployed at its border. This dual security approach has several advantages:
  - It disrupts the security solutions that are used on the end-to-end link and helps confuse attackers[13]: the attacker first has to deal with the security at the border of a domain or zone before being able to learn the first byte about the security solution deployed at the other side of that border;
  - It facilitates the modification of the security solutions within a domain or zone without affecting inter-operability with other domains or zones;
  - It enables customization of the solutions deployed from central servers domains towards the access domains depending on the specifics of the access technology;
  - It possibly offloads an important part of the security processing from central servers towards front-end servers.

Security technologies

This section is now somewhat more specific in terms of the security technologies to be used in the secured solution. Below is a list of security technologies that can be used:

- Protection of SNMP flows against eavesdropping, masquerade, DoS flooding: by using the additional security features specified in SNMP v3 (required when SNMP is used for configuration management), and rejecting SNMP traffic from outside the domain, with firewall and access control lists (ACL);
- Protection of SIP flows against flooding from CPE, from the transport domain, or from the Internet, with solutions such as ingress filtering, firewalls, packet filters, access control lists, and only allowing traffic from predetermined network elements;
- Protection of HTTP traffic is usually done with TLS/SSL (HTTPS). User authentication can take place in the secured TLS/SSL tunnel with HTTP Digest;
- Protection of protocols such as COPS or H.248, against eavesdropping, masquerade, and DoS flooding, with solutions such as firewalls, packet filters (access control lists, only accept traffic from predetermined network elements);
- Protection of FTP, Telnet, remote login, usually involves hardening by removing these services from the node and replacing them with SSH-based equivalent applications;
- Protection of media flows can involve, as alternatives to VPNs, either IPsec or SRTP, the latter being less mature but better adapted to a multipoint media topology.

Using either IPsec/IKE or TLS for the protection of SIP or H.323 traffic can be debated. It can depend on the availability of the implementation of these technologies in the end-user equipment and in the network elements involved in the end-to-end signaling flow. The IETF recommends TLS for protecting SIP (see [5]) in order to ensure inter-operability. However, TLS connections require that the protocol effectively runs on TCP. IPsec/IKE can be used whether the protocol runs over TCP or UDP. This is an advantage for protocols that run partly or entirely over UDP, for example for RAS over UDP, used in the H.323 protocol suite. While IPsec/IKE and TLS/SSL provide similar security services, there are also distinct differences between them, and they should be considered as alternatives. Depending on the problem to solve, one will usually be a better fit than the other.

It can also be appropriate to use security features when they are specified in the protocols themselves (integrated application security), depending on availability in deployed nodes and on interoperability with other components in the solution. Examples are COPS native authentication or Digest authentication for SIP. SIP Digest[14] only provides authentication, not always anti-replay, and never integrity or encryption. It only protects the SIP REGISTER and SIP INVITE messages. Reading the specification (see [5]) rapidly suggests better protection might be needed. In that case, either TLS/SSL or IPsec based authentication and integrity for all SIP messages can be considered (note that encryption is not always required).

Intrusion detection and prevention

Intrusion detection consists of detecting when unauthorized access to a network element, for example, has been performed, or even better, when attempts to obtain such an unauthorized access are being made. Due to the difficulty in handling the proliferation of false positives, the Intrusion Detection Systems (IDS) today tend to evolve to Intrusion Prevention Systems (IPS), at least in name. An IPS can be defined as an IDS coupled to a firewall or packet filter function, such that the IPS is able to take actions autonomously, based on policy rules. Actions can be packet drop, packet redirect to a quarantine network, or sending alarms. The IDS/IPS can be positioned, for example, in the ANP or ASP domains, in management domains, in the Enterprise, and so forth.

Today, IDS/IPS goes beyond its initial role and often includes protection against intrusions, denial service (DoS/DDoS[15]) attacks, viruses, Trojans, worms, and other known exploits. The IDS/IPS is wire-speed in-line equipment that is “usually open”, as compared to a firewall on which ports are “usually closed”. This is why the secured architecture will usually include both an IDS/IPS in the front-end and a firewall function right behind it (they could be in the same box or node).

For VoIP and multimedia needs, the IPS should operate at both network layers 3-4 (IP/TCP/UDP) and layer 7 (SIP, H.323, HTTP, XML, SMTP, etc.). It should attain true wire-speed performance, high throughput, with low latency, be able to support a very large number of sessions, generate few false positives, and have a high availability.

[13] It must be made clear that no security measure is sufficient on its own. The ultimate security will result from the combination of various security measures as described in this paper and that are distributed across the infrastructure to be protected.

[14] SIP Digest is somewhat simplified as compared to HTTP Digest.

[15] DDoS: Distributed DoS: a DoS attack launched from many corrupt sources in a synchronized fashion.

Firewall and NAT traversal issues and solutions

While the firewall and NAT traversal is not a security topic as such, the traversal of such infrastructure by protected flows is often an issue. Consequently it needs to be considered. The traversal of VoIP protocols through firewall and NAT infrastructure is a well-known problem. When this infrastructure is not VoIP application aware, the firewall will end up blocking incoming calls, and the NAT will cause the SIP and H.323 signaling sent out to the operator's network to contain non-routable private IP addresses.

Several techniques exist to solve this problem. Solutions such as using full SIP/H.323 proxies, multipoint control units in the DMZ, or proprietary solutions such as semi-tunnels will not be considered as they have several drawbacks such as causing latency, not being scalable, or being proprietary.

When possible, it is recommended to upgrade the firewall/NAT infrastructure to an Application Layer Gateway (ALG) type of infrastructure, which is VoIP application aware. On more recent FW/NAT infrastructures an ALG software upgrade can be available. The customer and operator should ask for advice before proceeding with such investments, as some ALG firewall/NAT implementations on the market are not fully VoIP compatible, and some inter-working problems remain.

More or less standardized solutions exist, such as Traversal Using Relay NAT (TURN), Interactive Connectivity Establishment (ICE, a Dynamicsoft proprietary solution taken up by the IETF in the MMUSIC group), and Universal Plug and Play (UPnP, a consortium supported by Microsoft).

Alcatel has implemented inter-working with UPnP in its VoIP solutions, as well as network-hosted FW/NAT traversal. The latter allows the ALG operations to be performed on SIP and H.323 signaling in a network node for the subscribers for which no other solution could be deployed (the node detects addressing mismatches in the signaling and corrects them automatically).

Conclusion

In the coming years, with an increasing number of NGN commercial rollouts, the exposure of the NGN infrastructure to attacks will increase significantly. Therefore, Alcatel believes that the trend towards the integration of more and more security in the solution's design and its operation will continue, until security becomes an integral part of any such solution and process.

Security is complex. Many aspects have to be looked at, and the security solution for VoIP and multimedia must be seen end-to-end. Both manufacturer and operator must have a security process in place. This paper has explained the most important security issues the NGN infrastructure is exposed to. For these problems, it has explained the possible solutions and discussed possible alternatives. Finally, this paper has provided an overview of the exhaustive security framework Alcatel has implemented to secure its VoIP and multimedia NGN offering end-to-end in a consistent and reliable manner.

References

[1] Service Providers Plans for Next Gen Voice, North America and Europe 2004, Infonetics Research, July 2004.

[2] ETSI, TR 101 771, version 1.1.1, "TIPHON Release 4, Service Independent Requirements Definition, Threat Analysis," April 2001.

[3] ETSI, TS 102 165-1, Version 4.1.1, "TIPHON Release 4, Protocol Framework Definition, Methods and Protocols for Security, Part 1: Threat Analysis," February 2003.

[4] 3GPP, TS 33.203, Version 6.5.0, "3G security, Access security for IP-based services (Release 6)," December 2004.

[5] J. Rosenberg, IETF, RFC 3261, "SIP: Session Initiation Protocol," June 2002.

Glossary of terms and abbreviations

ACL Access Control List
ALG Application Layer Gateway
ASP Application Service Provider
ATM Asynchronous Transfer Mode
BAS Broadband Access Server
BE Best Effort
BGP Border Gateway Protocol
BRAS Broadband Remote Access Server
CMTS Cable Modem Termination System
CORBA Common Object Request Broker Architecture
CPE Customer Premises Equipment
DDoS Distributed Denial of Service
DMZ Demilitarized Zone
DoS Denial of Service
DSL Digital Subscriber Line
ETSI European Telecommunications Standards Institute
FTP File Transfer Protocol
FW Firewall
HTTP Hypertext Transfer Protocol
HTTPS Hypertext Transfer Protocol Secured
IAD Integrated Access Device
ICE Interactive Connectivity Establishment
ICT Information and Communication Technology
IDS Intrusion Detection System
IETF Internet Engineering Task Force
IKE Internet Key Exchange
IP Internet Protocol
IPS Intrusion Prevention System
IPsec IP Security
ITSP Information Technology Service Provider
ITU International Telecommunication Union
LAN Local Area Network
MGCP Media Gateway Control Protocol
MPLS Multiprotocol Label Switching
NAP Network Access Provider
NAT Network Address Translation
NGN Next Generation Network
NM Network Management
OECD Organization for Economic Cooperation & Development
OSA Open Service Access

OSPF Open Shortest Path First
OSS Operational Support System
PABX Private Automatic Branch Exchange
PC Personal Computer
PCX Private Communication Exchange
POTS Plain Old Telephone Service
PSIRT Product Security Incident Response Team
PSTN Public Switched Telephone Network
QoS Quality of Service
RAS Remote Access Service
RSVP Reservation Protocol
RSVP-TE RSVP - Traffic Engineering
SBC Session Border Controller
SIP Session Initiation Protocol
SNMP Simple Network Management Protocol
SS7 Signaling System number 7
SSH Secure Shell
SSL Secured Socket Layer
TCP Transmission Control Protocol
TIPHON Telecommunications and Protocol Harmonization Over Networks
TLS Transport Layer Security
TNP Transport Network Provider
TURN Traversal Using Relay NAT
UDP User Datagram Protocol
UPnP Universal Plug and Play
VC Virtual Circuit
VLAN Virtual Local Area Network
VoIP Voice over IP
VP Virtual Path
VPN Virtual Private Network

Marcel Mampaey received an M.Sc. in electrical engineering at the Université Libre de Bruxelles, Belgium, in 1988. He joined the Alcatel Antwerp Research Center in 1989, working in the area of call and connection control protocols for B-ISDN networks, representing Alcatel in ETSI and ITU-T. From 1994 to 1996, he worked in the TINA-C core team in the United States and from 1998 to 2000, he represented Alcatel and TINA-C in the OMG telecom domain task force. From 2000 to 2002, he worked at Alcatel on service architecture for next generation networks. He has authored several publications, including contributions to IEEE Communications Magazine, has given presentations at various international congresses, and co-authored the book "3G Multimedia Network Services, Accounting, and User Profiles," published in 2003. In 2003, he joined the Alcatel Corporate Network Strategy Group in the Chief Technology Office, to work on NGN security architecture. He is also a distinguished member of the Alcatel Technical Academy. (Marcel.Mampaey@alcatel.be)

Olivier Paridaens has 15 years of experience in the ICT business, including more than 8 years in the security domain. He joined Alcatel in 2000 to manage the security strategy team within the Corporate Chief Technology Office. He is an external Professor at Université Libre de Bruxelles and has (co-)authored several IETF documents, conference papers and Alcatel external papers on various security topics. He also represented Alcatel at the 3GPP security group from 2000 to 2002. He is now Security Strategy Director within the Corporate Network Strategy Group at the Chief Technology Office, contributing to the definition of the overall Alcatel security strategy and setting Alcatel's future vision to build secured solutions. He also chairs the Network and Information Security committee of EICTA (European Association of ICT Industries). (Olivier.Paridaens@alcatel.be)