An Integrated Security Architecture for Next Generation Networks

Meenakshi Sundaram. R
Research Scholar
Dept. of Computer Science
St.Joseph's College
(Autonomous)
Tiruchirappalli,TamilNadu, India

Albert Rabara.S
Associate Professor
Dept. of Computer Science
St. Joseph's College
(Autonomous)
Tiruchirappalli, TamilNadu,India

Amutha.J and
Daisy Premila Bai.T
Research Scholars
Dept. of Computer Science
St.Joseph's College
Tiruchirappalli,TamilNadu, India

ABSTRACT

NGN is an IP based heterogeneous network environment, converges wired and wireless network technologies, offer a wide range of services to the customers with generalized mobility. It enables the customers to avail unrestricted services from different service providers of different networks, ensures enhanced and consistent services and reduces network and operational complexities. NGN, though, is embedded with unique characteristics of offering voice, data and video services over the same network with guaranteed quality of service, there are numerous critical security issues exist which need to be addressed. There are quite a lot of proposals for the security architecture of the NGN, but the ever growing vulnerabilities, threats and the attacks on NGN environment, demand the necessity for NGN security mechanisms. Hence, in this paper, a novel integrated security architecture for NGN has been proposed.

Keywords

NGN, Security, Vulnerability, Threat, IP-MPLS, DDoS

1. INTRODUCTION

The ever growing developments in the field of information technology have brought renaissance in the world of communication explosion as it has evolved into building Next Generation Networks (NGN), a dream of network operators, service providers and customers to provide and avail network services anywhere, anytime as always connected. NGN is the first full IP-based public telecommunications networks developed by ITU-T coordinated with various Standards Development Organizations (SDOs) such as Automatic Terminal Information Service (ATIS), European Telecommunication Standards Institute (ETSI), Telecommunications Industry Association (TIA) and 3GPP/3GPP2 (Third Generation Partnership Project) [1].

ITU-T defines NGN as, “A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users” [2].

Next Generation Networks (NGN) are intelligent, IP based infrastructure platforms capable of delivering a wide range of faster, better and cheaper communications services including voice, data, video, TV and messaging that meet evolving customers’ requirements [3]. The use of IP protocols as the foundation of NGNs gives greater flexibility and adaptability, but at the same time exposes the networks to all the security threats and attacks found on the Internet [4]. Denial of service attacks, toll fraud, information theft, and user privacy threats are very much factual in NGNs [5]. This poses a great challenge of providing robust security for NGN which will maintain safe and secure communications in inter and intra NGN environment.

The state of the art research status too recommends the need to develop dynamic reconfigurable, adaptive and autonomic security mechanisms for NGN which complicates the security issues with its heterogeneous nature of converging wired and wireless networks under the common platform [6]. Researchers have carried out the ample amount of work to resolve the security challenging issues emerge in NGN [7]. Yet there are open issues to be resolved to make NGN more reliable and adoptable [8].

Hence, in this paper, a novel integrated security architecture for NGN has been proposed. The proposed security design is an end-to-end integrated unified threat machine that provides an effective way to mitigate the modern threats and ensures effective protection without affecting the overall network performance.

This paper is organized as follows. Section II briefs the review of the literature with regard to the recent development of security mechanisms in NGN. Section III presents the proposed security architecture for NGN. An experimental study in a simulated environment and the performance results are illustrated in Section IV and Section V. Section VI concludes the paper.

2. RELATED WORK

Serap et al. have evaluated the state of the art vulnerability, threat and risk analysis methods in NGN, by analyzing the NGN security architecture model designed by ITU-T, in view of the new security requirements for NGN and they have identified the deficiencies of current security solutions to support security assessments. The authors have suggested to develop autonomic and self-adaptive systems which will be an important leap forward to ensure the security of NGN, because the attacks are unpredictable, frequent and from a wide range heterogeneous sources. They did insist that the autonomic applications and systems will be able to handle the unexpected threats with its self adaptive characteristics such as self awareness, self configuring, self healing, self protecting, context awareness, open and anticipatory which may result in the improvement of security, availability and reliability of the services requested. The challenge foreseen is that each component in NGN has to be designed with the overall architecture in mind and the delay in introducing autonomic attributes will affect the overall functionality of the NGN architecture. The research work on this area is in progress [9].

Mahdi et al. have identified the potential security challenges in 4G networks, the prerequisites for designing an efficient security module, by extending 3G security mechanism such as Authentication and Key Agreement protocol (AKA) to 4G networks such as Y-Comm, with the X.805 framework. The vulnerabilities identified exclusively for 4G networks are access control, communication security, data confidentiality, availability and privacy, which are not seen in 3G due to its homogeneous nature. This reveals that 4G systems require a more open architecture which will handle the inherent security vulnerabilities. And also the authors insist that there is a need for the integrated security module to protect data and targeted security model to protect the entities like users, servers and network infrastructures in 4G [10].

Yongsuk has made a survey of security threats on 4G networks, which cause unexpected service interruption and disclosure of information. The author has enumerated the number of potential security holes. First, the large number of external connectivity points with peer operators and service providers as well as the heterogeneous technologies accessing the infrastructure. Second, the entire network will be collapsed when a single service provider compromises, since multiple service providers share the same core network. Third, masquerading of third parties as legitimate one, will lead to service theft and billing fraud. Finally, end user equipment can be a source of malicious attacks, viruses, spam mails and calls. The author, giving possible security vulnerabilities in 4G, has insisted to develop appropriate security standards and technologies which will countermeasure the security threats [11].

Jaquith has remarked that the security of NGN systems cannot be determined in absolute terms because there is no security measurement definition and tool has proven its logical and mathematically validity. He has insisted that the appropriate security measurements and metrics are the most fundamental elements to evaluate whether new security scenarios or solutions have positive or negative effects upon the NGN network and its services. The author has suggested to fabricate the security measurements for NGN [12].

Sakib et al. have spelled out the different security vulnerabilities found in the existing NGN system such as possibilities to forge key messages, unauthenticated messages and man in the middle attack. To mitigate these vulnerabilities and to enhance the security level, they have proposed modified Diffie-Hellman key exchange protocol by using random numbers and function generation process. They did recommend the need for more reliable, flexible, secure methods for NGN, since it adopts different applications, offers different services having own authentication methods and using different credentials [13].

Diab et al. have proposed a new seamless vertical handover solution performing fast authentication while guaranteeing the QoS and the security of real-time communications over next-generation heterogeneous access networks. They have proposed an Enhanced Inter-Domain Manager (E-IDM) module to provide security functionalities by exchanging the information required to perform mutual authentication. Security parameters and authentication keys are stored in E-IDM for that purpose. The performance of the proposed solution is compared with conventional schemes such as FMIPv6 and the basic MIPv6 when applying the authentication over 3G networks in terms of signaling cost and packet loss and found to be efficient in achieving security. The authors further suggest to equip the next-generation heterogeneous access network systems with protections and security mechanisms to avoid risks of intrusion hacking and spamming [14].

Nazrul et al. discussed the incompatibility issues exist between IPv4/IPv6 translation gateway and IPSec. They have pointed out that the existing solutions to address the compatibility issues between translation gateway and IPSec are either to enhance the translation gateway operation or to modify IPSec architecture especially on the IKE negotiation process. Realizing the fact that most of the intermediate networking devices such as translation gateway are beyond the end nodes administration, they have proposed a new IKE authentication by using Address Based Keys (ABK) mechanism with certificateless authentication based on bilinear pairing over an elliptic curve to secure the communication channel between end nodes using their end IP addresses as public/secret keys for authentication. This proposed scheme significantly reduces system complexity and the cost for establishing and managing the public key authentication such as PKI. Implementing this design in NGN requires stronger security mechanisms to ensure confidentiality, integrity and availability [15].

Paolo has described the security issues that service providers and operators are facing in interconnecting core NGN to the customer’s home networks or customer premises networks (CPN) which is a special case of local area network. The security challenges encountered in CPN are denial of services, eavesdropping, masquerade, and social threats for instance SPAM and SPIT (SPAM over Internet Telephony) attacks. Identifying the threats, the author has listed out the existing countermeasures such as firewalling, network access control, intrusion detection systems, network address translation traversal and anti SPIT mechanisms, which can be implemented within the home gateway. Foreseeing the complexity of implementing security mechanisms at the customer premises, the author suggests that the autonomic computing could be a best solution where the CPN devices are able to manage autonomously the security mechanism with little interaction with management centers [16].

The review of the literature reveals that the research work towards mitigating the security issues arise in NGN environment is an ongoing process. Though a considerable amount of research work has been carried out in these areas, there are open and unresolved issues exist which hamper to provide end to end security for NGN. Hence, a novel, integrated security architecture for NGN has been proposed.

3. PROPOSED INTEGRATED SECURITY ARCHITECTURE

The unique feature of the proposed architecture is a multi-layer structure consists of operational layer, core network layer, access layer and application layer. In the operational layer, security spans the entire IP NGN architecture, protecting a service throughout the network to maintain service availability in the event of an attack. In the core network layer, security is built on the hardware and operating systems to secure the transport of services. In the access layer, security creates protection for users and forms a protection ring towards the core network infrastructure. In the application layer, security is resident in the applications themselves and links to the service layer to secure the integrity of the applications as they interface with the network. The proposed architecture is built around three levels of security with complete control: Level 1 - Network level protection for distributed denial of services (inter/intra NGN network), Level 2 - Access level security at the edge

(VLAN, MAC filtration, QoS), Level 3 - User level security (Authentication, Authorization and Profiling). Fig 1 depicts the proposed integrated security architecture for NGN.

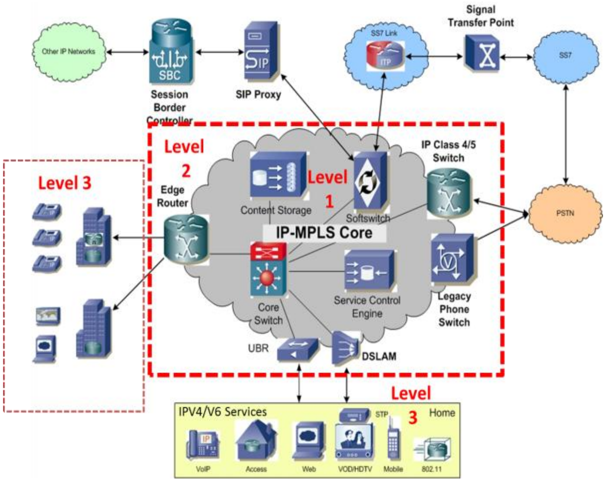


Fig 1: Integrated Security Architecture for NGN

This architecture uses Net Flow, a network telemetry to study the traffic patterns in real time, creates traffic baselines, detects anomalies and misuse, characterizes affected interfaces and handles threats in an effective way.

3.1 Level 1: Network Level Security for Distributed Denial of Services (Inter / Intra NGN)

Denial of Service (DOS) attacks happen when a hacker or malicious user gets physical access to the UNI or attacks the UNI from a remotely attached device on the customer bridge. These types of attacks are intended to bring a network to a state in which it can no longer carry legitimate user data. This is accomplished by attacking network components or by flooding the network with extraneous traffic. These attacks fall under two main classes such as spoofing attacks and flooding attacks. These occur via inter and intra NGN network.

3.1.1 Mitigation of attacks at level 1in hybrid NGN

Spoofing attacks are mitigated by deployment of AAA service (Authentication, Authorization and Accounting) per user per service and the services offered by each provider are secured by provisioning MD5 with authentication key and enablement of IPSec / MPLS VPN options. To mitigate flooding attacks, network traffic pattern is compared against the normal traffic patterns. If there is any anomaly signature traffics are observed, it is considered as a security attack detection. Net Flow is used along with tools like Arbor, to detect security attack in the core infrastructure. In hybrid NGN architecture, DDoS attack detection and mitigation can be employed under two scenarios. First DDoS protection for traffic flow between NGN to NGN and then between NGN to NoN-NGN.

3.1.1.1 Inter NGN DDoS Protection

The security component and configuration present in the hybrid core network collect and monitor the data flow based on the QoS netflow parameters specified from within the NGN network. Once it observes any anomaly, attack is confirmed and it auto mitigates /activates the protection for the specified IPv4/v6 customer WAN addresses. The customer IP is taken as self IP and reroutes the traffic to self and pre-established BGP session. Multi-GB attack routes the traffic through core security mitigation centers and scrubbed traffic is returned to the destination over dedicated IP Edge egress via GRE tunnel. Thus the attack from outside to any of the customer or core network is prevented via this DDoS mitigation mechanism.

3.1.1.2 Intra NGN DDoS Protection

In this scenario, when the attack is observed, the security component, auto mitigates/activates the protection for the entire subnet of IPv4/v6 addresses, since the attack is from a transit NoN NGN network; a BGP session is established and Multi-GB attack routes the traffic through core security mitigation centers and scrubbed traffic is returned to the destination over the Non NGN network IP edge egress via GRE tunnel. Thus the attack via NoN NGN network to any of the customer or core network is prevented via this DDoS mitigation mechanism.

3.2 Level 2: Access Level Security at Edge (VLAN MAC Filtration)

The possible attacks encountered at the access level are MAC attacks, PDU storms, VLAN hopping, VLAN broadcast storm, ARP attacks, STP attacks and VLAN leaking. It is the task of the service providers to guard their users from rapidly growing security risks. The following features prevent the threats posed by DoS attacks and hackers trying to access sensitive user data.

3.2.1 VLAN Security

In layer 2 environment, user isolation is achieved using the Private VLAN or Protected Port feature. These features allow users to be on the same VLAN, but at the same time prevent them from getting access to each other. With the “Protected Port” feature, all user ports are configured as “protected” while the two gigabit Ethernet ports are configured as “non-protected” and can therefore receive and transmit information from the protected user ports. Private VLAN with protected port share only securing ports on the same switch, all switches in a ring are assigned a unique VLAN id. Information that needs to be sent between the users connected to the same switch, like IP-telephony, gaming, etc., needs to go down to the first L3 switch and then back up to the receiving port.

However, it is not normal behavior for a router to forward IP ARP’s on the same VLAN or the same subnet; by design, the proxy ARP function does not reply to ARP requests for hosts on the same subnet. To solve this problem, a new feature called local Prpxy ARP was introduced on most L3 switches. The local proxy ARP feature allows the router to respond to ARP requests for IP addresses within a subnet where normally, no routing is required. With the local proxy ARP feature enabled, the router responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet.

3.2.2 Traffic Suppression

In L2 ring architecture, ring to ring security is achieved through ACL filtering and routing capabilities on the Cisco 7609. For example, VACL could be used in 7609 to filter NetBios, Appletalk or some other protocols. Broadcast suppression can be used to limit the amount of broadcast traffic on a given port as a percentage of the total bandwidth. Broadcast Suppression is usually set between 30 to 35%.

3.2.3 Traceability

There is a regulatory requirement of having to track which subscriber (port) owns which IP address at any given time. This information needs to be logged in real time and kept for a long period of time, usually years. Hence broadband needs the ability to tie an IP address to a MAC address and to specific port with this information, broadband can pinpoint the physical location of any user within the network in the event of DoS attacks. This information can also be used for access control and billing purposes. Traceability starts with subscriber identification which can be done via subscriber logging, or by using the MAC address or by having the access switch dynamically identifying the end user via DHCP Option 82.

3.2.4 Limiting the number of MAC Addresses

"Port Security" allows service providers to dynamically control the number of MAC addresses per Ethernet port. This capability enables them to limit the number of devices that can access the network using the same Ethernet port.

3.2.5 Scavanger Class

The Scavenger class is a critical component to the DoS/worm mitigation strategy.

3.3 Level 3 - User Level Security

The proposed user level Security architecture consists of device authentication, NGN service authentication, port authentication, subscriber authentication based on MAC and DHCP option 82.

3.3.1 Device Authentication

The three factor verification is carried out, which is a combination of unique IMEI number or serial number, WLAN MAC address of the device and the username and password for accessing NGN service. The user gets verified against the stored database and if any details do not match, access is denied to the user and after 3 failed attempts device gets blocked automatically. Further to activate user needs to reregister the MAC and IMEI with the service provider to avail the services.

3.3.2 NGN Service Authentication

The Service authentication is done with SSG/SESM and portal RADIUS. The SSG/SESM will display a login page when the user tries to access any service not offered by broadband. If the information matches, services will be provided. Services like access to the broadband servers, voice and video will not pass through the BRAS and authentication will be done by the end applications themselves.

3.3.3 Subscriber Identification

Subscriber identification refers to identifying, from which switch and port number a DHCP request originates. This is very important for user traceability and for the possibility of assigning different user profiles to each port. The various techniques used for subscriber identification are MAC notification and DHCP Option 82. The MAC Notification method is very similar to the VQP/VMPS method. When the access switch detects a new MAC address on a port, it sends an SNMP message to the management system and this information is populated in the customer's database. Port authentication and user traceability are achieved by using DHCP Option 82. It requires the Relay Agent (the Access Switch) to intercept the DHCP request and fill in option 82, which contains switches and port information to identify the user location. This information enables the service gateway to verify, if the port has access to the service and then associates a subnet with this port, which is then used for traceabillity.

4. EXPERIMENTAL STUDY

The main focus of the experimental study is to test the functionalities of the heterogeneous IPv4/IPv6 based NGN network with respect to security. The results are tabulated and depicted.

4.1 Experimental Set-up Test Bed

The proposed architecture is tested in a service provider lab environment. The test lab is an illustration of a secured integrated heterogeneous NGN environment. This design consists of the MPLS IPv4, IPv6 simulating as the core and accesses, the Internet exits simulating as dual homed environment, layered security design based on firewalls and authentication platform.

There are two simulated authenticating server, database SIP servers placed under the integrated platform on a VMware platform for three factors user authentication and SIP call routing and testing. Ixia network traffic generator is used. The Security test bed consists of an integration of QoS Scavenger class detection triggering a DDoS protection system. This prevents attack not only from the core, but end to end customer services as well. The flow collector configured as part of QoS, does flow analysis and sampling to have router record information about the IP packets that traverse through an interface.

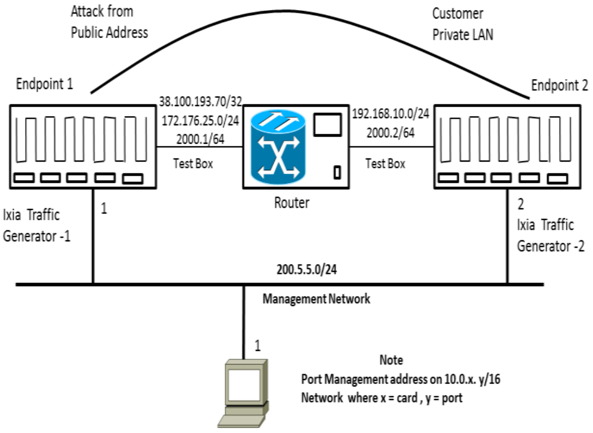


Fig 2 DDoS simulation test bed

Packets having similar characteristics are grouped together in a flow. A flow is defined as a set of packets that have the following in common: source IP address, destination IP address, layer protocol type and input logical interface. Fig 2 shows the setup that will be used for the test cases of DDoS. All addresses used in the course of testing appear in this figure, including both IPv4 and IPv6 addresses. Only two physical Ixia ports are used in this scenario.

5. PERFORMANCE ANALYSIS

The primary goal of this simulation experiment is to investigate the performance, whether the proposed architecture ensures end-to-end security while delivering services to the customers in a hybrid NGN environment with respect to DDoS attacks.

5.1 Security Testing

5.1.1 Core /Access Protection - DDoS Attack Testing

DDoS attack simulation is done to assess the impact of DoS traffic on existing network traffic, to measure the performance of devices responsible for denying DoS traffic network access and to determine the performance of network devices that are being attacked (e.g. routers, WLAN access points). The simulation consists of generating DoS traffic between two Ixia ports and measuring the performance of the overall network, directing DoS traffic against a specific QoS pattern and router while generating and measuring the performance of application traffic being sent between two customer endpoints. In each case, performance measurements were taken with both DoS filtering/blocking solutions being enabled as well as disabled. The below mentioned three attacks were simulated and results were recorded.

5.1.1.1 SYN Attack

Every TCP connection begins with a single TCP SYN flag being sent from the client host to a server. In response to receiving such a flag, the server typically allocates resources and then sends a TCP SYN-ACK packet back toward the client host station. A SYN attack overwhelms the victim computer with a rapid succession of SYN packets, causing it to over allocate resources and either crash or wait for the allocated resources to time out.

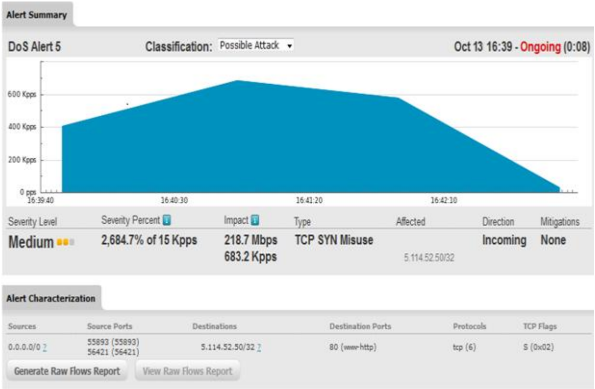
5.1.1.2 Ping Attack

An ICMP Ping Request is sent to a server at a high rate, causing bandwidth problems on the server’s network.

5.1.1.3 Ping of Death (POD) Attack

ICMP Ping Requests are sent from a client to a server; however, each packet is a fragment of a complete Ping Request of extremely large size. This may cause the Router to over allocate resources and crash.

Fig 3 depicts the bandwidth allocated to test the customer in the Y axis and the timestamp in the X axis. In this testing traffic of 683 Kbps, which is 281 Mbps was simulated as a TCP SYN attack from a source of 5. X, with a medium level of threat severity.



Alert Summary

DoS Alert 5 Classification: Possible Attack Oct 13 16:39 - Ongoing (0:08)

Severity Level	Severity Percent	Impact	Type	Affected	Direction	Mitigations
Medium	2,684.7% of 15 Kpps	218.7 Mbps 683.2 Kpps	TCP SYN Misuse	5.114.52.50/32	Incoming	None

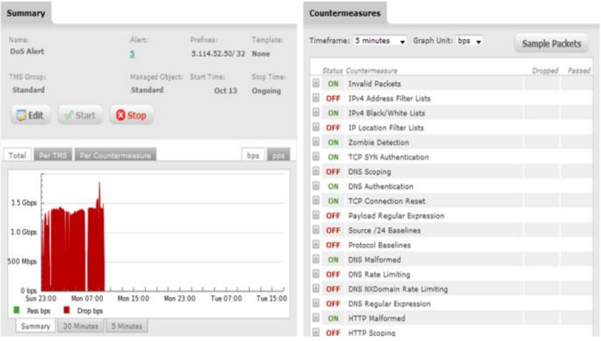
Alert Characterization

Sources	Source Ports	Destinations	Destination Ports	Protocols	TCP Flags
0.0.0.0/0 ?	55893 (55893) 56421 (56421)	5.114.52.50/32 ?	80 (www-http)	tcp (6)	S (0x02)

Fig 3: DDoS TCP SYN attack simulation in the core

It also illustrates that the DDos SYN attack is, in progress, in the core network. Fig 4 represents the SYN attack traffic mitigation / prevented / dropped by the core security device.

After applying the security configuration in the core, approximately 1.5 Gbps of traffics are dropped. This shows the architecture is secured against any denial of service attacks.



Summary

Name: DoS Alert
Alert: 5
Prefixes: 5.114.52.50/ 32
Template: None
TMS Group: Standard
Managed Object: Standard
Start Time: Oct 13
Stop Time: Ongoing

Countermeasures

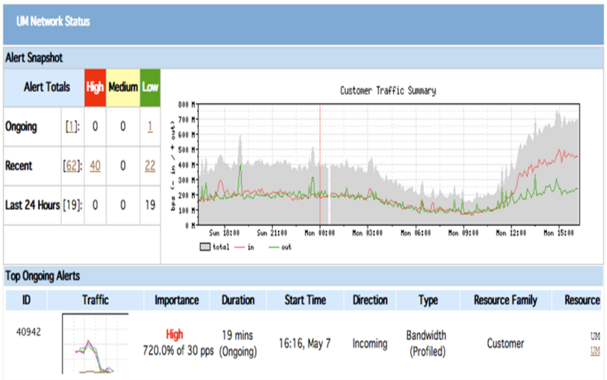
Timeframe: 5 minutes Graph Unit: bps

Status	Countermeasure	Dropped	Passed
ON	Invalid Packets		
OFF	IPv4 Address Filter Lists		
ON	IPv4 Black/White Lists		
OFF	IP Location Filter Lists		
ON	Zombie Detection		
ON	TCP SYN Authentication		
OFF	DNS Scoping		
ON	DNS Authentication		
ON	TCP Connection Reset		
OFF	Payload Regular Expression		
OFF	Source /24 Baselines		
OFF	Protocol Baselines		
ON	DNS Malformed		
OFF	DNS Rate Limiting		
OFF	DNS NXDomain Rate Limiting		
OFF	DNS Regular Expression		
ON	HTTP Malformed		
OFF	HTTP Scoping		

Fig 4: Dropping of malicious packets of the DDoS TCP SYN attack

5.1.2 Customer Edge Protection Level DDoS

Fig 5 represents the dashboard of customer traffic with respect to a DDoS attack. This simulation shows that the current progress of 1 low category attack under simulation 40942 as well as 40 high category and 22 low category attacks which were already simulated and recorded for the reference.



UM Network Status

Alert Snapshot

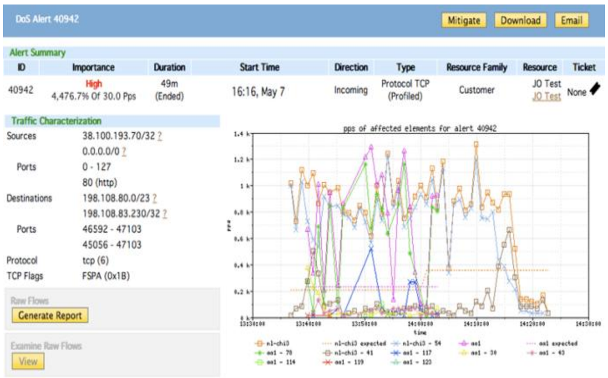
Alert Totals		High	Medium	Low
Ongoing	[1]:	0	0	1
Recent	[62]:	40	0	22
Last 24 Hours	[19]:	0	0	19

Top Ongoing Alerts

ID	Traffic	Importance	Duration	Start Time	Direction	Type	Resource Family	Resource
40942		High 720.0% of 30 pps	19 mins (Ongoing)	16:16, May 7	Incoming	Bandwidth (Profiled)	Customer	UM UM

Fig 5: DDoS attack simulation on customer edge 40942 and historical data of other attacks

Fig 6 depicts the sample 40942 on-going TCP SYN DDoS alert attacks. Packets are generated using Ixia traffic generator for about 49 minutes for managed object 38.100.193.70/32. It also represents CE level protocol analysis of DDoS attack with a bandwidth size of 1.4 K and its effected simulated network managed objects’ IP address and router elements.



DoS Alert 40942

Alert Summary

ID	Importance	Duration	Start Time	Direction	Type	Resource Family	Resource	Ticket
40942	High 4,476.7% Of 30.0 Pps	49m (Ended)	16:16, May 7	Incoming	Protocol TCP (Profiled)	Customer	JO Test JO Test	None

Traffic Characterization

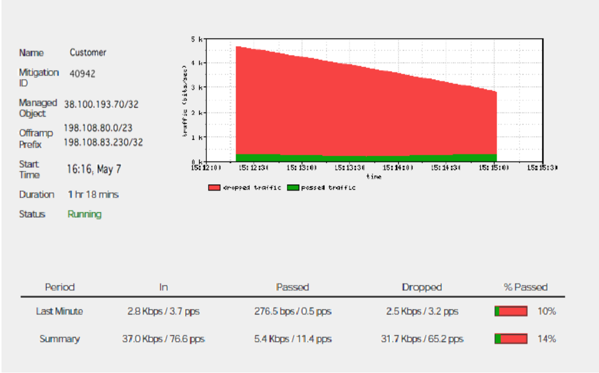
Sources	38.100.193.70/32 ? 0.0.0.0/0 ?
Ports	0 - 127 80 (http)
Destinations	198.108.80.0/23 ? 198.108.83.230/32 ?
Ports	46592 - 47103 45056 - 47103
Protocol	tcp (6)
TCP Flags	FSPA (0x1B)

Raw Flows

Examine Raw Flows

Fig 6: DDoS attack simulation on customer edge 40942

The proposed security configuration, studies the base line netflow and recognizes the attack and mitigate the traffic i.e. the customer IP is taken as self IP and reroutes the traffic to self and pre-established BGP session and Multi-GB attack routes the traffic through core security mitigation centers and scrubbed traffic returned to the destination over dedicated IP edge egress via GRE tunnel.



Name	Customer
Mitigation ID	40942
Managed Object	38.100.193.70/32
Offramp Prefix	198.108.80.0/23 198.108.83.230/32
Start Time	16:16, May 7
Duration	1 hr 18 mins
Status	Running

Period	In	Passed	Dropped	% Passed
Last Minute	2.8 Kbps / 3.7 pps	276.5 bps / 0.5 pps	2.5 Kbps / 3.2 pps	10%
Summary	37.0 Kbps / 76.6 pps	5.4 Kbps / 11.4 pps	31.7 Kbps / 65.2 pps	14%

Fig 7: Gradual drop of malicious traffic and passing of legitimate traffic

Fig 7 represents the mitigation process of 40942 sample attack, where the red (black) represents the dropped traffic and the green (gray) represents the permission of the legitimate traffic over a duration of 1hour and 18 minutes for managed object 38.100.193.70/32.

The results assure that the customer edge, provider edge and core are completely protected against any kind of attacks with the security mechanism deployed in the proposed architecture.

6. CONCLUSION

The proposed integrated security architecture for NGN provides end-to-end security for the delivery of quad play data, voice and video anywhere, anytime, any device across any access technology in a hybrid NGN environment against DDoS attacks. The performance analysis results guarantee the network security and ensures the network operators, service providers and the customers, have the benefits of migrating and availing the services to and from hybrid IP-MPLS NGN scenario.

7. REFERENCES

[1] ITU-T Technical Paper. 2013. Migration Scenarios from Legacy Networks to NGN in Developing Countries.

[2] ITU-T Recommendation Y.2401. 2006. Principles for the Management of the Next Generation Networks.

[3] Graham Titterington. 2011. Developing Secure NGN Infrastructure. OVUM Publications.

[4] T. im Kridel. 2010. Next Generation Network Secuirty. Intel Software Adrenaline.

[5] Tzouanopoulos Dionysis. 2012. Secuirty issues at NGN Networks. University of Piraeus. Piraeus-Greece.

[6] Dr. Mustafa Shakir. 2010. Challenging Issues in NGN Implementation and Regulation. IEEE.

[7] M. Hossein Ahmadzadegan, M. Elmusrati, and H. Mohammadi. 2013. Secure Communication and VoIP Threats in Next Generation Networks. International Journal of Computer and Communication Engineering. Vol. 2, No. 5.

[8] Mi-Jung Choi and James Won-Ki Hong. Towards Management of Next Generation Networks. POSTECH. Korea.

[9] Serap Atay, Marcelo Masera. 2011. Challenges for the security analysis of Next Generation Networks. Information Security Technical Report. Elsevier.

[10] Mahdi Aiash, Glenford Mapp and Aboubaker Lasebae, Raphael Phan. 2010. Providing Security in 4G Systems: Unveiling the Challenges. Sixth Advanced International Conference on Telecommunications. IEEE.

[11] Yongsuk Park. A Survey of Security Threats on 4G Networks” Samsung Advanced Institute of Technology. Korea.

[12] Jaquith A. 2007. Security Metrics Replacing Fear, Uncertainty and Doubt. Addison Wesley.

[13] A.K.M. Nazmus Sakib, Fauzia Yasmeen, Samiur Rahman, Md.Monjurul Islam, Dr. Md. Matiur Rahaman Mian. Security Thread Analysis & Solution for NGN. International Journal of Engineering Research and Applications. Vol. 1, Issue 4, pp. 1448-1452.

[14] Wafaa Bou Diab, Samir Tohme. 2009. Seamless Handover and Security Solution for Real-Time Services. 11th IEEE International Symposium on Multimedia. IEEE.

[15] Nazrul M. Ahmad and Asrul H. Yaacob. 2010. End to End IPSec Support across IPv4/IPv6 Translation Gateway. Second International Conference on Network Applications, Protocols and Services. IEEE.

[16] Paolo DE LUTIIS. 2010. Managing Home Networks Security Challenges, Security Issues & Countermeasures. IEEE.