



Ensure 911/112 emergency calls get through 24 x 7

Harnessing ESInet to defend against DDoS/TDoS attacks

White paper

As the use of digital technologies has become prevalent, many 911/112 authorities are upgrading their public safety answering points (PSAPs) to support next-generation 911/112 (NG911/NG112). Because NG911/NG112 is now connected to the internet, this greatly expands the attack surface of cyber threats, especially for distributed denial of service, telephony denial of service (DDoS/TDoS) attacks. This white paper explains the attack methods and how to mitigate the threats by harnessing ESInet.

Contents

911/112 is our lifeline	3
Protecting NG911/NG112 from DDoS/TDoS attacks	3
DDoS/TDoS attack methods	5
TCP SYN flood attack	5
UDP flood attack	6
SIP INVITE flood attack	6
Reflection/amplification attack	7
Multi-vector attacks	8
Mitigating the DDoS/TDoS threats	8
Infrastructure overprovisioning	8
Two-tier defense with a border router	9
Analytics-driven DDoS protection	9
A DDoS/TDoS defense blueprint for NG911/NG112	11
Tier-1 defense	11
Tier-2 mitigation defense	13
Keeping our lifeline open for real emergencies	13
Abbreviations	14

911/112 is our lifeline

As the use of digital technologies such as smart phones, wearable devices and CCTV has become prevalent, many 911/112 authorities are upgrading their public safety answering points (PSAPs) to support next-generation 911/112 (NG911/NG112).

To broaden situational awareness and provide faster and more effective response to citizens in emergency need, the 911/112 infrastructure must be able to seamlessly receive emergency calls requesting assistance and to accept new digital information (such as real-time text, images and video calls) from any networked device.

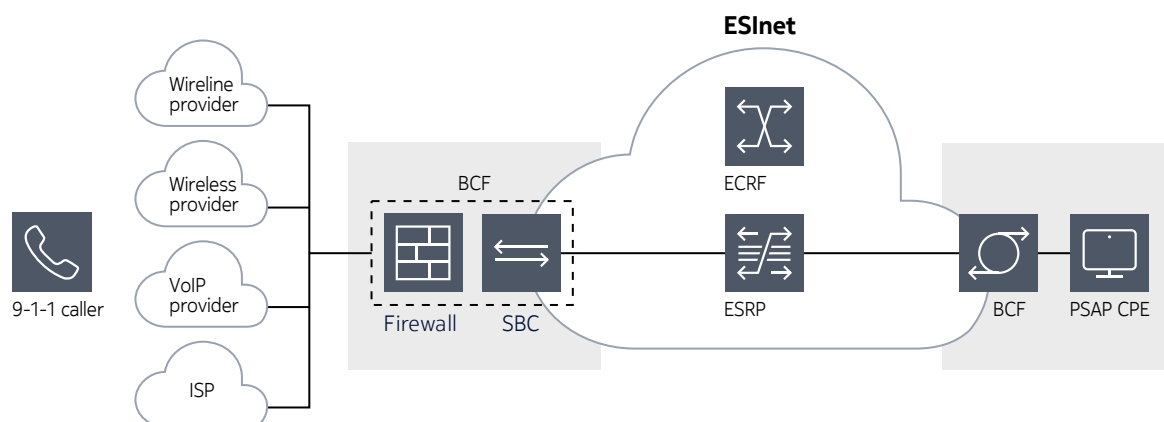
NG911/NG112 extends the connections of PSAPs and ESInets¹, its communications foundation, beyond the regular wireline and wireless phone networks to the internet. However, when NG911/NG112 connects to the internet, it is exposed to new and evolving cyberattack threats that can disrupt 911/112 communications and even PSAP operations, making emergency communications services unreliable or even unavailable.

According to a US Federal Communications Commission (FCC) [report](#), a one-minute decrease in ambulance response time reduces the 90-day mortality rate of patients by 17 percent. This statistic highlights the crucial importance of 24 x 7 accessibility to emergency communications services to save lives and protect citizens. Therefore, it is imperative that the NG911/NG112 infrastructure can withstand cyberattacks, keeping emergency services up and running at all times.

Protecting NG911/NG112 from DDoS/TDoS attacks

With viruses, ransomware and malware becoming widespread, cyber risks have become a real and constant threat to 911/112 service and PSAPs because NG911/NG112 infrastructure is connected to other network domains, particularly the internet. To combat this threat, the NENA i3 solution architecture has placed a border control function (BCF) at the edge of ESInets interconnecting with other networks (including the internet) that serve 911/112 callers (see Figure 1)². Sitting between an ESInet and external networks as well as other agency networks, the role of the BCF is to prevent, detect and block cyberattacks.

Figure 1. BCF as the demarcation point between ESInet and other network domains



As shown in Figure 1, the BCF comprises a firewall and a session border controller (SBC).

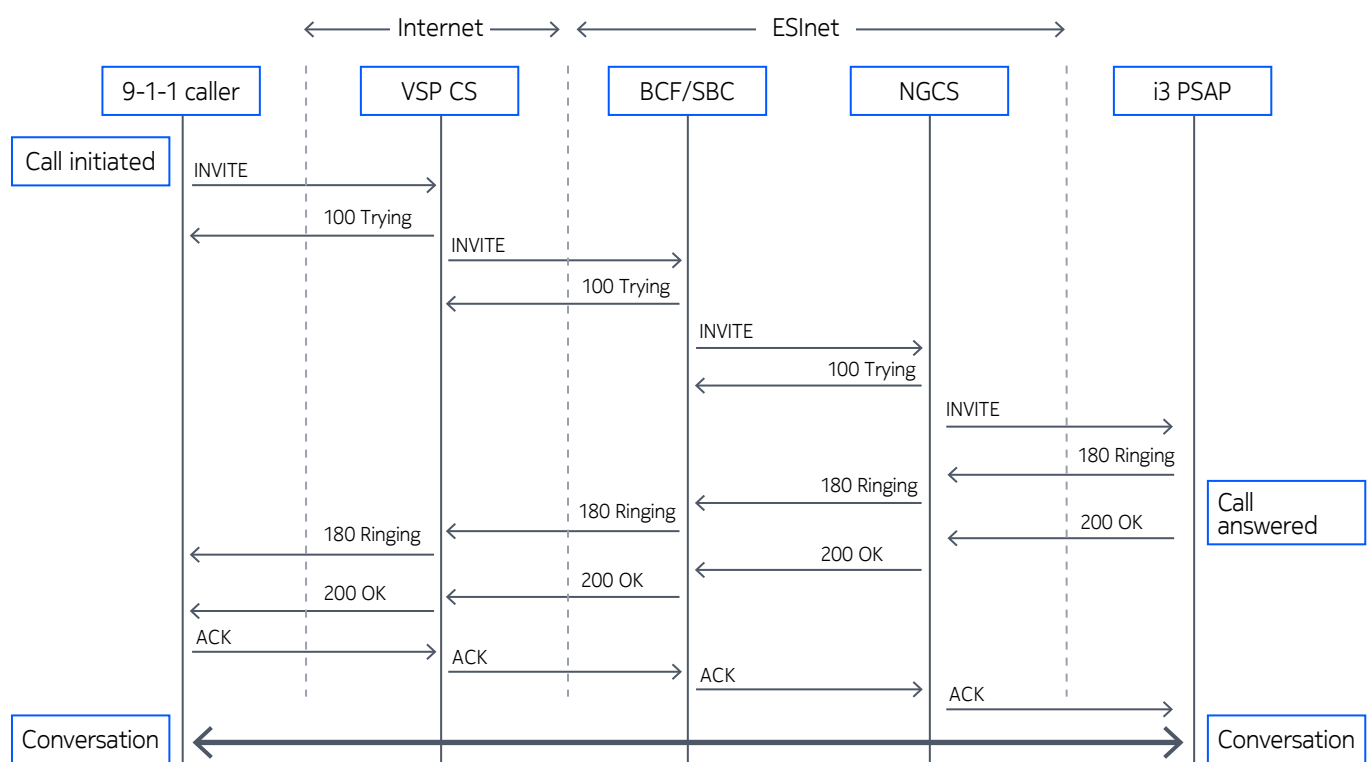
¹ For a more detailed discussion of ESInet, read the Nokia application note [“Providing highly dependable 9-1-1 emergency response services.”](#)

² For a detailed description of the NENA i3 solution, read the [NENA Detailed Functional and Interface Standards for the NENA i3 Solution](#), especially section 5.1 for BCF.

The firewall inspects all incoming traffic and stops illicit traffic from reaching the SBC. Typical firewall rules include permitting Session Initiation Protocol (SIP) connections to destination port number 5060. The firewall also inspects the media traffic encapsulated in the Session Description Protocol by opening a pinhole for authorized media streams.

An SBC is an application-layer gateway acting as a SIP proxy server. It terminates the incoming SIP sessions and creates new SIP sessions towards the emergency services routing proxy/emergency call routing function (ESRP/ECRF) in the NG911/NG112 domain after inspecting the SIP messages and searching for malicious ones. Then, based on caller location and other call information, the ESRP/ECRF routes the SIP messages to a telecommunicator in a PSAP (see Figure 2).

Figure 2. A simplified NG911/NG112 call flow



The SBC component of the BCF plays a critical role in thwarting cyberattacks, particularly network-layer attacks using traffic with unused TCP/UDP ports. However, the wide adoption of the Internet of Things (IoT) has changed the cyber security landscape and given rise to distributed denial of service (DDoS) attacks, requiring new cyber security measures to complement BCF security.

DDoS is a malicious attack that attempts to make a service or a host unavailable to legitimate users by flooding it with a high volume of traffic³. A DDoS attack typically tries to overwhelm the target application or server in one of two ways:

- By sending more requests than the target application or server can possibly handle
- By sending a gargantuan volume of traffic to clog the network connected to the target, thereby preventing legitimate requests from ever reaching the application or server; this process is called volumetric DDoS.

³ The NENA Next Generation 9-1-1 Security (NG-SEC) Information Document, section 3.8 also provides an excellent description of a DDoS attack.

The attacker orchestrates the attack by using a multitude of compromised connected devices globally across the internet (from hosts to CCTV cameras to IoT devices such as sensors) as sources of attack traffic. The attack takes down the target and the network infrastructure, preventing users and customers from accessing the services. The impact is worsening as [DDoS attack frequency and volume increases](#).

A specialized form of DDoS is telephony denial of service (TDoS), which instructs compromised devices to send a high volume of illicit traffic toward the ESInet. By jamming the internet pipes to the ESInet or exhausting the BCF resources with fake call attempts, legitimate 911/112 emergency calls cannot be processed, depriving citizens in need from emergency help. TDoS is analogous to a traffic jam delaying the arrival of emergency vehicles.

DDoS/TDoS attack methods

Formulating effective security measures to defend NG911/NG112 requires an understanding of SIP, an application-layer signaling protocol for establishing, modifying and terminating multimedia sessions. SIP is used in NG911/NG112 to establish media sessions between callers and telecommunicators in PSAPs. As an application-layer protocol, SIP rides on top of a transport layer protocol. The two transport protocol options are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

The following sections describe some common attack methods used by cyber attackers when launching a DDoS/TDoS attack on an NG911/NG112 system, particularly on the BCF⁴.

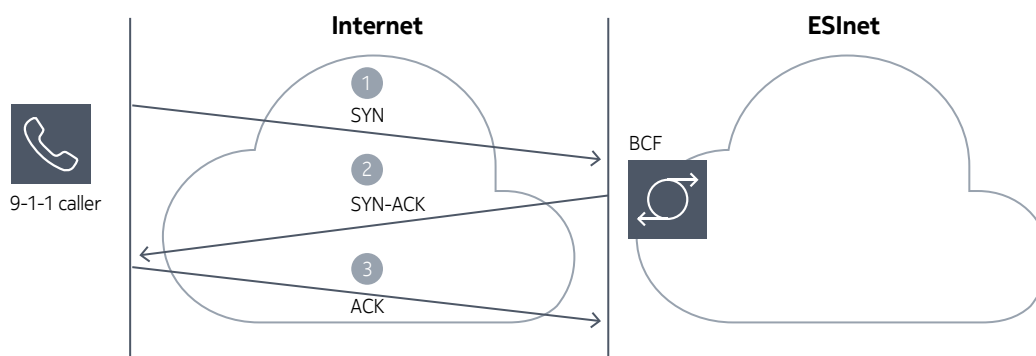
TCP SYN flood attack

Exploiting the TCP three-way handshake mechanism that establishes a connection for SIP communications, a TCP SYN flood attack is one of the most prevalent DDoS attacks on the internet.

The TCP three-way handshake mechanism works as follows (see Figure 3).

1. The BCF receives the SYN (synchronize) packet sent by the 911/112 caller who wants to initiate a 911/112 call.
2. The BCF acknowledges by sending a SYN-ACK (synchronize-acknowledge) packet back to the caller and changing the state of the TCP port to open.
3. The 911/112 caller responds with an ACK (acknowledge) packet. The TCP connection is then established for a SIP session.

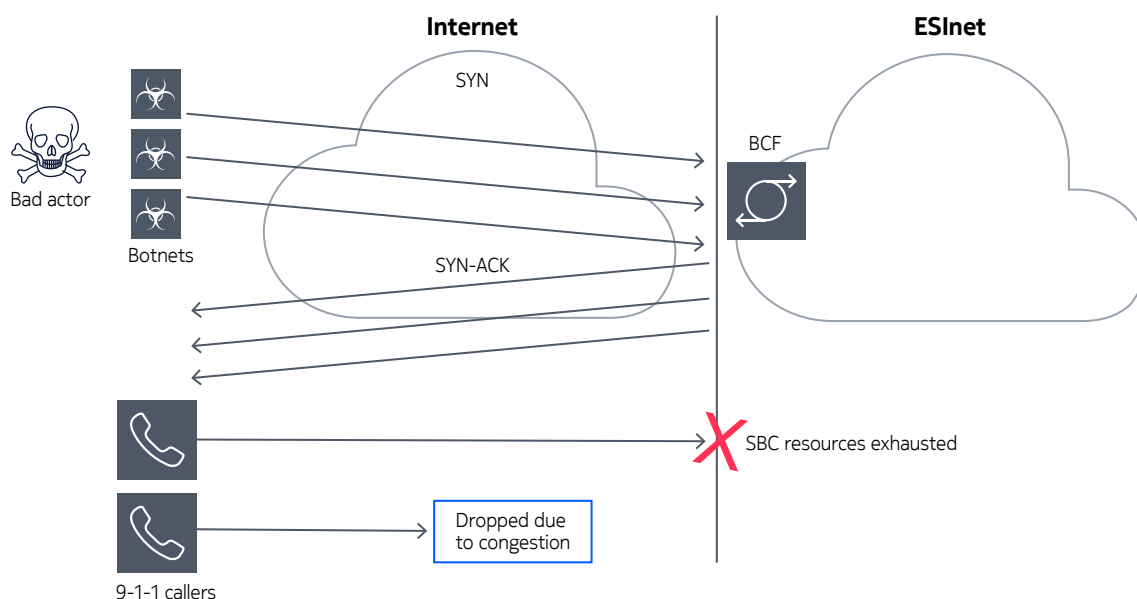
Figure 3. TCP three-way handshake initiation



⁴ For a more detailed discussion of DDoS attack vectors, read the Nokia application note [“Volumetric DDoS mitigation.”](#)

In a DDoS/TDoS attack using the SYN flood vector, the attacker amasses multitudes of virus-infected internet-connected devices (known as a botnet) to send SYN packets with a spoofed source address. (A spoofed source address is a technique using a fake address instead of the real address). Because the BCF responds with SYN-ACK packets for every SYN packet and waits endlessly for an ACK reply, the BCF's memory resources can be overwhelmed as the attacker repeatedly sends SYN packets to different ports on the SBC. Furthermore, the sheer volume of SYN packets can clog the network trunk that connects to the BCF; this can cause legitimate 911/112 emergency calls to be dropped, denying service to citizens who need emergency assistance (see Figure 4).

Figure 4. TCP SYN flood attack denies 911/112 emergency service to citizens in need



UDP flood attack

UDP is another transport option used by SIP. A UDP flood attack exploits the fact that the server reserves compute resources when receiving packets from ports that it is monitoring. In a DDoS/TDoS attack with UDP flooding, similar to a TCP SYN flood attack, multitudes of UDP packets targeting random ports are sent to the BCF in an attempt to overwhelm the BCF resources. For example, when the firewall allows in a UDP packet with a new destination port number, the firewall opens a “state” to the UDP session. A UDP flood attack exhausts the firewall memory resources.

Like a volumetric TCP SYN flood attack, a volumetric UDP flood attack can also clog the network trunk to the BCF, causing legitimate 911/112 emergency calls to be dropped.

SIP INVITE flood attack

Another common DDoS/TDoS attack is a SIP flood attack, which targets port number 5060 with SIP messages. The most common SIP message used is INVITE. Each time the BCF receives a SIP INVITE message, the firewall opens a state to track the UDP/TCP connection.

Furthermore, SIP is an application-layer protocol of a transactional nature: each transaction consists of a request and its corresponding responses. As a result, the SBC maintains the INVITE transaction state until the transaction timer expires if no ACK message is received. Flooding the SBC with SIP INVITE messages exhausts the SBC's memory and CPU resources, rendering it unable to accept legitimate 911/112 emergency calls.

Reflection/amplification attack

A reflection attack is another common volumetric DDoS attack that involves eliciting a response from a server on the internet to the target. The attacker typically sends a query message to a server with a spoofed IP address that belongs to the victim, and the server (commonly called the amplifier) then responds to this address.

Reflection attacks become even more damaging when the attacker exploits the application protocol to generate a disproportionately long packet, amplifying the attack traffic.

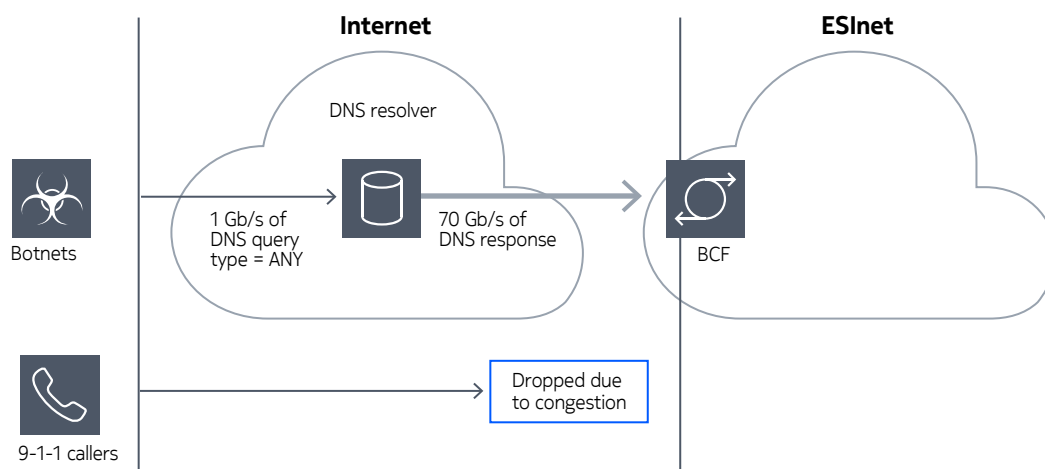
In the past, most of these attacks exploited UDP-based protocol loopholes. However, attackers have also started to exploit TCP-based application protocol loopholes.

UDP-based reflection/amplification attack

The UDP-based reflection attack most relevant to NG911/NG112 cybersecurity is related to the Domain Name Service (DNS) Protocol, which is essential for PSAPs to access information on the internet. A commonly exploited loophole is that a DNS query of the type “ANY” elicits the DNS server to respond with all known information about a DNS zone, typically resulting in a 70:1 amplification factor.

As shown in Figure 5, a 1 Gb/s flood of DNS requests results in 70 Gb/s of DNS response traffic targeting the SBC, overwhelming the target and its network infrastructure .

Figure 5. TA DNS reflection/amplification attack

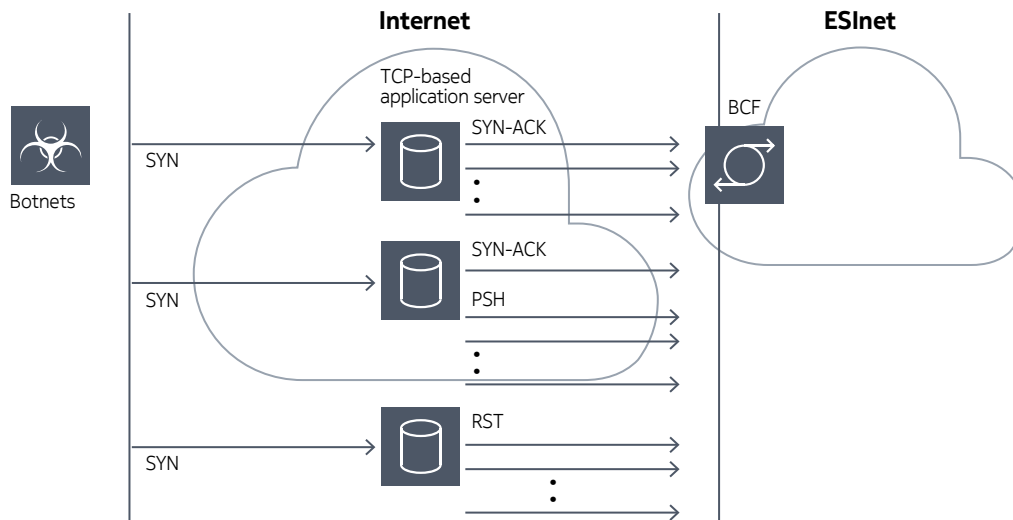


TCP-based reflection/amplification attack

TCP-based reflection attacks (see Figure 6) have started to become prevalent. In this type of attack, the attacker sends a TCP SYN packet with a spoofed IP source address to an internet server. The internet server, running applications such as HTTP, FTP or SIP, sends a SYN-ACK packet to the attack target. When the target does not respond with an ACK reply, the server re-transmits the SYN-ACK packet a number of times (the number of attempts is server- and application-dependent.), amplifying the attack traffic.

Some applications, such as FTP, will even push banner information via push (PSH) packets before the three-way handshake is completed. If the SYN packet is destined for a closed TCP port, the server might respond with a series of reset (RST) packets. This further amplifies the attack traffic.

Figure 6. Three TCP reflection/amplification attack types



Multi-vector attacks

Many DDoS attacks employ a multi-vector strategy that uses a combination of attack methods to make it difficult to determine the attack vector and deploy effective countermeasures. Other strategies are “pulsating attacks”, which quickly vary the attack volume, and “carpet bombing” attacks on entire IP subnets. Often volumetric DDoS attacks are deployed as a distraction from more insidious application-level attacks and hack attempts that are occurring at the same time. This combination is analogous to setting off an explosion at the front door of a house while trying to break in through the back door.

Mitigating the DDoS/TDoS threats

There are three approaches to mitigate DDoS/TDoS attacks:

- Infrastructure overprovisioning
- Two-tier defense with a border router
- Analytics-driven DDoS/TDoS protection

Infrastructure overprovisioning

Overprovisioning the infrastructure requires deploying a firewall and SBC that have excess capacity, and oversizing network trunks that connect to other networks. While overprovisioning does help withstand small DDoS/TDoS attacks, ultimately the added cost of firewalls and SBCs can quickly become exorbitant as the attack size continues to increase. In addition, even though an oversized network trunk can handle a gargantuan amount of attack traffic, the huge alarm log at the firewall and the SBC make it difficult to track the advance of an attack, thereby hampering investigation efforts.

Two-tier defense with a border router

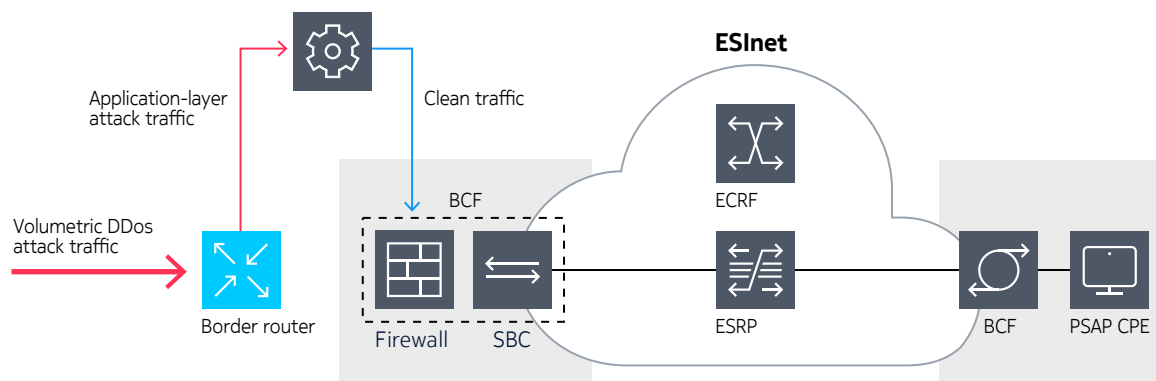
Deploying a border router with IP filtering (also known as an access control list [ACL]) along with centralized security appliances is another way to mitigate DDoS/TDoS attacks. In this two-tier defense architecture, a border router is paired with a centralized security appliance.

The border router is configured with IP filtering (also known as an access control list [ACL]) as a tier-1 defense measure. This tier-1 defense is a proactive measure that aims to reduce the attack surface by filtering common illicit traffic such as traffic from reserved IP blocks or with unused TCP/UDP ports.

The tier-1 defense complements the tier-2 defense measure, a centralized security appliance that performs stateful layer 4 – 7 traffic inspection and “scrubbing”, to stifle application-level DDoS attacks (see Figure 7).

Because centralized security appliances usually have limited throughput, with this two-tier defense architecture, the border router can play an essential role in pre-screening all traffic and stopping network-layer attacks while leaving the appliance to focus on application-level attacks. It is also important to note that while the security appliance aims to protect only high-value servers such as SBCs and ESRPs, the border router with IP filtering provides all-encompassing protection to the NG911/NG112 infrastructure.

Figure 7. A two-tier DDoS/TDoS defense architecture



Analytics-driven DDoS protection

The third approach to defend against DDoS/TDoS attacks is to harness the power of a centralized intelligent DDoS/TDoS analytics platform by pairing its detection capabilities with the advanced packet processing capabilities of routers. Grounded in advanced analytics as well as the powerful, dynamic and programmable deep IP filtering capabilities of routers (pattern matching beyond the IP header, in the payload), this approach establishes an automated closed loop between the analytics and the network itself.

As shown in Figure 8, network-based DDoS protection consists of three steps:

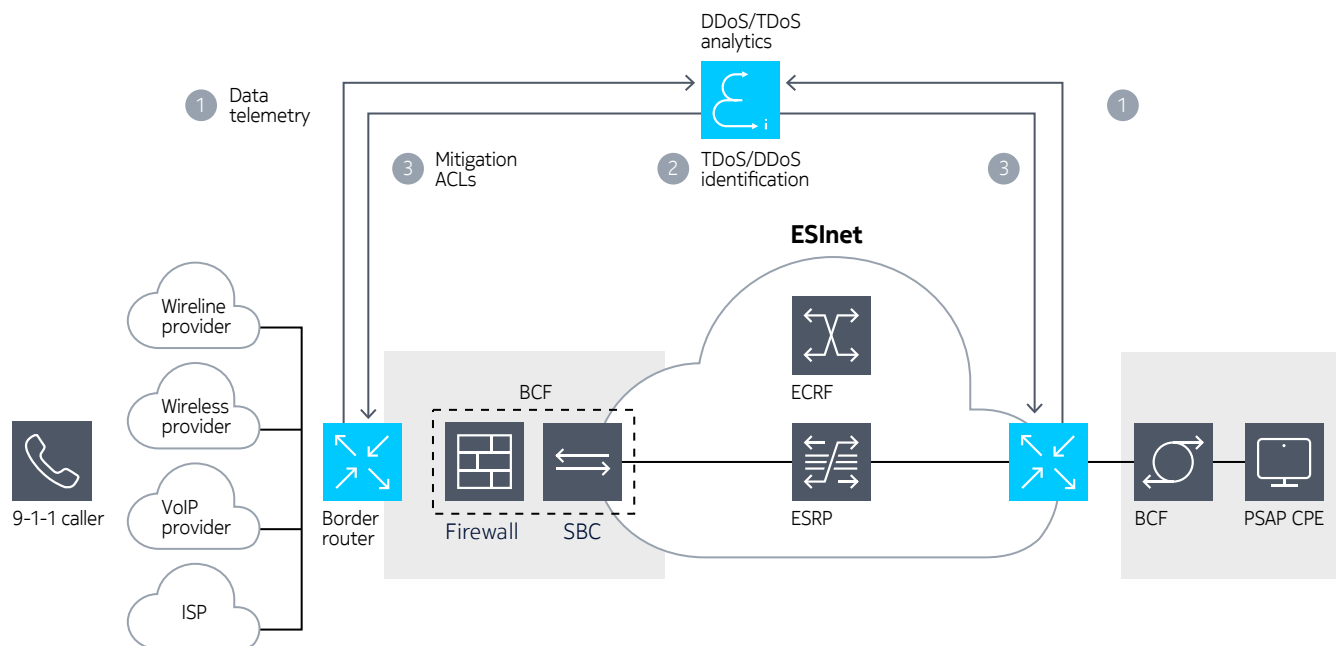
1. The DDoS analytics engine collects telemetry data and mirrors traffic samples of IP packets (including payloads) from routers.

2. The analytics engine continuously analyzes the data and looks for real-time anomalies to accurately detect DDoS attacks. During this real-time analysis, insights from the network (such as the attack type or a rogue packet pattern) are correlated with larger internet-based insights (blacklists, whitelists, known security threats, and patterns in the internet) to improve the accuracy of detection and to minimize the chance of false positives and false negatives.
3. Equipped with all of these real-time insights, after DDoS threats and attacks are identified, corrective actions such as customized mitigation filtering rules can be formulated and downloaded to routers to discard malicious flows.

This intelligence is particularly important to thwart "Zero-day attacks", a term used to describe any new type of DDoS attack. These are hard to defend against because there is no established attack signature or countermeasure.

Taking advantage of the latest router hardware innovation, the filtering rules can be extended to match patterns beyond the IP header. They can support deep IP packet inspection to match a pattern of invalid uniform resource names (URNs) found in INVITE messages. This matching is crucial to stop a volumetric DDoS attack exploiting an application-layer protocol, such as happens with a SIP INVITE flooding attack.

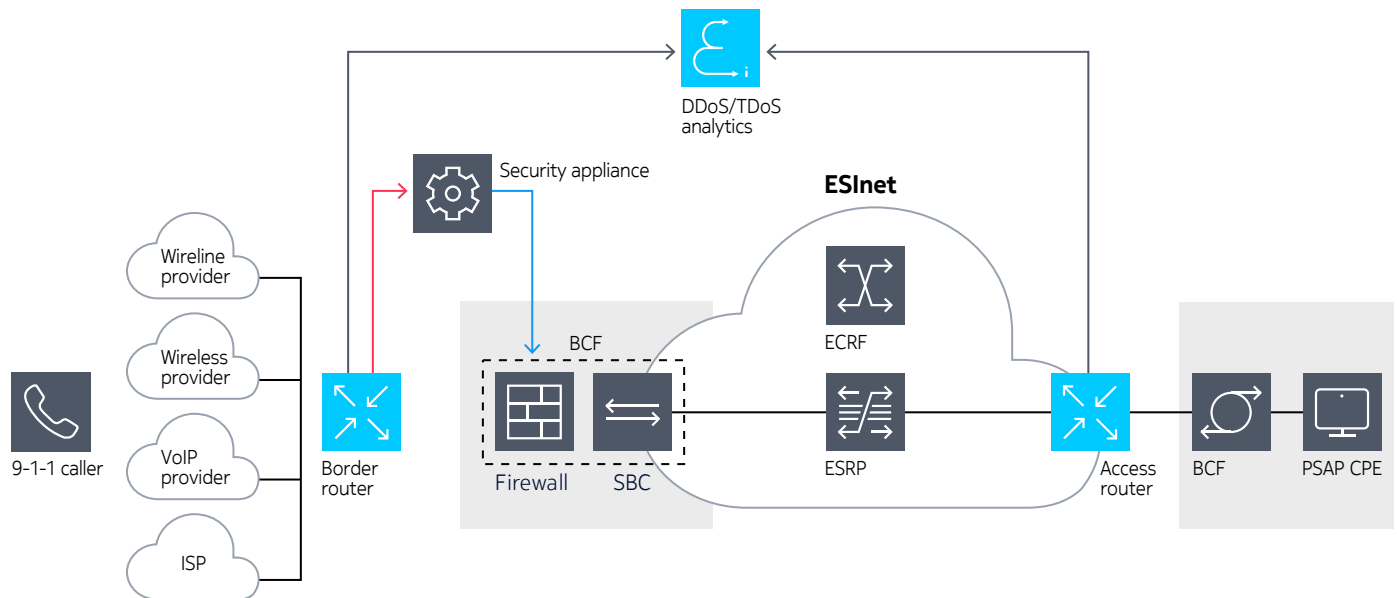
Figure 8. An analytics-driven defense architecture



A DDoS/TDoS defense blueprint for NG911/NG112

Combining the power of analytics with a two-tier defense is the best DDoS/TDoS defense strategy. Innovatively combining these approaches provides an intelligent, agile defense that effectively stifles DDoS/TDoS attacks on the NG911/NG112 infrastructure (see Figure 9).

Figure 9. An analytics-driven, two-tier DDoS/TDoS defense blueprint



Tier-1 defense

Tier-1 defense combines centralized DDoS/TDoS analytics and routers with deep IP filtering capabilities. The border router is preconfigured with IP filtering rules to defend against common volumetric DDoS attacks. The rules combine blacklisting and whitelisting.

Blacklisting

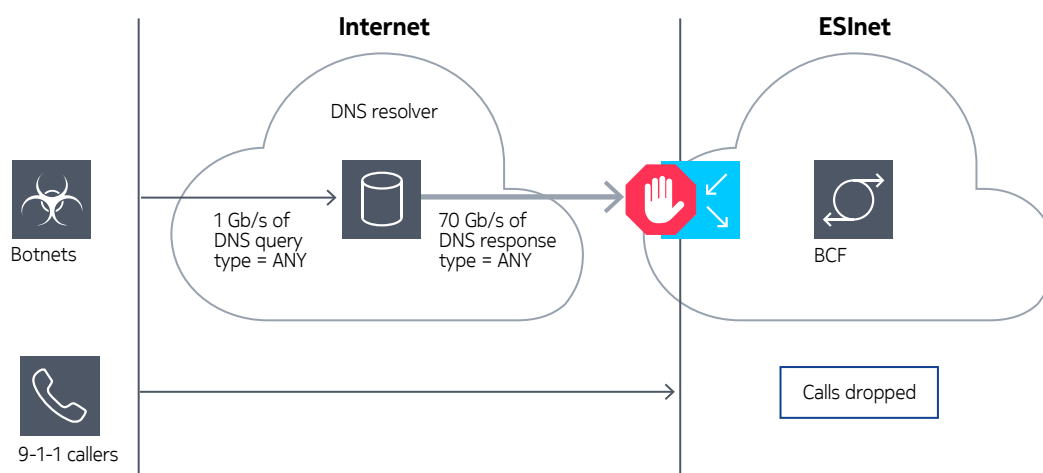
Blacklisting performs the following functions:

- Blocks identified invalid flows
- Blocks common volumetric DDoS attacks such as IP packets sent to broadcast or IANA-reserved addresses
- Turns on unicast reverse path forwarding to block packets with unreachable source IP addresses.

By capitalizing on advanced filtering capabilities that match patterns inside the payload, blacklisting can also detect an amplification attack that uses DNS (see Figure 10).

By filtering network layer volumetric attack traffic at the network interconnection point, blacklisting removes the need to over-provision the firewall and the SBC capacity, which is cost-prohibitive.

Figure 10. Border router inspecting payload pattern to stop amplification attacks



Whitelisting

Whitelisting allows only traffic carrying applications used in NG911/NG112, such as SIP flows on destination port 5060. Advanced filtering capabilities can even rate-limit the flows that are allowed in.

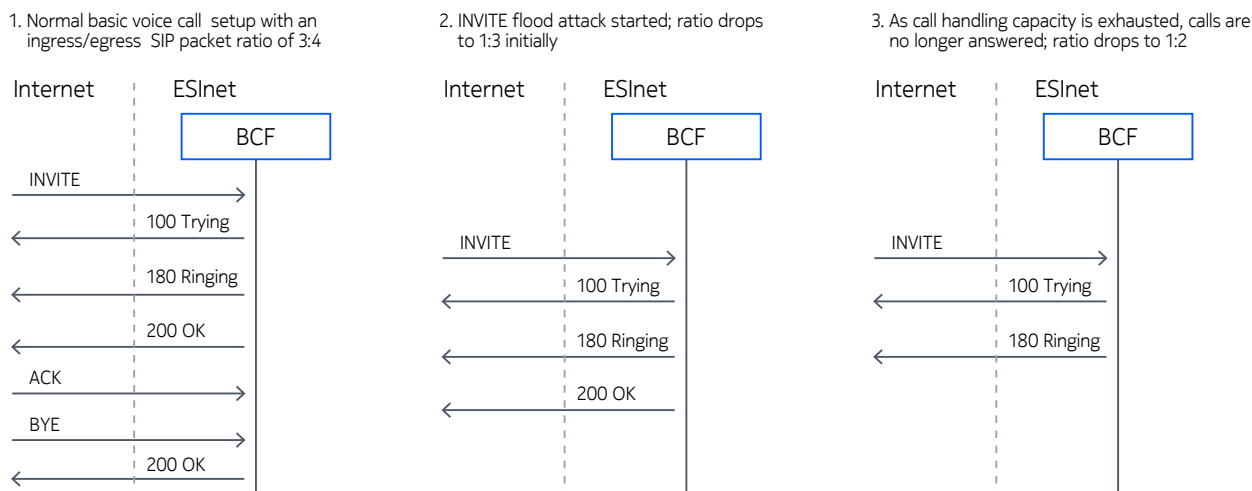
Normal SIP packets are long. Small SIP packets are likely to be malicious. The whitelisting rule can be set to rate-limit small SIP packets to mitigate an attack.

However, DDoS attacks are ever-evolving, and new attack methods constantly appear. To effectively mitigate attacks, particularly Zero-day attacks, DDoS/TDoS mitigation analytics is an essential component of cyber defense.

During normal operations, routers continuously mirror IP packets. The analytics platform performs sampling to constantly analyze traffic and establish baseline metrics. The platform also looks for traffic profile deviation to detect an attack. For example, by monitoring the SIP packet ingress/egress ratio, an INVITE flood attack can be detected as follows (see Figure 11):

1. The normal long-term ingress/egress ratio is 3:4.
2. When an INVITE flood attack occurs, INVITE packets dominate incoming SIP packets as the SBC and the ESRP try to answer without receiving any ACK message from compromised botnets. The packet ratio then drops to 1:3.
3. As the flood continues, the SBC and ESRP can no longer accept calls. The packet ratio becomes 1:2.

Figure 11. Detecting an INVITE flood attack



By analyzing traffic collected through analytics, operators can determine defense measures. For example, operators may see a pattern of usually high malicious INVITE packets that contain a rogue URN or they may see an unusually high number of SIP packets coming from a set of IP addresses. In response, they can thwart the attacks by using deep IP filtering rules to block SIP packets with the identified rogue URN or to rate-limit the SIP flow from an identified set of rogue IP addresses.

Tier-2 mitigation defense

When a DDoS/TDoS attack is detected, the border router can forward the filtered SIP flows to the security appliance to inspect all SIP messages. Because the border router has already mitigated the volumetric attack component, the security appliance has only a small volume of traffic to scrub to ensure there are no application-layer Trojan horses in the flows.

Keeping our lifeline open for real emergencies

911/112 is a crucial lifeline to citizens in need of emergency assistance. Because NG911/NG112 is now connected to the internet, this greatly expands the attack surface. To combat the increasing magnitude, frequency and sophistication of DDoS/TDoS attacks, it is essential to deploy an adaptable, cost-effective and scalable defense mitigation blueprint that can evolve to deal with volumetric and Zero-day attacks.

Harnessing the power of advanced IP filtering capabilities that can perform pattern-matching inside the packet payload, the ESInet can play a critical role as the tier-1 defense against known volumetric DDoS/TDoS attacks. Complemented by DDoS/TDoS analytics and actionable insight on DDoS attacks in progress, operators can quickly deploy surgical countermeasures to stop Zero-day attacks as they occur. This defense blueprint plays a key role in keeping 911/112 emergency communications services up and running 24 x 7 to protect citizens.

To learn more about Nokia public safety solutions, the IP portfolio and our analytics platform, visit these Nokia web pages:

- [Public safety](#)
- [Edge routers](#)
- [Deepfield solution](#)

Abbreviations

ACK	acknowledge
ACL	access control list
BCF	border control function
CCTV	closed circuit television
CPE	customer premises equipment
CPU	central processing unit
CS	core services
DDoS	distributed denial of service
DNS	Domain Name System
ECRF	emergency call routing function
ESInet	Emergency Services IP network
ESRP	emergency services routing proxy
FTP	File Transfer Protocol
IANA	Internet Assigned Numbers Authority
IoT	Internet of Things
IP	Internet Protocol
ISP	internet service provider
NGCS	next-generation call services
PSAP	public safety answering point
SBC	session border control
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SYN	synchronize
TCP	Transmission Control Protocol
TDoS	telephony denial of service
VoIP	Voice over Internet Protocol
VSP	voice service provider
UDP	User Datagram Protocol
URN	uniform resource name



About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia operates a policy of ongoing development and has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions. Nokia assumes no responsibility for any inaccuracies in this document and reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2023 Nokia

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

Document code: (March) CID207325