Secure the IP gateways in your 5G-era network

With Nokia IP gateways

Application note
Abstract

Cloud-based content consumption and ever-increasing bandwidth demands are driving networking suppliers to deliver higher subscriber scale, bandwidth capacity and performance in their IP gateways. However, a topic that often is not considered relates to security of these IP gateways.

It’s essential that these IP gateways, which typically need to validate subscriber and service credentials and therefore have access to subscriber data and service context, be protected. This document explains why Nokia IP gateways are the best choice for networks in the 5G era. Our “security by design” approach and comprehensive features help protect the gateways from threats and attacks, thereby ensuring the integrity of subscriber information.
Why security matters for IP gateways

IP gateways and subscriber context

IP gateways are critical elements in a communication service provider’s (CSP’s) network. They are the demarcation points of the network through which subscribers (and end-user devices) connect to their residential, mobile and enterprise services (see Figure 1).

Figure 1. IP gateways in a CSP network

IP gateways include:

- Broadband Network Gateways (BNGs) for residential services subscriber management
- Cloud Mobile Gateways (CMGs) for mobile services subscriber management
- IPsec Security Gateways (SeGWs) for securing traffic in mobile transport networks and enterprise VPNs
- Wireless LAN Gateways (WLGWs) for managing subscribers over Wi-Fi access.

IP gateways perform key functions ranging from access control to provisioning and policy enforcement. They play a critical role in providing secure access to communication services and in protecting valuable content from abuse and theft.

Key IP gateway functions include:

- Assigning IP addresses to user devices, enforcing service policies and accounting of usage
- Performing authentication and authorization of network access based on provided user credentials
- Performing encryption and providing security for end-user traffic (for SeGWs)
- Providing statistics data through streaming telemetry to assure quality of experience of consumed services
- Preventing unauthorized user behavior such as address spoofing and denial of service (DoS) attacks
- Safeguarding the privacy of subscriber data and user communications
- Supporting the designated authorities in lawful interception of user communication.

To perform these functions, IP gateways must have unique access to and granular visibility of sensitive subscriber data and service context. Subscriber information can be stored in the IP gateway, on dedicated servers (AAA, RADIUS, DHCP, policy, charging, SDM) and end devices (customer premises equipment, residential gateways). Each of these information repositories could potentially be compromised or hijacked for malicious purposes.
IP gateways must be secure

IP gateways are the crucial link for ensuring access, network priority, privacy and integrity of subscriber data by:

- Providing secure access to networking services for only authorized subscribers
- Preventing theft of subscriber credentials or abuse of account privileges
- Ensuring the privacy of user communications.

It is essential to ensure the integrity and security of IP gateways and their associated subscriber and service context. The following are a few examples of subscriber information that can be exploited to determine end-user identity:

- IP gateways save the context of end-user IP addresses; this information can be used to help determine end-user identity.
- BNGs and WLGWs may store end-user network access credentials (e.g., username and password for broadband services), which can be used to identify subscribers.
- A SeGW, if used as an enterprise remote-access VPN gateway, in some cases has visibility of users’ VPN tunnel credentials.

These security concerns are even more pressing in the 5G and cloud era, where billions of poorly secured end-user devices can easily be exploited to launch DoS attacks to disrupt essential communication services. Secure and reliable broadband access is critical for participating in the digital economy and social media. Businesses and consumers increasingly rely on the cloud to store and exchange personal and sensitive data, and IP gateways play a key role in ensuring that subscriber access remains private and secure.

IP gateway vulnerabilities and attacks

Security vulnerabilities are weaknesses that can make the IP gateway susceptible to being attacked. IP gateways can be impacted by software design errors, configuration errors, compromised or infected end-user devices, and a lack of (or weak) access control procedures.

Attacks are techniques that can be used to exploit security vulnerabilities. The objective of security-related attacks can range from disrupting subscriber services to theft of end-user credentials to espionage: spying or stealing subscriber data through communication snooping. The attacks can attempt to delay and/or disrupt data communications for the entire network or can be targeted attacks at network segments or specific subscribers.

Both employees and others can take advantage of any vulnerabilities or backdoors that exist within unsecure products.

Inside attacks can be unintentional, from infected employee or contractor devices, or they can be intentional, from rogue employees. Authorized subscribers can become unwitting attackers when home devices or residential gateways are compromised by hackers and leveraged in botnet attacks.

Attacks can come from spoofed IP addresses, botnet-infected devices, or can use amplification sources. Domain Name System (DNS), Simple Network Management Protocol (SNMP) and Network Transfer Protocol (NTP) have all been used to launch attacks in which the response from the servers is amplified many times higher than the size of the requests. This leads to a flood on the attacked network and the devices (e.g., routers and IP gateways) in the network.
Other attack methods include:

- Hacking into IP gateway devices to gain access to subscriber credentials, to intercept or disrupt subscriber sessions, to bring the device under control of a rogue authentication, authorization and accounting (AAA) server, or to compromise device operation in other ways
- Gaining access to IP gateway management and control infrastructure, such as AAA servers
- Generating much higher traffic or transaction rates to overwhelm the setup or operation of communications. These attacks can target the IP gateway interfaces, services, control plane or AAA processing.
- Interception or tampering with control plane communication to masquerade as legitimate subscribers or grant access to unauthorized subscribers
- DoS attacks on the control or data plane of the IP gateway.

Security in today's communication network devices, including routers and IP gateways, must anticipate and protect against threats and attacks. Suppliers such as Nokia play a key role to ensure that their IP gateway products are designed and operated using best security practices.

**Nokia IP gateways**

To ensure that IP gateways correctly perform their essential task of providing secure access to network services for legitimate subscribers, it is essential to protect the integrity of the gateways and ensure that their operation cannot be compromised by malicious actors.

Integrity of the gateways requires integrity of router hardware, firmware and operating system (OS) software, including how the router hardware, firmware and OS software are designed to handle security threats and vulnerabilities.

**A “security by design” philosophy**

The Nokia Service Router Operating System (SR OS) is the OS that runs on all Nokia fixed and mobile IP gateways. Nokia has designed security into our IP gateways and Nokia SR OS software from inception and we have proven our design credentials in CSP networks for over 15 years. Reliability, robustness, security and high availability are built into the design architecture, design approach and testing methodologies of the SR OS.

The SR OS is maintained as a single development stream, which avoids custom streams or forks and strengthens Nokia's ability to test the system for software quality. Nokia has invested heavily in test automation, with software designers and testers working side by side to write automated test code for every new line of code in the SR OS.

The SR OS is also continuously regression tested using tens of thousands of servers 24 x 7 x 365. With a single SR OS stream, all the test cycles focus on the same software image. This is a significant reason for the code robustness and eliminates the occurrence of major bugs in the field.

**SR OS development: Focus on testing, hardening and security**

Nokia invests heavily in IP routing security from the product development phase to testing, hardening and vulnerability management. In addition to following software coding best practices, static code analysis is performed throughout the product development phase using both third-party commercially available tools and internally-developed tools to identify potential vulnerabilities.
The SR OS is further hardened by a dedicated IP routing security test team that is independent from the software development and test teams. Security testing is conducted throughout the development of a new major release as well as for each minor release and includes:

- Testing for robustness and protection from DoS attacks
- Fuzzing tests for control and management protocols
- Port scanning
- Vulnerability scanning

Fuzz testing, performed as part of security hardening by the security team, ensures the platform robustness against malformed packets.

Security vulnerability management

The Nokia Product Security Incident Response Team continually monitors for new potential security vulnerabilities in third-party software that is included in the SR OS. If a vulnerability is found, it is addressed by the engineering team and subscribers are notified through the Nokia alert notification mechanism. The alert, including preventive action or a work-around, is posted on the customer support site and an email notification is sent to all registered subscribers. Fixes for security vulnerabilities are provided via software maintenance releases.

SR OS security best practices

Nokia publishes a security guidelines document with recommendations for network operators to protect their networking environment. This document discusses features, configuration and design recommendations to protect their IP networks.

Nokia IP gateways: Comprehensive security

Nokia IP gateways offer the industry’s most comprehensive security feature set and best practices, including:

- Protection for the IP gateway router control, data and management plane
- IP gateway-level protection features: BNG and SeGW protection
- Recommendations for best security practices.

Protection for the IP gateway router control, data and management plane

The SR OS has a robust set of features to protect and secure the router from attacks. This set of features includes securing access to the router, management to prevent administrative access, and using hardware queuing and filtering to prioritize and filter traffic to the control processors, which prevents DoS attacks aimed at the control plane.

The SR OS supports unique protection mechanisms to protect the router control plane, data plane and management plane. The following is an overview of key capabilities.

There is a set of mechanisms in the SR OS to protect the system, isolate subscribers and interfaces, and prevent the CPU from being flooded with control traffic. These mechanisms are both distributed in the line card to isolate subscribers as early as possible as well as centralized, providing multiple stages of queuing, prioritization, rate limiting and filtering.
Floods can occur from DoS attacks, network failures or misconfiguration. SR OS flood protection queuing, prioritization, rate-limiting and filtering mechanisms in hardware at both the line card and control card level drop the excess flood control traffic before it hits the CPU.

Preventing spoofing in a network is one of the most effective ways to reduce the likelihood and impact of DoS attacks. Nokia IP gateways support anti-spoofing and media access control (MAC) protection, which can protect against MITM (man in the middle) attacks by protecting the router’s MAC-IP mapping from Address Resolution Protocol (ARP) poisoning.

The management of the router is a critical aspect to ensure that the network remains secure. The SR OS supports several features to protect the management plane, including:

- CPU protection and distributed CPU protection
- Secure management via Secure Shell (SSH), SNMPv3 and Network Configuration Protocol (NETCONF) over Transport Layer Security (TLS)
- Secure telemetry via generalized Remote Procedure Call (gRPC) over TLS
- Dedicated ACL filters for dataplane and control plane protection
- Use of NTP to ensure that timestamps of logged activity are synchronized with other network activity, especially when malicious activity timelines are required.

**IP gateway-level protection features**

In addition to IP gateway control, data and management planes features, the SR OS provides additional layer protection features at the gateway level.

**BNG protection**

One of the security issues with BNG deployments is the direct result of sharing forwarding and routing tables among subscribers on the same interfaces. General attacks can be directed to the BNG itself or toward other customers. Security mechanisms need to be put in place at the aggregation or routing layer to limit the number of resources and the scope per subscriber.

The Nokia BNG supports several protection features, including:

- Dynamic anti-spoofing
- Limiting the number of leases allowed to protect against Dynamic Host Configuration Protocol (DHCP) starvation
- Limiting the per-subscriber control plane traffic, such as DHCP, Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), ARP and Point-to-Point Protocol over Ethernet (PPPoE)
- Discarding IP packets that lack a verifiable source address.

**SecGW protection**

The Nokia SeGW builds on the “security by design” principles. For example, there are no pre-provisioned certificate authority (CA) certificates. All trusted certificates must be explicitly provisioned by the user. The provisioned certificates/private keys are stored in a secure encrypted format to prevent snooping.

There are also multiple features to prevent DoS attacks, including limiting the number of ongoing tunnel setups, IKEv2 cookie mechanisms, and locking out clients that keep failing authentication attempts.
Recommendations for security best practices

The operations staff that manage the IP gateways have a crucial role to play in ensuring there is no unauthorized access to the IP gateways. Human error or a lack of diligence can often lead to undesirable security outcomes or the creation of loopholes that can be exploited by attackers.

Robust security guidelines and administrative discipline for user-account management will prevent attacks and prevent attackers from using methods that might go undetected. Policies such as determining roles for users and administrators will allow for configuring authorization rules that are consistent with job profiles and assigned responsibilities.

Accounting for user activity is another method that if left unattended can contribute to a lower security posture. Logging information such as session statistics and usage information will provide audit data. This data can be used to confirm information such as user identity, network address, services used, access time and date, and log origination data and time.

Conclusion

CSPs understand that security is a critical building block for their 5G and cloud-era networks. IP gateways are often evaluated solely on their scale, capacity and performance. While these are baseline and mandatory requirements, it’s time to rethink the role that security plays for IP gateways, given their added responsibility of protecting subscriber information and context.

Security cannot be an afterthought or an add-on feature. The IP gateway of choice must support a comprehensive and holistic approach to securing the router at the hardware and router OS software level with no loopholes or backdoors that can be exploited by bad actors or rogue operatives. Nokia IP gateways apply a “security by design” philosophy that helps protect subscriber information by ensuring that the gateway is secure from threats and attacks from various sources.

For more information about Nokia IP gateways, visit the Nokia 7750 Service Router and Nokia Virtualized Service Router web pages.
Abbreviations

AAA authentication, authorization and accounting
ARP Address Resolution Protocol
BNG Broadband Network Gateway
CPU Central Processing Unit
CSP communications service provider
DHCP Dynamic Host Configuration Protocol
DoS denial of service
IP Internet Protocol
LAN local area network
NTP Network Transfer Protocol
MAC media access control
OS operating system
RADIUS Remote Authentication Dial-in User Service
SDM Subscriber Data Management
SeGW Security Gateway
SNMP Simple Network Management Protocol
SR OS Nokia Service Router Operating System
TLS Transport Layer Security
WLGW Wireless LAN Gateway
VPN virtual private network

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

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.

© 2020 Nokia
Nokia Oyj
Karakaari 7
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code: SR2001040623EN (February) CID207071