DATASHEET

NSFOCUS

5G Security Solution

Build Resilient Security Over Your 5G Networks to Protect Against Threats Both Predictable and Unpredictable

KEY FEATURES

Intelligent AI-powered DDoS mitigation algorithms

Global Scrubbing Centers carrying terabit-level capacity

Truly global threat intelligence sourced from APAC and also the rest of the world

Smart traffic scrubbing scheduling platform

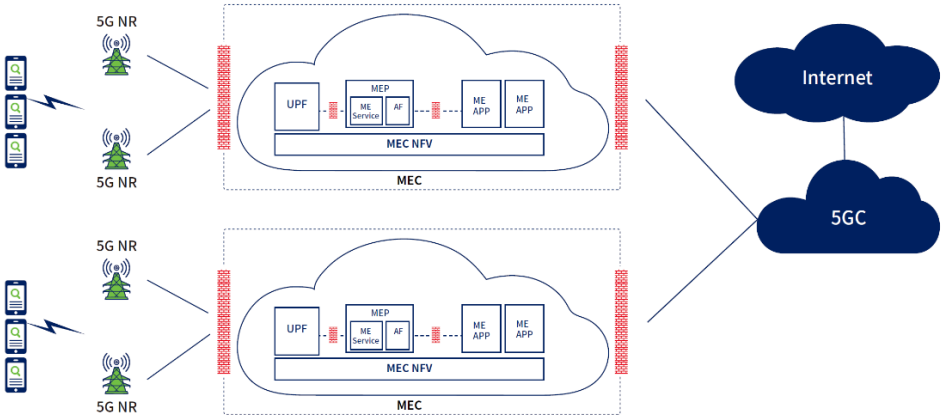
Deep Flow Inspection (DFI) and Deep Packet Inspection (DPI) technologies

Why MEC is so important to the 5G Network?

MEC (Multiple-access Edge Computing) is an important part of the 5G architecture, which is a type of distributed computing used to reduce bandwidth and improve response time, allowing operators to deploy their applications from centralized data centers to the edge of the network, closer to end-users and their devices. This effectively creates a shortcut for content delivery between the user and the applications.

MEC is an evolution of cloud computing, which is not exclusive to 5G but is certainly integral to its efficiency. Features of MEC, including low latency, high bandwidth, and real-time access to RAN, differentiate 5G architectures from previous generations of mobile networks.

Edge computing can also meet stringent performance requirements for a variety of 5G use cases, such as ultra-reliable, low-latency communications for mission-critical services, industrial automation, and vehicle-to-everything (V2X) applications. This network will have the ability to support the widespread deployment of Internet of Things (IoT) devices under a low-bandwidth use case known as a massive machine-type communication (mMTC). It also has the capability and bandwidth to provide enhanced mobile broadband (eMBB) services to meet consumer demand for high-performance applications such as gaming, augmented reality and virtual reality. Thus, MEC is a must-have capability for service providers as it enables higher quality service delivery.



Due to the data explosion enabled by 5G, securing every aspect of a service provider's network from the edge has never been more important. With the interconnection of a large number of IoT, the hosts that may be exploited to initiate DDoS attacks have increased exponentially, and DDoS attacks will become easier and more frequent than ever.

NSFOCUS Anti-DDoS Solution for MEC

Mitigating the risk of DDoS attacks has always been a key responsibility of network operators, but the rise of 5G networks could intensify the importance of DDoS attack protection. There is no doubt that 5G services are characterized by huge quantities of terminals and traffic data. Unlike previous 4G technologies, the radius of a 5G base station with high data bandwidth is relatively small, thus there has to be 5 to 10 times the density of the base station. The expected volume of the base station, stronger efficacy of cybercrimes, and high-risk botnets make the protection of evolving 5G networks strategically important.

NSFOCUS offers a smart and accurate mitigation solution in a software-based or hardware form factor to protect MEC against various DDoS attacks.

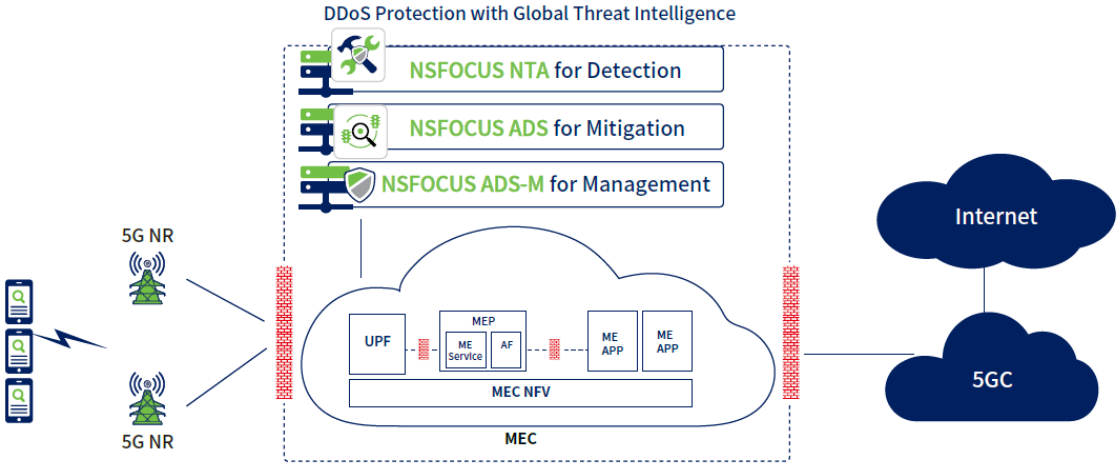
Leveraging technologies like Deep Flow Inspection (DFI) and Deep Packet Inspection (DPI), NSFOCUS Network Traffic Analyze (NTA) can detect DDoS attacks within high-bandwidth traffic with a granularity that can be as specific as user requirement.

NSFOCUS Anti-DDoS System (ADS), which can be deployed at the perimeters of the application server zone for low latency and high quality of experience (QoE), mitigates the ever-evolving DDoS attacks effectively and efficiently. As DDoS attacks increase in size, massive attack traffic will be easily tackled by subscribing to NSFOCUS's cloud-based DDoS Protection (DPS) service. With 8 global Scrubbing Centers carrying Terabit-level capacity, NSFOCUS Cloud DPS ensures its customers will be protected against even the largest DDoS attacks in history. NSFOCUS Threat Intelligence (NTI), a truly global threat intelligence sourced from APAC and also the rest of the world, augments the security capabilities with fresh, accurate, and unique TI, enabling proactive block of malicious traffic, nipping potential DDoS attacks in the bud and improving the DDoS protection efficiency.

The NSFOCUS Anti-DDoS System Manager (ADSM) provides critical visibility into network operations, allowing operators to optimize the process of mitigation and gain insight into the security and operational changes.

For the large deployment scenario, NSFOCUS also provides a smart traffic scrubbing scheduling platform— NSFOCUS Anti-DDoS Business Operations System (ADBOS) for centralized management of all on-premises Anti-DDoS devices and cloud services. This platform can be operated by a self-service portal that is friendly to multi-tenancy and allows you to monitor the scrubbing traffic. NSFOCUS ADBOS provides a unique user experience for each customer with customer-specific branding and corporate identity, per user/group/role permission for controlled access, and mass customization and configuration operation. It is a multi-tenant platform that brings lots of benefits to customers while ensuring their business continuity.

NSFOCUS Anti-DDoS Solution for MEC, tailored for 5G-based networks, allows 5G network operators to maximize DDoS protection and service availability while delivering new 5G outcomes.



© COPYRIGHT 2022, NSFOCUS. ALL RIGHTS RESERVED 5GSOLUTION | DS220719