Deploying a Multi-Layered Defense for Service Provider Networks

KEY BENEFITS

Deploy comprehensive and integrated security
across network domains to protect user devices, the core network, and applications.

Ensure unrivaled performance and scale
at the lowest power consumption and footprint for the lowest TCO.

Future-proof and protect network investments
with flexible deployment options offering carrier-grade hardware and VNFs supported on the same operating system.

Gain unsurpassed agility and extensibility
by deploying a programmable platform across the data, control, and application planes.

Consolidate services
to simplify network architectures, lower CapEx and OpEx, and improve agility while maintaining the highest level of security.

ICSA labs CERTIFIED

Protect against sophisticated and emerging threats across network domains within 4G, 5G, and network functions virtualization (NFV) networks and the Internet of Things (IoT). The F5® Carrier-Class Network Firewall (CCNF) delivers a multi-faceted security solution with unrivaled performance and scalability to protect service provider networks, brands, and revenues while increasing quality of experience (QoE) for subscribers.

Challenge

The IoT—from wearables to smart cities—is driving unprecedented mobile traffic growth. To keep up, service providers are evolving their networks towards supporting 5G and IoT. They are also continuing to see the depletion of IPv4 addresses and need to transition to IPv6. Finally, operators are facing the monumental challenge of securing devices, networks, and applications from attacks that include distributed denial-of-service (DDoS), signaling, DNS, and advanced persistent threats (APTs).

Solution

The F5 Carrier-Class Network Firewall changes the security paradigm, providing a comprehensive and integrated security solution that can be deployed across all network domains, including the data, signaling, and application plane environments. As architectures evolve, the F5 CCNF protects investments and helps future-proof networks with the capacity to evolve as required, with solutions that can be deployed on highly optimized hardware or as a virtual network function (VNF) in NFV environments. Either way, it delivers end-to-end security, with the highest performance and scalability, in a reduced footprint and with the lowest total cost of ownership (TCO).

Comprehensive and integrated portfolio of security solutions

The F5 CCNF is architected to meet evolving security requirements as service providers deploy security solutions across their networks. Within the core mobile network, the F5 CCNF secures the Gi LAN infrastructure and protects subscribers and networks by mitigating large DDoS attacks such as floods, port scans, and sweeps.

As service providers scale their networks and deploy new services in the data center, the risk of being impacted by a security attack increases. As a full proxy architecture, the F5 CCNF offers increased visibility and granular control of L4-L7 applications and services, providing extensive security functionality and comprehensive end-to-end protection. Within the signaling and control plane, the F5 CCNF provides DNS security services, mitigating DNS DDoS attacks and shielding the DNS infrastructure—both from malicious attacks via infected subscribers and from undesired DNS queries and responses that reduce DNS performance. Plus the solution provides carrier-grade NAT (CGNAT) functionality and tools to manage IPv4 devices traversing the network while migrating to IPv6.

Massive scale and performance

The sheer volume, tenacity, and sophistication of attacks can seem overwhelming, and service providers need dynamic and persistent security against this near-constant barrage. The F5 CCNF is designed for the massive scale and performance required to handle the surge of network attacks. Built on NEBS-compliant, F5 VIPRION® platforms certified by ICSA Labs, the F5 CCNF scales with support for 20 million connections per second (CPS) and an unprecedented number of concurrent connections—over 1 billion. As a result, it easily mitigates volumetric DDoS attacks designed to overwhelm network capacity. As a high-performance, stateful proxy, it protects against network-layer DDoS attacks by quickly ramping up to distinguish between malicious and legitimate connections, and then by absorbing or discarding malicious connections before they consume valuable network resources, so subscribers continue to enjoy a high QoE.

Unsurpassed flexibility and extensibility

Service providers' ability to rapidly respond to protect their networks—even from unknown or uncommon attacks—is paramount. The extensibility of the F5 iRules® scripting language enables expansion of F5 CCNF functionality to protect against complex and multi-level attacks. With iRules' open APIs, service providers can create and deploy custom rules to mitigate new or uncommon, highly sophisticated DDoS attacks. The scope of iRules commands provides deep visibility into packets, especially IP/TCP header fields, enabling effective L2-L4 DDoS signatures and flow control via iRules signatures. With the F5 CCNF and iRules, service providers can distinguish between good and bad traffic based on signatures, and then take action to block, drop, or redirect traffic for inspection.

The F5 Carrier-Class Network Firewall delivers end-to-end security for service provider networks within 5G, NFV, and IoT architectures while enhancing network agility, scalability, and performance.

OV-SEC-93069958-ccnf 0516