SOLUTION BRIEF

SECURE THE RAN – SECURITY GATEWAY SOLUTION FOR EVOLVING 5G NETWORKS

RAN NODE AUTHENTICATION AND BACKHAUL ENCRYPTION NOW MANDATED FOR 5G NETWORKS

Mobile operators are increasing their deployment of small cells and other access nodes to accommodate the expanding 5G traffic loads – often in less secure environments than traditional cell sites. If left unprotected, these nodes and their interfaces to the core can be breached by malicious actors and cause network failure or violate subscriber confidentiality. The 3GPP specifications now require the backhaul for S1/X2 and N2/N3 interfaces to be encrypted with IPsec, and recommend a security gateway to authenticate radio access network (RAN) nodes and facilitate the termination of IPsec encrypted tunnels.

The A10 Networks security gateway complies with 3GPP recommendations and provides authentication of RAN nodes and enables secure backhaul, thus ensuring the security of the RAN and protection of the core network.

RAN SECURITY CHALLENGES

SUSTAIN SECURITY, LOW LATENCY, PERFORMANCE AND SCALE

Mobile operators are rapidly deploying 5G radios and small cells throughout their networks to meet growing traffic demand, decrease latency and boost throughput and connection rates. However, recent 3GPP specification requirements now mandate authentication and encryption between nodes and core and for the supporting backhaul network. In addition, the specifications recommend the deployment of a security gateway. Operators need a

CHALLENGE

Increased deployments of radio access nodes reduce latency and provide capacity for increased 5G traffic loads. If left unprotected, RAN nodes and interfaces can be breached for malicious purposes, exposing the core network to multiple threats including DDoS and fraud.

SOLUTION

A10 Networks' security gateway authenticates RAN nodes to the 4G/5G core to eliminate unauthorized access. It further provides high performance and massive scale for the termination of IPsec tunnels used to secure the backhaul between the RAN and core network.

BENEFITS

Operators can grow needed RAN capacity for 5G traffic loads while protecting the core network from rogue nodes or malicious actors and maintaining subscriber confidentiality.

high-performance security gateway that can provide high throughput with IPsec decryption, as well as high connection rates to rapidly authenticate nodes, establish tunnels and support failover.

THE A10 NETWORKS SECURITY GATEWAY SOLUTION

HIGH-PERFORMANCE IPSEC TUNNEL TERMINATON AND AUTHENTICATION

The security gateway solution provides high-performance authentication of g/eNodeBs to the core network or edge node, establishes tunnels and terminates IPsec tunnels on the S1 and X2 interfaces in 4G mobile networks and the N2/N3 interfaces in 5G mobile networks.

FEATURES AND BENEFITS

The security gateway solution includes the following features:

- Supports g/eNodeB RAN-EPC authentication
- Establishes and terminates IPsec tunnels
- Provides high-performance firewall rule mechanisms
- Decrypts IPsec tunnels between cell sites and the packet core or edge node
- Certificate Management Protocol version 2 (CMPv2) for automatic enrollment and renewal
- DHCP-relay
- Tunnel profiles – Provide a simplified gateway configuration that eliminates the need to configure multiple tunnels individually.
- IKE-CP (IKE Configuration Payload) configures VPN client with private IP address, netmask, and gateway
- Reverse route injection – to dynamically control paths that will be accessible via the IPsec tunnels
- ToS/DSCP tunnel traffic marking – to allow for traffic segregation, categorization and prioritization, an important feature since IPsec traffic carries both user and control traffic

The A10 Networks security gateway solution minimizes the potential for traffic between the RAN nodes and the core network to be intercepted. This protects the network from malicious intrusion and ensures data confidentiality for the subscriber.

The secure gateway provides the following benefits:

- Carrier-class throughput and scalability, with high connection rates
- Low latency
- Carrier-grade scalability and reliability
- Included as part of the A10 Networks 5G security suite
- Flexible deployment options

Protocols supported:

- IPv4 and IPv6 ESP tunnels
- IKE v1 and v2
- OSPFv3, BGP 4+, BFD over IPsec tunnel
- 64 ECMP routes
- NAT traversal, Dead Peer Detection
- PKI with SCEP, CRL and OCSP
- IKE v2 EAP

Crypto:

- AES-128, AES-192, AES-256 CBC and GCM modes, 3DES, NULL
- MD5, SHA1, SHA-256, SHA-384, SHA-512
- Diffie-Hellman Groups: 1,2,5,14,15, 16,18,19 (256 EC), 20 (384 EC)
- Authentication methods: Pre-shared Key, RSA (8192), ECDSA (256, 384) PKI Certificates
- Perfect Forward Secrecy (PFS)
- Cryptographic hardware acceleration on appliances

Performance and Scale

- 70 Gbps for single RU device
- Tunnels set-up: 1,000 tunnels per second
- Concurrent tunnels: 64,000 concurrent tunnels

High Availability

- Stateful Failover
- Active-Standby
- Active-Active
- N+M Redundancy
- VRRP-a

Virtual Chassis

- Central cluster management
- 8 device cluster

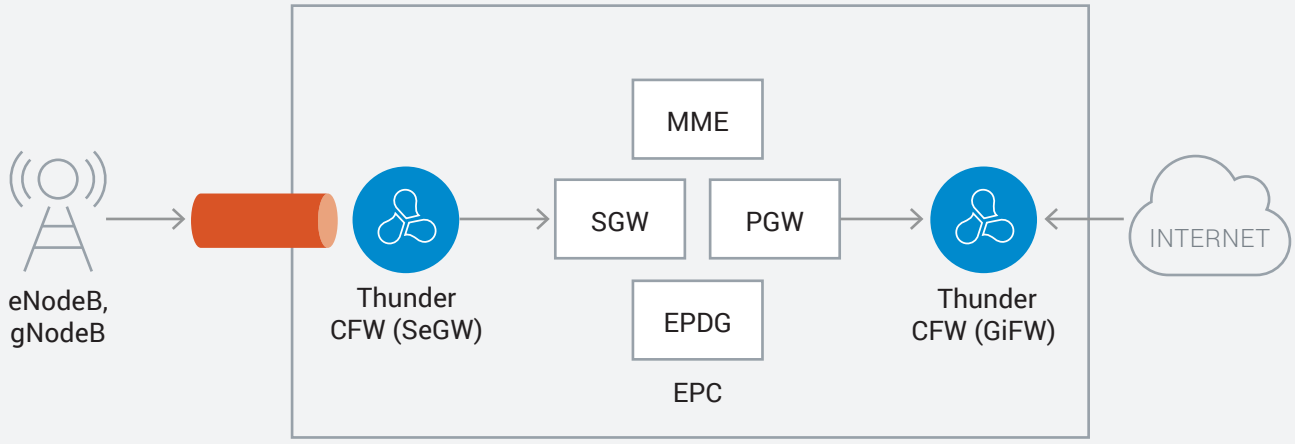

Figure 1. In 5G NSA networks, the A10 Networks security gateway terminates IPsec tunnels to the core network

SOLUTION COMPONENTS

The A10 Networks security gateway solution is available with the Thunder CFW and is part of the 5G security suite. It is available in multiple form factors—physical appliances, as a virtual network function, container and bare metal.

SECURITY, HIGH PERFORMANCE AND SCALABILITY

The A10 Networks security gateway provides rapid tunnel termination and authentication of RAN nodes, providing operators security and performance needed for evolving 5G networks.

NEXT STEPS

For more information, please visit https://www.a10networks.com/solutions/service-provider/5g-security-and-scale/

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™, with a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices in more than 80 countries worldwide. For more information, visit: www.a10networks.com and @A10Networks.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19204-EN-01 NOV 2019