WHITE PAPER

Sicurezza delle reti di accesso radio (RAN) 4G e 5G

Evoluzione delle reti di accesso radio: la pietra angolare della crescita

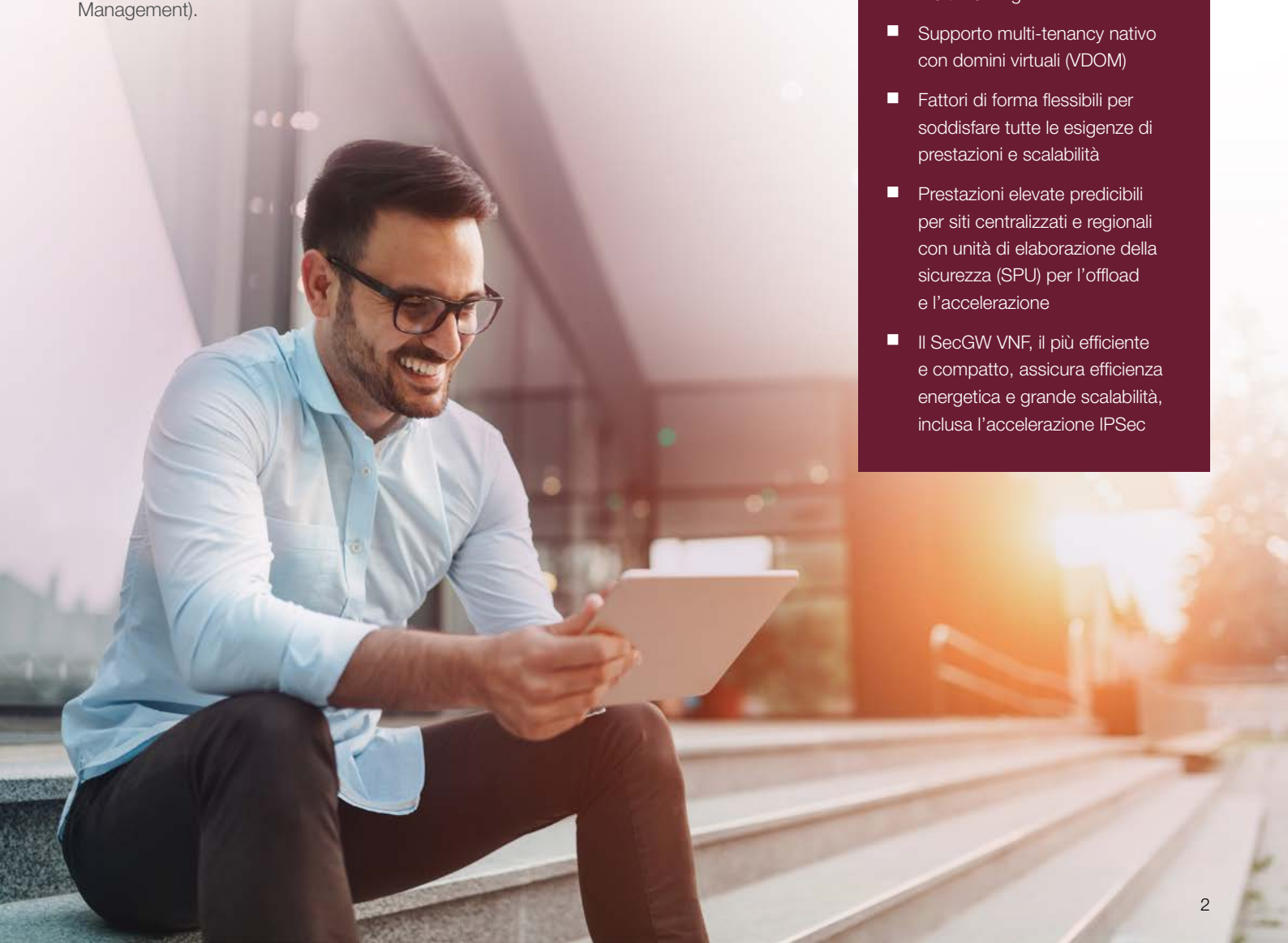
L'evoluzione delle tecnologie LTE (Long Term Evolution) e NR (New Radio) è una componente fondamentale della capacità di un operatore di rete mobile (MNO) di mantenere la promessa del 5G e della crescita. È infatti fondamentali per realizzare le capacità essenziali del 5G: banda larga, scalabilità, grande affidabilità e bassa latenza.

L'evoluzione delle tecnologie e delle architetture LTE e RAN 5G sta inoltre espandendo la clientela degli operatori, dai consumatori alle imprese e alle industrie, creando nuovi mercati e volani di crescita. Al tempo stesso, però, introduce complessità e amplia la superficie di attacco e il rischio potenziale posto dall'infrastruttura di accesso radio 5G. È chiaro dunque che la proposta di casi d'uso alle imprese e alle industrie per sostenere la crescita deve essere accompagnata da adeguati controlli di sicurezza, nella RAN e altrove nel cloud telco.

Il 3GPP (3rd Generation Partnership Project) ha raccomandato l'uso dei SecGW (Security Gateway) per proteggere le comunicazioni RAN e RAN-to-core e garantire la continuità del servizio e la riservatezza. Il Security Gateway del 3GPP si basa sulla capacità di gestire certificati e IPSec per garantire da un lato il controllo dell'accesso attraverso l'autenticazione, dall'altro la riservatezza e l'integrità del traffico attraverso la crittografia. L'autenticazione e la crittografia possono estendersi al traffico utente (user plane), al traffico di controllo (control plane) e al traffico O&M (Operation and Management).

Il vantaggio di FortiGate per la sicurezza RAN 5G

- Terminazione tunnel IPsec e aggregazione per eNB e gNB con autorizzazione e autenticazione
- Segmentazione degli accessi site-to-site
- Protegge le interfacce S1-U e S1-MME LTE
- Protegge le interfacce N2 e N3 5G
- Protegge l'interfaccia F1-C DU-to-CU
- L'ispezione profonda del traffico incapsulato GTP-U protegge dalle minacce note e ignote L2-to-L7
- Firewall SCTP per l'ispezione e l'applicazione della sicurezza, compreso il supporto multi-homing
- Supporto multi-tenancy nativo con domini virtuali (VDOM)
- Fattori di forma flessibili per soddisfare tutte le esigenze di prestazioni e scalabilità
- Prestazioni elevate predicibili per siti centralizzati e regionali con unità di elaborazione della sicurezza (SPU) per l'offload e l'accelerazione
- Il SecGW VNF, il più efficiente e compatto, assicura efficienza energetica e grande scalabilità, inclusa l'accelerazione IPSec



L'esigenza crescente di sicurezza della RAN

L'evoluzione della RAN e tutti i segmenti di mercato e casi d'uso attuali e futuri resi possibili dalle tecnologie e dalle infrastrutture 4G/5G hanno un forte impatto sull'esigenza di aumentare la sicurezza della RAN:

- **Grande, più grande, grandissima.**
  Per attuare la crescente scalabilità della tecnologia LTE-A e soprattutto 5G, è necessario l'impiego di una rete sempre più ampia di "piccole celle". Molte di queste femtocelle, picocelle e microcelle eNobeB (eNB) e gNodeB (gNB) saranno collocate nel dominio pubblico e in altri luoghi non sicuri. Inoltre, nella maggior parte dei casi, saranno anche collegate alla rete del MNO tramite un backhaul non affidabile. Questi elementi assieme rappresentano un fattore di rischio crescente che contribuisce all'aumento della superficie di attacco nel suo complesso e al rischio di manomissione, uso improprio e manipolazione del traffico.
- **Importanza e dimensione crescente del traffico utente (user plane).**
  La continua evoluzione del 4G e l'introduzione del 5G stanno gradualmente consentendo la realizzazione di casi d'uso commerciali e verticali che forniscono valore al di là della semplice connettività wireless. I MNO ora possono costruire casi d'uso in cui interi ecosistemi si uniscono per creare e promuovere l'innovazione nella produzione, nella sanità, nei trasporti, nell'energia e in altri settori. La fornitura di questi servizi "oltre la connettività" attribuisce un'importanza crescente alla RAN e al core per l'integrità e la continuità del traffico utente (user plane). Il traffico utente diventerà potenzialmente uno degli elementi più importanti della capacità dei MNO di fornire servizi a valore aggiunto (VAS) come infotainment, servizi Internet of Things (IoT) e servizi di realtà aumentata (AR), solo per citarne alcuni, dato che le applicazioni/servizi data target degli utenti risiedono all'interno del cloud telco o nell'ecosistema generale dei casi d'uso.

  Ciò determina la necessità di una maggiore sicurezza, integrità e continuità del traffico utente, che in alcuni casi d'uso della RAN subiranno una crescita significativa, assieme al traffico di controllo e O&M.
- **Architetture RAN diversificate e distribuite.**
  La necessità di migliori prestazioni, agilità, scalabilità, flessibilità ed economicità per la RAN hanno portato al suo graduale passaggio alle tecnologie LTE e 5G. Di conseguenza, i MNO gestiranno un ambiente RAN ibrido composto da diverse architetture centralizzate, distribuite e virtualizzate/cloud.

  Le architetture RAN dipenderanno anche dai requisiti specifici dei casi d'uso di ogni segmento di mercato o network slice. Ad esempio, la posizione delle unità distribuite e centralizzate (DU e CU) di eNB e gNB dipenderà da requisiti quali latenza e larghezza di banda/prestazioni.

  In un ambiente ibrido di questo tipo, composto da architetture e componenti LTE -A e RAN 5G, è indispensabile mantenere la sicurezza, l'integrità e la visibilità del control plane, dello user plane e dell'O&M attraverso un insieme comune di strumenti di sicurezza sufficientemente flessibili da adattarsi ai diversi requisiti, vincoli e architetture della RAN.
- **Casi d'uso critici dell'infrastruttura mobile.**
  Sia LTE-A che 5G sono in grado di fornire casi d'uso critici e innovazione in diversi settori come sanità, energia e trasporti. A differenza della precedente generazione mobile, la "standardizzazione" dell'infrastruttura mobile e la crescente dipendenza dai suoi servizi per alcuni casi d'uso critici stuzzicherà ulteriormente l'"interesse" della cybercriminalità per l'infrastruttura mobile come vettore e bersaglio degli attacchi e determinerà una crescente esigenza di sicurezza della RAN.

L'evoluzione dell'infrastruttura mobile 4G e 5G nel suo complesso, e della rete di accesso radio in particolare, sta determinando una maggiore esigenza di evoluzione della sicurezza della RAN: da SecGW a un'infrastruttura veramente sicura, iperscalabile, ibrida ed efficiente, che fornisca funzionalità di sicurezza avanzate SecGW e L3-L7.

Minacce in agguato nella RAN

Queste sono alcune delle principali forze che spingono i MNO a modernizzare e rafforzare l'attuale sicurezza della RAN per garantire la riservatezza, l'integrità e la continuità del servizio. In caso contrario, tutti i piani di comunicazione (control plane, user plane e O&M) potrebbero essere esposti a vari tipi di attacchi:

- Introduzione di eNB e gNB non autorizzati come punto di lancio per attacchi contro l'infrastruttura core
- Attacchi MIM (Man-In-the-Middle) per intercettare il traffico utente e di controllo
- Attacchi DoS/DDoS (Denial-of-Service)
- Iniezione di traffico dannoso (malware) per attaccare e manipolare elementi del core
- Errata configurazione o aggiornamenti software non riusciti all'interno della RAN

Uno qualsiasi di tali attacchi può interrompere la continuità della RAN, del core e del servizio nel suo complesso, esporre e modificare i dati utente, colpire sia i clienti che le applicazioni e i servizi del cloud telco, nonché in generale compromettere la capacità dei MNO di rispettare la normativa sulla privacy e la sicurezza dei dati.

La piattaforma FortiGate fornisce una vasta gamma di funzioni di rete fisica e virtuale con funzionalità SecGW e Next Generation Firewall (NGFW) incorporate. La riservatezza e l'integrità del traffico utente e di controllo sono protette, salvaguardando al tempo stesso la disponibilità e la continuità del servizio dagli attacchi informatici.

Infrastruttura di sicurezza della RAN di Fortinet

La soluzione Fortinet per la sicurezza della RAN sfrutta la piattaforma FortiGate nei suoi diversi fattori di forma della funzione di rete sia fisica che virtuale (PNF e VNF). FortiGate assicura tre funzioni di sicurezza fondamentali per la RAN:

- **Riservatezza** – FortiGate garantisce la protezione del traffico utente in tutta la RAN e nel core distribuito del data center (DC) centrale o dei siti MEC (Multi-access Edge Computing).
- **Integrità** – FortiGate protegge dalle modifiche illegali dei dati utente, come le iniezioni di malware o il traffico non autorizzato.
- **Disponibilità e continuità** – FortiGate protegge da attacchi che possono portare a un uso improprio della RAN e di elementi del core allo scopo di causare il degrado o l'interruzione del servizio.

FortiGate mette a disposizione un'unica piattaforma con funzionalità SecGW e un firewall di nuova generazione (NGFW) all'avanguardia, combinazione che garantisce un potente strumento con un ricco set di funzionalità versatili adatto alle più grandi distribuzioni di RAN 4G e 5G tier 1:

- Terminazione tunnel IPsec e aggregazione per eNB e gNB con autorizzazione e autenticazione PKI (Public Key Infrastructure)
- Le funzionalità di segmentazione interna garantiscono la segmentazione dell'accesso site-to-site
- Protegge le interfacce S1-U e S1-MME LTE
- Protegge le interfacce N2 e N3 5G
- Protegge l'interfaccia F1 DU-to-CU
- L'ispezione profonda del traffico incapsulato GTP-U protegge dalle minacce note e ignote L2-to-L7
- Firewall SCTP per l'ispezione e l'applicazione della sicurezza, compreso il supporto multi-homing
- Supporto multi-tenancy nativo con domini virtuali (VDOM)
- Fattori di forma flessibili per soddisfare tutte le esigenze di prestazioni e scalabilità
- Prestazioni elevate predicibili per siti centralizzati e regionali con unità di elaborazione della sicurezza (SPU) per l'offload e l'accelerazione
- Il SecGW VNF, il più efficiente e compatto, assicura efficienza energetica e grande scalabilità, inclusa l'accelerazione IPSec
- Ricco ecosistema di API e connettori per agevolare l'onboarding e l'integrazione nell'ecosistema generale del MNO come l'operatività e la gestione, l'orchestrazione e il sistema di supporto al business (BSS).

Architettura dell'infrastruttura di sicurezza della RAN di Fortinet

I MNO stanno progressivamente migrando verso distribuzioni 5G non standalone (NSA) e standalone (SA), per cui le RAN LTE e 5G in un modo o nell'altro coesisteranno. Le funzionalità e i fattori di forma flessibili di FortiGate ne fanno la scelta logica per proteggere RAN e architetture miste. Con le tecnologie LTE-A e NR 5G vi è una forte relazione tra categorie di servizio/qualità del servizio (QoS)/SLA e distribuzione della RAN, e quindi una relazione diretta con l'infrastruttura di sicurezza e i servizi distribuiti.

Ad esempio, gli SLA/QoS per le categorie di servizio eMBB (Enhanced Mobile Broadband, la telefonia mobile avanzata a banda larga), mMTC (Massive Machine-Type Communication, le comunicazioni macchina-macchina massive) e uRLLC (Ultra-Reliable Low Latency Communication, le comunicazioni ultra-affidabili a bassa latenza) utilizzano network slice i cui requisiti sono soddisfatti tramite un mix di componenti RAN e core centralizzati e distribuiti, che determinano l'architettura SecGW e le opzioni di distribuzione, come si evince dalla figura 1 qui sotto.

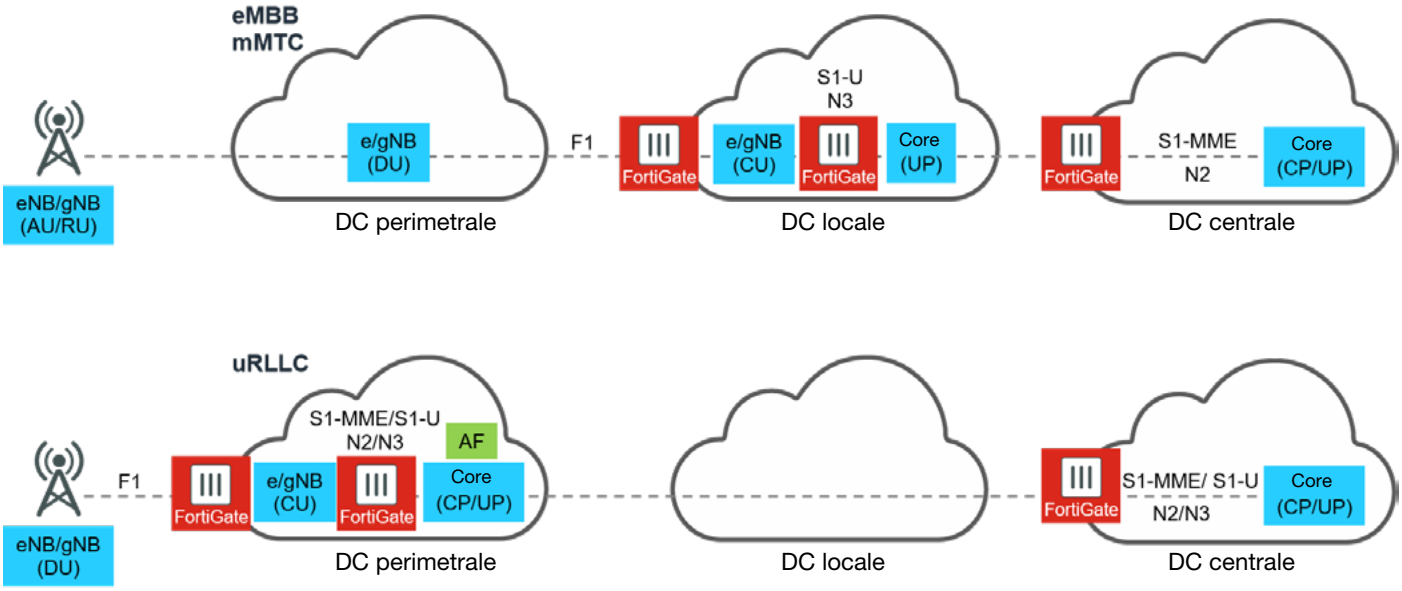


Figura 1: Possibile distribuzione delle network slice eMBB, mMTC e uRLLC e dei componenti della RAN

Gli operatori di reti mobili stanno costruendo l'infrastruttura 5G e il loro ambiente RAN è costituito da un insieme ibrido di architetture e tecnologie LTE, LTE-A e NR G5 che negli anni a venire coesisteranno e interagiranno. L'infrastruttura creata per la sicurezza della RAN dovrebbe fornire un insieme comune di strumenti applicabili al mix di tecnologie e architetture RAN per una maggiore agilità e flessibilità.

Distribuzione SecGW centralizzata

In un'architettura SecGW centralizzata, gli elementi del control plane e dello user plane si situano tutti nei siti eNB e gNB con connettività tunnel IPSec al FortiGate SecGW centrale che supporta il traffico di controllo, il traffico utente e il traffico O&M, nonché i servizi di sicurezza avanzati.

Trattandosi di un SecGW centralizzato, le prestazioni e la scalabilità a livello di IPSec e sicurezza sono di fondamentale importanza, assieme alla resilienza e alla disponibilità del servizio. Partendo da tali considerazioni, le appliance fisiche FortiGate sono la scelta più adatta perché garantiscono prestazioni di sicurezza e IPSec predicibili e accelerate, con latenza ultrabassa e alta disponibilità flessibile.

La nuovissima serie FortiGate 4000F è equipaggiata con l'ultima generazione, la settima, della tecnologia SPU del processore di rete Fortinet, in grado di offrire le prestazioni necessarie per LTE-A e NR 5G:

- Notevoli prestazioni in termini di throughput per tunnel singolo, fino a 110 Gbbps
- Prestazioni elevate a livello di flussi di lunga durata
- Latenza ultrabassa dell'ordine di µs
- Tecnologia "re-ordering avoidance"
- Supporto QoS completo
- Mirroring del traffico X2/Xn
- Scalabilità orizzontale dei cluster e georidondanza
- Supporto QKD (distribuzione di chiavi quantistiche)
- Failover automatico dei siti e aggiornamento del software in servizio
- Fattore di forma compatto e altamente efficiente dal punto di vista energetico

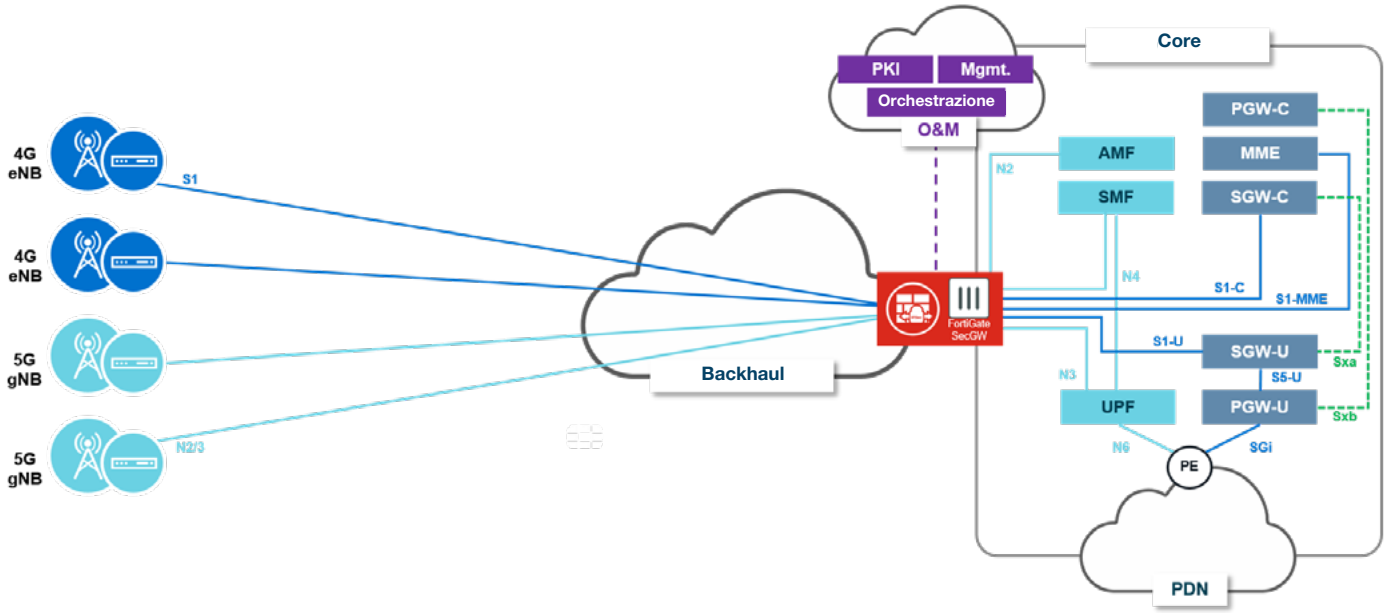


Figure 2: Distribuzione SecGW centralizzata

Il FortiGate assicura funzionalità SecGW e NGFW complete in quella che è la funzione di rete virtuale (VNF) più compatta ed efficiente del settore per small cell e siti di edge computing. La gamma FortiGate di funzioni di rete fisica (PNF) utilizza le SPU Fortinet, fornendo prestazioni hyperscale con latenza ultrabassa per grandi data center regionali e core mobile.

SecGW distribuito con distribuzione edge cloud

La capacità di terminare le connessioni VPN (Virtual Private Network) IPSec dello user plane con gli opportuni controlli di sicurezza a livello di edge cloud/MEC è d'obbligo in casi d'uso come i servizi basati sulla localizzazione, le applicazioni IoT critiche, la guida autonoma, ecc. L'edge cloud/MEC offre un breakout PDN (Packet Data Network) locale, ma può anche ospitare applicazioni come componenti della piattaforma IoT e applicazioni industriali per fornire la funzionalità e il servizio richiesti il più vicino possibile al consumatore del servizio.

In questa architettura, oltre al SecGW centrale che termina la connettività RAN al core, viene aggiunto un FortiGate SecGW all'edge cloud/MEC, terminando così le reti VPN dello user plane e proteggendo i dati utente per il breakout PDN locale e le applicazioni/servizi residenti localmente lungo il perimetro.

La scelta tra un FortiGate SecGW PNF o VNF per l'edge cloud/DC dipende sostanzialmente da considerazioni di scala e latenza:

- Numero di VPN IPSec terminate
- Volume previsto di dati utente terminati
- Modello di utilizzo (stabile o variabile nel tempo, upscale e downscale predicibili)
- Requisiti di latenza
- Efficienza in termini di prestazioni e consumo energetico

L'uso del FortiGate SecGW con funzione di rete virtuale (VNF) garantisce un'elevata flessibilità e agilità nella scalabilità dei servizi, ma con l'utilizzo di risorse VNFI (Virtual Network Function Infrastructure) condivise con prestazioni elevate, scalabilità e latenza per VNF limitate, l'ottimizzazione delle prestazioni della VNFI potrebbe non essere possibile. Se ne raccomanda pertanto l'adozione nei casi d'uso con requisiti di prestazioni e latenza medio-bassi.

Viceversa, l'uso del FortiGate SecGW con funzione di rete fisica (PNF) garantisce alte prestazioni predicibili e latenza ultrabassa grazie all'uso della tecnologia SPU Fortinet. Se ne raccomanda dunque la scelta nei casi d'uso che richiedono livelli di prestazioni e scalabilità alti o altissimi e/o per gli ambienti DC regionali e periferici con grande concentrazione di eNB/gNB.

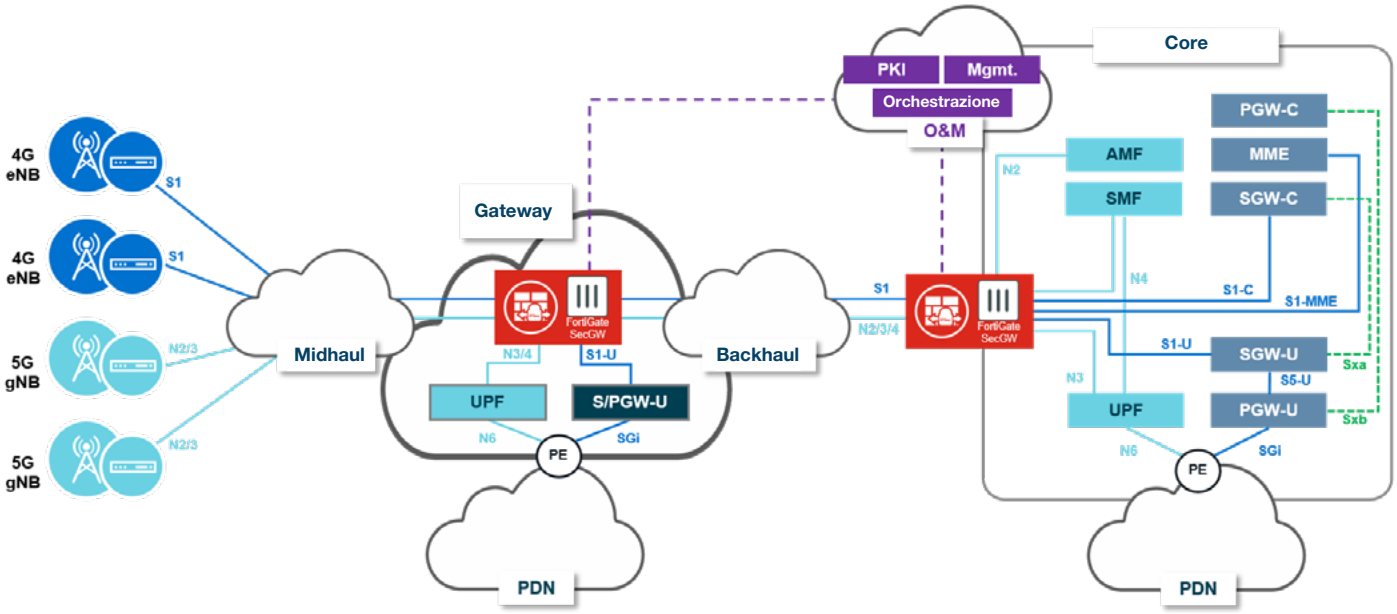


Figura 3: SecGW distribuito con distribuzione edge cloud

SecGW distribuito in una RAN virtuale scomposta

Nel caso di una vRAN scomposta, il SecGW fornisce la funzionalità IPSec e di sicurezza alla connettività DU-CU divisa perché sono disaccoppiate e residenti in diverse parti della rete, come illustrato nella figura 4. L'integrità e la privacy sono garantite per control plane e lo user plane dal Packet Data Convergence Protocol (PDCP-U & PDCP-U), ma alcuni messaggi di controllo sono trasmessi in chiaro, il che lascia il control plane F1 (F1-C) vulnerabile alle minacce e agli attacchi SCTP se non protetto adeguatamente da un SecGW. Nel caso specifico dell'architettura scomposta, la soluzione Fortinet SecGW garantisce l'autenticazione e l'autorizzazione DU-CU con IPSec (tunnelling compreso), la riservatezza (ricorrendo ove necessario alla crittografia) e la protezione dagli attacchi a livello di SCTP per F1-C.

Visto il volume relativamente ridotto dei dati di controllo, il FortiGate SecGW può essere utilizzato prima della CU come VNF per la sicurezza di F1-C.

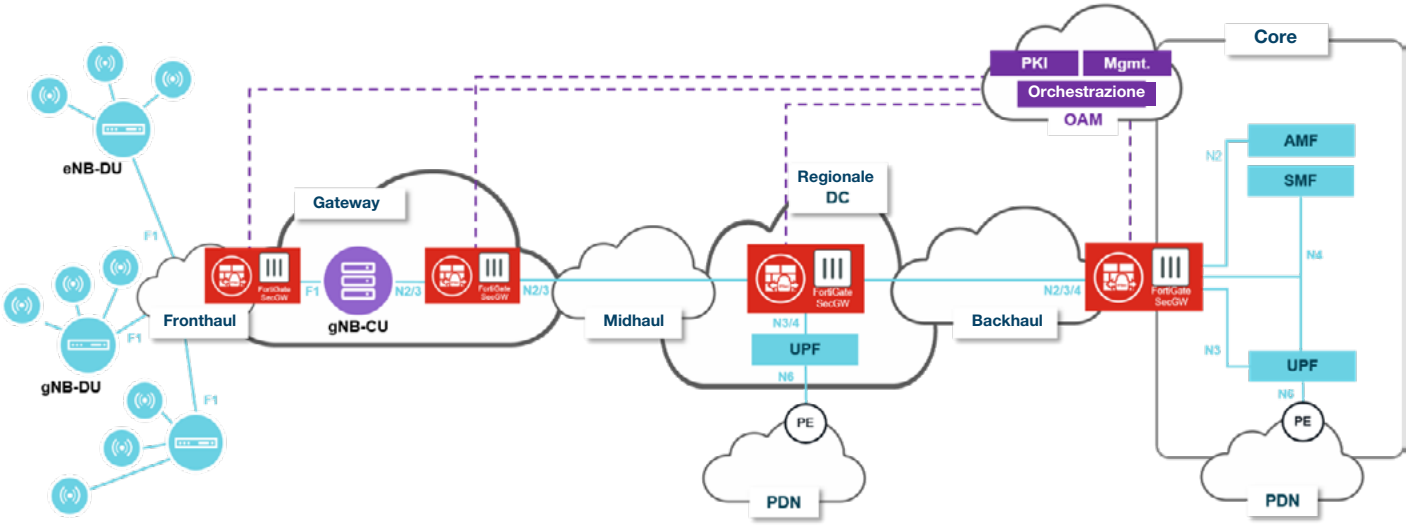


Figura 4: Distribuzione di un SecGW distribuito in una RAN virtuale scomposta

Connettività delle small cell

Femtocelle, picocelle e microcelle creano una fitta rete di piccole celle necessarie per ottenere sia la capacità che la scalabilità di copertura richieste dalle tecnologie LTE-A e NR 5G.

Distribuire e gestire una rete così grande è molto impegnativo sotto diversi profili, tra cui costi e sicurezza. Alcune di queste microcelle possono anche essere asset multi-tenant condivisi che consentono di ottenere una riduzione complessiva dei costi/un miglioramento del ROI.

Le principali sfide specifiche poste a livello di sicurezza dalle small cell possono riassumersi così:

- **Connettività di backhaul non sicura:** poiché nella maggior parte dei casi le small cell sono collegate a siti/DC centrali, regionali o anche perimetrali del MNO tramite una PDN non affidabile, che espone dunque sia il control plane che lo user plane a molte minacce, possono manifestarsi problemi a livello di privacy e verificarsi attacchi con effetti deleteri sulla disponibilità e la qualità del servizio.
- **Scalabilità:** le small cell si sommano ai requisiti di scalabilità del SecGW poiché rappresentano una potenziale aggiunta di reti di piccole celle dense, tutte connesse tramite VPN IPSec ai siti core/regionali/MEC del MNO.

La grande scalabilità e le notevoli prestazioni del SecGW Fortinet con sua vasta gamma di fattori di forma fisici e virtuali forniscono al MNO la capacità di affrontare tali sfide e proteggere la connettività delle small cell con gli stessi strumenti e funzionalità comuni forniti alle macrocelle.

L'ULTIMA PAROLA

Proteggere una rete di accesso radio 4G e 5G versatile, ibrida e altamente scalabile è più importante che mai proprio in ragione della natura evolutiva della tecnologia e dei nuovi possibili casi d'uso. Proteggere la RAN impone un nuovo tipo di infrastruttura SecGW, che sia agile e ibrido, ma al tempo stesso in grado di supportare le architetture miste e i diversi requisiti a livello di prestazioni, scalabilità e QoS che caratterizzano le tecnologie LTE-A e 5G.

La piattaforma FortiGate di Fortinet offre una piattaforma SecGW comune, flessibile e hyperscale già in uso presso i principali MNO tier 1 in tutto il mondo. La sua gamma di funzionalità e prestazioni SecGW e NGFW non ha eguali nel settore e garantisce una piattaforma su cui i MNO possono promuovere in tranquillità ricavi e crescita con i nuovi casi d'uso del 4G e del 5G.

FORTINET

www.fortinet.com

febbraio 16, 2021 11:55 AM

668851-0-1-IT