SINTESI DELLA SOLUZIONE

Proteggere infrastrutture e servizi 4G e 5G con Fortinet

Sintesi preliminare

L'evoluzione tecnologica delle reti mobili nel 4G e l'introduzione del 5G offrono agli operatori di reti mobili (MNO) l'opportunità di un profondo cambiamento nei segmenti di mercato indirizzabili, come anche nei servizi e nel valore offerti. Tali nuovi servizi e funzionalità sono fondamentali per consentire l'innovazione in tutti i campi, dalla produzione e dall'energia ai trasporti, alla logistica e alla sanità. La promessa del 5G, in particolare, è grande, ma solo se adeguatamente protetto.

L'innovazione digitale delle reti mobili crea una dualità nel ruolo che la sicurezza gioca negli ambienti mobili: la sicurezza interna dell'infrastruttura mobile e la sicurezza esterna dei casi d'uso con la loro monetizzazione. Fortinet è nella posizione migliore per aiutare diversi settori a realizzare i benefici del 4G e dell'imminente era del 5G attraverso una strategia di networking globale orientata alla sicurezza e il giusto supporto per un servizio e un'esperienza utente di qualità.

Sicurezza interna dell'infrastruttura mobile

Nelle precedenti generazioni di tecnologie mobili, il mercato consumer era il principale mercato indirizzabile, dove il valore fornito e, dunque i ricavi generati si limitavano a un piccolo insieme di servizi, principalmente voce, messaggistica e connettività internet. La maggior parte del valore e dei contenuti veniva fornita da terzi, non dal MNO.

Ciò ha portato a un'implementazione limitata della sicurezza per proteggere i punti di esposizione dell'infrastruttura mobile (come PDN non affidabili, core della RAN e connettività in roaming) dalle minacce esterne quale mezzo per contribuire a garantire la continuità del servizio. Tuttavia, poiché l'infrastruttura e le tecnologie mobili hanno continuato a evolversi, parimenti deve evolvere l'infrastruttura che le protegge, e il 5G sarà la cartina tornasole per capire quali reti possono rimanere sicure pur offrendo un'esperienza utente di prim'ordine.

Sicurezza esterna dei casi d'uso e loro monetizzazione

L'introduzione e l'implementazione di nuove tecnologie nelle reti 4G e 5G consentono ai MNO di offrire servizi a valore aggiunto che vanno ben oltre la connettività mobile. Questo mix di funzionalità può trasformarsi in servizi chiave per la capacità di un MNO di rivolgersi a diversi settori e soddisfare le loro esigenze in continua evoluzione.

La sicurezza nell'ambito di un caso d'uso per un determinato settore è importante sotto i seguenti profili:

- L'accettazione e l'adattamento del caso d'uso dipende dalla capacità del MNO di garantire i contratti sul livello di servizio (SLA) appropriati.
- Poiché nel contesto di un caso d'uso (al di là della semplice connettività) i MNO forniscono servizi a valore aggiunto (applicazioni, piattaforme, ecosistemi partner, ecc.), la loro capacità di proteggere questi componenti diventa una parte fondamentale della loro capacità di fornire il caso d'uso.
- La visibilità e il controllo della sicurezza all'interno di un caso d'uso possono essere monetizzati per la fornitura di servizi di sicurezza gestiti al cliente, creando così ulteriori ricavi e crescita per il MNO.

È prevedibile che, con la crescente disponibilità di servizi mobili innovativi, casi d'uso e relativi clienti, questi casi d'uso susciteranno l'attenzione degli autori delle minacce come possibili vettori o addirittura obiettivi di attacco. Si tratta di un'altra importante considerazione per la strategia globale di sicurezza del MNO.

Infrastruttura di sicurezza Fortinet per i MNO: salvaguardare l'innovazione e favorire la crescita

Fortinet propone un insieme comune di soluzioni e strumenti di sicurezza che forniscono visibilità e controllo della sicurezza end-to-end per infrastrutture mobili 4G e 5G, consentendo al contempo la sicurezza e la monetizzazione dei casi d'uso per diversi settori. Questo approccio facilita l'integrazione e l'onboarding, mantenendo al minimo le operazioni e gli sforzi di gestione. I prodotti e i servizi includono il firewall di prossima generazione FortiGate (NGFW) e il firewall per applicazioni web FortiWeb (WAF) che, insieme, consentono ai MNO di promuovere in modo sicuro l'innovazione di tecnologie, servizi e casi d'uso sia presso il segmento consumer che presso quello business.

Una sicurezza interna agile e performante per i servizi e l'infrastruttura mobile

Il diagramma sottostante illustra la soluzione Fortinet per proteggere l'infrastruttura del MNO dalle minacce e contribuire a garantire la disponibilità e la continuità del servizio.

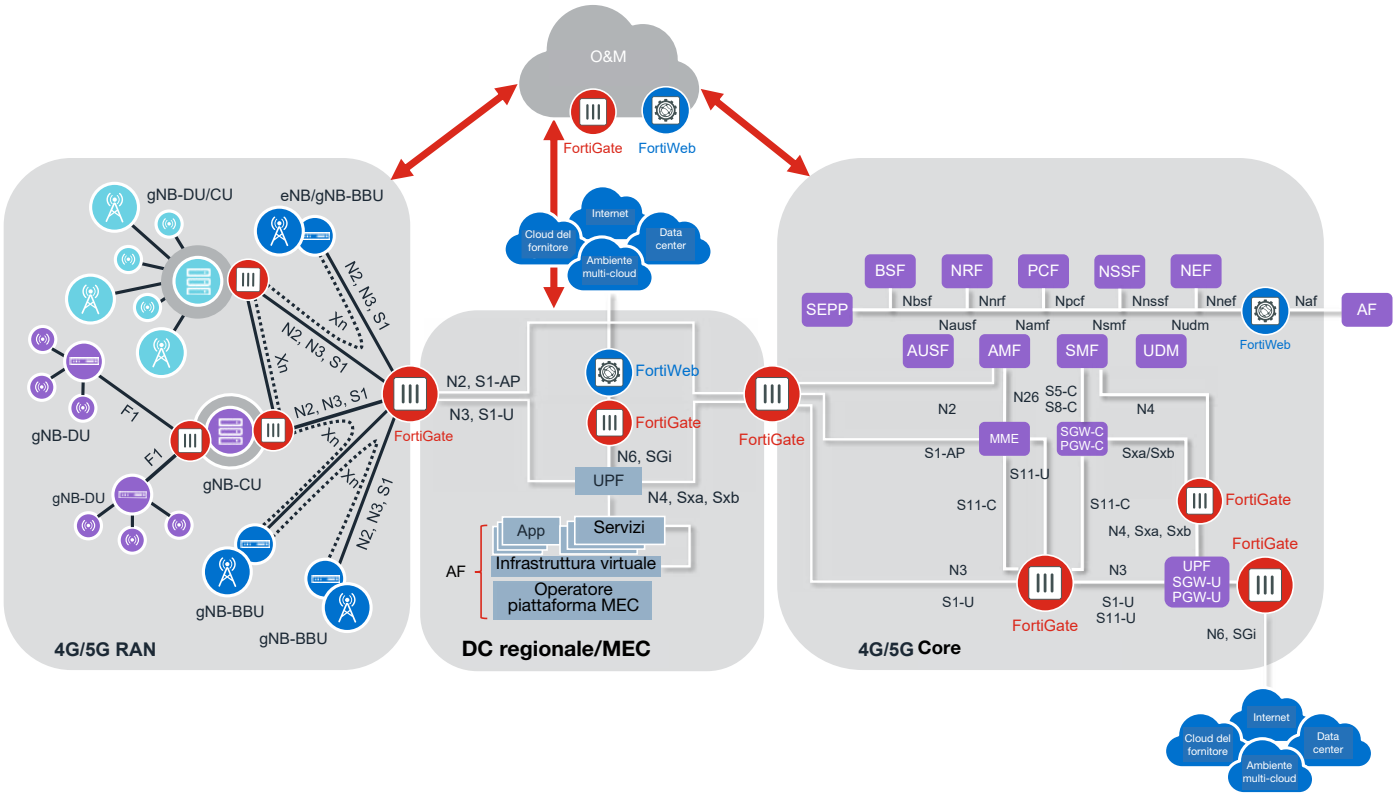

Figura 1: Proteggere l'ecosistema del MNO.

Sicurezza della rete di accesso radio (RAN)

Proteggere una RAN 4G e 5G versatile, ibrida e altamente scalabile è più importante che mai proprio in ragione della natura evolutiva della tecnologia radio e dei 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. Il FortiGate di Fortinet con la sua funzione di rete fisica (PNF) e la sua funzione di rete virtuale (VNF) 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 gestire le loro reti private virtuali (VPN) IPsec RAN e proteggere lo user plane e il control plane a livello S1, N2, N3 e Xn.

Sicurezza dell'ecosistema MEC (Multi-access Edge Computing)

La distribuzione di siti MEC con risorse di rete, storage e computing consente ai MNO di offrire applicazioni a bassissima latenza e casi d'uso, siano essi completamente ospitati nel sito MEC o parte di una più ampia distribuzione dell'ecosistema nel cloud telco e in cloud partner/nel cloud pubblico. Ciò richiede anche la capacità di terminare i dati utente con la funzione user plane locale (UPF) e il breakout PDN locale per il protocollo Internet (IP) e la connettività dell'API con le applicazioni e i partner dell'ecosistema.

La piattaforma FortiGate VNF/PNF fornisce una visibilità e un controllo di sicurezza NAT (CGNAT) di livello carrier-grade e NGFW L3-L7 completo per proteggere sia il traffico utente e di controllo che la connettività PDN a livello MEC. La piattaforma FortiGate può anche essere utilizzata per monetizzare la sicurezza fornendo servizi di sicurezza gestiti ai clienti mobili, tra cui sicurezza dell'Internet-of-Things (IoT), controllo delle applicazioni, protezione botnet e molto altro.

La piattaforma FortiWeb PNF, VNF o CNF (Cloud-native Network Function) garantisce la sicurezza delle applicazioni basate sull'intelligenza artificiale (AI) e delle API per applicazioni MEC ospitate localmente, nonché l'integrazione e la disponibilità di applicazioni e servizi di cloud partner.

Sicurezza dell'accesso non-3GPP

Tecnologie di accesso non-3GPP quali le tecnologie WLAN wireless possono essere collegate alla rete core 3GPP come EPC (Evolved Packet Core) in vari modi in base al business model dell'operatore e all'architettura preferita. Per l'accesso non-3GPP non protetto, l'apparecchiatura dell'utente si collega prima alla funzione di interworking non-3GPP (N3IWF) e poi rispettivamente alla funzione AMF (Access ad Mobility Management Function) e UPF per l'accesso 3GPP.

La piattaforma FortiGate fornisce il firewalling SCTP (Stream Control Transmission Protocol) per il control plane N3IWF N2 e i servizi L4-L7 NGFW per il traffico utente N3, garantendo a entrambi i piani la protezione da accessi ritenuti non affidabili.

Sicurezza del core mobile

Il core mobile, assieme alla RAN, è il nucleo che consente di proporre un'ampia gamma di servizi (da servizi di base ad avanzati) e casi d'uso a consumatori e imprese. Questo, unitamente a varie evoluzioni tecnologiche, come la separazione tra control plane e user plane 4G e 5G (CUPS), la virtualizzazione, la connettività PDN, la connettività dei roaming partner, la connettività RAN, l'architettura basata sul servizio (SBA), l'esposizione alle funzioni applicazione e molto altro, fanno del core mobile un obiettivo sempre più ricercato dagli autori delle minacce.

Gli stessi strumenti usati per proteggere la RAN e il MEC vengono impiegati per proteggere il core mobile, offrendo vere e proprie funzioni di visibilità e controllo della sicurezza dell'infrastruttura mobile end-to-end.

La piattaforma FortiGate PNF/VNF assicura:

- Sicurezza NGFW L4-L7 PDN 4G/5G e servizi CGNAT con grande scalabilità e bassissima latenza sulla connettività SGi e N6
- Sicurezza del data plane con firewalling GTP-U e ispezione profonda dei contenuti a livello N3 e S1-U
- Gateway di sicurezza core-to-RAN (SecGW) con grande throughput e scalabilità VPN
- Sicurezza da control plane a data plane a livello di Sxa/Sxb e N4

Le funzioni SBA del 5G usano le chiamate API su HTTP V2 per le comunicazioni di controllo. La piattaforma FortiWeb protegge dagli attacchi a livello di HTTP e applicazione, garantendo anche il rispetto dello schema e dei valori dell'API, nonché le funzionalità gateway dell'API per la funzione di esposizione SBA.

Sicurezza per le reti private 4G e 5G

Le reti private cellulari forniscono funzionalità che possono essere necessarie per servire i casi d'uso mission-critical o business-critical di un'organizzazione, dalla connettività alla qualità del servizio, passando per la sicurezza, la disponibilità, la latenza, ecc., tutto personalizzato in base alle esigenze dell'azienda.

La realizzazione e la gestione di reti cellulari private variano a seconda dell'architettura, dei servizi e delle funzionalità, della complessità, ma anche a seconda delle esigenze e dei requisiti dell'impresa. Le reti private possono essere fornite come ambiente chiuso e completamente privato presso la sede del cliente (compresi RAN, MEC e core), come ambiente condiviso tra l'azienda e il MNO (RAN e control plane condivisi) o come rete end-to-end.

Indipendentemente dall'architettura e dalla soluzione, la sicurezza deve essere integrata in diversi punti dell'architettura creata per garantire la disponibilità del servizio e l'integrità dei dati utente. Il FortiGate e la piattaforma FortiWeb garantiscono queste funzioni comuni di visibilità e controllo della sicurezza, a prescindere dall'architettura della rete e dai servizi, tra cui sicurezza di SecGW RAN, CGNAT, NGFW L4-L7, API e applicazioni.

Sicurezza dei casi d'uso per diversi settori e loro monetizzazione

I servizi di sicurezza integrati nelle piattaforme FortiGate e FortiWeb già usati per proteggere l'infrastruttura mobile possono anche servire a proteggere i casi d'uso per diversi settori e consentire la monetizzazione della sicurezza attraverso la fornitura di servizi di sicurezza gestiti adeguati a ciascun caso d'uso.

Ad esempio, per la digitalizzazione di uno stabilimento (connect smart factory) si può utilizzare il FortiGate nel MEC locale o nel data center più vicino per proteggersi da attacchi IoT, tempeste di segnali e malfunzionamenti, fornendo al tempo stesso servizi di sicurezza allo stabilimento stesso come, ad esempio, protezione da malware, protezione botnet, controllo delle applicazioni, URL filtering, ecc. Il FortiWeb può fornire sicurezza a livello di applicazioni e API per le applicazioni industriali che risiedono nel MEC e la loro integrazione con applicazioni di terzi. E, con le stesse piattaforme FortiGate e FortiWeb usate nella RAN, nel MEC e nel core, l'onboarding e le operazioni di protezione di nuovi casi d'uso e la fornitura di servizi di sicurezza al cliente aziendale diventano rapidi ed economici.

In sintesi

Attraverso l'uso di due piattaforme carrier-grade, FortiGate e FortiWeb, Fortinet consente ai MNO di salvaguardare la loro infrastruttura mobile 4G e 5G, proteggere un'ampia gamma di casi d'uso innovativi per le imprese, fornire reti private con servizi di sicurezza integrati e monetizzare l'investimento nella sicurezza Fortinet.

L'utilizzo di un insieme di strumenti di sicurezza consente agli operatori di razionalizzare gli aspetti operativi e di onboarding della sicurezza complessiva dell'infrastruttura mobile e dei servizi, riducendo i costi, ovviando alla carenza di tecnici formati in materia e migliorando, in generale, l'agilità e la capacità di creare valore per conquistare la fiducia e il consenso dei clienti.

febbraio 16, 2021 11:43 AM

734139-0-1-IT