WHITE PAPER

Proteggere le reti mobili private 5G

Le imprese di molti settori guardano alla tecnologia e ai servizi 5G come a un fattore chiave per la trasformazione e l'innovazione digitale.

Le reti mobili non pubbliche, ovvero le reti mobili private, promettono i vantaggi della tecnologia 5G personalizzati in base alle esigenze specifiche dell'impresa, casi d'uso, privacy, gestione e controllo.

Studi indicano che la spesa per le reti mobili private registrerà una crescita continua. ABI Research ha recentemente stimato che nell'arco di circa 15 anni la spesa per le reti private e le reti aziendali condivise 5G supererà la spesa per le reti mobili pubbliche.[1]

È chiaro che le reti mobili private sono tra i casi d'uso critici del 5G e, pertanto, devono diventare offerte importanti da parte degli operatori di reti mobili (MNO), soprattutto perché le imprese e le industrie progrediscono con l'innovazione digitale e l'Industria 4.0.

La capacità giuridiche e pratica delle imprese di costruire le proprie reti private 5G, indipendentemente dalle infrastrutture e dai servizi pubblici 5G, è sia una minaccia sia un'opportunità per i MNO:

- **Una minaccia** di potenziale perdita di fatturato e rallentamento della crescita in assenza di un'offerta completa per una rete 5G privata.
- **Un'opportunità** per creare una vera e propria differenziazione competitiva 5G oltre che un volano di reddito e crescita con un'offerta completa per una rete 5G privata e un ecosistema che la supporti.

La costruzione di reti mobili private alimenterà nuovi casi d'uso, promuoverà l'innovazione e l'efficienza e diventerà una delle principali tecnologie di connettività per l'Industria 4.0. La sicurezza informatica deve essere al primo posto sia per le imprese che per i MNO in modo da garantire disponibilità, continuità, privacy e integrità della rete, dei suoi servizi, delle sue applicazioni, dei suoi dati e dei partner del suo ecosistema.

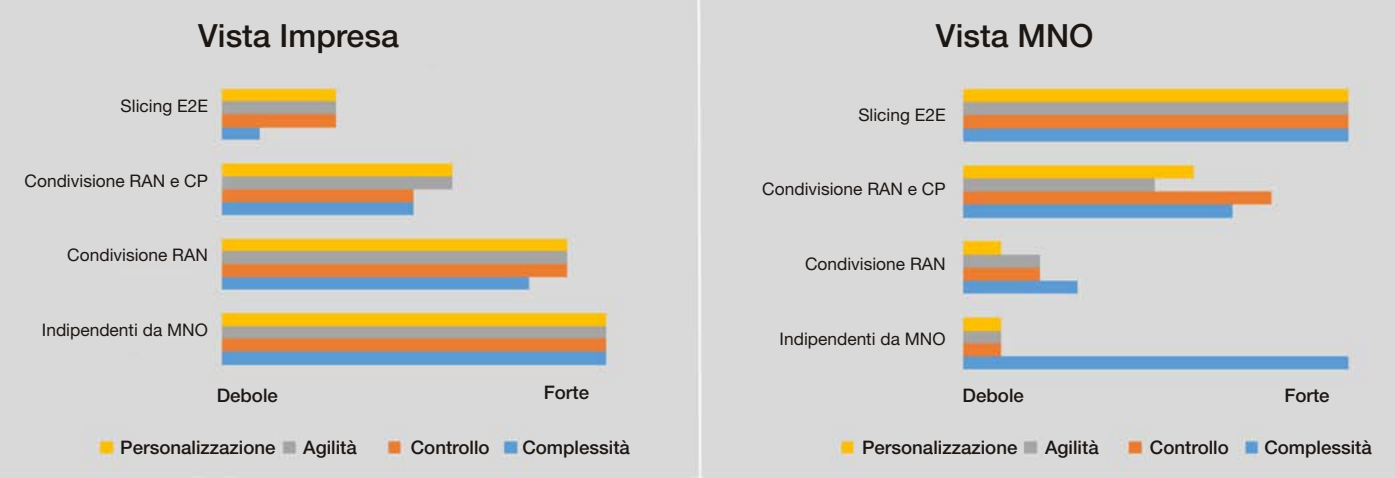
Architetture mobili private e sicurezza informatica

Le reti private 5G possono essere realizzate con due categorie principali di architettura, ciascuna con un impatto diretto sui rischi per la sicurezza informatica, la proprietà e le soluzioni. Le architetture indipendenti dai MNO e quelle dipendenti dai MNO si differenziano per il livello di dipendenza dall'infrastruttura 5G pubblica, la posizione fisica dei loro componenti e la possibile proprietà e gestione, come indicato nello schema 1 di seguito.

		Categoria: architetture di rete mobile privata			
		Indipendenti da MNO	**Dipendenti da MNO**		
		Nessuna condivisione	Condivisione RAN 5G pubblica	Condivisione control plane e RAN 5G pubblica	Condivisione totale 5G pubblica (slicing end-to-end)
Componente	Rete di accesso radio (RAN)				
	Control plane (CP)				
	Data plane (UPF)				
	Multi-access edge computing (MEC)				
Componente della rete 5G privata fisicamente isolato dalla rete 5G pubblica			**Componente della rete 5G privata logicamente isolato dalla rete 5G pubblica**		

Schema 1: Componenti della rete 5G privata e relazione con le risorse della rete 5G pubblica.

Il livello di dipendenza dalle risorse della rete 5G pubblica ha un impatto considerevole, sia per un'impresa che per un MNO, su fattori quali la complessità, l'agilità e il controllo. Questi impatti, tuttavia, possono essere diversi per le imprese e i MNO e vanno considerati nella scelta dell'architettura di rete privata appropriata da realizzare, oltre ai requisiti dello specifico caso d'uso distribuito.



Schema 2: Principali considerazioni sull'architettura delle reti private al di là dei requisiti del caso d'uso.

Reti private 5G: rischio per la sicurezza informatica e soluzioni

Sono molte le architetture per distribuire reti mobili private, che variano in base alle esigenze dell'impresa/industria e ai casi d'uso, oltre che in base alle normative sullo spettro e l'allocazione dello spettro per ciascun paese. Ogni architettura introduce rischi per la sicurezza informatica che devono essere ridotti al minimo dal MNO, dall'impresa o da entrambi.

Indipendentemente dall'architettura, garantire la sicurezza di una rete mobile 5G privata deve essere considerato fondamentale sia per l'impresa che per il MNO. La tabella che segue riassume le soluzioni di sicurezza Fortinet per le reti mobili private 5G, compresi gli obiettivi di sicurezza e i principali servizi. Le soluzioni Fortinet garantiscono protezione e integrità del servizio, privacy, disponibilità e continuità di fronte ai possibili rischi e attacchi informatici.

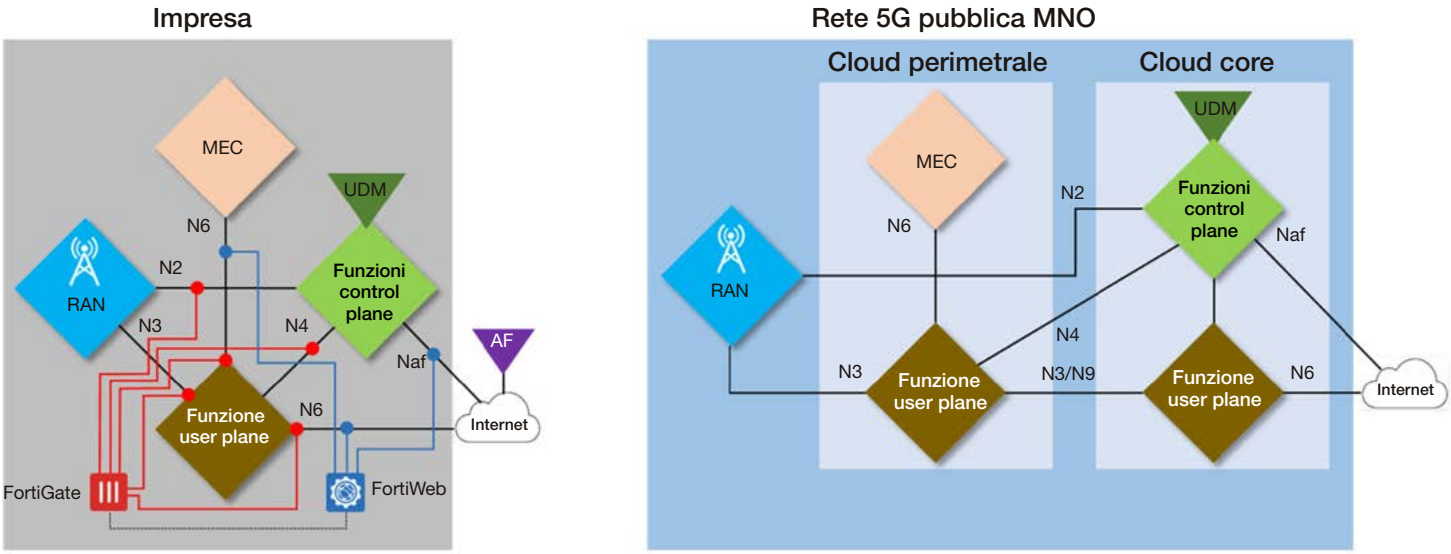
Piattaforma di sicurezza	Fattore di forma	Obiettivo	Servizi piattaforma di sicurezza
FortiGate	Fisica (PNF) Virtuale (VNF)	Proteggere le comunicazioni tra RAN privata (gNB) e core	■ Autenticazione gNB ■ Terminazione gNB-to-VPN core ■ Protezione da minacce tramite ispezione profonda (GTP-U) user plane ■ Firewalling SCTP ■ Firewall L4-L7 per protezione core
		Proteggere dalle tempeste di segnali IoT nella rete privata	■ Limitazione rate di tunnel e sessioni su N3 con monitoraggio N4 ■ Blocco sessioni non autorizzate su N3 ■ Blocco tempeste di riconnessione
		Proteggere la rete privata dalle minacce provenienti da PDN/internet	■ Servizi IPS e antivirus ■ Firewall L4-L7 per protezione da minacce PDN/Internet ■ Protocollo applicazioni e URL filtering ■ Attenuazione bot
		Garantire la connettività da rete privata a indirizzo PDN	■ Traduzione di indirizzi di rete IPv4 - IPv6

Piattaforma di sicurezza	Fattore di forma	Obiettivo	Servizi piattaforma di sicurezza
FortiWeb	Fisica (PNF) Virtuale (VNF) Contenitore (CNF)	Proteggere da minacce e attacchi a livello di applicazione MEC	▪ Attenuazione di attacchi contro applicazioni Top 10 OWASP ▪ Protezione da minacce note e attacchi zero-day ▪ Attenuazione bot ▪ ML per minimizzazione falsi positivi ▪ Validazione protocollo
		Proteggere le API della rete privata da: attacchi API, comportamenti anomali, configurazioni errate Proteggere l'esposizione delle API del signaling plane della rete privata alle funzioni delle applicazioni esterne (AF)	▪ Supporto nativo per HTTP/2 ▪ Verifica OpenAPI 3.0 ▪ Conformità protocollo JSON, limiti e validazione schema ▪ Conformità protocollo XML, limiti, validazione schema, entità esterne, SOAP ▪ Supporto WebSocket: applicazione di signature su connessioni WebSocket, limiti di frame e messaggi, disabilitazione estensioni ▪ Gateway API: gestione chiavi API, limiti rate di accesso e controllo

Tabella 1: Piattaforme di sicurezza Fortinet e servizi per reti 5G private.

Architettura di rete mobile privata indipendente dal MNO

In questa variante, non vi è alcun tipo di relazione tra la rete 5G privata e quella pubblica. Questa distribuzione può essere costruita e gestita dall'impresa, dal MNO, da un fornitore di tecnologia mobile o una loro combinazione. Tuttavia, la complessità e la potenziale mancanza di know-how tecnico escludono, nella maggior parte dei casi, la realizzazione da parte dell'impresa.



Schema 3: Architettura di rete 5G privata protetta e indipendente da MNO.

Come illustrato nello schema 1, una rete privata completamente indipendente dal MNO e protetta conterrà autonomamente tutti i componenti (RAN, control plane, data plance e MEC) necessari presso la sede dell'impresa. Lo spettro 5G utilizzato potrà essere concesso in licenza/non concesso in licenza oppure si potrà utilizzare lo spettro 5G concesso in licenza al MNO nei casi in cui la rete privata sia costruita e gestita dall'operatore.

In base ai servizi di rete privata e ai casi d'uso realizzati, può essere necessaria la connettività alle reti dati a pacchetto e a Internet per i data center aziendali, i sistemi e le applicazioni di partner e personale esterno, i cloud pubblici, l'intercettazione legale e altre interazioni.

In una soluzione Fortinet, la sicurezza viene attuata on-premises con FortiGate e FortiWeb per garantire:

- **Isolamento RAN-to-core privato e attenuazione dei possibili attacchi.** Sebbene in questa architettura tutti i componenti della rete privata siano completamente isolati per la rete pubblica 5G, un UE infetto o una minaccia interna devono essere considerati possibili rischi. (In alcuni paesi la legge prevede che anche una RAN 5G privata debba fornire l'accesso alla rete 5G pubblica. Anche se non rappresentata in questa architettura, tale situazione richiederebbe una connettività di rete 5G privata-pubblica e un isolamento di sicurezza completo tra VNP RAN-to-core privata e pubblica sia per il control plane che per lo user plane.)
- **Sicurezza contro le minacce provenienti da UE/IoT**, come le tempeste di segnali, i dispositivi infetti/malfunzionanti e la protezione bot IoT.
- Quando serve una connettività esterna alla rete dati pubblica (PDN), vengono applicati i servizi di **firewall di prossima generazione (NGFW)** per proteggere da minacce note e ignote provenienti da PDN/Internet.
- La **protezione a livello di applicazione** è garantita per l'IoT e l'ecosistema di applicazioni nel MEC della rete privata e altrove.
- È inoltre garantita la **sicurezza a livello di API** per le applicazioni esterne e MEC basate su API e l'integrazione di terzi.

La sicurezza può essere implementata e gestita dall'impresa stessa, da un partner o dal MNO nell'ambito di una rete mobile privata fornita come servizio gestito.

Architettura di rete mobile privata dipendente dal MNO

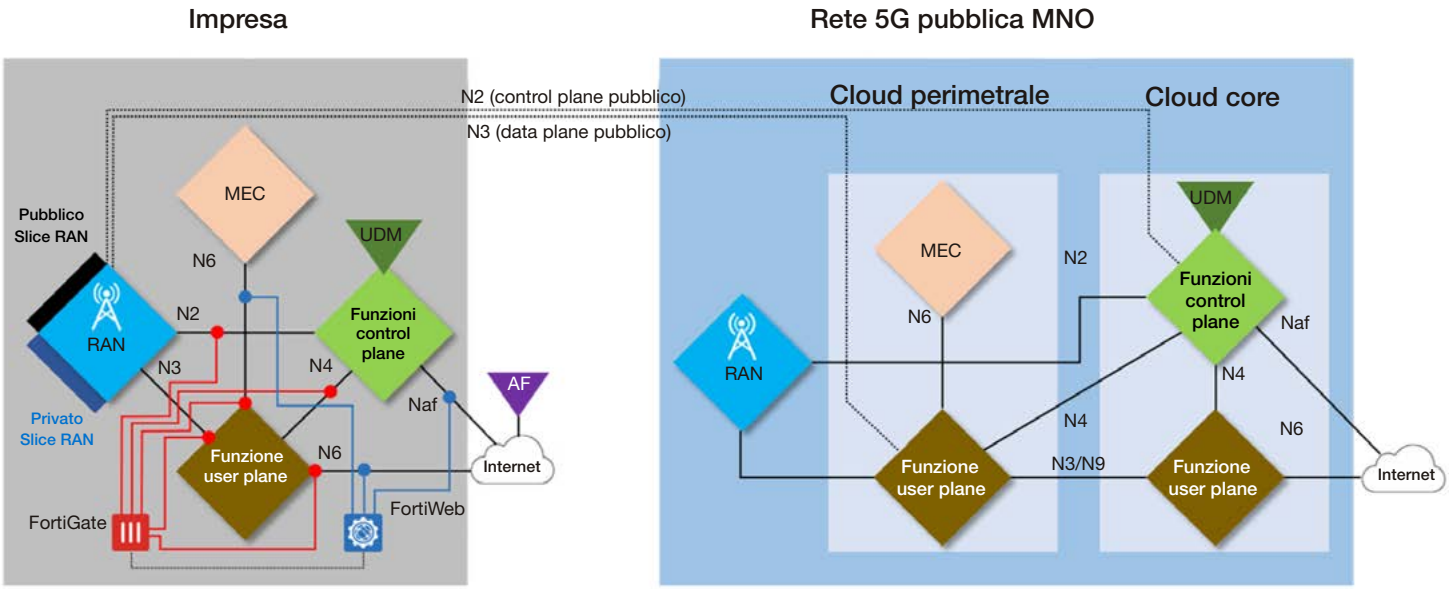
In questa categoria, le architetture si differenziano in base alla quantità di risorse 5G pubbliche necessarie, come precedentemente illustrato nel schema 1. È più probabile che queste architetture siano distribuite dall'operatore e co-gestite con il cliente. Di seguito sono descritte alcune delle possibili architetture che rientrano in questa categoria.

Architettura di rete mobile privata con condivisione della RAN

In questa architettura, la RAN (gNB situati all'interno della sede dell'impresa) è condivisa tra la rete 5G privata e quella pubblica con l'implementazione dello slicing della RAN. Questo significa:

- **Slice privata** in cui tutto il traffico dati e di controllo dei dispositivi UE/IoT della rete privata rimane all'interno della rete privata ed è servito dai componenti della rete privata
- **Slice pubblica** in cui il traffico dati e di controllo dei dispositivi UE/IoT della rete pubblica lascia la sede dell'impresa ed è servito dalla rete 5G pubblica del MNO

Come in tutte le architetture, è probabile che sia necessaria una connettività PDN esterna alla rete privata e al MEC.



Schema 4: Architettura di rete 5G privata con condivisione della RAN.

Oltre all'implementazione della sicurezza descritta nell'architettura indipendente dal MNO, occorre prestare particolare attenzione all'isolamento e all'ispezione profonda dei pacchetti delle VPN (control plane e data plane) private e pubbliche, in modo da salvaguardarsi da attacchi alle reti private provenienti dalla slice pubblica della RAN ed evitare possibili fughe di dati.

Nelle soluzioni Fortinet, il FortiGate e il FortiWeb sono distribuiti presso la sede dell'impresa e forniscono la visibilità e il controllo della sicurezza richiesti, come indicato nella tabella 1.

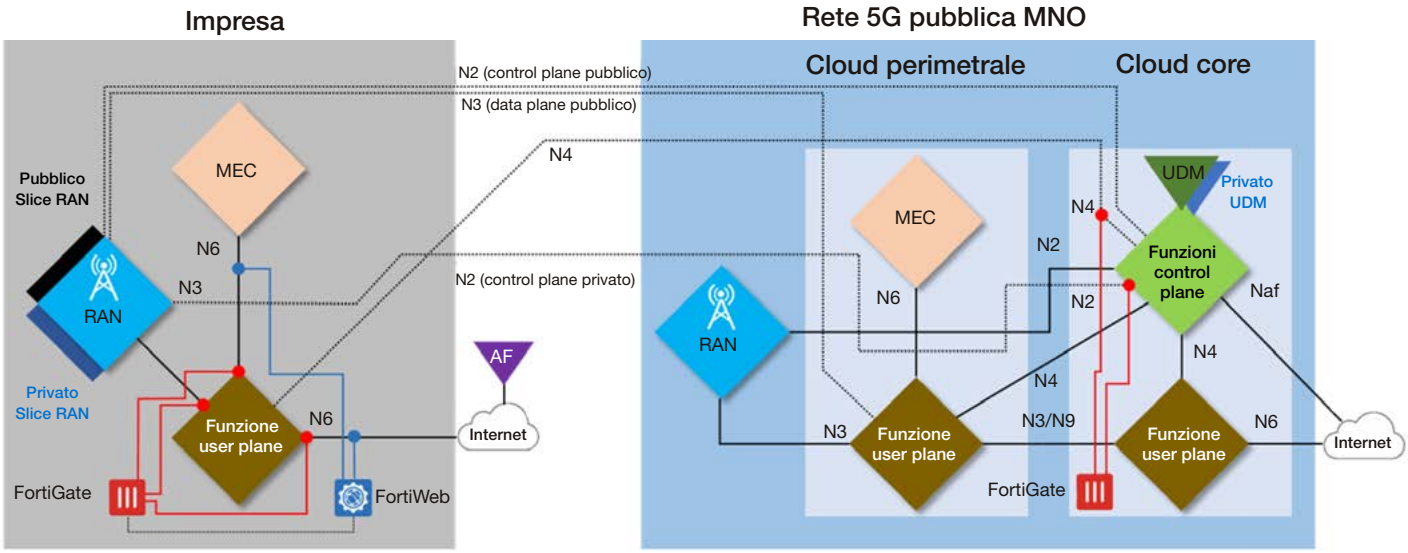
Architettura con condivisione della RAN e del control plane

In questa architettura, la RAN (presso la sede dell'impresa) e il control plane sono forniti attraverso la rete pubblica del MNO e separati logicamente dalla parte pubblica del control plane e dalla RAN pubblica tramite una slice privata dedicata. Ciò consente di mantenere i dati dell'impresa all'interno dell'impresa e di isolarli dalla rete pubblica del MNO.

È necessario garantire l'interazione delle funzioni del control plane con i componenti della rete privata come l'UPF ed eventuali funzioni di applicazioni esterne (AF). Ciò si ottiene con la distribuzione della piattaforma FortiGate da parte del MNO nel suo core cloud, come mostra lo schema 5 di seguito. Il supporto multi-tenancy del FortiGate permette l'implementazione della sicurezza RAN-to-core per più slice (control plane e RAN) private con un unico FortiGate VNF/PNF.

Vale la pena di notare che, poiché le funzioni del control plane sono eseguite nella rete pubblica, possono esporre alcuni dati sensibili dell'impresa, come le informazioni dei dispositivi UE/IoT, che sono memorizzati nel core della rete pubblica del MNO (nell'UDM). Pertanto, in questa architettura, il controllo e la riservatezza devono essere garantiti dal MNO.

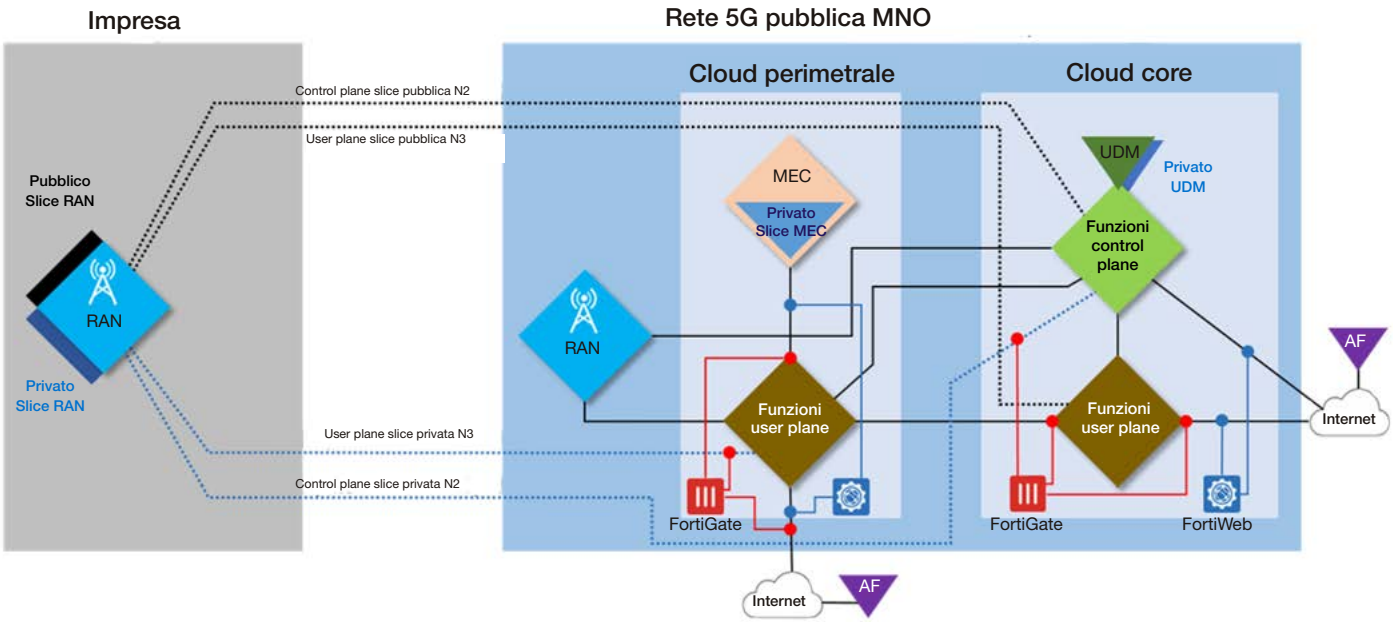
Il MEC e la funzione del data plane sono presso la sede dell'impresa, consentendo casi d'uso e applicazioni che richiedono una latenza ultrabassa.



Schema 5: Architettura di rete 5G privata con condivisione della RAN e del control plane.

Architettura di rete mobile privata con slicing end-to-end

In questa architettura, la rete mobile privata dell'impresa è una rete logica creata con slice di rete end-to-end (o più slice) sull'infrastruttura 5G pubblica. Solo il gNB viene distribuito presso la sede dell'impresa per servire i dispositivi UE/IoT locali. Il MEC e l'UPF sono il più vicino possibile all'impresa, addirittura al suo interno, per consentire applicazioni e casi d'uso a bassa latenza.



Schema 6: Architettura di rete 5G privata con slicing end-to-end.

Poiché la rete 5G privata è fornita logicamente su una rete 5G condivisa pubblicamente, il control plane e il data plane, così come qualsiasi interazione delle API con le AF esterne/basate su MEC dovrebbero essere visibili e protetti. (Nelle soluzioni Fortinet, questo è gestito tramite FortiGate e FortiWeb.) Ciò è fondamentale per garantire la sicurezza della rete privata e la sicurezza della rete 5G pubblica condivisa. Dal punto di vista della sicurezza, tale architettura può essere considerata come un'"immagine speculare" all'architettura indipendente dal MNO, in cui il MNO ha la massima responsabilità di garantire la sicurezza della sua offerta di rete mobile 5G privata.

In sintesi

Le reti 5G private sono un chiaro caso d'uso precoce del 5G, ma non potranno svilupparsi senza la giusta sicurezza. Per conquistare quote di mercato e ricavi, i MNO devono fornire un insieme di architetture e servizi flessibili e sicuri per soddisfare la domanda di 5G privato da parte di diversi settori.

Con un insieme comune di soluzioni di sicurezza applicabili ad un'ampia gamma di architetture e casi d'uso, le soluzioni Fortinet consentono ai MNO di soddisfare i requisiti di sicurezza fondamentali per le imprese, sia come parte di un'offerta di rete 5G privata che come insieme di servizi di sicurezza gestiti.

[1] ABI Research 5G Summit, 14 luglio 2020.

febbraio 16, 2021 12:19 PM

771877-0-0-IT