GUIDA ALLA PROGETTAZIONE

CLOUDFLARE

Cloudflare One, la nostra piattaforma SASE

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

INDICE

Nota: altri casi d'uso saranno aggiunti a breve

Informazioni su questa guida

Questa guida alla progettazione è destinata a professionisti con una mentalità tecnica e fornisce esempi illustrativi di come le organizzazioni possono semplificare e rafforzare la loro architettura di rete e sicurezza con Cloudflare One, la nostra piattaforma SASE. Cloudflare One unifica i servizi di connettività di rete con i servizi di sicurezza Zero Trust, tutti forniti sulla rete globale di Cloudflare.

La prima sezione di questa guida alla progettazione si concentra sulla trasformazione olistica e sulla modernizzazione illustrando tutti i possibili elementi di connettività e sicurezza allineati alle reti in entrata, alle reti in uscita e alle applicazioni prima e dopo Cloudflare. Si confronta quindi l'approccio perimetrale di sicurezza centralizzato legacy basato su soluzioni multi-vendor con l'approccio di rete globale Cloudflare che sfrutta un'architettura di piattaforma componibile.

Nelle sezioni successive sono illustrati i casi d'uso tecnici comuni: in primo luogo, come viene generalmente risolto il problema con un approccio legacy e, quindi, come Cloudflare One risolve lo stesso problema con maggiore efficienza e migliore esperienza.

A due casi d'uso è stata assegnata la priorità in base alla loro popolarità tra i clienti, ma non rappresentano in alcun modo l'intero ambito delle capacità di Cloudflare One.

- Accesso sicuro per applicazioni Web private e pubbliche
- Filtro DNS per dipendenti locali e remoti

Continueremo ad ampliare questa guida con ulteriori casi d'uso, tra cui l'accesso sicuro a reti private, minacce avanzate/protezione dei dati e altro ancora.

Trasformazione: prima e dopo Cloudflare

Connettività sicura, veloce, affidabile e privata per qualsiasi utente

Qualsiasi utente

Le organizzazioni devono abilitare una connettività sicura, veloce, affidabile e privata per due tipi di utenze.

Gli **utenti gestiti** sono dipendenti che accedono a una risorsa con un dispositivo aziendale o personale da casa, dall'ufficio o da qualsiasi altra posizione intermedia.

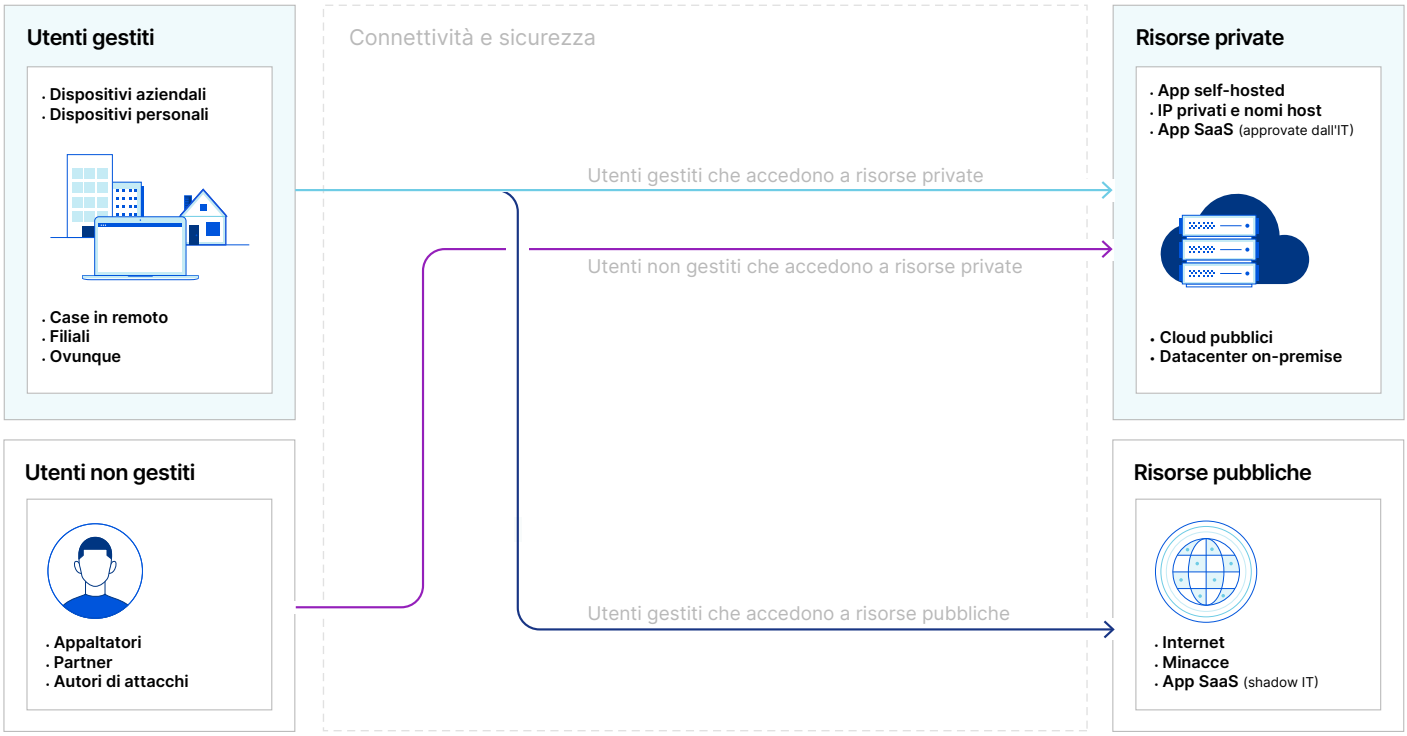
Gli **utenti non gestiti** includono appaltatori o partner autorizzati ad accedere a una risorsa ma anche autori di attacchi che non lo sono.

Tutte le risorse

Le organizzazioni devono abilitare la gestione degli accessi con minacce e protezione dei dati per due gruppi di risorse.

Le **risorse private** includono app self-hosted e IP privati o nomi host all'interno di cloud pubblici e data center on-premise, oltre ad app SaaS approvate dall'IT.

Le **risorse pubbliche** su Internet includono app e minacce SaaS non autorizzate.



Confronto di connettività e sicurezza prima e dopo Cloudflare

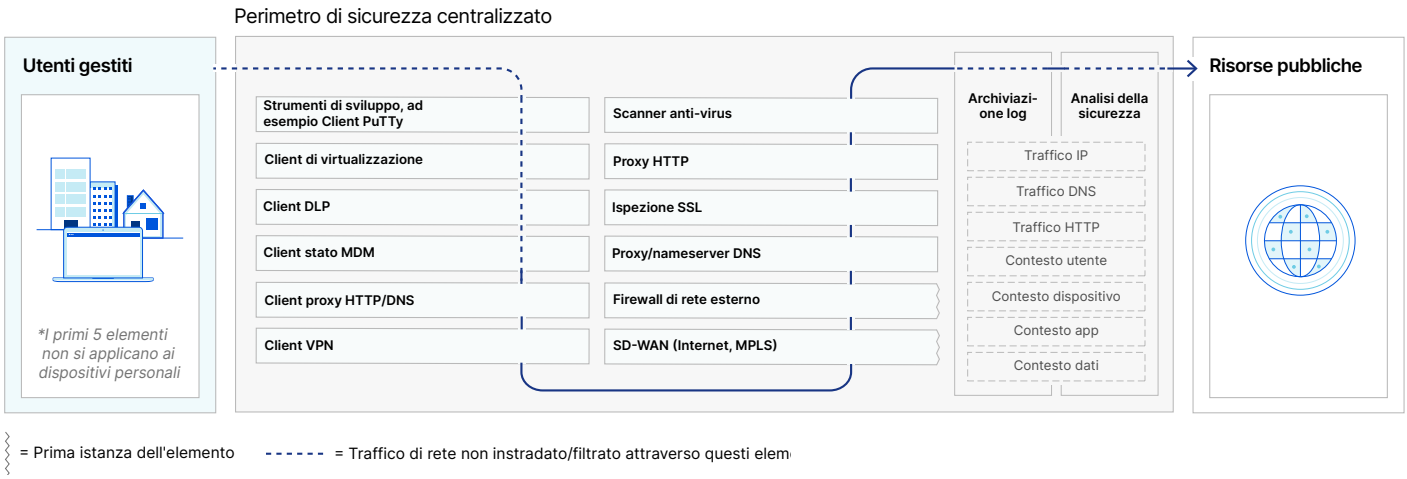
Nelle sei pagine successive, una serie di diagrammi "prima e dopo" riportano in modo incrementale i dettagli di tutti i possibili elementi di connettività e sicurezza richiesti dall'organizzazione per gli utenti gestiti che accedono alle risorse pubbliche e gli utenti gestiti o non gestiti che accedono alle risorse private.

Il primo diagramma "prima" illustra il calcolo dell'endpoint e le appliance di rete distribuite in un perimetro di sicurezza centralizzato.

Il secondo diagramma "dopo" illustra i servizi cloud comparabili forniti tramite la rete globale di Cloudflare.

1a. Semplificazione di connettività e sicurezza per le risorse pubbliche

Prima di Cloudflare



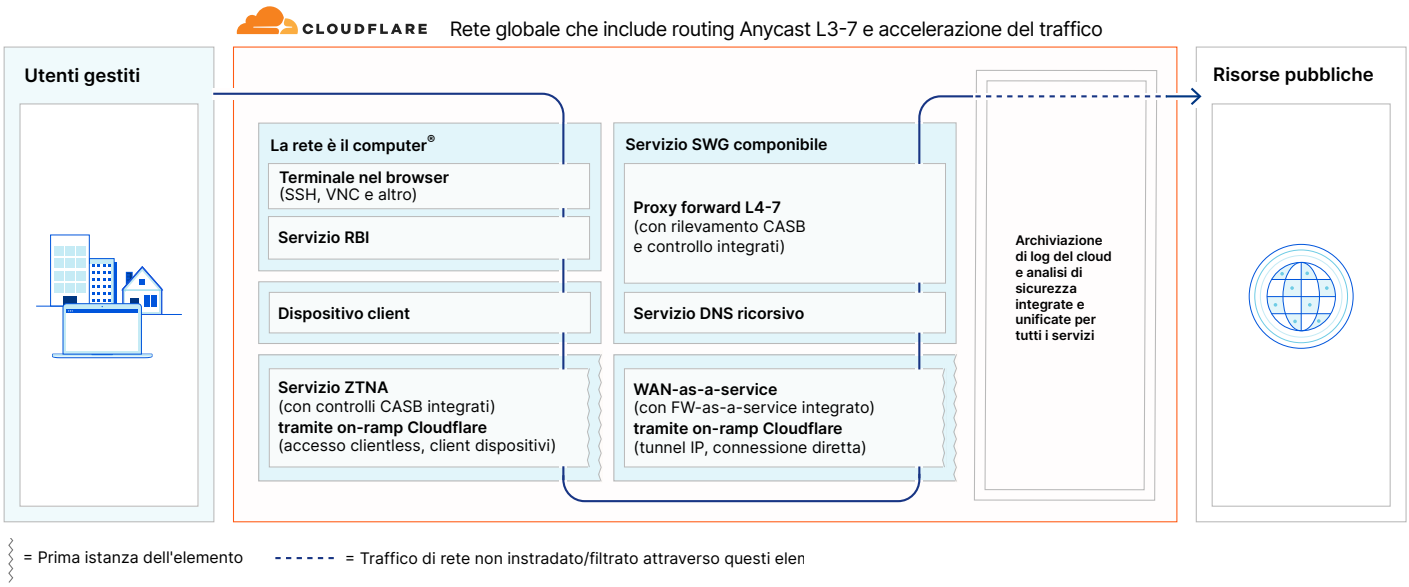
Utenti gestiti (per risorse pubbliche e private)

I team IT hanno dovuto gestire connettività e sicurezza per molti client o peggio, non potevano farlo per i dispositivi personali. Strumenti di sviluppo e VPN per l'accesso privato. Proxy HTTP/DNS per l'accesso pubblico. Virtualizzazione, DLP e MDM per una migliore protezione.

Risorse pubbliche

I team di sicurezza si sono affidati al client VPN o all'SD-WAN per instradare il traffico da utenti remoti o dell'ufficio attraverso il firewall di rete, il proxy DNS, l'ispezione SSL, il proxy HTTP e gli scanner antivirus per proteggere l'accesso alle risorse pubbliche.

Dopo Cloudflare



Utenti gestiti (per risorse pubbliche e private)

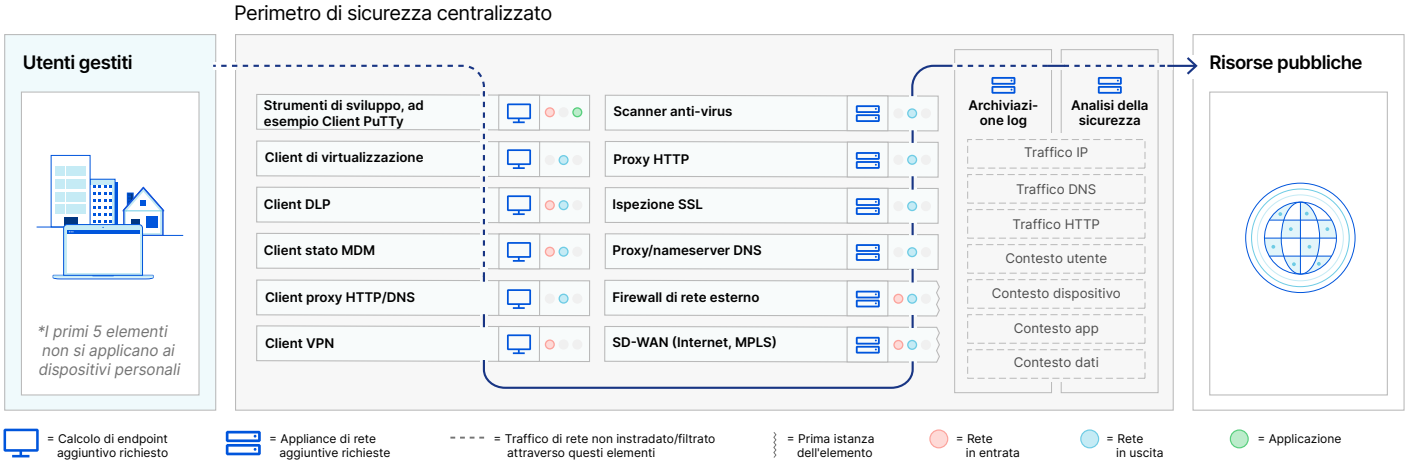
La rete rimuove molte funzioni dal computer o un client consolida molte funzioni.

Risorse pubbliche

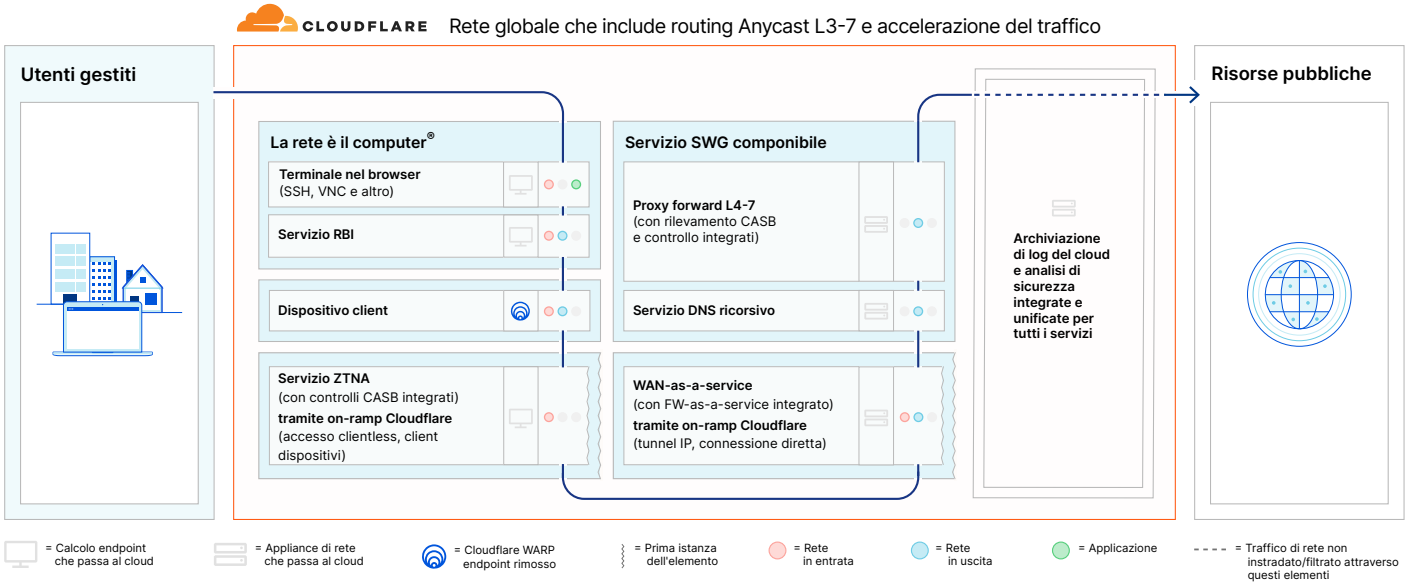
Il nostro servizio SWG componibile ispeziona il traffico in un unico passaggio prima o dopo l'adozione della nostra WAN come servizio e/o servizio ZTNA con sicurezza integrata.

1a. Semplificazione di connettività e sicurezza per le risorse pubbliche

Prima di Cloudflare



Dopo Cloudflare



Servizi nativi per il cloud

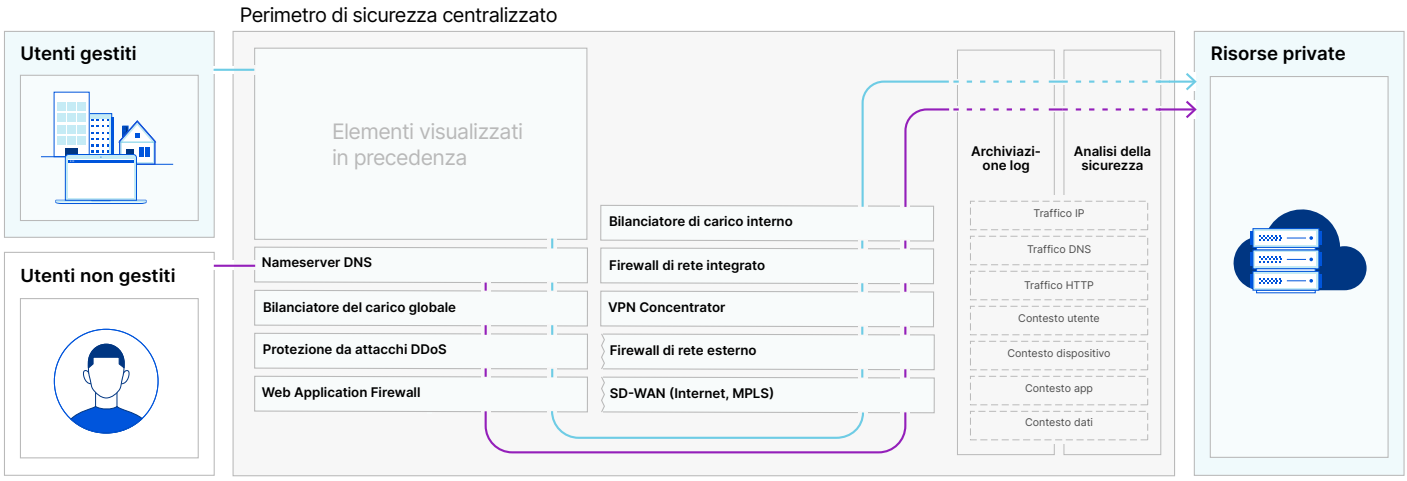
I requisiti di elaborazione degli endpoint e delle appliance di rete sono stati ridotti.

Architettura componibile

Gli stack di rete in entrata e in uscita sono unificati con lo stack dell'applicazione per la sicurezza e le prestazioni end-to-end.

2a. Semplificazione di connettività e sicurezza per le risorse private

Prima di Cloudflare



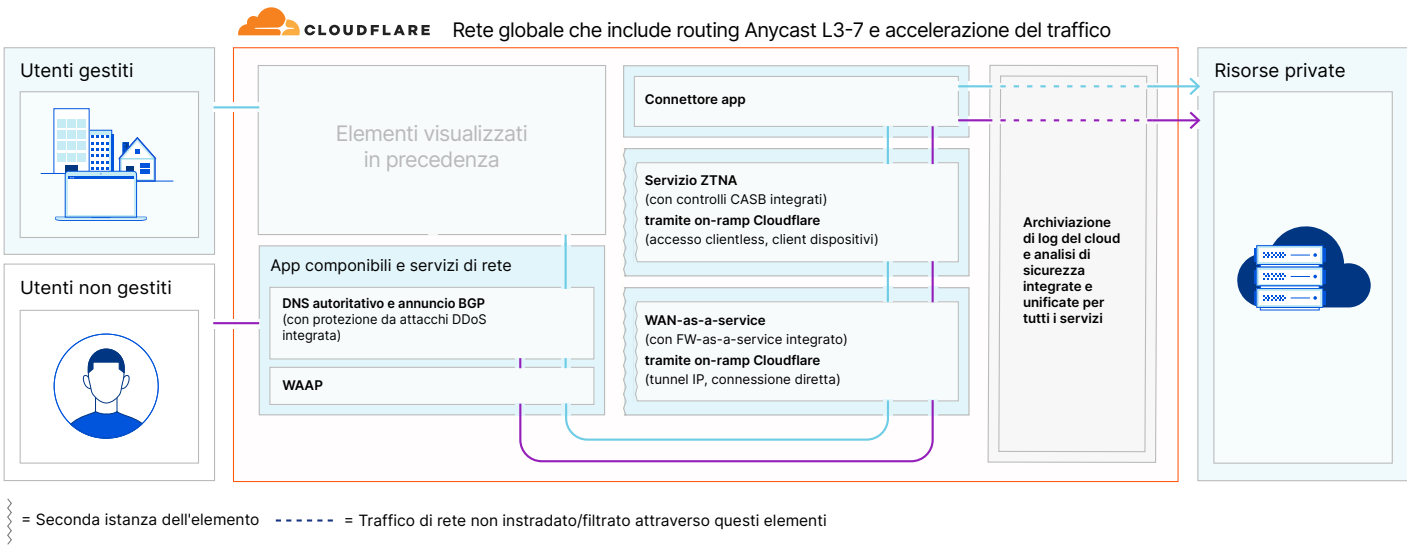
Utenti non gestiti

I team di rete hanno dovuto gestire l'annuncio pubblico della disponibilità di risorse private ad appaltatori e partner e proteggersi dagli attacchi DDoS o dallo sfruttamento da parte di utenti malintenzionati.

Risorse private (da utenti gestiti e non gestiti)

I team di sicurezza si affidavano al client VPN o alla SD-WAN per instradare il traffico dagli utenti attraverso firewall di rete, concentratori VPN e bilanciatori di carico per proteggere l'accesso alle risorse private.

Dopo Cloudflare



Utenti non gestiti

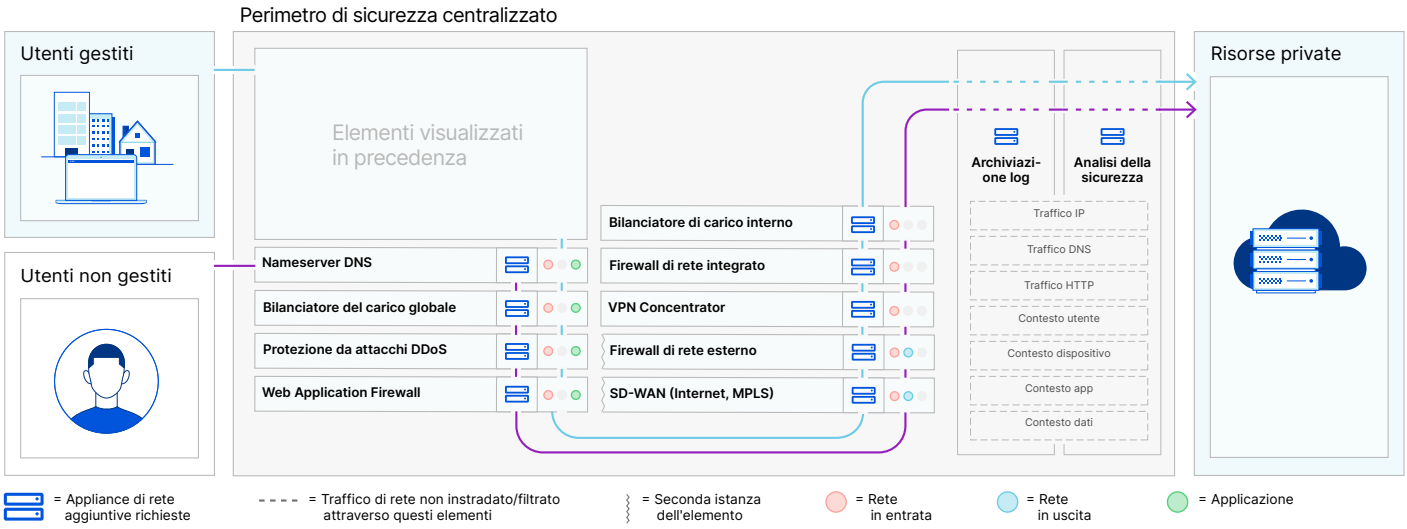
Le nostre applicazioni componibili e i servizi di rete eliminano questo onere prima o dopo l'adozione del nostro servizio ZTNA o WAN come servizio con sicurezza integrata.

Risorse private (da utenti gestiti e non gestiti)

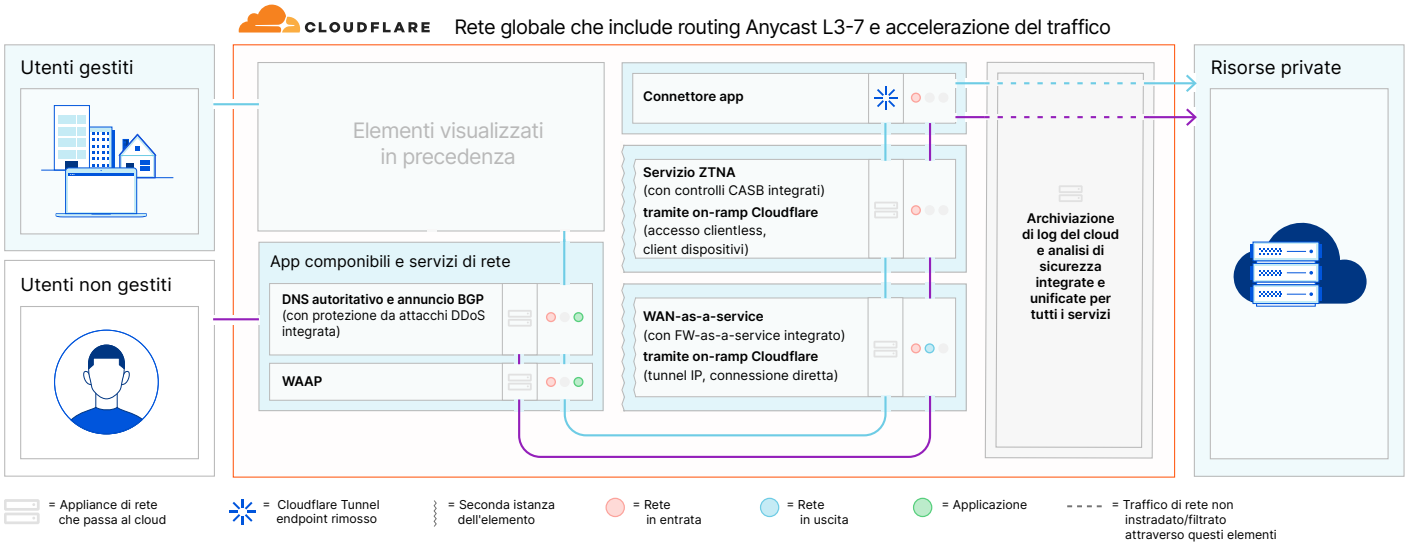
Il nostro servizio ZTNA e/o WAN-as-a-service con sicurezza integrata semplifica l'accesso utilizzando il nostro connettore per app.

2b. Semplificazione di connettività e sicurezza per le risorse private

Prima di Cloudflare



Dopo Cloudflare



Servizi nativi per il cloud

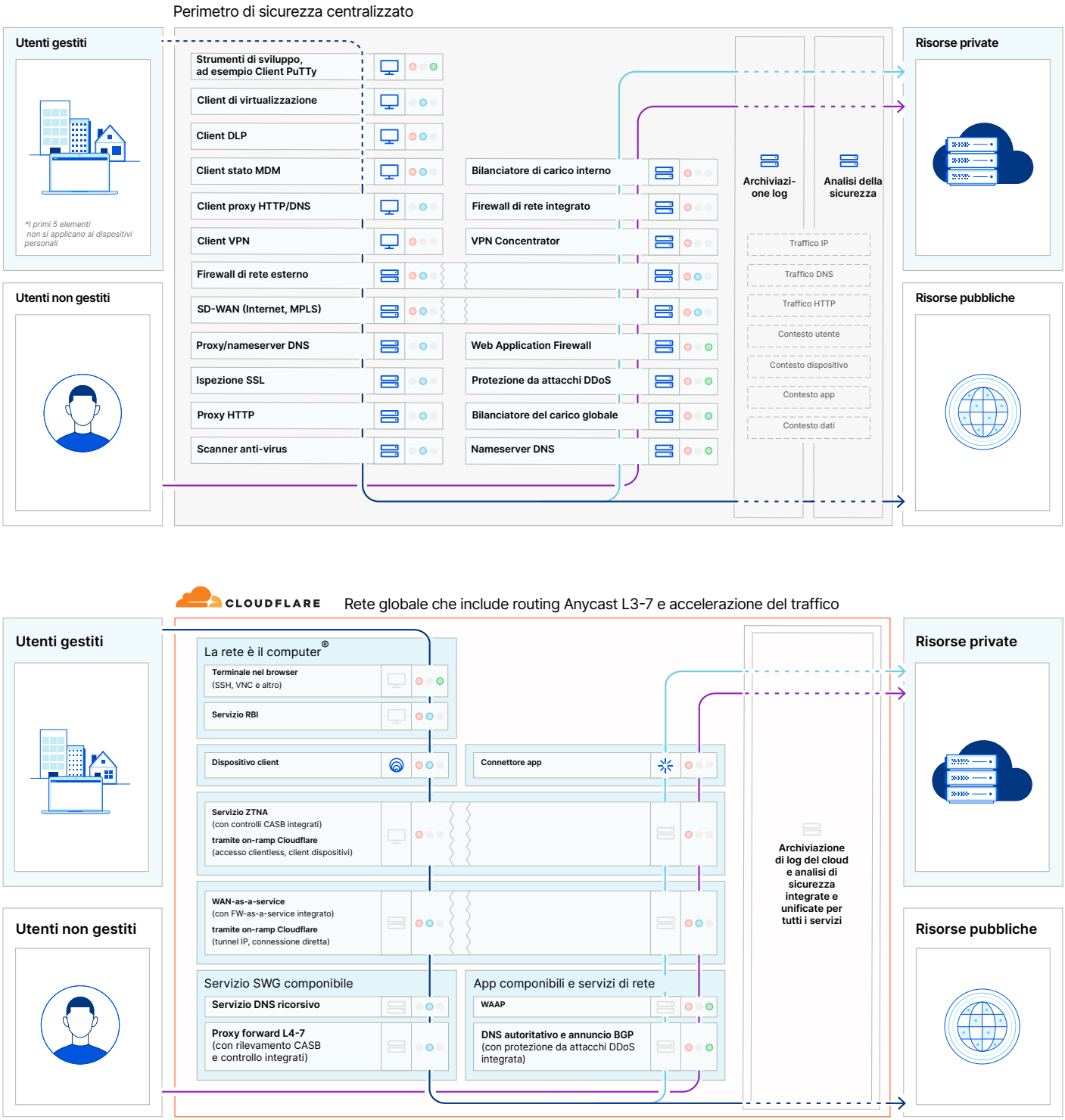
I requisiti di elaborazione degli endpoint e delle appliance di rete sono stati ridotti.

Architettura componibile

Gli stack di rete in entrata e in uscita sono unificati con lo stack dell'applicazione per la sicurezza e le prestazioni end-to-end.

Semplificazione di connettività e sicurezza per qualsiasi risorsa

Questa vista combina i diagrammi 1 e 2 insieme.



Dopo

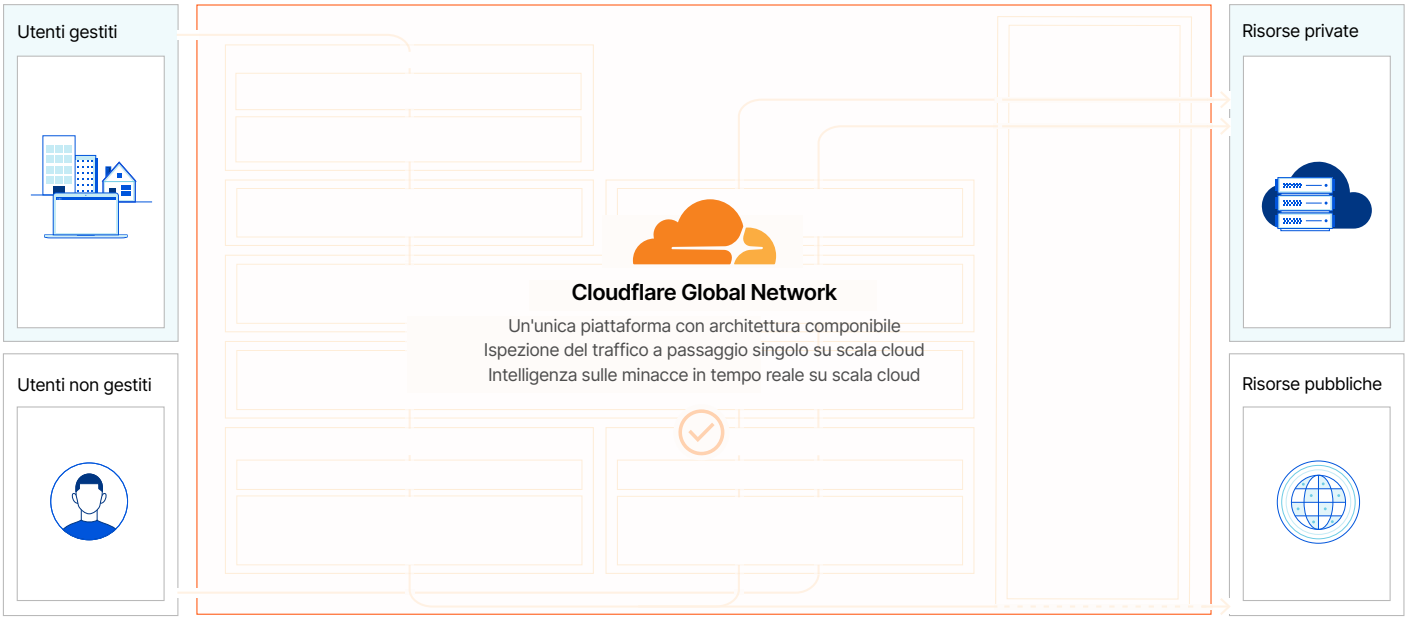
Gli elementi di connettività e sicurezza vengono riutilizzati quando qualsiasi utente accede a qualsiasi risorsa, migliorando l'efficienza e l'esperienza. Inoltre, il nostro servizio ZTNA e WAN-as-a-service comprende elementi che tradizionalmente venivano gestiti in silos tra i team IT, di rete e di sicurezza.

Una sola piattaforma per connettività e sicurezza semplificate

Perimetro di sicurezza centralizzato e rete globale Cloudflare

Prima

I team di IT, rete e sicurezza si basavano sulle soluzioni di molti fornitori, ciascuno con un'architettura diversa, in modo tale che le integrazioni point-to-point portassero a lacune di connettività e sicurezza con prestazioni limitate.



Dopo

Tutti i team sfruttano un'unica piattaforma con la stessa architettura componibile per eliminare lacune e compromessi in termini di prestazioni. La nostra intera piattaforma funziona ovunque ed è costruita per adattarsi al tuo mondo, non viceversa. Puoi distribuire qualsiasi numero di servizi, in qualsiasi sequenza, e continuerà a funzionare in modo uniforme.

Caso d'uso 1:
Accesso sicuro per le applicazioni Web

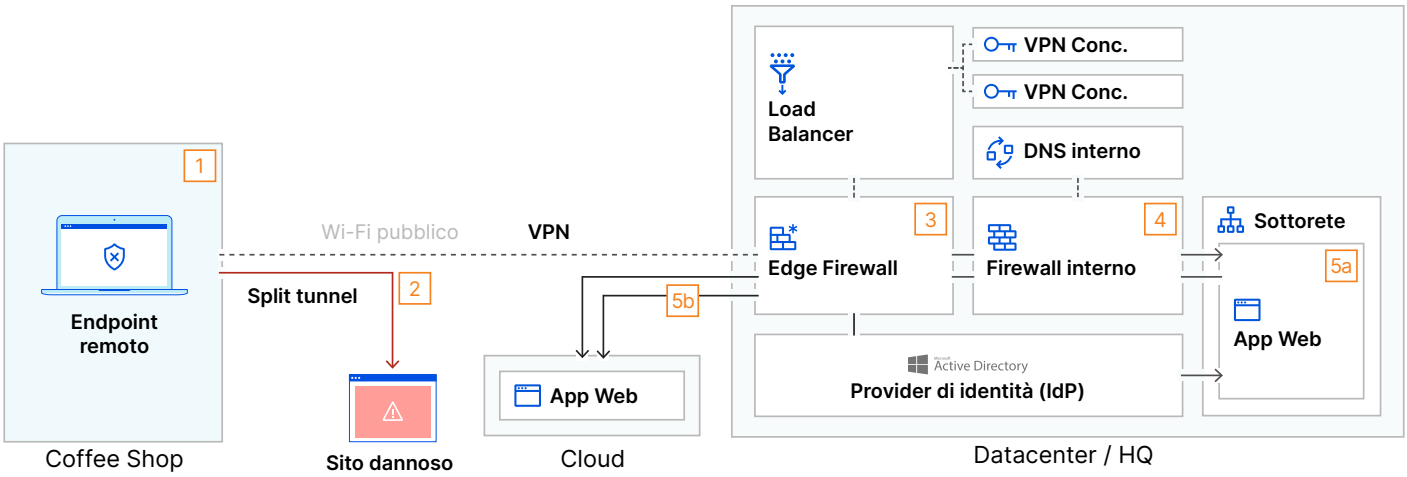
Progettazione legacy: a prima vista

Questo grafico rappresenta un metodo tradizionale per fornire l'accesso remoto alle applicazioni Web. Qui, un dipendente remoto accede alle risorse aziendali, in particolare a un'applicazione Web privata (self-hosted) e pubblica (basata su cloud).

Abbiamo incluso alcune delle misure di sicurezza più comuni che qualsiasi organizzazione ragionevole avrebbe adottato, tra cui un firewall perimetrale, un firewall interno per la segmentazione e una VPN.

Da sinistra a destra, questo scenario illustra la vita di una sessione quando un utente accede da una posizione pubblica, uno scenario su cui si baserà la grafica di progettazione successiva.

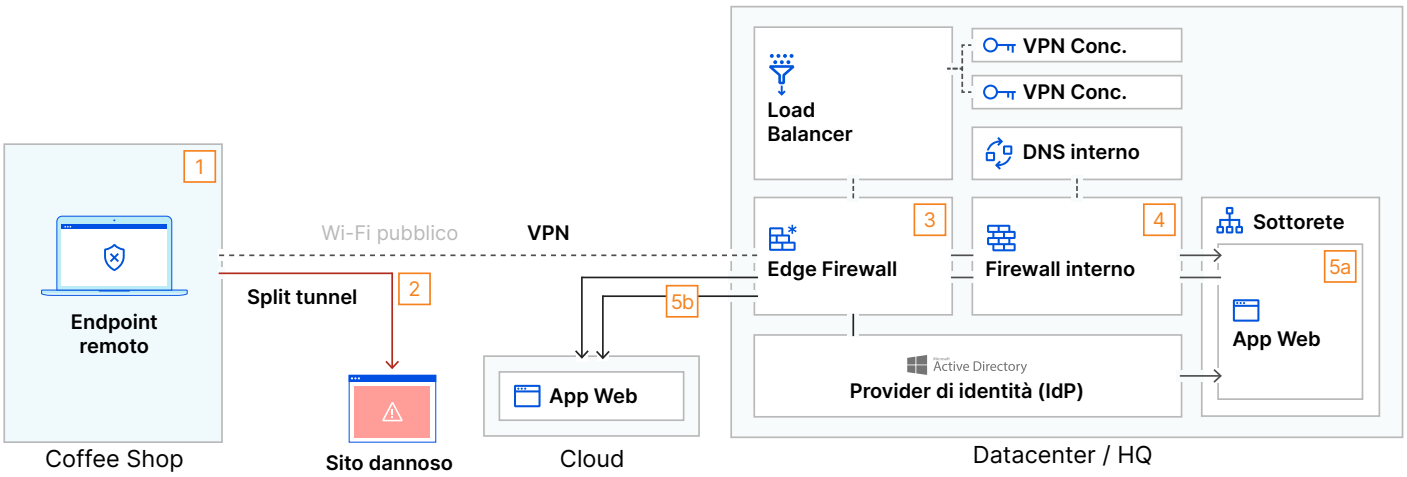
Nota: Questo grafico rappresenta solo i dispositivi, le appliance e i flussi di traffico coinvolti in questa specifica transazione di rete e non rappresenta un'istantanea completa di tutte le tecnologie che sarebbero presenti in un'architettura di rete legacy.



	Azione di rete/sicurezza
1	Un dispositivo remoto si connette alle risorse aziendali tramite Wi-Fi pubblico
2	Il dispositivo remoto raggiunge il perimetro aziendale tramite il client VPN, ma suddivide il tunnel in altro traffico
3	La VPN termina su Edge Firewall o VPN Concentrator dietro il firewall
4	I criteri del firewall garantiscono l'accesso gli utenti remoti alla sottorete con un'applicazione Web privata
5	L'utente accede all'app Web tramite un IP/URL privato **[5a]** o un URL pubblico **[5b]** dopo l'autenticazione con IDP

Progettazione legacy: difetti di sicurezza

Questo grafico aggiunge un'altra colonna alla tabella seguente evidenziando i problemi dei difetti di sicurezza associati a ogni passaggio specifico in questo scenario e che rendono un'organizzazione vulnerabile.

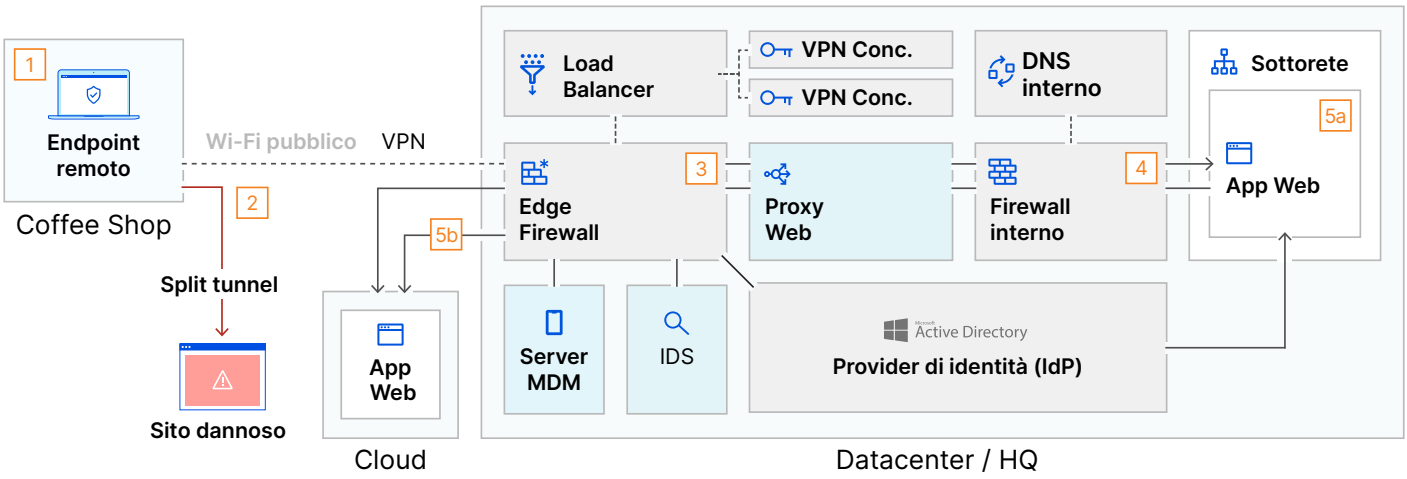


	Azione di rete/sicurezza	Soluzione legacy rilevante	Difetti nella progettazione legacy
1	Un dispositivo remoto si connette alle risorse aziendali tramite Wi-Fi pubblico	Client VPN aziendale	Un dispositivo non protetto su una rete Wi-Fi pubblica è un bersaglio per gli utenti malintenzionati
2	L'endpoint remoto raggiunge il perimetro aziendale tramite il client VPN, ma suddivide il tunnel in altro traffico	Client VPN aziendale	La sicurezza specifica della VPN non proteggerà il traffico split-tunnel
3	La VPN termina su Edge Firewall o VPN Concentrator dietro il firewall	Load Balancer Edge Firewall VPN Concentrator	Le regole FW/VPN in entrata possono esporre porte/protocolli a Internet, espandendo la potenziale superficie di attacco
4	I criteri del firewall garantiscono l'accesso gli utenti remoti alla sottorete con un'applicazione Web privata	Firewall interno	L'utente ha accesso a risorse al di fuori della propria funzione lavorativa
5	L'utente accede all'app Web tramite un IP/URL privato **[5a]** o un URL pubblico **[5b]** dopo l'autenticazione con IDP	Active Directory DNS interno (privato)	Se l'endpoint è compromesso, l'app/la rete aziendale è a rischio

Progettazione legacy: componenti aggiuntivi richiesti per la sicurezza

Per correggere i difetti di progettazione evidenziati nella pagina precedente, l'organizzazione deve ora modificare l'architettura di rete esistente. Questo grafico aggiunge un'altra colonna alla tabella seguente, che descrive in dettaglio le soluzioni tipiche per proteggere utenti e risorse.

La stratificazione di ogni componente aggiuntivo di sicurezza aggiunge complessità e costi di gestione continua all'ambiente legacy tra più fornitori probabili.



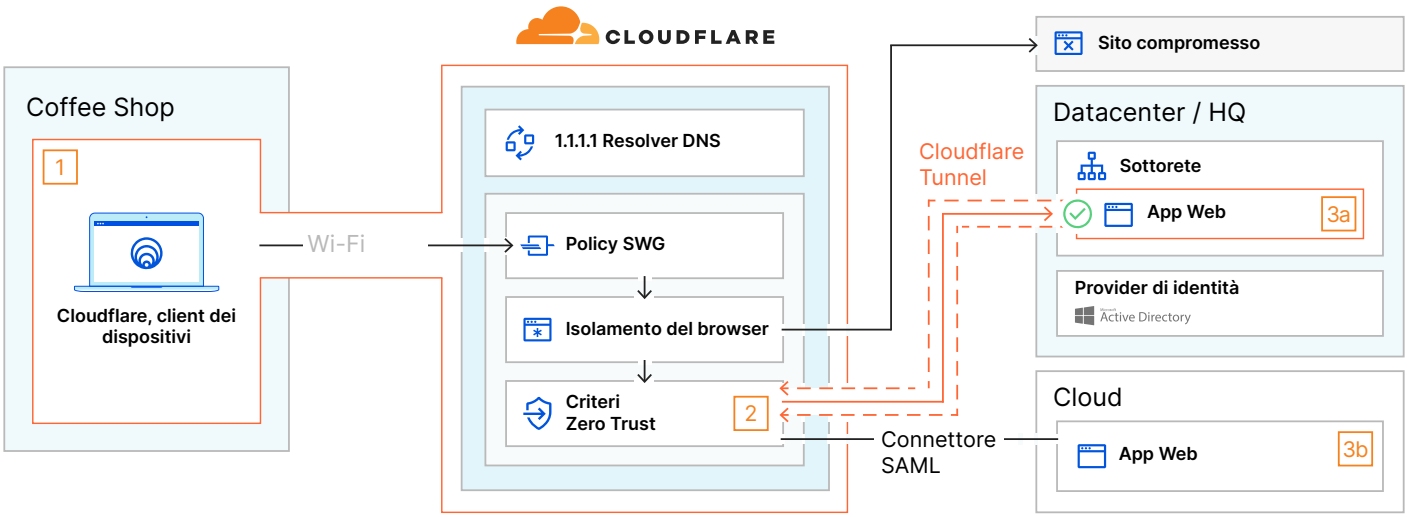
	Azione di rete/sicurezza	Soluzione legacy rilevante	Difetti nella progettazione legacy	Componente aggiuntivo richiesto per la sicurezza
1	Un dispositivo remoto si connette alle risorse aziendali tramite Wi-Fi pubblico	Client VPN aziendale	Un dispositivo non protetto su una rete Wi-Fi pubblica è un bersaglio per gli utenti malintenzionati	Endpoint Protection Platform (EPP)
2	Il dispositivo remoto raggiunge il perimetro aziendale tramite il client VPN, ma suddivide il tunnel in altro traffico	Client VPN aziendale	La sicurezza specifica della VPN non proteggerà il traffico split-tunnel	Disabilitazione dello split tunneling
3	La VPN termina su Edge Firewall o VPN Concentrator dietro il firewall	Load Balancer Edge Firewall VPN Concentrator	Le regole FW/VPN in entrata possono esporre porte/protocolli a Internet, espandendo la potenziale superficie di attacco	Intrusion Detection System (IDS)
4	I criteri del firewall garantiscono l'accesso gli utenti remoti alla sottorete con un'applicazione Web privata	Firewall interno	L'utente ha accesso a risorse al di fuori della propria funzione lavorativa	Proxy Web
5	L'utente accede all'app Web tramite un IP/URL privato **[5a]** o un URL pubblico **[5b]** dopo l'autenticazione con IDP	Active Directory DNS interno (privato)	Se l'endpoint è compromesso, l'app/la rete aziendale è a rischio	Server Mobile Device Mgmt (MDM)

Progetto Cloudflare One

Il grafico seguente evidenzia come un'organizzazione può adottare un approccio più semplice ed efficiente per proteggere l'accesso alle applicazioni implementando Cloudflare One.

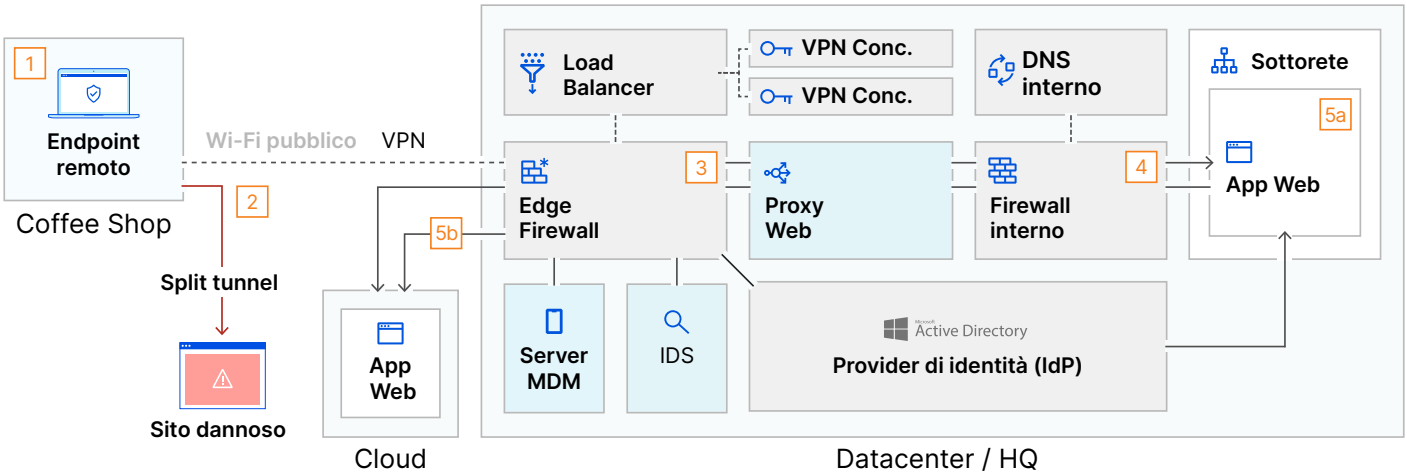
Qui, gran parte dell'architettura di rete legacy mostrata in precedenza viene scaricata su Cloudflare e molti dei difetti di progettazione esistenti vengono corretti senza la necessità di soluzioni aggiuntive.

Con Cloudflare One, il traffico tra l'utente remoto e le risorse dell'organizzazione scorre lungo la rete globale di Cloudflare con ispezione a passaggio singolo. Tutti i servizi mostrati di seguito vengono eseguiti in tutti i datacenter di Cloudflare, situati in oltre 250 città in oltre 100 paesi.

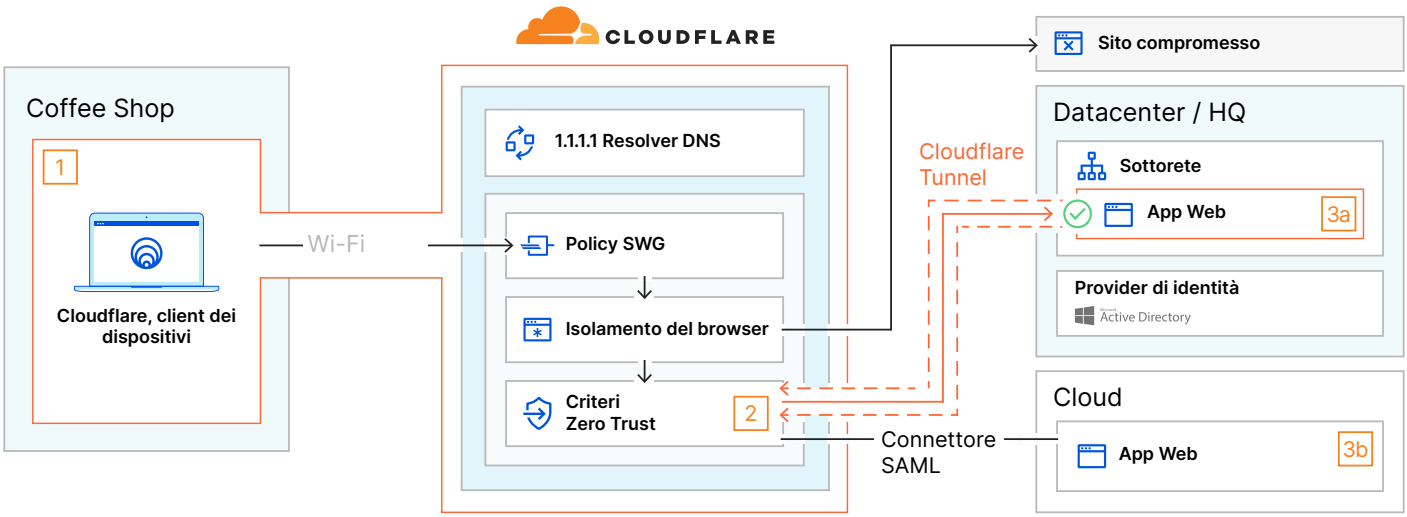


	Azione di rete/sicurezza	Elementi rilevanti di Cloudflare One	Correzione dei difetti di progettazione
1	Un dispositivo remoto si connette alle risorse aziendali e a Internet tramite Cloudflare	**Client dei dispositivi Cloudflare** **Criteri di Secure Web Gateway** **Browser Isolation**	Il client locale Secure Web Gateway consente a Cloudflare One di filtrare il traffico DNS/HTTP/di rete verso il dispositivo dell'utente tramite i criteri del gateway Browser Isolation assorbe/isola l'impatto degli attacchi malware riusciti dai siti Web
2	L'utente viene sottoposto a controlli IDP e di stato del dispositivo in Cloudflare	**Criteri Zero Trust**	I criteri Zero Trust eseguono il controllo dello stato del dispositivo prima di consentire l'accesso, riducendo il rischio di compromissione dei dispositivi I criteri Zero Trust autenticano l'utente sulla risorsa anziché sulla rete sottostante, prevenendo il movimento laterale
3	Accesso [privato | pubblico] all'app Web direttamente tramite [Cloudflare Tunnel | SAML Connector]	**Cloudflare Tunnel** **1.1.1.1 Resolver DNS**	Cloudflare Tunnel gestisce in modo sicuro una connessione all'applicazione Web ed elimina l'uso di regole FW esplicite

Progettazione legacy: componenti aggiuntivi richiesti per la sicurezza



Progetto Cloudflare One



Progettazione legacy: componenti aggiuntivi richiesti per la sicurezza

	Azione di rete/sicurezza	Soluzione legacy rilevante	Difetti nella progettazione legacy	Componente aggiuntivo richiesto per la sicurezza
1	Un dispositivo remoto si connette alle risorse aziendali tramite Wi-Fi pubblico	Client VPN aziendale	Un dispositivo non protetto su una rete Wi-Fi pubblica è un bersaglio per gli utenti malintenzionati	Endpoint Protection Platform (EPP)
2	Il dispositivo remoto raggiunge il perimetro aziendale tramite il client VPN, ma suddivide il tunnel in altro traffico	Client VPN aziendale	La sicurezza specifica della VPN non proteggerà il traffico split-tunnel	Disabilitazione dello split tunneling
3	La VPN termina su Edge Firewall o VPN Concentrator dietro il firewall	Load Balancer Edge Firewall VPN Concentrator	Le regole FW/VPN in entrata possono esporre porte/protocolli a Internet, espandendo la potenziale superficie di attacco	Intrusion Detection System (IDS)
4	I criteri del firewall garantiscono l'accesso gli utenti remoti alla sottorete con un'applicazione Web privata	Firewall interno	L'utente ha accesso a risorse al di fuori della propria funzione lavorativa	Proxy Web
5	L'utente accede all'app Web tramite un IP/URL privato **[5a]** o un URL pubblico **[5b]** dopo l'autenticazione con IDP	Active Directory DNS interno (privato)	Se l'endpoint è compromesso, l'app/la rete aziendale è a rischio	Server Mobile Device Mgmt (MDM)

Progetto Cloudflare One

	Azione di rete/sicurezza	Elementi rilevanti di Cloudflare One	Correzione dei difetti di progettazione
1	Un dispositivo remoto si connette alle risorse aziendali e a Internet tramite Cloudflare	**Client dei dispositivi Cloudflare** **Criteri di Secure Web Gateway** **Browser Isolation**	Il client locale Secure Web Gateway consente a Cloudflare One di filtrare il traffico DNS/HTTP/di rete verso il dispositivo dell'utente tramite i criteri del gateway Browser Isolation assorbe/isola l'impatto degli attacchi malware riusciti dai siti Web
2	L'utente viene sottoposto a controlli IDP e di stato del dispositivo in Cloudflare	**Criteri Zero Trust**	I criteri Zero Trust eseguono il controllo dello stato del dispositivo prima di consentire l'accesso, riducendo il rischio di compromissione dei dispositivi I criteri Zero Trust autenticano l'utente sulla risorsa anziché sulla rete sottostante, prevenendo il movimento laterale
3	Accesso [privato | pubblico] all'app Web direttamente tramite [Cloudflare Tunnel | SAML Connector]	**Cloudflare Tunnel** **1.1.1.1 Resolver DNS**	Cloudflare Tunnel gestisce in modo sicuro una connessione all'applicazione Web ed elimina l'uso di regole FW esplicite

Caso d'uso 2: DNS Filtering

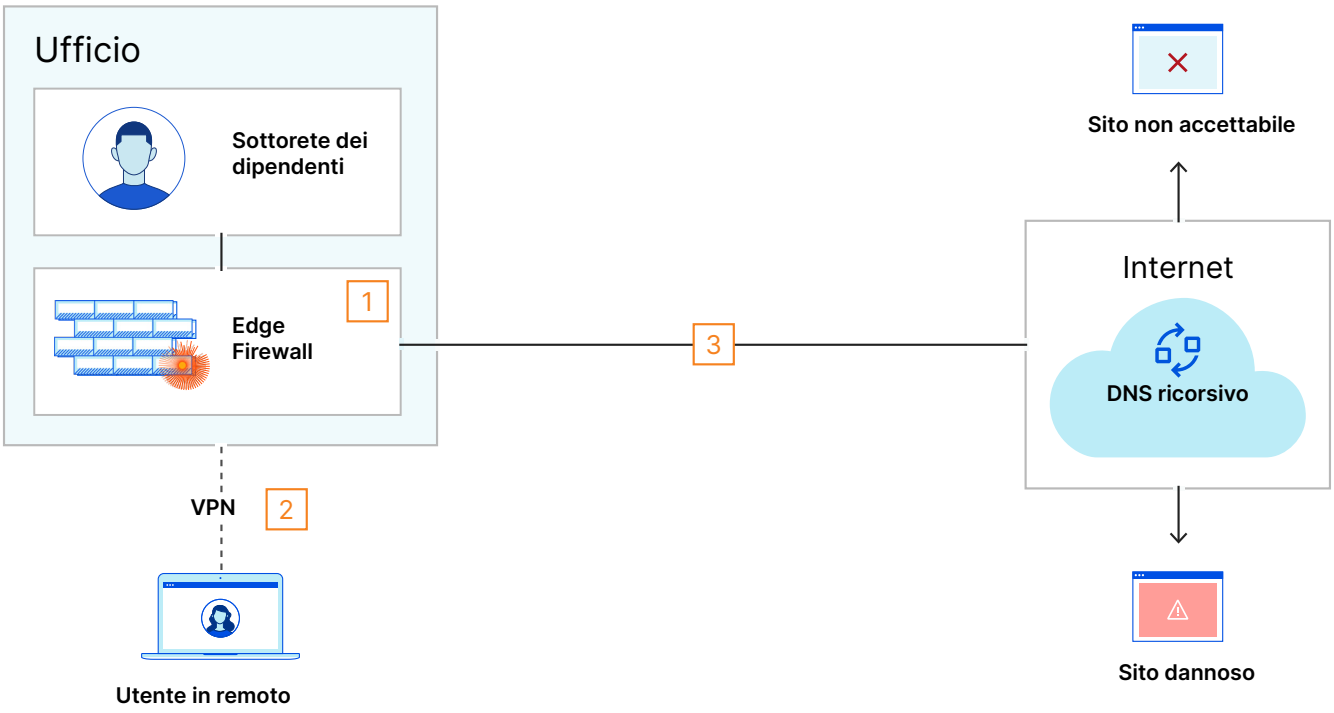
Progettazione legacy: a prima vista

Questo grafico rappresenta il modo in cui le organizzazioni implementano il filtraggio DNS per i dipendenti in loco e remoti in un ambiente legacy.

In genere, il filtro DNS per le organizzazioni viene realizzato tramite funzionalità integrate di soluzioni locali come un firewall. Gli utenti remoti inviano le richieste attraverso questo firewall effettuando prima il backhaul del traffico attraverso una VPN full-tunnel.

Per risolvere i siti Web, l'organizzazione invia le sue query DNS a un DNS ricorsivo (come 8.8.8.8 di Google).

Nota: proprio come con altre sezioni di questa guida, questo ambiente legacy non rappresenta tutte le tecnologie all'interno di un ufficio, ma solo quelle coinvolte in questo caso d'uso specifico.



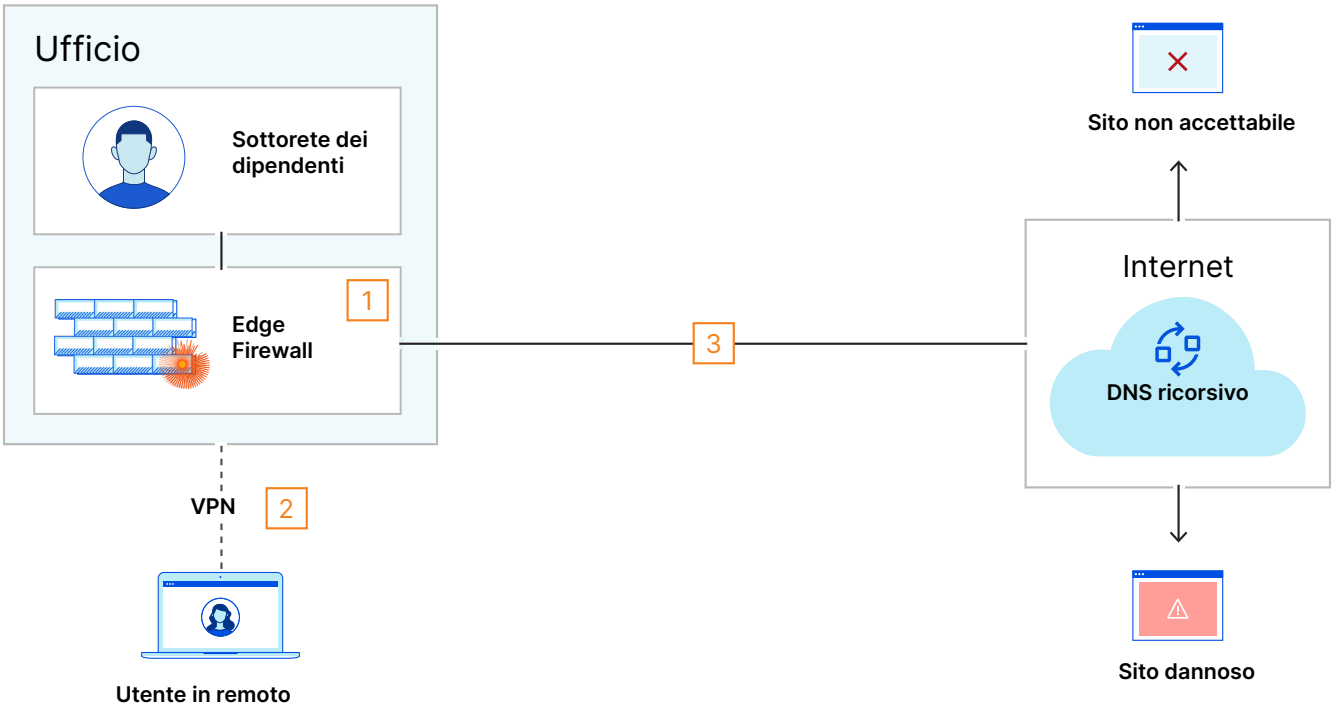
	Evento correlato al DNS
1	Un utente in loco fa filtrare il contenuto delle proprie richieste DNS per motivi di sicurezza dalla funzionalità integrata in Edge Firewall
2	Un utente remoto ha le proprie richieste DNS filtrate dopo la connessione alla VPN full tunnel dell'organizzazione
3	Le richieste DNS in uscita vengono trasmesse in chiaro.

Progettazione legacy: difetti operativi

Il grafico successivo aggiunge una colonna alla tabella sottostante che articola le sfide associate a questo design tradizionale.

Il problema più urgente è che fare affidamento sull'hardware locale per eseguire il filtro DNS su larga scala finirà per creare colli di bottiglia per tutti gli utenti, specialmente quando quell'hardware è responsabile anche di altri servizi critici (come la terminazione della VPN dell'utente remoto).

Inoltre, l'invio di query DNS senza crittografia (che si verifica per impostazione predefinita) crea un nuovo vettore di attacco con rischio sconosciuto.



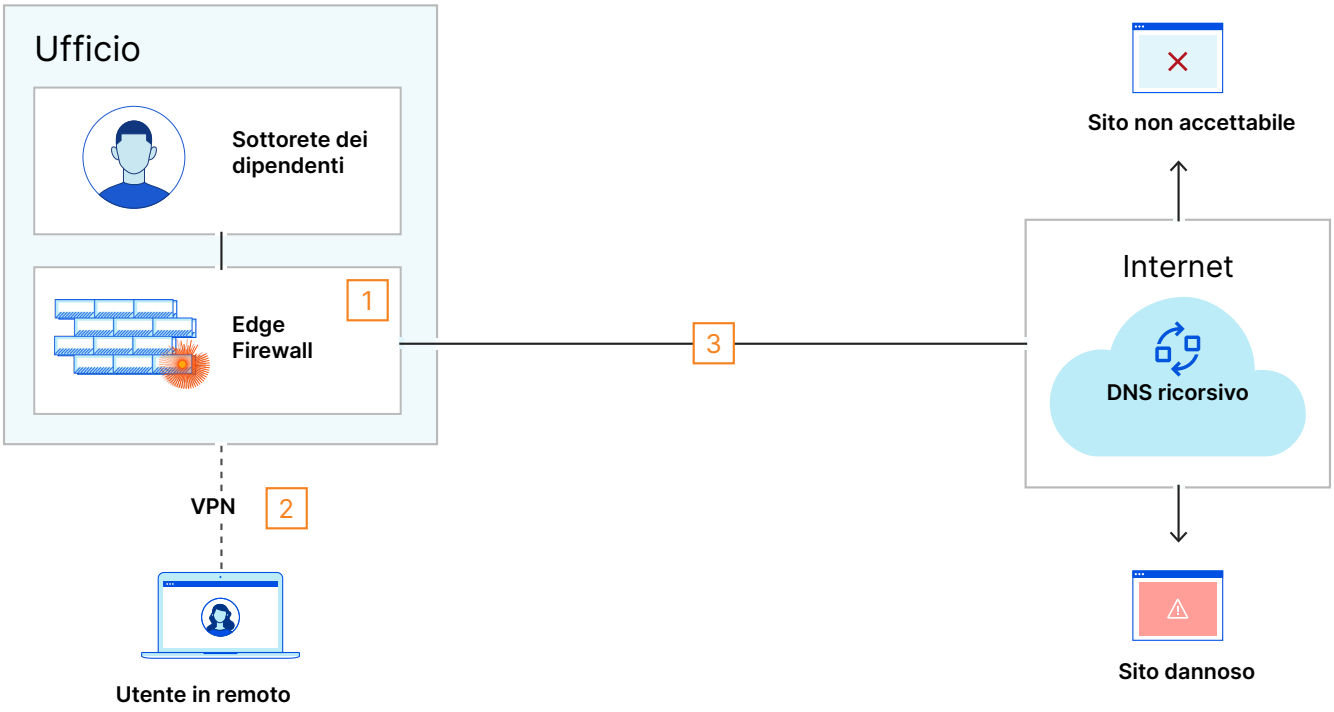
	Evento correlato al DNS	Elementi rilevanti	Difetto di progettazione
1	Un utente in loco fa filtrare il contenuto delle proprie richieste DNS per motivi di sicurezza dalla funzionalità integrata in Edge Firewall	Edge Firewall	Affidarsi all'Edge FW per un numero di operazioni essenziali eccessivo può peggiorare le prestazioni nell'intera organizzazione
2	Un utente remoto ha le proprie richieste DNS filtrate dopo la connessione alla VPN full tunnel dell'organizzazione	VPN Concentrator Edge Firewall	Una VPN full-tunnel crea una "doppia tassazione" dei pacchetti Internet, che può creare un collo di bottiglia delle prestazioni per il traffico in tunnel dell'intera organizzazione
3	Le richieste DNS in uscita vengono trasmesse in chiaro.	UDP53	La porta 53 del DNS su UDP non è crittografata e quindi non è privata. Chiunque la veda può ricostruire il comportamento degli utenti sul Web

Progettazione legacy: modifiche necessarie alla rete

Per correggere i difetti di progettazione evidenziati nella pagina precedente, l'organizzazione deve ora modificare l'architettura di rete esistente. Questo grafico aggiunge un'altra colonna alla tabella sottostante, evidenziando soluzioni comuni con i propri inconvenienti.

In questo caso, l'acquisto di nuovo hardware per gestire più utenti o aumentare il consumo di larghezza di banda comporterà nel tempo maggiori spese di capitale e operative.

Le organizzazioni che tentano di scalare da sole questo approccio spesso incontrano notevoli difficoltà di crescita e, in effetti, molte organizzazioni evitano completamente il filtro DNS a causa di questi problemi operativi.



	Evento correlato al DNS	Elementi rilevanti	Difetto di progettazione	Soluzione non Cloudflare
1	Un utente in loco fa filtrare il contenuto delle proprie richieste DNS per motivi di sicurezza dalla funzionalità integrata in Edge Firewall	Edge Firewall	Affidarsi all'Edge FW per un numero di operazioni essenziali eccessivo può peggiorare le prestazioni nell'intera organizzazione	Filtro DNS discreto
2	Un utente remoto ha le proprie richieste DNS filtrate dopo la connessione alla VPN full tunnel dell'organizzazione	VPN Concentrator Edge Firewall	Una VPN full-tunnel crea una "doppia tassazione" dei pacchetti Internet, che può creare un collo di bottiglia delle prestazioni per il traffico in tunnel dell'intera organizzazione	Aumento della larghezza di banda dell'ISP Upgrade dell'hardware Abilitazione dello split tunneling*
3	Le richieste DNS in uscita vengono trasmesse in chiaro.	UDP53	La porta 53 del DNS su UDP non è crittografata e quindi non è privata. Chiunque la veda può ricostruire il comportamento degli utenti sul Web	DNS su TLS/HTTPS

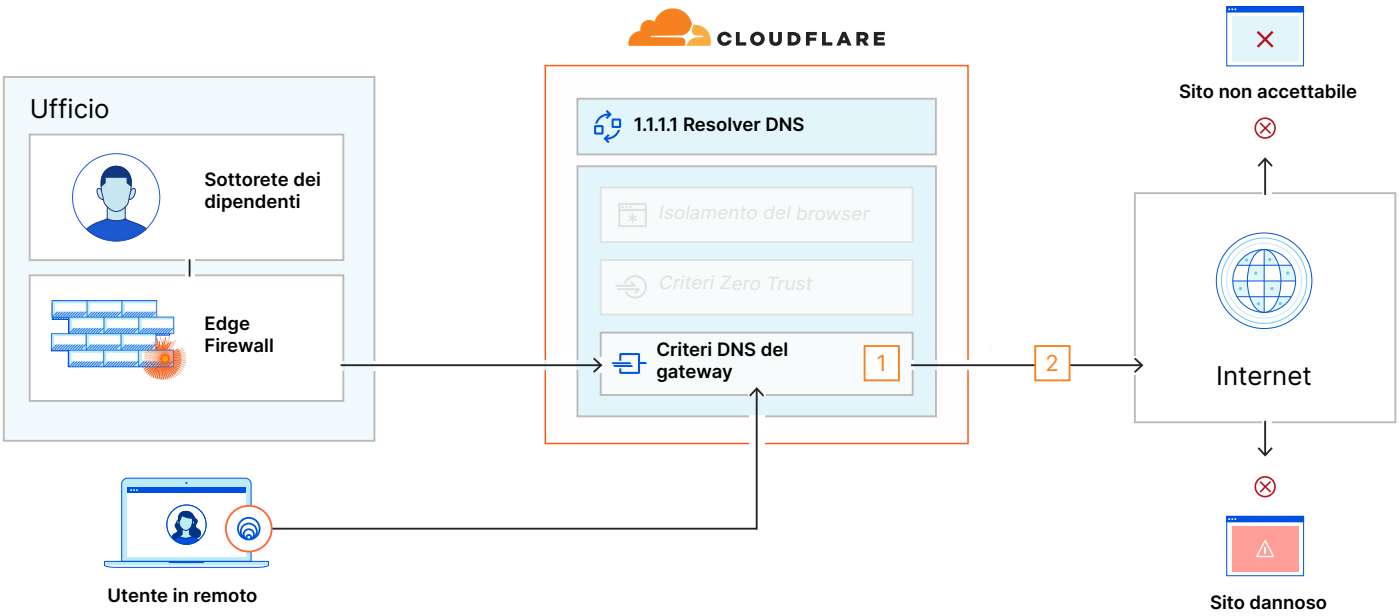
Progetto Cloudflare One

Le organizzazioni che adottano Cloudflare One indirizzano il loro traffico verso la rete globale di Cloudflare e possono eseguire il filtro DNS per l'intera forza lavoro senza preoccuparsi dei limiti operativi del loro hardware locale.

Il DNS filtrato di Cloudflare è facile da implementare sia per gli utenti in locale che per quelli in remoto:

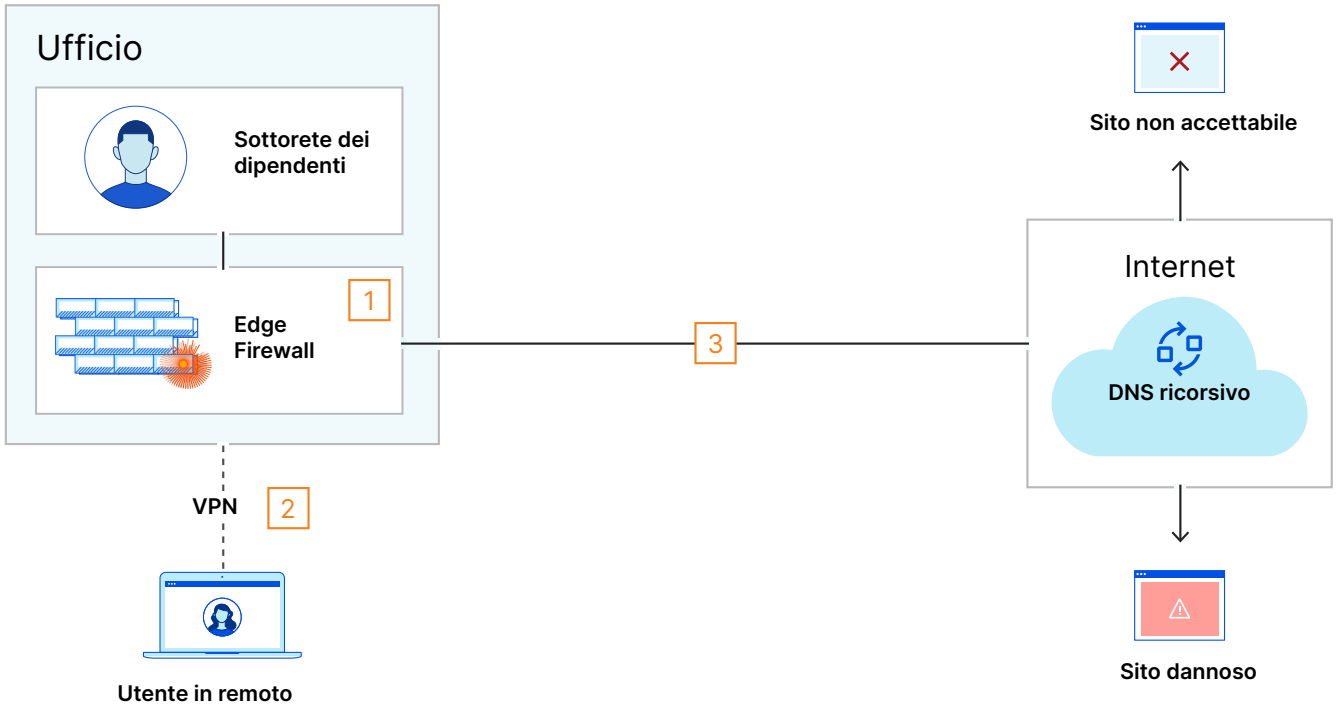
- Il traffico degli utenti in ufficio viene inviato a Cloudflare in base all'IP di uscita dal firewall perimetrale
- Il traffico degli utenti remoti viene inviato a Cloudflare dal nostro client del dispositivo

Inoltre, il resolver DNS 1.1.1.1 di Cloudflare supporta DNS su TLS/HTTPs, che risolve il problema di sicurezza dettagliato nell'ambiente legacy.

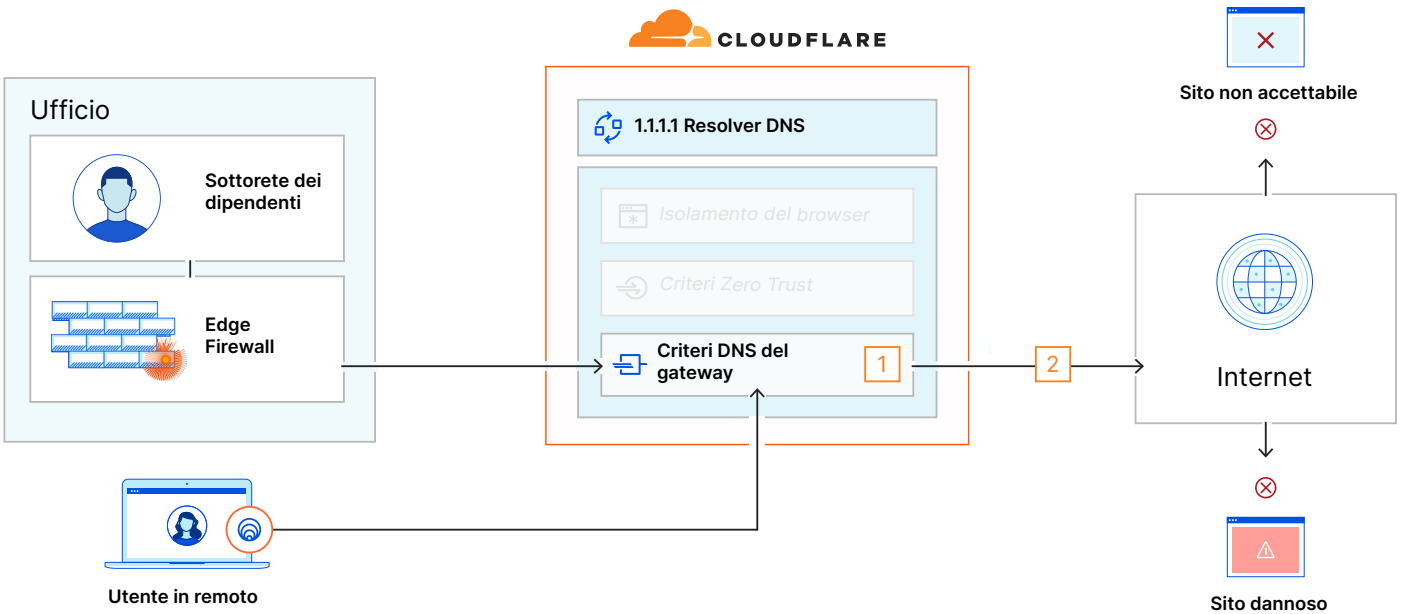


	Evento correlato al DNS	Elementi rilevanti di Cloudflare One	Correzione dei difetti di progettazione
1	Sia gli utenti in loco che quelli remoti hanno il contenuto delle loro richieste DNS filtrato da Cloudflare	**Secure Web Gateway**	**Gateway** I criteri DNS scaricano il filtro DNS dall'hardware locale (o lo forniscono per la prima volta)
2	Le richieste DNS dell'organizzazione vengono crittografate prima di essere inviate.	**1.1.1.1 Resolver DNS**	Il resolver DNS **1.1.1.1 di Cloudflare** supporta DNS su TLS/HTTPs, crittografando le richieste DNS e ostacolando la ricognizione ostile

Progettazione legacy



Progetto Cloudflare One



Progettazione legacy

	Evento correlato al DNS	Elementi rilevanti	Difetto di progettazione	Soluzione non Cloudflare
1	Un utente in loco fa filtrare il contenuto delle proprie richieste DNS per motivi di sicurezza dalla funzionalità integrata in Edge Firewall	Edge Firewall	Affidarsi all'Edge FW per un numero di operazioni essenziali eccessivo può peggiorare le prestazioni nell'intera organizzazione	Filtro DNS discreto
2	Un utente remoto ha le proprie richieste DNS filtrate dopo la connessione alla VPN full tunnel dell'organizzazione	VPN Concentrator Edge Firewall	Una VPN full-tunnel crea una "doppia tassazione" dei pacchetti Internet, che può creare un collo di bottiglia delle prestazioni per il traffico in tunnel dell'intera organizzazione	Aumento della larghezza di banda dell'ISP Upgrade dell'hardware Abilitazione dello split tunneling*
3	Le richieste DNS in uscita vengono trasmesse in chiaro.	UDP53	La porta 53 del DNS su UDP non è crittografata e quindi non è privata. Chiunque la veda può ricostruire il comportamento degli utenti sul Web	DNS su TLS/HTTPS

Progetto Cloudflare One

	Evento correlato al DNS	Elementi rilevanti di Cloudflare One	Correzione dei difetti di progettazione
1	Sia gli utenti in loco che quelli remoti hanno il contenuto delle loro richieste DNS filtrato da Cloudflare	**Secure Web Gateway**	**Gateway** I criteri DNS scaricano il filtro DNS dall'hardware locale (o lo forniscono per la prima volta)
2	Le richieste DNS dell'organizzazione vengono crittografate prima di essere inviate.	**1.1.1.1 Resolver DNS**	Il resolver DNS **1.1.1.1 di Cloudflare** supporta DNS su TLS/HTTPs, crittografando le richieste DNS e ostacolando la ricognizione ostile