Whitepaper AWS

Opzioni di connettività di Amazon Virtual Private Cloud

Opzioni di connettività di Amazon Virtual Private Cloud: Whitepaper AWS

Table of Contents

Opzioni di connettività di Amazon Virtual Private Cloud

Data di pubblicazione: 5 aprile 2023 () Revisioni del documento

Sintesi

Amazon Virtual Private Cloud (Amazon VPC) consente ai clienti di fornire una sezione privata e isolata del cloud Amazon Web Services (AWS) in cui possono avviare risorse AWS in una rete virtuale utilizzando intervalli di indirizzi IP definiti dal cliente. Amazon VPC offre ai clienti diverse opzioni per connettere le loro reti virtuali AWS con altre reti remote. Questo documento descrive diverse opzioni di connettività di rete comuni disponibili per i nostri clienti. Queste includono opzioni di connettività per l'integrazione di reti di clienti remoti con Amazon VPC e il collegamento di più Amazon VPC in una rete virtuale contigua.

Questo white paper è destinato agli architetti e agli ingegneri di rete aziendali o agli amministratori di Amazon VPC che desiderano esaminare le opzioni di connettività disponibili. Fornisce una panoramica delle varie opzioni per facilitare le discussioni sulla connettività di rete, nonché riferimenti a documentazione e risorse aggiuntive con informazioni o esempi più dettagliati.

Introduzione

Amazon VPC offre diverse opzioni di connettività di rete da utilizzare, a seconda dei progetti e dei requisiti di rete attuali. Queste opzioni di connettività includono l'utilizzo di Internet o di una AWS Direct Connect connessione come dorsale di rete e l'interruzione della connessione in AWS o negli endpoint di rete gestiti dall'utente. Inoltre, con AWS, puoi scegliere come distribuire il routing di rete tra Amazon VPC e le tue reti, sfruttando i servizi AWS o apparecchiature e percorsi di rete gestiti dagli utenti. Questo white paper prende in considerazione le seguenti opzioni con una panoramica e un confronto di alto livello tra ciascuna di esse:

- Opzioni di connettività da rete ad Amazon VPC
  - VPN da sito a sito AWS: descrive la creazione di una connessione VPN IPSec gestita dalle apparecchiature di rete su una rete remota ad Amazon VPC.
  - AWS Transit Gateway + AWS Site-to-Site VPN: descrive la creazione di una connessione VPN IPSec gestita dalle apparecchiature di rete su una rete remota a un hub di rete regionale per Amazon VPC, utilizzando. AWS Transit Gateway
  - AWS Direct Connect- Descrive la creazione di una connessione logica privata dalla rete remota ad Amazon VPC, utilizzando. AWS Direct Connect
  - AWS Direct Connect + AWS Transit Gateway— Descrive la creazione di una connessione logica privata dalla rete remota a un hub di rete regionale per Amazon VPC, utilizzando AWS Direct Connect eAWS Transit Gateway.
  - AWS Direct Connect+ AWS Site-to-Site VPN: descrive la creazione di una connessione privata e crittografata dalla rete remota ad Amazon VPC, utilizzando una VPN da sito a sito AWS. AWS Direct Connect
  - AWS Direct Connect + AWS Transit Gateway + VPN da sito a sito AWS— Descrive la creazione di una connessione privata e crittografata dalla rete remota a un hub di rete regionale per Amazon VPC, utilizzando AWS Direct Connect eAWS Transit Gateway.
  - AWS VPN CloudHub— Descrive la creazione di un hub-and-spoke modello per connettere le filiali remote.
  - Software VPN— Descrive la creazione di una connessione VPN dalle apparecchiature su una rete remota a un'appliance VPN software gestita dall'utente in esecuzione all'interno di un Amazon VPC.

  - AWS Transit Gateway + Soluzioni SD-WAN- Descrive l'integrazione di soluzioni SD-WAN (Software-Defined Wide Area Network) per interconnettere diverse postazioni remote a un hub di rete regionale per Amazon VPC, utilizzando la AWS dorsale o Internet come rete di transito.
- Opzioni di connettività da Amazon VPC ad Amazon VPC
  - Peering VPC— Descrive la connessione di Amazon VPC all'interno e tra regioni diverse utilizzando la funzionalità di peering Amazon VPC.
  - AWS Transit Gateway— Descrive la connessione di Amazon VPC all'interno e tra regioni utilizzando AWS Transit Gateway un hub-and-spoke modello.
  - AWS PrivateLink— Descrive la connessione di Amazon VPC con endpoint di interfaccia VPC e servizi endpoint VPC.
  - Software VPN— Descrive la connessione di Amazon VPC utilizzando connessioni VPN stabilite tra appliance VPN software gestite dall'utente in esecuzione all'interno di ogni Amazon VPC.
  - Software da VPN a VPN da sito a sito AWS— Descrive la connessione di Amazon VPC con una connessione VPN stabilita tra un'appliance VPN software gestita dall'utente in un Amazon VPC e una VPN da sito a AWS sito collegata all'altro Amazon VPC.
- Accesso remoto del software alle opzioni di connettività Amazon VPC
  - AWS Client VPN— Descrive la connessione dell'accesso remoto del software ad Amazon VPC, sfruttando AWS Client VPN.
  - Client software VPN— Descrive la connessione dell'accesso remoto del software ad Amazon VPC, sfruttando appliance VPN software gestite dall'utente.
- VPC di transito- Descrive la creazione di una rete di transito globale su AWS utilizzando una VPN software in combinazione con una VPN gestita da AWS.
- WAN nel cloud AWS- Descrive la creazione di una rete WAN (Wide Area Network) gestita per creare, gestire e monitorare facilmente le interconnessioni globali tra le risorse in Amazon VPC, datacenter e filiali remote.

Opzioni di connettività da rete ad Amazon VPC

Questa sezione fornisce modelli di progettazione per connettere reti remote con il tuo ambiente Amazon VPC. Queste opzioni sono utili per integrare le risorse AWS con i servizi locali esistenti (ad esempio monitoraggio, autenticazione, sicurezza, dati o altri sistemi) estendendo le reti interne nel cloud AWS. Questa estensione di rete consente inoltre agli utenti interni di connettersi senza problemi alle risorse ospitate su AWS proprio come qualsiasi altra risorsa rivolta internamente.

La connettività VPC alle reti di clienti remoti si ottiene al meglio quando si utilizzano intervalli IP non sovrapposti per ogni rete connessa. Ad esempio, se desideri connettere uno o più VPC alla tua rete aziendale, assicurati che siano configurati con intervalli CIDR (Classless Inter-Domain Routing) unici. Consigliamo di allocare un singolo blocco CIDR contiguo e non sovrapposto da utilizzare da ogni VPC. Per ulteriori informazioni sul routing e sui vincoli di Amazon VPC, consulta le domande frequenti su Amazon VPC.

Opzione	Caso d'uso	Vantaggi	Limitazioni
AWS Site-to-Site VPN	Connessione VPN IPSec gestita da AWS su Internet a un singolo VPC	Riutilizza le apparecchiature e i processi VPN esistenti Riutilizza le connessioni Internet esistenti Servizio VPN ad alta disponibilità gestito da AWS Supporta percorsi statici o politiche di peering e routing dinamiche del Border Gateway Protocol (BGP)	La latenza, la variabilità e la disponibilità della rete dipendono dalle condizioni di Internet L'utente è responsabile dell'implementazione della ridondanza e del failover (se necessario) Il dispositivo remoto deve supportare BGP a hop singolo (quando si utilizza BGP per il routing dinamico)

Opzione	Caso d'uso	Vantaggi	Limitazioni
AWS Transit Gateway + VPN da sito a sito AWS	Connessione VPN IPSec gestita da AWS via Internet al router regionale per più VPC	Uguale all'opzione precedente AWS ha gestito un hub di rete regionale ad alta disponibilità e scalabilità per un massimo di 5.000 allegati	Uguale all'opzione precedente
AWS Direct Connect	Connessione di rete dedicata tramite linee private	Prestazioni di rete più prevedibili Costi di larghezza di banda ridotti Supporta le politiche di peering e routing BGP	Potrebbe richiedere ulteriori relazioni con fornitori di servizi di telecomunicazione e hosting o il provisioning di nuovi circuiti di rete
AWS Direct Connect + AWS Transit Gateway	Connessione di rete dedicata tramite linee private al router regionale per più VPC	Uguale all'opzione precedente AWS ha gestito un hub di rete regionale ad alta disponibilità e scalabilità per un massimo di 5.000 allegati	Uguale all'opzione precedente

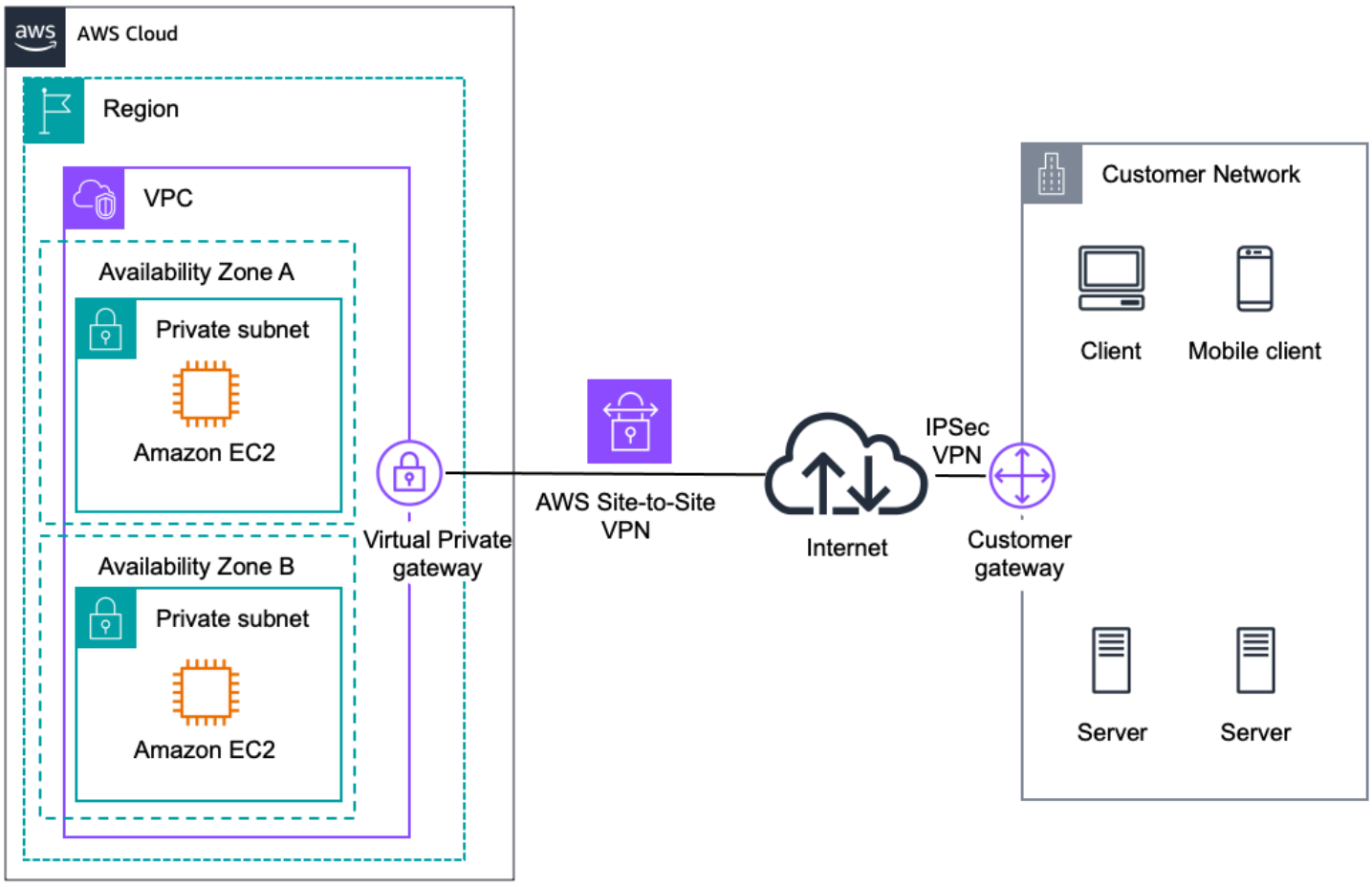
Opzione	Caso d'uso	Vantaggi	Limitazioni
AWS Direct Connect + VPN da sito a sito AWS	Connessione VPN IPSec su linee private	Prestazioni di rete più prevedibili Costi di larghezza di banda ridotti Supporta le politiche di peering e routing BGP su AWS Direct Connect Riutilizza le apparecchiature e i processi VPN esistenti Servizio VPN ad alta disponibilità gestito da AWS Supporta percorsi statici o politiche dinamiche di peering e routing del Border Gateway Protocol (BGP) sulla connessione VPN	Potrebbe richiedere relazioni aggiuntive con fornitori di servizi di telecomunicazione e hosting o il provisioning di nuovi circuiti di rete L'utente è responsabile dell'implementazione della ridondanza e del failover (se necessario) Il dispositivo remoto deve supportare BGP a hop singolo (quando si utilizza BGP per il routing dinamico)

Opzione	Caso d'uso	Vantaggi	Limitazioni
AWS Direct Connect + AWS Transit Gateway + VPN da sito a sito AWS	Connessione VPN IPSec su linee private al router regionale per più VPC	Uguale all'opzione precedente AWS ha gestito un hub di rete regionale ad alta disponibilità e scalabilità per un massimo di 5.000 allegati	Uguale all'opzione precedente
AWS VPN CloudHub	Connetti le filiali remote in un hub-and-spoke modello per la connettività principale o di backup	Riutilizza le connessioni e AWS VPN le connessioni Internet esistenti Servizio VPN ad alta disponibilità gestito da AWS Supporta BGP per lo scambio di rotte e priorità di routing	La latenza, la variabilità e la disponibilità della rete dipendono da Internet Gli endpoint delle filiali gestiti dagli utenti sono responsabili dell'implementazione della ridondanza e del failover (se necessario)
AWS Transit Gateway + Soluzioni SD-WAN	Connect filiali e uffici remoti con una rete WAN (Wide Area Network) definita dal software utilizzando la AWS backbone o Internet come rete di transito.	Supporta una gamma più ampia di fornitori, prodotti e protocolli SD-WAN Alcune soluzioni dei fornitori sono integrate con i servizi nativi di AWS.	Sei responsabile dell'implementazione dell'HA (alta disponibilità) delle appliance SD-WAN se sono collocate in un Amazon VPC.

Opzione	Caso d'uso	Vantaggi	Limitazioni
Software VPN	Connessione VPN basata su appliance software su Internet	Supporta una gamma più ampia di fornitori , prodotti e protocolli VPN Soluzione completamente gestita dal cliente	Sei responsabile dell'implementazione delle soluzioni HA (alta disponibilità) per tutti gli endpoint VPN (se necessario)

AWS Site-to-Site VPN

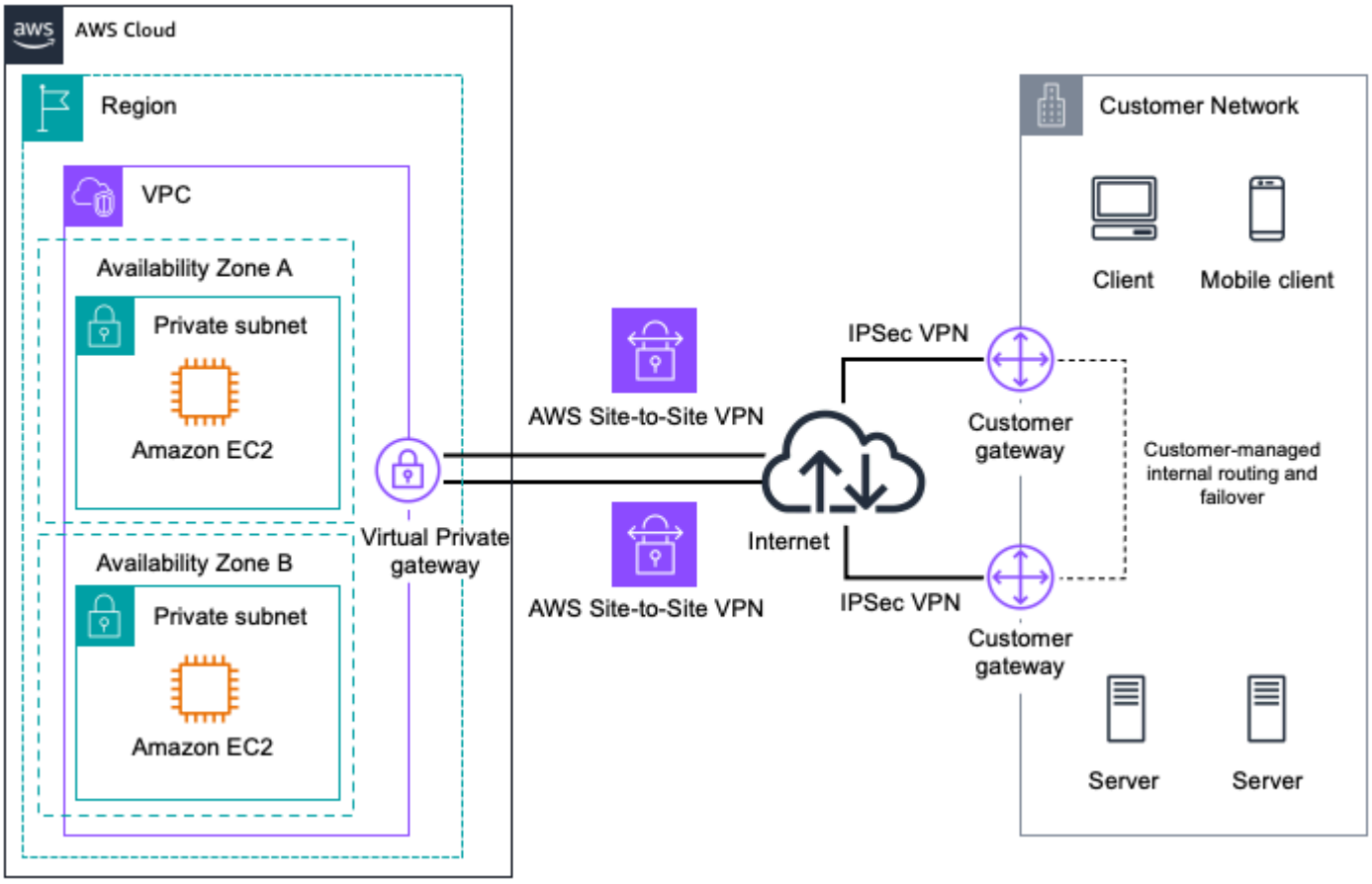
Amazon VPC offre la possibilità di creare una connessione VPN IPSec tra le reti remote e Amazon VPC tramite Internet, come illustrato nella figura seguente.



AWS Managed VPN

Prendi in considerazione l'adozione di questo approccio quando desideri sfruttare un endpoint VPN gestito da AWS che include ridondanza e failover automatizzati integrati nel lato AWS della connessione VPN.

Il gateway privato virtuale supporta e incoraggia inoltre le connessioni gateway di più utenti in modo da poter implementare la ridondanza e il failover sul lato della connessione VPN, come mostrato nella figura seguente.



Redundant AWS Site-to-Site VPN Connections

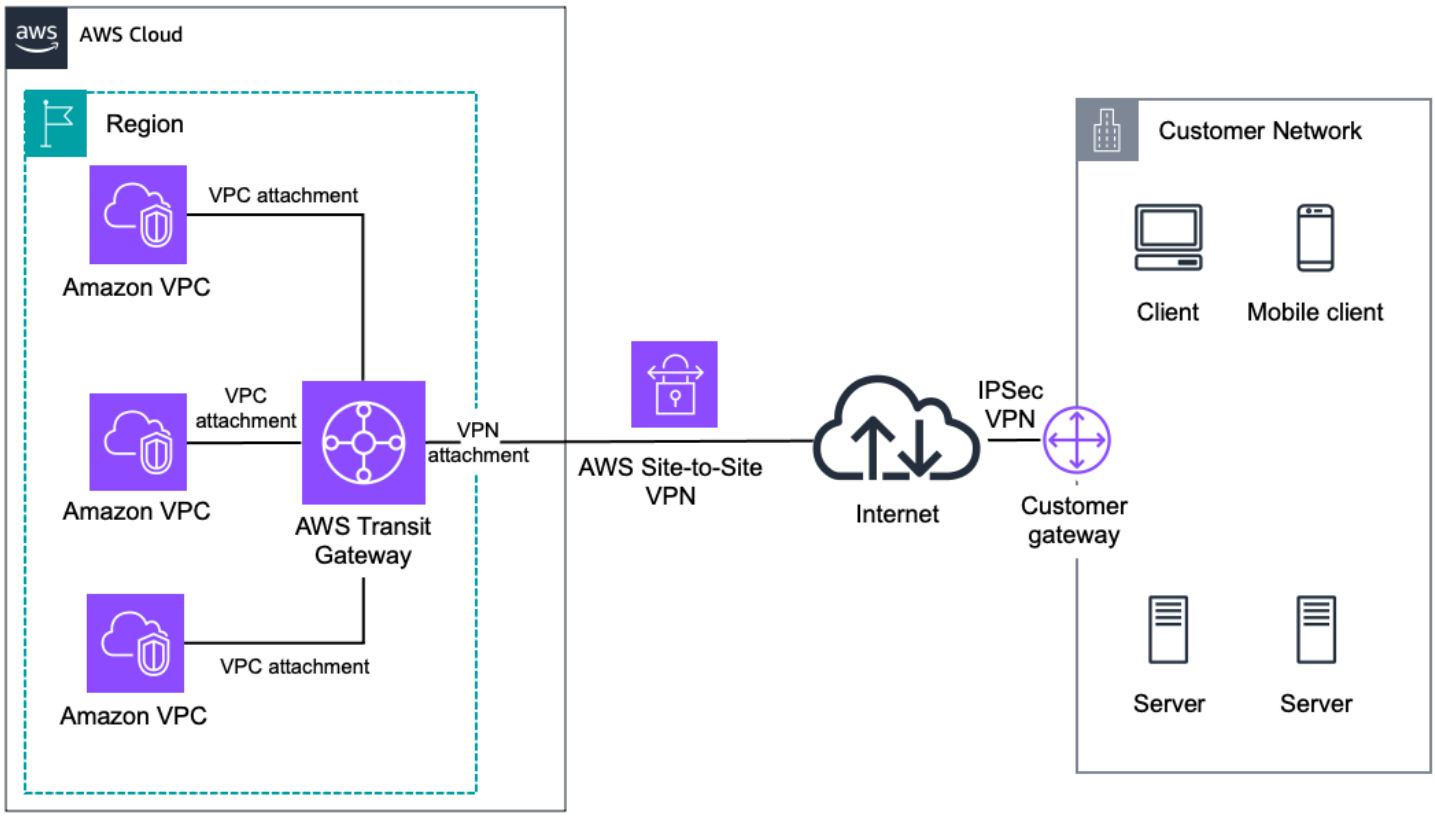
Sono disponibili opzioni di routing dinamico e statico per offrire flessibilità nella configurazione del routing. Il routing dinamico utilizza il peering BGP per lo scambio di informazioni di routing tra AWS e questi endpoint remoti. Con il routing dinamico, puoi anche specificare priorità, politiche e pesi (metriche) di routing nelle tue pubblicità BGP e influenzare il percorso di rete tra le tue reti e AWS. È importante notare che quando si utilizza BGP, sia la sessione IPSec che quella BGP devono essere terminate sullo stesso dispositivo gateway utente, quindi deve essere in grado di terminare sia le sessioni IPSec che BGP.

Risorse aggiuntive

- Guida per l'utente di AWS Site-to-Site VPN
- Requisiti per i dispositivi gateway del cliente
- Dispositivi gateway dei clienti testati con Amazon VPC

AWS Transit Gateway + VPN da sito a sito AWS

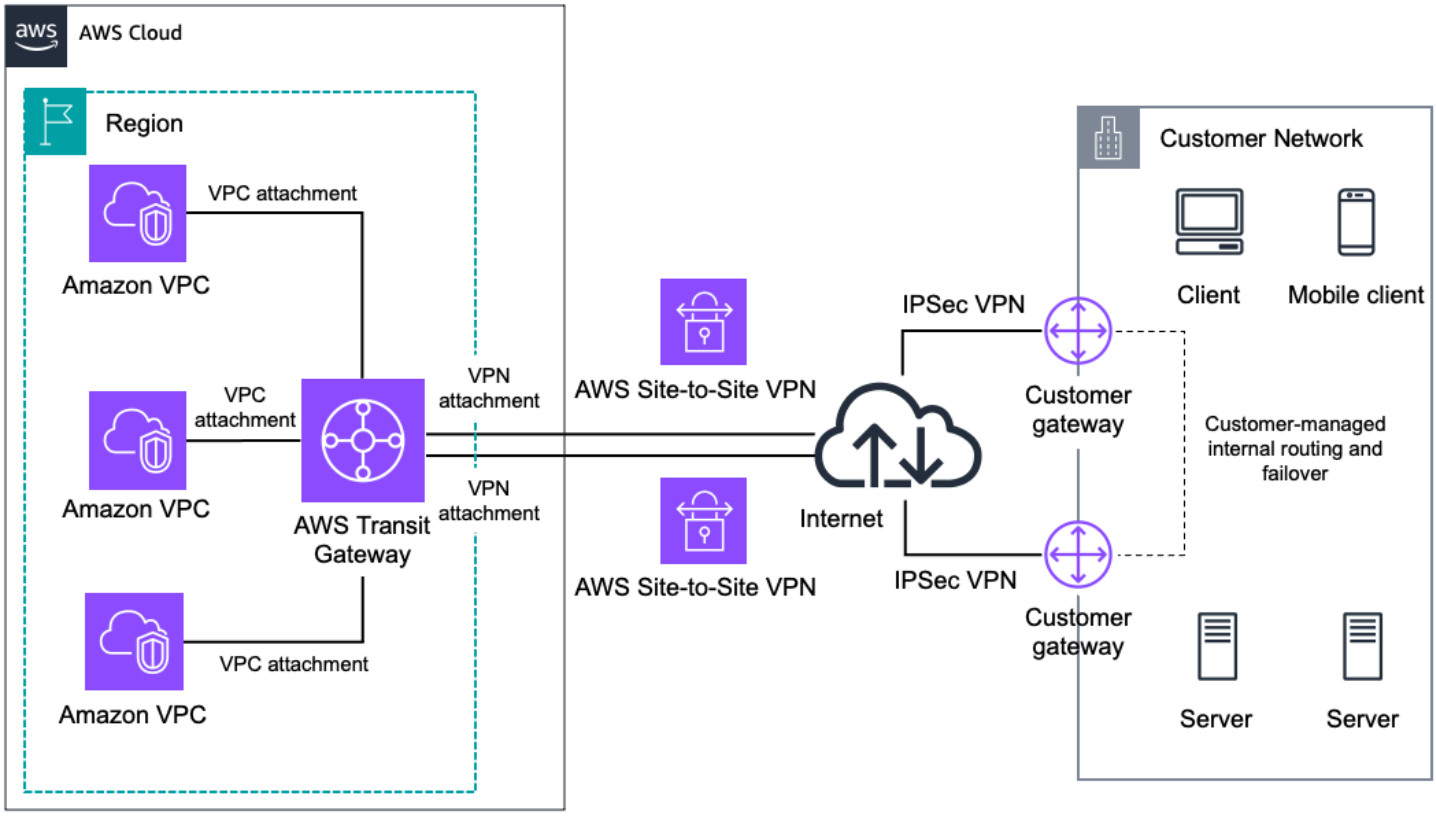
AWS Transit Gateway è un hub di transito di rete regionale ad alta disponibilità e scalabilità gestito da AWS utilizzato per interconnettere VPC e reti di clienti. AWS Transit Gateway + VPN, utilizzando l'allegato Transit Gateway VPN, offre la possibilità di creare una connessione VPN IPSec tra la rete remota e il Transit Gateway tramite Internet, come mostrato nella figura seguente.



AWS Transit Gateway and AWS Site-to-Site VPN

Prendi in considerazione l'utilizzo di questo approccio quando desideri sfruttare un endpoint VPN gestito da AWS per connetterti a più VPC nella stessa regione senza i costi aggiuntivi e la gestione di più connessioni VPN IPSec a più Amazon VPC.

AWS Transit Gateway supporta e incoraggia anche le connessioni gateway multiutente in modo da poter implementare ridondanza e failover sul lato della connessione VPN, come mostrato nella figura seguente.

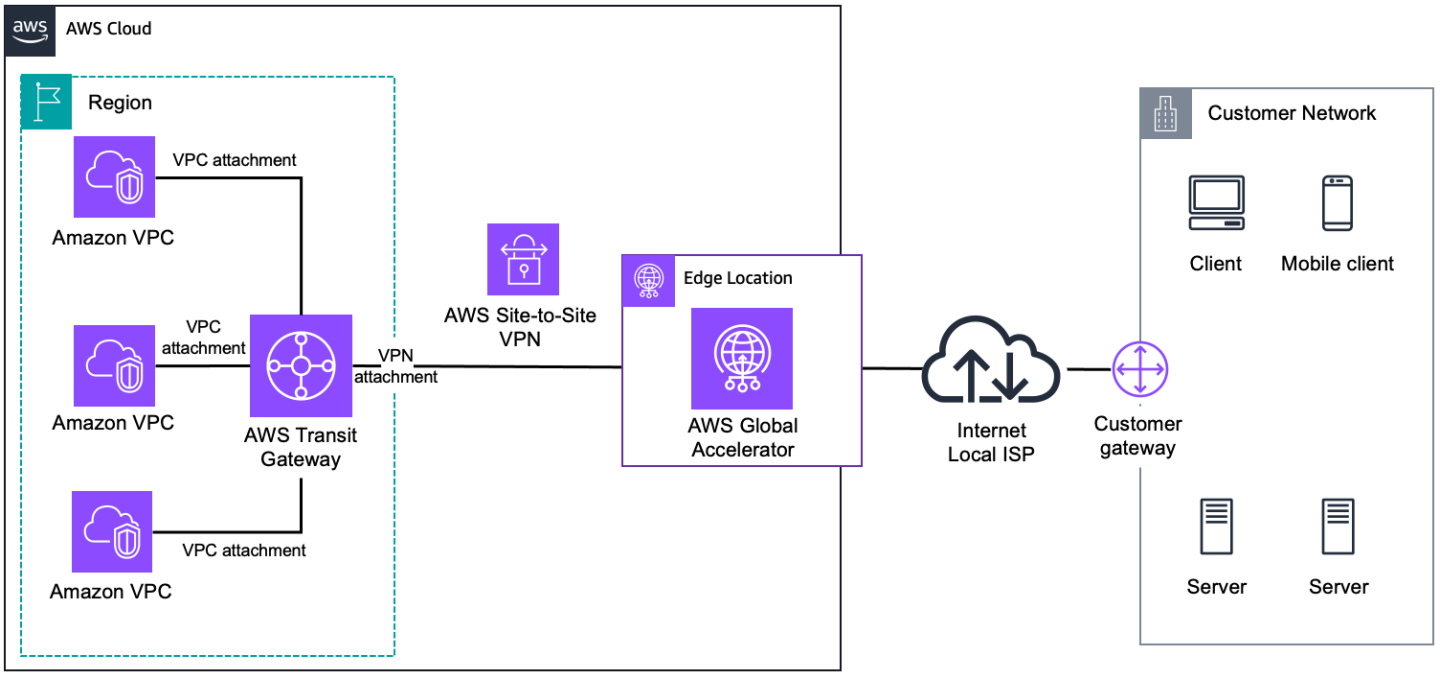


AWS Transit Gateway and Redundant VPN

Sono disponibili opzioni di routing dinamico e statico per offrire flessibilità nella configurazione di routing sull'allegato Transit Gateway VPN IPSec. Il routing dinamico utilizza il peering BGP per lo scambio di informazioni di routing tra AWS e questi endpoint remoti. Con il routing dinamico, puoi anche specificare priorità, politiche e pesi (metriche) di routing nelle tue pubblicità BGP e influenzare il percorso di rete tra le tue reti e AWS. È importante notare che quando si utilizza BGP, sia la sessione IPSec che quella BGP devono essere terminate sullo stesso dispositivo gateway utente, quindi deve essere in grado di terminare sia le sessioni IPSec che BGP.

Per ogni connessione VPN, è possibile raggiungere 1,25 Gbps di throughput e 140.000 pacchetti al secondo. Quando si terminano le connessioni VPN nel Transit Gateway, è possibile utilizzare il routing Equal Cost Multi-Path (ECMP) per ottenere una maggiore larghezza di banda VPN aggregando più tunnel VPN. Per utilizzare ECMP, è necessario configurare il routing dinamico nelle connessioni VPN: ECMP non è supportato utilizzando il routing statico.

Inoltre, puoi abilitare l'accelerazione nelle connessioni VPN da sito a sito AWS. Una connessione VPN accelerata utilizza AWS Global Accelerator per indirizzare il traffico dalla rete a una edge location AWS più vicina al dispositivo gateway del cliente. Puoi utilizzare questa opzione per evitare interruzioni di rete che potrebbero verificarsi quando il traffico viene instradato sulla rete Internet pubblica. L'accelerazione è supportata solo per le connessioni VPN collegate a un Transit Gateway, come illustrato nella figura seguente:



Accelerated AWS Site-to-Site VPN

Infine, per quanto riguarda l'indirizzamento IP, le connessioni VPN da sito a sito supportano sia il traffico IPv4 che AWS Transit Gateway IPv6. Si applicano le regole seguenti:

- IPv6 è supportato solo per gli indirizzi IP interni del tunnel VPN. Gli indirizzi IP esterni per gli AWS endpoint sono indirizzi IPv4 pubblici. L'indirizzo IP del gateway del cliente deve essere un indirizzo IPv4 pubblico.
- Una connessione Site-to-Site VPN non può supportare sia il traffico IPv4 che IPv6. Se la connettività ibrida richiede una comunicazione dual-stack, è necessario creare diversi tunnel VPN per il traffico IPv4 e IPv6.

Risorse aggiuntive

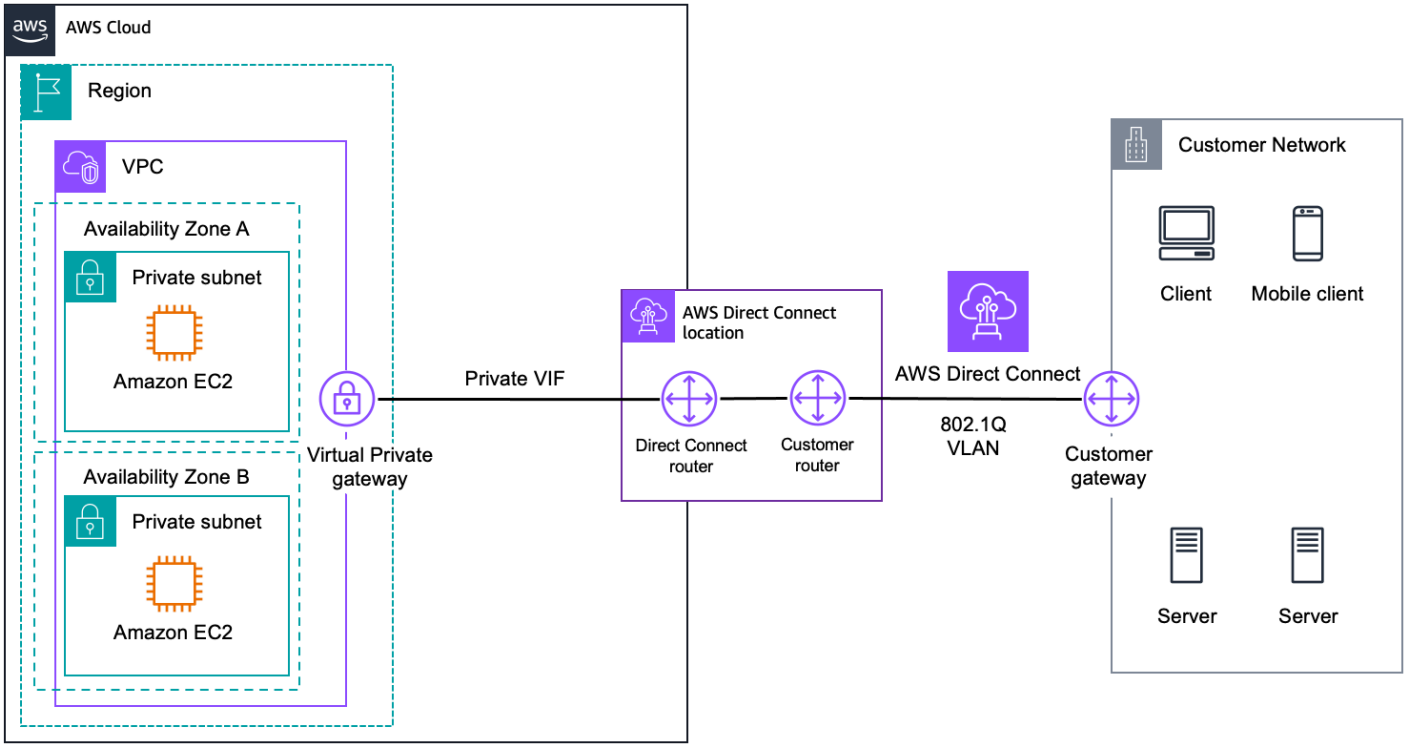
- Allegati Transit Gateway VPN
- Gateway per clienti

- Utilizzo della VPN da sito a sito
- Connessioni VPN da sito a sito accelerate

AWS Direct Connect

AWS Direct Connectsemplifica la creazione di una connessione dedicata da una rete locale a uno o più VPC. AWS Direct Connect può ridurre i costi di rete, aumentare la velocità di trasmissione della larghezza di banda e fornire un'esperienza di rete più coerente rispetto alle connessioni basate su Internet. Utilizza VLAN 802.1Q standard di settore per connettersi ad Amazon VPC utilizzando indirizzi IP privati. Le VLAN sono configurate utilizzando interfacce virtuali (VIF) e puoi configurare tre diversi tipi di VIF:

- Interfaccia virtuale pubblica: stabilisci la connettività tra gli endpoint AWS pubblici e il data center, l'ufficio o l'ambiente di colocation.
- Interfaccia virtuale di transito: stabilisci una connettività privata tra AWS Transit Gateway il data center, l'ufficio o l'ambiente di colocation. Questa opzione di connettività è trattata nella sezione. ???
- Interfaccia virtuale privata: stabilisci una connettività privata tra le risorse Amazon VPC e il tuo data center, ufficio o ambiente di colocation. L'uso di VIF private è illustrato nella figura seguente.



AWS Direct Connect

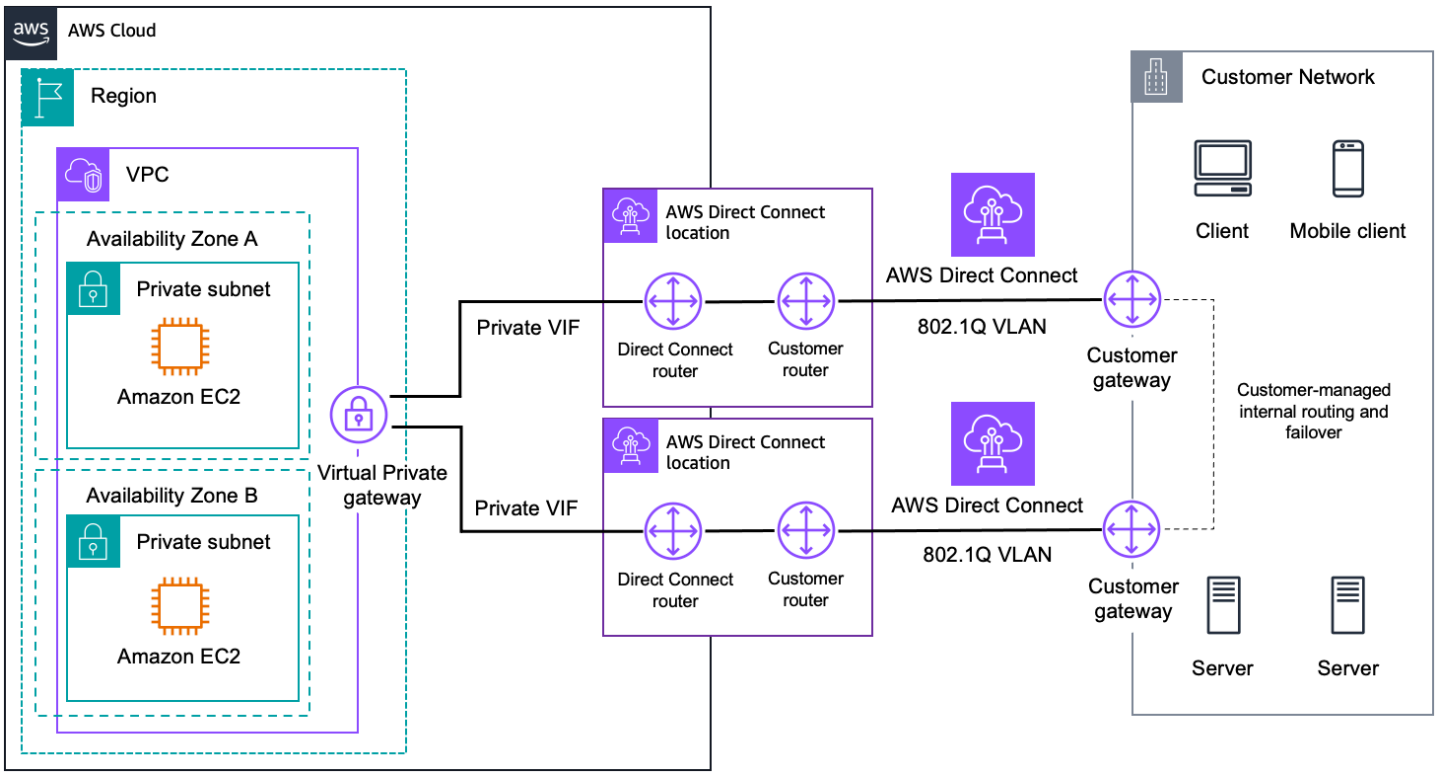
È possibile stabilire la connettività alla AWS dorsale AWS Direct Connect utilizzando una connessione incrociata ai AWS dispositivi in una posizione Direct Connect. Puoi accedere a qualsiasi AWS regione da qualsiasi delle nostre sedi Direct Connect (eccetto la Cina). Se non disponi di apparecchiature in loco, puoi scegliere tra un ecosistema di provider di servizi WAN per integrare il tuo AWS Direct Connect endpoint in una AWS Direct Connect posizione con le tue reti remote.

Con AWS Direct Connect, hai due tipi di connessione:

- Connessioni dedicate, in cui una connessione Ethernet fisica è associata a un singolo cliente. È possibile ordinare velocità di porta di 1, 10 o 100 Gbps. Potrebbe essere necessario collaborare con un AWS Direct Connect partner del Partner Program per aiutarti a stabilire circuiti di rete tra una AWS Direct Connect connessione e il tuo data center, ufficio o ambiente di colocation.
- Connessioni ospitate, in cui una connessione Ethernet fisica viene fornita da un AWS Direct Connect partner e condivisa con te. È possibile ordinare velocità di porta comprese tra 50 Mbps e 10 Gbps. Collaborate con il partner sia per la AWS Direct Connect connessione che ha stabilito sia per i circuiti di rete tra una AWS Direct Connect connessione e il data center, l'ufficio o l'ambiente di colocation.

Per le connessioni dedicate, puoi anche utilizzare un gruppo di aggregazione dei link (LAG) per aggregare più connessioni su un singolo endpoint. AWS Direct Connect Le trattate come un'unica connessione gestita. È possibile aggregare fino a quattro connessioni da 1 o 10 Gbps e fino a due connessioni da 100 Gbps.

Quando si parla di alta disponibilità in AWS Direct Connect, si consiglia di utilizzare connessioni aggiuntive. AWS Direct Connect Il AWS Direct Connect Resiliency Toolkit offre indicazioni per creare connessioni di rete altamente resilienti tra AWS il data center, l'ufficio o l'ambiente di colocation. La figura seguente mostra un esempio di opzione di connettività ad alta resilienza, con due connessioni terminate in due AWS Direct Connect posizioni diverse. AWS Direct Connect

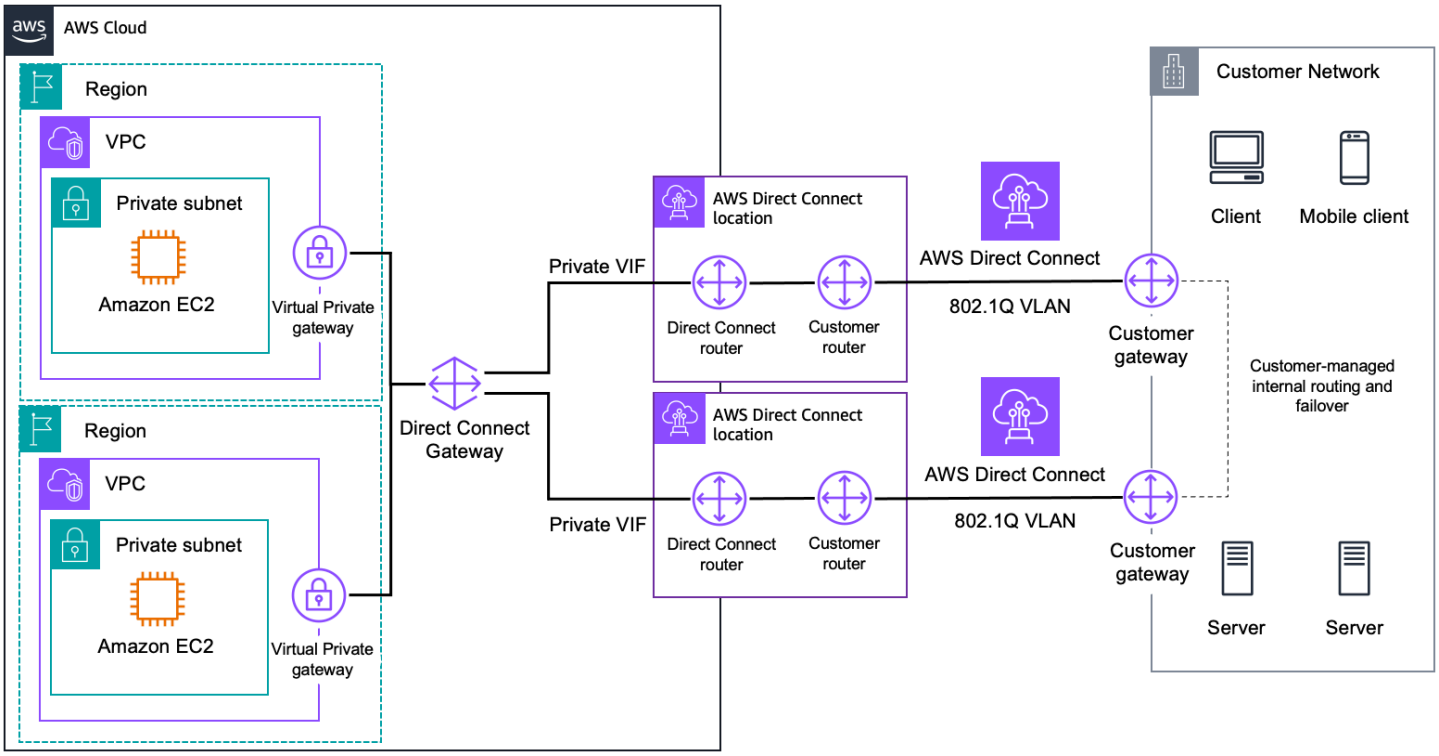


Ridondante AWS Direct Connect

AWS Direct Connect non è crittografato per impostazione predefinita. Per connessioni dedicate da 10 o 100 Gbps, è possibile utilizzare la sicurezza MAC (MacSec) come opzione di crittografia. Per connessioni pari o inferiori a 1 Gbps, puoi creare tunnel VPN sulla parte superiore della connessione: questa opzione è trattata in 3 sezioni. AWS Direct Connect + VPN da sito a sito AWS AWS Direct Connect + AWS Transit Gateway + VPN da sito a sito AWS

Una risorsa importante AWS Direct Connect è il gateway Direct Connect, una risorsa disponibile a livello globale per consentire connessioni a più Amazon VPC o Transit Gateway in diverse regioni o AWS account. Questa risorsa consente inoltre di connettersi a qualsiasi VPC o Transit Gateway

partecipante da un VIF privato o un VIF di transito, riducendo la AWS Direct Connect gestione, come illustrato nella figura seguente.



AWS Direct Connect Gateway

Per quanto riguarda l'indirizzamento IP, le interfacce AWS Direct Connect virtuali supportano sessioni BGP sia IPv4 che IPv6 per il funzionamento dual-stack.

- La configurazione IPv4 dei VIF privati e di transito utilizza indirizzi IPv4 generati da AWS o indirizzi configurati dall'utente. Per il peering BGP IPv4 pubblico di VIF, devi specificare un CIDR IPv4 IPv4 pubblico univoco di tua proprietà (o inviare una richiesta per l'assegnazione di un blocco CIDR).
- Per tutti i tipi di peering BGP IPv6 di VIF, AWS assegna un /125 CIDR, che non è configurabile.

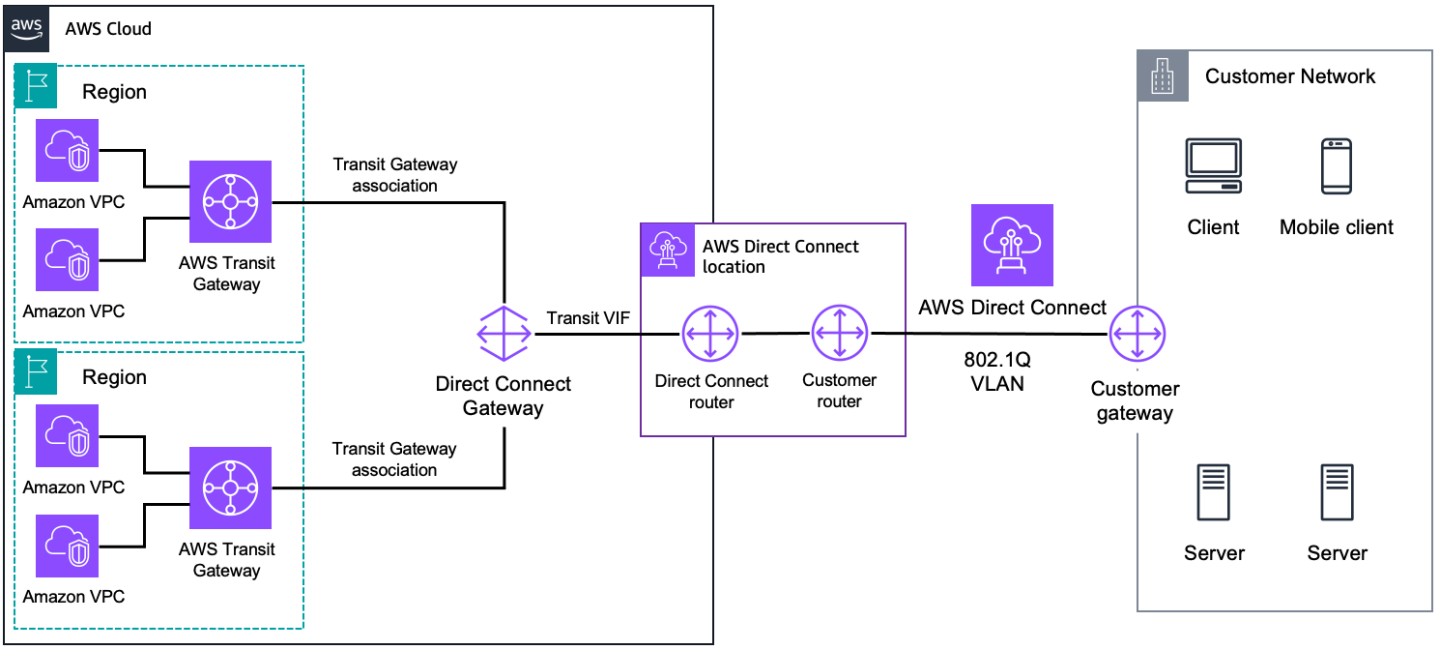
Risorse aggiuntive

- AWS Direct Connect Guida per l'utente
- AWS Direct Connect interfacce virtuali
- AWS Direct Connect gateway
- AWS Direct Connect Toolkit di resilienza
- AWS Direct Connect Sicurezza MAC
- AWS Direct Connect sedi

- AWS Direct Connect Partner di consegna

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect+ AWS Transit Gateway, utilizzando l'attacco Transit VIF al gateway Direct Connect, consente alla rete di connettere diversi router centralizzati regionali tramite una connessione privata dedicata. Il diagramma seguente mostra la connessione a due router.



AWS Direct Connect and AWS Transit Gateway

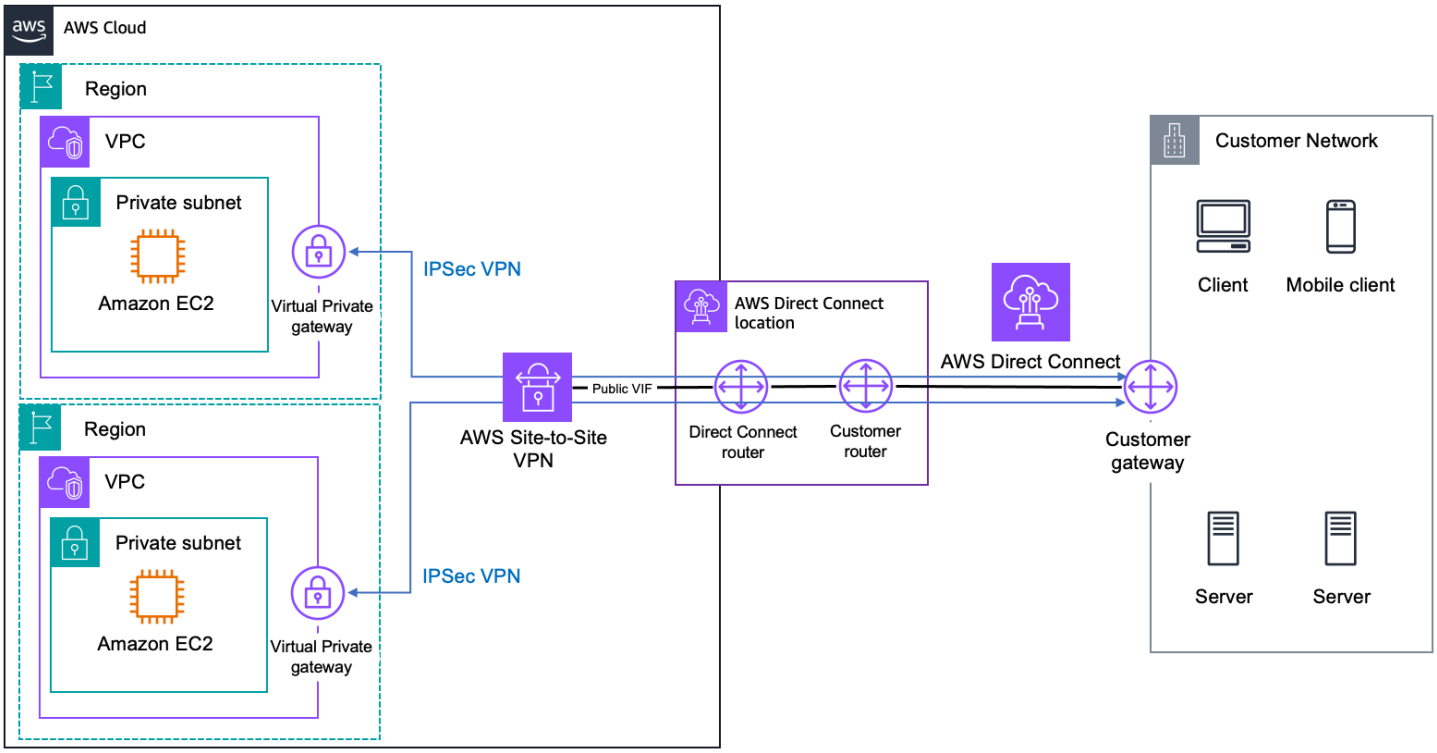
Ciascuno AWS Transit Gateway è un hub di transito di rete per interconnettere i VPC nella stessa regione, consolidando la configurazione di routing di Amazon VPC in un unico posto. Questa soluzione semplifica la gestione delle connessioni tra un Amazon VPC e le tue reti tramite una connessione privata che può ridurre i costi di rete, aumentare il throughput della larghezza di banda e fornire un'esperienza di rete più coerente rispetto alle connessioni basate su Internet.

Risorse aggiuntive

- Guida per l'utente di AWS Direct Connect
- Collega gruppi di aggregazione in AWS Direct Connect
- Post del blog: Integrazione di connessioni ospitate inferiori a 1 Gbps con AWS Transit Gateway

AWS Direct Connect + VPN da sito a sito AWS

Con AWS Direct Connect+ AWS Site-to-Site VPN, puoi AWS Direct Connect combinare connessioni con una soluzione VPN gestita da AWS. AWS Direct Connect le VIF pubbliche stabiliscono una connessione di rete dedicata tra la tua rete e le risorse AWS pubbliche come un endpoint VPN da sito a sito AWS. Una volta stabilita la connessione al servizio, puoi creare connessioni IPSec ai corrispondenti gateway privati virtuali Amazon VPC. La figura seguente illustra questa opzione.



AWS Direct Connect and AWS Site-to-Site VPN

Questa soluzione combina i vantaggi della connessione IPSec end-to-end sicura con una bassa latenza e una maggiore larghezza di banda AWS Direct Connect per fornire un'esperienza di rete più coerente rispetto alle connessioni VPN basate su Internet. Viene stabilita una sessione di connessione BGP tra AWS Direct Connect e il router sulla VIF pubblica. Verrà stabilita un'altra sessione BGP o una route statica tra il gateway privato virtuale e il router sui tunnel VPN IPSec.

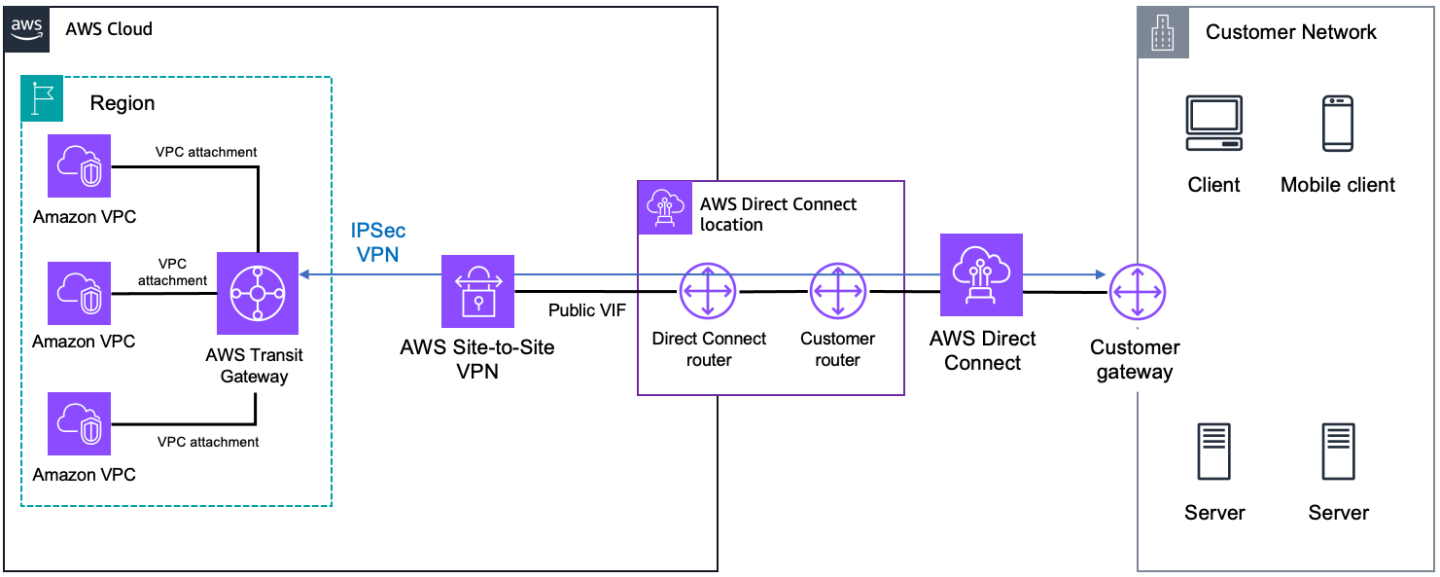
Risorse aggiuntive

- AWS Direct Connect
- AWS Direct Connect interfacce virtuali
- Guida per l'utente di AWS Site-to-Site VPN

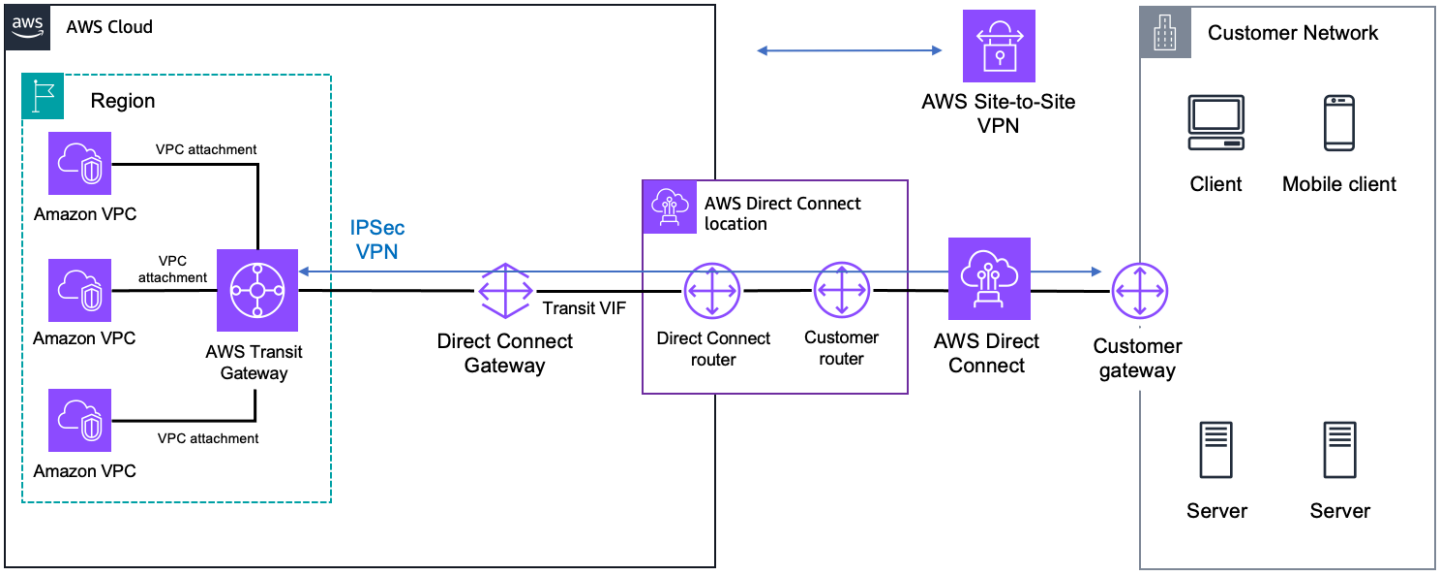
AWS Direct Connect + AWS Transit Gateway + VPN da sito a sito AWS

Con AWS Direct Connect+ AWS Transit Gateway+ AWS Site-to-Site VPN, puoi end-to-end abilitare connessioni crittografate con IPSec tra le tue reti e un router centralizzato regionale per Amazon VPC tramite una connessione privata dedicata.

Puoi utilizzare i file VIF AWS Direct Connect pubblici per stabilire innanzitutto una connessione di rete dedicata tra la tua rete e le risorse AWS pubbliche, come gli endpoint VPN da sito a sito di AWS. Una volta stabilita questa connessione, puoi creare una connessione IPSec a. AWS Transit Gateway La figura seguente illustra questa opzione.



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (public VIF)



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (transit VIF)

Prendi in considerazione l'adozione di questo approccio quando desideri semplificare la gestione e ridurre al minimo il costo delle connessioni VPN IPSec a più Amazon VPC nella stessa regione, con i vantaggi della bassa latenza e dell'esperienza di rete coerente di una connessione privata dedicata rispetto a una VPN basata su Internet. Viene stabilita una sessione BGP tra AWS Direct Connect e il router utilizzando il VIF pubblico o quello di transito. Verrà stabilita un'altra sessione BGP o una route statica tra AWS Transit Gateway e il router sul tunnel VPN IPSec.

Risorse aggiuntive

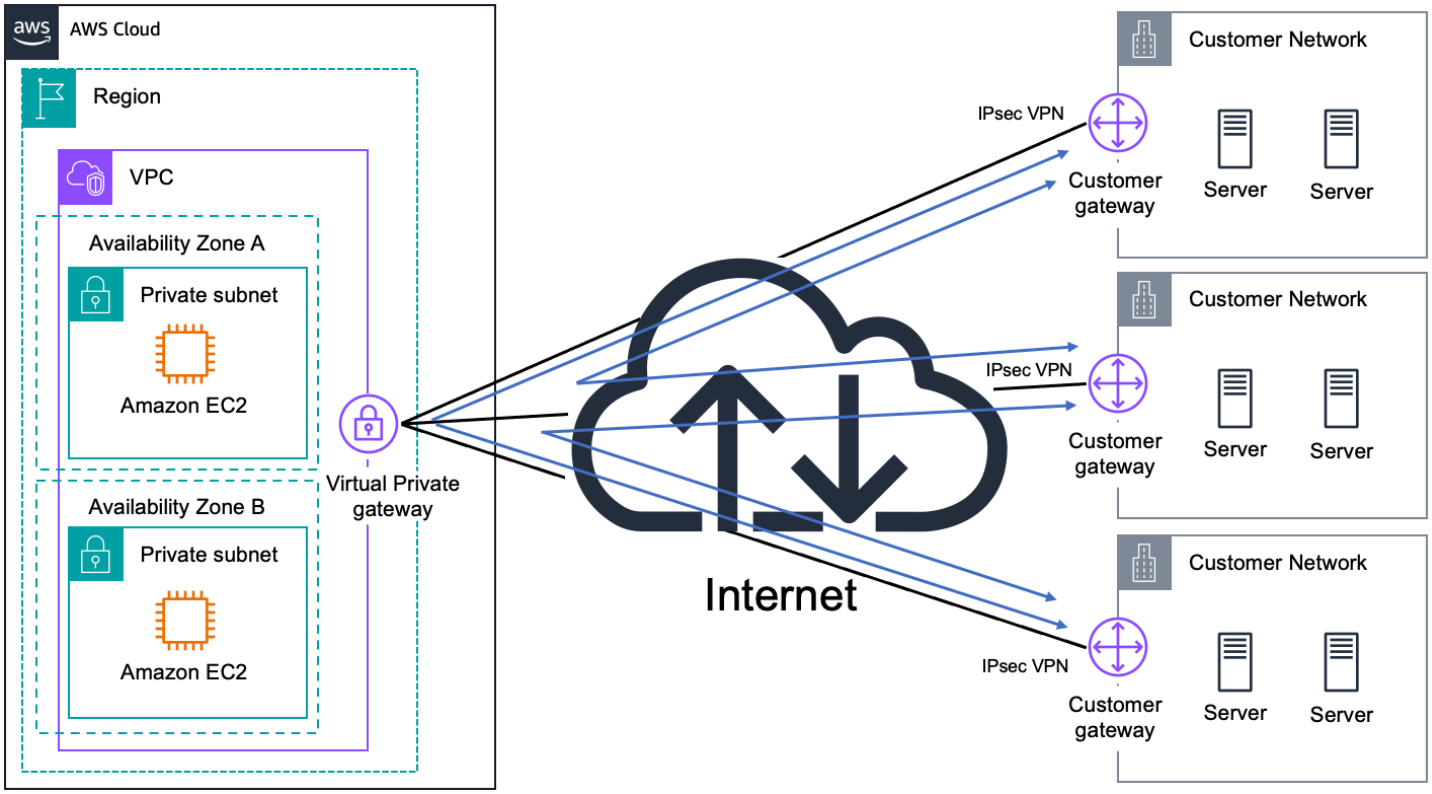
- Interfacce virtuali AWS Direct Connect
- Allegati VPN Transit Gateway
- Requisiti per i dispositivi gateway del cliente
- Dispositivi gateway dei clienti testati con Amazon VPC
- VPN da sito a sito AWS: VPN IP privata con AWS Direct Connect

AWS VPN CloudHub

Basandosi sulle opzioni VPN gestite di AWS descritte in precedenza, puoi comunicare in modo sicuro da un sito all'altro utilizzando il AWS VPN CloudHub. AWS VPN CloudHub Funziona su un hub-and-spoke modello semplice che puoi usare con o senza un VPC. Utilizza questo approccio se disponi di più filiali e di connessioni Internet esistenti e desideri implementare un hub-and-spoke modello

conveniente e potenzialmente a basso costo per la connettività principale o di backup tra queste sedi remote.

La figura seguente mostra l' AWS VPN CloudHub architettura, con linee che indicano il traffico di rete tra siti remoti instradato tramite le relative AWS VPN connessioni.



AWS VPN CloudHub

AWS VPN CloudHub utilizza un gateway privato virtuale Amazon VPC con più gateway per clienti, ciascuno dei quali utilizza numeri di sistema autonomi (ASN) BGP univoci. I siti remoti non devono avere intervalli IP sovrapposti. I tuoi gateway pubblicizzano i percorsi appropriati (prefissi BGP) tramite le loro connessioni VPN. Questi annunci di routing vengono ricevuti e ripubblicizzati a ciascun peer BGP in modo che ogni sito possa inviare e ricevere dati dagli altri siti.

Risorse aggiuntive

- Fornire comunicazioni sicure tra siti tramite VPN CloudHub
- Guida per l'utente di AWS Site-to-Site VPN
- Requisiti per i dispositivi gateway dei clienti
- Dispositivi gateway dei clienti testati con Amazon VPC

AWS Transit Gateway + Soluzioni SD-WAN

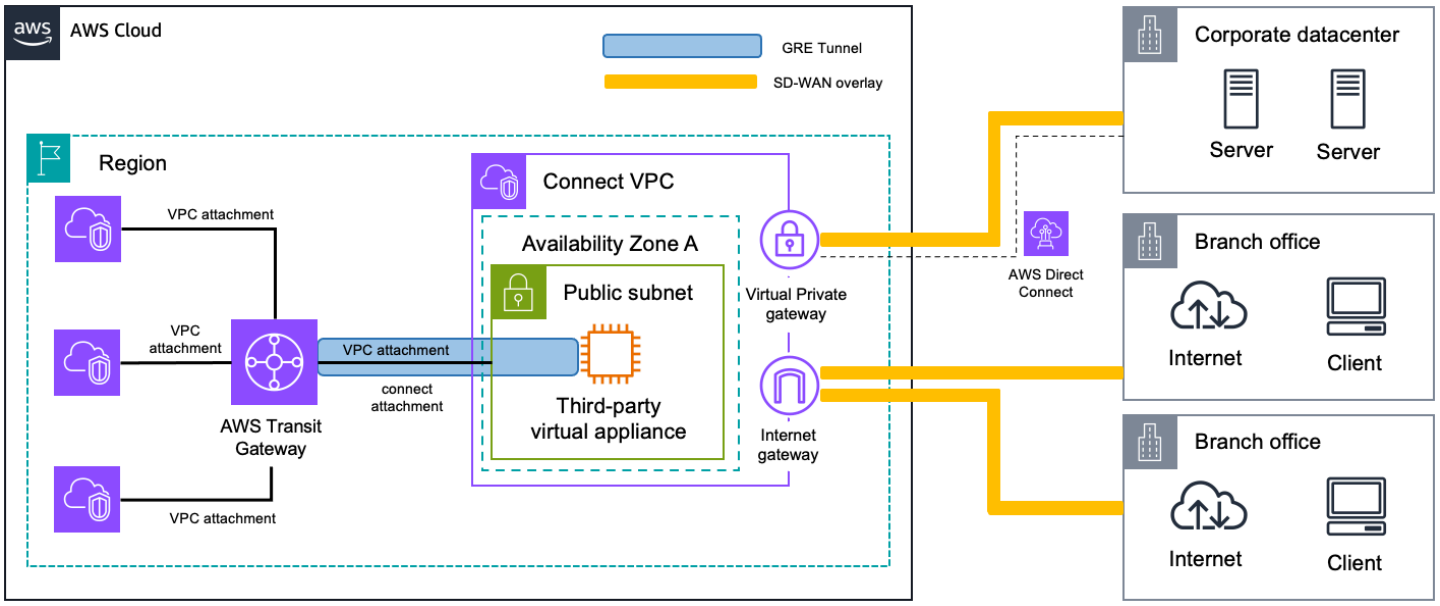
Le reti SD-WAN (Software Defined Wide Area Network) vengono utilizzate per connettere i data center, gli uffici o gli ambienti di colocation su diverse reti di transito (come l'Internet pubblico, le reti MPLS o la dorsale AWS Direct Connect di AWS), gestendo il traffico automaticamente e dinamicamente attraverso il percorso più appropriato ed efficiente in base alle condizioni di rete, al tipo di applicazione o ai requisiti di qualità del servizio (QoS).

Utilizza questo approccio se disponi di una topologia di rete complessa, con diversi data center, uffici o ambienti di colocation che devono comunicare tra loro e con AWS. Le soluzioni SD-WAN possono aiutarti a gestire in modo efficiente questo tipo di rete.

Quando si parla della connessione di una rete SD-WAN ad AWS, AWS Transit Gateway fornisce un hub di transito di rete regionale gestito, altamente disponibile e scalabile per interconnettere i VPC e la rete SD-WAN. Gli allegati Transit Gateway Connect forniscono un modo nativo per connettere l'infrastruttura e le appliance SD-WAN con AWS. In questo modo è facile estendere la tua SD-WAN in AWS senza dover configurare VPN IPSec.

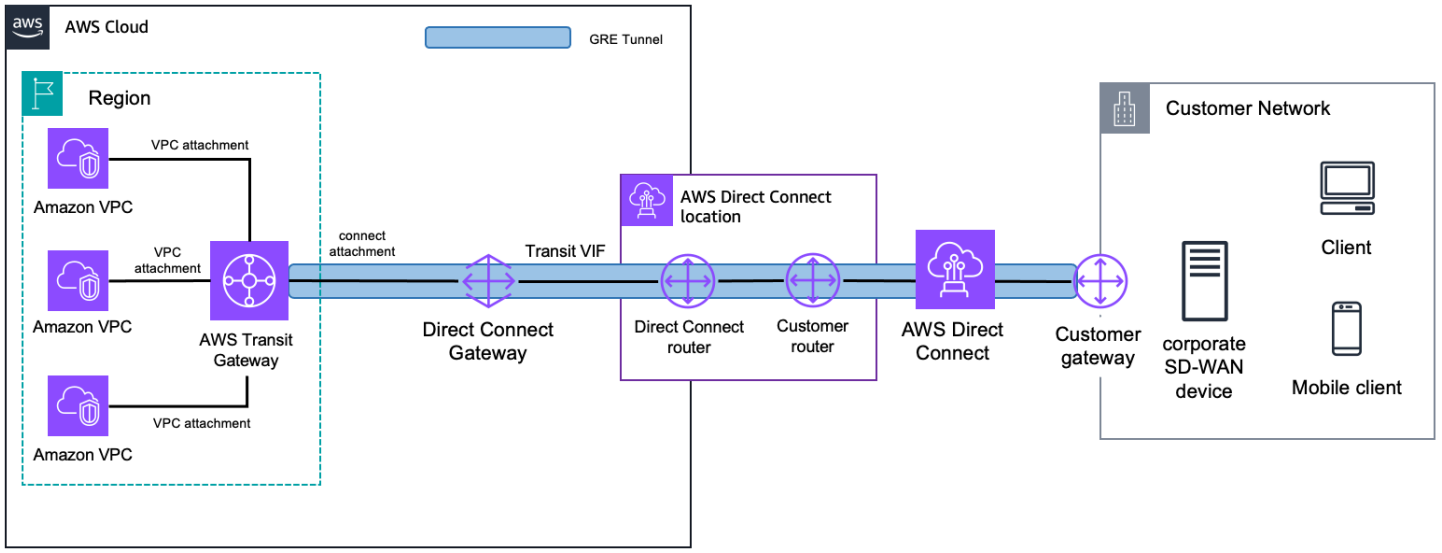
Gli allegati Transit Gateway Connect supportano Generic Routing Encapsulation (GRE) per prestazioni di larghezza di banda più elevate rispetto a una connessione VPN. Supporta il Border Gateway Protocol (BGP) per il routing dinamico ed elimina la necessità di configurare percorsi statici. Ciò semplifica la progettazione della rete e riduce i costi operativi associati. Inoltre, la sua integrazione con Transit Gateway Network Manager offre una visibilità avanzata attraverso la topologia di rete globale, le metriche delle prestazioni a livello di allegato e i dati di telemetria.

Quando si integra la rete SD-WAN con Transit Gateway utilizzando gli allegati di connessione, si hanno due schemi comuni. Il primo consiste nel collocare le appliance virtuali della rete SD-WAN in un VPC all'interno di AWS. Quindi, si utilizza un allegato VPC come trasporto sottostante per l'allegato di connessione Transit Gateway tra le appliance virtuali e il Transit Gateway, come illustrato nella figura seguente.



SD-WAN connectivity with AWS Transit Gateway (virtual appliance in AWS)

In alternativa, puoi estendere e segmentare il traffico SD-WAN verso AWS senza aggiungere un'infrastruttura aggiuntiva. È possibile creare allegati di connessione Transit Gateway utilizzando una AWS Direct Connect connessione come trasporto sottostante, come illustrato nella figura seguente.



SD-WAN connectivity with AWS Transit Gateway (Direct Connect as transport)

Quando si utilizzano gli allegati Transit Gateway Connect, occorre tenere presente alcune considerazioni:

- È possibile creare allegati di connessione su Transit Gateway esistenti.

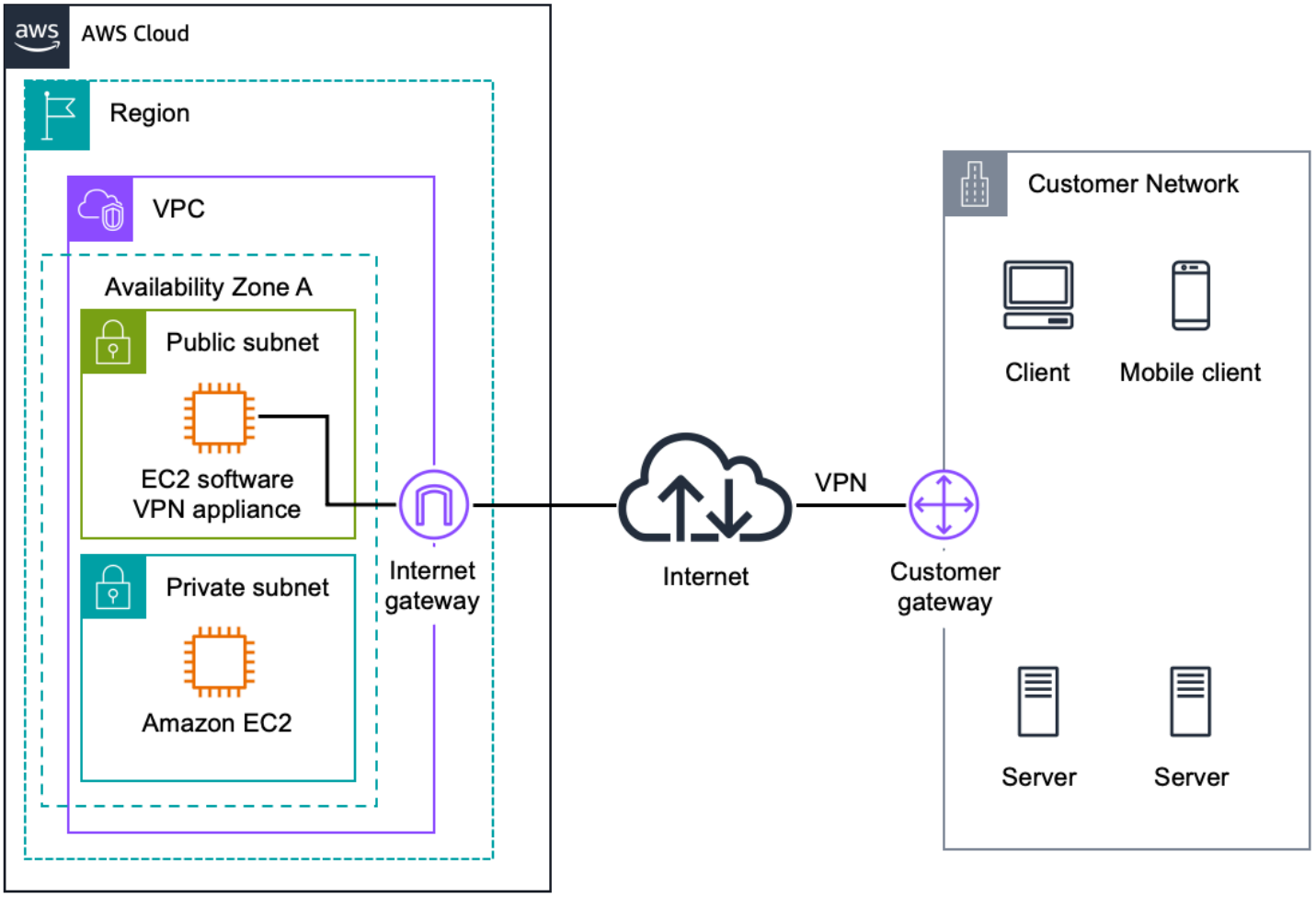
- Le apparecchiature di terze parti devono essere configurate con un tunnel GRE per inviare e ricevere traffico da Transit Gateway utilizzando gli allegati di connessione. L'appliance deve essere configurata con BGP per gli aggiornamenti dinamici delle rotte e i controlli di integrità.
- Gli allegati Connect non supportano le route statiche.
- Gli allegati Transit Gateway Connect supportano una larghezza di banda massima di cinque Gbps per tunnel GRE. È possibile ottenere una larghezza di banda superiore a cinque Gbps pubblicizzando gli stessi prefissi su più peer Connect (tunnel GRE) per lo stesso allegato Connect.
- Sono supportati un massimo di quattro peer Connect per ogni allegato Connect.
- Gli allegati Transit Gateway connect supportano IPv6 e annunci di routing dinamico tramite Multiprotocol Extensions for BGP (MBGP o MP-BGP).

Risorse aggiuntive

- Allegati di peering Transit Gateway
- Requisiti e considerazioni
- Post del blog: Semplifica la connettività SD-WAN con AWS Transit Gateway Connect

Software VPN

Amazon VPC ti offre la flessibilità necessaria per gestire completamente entrambi i lati della connettività Amazon VPC creando una connessione VPN tra la tua rete remota e un'appliance VPN software in esecuzione nella tua rete Amazon VPC. Questa opzione è consigliata se devi gestire entrambe le estremità della connessione VPN, per motivi di conformità o per sfruttare dispositivi gateway che attualmente non sono supportati dalla soluzione VPN di Amazon VPC. La figura seguente mostra questa opzione.



Software VPN da sito a sito

Puoi scegliere tra un ecosistema di più partner e comunità open source che hanno prodotto appliance VPN software che funzionano su Amazon EC2. Oltre a questa scelta, c'è la responsabilità di gestire l'appliance software, inclusa la configurazione, le patch e gli aggiornamenti.

Tieni presente che questo design introduce un potenziale punto di errore singolo nella progettazione di rete perché l'appliance software VPN viene eseguita su una singola istanza Amazon EC2. Per ulteriori informazioni, consulta Appendice A: Architettura HA di alto livello per istanze software VPN Architecture for Software VPN Instances.

Risorse aggiuntive

- Dispositivi VPN disponibili in Marketplace AWS
- Descrizione tecnica - Connessione di Cisco ASA a un'istanza VPC EC2 (IPSec)
- Descrizione tecnica - Connessione di più VPC con istanze EC2 (IPSec)

- Descrizione tecnica - Connessione di più VPC con istanze EC2 (SSL)

Opzioni di connettività da Amazon VPC ad Amazon VPC

Utilizza questi modelli di progettazione quando desideri integrare più Amazon VPC in una rete virtuale più ampia. Ciò è utile se hai bisogno di più VPC per motivi di sicurezza, fatturazione, presenza in più regioni o requisiti interni di charge-back, per integrare più facilmente le risorse AWS tra Amazon VPC. Puoi anche combinare questi modelli con le opzioni di connettività da rete ad Amazon VPC per creare una rete aziendale che si estende su reti remote e più VPC.

La connettività VPC tra VPC si ottiene al meglio quando si utilizzano intervalli IP non sovrapposti per ogni VPC collegato. Ad esempio, se desideri connettere più VPC, assicurati che ogni VPC sia configurato con intervalli CIDR (Classless Inter-Domain Routing) unici. Pertanto, ti consigliamo di allocare un singolo blocco CIDR contiguo e non sovrapposto da utilizzare da ciascun VPC. Per ulteriori informazioni sul routing e sui vincoli di Amazon VPC, consulta le domande frequenti su Amazon VPC.

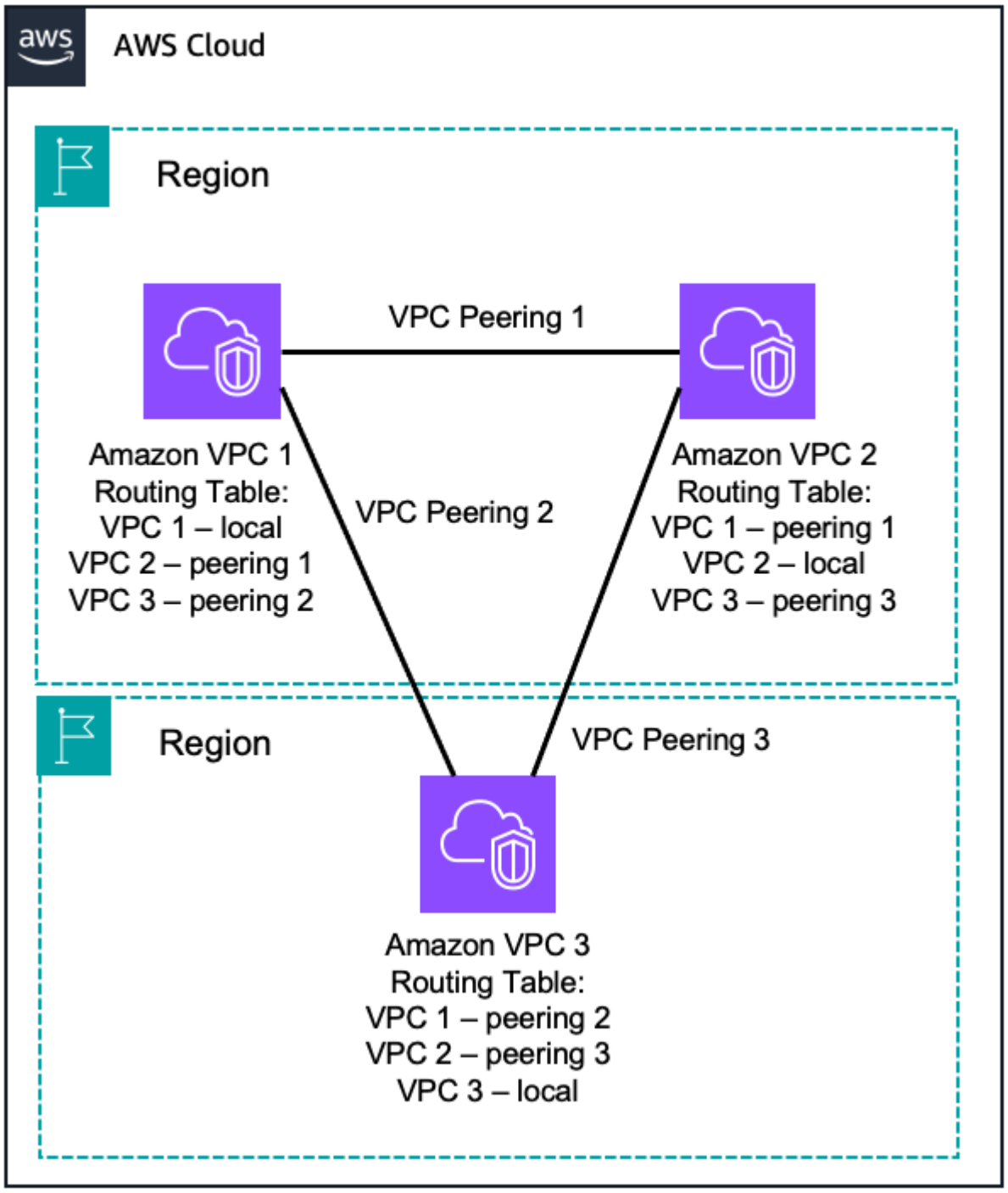
Opzione	Caso d'uso	Vantaggi	Limitazioni
Peering VPC	Connettività di rete fornita da AWS tra due VPC.	Sfrutta l'infrastruttura di rete scalabile gestita da AWS	Il peering VPC non supporta le relazioni di peering transitive Difficile da gestire su larga scala
AWS Transit Gateway	Connettività router regionale fornita da AWS per VPC	Servizio di alta disponibilità e scalabilità gestito da AWS Hub di rete regionale per un massimo di 5.000 allegati	Il peering Transit Gateway supporta solo route statiche
AWS PrivateLink	Connettività di rete fornita da AWS tra due VPC utilizzando endpoint di interfaccia	Sfrutta l'infrastruttura di rete scalabile gestita da AWS	I servizi VPC Endpoint sono disponibili solo nella regione AWS in cui vengono creati

Opzione	Caso d'uso	Vantaggi	Limitazioni
Software VPN	Connessioni VPN basate su appliance software tra VPC	Supporta un'ampia gamma di fornitori, prodotti e protocolli VPN Gestito interamente da te	Sei responsabile dell'implementazione delle soluzioni HA per tutti gli endpoint VPN (se necessario) Le istanze VPN potrebbero diventare un collo di bottiglia della rete
Software da VPN a VPN da sito a sito AWS	Da dispositivo software a connessione VPN tra VPC	Connessione VPN VPC ad alta disponibilità gestita da AWS Supporta un'ampia gamma di fornitori e prodotti VPN gestiti da te Supporta percorsi statici e politiche dinamiche di peering e routing BGP	L'utente è responsabile dell'implementazione delle soluzioni HA per gli endpoint VPN dell'appliance software (se necessario) Le istanze VPN potrebbero diventare un collo di bottiglia della rete Protocollo VPN IPSec solo per AWS Managed VPN

Peering VPC

Una connessione peering di VPC è una connessione di rete tra due VPC che consente di eseguire l'instradamento tramite gli indirizzi IP privati di ciascun VPC come se si trovassero sulla stessa rete. Le connessioni peering VPC possono essere create tra i tuoi VPC o con un VPC in un altro account AWS. Il peering VPC supporta anche il peering interregionale.

Il traffico che utilizza il peering VPC interregionale rimane sempre sulla spina dorsale globale di AWS e non attraversa mai la rete Internet pubblica, riducendo così i vettori di minaccia, come gli exploit comuni e gli attacchi DDoS.



VPC-to-VPC Peering

AWS utilizza l'infrastruttura esistente di un VPC per creare connessioni peering VPC e non si basa su un hardware fisico separato. Pertanto, non introducono un potenziale punto di errore singolo o un

collo di bottiglia della larghezza di banda di rete tra i VPC. Inoltre, è possibile utilizzare le tabelle di routing VPC, i gruppi di sicurezza e gli elenchi di controllo degli accessi alla rete per controllare quali sottoreti o istanze sono in grado di utilizzare la connessione peering VPC.

Amazon VPC non supporta il peering transitivo, il che significa che non è possibile comunicare due VPC che non sono direttamente peerizzati utilizzando un terzo VPC come transito. Se desideri che tutti i tuoi VPC comunichino tra loro utilizzando il peering VPC, dovrai creare connessioni peering VPC 1:1 tra ciascuno di essi. In alternativa, puoi utilizzare AWS Transit Gateway o AWS Cloud WAN per fungere da hub di transito di rete.

Sia il traffico IPv4 che IPv6 sono supportati nelle connessioni peering VPC. Tuttavia, non è possibile effettuare il peering di due VPC se il blocco CIDR IPv4 primario si sovrappone, indipendentemente dai blocchi CIDR IPv4 o IPv6 secondari utilizzati. Tienilo in considerazione quando assegni il blocco CIDR primario ai tuoi VPC se prevedi di utilizzare il peering VPC tra di loro.

Risorse aggiuntive

- Peering con Amazon VPC
- Cos'è il peering VPC?

AWS Transit Gateway

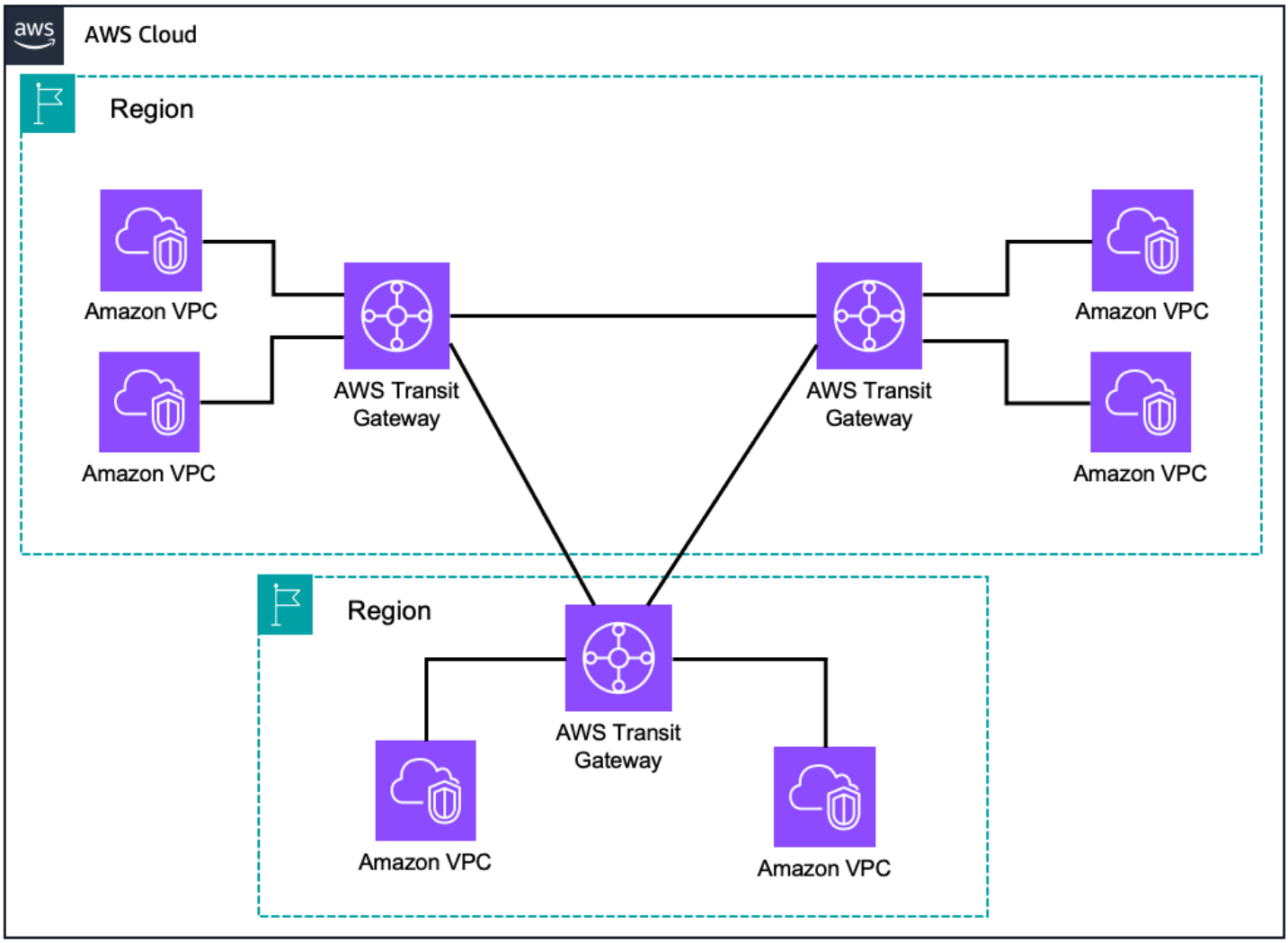
AWS Transit Gatewayè un servizio altamente disponibile e scalabile per consolidare la configurazione di routing VPC di AWS per una regione con un'architettura. hub-and-spoke Ogni VPC a pozze deve solo connettersi al Transit Gateway per accedere ad altri VPC connessi. Il traffico IPv4 e IPv6 è supportato in. AWS Transit Gateway

Puoi sfruttare diverse tabelle di routing, associazioni e propagazioni di Transit Gateway per segmentare il traffico all'interno dello stesso Transit Gateway. Sarete in grado di gestire diversi domini di routing (ad esempio, traffico di produzione e non di produzione) da un unico punto di gestione, assicurandovi che questi domini di routing non siano in grado di comunicare tra loro.

Puoi anche sfruttare l' hub-and-spoke architettura creata da Transit Gateway per centralizzare l'accesso a servizi condivisi come l'ispezione del traffico, l'interfaccia, l'accesso agli endpoint VPC o il traffico in uscita attraverso un gateway NAT o istanze NAT. Questa centralizzazione semplifica la complessità della gestione di queste risorse in diversi VPC e consente un controllo migliore man mano che estendi la tua presenza in AWS.

I Transit Gateway possono essere collegati tra loro all'interno della stessa regione AWS o tra diverse regioni AWS. AWS Transit Gatewayil traffico rimane sempre sulla spina dorsale globale di AWS e non attraversa mai la rete Internet pubblica, riducendo così i vettori di minaccia come gli exploit comuni e gli attacchi DDoS.

Con un gran numero di VPC, Transit Gateway offre una gestione più semplice delle comunicazioni da VPC a VPC tramite peering VPC, come mostrato nella figura seguente.



AWS Transit Gateway

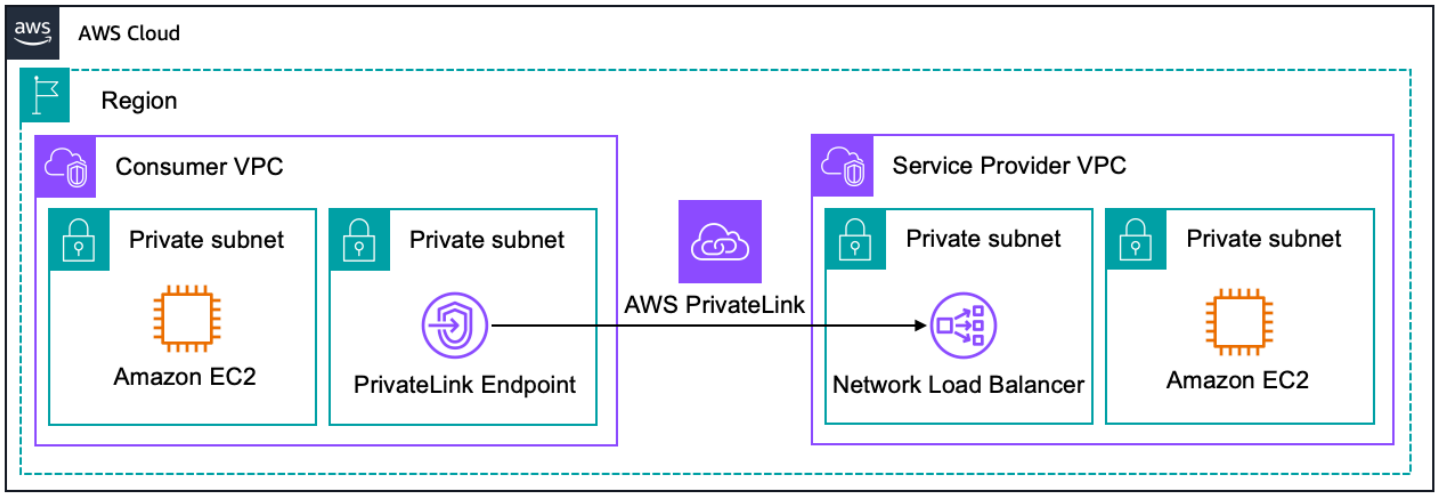
Per una visibilità centralizzata del traffico IP in entrata e in uscita dai tuoi Transit Gateway, puoi pubblicare i Transit Gateway Flow Logs su Amazon CloudWatch Logs e Amazon S3. I dati di log del flusso vengono raccolti al di fuori del percorso del traffico di rete e pertanto non influiscono sulla velocità effettiva o sulla latenza della rete.

Risorse aggiuntive

- Gateway di transito Amazon VPC
- Allegati di peering Transit Gateway
- Lavora con Transit Gateways
- Registrazione del traffico di rete tramite Transit Gateway Flow Logs

AWS PrivateLink

AWS PrivateLinkti consente di connetterti ad alcuni servizi AWS, servizi ospitati da altri account AWS (denominati servizi endpoint) e servizi Marketplace AWS partner supportati, tramite indirizzi IP privati nel tuo VPC. Gli endpoint dell'interfaccia vengono creati direttamente all'interno del tuo VPC, utilizzando interfacce di rete elastiche e indirizzi IP nelle sottoreti del tuo VPC. Ciò significa che i gruppi di sicurezza VPC possono essere utilizzati per gestire l'accesso agli endpoint.



AWS PrivateLink

Consigliamo questo approccio se desideri utilizzare i servizi offerti da un altro VPC in modo sicuro all'interno di una rete AWS, utilizzando indirizzi IP privati. In alternativa, AWS PrivateLink è una buona soluzione quando i VPC hanno indirizzi IP sovrapposti.

AWS PrivateLinksupporta completamente IPv6, ma entrambi i VPC di destinazione, le sottoreti VPC, il Network Load Balancer e i nomi DNS devono essere abilitati o modificati per utilizzare il dual-stack. Una volta soddisfatti questi prerequisiti, è possibile abilitare IPv6 nella configurazione del servizio per l'endpoint.

Controlli di accesso a AWS PrivateLink

Gli endpoint dell'interfaccia vengono creati direttamente all'interno del tuo VPC utilizzando interfacce di rete elastiche e indirizzi IP nelle sottoreti del tuo VPC. Ciò significa che i gruppi di sicurezza VPC possono essere utilizzati per gestire l'accesso di rete agli endpoint.

Quando crei un endpoint di interfaccia o un endpoint gateway, puoi anche allegare una policy per gli endpoint. La policy degli endpoint controlla quali responsabili AWS (account AWS, utenti IAM e ruoli) possono utilizzare l'endpoint VPC per accedere al servizio endpoint.

Non è possibile collegare più policy a un endpoint. Tuttavia, è possibile modificare la policy di endpoint in qualsiasi momento.

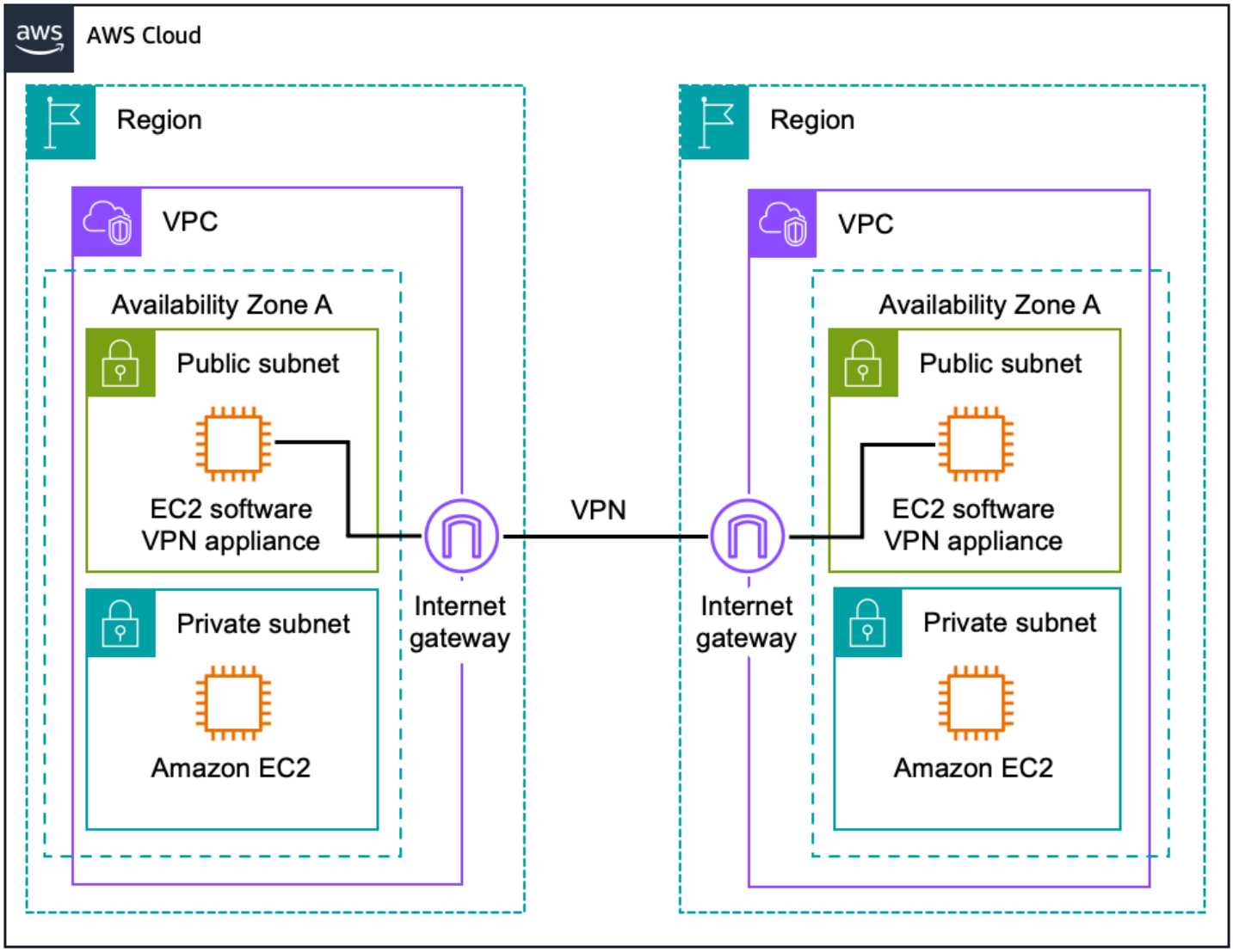
Una policy per gli endpoint non sovrascrive o sostituisce le policy degli utenti IAM o le policy specifiche dei servizi (come le policy dei bucket di Amazon S3). Se stai utilizzando un endpoint dell'interfaccia per connetterti ad Amazon S3, puoi anche utilizzare le policy dei bucket Amazon S3 per controllare l'accesso ai bucket da endpoint o VPC specifici.

Risorse aggiuntive

- Endpoint VPC di interfaccia () AWS PrivateLink
- Servizi endpoint VPC () AWS PrivateLink
- Post sul blog: Accelera l'adozione dell'IPv6 con servizi ed endpoint PrivateLink
- Post sul blog: Connessione di reti con intervalli IP sovrapposti
- AWS PrivateLinkPartner

Software VPN

Amazon VPC offre flessibilità di routing di rete. Ciò include la possibilità di creare tunnel VPN sicuri tra due o più appliance VPN software per connettere più VPC in una rete privata virtuale più ampia in modo che le istanze di ogni VPC possano connettersi tra loro senza problemi utilizzando indirizzi IP privati. Questa opzione è consigliata quando desideri gestire entrambe le estremità della connessione VPN utilizzando il tuo provider di software VPN preferito. Questa opzione utilizza un gateway Internet collegato a ciascun VPC per facilitare la comunicazione tra i dispositivi software VPN.



Software Site-to-Site VPN VPC-to-VPC Routing

Puoi scegliere tra un ecosistema di più partner e comunità open source che hanno prodotto appliance VPN software che funzionano su Amazon EC2. Oltre a questa scelta, spetta a te la responsabilità di gestire l'appliance software, inclusi configurazione, patch e aggiornamenti.

Tieni presente che questo design introduce un potenziale punto di errore singolo nella progettazione di rete poiché l'appliance VPN software viene eseguita su una singola istanza Amazon EC2. Per ulteriori informazioni, consulta Appendice A: Architettura HA di alto livello per istanze software VPN.

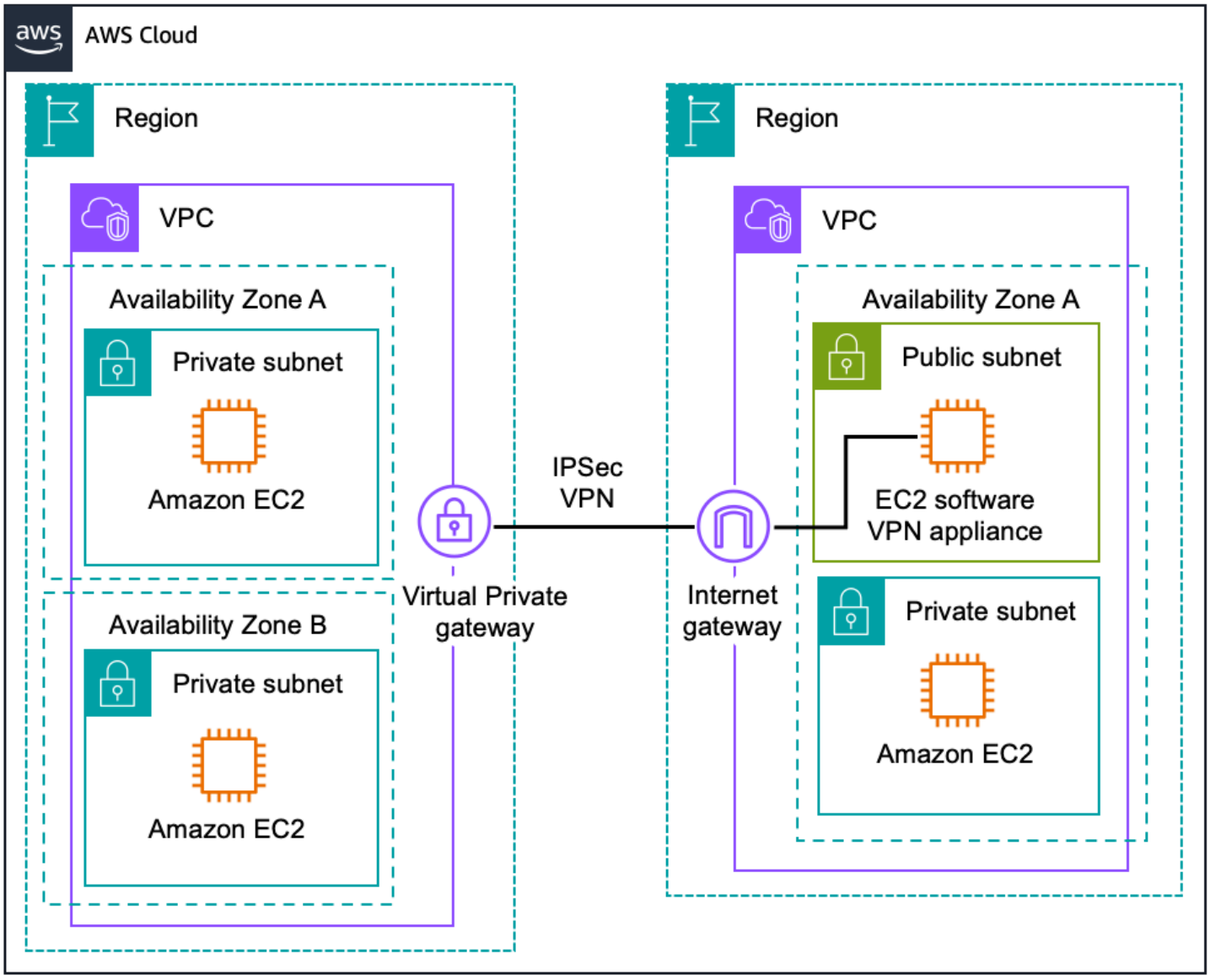
Risorse aggiuntive

- Apparecchiature VPN disponibili presso Marketplace AWS
- Descrizione tecnica - Connessione di più VPC con istanze EC2 (IPSec)

- Descrizione tecnica - Connessione di più VPC con istanze EC2 (SSL)

Software da VPN a VPN da sito a sito AWS

Amazon VPC offre la flessibilità necessaria per combinare le opzioni VPN gestite da AWS e VPN software per connettere più VPC. Con questo design, è possibile creare tunnel VPN sicuri tra un'appliance VPN software e un gateway privato virtuale, consentendo alle istanze di ciascun VPC di connettersi senza problemi tra loro utilizzando indirizzi IP privati. Questa opzione utilizza un gateway privato virtuale in un Amazon VPC e una combinazione di un gateway Internet e un'appliance VPN software in un altro Amazon VPC, come illustrato nella figura seguente.



Software VPN to AWS Site-to-Site VPN VPC-to-VPC Routing

Tieni presente che questo design introduce un potenziale punto di errore singolo nella progettazione della rete. Per ulteriori informazioni, consulta Appendice A: Architettura HA di alto livello per istanze software VPN.

Risorse aggiuntive

- Dispositivi VPN disponibili presso Marketplace AWS
- Guida per l'utente di AWS Site-to-Site VPN
- Requisiti per i dispositivi gateway del cliente

Accesso remoto del software alle opzioni di connettività Amazon VPC

Con la VPN per l'accesso remoto al software, puoi sfruttare servizi a basso costo, elastici e sicuri per implementare soluzioni di accesso remoto, fornendo al contempo un'esperienza di connessione senza interruzioni alle risorse ospitate da AWS. Questa opzione è in genere preferita dalle aziende più piccole con reti remote meno estese o che non hanno ancora creato e distribuito soluzioni di accesso remoto per i propri dipendenti.

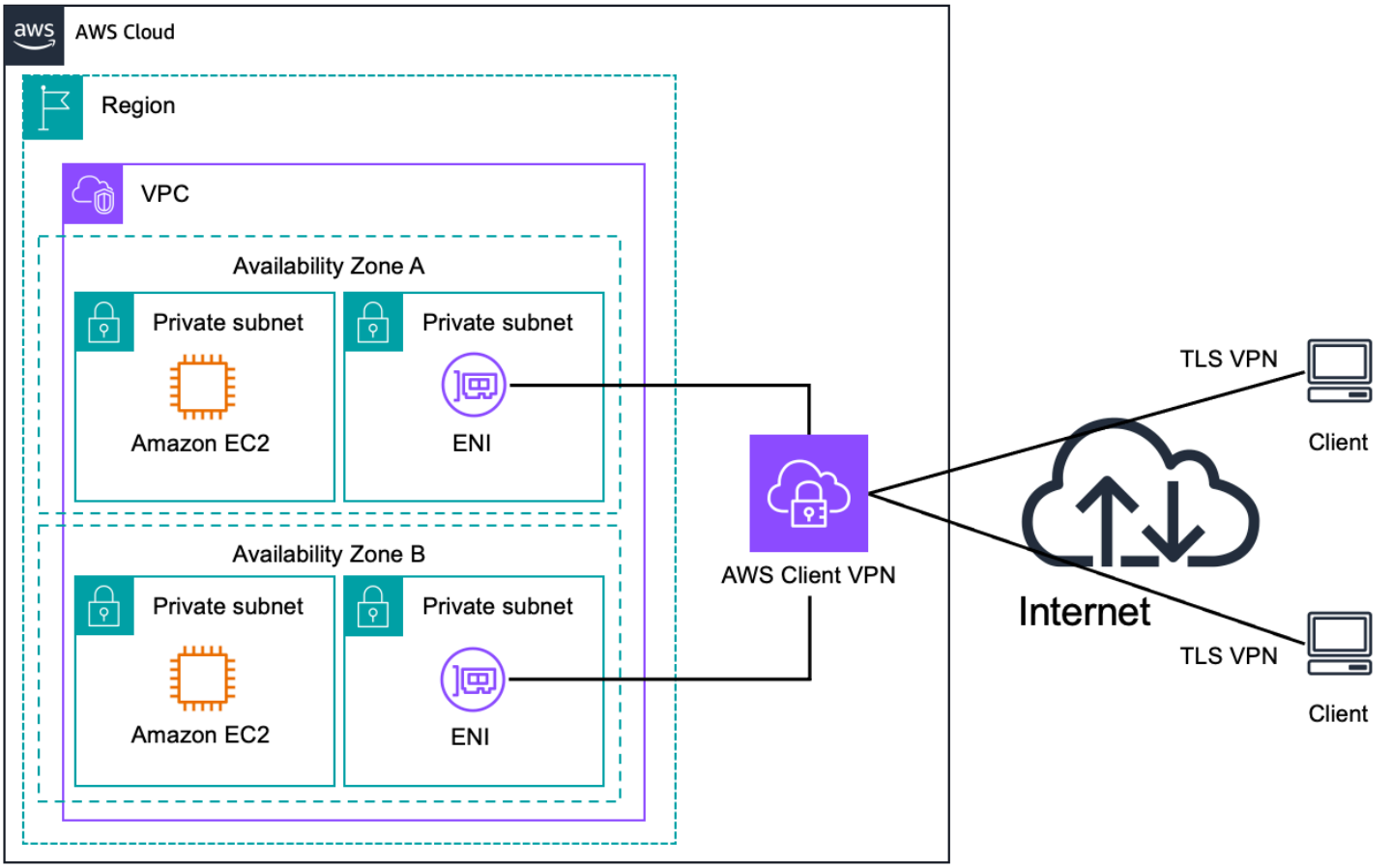
È possibile combinare questi modelli con le opzioni di Opzioni di connettività da rete ad Amazon VPC connettività e Opzioni di connettività da Amazon VPC ad Amazon VPC creare una rete che si estenda su reti remote e più VPC.

La tabella seguente illustra i vantaggi e i limiti di queste opzioni.

Opzione	Caso d'uso	Vantaggi	Limitazioni
AWS Client VPN	Soluzione di accesso remoto gestito da AWS ad Amazon VPC e/o reti interne	Servizio di alta disponibilità e scalabilità gestito da AWS	Solo client OpenVPN
Client software VPN	Soluzione di accesso remoto dell'appliance VPN software ad Amazon VPC e/o reti interne	Supporta una gamma più ampia di fornitori, prodotti e protocolli VPN Soluzione completamente gestita dal cliente	Sei responsabile dell'implementazione delle soluzioni HA

AWS Client VPN

AWS Client VPN è un servizio gestito da AWS ad alta disponibilità e scalabilità che consente l'accesso remoto sicuro al software. Offre la possibilità di creare una connessione TLS sicura tra i client remoti e i tuoi Amazon VPC, per accedere in modo sicuro alle risorse AWS e in locale tramite Internet, come mostrato nella figura seguente.



AWS Client VPN Remote Access

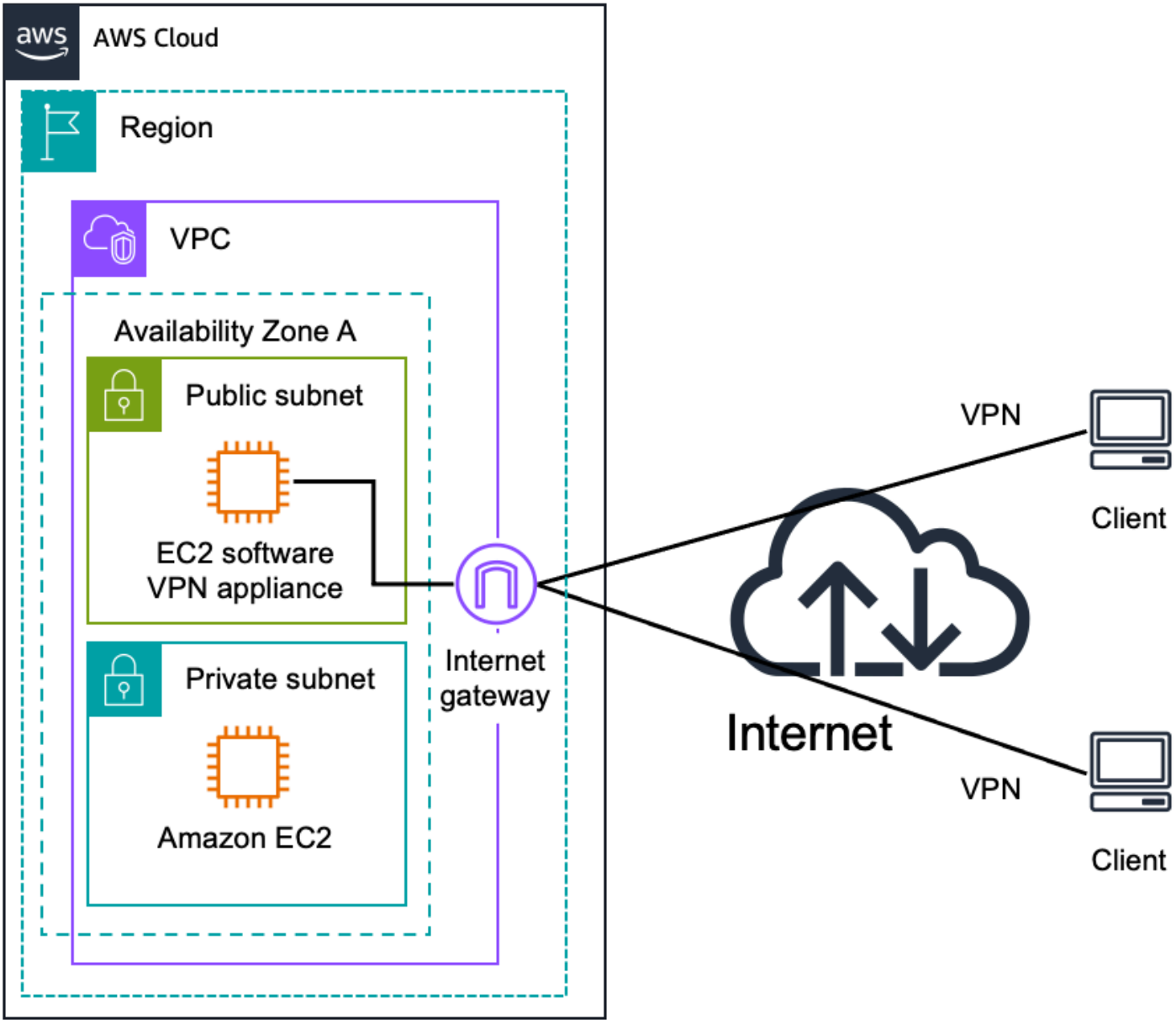
I client remoti possono essere AWS Client VPN for Desktop o client VPN OpenVPN di terze parti, con autenticazione tramite Active Directory o autenticazione con certificato reciproco.

Risorse aggiuntive

- Guida per l'amministratore di AWS Client VPN

Client software VPN

Puoi scegliere tra un ecosistema di più partner e comunità open source che hanno prodotto soluzioni di accesso remoto eseguite su Amazon EC2. Queste soluzioni offrono una grande flessibilità nell'uso del protocollo di sicurezza per l'accesso remoto ai tuoi Amazon VPC, per accedere in modo sicuro alle risorse AWS e in locale tramite Internet, come mostrato nella figura seguente.



Software Client VPN Remote Access

Le soluzioni di accesso remoto variano in complessità, supportano più opzioni di autenticazione client (inclusa l'autenticazione a più fattori) e possono essere integrate con Amazon VPC o con soluzioni di gestione delle identità e degli accessi ospitate in remoto (sfruttando una delle opzioni VPC da rete ad Amazon) come Microsoft Active Directory o altre soluzioni di autenticazione LDAP/multifattoriale.

Sei responsabile della gestione del software di accesso remoto, inclusa la gestione degli utenti, la configurazione, le patch e gli aggiornamenti. Questo design introduce un potenziale punto di errore singolo nella progettazione di rete poiché il server di accesso remoto viene eseguito su una singola

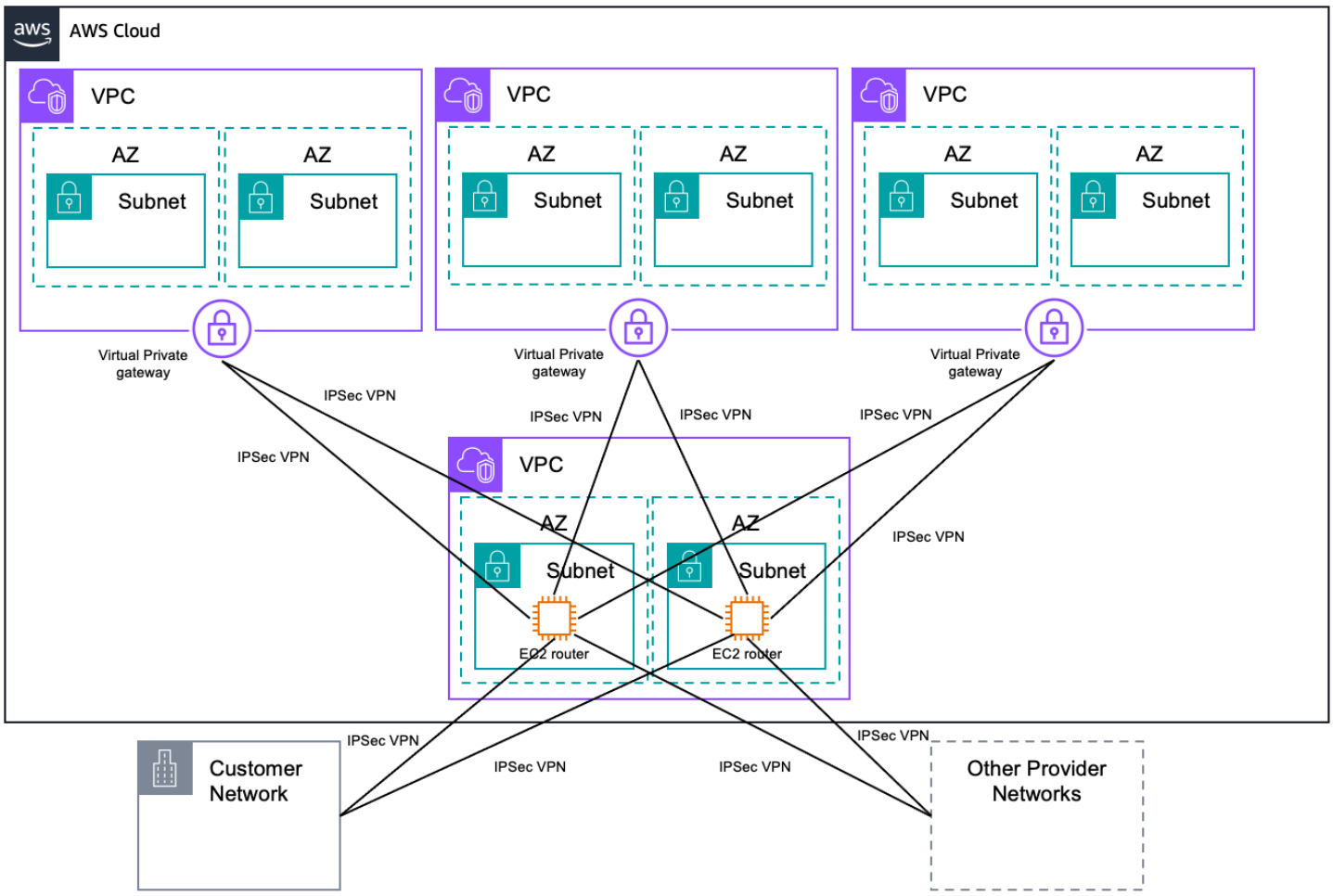
istanza Amazon EC2. Per ulteriori informazioni, consulta l'Appendice A: Architettura HA di alto livello per istanze VPN software.

Risorse aggiuntive

- Dispositivi VPN disponibili presso Marketplace AWS
- Guida introduttiva rapida a OpenVPN Access Server

VPC di transito

Basandoti sui progetti Software VPN sopra menzionati, puoi creare una rete di transito globale su AWS. Un VPC di transito è una strategia comune per connettere più VPC e reti remote distribuiti geograficamente al fine di creare un centro di transito di rete globale. Un VPC di transito semplifica la gestione della rete e riduce al minimo il numero di connessioni necessarie per connettersi a più VPC e reti remote. La figura seguente illustra questo design.



Transit VPC

Oltre a fornire un routing di rete diretto tra VPC e reti locali, questo design consente anche al VPC di transito di implementare regole di routing più complesse, come la traduzione degli indirizzi di rete tra intervalli di rete sovrapposti o di aggiungere ulteriori filtri o ispezioni dei pacchetti a livello di rete. Il design VPC di transito può essere utilizzato per supportare casi d'uso importanti come reti private, connettività condivisa e utilizzo di AWS tra account.

Risorse aggiuntive

- AWS Transit Gateway
- Cisco Catalyst 8000V per SD-WAN e routing in Marketplace AWS

WAN nel cloud AWS

AWS Cloud WAN è una rete WAN (Managed Wide Area Network) gestita dagli intenti, descritta da una policy definita dall'utente che unifica data center, filiali e reti AWS. Sebbene sia possibile creare la propria rete globale interconnettendo più gateway di transito tra regioni, Cloud WAN offre funzionalità integrate di automazione, segmentazione e gestione della configurazione progettate specificamente per la creazione e la gestione di reti globali, in base alla politica di rete di base. Cloud WAN ha aggiunto funzionalità come allegati VPC automatizzati, monitoraggio integrato delle prestazioni e configurazione centralizzata.

La policy di rete di base è scritta in un linguaggio dichiarativo che definisce i segmenti, il routing della regione AWS e il modo in cui gli allegati devono essere mappati ai segmenti. Con una policy di rete di base, puoi descrivere il tuo intento per il controllo degli accessi e il routing del traffico, mentre AWS Cloud WAN gestisce i dettagli della configurazione di rete.

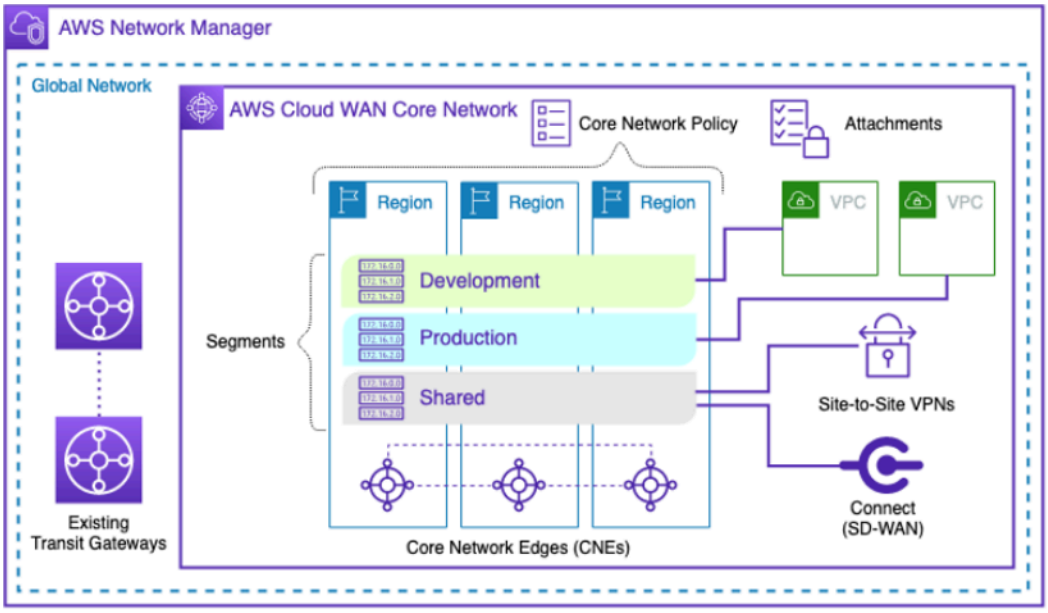
Cloud WAN è gestito all'interno di AWS Network Manager, che consente di gestire e visualizzare centralmente la rete principale Cloud WAN e le reti Transit Gateway su account AWS, regioni e sedi locali. Network Manager offre diverse visualizzazioni di dashboard per aiutarti a visualizzare e monitorare tutti gli aspetti della tua rete globale. Alcune delle dashboard includono:

- Mappe del mondo che indicano dove si trovano le risorse di rete, come postazioni periferiche, dispositivi e allegati.
- Monitoraggio che utilizza CloudWatch Events per tenere traccia di statistiche di 15 mesi, offrendoti una prospettiva migliore sulle prestazioni delle tue reti.
- Monitoraggio degli eventi che trasmette gli eventi in tempo reale a una dashboard degli eventi.
- Diagrammi topologici e logici delle reti di gateway di transito e dei gateway di transito.

Sia Transit Gateway che Cloud WAN consentono una connettività centralizzata tra VPC e sedi locali. Transit Gateway è un hub di connettività di rete regionale ed è ottimale per i clienti che operano in alcune regioni AWS, desiderano gestire la propria configurazione di peering e routing o preferiscono utilizzare la propria automazione. Il cloud WAN è ottimale per i clienti che desiderano definire la propria rete globale tramite policy e fare in modo che il servizio implementi automaticamente i componenti sottostanti.

Da sapere

- CNE (Core network edge) eredita molte caratteristiche del Transit Gateway, come la velocità effettiva per allegato VPC.
- Cloud WAN supporta sia IPv4 che IPv6.
- Attualmente, Cloud WAN non supporta nativamente gli allegati. AWS Direct Connect Per utilizzarlo AWS Direct Connect con Cloud WAN, è necessario un Transit Gateway collegato a un AWS Direct Connect gateway e quindi il Transit Gateway peer su Cloud WAN.
- Per reti di grandi dimensioni con molte modifiche, prendi in considerazione la creazione di una rete globale di sviluppo e test separata in cui convalidare le modifiche.



AWS Cloud WAN

Risorse aggiuntive

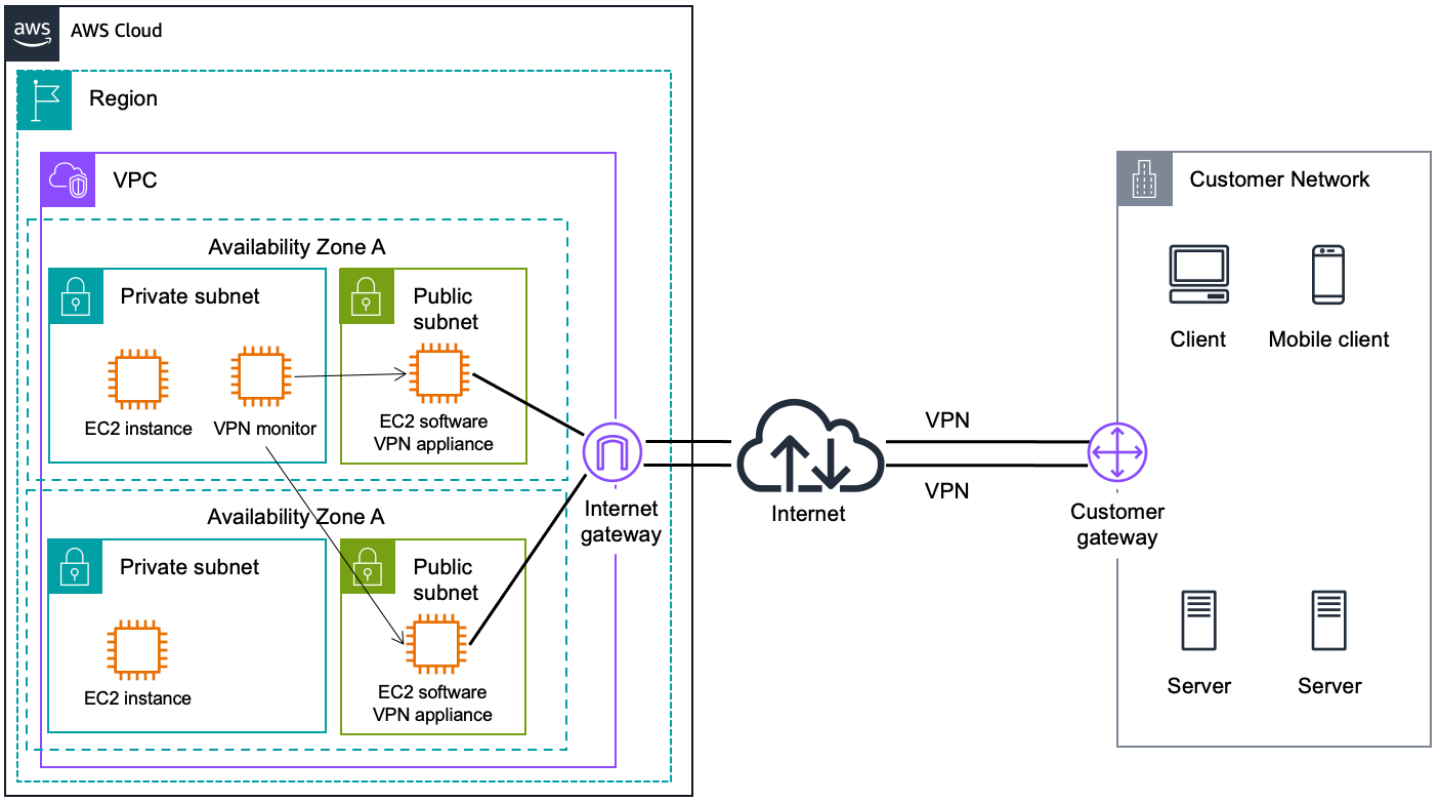
- Documentazione AWS Cloud WAN
- Post del blog: Modelli di migrazione e interoperabilità di AWS Cloud WAN e AWS Transit Gateway

Conclusione

AWS offre una serie di opzioni di connettività efficienti e sicure per aiutarti a ottenere il massimo da AWS in caso di integrazione delle reti remote mediante Amazon VPC. Le opzioni fornite in questo whitepaper evidenziano diverse opzioni e modelli di connettività utilizzati dai clienti per integrare con successo le loro reti remote o più reti Amazon VPC. È possibile utilizzare le informazioni fornite qui per determinare il meccanismo più appropriato per connettere l'infrastruttura necessaria per gestire la propria azienda indipendentemente da dove si trova fisicamente o in hosting.

Appendice A: Architettura HA di alto livello per istanze software VPN

La creazione di una connessione VPC completamente resiliente per le istanze VPN software richiede l'installazione e la configurazione di più istanze VPN e un'istanza di monitoraggio per monitorare lo stato delle connessioni VPN.



Software di alto livello VPN HA

Ti consigliamo di configurare le tabelle di routing VPC per sfruttare tutte le istanze VPN contemporaneamente, indirizzando il traffico da tutte le sottoreti di una zona di disponibilità attraverso le rispettive istanze VPN nella stessa zona di disponibilità. Ogni istanza VPN fornisce quindi connettività VPN per le istanze che condividono la stessa zona di disponibilità.

Monitoraggio VPN

Per monitorare un'appliance VPN basata su software, puoi creare un VPN Monitor. Il monitor VPN è un'istanza personalizzata di cui avrai bisogno per eseguire gli script di monitoraggio VPN. Questa istanza ha lo scopo di eseguire e monitorare lo stato della connessione VPN e delle istanze

VPN. Se un'istanza o una connessione VPN si interrompe, il monitor deve arrestare, terminare o riavviare l'istanza VPN e allo stesso tempo reindirizzare il traffico dalle sottoreti interessate all'istanza VPN funzionante fino a quando entrambe le connessioni non saranno nuovamente funzionanti. Poiché i requisiti dei clienti variano, AWS attualmente non fornisce linee guida prescrittive per la configurazione di questa istanza di monitoraggio. Tuttavia, uno script di esempio per abilitare l'HA tra le istanze NAT potrebbe essere utilizzato come punto di partenza per creare una soluzione HA per le istanze Software VPN. Ti consigliamo di riflettere sulla logica aziendale necessaria per fornire notifiche o tentare di ripristinare automaticamente la connettività di rete in caso di errore di connessione VPN.

Inoltre, puoi monitorare i tunnel AWS Managed VPN utilizzando Amazon CloudWatch metrics, che raccoglie i punti dati dal servizio VPN in metriche leggibili e quasi in tempo reale. Ogni connessione VPN raccoglie e pubblica una varietà di metriche del tunnel su Amazon. CloudWatch Queste metriche consentono di monitorare lo stato e l'attività del tunnel e di creare azioni automatizzate.

Collaboratori

Hanno collaborato alla stesura del presente documento:

- Daniel Yu, Senior Technical Account Manager, AWS Enterprise Support
- Garvit Singh, Solutions Builder, Architettura della soluzione AWS
- Steve Morad, Senior Manager, Solution Builders, AWS Solution Architecture
- Sohaib Tahir, architetto di soluzioni, architettura della soluzione AWS
- Fiona Armada, Principal Solutions Architect, AWS Solution Architecture
- Pablo Sánchez Carbona, Architetto di soluzioni specializzato in reti, AWS Solution Architecture
- Tony Hawke, Account Manager tecnico specializzato in reti senior, AWS Enterprise Support

Revisioni del documento

Per ricevere notifiche sugli aggiornamenti di questo white paper, iscriviti al feed RSS.

Modifica	Descrizione	Data
Whitepaper aggiornato	Sono state aggiunte le opzioni di collegamento di AWS Cloud WAN e Transit Gateway Connect, diagrammi e informazioni aggiornati in tutto.	5 aprile 2023
Whitepaper aggiornato	Aggiunte le opzioni AWS Transit Gateway e AWS Client VPN, diagrammi e informazioni aggiornati in tutto.	6 giugno 2020
Aggiornamento secondario	Piccola modifica per correggere il riferimento all'appliance VPN software.	20 maggio 2020
Whitepaper aggiornato	Informazioni sempre aggiornate. Concentrati sui seguenti design/funzionalità: VPC di transito, gateway Direct Connect e. AWS PrivateLink	1 gennaio 2018
Pubblicazione iniziale	Pubblicate le opzioni di connettività di Amazon Virtual Private Cloud.	1 luglio 2014

Avvisi

I clienti sono responsabili della propria valutazione autonoma delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) mostra le offerte e le pratiche attuali dei prodotti AWS soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte di AWS e dei suoi affiliati, fornitori o licenziatari. I prodotti o servizi AWS sono forniti "così come sono" senza garanzie, dichiarazioni o condizioni di alcun tipo, sia esplicite che implicite. Le responsabilità e gli obblighi di AWS verso i propri clienti sono disciplinati dagli accordi AWS e il presente documento non fa parte né modifica alcun accordo tra AWS e i suoi clienti.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.