netskope

5 segni rivelatori che indicano che la tua VPN è in difficoltà

Un tempo, le reti private virtuali (VPN) erano considerate tecnologicamente all'avanguardia e offrivano agli utenti remoti un modo semplice e sicuro per accedere alle risorse protette sulle reti aziendali. Ma attualmente, le VPN hanno difficoltà a stare al passo con il lavoro ibrido e le minacce correnti. Per troppo tempo, le aziende hanno esteso e aggiornato la loro infrastruttura VPN esistente, tollerando i conseguenti problemi di prestazioni della rete e le vulnerabilità della sicurezza. È tempo di riconsiderare la nostra continua dipendenza da questa tecnologia legacy. Ecco cinque segni rivelatori che indicano che la tua VPN è in difficoltà e segnalano la necessità di esplorare alternative di accesso più moderne come Zero Trust Network Access (ZTNA).

1 Rallenta i tuoi utenti

Le configurazioni VPN tradizionali effettuano il backhaul del traffico degli utenti remoti a un data center centralizzato attraverso uno stack di sicurezza in entrata, per applicare le politiche aziendali. Questo approccio alla sicurezza della rete, spesso chiamato modello “castello e fossato” (castle-and-moat), diventa un collo di bottiglia quando le applicazioni sono sul cloud o gli utenti sono lontani dal data center.

Hai l'impressione che la tua rete sia in difficoltà? Il backhauling comporta un notevole aumento della latenza e causa notevoli ritardi, che incidono direttamente sulla produttività e sulla soddisfazione dei dipendenti. Occorre tenere d'occhio questi segnali; potrebbero essere solo un campanello d'allarme che indica che l'organizzazione deve rivalutare la propria architettura di rete.

2 Si è sommersi da problemi tecnici e patch

Ogni mese sembra portare nuovi avvisi di sicurezza per le VPN. Il database CVE pubblicamente disponibile elenca quasi 700 vulnerabilità relative alle VPN. Notoriamente piene di bug, le VPN rappresentano una miniera d'oro per gli aggressori. Un singolo exploit riuscito può dare l’accesso senza restrizioni a livello di sistema alla rete aziendale, diventando un gateway per gli attacchi ransomware e il furto di dati.

Un flusso infinito di patch unito a un backlog in crescita segnala che la VPN è in difficoltà. Questo può essere travolgente, soprattutto se non si dispone delle risorse richieste per restare al passo con tutti gli aggiornamenti da applicare alle VPN. Data l'ampia superficie di attacco hardware e software da proteggere, i rischi possono penetrare con facilità attraverso le crepe, lasciando i sistemi esposti e vulnerabili.

3 La sua gestione richiede troppo tempo e troppe risorse

Per gli amministratori non è facile decidere come impostare le politiche VPN: optare per politiche ampie e aperte e affrontare potenziali rischi di sicurezza, o imporne di restrittive, bloccando gli utenti e impantanandosi in operazioni manuali di fornitura o risoluzione dell'accesso. Per complicare ulteriormente le cose, molte aziende implementano anche regole firewall con la propria VPN.

Quando la gestione delle politiche VPN diventa fonte di complessità e un peso in termini di risorse per gestirla, mantenerla e controllarla, è evidente che ci si trova in una situazione è difficile. Si consideri la ricerca di alternative in grado di bilanciare l'accessibilità con la sicurezza, senza richiedere interventi manuali per gestire le politiche e le richieste di accesso.

4 L'accesso di terze parti è fuori controllo

Solitamente, le organizzazioni forniscono ai collaboratori terzi l'accesso ai sistemi interni tramite VPN, ma questo implica sfide uniche per i team I&O. Gran parte dei collaboratori terzi opera su endpoint non gestiti, rendendo l'implementazione del client VPN aziendale poco pratica e non certo benvenuta. Inoltre, questi utenti richiedono solitamente solo l'accesso a una manciata di applicazioni, spesso però accumulando autorizzazioni troppo ampie che aumentano il rischio di utilizzi impropri e compromissioni.

Gestire l'accesso di terzi non è facile quando si ha a che fare con dispositivi non gestiti e con la mancanza di strumenti adeguati e granulari. Si ha visibilità sugli utenti esterni che si connettono alla propria rete e su come tale accesso viene utilizzato? Occorre evitare questo problema dell'accesso di terzi con un'alternativa senza agenti.

5 I reclami VoIP stanno colpendo l'help desk

Se i team dei call center remoti hanno problemi con chiamate VoIP interrotte, lente o perse, il problema potrebbe essere la VPN. I protocolli VoIP e UCaaS sono molto sensibili alle condizioni della rete e richiedono connessioni stabili e ininterrotte per mantenere la qualità delle chiamate: anche il minimo intoppo può portare a un degrado significativo.

Il backhauling del traffico VoIP attraverso una VPN al data center aziendale può introdurre perdite di pacchetti, jitter e latenza, impattando l'esperienza utente e la produttività complessiva. Se questo risulta fin troppo familiare, ecco un altro segnale rivelatore di come la VPN sia in difficoltà. Forse è il momento di riconsiderare la soluzione di accesso remoto ed esplorare alternative di più facile utilizzo per ridurre il carico sul servizio di help desk.

La presenza di uno qualsiasi di questi segnali indica che è arrivato il momento di cambiare! Scopri le possibilità offerte da Netskope

Netskope One Private Access

Scopri di più

netskope