

I 5 rischi principali dei firewall perimetrali e come superarli

I firewall sono da tempo parte integrante dell'architettura di rete delle aziende. Tuttavia, con il passaggio ai modelli di business digitali, il firewall è passato dall'essere un solido punto di riferimento per la sicurezza a rappresentare un vero e proprio rischio. Ecco perché.

In un'architettura di sicurezza tradizionale basata sul perimetro che utilizza firewall e VPN, la sicurezza si limita al perimetro o alla zona di attendibilità. Tutte le applicazioni o gli utenti all'interno di quest'area sono considerati attendibili, mentre quelli esterni sono considerati malevoli. Questo sistema funzionava bene quando la maggior parte degli utenti e delle applicazioni si trovavano all'interno del perimetro. Chiunque si trovasse all'esterno del perimetro doveva essere portato sulla rete attraverso l'estensione del perimetro. Questa pratica era considerata un'eccezione che consentiva di includere queste entità all'interno della zona di attendibilità.

Il modo di lavorare delle aziende è cambiato notevolmente da quando sono stati introdotti i firewall. I dipendenti aziendali di oggi possono lavorare ovunque: a casa, in spazi di lavoro condivisi, nelle filiali e in qualsiasi altro luogo; basta avere a disposizione una connessione Internet e una fonte di alimentazione. Estendere il perimetro a ogni utente in remoto non è più efficiente, perché applicazioni e utenti distribuiti rappresentano ormai la norma, e non più un'eccezione. Il concetto di zona attendibile non è più applicabile, perché oggi le applicazioni e gli utenti possono essere ovunque. Questo richiede il passaggio a un modello zero trust. Tuttavia, un vero modello zero trust non può essere implementato con firewall e VPN, e sono diversi i rischi associati all'uso di queste soluzioni tradizionali.

In questo articolo, descriveremo nel dettaglio i cinque principali rischi associati all'utilizzo dei firewall in un mondo cloud e mobile, e scopriremo come superarli adottando un approccio zero trust moderno.

Ampia superficie di attacco

Per superficie di attacco si intende la somma di tutti i punti esposti, come gli indirizzi IP, che possono consentire agli aggressori di individuare le vulnerabilità, dirigersi verso di esse e sfruttarle per accedere al sistema ed estrarre dati preziosi. In poche parole, più la superficie di attacco è ridotta, più è difficile che gli aggressori riescano ad accedervi. Tuttavia la distribuzione delle applicazioni sul cloud e l'aumento della forza lavoro mobile hanno ampliato in modo esponenziale questa superficie, rendendo le organizzazioni e le aziende più vulnerabili che mai. L'uso di firewall fisici e virtuali basati sul perimetro non solo non riesce a risolvere questo problema, ma arriva persino a peggiorarlo, perché estende la superficie di attacco consentendo agli aggressori di ottenere un punto di accesso alla rete o all'istanza cloud.

In che modo? I firewall pubblicano gli indirizzi IP dei server e delle applicazioni su Internet per essere trovati da dipendenti e partner, ma questo significa che anche gli aggressori sono in grado di rilevarli. Ogni firewall esposto a Internet, che si trovi nel data center, sul cloud o in una filiale, può essere individuato, attaccato e sfruttato. I firewall virtuali sono rischiosi tanto quanto le loro controparti fisiche, perché anch'essi espongono gli IP a Internet, spesso molto di più rispetto ai firewall fisici, incrementando ulteriormente il rischio.

Come eliminare la superficie di attacco con lo zero trust

Eliminare la superficie di attacco è il segreto per proteggere la rete, le applicazioni e, soprattutto, i dati. Una vera soluzione zero trust fa sì che le applicazioni diventino entità non instradabili, quindi invisibili ai potenziali aggressori, in modo che le risorse aziendali non possano essere individuate su Internet. Una vera piattaforma zero trust si pone tra l'utente e l'applicazione. Così facendo, tutte le comunicazioni passano attraverso di essa, e nulla raggiunge le applicazioni senza il consenso della piattaforma.

Questo approccio è radicalmente diverso rispetto a quello dei firewall perimetrali, perché vengono consentite solo connessioni dall'interno verso l'esterno, al contrario dell'approccio tradizionale, che ammette connessioni dall'esterno verso l'interno e che richiede la pubblicazione degli indirizzi. Rendendo le app invisibili agli aggressori e accessibili solo agli utenti autorizzati, la superficie di attacco viene praticamente azzerata e l'accesso alle applicazioni su Internet, SaaS e nei cloud pubblici o privati è sempre sicuro.

Rilevamento della superficie di attacco

Le superfici di attacco possono essere difficili da individuare manualmente, ma servizi come l'analisi della superficie di attacco Internet forniscono visibilità sulla superficie di attacco complessiva, e consentono di individuare server, spazi dei nomi, vulnerabilità, e istanze cloud che sono attualmente visibili su Internet. La valutazione interroga le fonti pubbliche per rivelare eventuali aree di esposizione che generano rischi. In questo modo, le aziende possono valutarle, analizzarle ed eliminarle grazie allo zero trust.

Strozzamento delle prestazioni delle applicazioni

Gli utenti ormai si aspettano una certa reattività dalle applicazioni cloud che utilizzano nella loro vita privata. Tuttavia, l'esperienza degli utenti è significativamente più scarsa quando accedono alle applicazioni aziendali con le soluzioni di accesso alla rete dell'azienda, perché non godono di un accesso rapido e diretto alle applicazioni cloud. Di conseguenza, la produttività degli utenti diminuisce, e la collaborazione diventa più difficoltosa a causa dell'abbassamento delle prestazioni delle applicazioni. È per questo motivo che in molti sono indotti a bypassare i controlli di sicurezza, una pratica particolarmente rischiosa, soprattutto quando si utilizzano dispositivi non gestiti o reti Wi-Fi domestiche o non protette. I problemi prestazionali dell'utente finale sono anche causati dalla disponibilità di applicazioni SaaS o cloud, dalla capacità del dispositivo, dalle interruzioni del percorso di rete o dalla congestione della rete, tutti fattori che non sono facilmente isolabili e diagnosticabili dall'operatore.

Perché? L'architettura di rete "hub and spoke" richiede che le sedi in remoto e le filiali si colleghino all'ufficio centrale (data center) tramite firewall con MPLS e agli utenti in remoto con una VPN. Questa architettura crea una rete di tipo "flat" che si estende a tutte le posizioni e prevede che tutto il traffico di rete fluisca verso un set centralizzato di soluzioni di sicurezza. L'invio del traffico proveniente da un utente in remoto al data center e in seguito verso il cloud, per poi tornare all'utente e seguire lo stesso percorso al contrario, aumenta significativamente la latenza e peggiora l'esperienza utente. I firewall virtuali nel cloud subiscono la stessa sorte, in quanto il traffico deve essere reindirizzato verso di essi allo stesso modo in cui questo avviene per i data center fisici, perché non sono inline con i server delle applicazioni.

Le applicazioni cloud sono state progettate per offrire l'accesso diretto, con il minor numero possibile di hop, per massimizzare le prestazioni. Di conseguenza, molti provider di applicazioni SaaS (ad esempio Microsoft 365) indicano espressamente che, per un supporto completo, non devono essere impiegati i firewall.

Come superare i problemi prestazionali con lo zero trust

Un'architettura zero trust si allontana dal concetto di rete tradizionale "hub and spoke" e di sicurezza a castello e fossato. Fornisce una connettività diretta alle applicazioni e riduce i rischi, offrendo al contempo un'esperienza utente di livello superiore.

Una piattaforma zero trust efficace applica le policy inline, all'edge, e non sono quindi necessari ulteriori hop; inoltre, il peering diretto con le società delle applicazioni consente di ottenere una connessione diretta in base alla disponibilità e alla capacità. Operando nel percorso dati, una piattaforma zero trust può inoltre monitorare ogni connessione e individuare e risolvere automaticamente i problemi prestazionali. Questa funzionalità è fondamentale per le applicazioni a bassa latenza, ad esempio le applicazioni UCaaS (Unified Communications as a Service) come Microsoft Teams e Zoom. La possibilità di monitorare queste applicazioni e risolvere rapidamente i problemi, grazie alle funzionalità di monitoraggio dell'esperienza digitale (DEM, Digital Experience Monitoring), consente alle organizzazioni di identificare e risolvere i problemi prima che gli utenti ne subiscano le conseguenze, migliorando così la collaborazione e la produttività.

Valutazione dell'esperienza utente

*L'esperienza utente può essere valutata utilizzando uno **strumento di monitoraggio** avanzato che fornisce informazioni sull'esperienza digitale per comprendere, diagnosticare e migliorare i problemi relativi all'utilizzo di applicazioni all'interno dell'organizzazione. Il punteggio consente di identificare le anomalie utilizzando il machine learning e di ottenere informazioni concrete.*

Complessità operativa e costi elevati

L'utilizzo di firewall, MPLS e VPN, o persino di appliance virtuali, non rappresenta un approccio efficace per l'implementazione dello zero trust. Gestire e implementare firewall perimetrali per garantire una sicurezza uniforme a tutti gli utenti, alle applicazioni, ai dispositivi e alle sedi è troppo complesso e costoso. L'azienda non è in grado di garantire la scalabilità per gestire la distribuzione delle policy nel perimetro, gli aggiornamenti e l'applicazione delle patch. L'hardware e i firewall virtuali devono essere acquistati e distribuiti solo in casi estremi, e il backhauling del traffico verso un singolo set di soluzioni di sicurezza impiega eccessiva larghezza di banda e consuma troppe risorse.

Il processo di capacity planning, o pianificazione della capacità, richiede ai CIO e ai CISO di prevedere con precisione il futuro, per stimare i requisiti relativi all'hardware e i costi di consumo della larghezza di banda necessari per inviare tutto il traffico su MPLS al data center per l'ispezione. Sottovalutare le esigenze di rete compromette le prestazioni, mentre sopravvalutarle significa andare incontro a costi inutilmente elevati e ad apparecchiature che rimangono inattive. Inoltre, non è possibile distribuire lo stesso identico set di appliance in ogni sede, e questo porta all'accumulo di prodotti eterogenei nell'infrastruttura. La raccolta e la gestione dei log per tutti questi dispositivi rappresenta un'altra difficoltà, e gli operatori spesso trascurano i log critici, con un conseguente rischio per la sicurezza. Il 75% degli operatori ritiene che la gestione dell'hardware, degli aggiornamenti e delle distribuzioni dei firewall sia un'attività complessa e difficoltosa.[2]

E questa è solo una parte della sfida. Questo approccio frammentato richiede al personale addetto alla sicurezza di utilizzare servizi e piattaforme di gestione separate per implementare policy diverse e gestire zone diverse con la segmentazione della rete. Bisogna inoltre ricollegare le informazioni di visibilità ottenute per ogni utente, applicazione e posizione. I dipendenti devono dedicarsi a tempo pieno a implementare patch, eseguire aggiornamenti, aggiornare l'hardware e gestire policy su tutto questo insieme incoerente di dispositivi firewall e di sicurezza. È un insieme di attività che prosciuga le finanze e la produttività, e non è sostenibile.

Come evitare la complessità con lo zero trust

Invece di molteplici hardware o soluzioni cloud ad hoc difficili da gestire, una soluzione zero trust integrata protegge tutte le applicazioni SaaS, Internet e private con un'unica piattaforma. Lo zero trust elimina la necessità di costose reti MPLS che richiedono operazioni complesse di routing, switching, segmentazione di rete e altro, e offre un accesso diretto, rapido e sicuro al cloud e una connettività tra cloud affidabile. La necessità di eseguire il backhauling del traffico verso il data center viene praticamente eliminata. Una piattaforma zero trust unificata, con una singola console di gestione, è molto più rapida da configurare, più facile da gestire, dispone di policy semplificate e offre una maggiore sicurezza rispetto alla sicurezza tradizionale del perimetro.

Con una soluzione zero trust con base cloud, i controlli di sicurezza si trovano dove si trovano anche gli utenti e le applicazioni, e cioè sul cloud. Grazie alla visibilità su tutti gli utenti, i cloud e i carichi di lavoro, lo zero trust semplifica le operazioni e la risoluzione dei problemi. Il passaggio al cloud riduce il carico relativo all'acquisto, alla gestione, alla manutenzione e al controllo di firewall e altro hardware di sicurezza, e consente ai team IT di avere più tempo a disposizione per concentrarsi su altri progetti. Infine, una soluzione zero trust cloud permette alle aziende di garantire una rapida scalabilità all'aumentare del volume di utenti e applicazioni.

Costi

*L'indagine **sui rischi associati alle VPN** del 2021 ha concluso che l'elevato costo dei dispositivi e delle infrastrutture per la sicurezza rappresenta la seconda sfida più grande che le aziende si trovano a dover affrontare con la loro soluzione di accesso remoto. Le aziende che hanno adottato lo zero trust tramite **Zero Trust Exchange** hanno ottenuto in media un ROI del 139% e vantaggi pari a 4,1 milioni di dollari, con maggiore produttività, meno incidenti e meno dispositivi.[3]*

Movimento laterale delle minacce

Gli aggressori utilizzano vari mezzi per accedere alla rete di un'azienda, spesso impiegando attacchi di phishing o infezioni da malware. Quando sono nella rete, il loro obiettivo è quello di spostarsi lateralmente all'interno dell'organizzazione, nel tentativo di accedere ai dati sensibili per esfiltrarli, criptarli, richiedere riscatti o causare interruzioni di altro tipo. Il movimento laterale consente agli aggressori di non essere rilevati e di mantenere l'accesso, anche se vengono individuati sul primo computer infettato. E quando il periodo di permanenza è lungo, il furto dei dati potrebbe non verificarsi per settimane, o addirittura per mesi, dopo la violazione originale.

Per proteggere i dati da attacchi, le aziende si sono tradizionalmente affidate a un approccio a "castello e fossato" per la sicurezza, noto anche come "sicurezza del perimetro". Come per i castelli medievali che venivano protetti da muri in pietra, fossati e cancelli, la sicurezza del perimetro punta a fortificare il perimetro della rete con firewall e altri strumenti. In questo modo vengono protetti i punti di ingresso e di uscita della rete, con la verifica dei pacchetti di dati e dell'identità degli utenti che entrano ed escono. Questo approccio presuppone quindi che l'attività all'interno del perimetro fortificato sia relativamente sicura.

Le architetture di sicurezza tradizionali non sono in grado di bloccare gli attacchi sofisticati, perché una volta che l'utente entra in una rete "protetta", viene considerato automaticamente attendibile e ottiene l'accesso laterale a tutte le applicazioni, anche se non dovrebbe. La riduzione del movimento laterale nelle architetture perimetrali richiede la segmentazione della rete (perimetri interni), che è un'operazione molto complessa, in quanto richiede alle aziende di distribuire e gestire più firewall con molteplici policy, senza comunque riuscire a risolvere adeguatamente il problema alla base.

Come superare il movimento laterale con lo zero trust

Lo zero trust impedisce il movimento laterale, perché collega direttamente gli utenti e i carichi di lavoro alle applicazioni, e mai alla rete aziendale. Questo significa che le minacce non possono propagarsi lateralmente per infettare altri dispositivi e applicazioni, e non vi è la necessità di una complessa segmentazione della rete. Lo zero trust non si applica solo agli utenti che accedono alle applicazioni, ma può essere esteso a tutte le connessioni all'interno dell'azienda, dai dispositivi IoT, alle applicazioni che comunicano tra loro. In quest'ultimo caso, un'app che si trova in un'unica posizione (cloud o data center) può connettersi in modo sicuro a un'altra applicazione, indipendentemente dalla posizione. Grazie a queste connessioni dirette e sicure, il rischio di movimento laterale viene eliminato.

Il modello zero trust si basa sul concetto che tutto è potenzialmente ostile, e stabilisce l'attendibilità solo in base all'identità e al contesto. Questo approccio autorizza le connessioni in base alle informazioni sulle entità che si connettono e al contesto delle relative connessioni, e garantisce che l'accesso sia sempre limitato solo a ciò che è necessario, in qualsiasi momento. In questo modo, il pesante carico di lavoro dei team IT e di sicurezza viene alleggerito, perché tutto avviene automaticamente e può cambiare dinamicamente al mutare delle condizioni per quelle determinate entità e le relative connessioni.

Infine, lo zero trust fornisce controlli granulari con accesso condizionale. Un amministratore può configurare le policy in modo che gli utenti possano accedere a determinate applicazioni solo se il loro traffico proviene da una posizione attendibile, come una rete aziendale, e gli utenti hanno abilitato l'autenticazione a più fattori. L'amministratore può inoltre bloccare il traffico proveniente da determinate posizioni o aree geografiche, da un dispositivo non attendibile, o se i dati richiesti superano le autorizzazioni specifiche di un utente. Tutte le connessioni sono basate sul contesto, e se questo cambia, l'attendibilità viene rivalutata.

La nuova segmentazione

Il costo, la complessità e il tempo necessari per la segmentazione della rete impiegando dei firewall virtuali superano i vantaggi per la sicurezza. La segmentazione dei carichi di lavoro rappresenta un nuovo modo per segmentare i carichi di lavoro delle applicazioni. Con un solo clic, questo tipo di segmentazione potenzia la sicurezza, in quanto consente di individuare eventuali rischi e proteggere i carichi di lavoro in base all'identità, senza apportare modifiche alla rete. Questa tecnologia di segmentazione dei carichi di lavoro basata sull'identità offre una protezione completa, con policy che si adattano automaticamente ai cambiamenti nell'ambiente.

Perdita dei dati

I dati sono essenziali per le aziende e le organizzazioni, per motivi strategici, finanziari e di sicurezza. In alcuni casi possono essere fondamentali per la sicurezza nazionale. Anche con i perimetri di sicurezza della rete, i dati possono essere divulgati a causa della mancanza di consapevolezza degli utenti, azioni involontarie, problemi di sistema e attività malevole sempre più sofisticate. Questo può causare una serie di problematiche, tra cui sanzioni, perdita di clienti, conseguenze legali, mancanza di conformità alle normative e danni al marchio dell'azienda. Esaminiamo i diversi tipi di dati e in che modo potrebbero essere a rischio:

- **Dati in movimento:** i dati in transito su Internet costituiscono la maggior parte dei dati in movimento di oggi, in quanto le applicazioni sono accessibili principalmente attraverso il web; questo vale per le applicazioni SaaS, quelle nel data center e nei cloud pubblici. Se gli utenti accedono a Internet e a destinazioni rischiose da cui è possibile esfiltrare le informazioni sensibili, i dati aziendali vengono messi a rischio. I firewall non sono in grado di seguire gli utenti fuori dalla rete o di proteggere il loro traffico web critico in movimento. Sempre meno dati e meno applicazioni rimangono sugli endpoint, e questo aumenta l'importanza di proteggere i dati che si spostano tra endpoint, applicazioni cloud e punti di archiviazione con una soluzione appositamente pensata per i dati in movimento.
- **Dati inattivi:** i dati che risiedono all'interno di data center, applicazioni SaaS e cloud pubblici rappresentano la maggioranza dei dati inattivi. In particolare, la protezione dei dati inattivi nelle app SaaS è fondamentale per la sicurezza; anche se protetti dai firewall, bastano pochi clic per condividere i dati con un utente non autorizzato tramite app come Microsoft OneDrive. Inoltre, le violazioni del cloud possono essere causate da errori di configurazione o autorizzazioni pericolose. Dato che i servizi SaaS e IaaS sono altamente dinamici e spesso configurati da persone che non sono esperte di sicurezza, tali lacune vengono spesso trascurate e sfruttate.

L'obiettivo finale di qualsiasi tecnologia di sicurezza consiste nel proteggere i dati sensibili, ma i firewall non sono in grado di identificare e controllare in modo efficiente i dati in movimento o inattivi, e ciò mette a rischio l'azienda. Ma soprattutto, non sono in grado di ispezionare in modo efficace il traffico criptato, che rappresenta più del 90% di tutto il traffico[1], consentendogli di passare senza essere ispezionato.

Come evitare la perdita dei dati con lo zero trust

Una vera piattaforma zero trust è in grado di ispezionare tutto il traffico, sia all'interno che all'esterno della rete, incluso tutto il traffico criptato, e di colmare le lacune nella visibilità e nell'ispezione per fornire un'efficace prevenzione della perdita di dati (DLP) e una protezione dalle minacce informatiche. È inoltre in grado di decriptare tutti i dati, determinarne la condizione e quindi di autorizzare le connessioni attraverso il contesto, considerando fattori come tipo di utente, dati di geolocalizzazione, indirizzo IP, profilo del dispositivo, ora del giorno, ecc. Le policy di DLP di una soluzione zero trust proteggono i dati in movimento, e gli utenti ottengono una sicurezza rapida e uniforme, ovunque.

Una soluzione zero trust inline offre il rilevamento e il controllo completo dello shadow IT. Protegge dalle minacce web con l'isolamento del browser, che consente l'accesso da dispositivi non gestiti senza influire negativamente sulle prestazioni. L'isolamento del browser prevede lo streaming dei dati sotto forma di pixel da una sessione isolata in un ambiente sotto container, abilitando il dispositivo BYOD, ma impedendo la perdita dei dati tramite le operazioni di download, copia e incolla e stampa. La DLP fuori banda e la protezione dalle minacce avanzate (ATP) prevengono la condivisione rischiosa dei file e i malware inattivi sul cloud. Per proteggere i dati sul cloud, vengono risolti anche eventuali errori di configurazione, violazioni della conformità, autorizzazioni e diritti che potrebbero essere potenzialmente fatali. Lo zero trust fornisce quindi una sicurezza uniforme e unificata per i dati inattivi e in movimento, incluso il traffico criptato, su Internet, SaaS e applicazioni su cloud pubblico su larga scala, indipendentemente dal dispositivo dell'utente.

Vulnerabilità del browser web

La percentuale di traffico web criptato su Internet è in costante aumento, ed è passata dal 50% del 2014 all'incredibile 95% di oggi.[1] Nonostante ciò, i browser web sono l'obiettivo principale degli aggressori, poiché, secondo Gartner, il 98% degli attacchi viene effettuato sulla rete Internet pubblica, e l'80% di questi attacchi prende di mira gli utenti finali attraverso i browser. Gli strumenti di isolamento del browser, come Cloud Browser Isolation, aiutano a mitigare queste vulnerabilità, in particolare quando possono essere distribuiti senza installazioni software lato client, un aspetto che li rende più adatti per i dispositivi non gestiti che accedono alle risorse IT aziendali.

Raggiungere un vero modello zero trust con Zscaler

Zscaler fornisce lo zero trust attraverso Zero Trust Exchange, una piattaforma nativa del cloud che opera su 150 data center in tutto il mondo, e che usa il security cloud più grande del pianeta per fornire connessioni veloci e sicure. Con questa soluzione, i dipendenti possono lavorare in modo sicuro da qualsiasi luogo e su qualsiasi dispositivo, utilizzando Internet come rete aziendale. A differenza dei firewall e delle VPN, Zero Trust Exchange si basa sul principio dell'accesso a privilegi minimi e sul concetto che nessuna applicazione e nessun utente debbano essere automaticamente ritenuti attendibili. Al contrario, le connessioni vengono autorizzate in base all'identità e al contesto dell'utente prendendo in considerazione fattori come la posizione, il profilo di sicurezza del dispositivo, l'applicazione a cui si vuole accedere e i contenuti scambiati.

Come? Per prima cosa, Zero Trust Exchange termina la connessione, per consentire un'ispezione approfondita dei contenuti, tra cui il traffico criptato, eseguendo un'analisi accurata dei dati e delle minacce. Determina quindi l'identità e il dispositivo e verifica i diritti di accesso, utilizzando le policy aziendali basate sul contesto, prendendo in considerazione l'utente, il dispositivo, l'applicazione richiesta e il tipo di contenuto. Una volta verificata e applicata la policy aziendale, Zero Trust Exchange agisce da broker e stabilisce la connessione tra le risorse. Gli utenti e i dispositivi vengono collegati direttamente alle applicazioni e non alla rete aziendale.

Per saperne di più

Visita la pagina di **Zero Trust Exchange** per saperne di più sullo zero trust e su come Zscaler può essere d'aiuto.

Fonti

[1] *Google Transparency Report https://transparencyreport.google.com/https/overview?hl=it*
[2] *Zscaler Networks Security Survey 2020*
[3] *ESG Economic Validation Study 2021*

Informazioni su Zscaler

Zscaler consente alle organizzazioni di trasformare in sicurezza le proprie reti e applicazioni per un mondo mobile e cloud-first. Zscaler collega gli utenti ad applicazioni e servizi cloud, indipendentemente dal dispositivo, dalla posizione o dalla rete, fornendo allo stesso tempo una sicurezza completa e un'esperienza utente veloce. Tutto questo senza dispositivi gateway costosi e complessi.

©2022 Zscaler, Inc. Tutti i diritti riservati. Zscaler™ è (I) un marchio registrato o un marchio di servizio o (II) un marchio commerciale o un marchio di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi commerciali sono di proprietà dei rispettivi proprietari.