L'APPROCCIO SONICWALL CLEAN VPN PER LA FORZA LAVORO MOBILE

L'approccio di Clean VPN offre protezione su più livelli con difesa in profondità per gli elementi essenziali alle comunicazioni aziendali.

Abstract

La consumerizzazione dell'IT e l'adozione di politiche BYOD (Bring Your Own Device) in azienda rendono più difficile per i responsabili dei sistemi informatici garantire un accesso sicuro alla rete da dispositivi mobili quali laptop, smartphone e tablet. L'approccio di SonicWall™ Clean VPN™ combina l'accesso remoto sicuro tramite VPN SSL alla tecnologia firewall di ultima generazione per fornire protezione con una difesa approfondita su più livelli per gli elementi fondamentali della comunicazione aziendale:

- endpoint e utenti
- dati e applicazioni
- il traffico che li collega

Introduzione

Una rete di dispositivi mobili personali

Oggigiorno i dipendenti lavorano ovunque e in qualsiasi momento. Solo negli Stati Uniti, il 50% delle persone operanti nel settore dell'informazione lavora sia in ufficio che da casa e da altri luoghi. Questa forza lavoro mobile necessita di un accesso costante alle principali risorse aziendali in rete. È ormai anacronistico pensare che i collaboratori utilizzino per lavoro solo dispositivi forniti dall'IT aziendale all'interno del perimetro di rete tradizionale. Per prolungare la giornata lavorativa e incrementare il grado di efficienza, i dipendenti si affidano alla stessa tecnologia che usano per la propria vita privata, come ad esempio laptop, smartphone e tablet.

Non a caso la maggior parte delle nuove tecnologie adottate dalle imprese si basa su prodotti di consumo. Questa consumerizzazione dell'IT ha permesso agli utenti finali di scegliere le piattaforme informatiche da utilizzare per svolgere il proprio lavoro sia in ufficio che da casa o in viaggio. Di conseguenza, i responsabili IT non sono più in grado di verificare quali dispositivi endpoint si connettono alla rete aziendale.

Sempre più aziende adottano l'approccio BYOD mediante policy che consentono ai dipendenti di utilizzare per lavoro i propri dispositivi mobili personali. Permettere ai collaboratori di usare i propri apparecchi acquistati privatamente offre un vantaggio anche in termini di budget, poiché riduce le spese legate all'acquisto anticipato di hardware.

I requisiti di sicurezza variano in base ai dispositivi

Esistono differenze sottili ma rilevanti tra le varie piattaforme di dispositivi mobili di largo consumo. I laptop, ad esempio, richiedono di solito un maggiore controllo del terminale rispetto a smartphone e tablet, che di norma possono scaricare e installare solo applicazioni sottoposte a rigorose verifiche preventive basate su white list (ovviamente questo discorso non vale per i dispositivi sbloccati con jailbreak o con permessi di root abilitati per poter scaricare app non presenti nelle white list). Per garantire un accesso remoto sicuro dei laptop non gestiti occorre utilizzare un portale con proxy inverso oppure un tunnel VPN (Virtual Private Network) con controllo degli endpoint. Ciò consente all'IT di verificare che sui dispositivi siano presenti e attive le applicazioni di sicurezza previste e di applicare policy di sicurezza per autorizzare, mettere in quarantena o negare l'accesso in base ai criteri di sicurezza prestabiliti.

In generale le piattaforme mobili sono considerate più sicure perché la maggior parte delle applicazioni viene distribuita solo tramite fornitori inclusi nella white list. In ogni caso sarebbe un errore fidarsi semplicemente delle applicazioni o dei dati che girano su questi dispositivi. Le minacce sono reali ed esistono tanti modi per sfruttare questi dispositivi se non sono dotati di misure di sicurezza specifiche per queste piattaforme.

> Per proteggere la rete aziendale, l'IT deve partire dal presupposto che nessun dispositivo mobile è affidabile e che tutti gli accessi eseguiti dall'esterno della rete aziendale sono fuori dal suo controllo.

Gli endpoint – e le minacce – sono ovunque

Per proteggere la rete aziendale, l'IT deve partire dal presupposto che nessun dispositivo mobile è totalmente affidabile e che tutti gli accessi eseguiti dall'esterno della rete aziendale sono fuori dal suo controllo.

Esiste inoltre il rischio di potenziali perdite di dati, causate da furti o da trasmissioni o accessi non autorizzati, anche su piattaforme smartphone apparentemente "a prova di hacker". Durante una connessione alla rete wireless aziendale, i dispositivi mobili possono acquisire dati sensibili o proprietari e poi esporli al rischio di furti nel web attraverso l'invio di allegati e-mail o upload su FTP realizzati su reti cellulari non protette.

Le divisioni IT devono adottare misure esaustive per proteggere le risorse aziendali dalle minacce esistenti e in continua evoluzione. I dati in transito sono vulnerabili ad attacchi man-in-the-middle e ad intercettazioni, e per tale motivo devono essere crittografati. Occorre inoltre scansionare tutti i flussi di dati trasmessi per rilevare eventuali malware e prevenire attacchi botnet in uscita lanciati dall'interno della rete, che possono danneggiare la reputazione aziendale e causare l'inserimento in blacklist dei server di posta strategici per l'azienda. Allo stesso tempo, l'IT deve implementare una soluzione in grado di ispezionare il traffico in uscita – anche quello crittografato - per impedire perdite di dati.

Una soluzione "Clean VPN" può fornire questa e molte altre opzioni di protezione grazie alla combinazione di VPN SSL e firewall di nuova generazione.

L'approccio SonicWall Clean VPN

SonicWall Clean VPN offre la duplice protezione avanzata di una VPN SSL e di un firewall di nuova generazione ad alte prestazioni, necessaria per proteggere sia l'accesso che il traffico VPN. La protezione multilivello di Clean VPN consente alle imprese di decrittografare e analizzare tutto il traffico VPN SSL autorizzato per rilevare eventuali malware prima che entri nell'ambiente di rete.

- Il componente VPN SSL di Clean VPN utilizza SonicWall Secure Mobile Access (SMA) con Advanced End Point Control™ (EPC) per proteggere l'integrità dell'accesso VPN. EPC verifica l'attendibilità degli utenti remoti e dei rispettivi dispositivi endpoint applicando l'autenticazione forzata, la crittografia dei dati e policy di accesso granulari a livello di applicazione. EPC consente di verificare se un dispositivo iOS o Android è stato sbloccato tramite jailbreak o permessi di root, in modo da rifiutare o mettere in quarantena le connessioni da quei sistemi.

- Il componente firewall di nuova generazione di Clean VPN assicura allo stesso tempo l'integrità del traffico VPN. Una volta autorizzato il traffico VPN, rimuove eventuali malware dal traffico in entrata e verifica tutto il traffico VPN in uscita in tempo reale. In questo modo si ha la garanzia che i dati trasmessi e ricevuti dagli utenti vengano analizzati con le stesse procedure di sicurezza sia all'interno che all'esterno della rete aziendale. SonicWall Application Intelligence and Control offre il controllo granulare e la visualizzazione in tempo reale delle applicazioni per assicurare alle applicazioni business-critical un accesso prioritario alla larghezza di banda, garantendo il massimo livello di produttività e protezione della rete.

Opzioni di implementazione

SonicWall offre agli amministratori la flessibilità e la scalabilità di implementare Clean VPN in due modi diversi:

- Implementazione integrata di Clean VPN – Gli amministratori possono realizzare una Clean VPN utilizzando la VPN SSL integrata nei firewall SonicWall delle serie SuperMassive, NSA e TZ.

- Implementazione combinata di Clean VPN – In alternativa è possibile realizzare una Clean VPN combinando un firewall SonicWall di nuova generazione con un SonicWall Secure Mobile Access (SMA).

Implementazione integrata di Clean VPN

In un approccio Clean VPN integrato, i firewall SonicWall di nuova generazione con tecnologia Reassembly-Free Deep Packet Inspection® (RFDPI) applicano funzioni integrate di prevenzione delle intrusioni, protezione anti-malware e controllo, intelligence e visualizzazione in tempo reale delle applicazioni a tutto il traffico VPN SSL proveniente da notebook, smartphone e tablet. I firewall SonicWall di nuova generazione analizzano tutto il traffico in entrata e in uscita e sono scalabili per soddisfare le esigenze delle reti con i massimi livelli di prestazioni. La funzionalità integrata di controllo, intelligence e visualizzazione delle applicazioni aiuta gli amministratori a monitorare e gestire gli applicativi (aziendali e non) per garantire la produttività della rete e degli utenti.

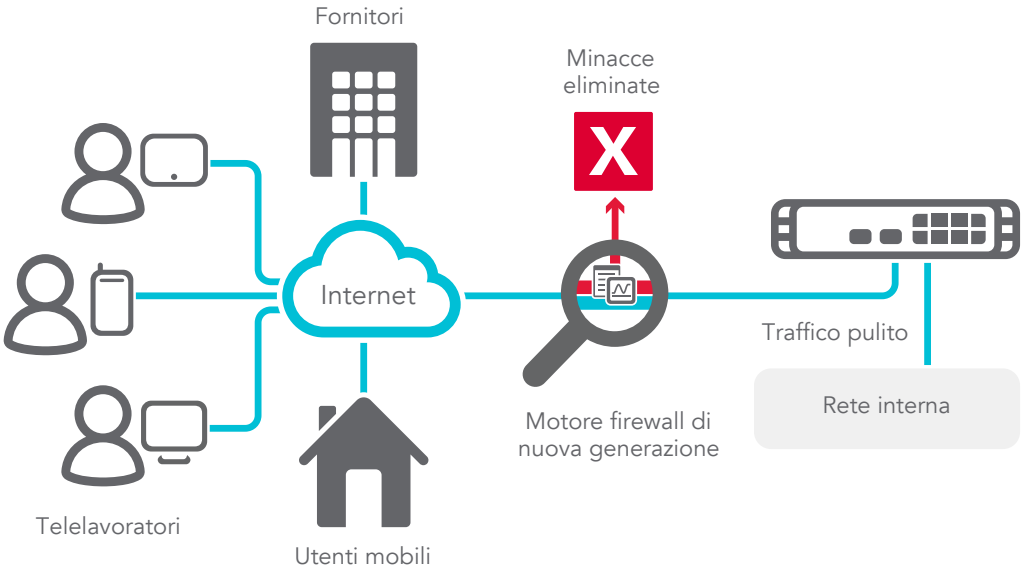

Figura 1. Approccio Clean VPN integrato, utilizzando la VPN SSL integrata nei firewall SonicWall di nuova generazione

Un approccio Clean VPN integrato consente agli amministratori di dare priorità alle applicazioni aziendali strategiche nell'uso della larghezza di banda disponibile nella VPN SSL. Per l'accesso VPN SSL tramite i firewall SonicWall di nuova generazione, il SonicWall NetExtender fornisce un accesso da thin-client per i sistemi basati su Windows, Windows Phone, Mac OS e Linux.

Le applicazioni mobili di SonicWall Mobile Connect™ per iOS, OS X, Android, Chrome OS, Kindle Fire e Windows 10 forniscono agli utenti di smartphone e tablet un accesso semplice e veloce a livello di rete a risorse aziendali, accademiche e governative attraverso una VPN SSL crittografata.

> Un approccio Clean VPN integrato consente agli amministratori di dare priorità alle applicazioni aziendali strategiche nell'uso della larghezza di banda disponibile nella VPN SSL.

Solo SonicWall offre una Clean VPN (in caso di utilizzo con un firewall di nuova generazione) per autorizzare, decrittografare e rimuovere le minacce dal traffico di tutte le principali piattaforme mobili attraverso una VPN SSL all'esterno del perimetro di rete. Inoltre, SonicWall Application Intelligence and Control permette alle aziende di definire e imporre in quale modo verranno utilizzate le applicazioni e la larghezza di banda.

Implementazione combinata di Clean VPN

Un approccio Clean VPN combinato offre, oltre a tutti gli elementi di sicurezza e VPN SSL di un'implementazione Clean VPN integrata, la funzionalità SonicWall SMA aggiuntiva per interrogare i dispositivi e applicare controlli degli endpoint basati su policy.

Una Clean VPN combinata con SonicWall SMA

SonicWall EPC (disponibile per dispositivi basati su Windows, Macintosh e Linux) integra la protezione degli endpoint non gestiti, un desktop virtuale sicuro e il controllo approfondito della cache. EPC offre funzioni avanzate per il rilevamento degli endpoint e la protezione dei dati aziendali. Mediante l'interrogazione dei dispositivi endpoint permette di verificare la presenza di tutte le soluzioni antivirus, personal firewall e antispyware supportate di fornitori leader quali McAfee®, Symantec®, Computer Associates®, Sophos® e Kaspersky Lab®. In caso di utilizzo con SonicWall Mobile Connect, l'identificazione e l'applicazione basate su policy vengono estese anche a tutte le principali piattaforme mobili. Ciò consente al reparto IT di applicare un ID ai dispositivi, limitare i dispositivi utilizzabili dagli utenti per accedere alla rete, garantire la presenza dei certificati client e verificare se un dispositivo iOS o Android è stato sbloccato tramite jailbreak o permessi di root.

In combinazione con un firewall SonicWall di nuova generazione come Clean VPN, la soluzione SMA offre il controllo centralizzato delle policy di accesso e la protezione anti-malware.

SonicWall SMA fornisce una connettività clientless o thin-client "come in ufficio", semplice da gestire e ricca di funzionalità, per un massimo di 20.000 utenti mobili aziendali simultanei da un'unica appliance. SMA incrementa la produttività e la continuità aziendale garantendo l'accesso remoto basato su policy alle risorse di rete da dispositivi con sistema Windows, Apple Mac OS, iOS, Linux e Android.

Basata sulla potente piattaforma VPN SSL avanzata di SonicWall, l'appliance SMA connette solo gli utenti autorizzati a determinate risorse autorizzate. Inoltre, SMA supporta l'autenticazione Vasco, RSA, Active Directory, LDAP, RADIUS e SAML e la generazione di password monouso OTP (One-Time Password) integrata per l'autenticazione a due fattori.

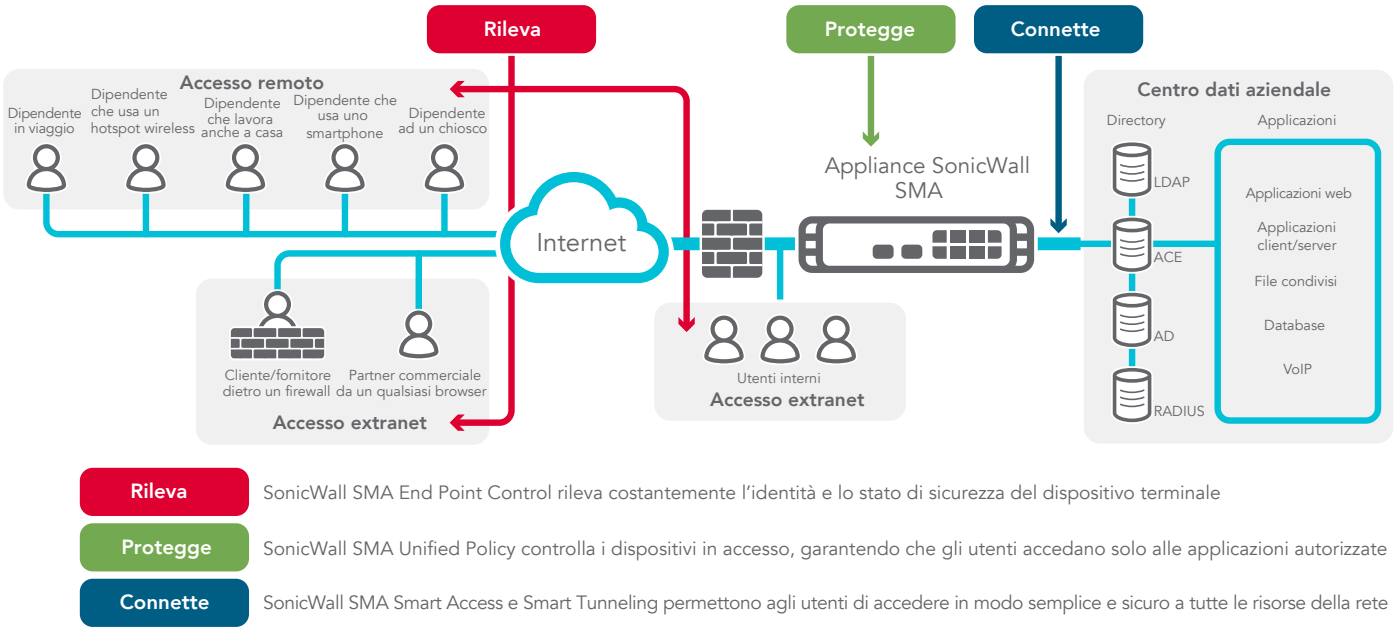

Figura 2. Approccio Clean VPN combinato, utilizzando un firewall SonicWall di nuova generazione con una appliance SonicWall SMA

Un approccio Clean VPN combinato con una soluzione SonicWall SMA incorporata è in grado di:

- Rilevare l'integrità degli utenti, degli endpoint e del traffico all'esterno del tradizionale perimetro di rete.
- Proteggere le applicazioni e le risorse dall'accesso non autorizzato e da attacchi malware.
- Connettere gli utenti autorizzati alle risorse appropriate in modo semplice e trasparente.

Una Clean VPN combinata con una soluzione SonicWall SMA per le PMI

L'amministratore di una piccola o media impresa può anche realizzare una Clean VPN combinata collegando un firewall SonicWall di nuova generazione con una soluzione SonicWall SMA per le PMI.

SonicWall SMA offre l'accesso senza client e tramite tunnel per dispositivi Windows, Windows Phone, Mac OS, iOS, Linux e Android, oltre al servizio opzionale Web Application Firewall e al supporto remoto multipiattaforma. SMA offre policy granulari unificate, autenticazione a due fattori, bilanciamento del carico e alta disponibilità. Inoltre consente a lavoratori mobili e fornitori autorizzati di connettersi attraverso la VPN SSL utilizzando l'applicazione Mobile Connect o un comune browser. Installabile in modo semplice e flessibile praticamente in qualsiasi rete, senza necessità di client preinstallati, la soluzione SRA elimina anche i costi associati all'implementazione e alle manutenzione delle VPN IPSec tradizionali. SonicWall Virtual Assist permette ai tecnici che operano con sistemi Windows di supportare in remoto dispositivi Windows, Mac OS o Linux.

Gestione di una Clean VPN combinata

Mediante il SonicWall Global Management System (GMS), gli amministratori possono configurare e gestire la propria implementazione Clean VPN combinata da un'unica interfaccia di gestione. SonicWall GMS offre una piattaforma potente, resiliente e flessibile per gestire centralmente e implementare con rapidità le appliance SonicWall e le configurazioni di sicurezza. Oltre al monitoraggio centralizzato in tempo reale, offre report esaustivi sulle policy e la conformità, permettendo di soddisfare i più rigorosi requisiti di controllo e conformità alle normative.

Infine SonicWall Analyzer, uno strumento di reporting e analisi dei flussi di traffico facile da usare e basato sul Web, fornisce una visione dettagliata in tempo reale e storica sullo stato, le prestazioni e la sicurezza della rete. Analyzer supporta i firewall SonicWall e i dispositivi di accesso remoto sicuro e utilizza l'analisi dei flussi di traffico delle applicazioni per fornire report sugli eventi di sicurezza. Aziende e organizzazioni di ogni dimensione possono così migliorare la produttività dei dipendenti, ottimizzare l'uso della larghezza di banda e aumentare la consapevolezza della sicurezza. SonicWall è l'unico fornitore di firewall ad offrire una soluzione completa che combina uno strumento integrato di analisi dei flussi di traffico delle applicazioni con i dati IPFIX granulari generati dai firewall SonicWall.

Clean VPN integrata	
Tecnologia	Soluzione SonicWall
Firewall di nuova generazione	Serie SuperMassive, NSA o TZ
Ispezione deep packet	Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service
Controllo, intelligence e visualizzazione delle applicazioni	Servizio Application Intelligence and Control
VPN SSL	Mobile Connect, Net Extender

Clean VPN combinata	
Tecnologia	Soluzione SonicWall
VPN SSL	SMA con Advanced End Point Control, Connect Tunnel e Mobile Connect
Firewall di nuova generazione	Serie SuperMassive e NSA
Ispezione deep packet	Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service
Controllo, intelligence e visualizzazione delle applicazioni	Servizio Application Intelligence and Control

Figura 3. Confronto tra le due opzioni di implementazione di Clean VPN

Conclusioni

SonicWall si è posizionata strategicamente come leader di settore nella proposta di soluzioni all'avanguardia con tecnologia Clean VPN per aziende di qualsiasi dimensione, consentendo un'integrazione gestita delle sue premiate linee di accesso remoto sicuro, firewall di nuova generazione e soluzioni di gestione e reporting. L'implementazione integrata o combinata di queste soluzioni offre alle aziende un'unica soluzione di protezione con difesa approfondita.

Una soluzione SonicWall Clean VPN può rilevare l'identità degli utenti e lo stato di sicurezza dei dispositivi endpoint, proteggere dal malware e da accessi non autorizzati in base a policy granulari prima di autorizzare l'accesso e, infine, connettere facilmente gli utenti autorizzati alle risorse di rete strategiche. Solo SonicWall è in grado di fornire una Clean VPN realmente valida essendo l'unico vendor ad offrire il controllo granulare degli endpoint, un modello di policy unificato con policy di accesso dinamiche e la rivoluzionaria tecnologia di sicurezza Reassembly-Free Deep Packet Inspection® ad alte prestazioni su una piattaforma di elaborazione multi-core.

© 2017 SonicWall Inc. TUTTI I DIRITTI RISERVATI.

SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari.

Le informazioni contenute nel presente documento si riferiscono ai prodotti di SonicWall Inc. e/o delle sue affiliate. Né il presente documento né la vendita di prodotti SonicWall costituiscono alcuna licenza, espressa o implicita, di estoppel o di altro tipo, né garantiscono diritti di proprietà intellettuale. SALVO QUANTO SPECIFICATO NEI TERMINI E NELLE CONDIZIONI STABILITI NEL CONTRATTO DI LICENZA DI QUESTO PRODOTTO, SONICWALL E/O LE SUE AFFILIATE NON SI ASSUMONO ALCUNA RESPONSABILITÀ ED ESCLUDONO GARANZIE DI QUALSIASI TIPO, ESPLICITE, IMPLICITE O LEGALI, IN RELAZIONE AI PROPRI PRODOTTI, INCLUSE, IN VIA ESEMPLIFICATIVA, QUALSIASI GARANZIA IMPLICITA DI COMMERCIABILITÀ, IDONEITÀ A SCOPI SPECIFICI O VIOLAZIONE DI DIRITTI ALTRUI. SONICWALL E/O LE SUE AFFILIATE DECLINANO OGNI RESPONSABILITÀ PER DANNI DI QUALUNQUE TIPO, SIANO ESSI DIRETTI, INDIRETTI, CONSEQUENZIALI, PUNITIVI, SPECIALI O INCIDENTALI (INCLUSI, SENZA LIMITAZIONI, DANNI PER MANCATO GUADAGNO, INTERRUZIONI DELL'ATTIVITÀ O PERDITE DI DATI) DERIVANTI DALL'UTILIZZO O DALL'IMPOSSIBILITÀ DI UTILIZZARE IL PRESENTE DOCUMENTO, ANCHE NEL CASO IN CUI SONICWALL E/O LE SUE AFFILIATE SIANO STATE AVVERTITE DELL'EVENTUALITÀ DI TALI DANNI. SonicWall e/o le sue affiliate non rilasciano alcuna garanzia o dichiarazione relativamente alla precisione o completezza dei contenuti del presente documento e si riserva il diritto di apportare modifiche, in qualsiasi momento e senza preavviso, alle specifiche e alle descrizioni dei prodotti. SonicWall Inc. e/o le sue affiliate non si assumono alcun impegno di aggiornare le informazioni contenute in questo documento.

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

© 2017 SonicWall Inc. TUTTI I DIRITTI RISERVATI. SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari.