



- **Accesso “come in ufficio” da qualsiasi luogo**
- **Facile da distribuire, gestire e controllare**
- **SonicWALL Aventail Unified Policy**
- **Accesso sicuro a tutte le applicazioni**
- **Controllo dello split tunneling**

Accesso semplificato, come dall'ufficio

Nelle aziende moderne, una quantità crescente di lavoro viene svolto all'esterno dell'ufficio da dipendenti che lavorano da casa, dirigenti in viaggio d'affari con laptop gestiti e partner collegati tramite extranet. Questi utenti di importanza strategica devono poter accedere alle applicazioni cruciali – tra cui applicazioni back-connect come telefonia VoIP o help desk remoto – come se si trovassero in ufficio. La sfida per i manager IT consiste nel fornire un accesso completo garantendo massima sicurezza, controllo dello split tunneling e rilevamento del personal firewall.

SonicWALL® Aventail® Connect Tunnel™ offre agli utenti delle SSL VPN di classe E di SonicWALL Aventail un'alternativa semplice e sicura alla tradizionale postazione in ufficio. Connect Tunnel è un client che può essere distribuito via Web per fornire agli utenti di desktop e laptop remoti autorizzati un accesso sicuro all'intera rete da qualsiasi luogo. Connect Tunnel fornisce il metodo di accesso remoto sicuro più semplice e completo sul mercato ed è quindi la soluzione ideale per garantire la massima sicurezza all'interno delle WLAN (Wireless Local Area Network) e ai lavoratori mobili con la necessità di accedere alla rete dall'esterno dell'ufficio.

Caratteristiche e vantaggi

L'accesso “come in ufficio” da qualsiasi luogo

consente agli utenti di dispositivi IT gestiti (come ad esempio computer desktop e laptop autorizzati) di accedere in remoto alle risorse di rete proprio come se fossero collegati alla LAN dell'ufficio. Connect Tunnel fornisce il massimo livello di trasparenza e funzioni avanzate tra cui single sign-on, ricerca automatica della rete e integrazione con programmi di connessione a Internet di altri produttori. Gli utenti non devono preoccuparsi di come accedere alle risorse aziendali. Con un semplice clic sull'icona del dispositivo IT remoto gestito, ogni utente autorizzato può connettersi automaticamente alla rete aziendale tramite Internet. La tecnologia SonicWALL Aventail Smart Access™ rileva e implementa automaticamente il metodo di accesso remoto alle risorse aziendali in base alle policy stabilite per ogni singolo utente.

Facile da distribuire, gestire e controllare. Gli amministratori devono semplicemente installare Connect Tunnel sui computer e dispositivi gestiti. L'aggiornamento alle nuove versioni ed eventuali modifiche alla configurazione vengono poi eseguiti automaticamente senza necessità di ulteriori interventi. Il leggerissimo client di Connect Tunnel di Aventail può essere preinstallato su un dispositivo IT gestito o essere scaricato in modalità sicura da un portale Web dedicato, offrendo un'alternativa ideale – e semplice da implementare – ai client VPN IPSec di tipo “fat”.

SonicWALL Aventail Unified Policy™ consente agli amministratori di controllare centralmente tutti gli utenti, i gruppi, le risorse e i dispositivi, con la possibilità di creare velocemente policy unitarie per tutti gli oggetti. SonicWALL Aventail End Point Control™ identifica e applica le policy di sicurezza a tutti i

dispositivi con sistema Windows®, Macintosh® e Linux®, rilevando automaticamente le informazioni essenziali come software anti-virus, personal firewall, applicativi, directory, nomi e dimensioni dei file, data e ora come pure versioni, domini e voci di registro di Windows.

Accesso sicuro a tutte le applicazioni – tra cui VoIP ed help desk remoto – mediante la tecnologia SonicWALL Aventail Smart Tunneling™, un'architettura esclusiva che combina il controllo SSL a livello di applicazione con la portata di un tunnel di livello 3. Gli utenti possono così accedere a una gamma di applicazioni pressoché illimitata, incluso il supporto dei protocolli UDP, TCP e IP, e dispongono di un controllo granulare e bidirezionale degli accessi a tutte le applicazioni, incluse quelle di telefonia VoIP e di help desk remoto. Un dispositivo VoIP e il relativo utente possono essere verificati e autenticati prima della connessione, escludendo così il rischio di attacchi malevoli.

Il **controllo dello split tunneling** consente allo staff IT di verificare se gli utenti si collegano a reti multiple mentre sono connessi alla VPN. Ulteriori funzionalità tra cui NAT traversal, rilevamento del proxy, traversal e adattamento dinamico per ridurre i conflitti di indirizzi garantiscono l'accesso universale alle applicazioni. Connect Tunnel può essere facilmente integrato con programmi di connessione a Internet e altri prodotti software desktop. Grazie alla possibilità di fornire agli utenti un accesso completo ad ogni applicazione e alle funzioni avanzate di protezione e controllo delle policy, Connect Tunnel rappresenta un'alternativa semplice ed efficace alle complicate distribuzioni IPSec.

**Connect Mobile**

E-Class EX-750

01-SSC-7704

A richiesta

E-Class EX-1600

Incluso

E-Class EX-2500

Incluso

Come funziona SonicWALL Aventail Connect Tunnel?

Il thin client di SonicWALL Aventail Connect Tunnel può essere preinstallato su un dispositivo IT gestito o scaricato da un portale Web dedicato. Una volta installato il client di Connect Tunnel, l'utente può accedere alle risorse di rete autorizzate e lavorare come se si trovasse in ufficio, senza bisogno di collegarsi a siti o portali Web. Con un semplice clic sull'icona SonicWALL Aventail Connect presente sul desktop, l'utente può autenticarsi e accedere alla rete aziendale con il proprio dispositivo IT tramite Internet – in modo automatico e assolutamente trasparente.

Specifiche tecniche	Browser	Note
Sistema operativo Windows Vista® Windows XP Pro, SP2 Windows 2000 Pro, SP4 Windows XP Home, SP2	N/D	Per l'installazione sono richiesti diritti di amministratore di Windows.
Piattaforma server Windows: Windows 2003 Server Windows 3000 Server, SP4	N/D	Per l'installazione sono richiesti diritti di amministratore di Windows.
Macintosh OS X v. 10.5	N/D	Per l'installazione sono richiesti diritti di amministratore. Nessun supporto per End Point Control Macintosh OS X v. 10.5 è stato testato solo su computer con processore Intel
Linux kernel 2.4.20 o successivo	Mozilla Firefox 2.0 (Mozilla Firefox 1.5)	Per l'installazione sono richiesti diritti di amministratore. Browser richiesto solo per il rilevamento del proxy Nessun supporto per End Point Control

Per ulteriori informazioni sulle soluzioni SSL VPN di classe E di SonicWALL Aventail, visitate il nostro sito all'indirizzo **www.sonicwall.com**.

Italia / Supporto

Numero verde: 800.909.106

Telefono: +31 (0) 411.617.814

E-mail: sales_support-europe@sonicwall.com

Italia / Uffici

Telefono: +39.010.7407851

E-mail: italy@sonicwall.com



PROTEZIONE ALLA VELOCITÀ DEL BUSINESS™