



Serie SonicWALL TZ

ACCESSO REMOTO SICURO

- Basata sulla comprovata architettura di sicurezza di SonicOS, la serie TZ offre una **prevenzione delle intrusioni e anti-malware ad alta efficacia** per mantenere le reti al sicuro dalle sofisticate minacce moderne.
- **Un accesso remoto SSL VPN ad alta sicurezza** è disponibile in modo nativo per dispositivi Apple iOS, Google Android, Windows, Mac OS e Linux per sfruttare le potenzialità di una forza lavoro mobile.
- Il filtraggio dei contenuti e degli URL SonicWALL **blocca diverse categorie di contenuti Web ritenuti non idonei** per consentire un'elevata produttività sul posto di lavoro e ridurre la responsabilità legale.
- Di facile comprensione e rapida implementazione, l'interfaccia grafica utente della serie TZ **elimina la necessità di scegliere fra semplicità di utilizzo e potenza**, riducendo il TCO.

Gestione unificata delle minacce (UTM)

La serie SonicWALL® TZ è il più sicuro firewall per la gestione unificata delle minacce (UTM, Unified Threat Management) per piccole aziende, applicazioni retail, pubbliche amministrazioni e filiali in località remote e sedi distaccate. A differenza dei prodotti per uso domestico, la serie TZ fornisce le più efficaci funzionalità anti-malware, per la prevenzione delle intrusioni, per il filtraggio dei contenuti/URL e per il controllo delle applicazioni, unitamente al più ampio e sicuro supporto per piattaforme mobili per laptop, smartphone e tablet. La serie offre la completa funzionalità di ispezione deep packet (DPI) a livelli prestazionali molto elevati, eliminando il collo di bottiglia di rete causato da altri prodotti e consentendo alle aziende di realizzare maggiori guadagni in produttività. La serie TZ è la più sicura e sofisticata piattaforma di sicurezza, ampiamente diffusa sul mercato odierno.

Inoltre, le funzionalità SonicWALL Application Intelligence and Control di TZ 215 assicurano la disponibilità della larghezza di banda per applicazioni fondamentali per l'attività aziendale, con limitazione del traffico di applicazioni non produttive. La TZ 215 offre inoltre funzioni avanzate di analisi del traffico delle applicazioni e di reporting per un esame approfondito dell'utilizzo della larghezza di banda e delle minacce alla sicurezza.

La serie TZ include ulteriori caratteristiche avanzate di networking come IPSec e SSL VPN, ISP Failover multiplo, bilanciamento del carico, wireless opzionale integrato 802.11n e segmentazione della rete, consentendo inoltre la conformità PCI. La serie TZ è l'unico firewall UTM disponibile a offrire un client di accesso remoto VPN nativo per Apple® iOS, Google® Android™, Windows, Mac OS e Linux. Questo client unico supporta Clean VPN™, che neutralizza le minacce provenienti dal traffico VPN. Proponendo il supporto più sicuro per piattaforme mobili, solo SonicWALL offre una scansione completa del malware del traffico SSL crittografato e il controllo delle applicazioni per dispositivi Android e iOS.

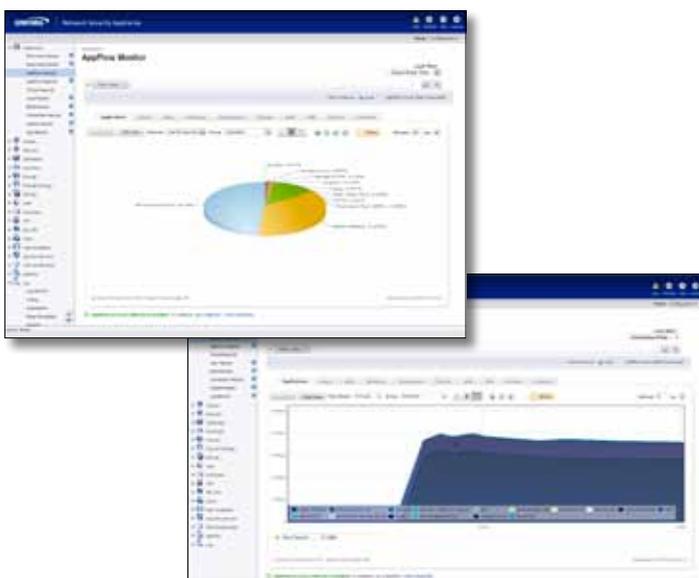
La nuova serie TZ è un'elegante integrazione di più prodotti singoli, combinati in una soluzione unica in grado di offrire valore riducendo la complessità

Profilo di SonicWALL

Guidata da una vision orientata alla sicurezza dinamica per la rete globale, SonicWALL sviluppa soluzioni avanzate, intelligenti e scalabili per la sicurezza di rete e la protezione dei dati in base all'evolversi delle aziende e delle minacce. SonicWALL progetta soluzioni pluripremiate per hardware, software e dispositivi virtuali per il rilevamento e il controllo delle applicazioni, oltre che per la protezione della rete da intrusioni e attacchi malware. Le soluzioni SonicWALL sono implementate da aziende sia di piccole che di grandi dimensioni in tutto il mondo. Sin dal 1991, l'azienda ha venduto oltre un milione di appliance attraverso la propria rete globale di partner di canale, destinate a proteggere e tenere sotto controllo i dati e i computer di decine di milioni di utenti aziendali.

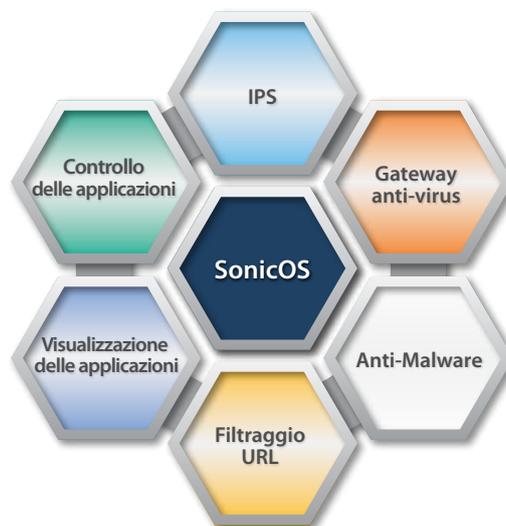
Architettura SonicWALL

SonicWALL TZ 205 e TZ 215 sono dotati di CPU dual-core Cavium, che elaborano contemporaneamente i flussi di dati in parallelo, aumentando la protezione e le prestazioni complessive. La tecnologia dual-core offre prestazioni, scalabilità ed efficienza energetica superiori rispetto alle piattaforme di sicurezza di rete basate su processori generici con coprocessori di sicurezza separati o sistemi ASIC (Application-Specific Integrated Circuit) che non sono in grado di tenere il passo con l'evoluzione dei complessi attacchi in tempo reale provenienti dall'interno e dall'esterno del perimetro di rete. L'architettura dual-core avanzata ad alte prestazioni rende la serie TZ la soluzione più veloce nella sua categoria, con livelli prestazionali fino a 500 Mbps di throughput stateful, 110 Mbps di throughput ispezione deep packet e 130 Mbps di throughput 3DES o AES VPN.

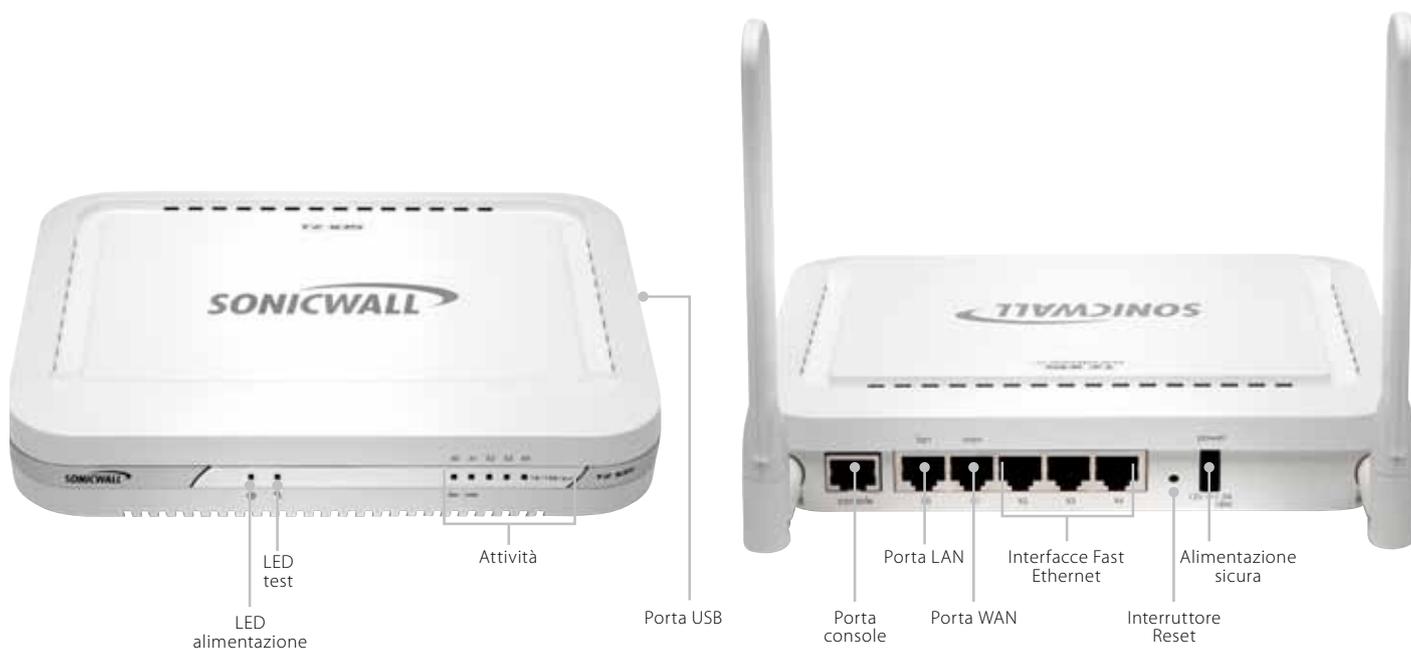


Software SonicOS

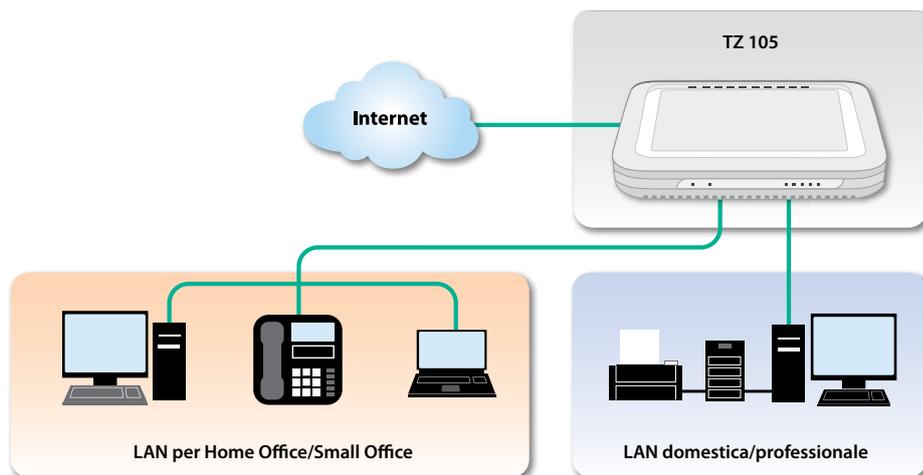
La tecnologia brevettata da SonicWALL Reassembly-Free Deep Packet Inspection® (RFDPI) consente la scansione e l'analisi simultanea di minacce multiple e applicazioni senza limiti di dimensioni dei file e connessioni ad altissima velocità. Questa singola base di codice è al centro di ogni firewall SonicWALL, dal TZ 105 al SonicWALL SuperMassive E10800. SuperMassive E10800 con SonicOS è il firewall di nuova generazione a protezione globale di più alto livello a ricevere la valutazione NSS Labs Recommend. La tecnologia RFDPI è strettamente integrata nella piattaforma firewall, ottimizzando così la gestione delle politiche firewall granulari, direttamente attraverso l'interfaccia firewall o attraverso il SonicWALL Global Management System. Le aziende possono scegliere da un'intera linea di collaudati firewall SonicWALL con SonicOS, ad altissima scalabilità per soddisfare le esigenze delle reti più performanti.



	Serie TZ 105	Serie TZ 205	Serie TZ 215
Panoramica dei firewall			
Throughput firewall ispezione Stateful Packet	200 Mbps	500 Mbps	500 Mbps
Throughput IPS	60 Mbps	80 Mbps	110 Mbps
GAV/Throughput	40 Mbps	60 Mbps	70 Mbps
Throughput VPN	75 Mbps	100 Mbps	110 Mbps
DPI completa (UTM)	25 Mbps	40 Mbps	60 Mbps
Connessioni UTM/DPI max.	8.000	12.000	32.000
Protezione senza limiti di dimensioni dei file	✓	✓	✓
Hardware			
Processore dual-core		✓	✓
Gigabit Ethernet		✓	✓
Supporto 802.11n	✓	✓	✓
Supporto dual band 802.11a/b/g/n		✓	✓
Servizi di sicurezza			
Protezione contro le intrusioni*	✓	✓	✓
Gateway anti-virus, anti-spyware e cloud anti-virus*	✓	✓	✓
Filtraggio dei contenuti e URL (CFS)*	✓	✓	✓
Enforced Client Anti-Virus and Anti-Spyware*	✓	✓	✓
Application Intelligence and Control*			✓
*Disponibile con servizio in abbonamento			



Il nuovo SonicWALL TZ 105 è il più sicuro firewall per Unified Threat Management (UTM) disponibile per piccoli uffici, home office e piccole applicazioni retail. A differenza dei prodotti per uso domestico, il TZ 105 fornisce le più efficaci funzionalità per la prevenzione delle intrusioni, anti-malware, per il filtraggio dei contenuti/URL unitamente al più ampio e sicuro supporto per piattaforme mobili per laptop, smartphone e tablet. La serie offre la completa funzionalità di ispezione deep packet (DPI) a livelli prestazionali molto elevati, eliminando il collo di bottiglia di rete causato da altri prodotti e consentendo alle aziende di realizzare maggiori guadagni in produttività senza costi aggiuntivi.



Descrizione hardware

TZ 105 TotalSecure 1 anno
 TZ 105 Wireless-N TotalSecure 1 anno
 TZ 105 Wireless-N TotalSecure International 1 anno

Codice

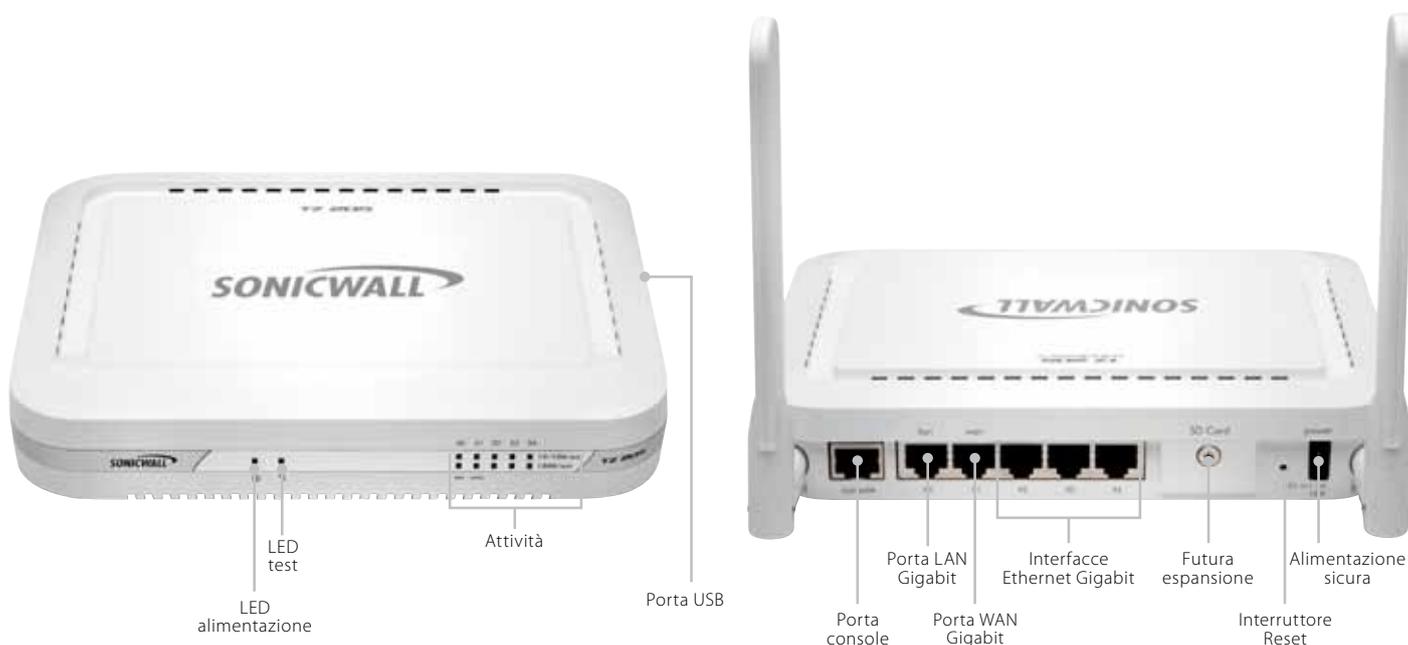
01-SSC-4906
 01-SSC-4908
 01-SSC-4910

Descrizione servizio

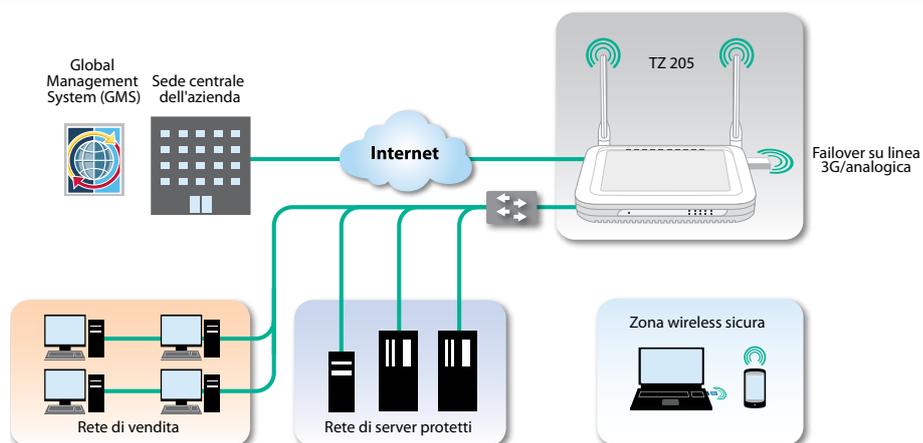
Comprehensive Gateway Security Suite 1 anno
 Gateway Anti-Virus e
 Intrusion Prevention Service 1 anno
 Filtraggio dei contenuti/URL 1 anno
 Comprehensive Anti-Spam Service 1 anno
 Supporto 8x5 1 anno
 Supporto 24x7 1 anno

Codice

01-SSC-4877
 01-SSC-4844
 01-SSC-4850
 01-SSC-4871
 01-SSC-4856
 01-SSC-4862



Piccole aziende, applicazioni retail, pubbliche amministrazioni, filiali in località remote e sedi distaccate possono beneficiare delle potenti prestazioni di sicurezza a livello professionale del nuovo SonicWALL TZ 205. A differenza dei prodotti per uso domestico, questo potente firewall per Unified Threat Management (UTM) unisce le più efficaci funzioni di prevenzione delle intrusioni, anti-malware e filtraggio dei contenuti/URL al più ampio e sicuro supporto per piattaforme mobili per laptop, smartphone e tablet. Fornendo la completa funzionalità di ispezione deep packet (DPI) a livelli di prestazione molto elevati, elimina il compromesso tra protezione completa e prestazioni.

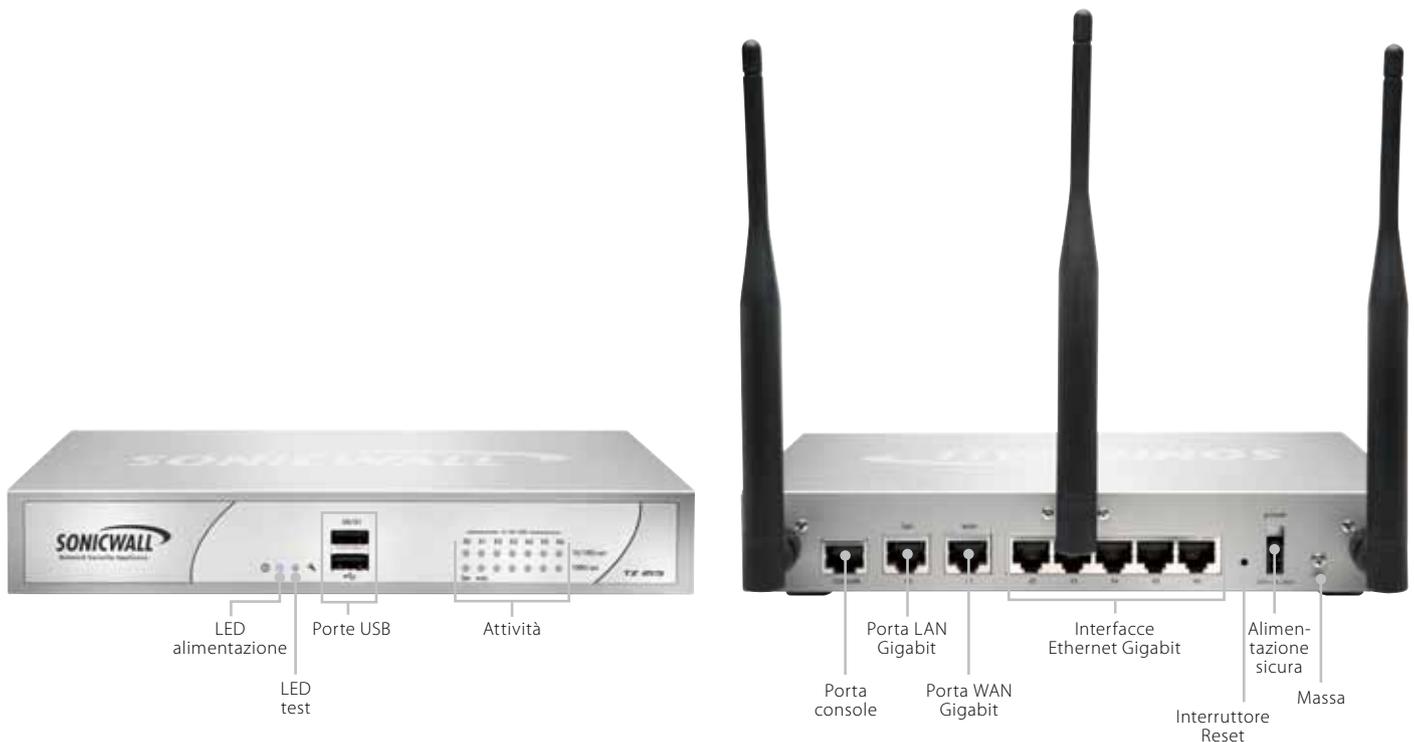


Descrizione hardware

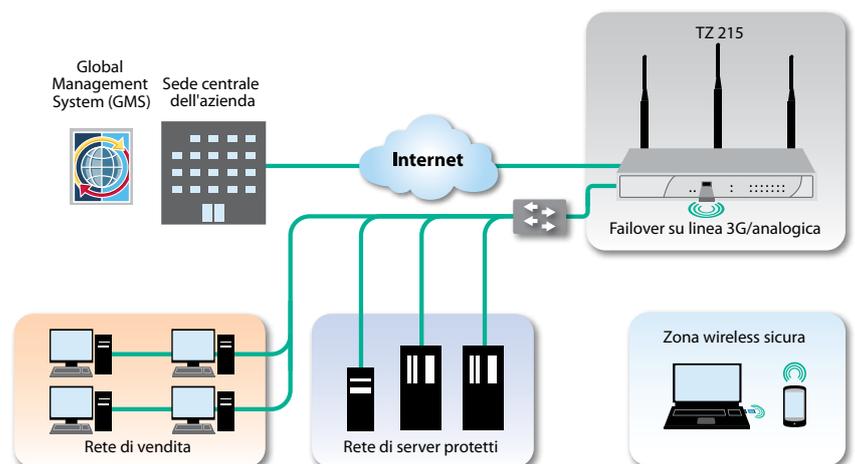
Descrizione hardware	Codice
Hardware TZ 205: cablato	01-SSC-6945
Hardware TZ 205: Wireless-N	01-SSC-6947
Hardware TZ 205: Wireless-N internazionale	01-SSC-4883
TotalSecure TZ 205 1 anno	01-SSC-4906
Wireless-N TotalSecure TZ 205 1 anno	01-SSC-4908
Wireless-N TotalSecure internazionale TZ 205 1 anno	01-SSC-4910

Descrizione servizio

Descrizione servizio	Codice
Comprehensive Gateway Security Suite 1 anno	01-SSC-4838
Gateway Anti-Virus e	01-SSC-4799
Intrusion Prevention Service 1 anno	
Filtraggio dei contenuti/URL 1 anno	01-SSC-4805
Comprehensive Anti-Spam Service 1 anno	01-SSC-4832
Supporto 8x5 1 anno	01-SSC-4811
Supporto 24x7 1 anno	01-SSC-4817



Il nuovo SonicWALL TZ 215 è il più sicuro firewall per Unified Threat Management (UTM) ad alte prestazioni disponibile per piccole aziende e sedi distaccate. Progettato per piccole aziende, aziende distribuite, sedi distaccate e applicazioni retail, il TZ 215 integra funzionalità anti-malware, prevenzione delle intrusioni, controllo delle applicazioni e filtraggio URL, abbattendo i costi e la complessità. Il firewall offre un'architettura dual-core con funzionalità completa di ispezione deep packet (DPI) senza ridurre le prestazioni della rete, eliminando i colli di bottiglia causati da altri prodotti e consentendo alle aziende di realizzare maggiori guadagni in produttività. Il TZ 215 offre inoltre il controllo delle applicazioni per garantire la larghezza di banda per applicazioni strategiche e limitandone l'uso da parte delle applicazioni non produttive. Le funzionalità di networking avanzate comprendono ISP failover multiplo e bilanciamento del carico, wireless dual-band protetto opzionale, supporto IPSec VPN, segmentazione della rete e conformità PCI.



Descrizione hardware

Hardware TZ 215: cablato	01-SSC-4976
Hardware TZ 215: Wireless-N	01-SSC-4977
Hardware TZ 215: Wireless-N internazionale	01-SSC-4969
TotalSecure TZ 215 1 anno	01-SSC-4982
Wireless-N TotalSecure TZ 215 1 anno	01-SSC-4984
Wireless-N TotalSecure internazionale TZ 215 1 anno	01-SSC-4986

Codice

Descrizione servizio

Comprehensive Gateway Security Suite 1 anno	01-SSC-4793
Gateway Anti-Virus e Intrusion Prevention Service 1 anno	01-SSC-4757
Filtraggio dei contenuti/URL 1 anno	01-SSC-4763
Comprehensive Anti-Spam Service 1 anno	01-SSC-4787
Supporto 8x5 1 anno	01-SSC-4769
Supporto 24x7 1 anno	01-SSC-4775

Codice

Funzionalità

Prevenzione delle intrusioni

Scansione basata sulle signature	La prevenzione delle intrusioni integrata e basata sulle signature scansiona i payload dei pacchetti alla ricerca di vulnerabilità ed exploit diretti ai sistemi interni critici.
Aggiornamenti automatici delle signature	Il team di ricerca di SonicWALL aggiorna e distribuisce costantemente un elenco dettagliato di oltre 5.400 signature IPS relative a 52 categorie di attacchi. Queste signature sono immediatamente attive e non richiedono il reboot del sistema o altre interruzioni dei servizi.
Prevenzione delle minacce in uscita	La capacità di ispezionare il traffico sia in entrata che in uscita garantisce che la rete non venga utilizzata a insaputa degli amministratori per attacchi DDoS (Distributed Denial of Service) e impedisce qualsiasi comunicazione tramite canali "Command & Control" di botnet.
Protezione IPS interzona	La prevenzione delle intrusioni può essere implementata tra diverse zone di sicurezza interne per proteggere server con dati sensibili e impedire attacchi interni.

VPN

VPN IPSec per connettività site-to-site	La tecnologia IPSec VPN ad alte prestazioni consente al firewall di collegare filiali aziendali distaccate a una sede centrale.
Accesso remoto tramite VPN SSL o client IPSec	Possibilità di usare la tecnologia clientless VPN SSL oppure un client IPSec di facile gestione per offrire un accesso semplificato a posta elettronica, file, computer, siti intranet e applicazioni da svariate piattaforme.
Gateway VPN ridondante	Se si utilizzano più WAN è possibile configurare una VPN principale e una secondaria per assicurare failover e failback automatizzati e trasparenti per tutte le sessioni VPN.
VPN route-based	La capacità di eseguire il routing dinamico tramite collegamenti VPN garantisce la continuità delle connessioni in caso di interruzione temporanea del tunnel VPN, con un reinstradamento trasparente del traffico tra gli endpoint attraverso percorsi alternativi.
Clean VPN	SonicWALL Clean VPN™ garantisce l'integrità degli accessi alla VPN e neutralizza le minacce nocive prima che possano introdursi nella rete aziendale.

Prevenzione delle minacce a livello del gateway

Gateway Anti-Malware	Il motore RFDPI brevettato da SonicWALL scansiona tutte le porte e i protocolli alla ricerca di virus, senza alcuna limitazione a livello di dimensioni dei file o lunghezza dei flussi di dati. I ricercatori del SonicLabs forniscono costantemente una protezione aggiornata contro le minacce per garantire tempi di risposta e prevenzione più rapidi.
Reassembly-Free Deep Packet (RFDPI) Inspection	L'ispezione approfondita dei pacchetti senza riassemblaggio tiene traccia del malware indipendentemente dalla sequenza e dalla tempistica di ispezione in arrivo dei pacchetti, garantendo una latenza estremamente bassa senza limitazioni sulle dimensioni dei file e dei flussi di dati. In questo modo fornisce migliori prestazioni e una maggiore sicurezza rispetto alla tradizionale architettura proxy, che riassume il contenuto tramite socket associati a programmi anti-virus tradizionali con notevoli inefficienze e un eccessivo thrashing per la memoria dei socket, che provoca elevati ritardi, calo di prestazioni e limitazioni alle dimensioni dei file.
Cloud Anti-Virus (AV)	Utilizzando il motore RFDI integrato, SonicWALL può sfruttare la potenza del cloud per fornire il più completo set di signature anti-malware disponibili, riducendo al minimo la latenza o il ritardo. Il servizio SonicWALL Cloud Anti-Virus fornisce milioni di signature di malware aggiuntive per il controllo dei file eseguibili che utilizzano le informazioni più aggiornate disponibili.
Ispezione bidirezionale	L'ispezione RFDPI può essere eseguita sulle connessioni in entrata e in uscita dalla rete, garantendo protezione per ogni direzione del traffico.
Aggiornamenti delle signature 24x7	Il team di ricerca del SonicLabs crea e aggiorna i database di signature, che vengono automaticamente inviati ai firewall in uso. Le signature hanno effetto immediato, senza bisogno di riavviare il sistema o interrompere i servizi.

Firewall e networking

Ispezione Stateful Packet	Tutto il traffico in transito nella rete viene ispezionato, analizzato e conformato alle policy di accesso del firewall.
Protezione da attacchi DoS	La protezione SYN Flood offre una difesa contro gli attacchi DoS mediante tecnologie di blacklisting sia al layer 3 (SYN proxy) che al layer 2 (SYN).
Implementazione flessibile	Possibilità di implementazione nelle tradizionali modalità NAT e Bridge Layer 2.
Routing basato sulle policy	Creazione di instradamenti basati sui protocolli per dirigere il traffico verso una determinata connessione WAN, con possibilità di commutare su una WAN secondaria in caso di caduta dell'alimentazione.
Alta disponibilità	Supporto failover attivo/passivo per garantire una maggiore affidabilità con la protezione da errori hardware o software.
Bilanciamento del carico WAN	Bilanciamento del carico per un massimo di quattro interfacce WAN con metodi basati sulle modalità round robin, percentuale e spill-over.
Accelerazione della WAN	L'accelerazione WAN riduce la latenza e aumenta le velocità di trasferimento tra siti remoti, favorendo una maggiore efficienza della rete.

Funzionalità

VoIP

QoS avanzata	Protezione delle comunicazioni mission-critical tramite tagging 802.1p e DSCP e rimappatura del traffico VoIP sulla rete.
Ispezione deep packet del traffico VoIP	Rilevazione e blocco di minacce specifiche del traffico VoIP mediante signature predefinite.
Supporto per gatekeeper H.323 e proxy SIP	Blocco delle chiamate di spam: tutte le chiamate in entrata devono essere autorizzate e autenticate dal gatekeeper H.323 o dal proxy SIP.

Gestione e monitoraggio

GUI basata sul Web	Un'intuitiva interfaccia basata sul Web consente una configurazione rapida e conveniente, con possibilità di gestione tramite il Global Management System di SonicWALL (GMS®) o l'interfaccia a riga di comando (CLI).
SNMP	SNMP offre la possibilità di monitorare il sistema e reagire prontamente a minacce e allarmi.
Netflow/IPFIX	Mediante i protocolli IPFIX o Netflow è possibile esportare un ampio set di dati per ottenere una visione granulare su traffico delle applicazioni, banda utilizzata e minacce alla sicurezza, insieme a potenti funzioni di risoluzione dei problemi e analisi forense. Compatibile con SonicWALL Scrutinizer e applicazioni di reporting e monitoraggio di terzi (solo TZ 215).
Gestione centralizzata delle policy	Il sistema SonicWALL GMS consente di monitorare, configurare e creare report per svariate appliance SonicWALL da un'unica e intuitiva interfaccia, con possibilità di personalizzare il proprio ambiente di sicurezza in conformità alle policy definite.

Application Intelligence and Control

Controllo delle applicazioni	Identificazione e controllo di applicazioni o singoli componenti di un'applicazione mediante la tecnologia RFDPI e non in base al controllo di porte e protocolli conosciuti.
Gestione della larghezza di banda delle applicazioni	Assegnazione della banda ad applicazioni strategiche, con limitazione del traffico di applicazioni non produttive, per una rete efficiente e produttiva.
Identificazione personalizzabile delle applicazioni	Creazione e configurazione di criteri personalizzati per identificare le applicazioni in base a parametri di traffico o a modelli di comunicazione univoci per ogni applicazione.
Analisi del traffico delle applicazioni	Offre alle aziende una visione granulare su traffico delle applicazioni, uso della larghezza di banda e sicurezza, integrata da potenti funzioni di risoluzione dei problemi e analisi forense (solo TZ 215).
Database di signature delle applicazioni	Un database in continua espansione, con oltre 3.500 firme di applicazioni, consente agli amministratori di monitorare l'uso di tutte le più recenti applicazioni nella rete, sia per categoria che a livello singolo.
Monitoraggio delle attività degli utenti	Il servizio di identificazione degli utenti, integrabile in modo trasparente con Microsoft® Active Directory e altri sistemi di autenticazione, consente di monitorare le attività di singoli utenti e generare report.
Identificazione del traffico in base al paese (GeoIP)	Rilevamento e controllo del traffico di rete proveniente o diretto in paesi specifici (solo TZ 215).

Firewall e networking

Firewall

- Reassembly-Free Deep Packet Inspection
- Ispezione Stateful Packet
- Protezione da attacchi DoS
- Reassembly TCP
- Modalità Stealth

Controllo delle applicazioni

- Controllo delle applicazioni
- Blocco di componenti delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme personalizzate per le applicazioni
- Visualizzazione del flusso delle applicazioni
- Prevenzione di fughe di dati
- IPFIX con reporting sulle estensioni
- Monitoraggio delle attività degli utenti
- Identificazione del traffico in base al paese (GeoIP)
- Ampio database di signature delle applicazioni

Prevenzione delle intrusioni

- Scansione basata sulle signature
- Aggiornamenti automatici delle signature
- Prevenzione delle minacce in uscita
- Lista di esclusione IPS
- Messaggi di log interattivi
- CFS e controllo applicazioni unificati con limitazione della larghezza di banda

Anti-Malware

- Scansione anti-malware basata sui flussi
- Gateway anti-virus
- Gateway anti-spyware
- Servizio Cloud Anti-Virus

VoIP

- QoS avanzata
- Gestione della larghezza di banda
- Ispezione deep packet del traffico VoIP
- Interoperabilità completa
- Supporto per gatekeeper H.323 e proxy SIP

Networking

- Routing dinamico
- Routing basato sulle policy
- NAT avanzato
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link
- Ridondanza delle porte
- Alta disponibilità
- IPv6 compatibile
- Bilanciamento del carico

Gestione e monitoraggio

- GUI basata sul Web
- Interfaccia a riga di comando
- SNMP
- Reporting con Analyzer
- Reporting con Scrutinizer
- Gestione policy e reporting con GMS
- Logging
- Netflow/IPFIX
- Visualizzazione delle applicazioni
- Gestione centralizzata delle policy
- Single Sign-On
- Supporto Terminal Service/Citrix

Servizi di sicurezza

- Servizio di prevenzione delle intrusioni
- Anti-malware a livello del gateway
- Content Filtering Service
- Opzioni Enforced Client Anti-Virus e Anti-Spyware Service – McAfee® o Kaspersky®
- Controllo intelligente e visualizzazione delle applicazioni

Specifiche del prodotto

Firewall	Serie TZ 105	Serie TZ 205	Serie TZ 215
Versione SonicOS	SonicOS 5.8.1 e successivo		
Throughput Stateful¹	200 Mbps	500 Mbps	500 Mbps
Throughput IPS²	60 Mbps	80 Mbps	110 Mbps
GAU/Throughput²	40 Mbps	60 Mbps	70 Mbps
Throughput UTM²	25 Mbps	40 Mbps	60 Mbps
Connessioni (max.)³	8.000	12.000	48.000
Connessioni UTM/DPI max.	8.000	12.000	32.000
Nuove connessioni/sec.	1.000	1.500	1.800
Nodi supportati	Illimitati		
Protezione da attacchi Denial of Service	22 classi di attacchi DoS, DDoS e scanning		
SonicPoint supportati	1	2	16
VPN			
Throughput 3DES/AES⁴	75 Mbps	100 Mbps	130 Mbps
Tunnel VPN site-to-site	5	10	15
Licenze GVC in bundle (max.)	0 (5)	2 (10)	2 (25)
Licenze SSL VPN in bundle (max.)	1 (5)	1 (10)	2 (10)
Crittografia/autenticazione/DH Group	DES, 3DES, AES (a 128, 142, 256 bit), MD5, SHA-1/DH Gruppo 1, 2, 5, 14		
Virtual Assist in bundle (max.)	—	1 versione di prova gratuita per 30 giorni	2 versione di prova gratuita per 30 giorni
Scambio delle chiavi	IKE, connessione manuale, certificati (X.509), L2TP over IPsec		
Supporto certificati	Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA per VPN da SonicWALL, SCEP		
Caratteristiche VPN	Dead Peer Detection, DHCP Over VPN, IPsec NAT Traversal, Gateway VPN ridondante, VPN route-based		
Global VPN Client, piattaforme supportate	Microsoft® Windows XP, Vista a 32/64 bit, Windows 7 a 32/64 bit		
SSL VPN, piattaforme supportate	Microsoft Windows XP/Vista 32/64 bit/Windows 7, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE		
Mobile Connect, piattaforma supportata	Apple iOS 4.2 e superiore, Google® Android™ 4.0 e superiore		
Servizi di sicurezza			
Servizi di ispezione Deep Packet	Gateway anti-virus, anti-spyware, prevenzione delle intrusioni, Application Intelligence and Control (solo TZ 215)		
Content Filtering Service (CFS)	Scansione HTTP URL, HTTPS IP, parole chiave e contenuti, blocco controlli ActiveX, applet Java e cookie, gestione della banda per le categorie di filtraggio, liste di autorizzazione/blocco		
Enforced Client Anti-Virus and Anti-Spyware	McAfee® oppure Kaspersky®		
Comprehensive Anti-Spam Service⁵	Supportato		
Application Intelligence and Control	Controllo delle applicazioni	Visualizzazione del traffico delle applicazioni e gestione della larghezza di banda	
Networking			
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay		
Modalità NAT	1:1, 1:many, many:1, many:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente		
VLAN	5, PortShield	10, PortShield	20, PortShield
DHCP	Server interno, relay		
Routing	OSPF, RIP v1/v2, route statici, routing basato su policy, multicast		
Autenticazione	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, database utenti interno, servizi Terminal Server, Citrix		
Database utenti locale	150 utenti		
VoIP	Supporto completo H.323 v. 1-5, SIP e gatekeeper, gestione larghezza di banda in uscita, VoIP over WLAN, protezione Deep Inspection, interoperabilità completa con i gateway VoIP e i dispositivi di comunicazione più comuni		
Sistema			
Sicurezza di zona	SI		
Planificazioni	SI		
Gestione basata su oggetti/gruppi	SI		
DDNS	I fornitori di DNS dinamico includono: dyndns.org, yi.org, no-ip.com e changeip.com		
Gestione e monitoraggio	Gestione e monitoraggio, Web GUI (HTTP, HTTPS), SNMP v2; gestione globale con SonicWALL GMS		
Logging e reporting	Analyzer, Scrutinizer, GMS, registro locale, Syslog, reti Solera, NetFlow v5/v9, IPFIX con estensioni, visualizzazione in tempo reale		
Hardware failover	—	Attivo/Passivo	Attivo/Passivo
Anti-spam	Supporto RBL, elenchi di autorizzazione/blocco, SonicWALL Comprehensive Anti-Spam Service opzionale ⁶		
Bilanciamento del carico	SI, in uscita e in entrata		
Standard	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
Supporto per accelerazione della WAN⁷	SI, con Appliance SonicWALL WXA		
Wireless LAN integrata			
Standard	802.11b/g/n	802.11a/b/g/n (2x2)	802.11a/b/g/n (3x3)
Standard di sicurezza wireless	(WEP, WPA, WPA2, 802.11i, TKIP, PSK, 02, tx, EAP-PEAP, EAP-TLS)		
Access Point virtuali (VAP)	fino a 8		
Antenne	Doppia esterna, staccabile	Doppia esterna, staccabile	Tre esterne, staccabili
Potenza radio-802.11b/802.11g/802.11n	18 dBm max/18 dBm a 6 Mbps, 15 dBm a 54 Mbps	15.5 dBm max/18 dBm max/17 dBm a 6 Mbps, 13 dBm a 54 Mbps	15.5 dBm max/18 dBm max/17 dBm a 6 Mbps, 13 dBm a 54 Mbps
Potenza radio-802.11a/802.11b/802.11n	—	15.5 dBm max/18 dBm max/17 dBm a 6 Mbps, 13 dBm a 54 Mbps	15.5 dBm max/18 dBm max/17 dBm a 6 Mbps, 13 dBm a 54 Mbps
Potenza radio-802.11n (2,4 GHz)/802.11n (5,0 GHz)	19 dBm MCS 0, 12 dBm MCS 15	19 dBm MCS 0, 11 dBm MCS 15/17 dBm MCS 0, 12 dBm MCS 15	19 dBm MCS 0, 11 dBm MCS 15/17 dBm MCS 0, 12 dBm MCS 15
Sensibilità in ricezione radio-802.11a/802.11b/802.11g	-90 dBm a 11Mbps/-91 dBm a 6 Mbps, -74 dBm a 54 Mbps	-95 dBm MCS 0, -81 dBm MCS 15/-90 dBm a 11Mbps/-91 dBm a 6Mbps, -74 dBm a 54 Mbps	-95 dBm MCS 0, -81 dBm MCS 15/-90 dBm a 11Mbps/-91 dBm a 6Mbps, -74 dBm a 54 Mbps
Sensibilità in ricezione radio-802.11n (2,4GHz)/802.11n (5,0GHz)	-89 dBm MCS 0, -70 dBm MCS 15	-89 dBm MCS 0, -70 dBm MCS 15/ -95 dBm MCS 0, -76 dBm MCS 15	-89 dBm MCS 0, -70 dBm MCS 15/ -95 dBm MCS 0, -76 dBm MCS 15
Wireless LAN hardware integrata			
Interfacce	(5) 10/100 Fast Ethernet, 1 USB, 1 Console	(5) 10/100/1000 porte Gigabit in rame, 1 USB, 1 Console	(7) 10/100/1000 porte Gigabit in rame, 2 USB, 1 Console
Processore	Single-Core	Dual-Core	Dual-Core
Memoria Flash/RAM	32 MB/256 MB	32 MB/256 MB	32 MB/512 MB
3G Wireless/modem⁸	Supportato con adattatori approvati ⁹		
Porte USB	1	1	2
Alimentazione	da 100 a 240 VAC, 50-60 Hz, 1 A		
Potenza max. assorbita	5,2W/7,0W	6,4W/10,5W	9,0W/12,0W
Calore sviluppato	17,8 BTU/23,7 BTU	21,9 BTU/35,8 BTU	30,6 BTU/41,4 BTU
Certificazioni	EAL4+, FIPS 140-2 Level 2, IPv6 Phase 1, IPv6 Phase 2		
Certificazioni (in attesa)	VPNC, ICSA Firewall 4.1		
Fattore di forma e misure	5.555 x 1.42 x 7.48 in (14,1 x 3,6 x 19 cm)	5.555 x 1.42 x 7.48 in (14,1 x 3,6 x 19 cm)	7.125 x 1.5 x 10.5 in (18,1 x 3,81 x 26,67 cm)
Peso	0.75 lbs/0,34 kg 0.84 lbs/0,38 kg	0.75 lbs/0,34 kg 0.84 lbs/0,38 kg	1.95 lbs/0,97 kg 2.15 lbs/0,97 kg
Principali normative di conformità	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, NOM, UL, cUL, TUV/GS, CB, NOM, WEEE, RoHS		
Condizioni ambientali/umidità	0-40 °C, umidità 5-95% non condensante		
MTBF	28 anni/15 anni		

¹ Metodologie di test: prestazioni massime come da RFC 2544 (per il firewall). Le prestazioni effettive possono variare in base alle condizioni della rete e ai servizi attivati. ² Rilevazione throughput per UTM/Gateway AV/Anti-Spyware/IPS tramite il test di performance Spirent WebAvalanche HTTP standard nell'industria e gli strumenti di test Ixia. Test eseguiti con flussi multipli attraverso coppie di porte multiple. ³ Il numero massimo effettivo di connessioni diminuisce quando sono attivati i servizi DPI. ⁴ Rilevazione throughput VPN tramite traffico UDP con pacchetti da 1280 byte, in conformità a RFC 2544. ⁵ Scheda 3G e modem non inclusi. Per i dispositivi USB supportati vedi <http://www.sonicwall.com/us/products/cardsupport.html>. ⁶ Il Comprehensive Anti-Spam Service supporta un numero illimitato di utenti ma è consigliato per un massimo di 250 utenti. ⁷ Con Appliance SonicWALL Serie WXA.



Linea di soluzioni di sicurezza dinamica SonicWALL



SICUREZZA DI RETE



ACCESSO REMOTO SICURO



SICUREZZA WEB / E-MAIL



BACKUP E RECOVERY



GESTIONE BASATA SU POLICY

SonicWALL Italy

T + 39.010.7407851

Italy@sonicwall.com

Contatti Supporto SonicWALL

www.sonicwall.com/emea/4724.html

SONICWALL

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™