SONICWALL

SONICWALL SECURE MOBILE ACCESS (SMA)

Accesso sicuro dovunque e in qualsiasi momento a risorse aziendali in ambienti multi-cloud basato sull'identità, l'ubicazione e l'affidabilità di utenti e dispositivi.

SonicWall SMA costituisce un gateway di accesso sicuro unificato che consente alle organizzazioni di accedere - in qualsiasi luogo e in qualsiasi momento e su qualsiasi dispositivo - a risorse aziendali mission critical. L'engine delle politiche di controllo granulare degli accessi di SMA, l'autorizzazione dei dispositivi in base al contesto, la VPN a livello di applicazione e l'autenticazione avanzata con Single Sign-on consentono alle aziende di adottare il BYOD e la mobilità in un ambiente informatico multi-cloud.

Mobilità e BYOD

Per le organizzazioni che desiderano adottare il BYOD, lavorare in modo flessibile o consentire l'accesso a terzi, SMA diventa il punto di attuazione centrale per tutti questi aspetti. SMA offre la migliore sicurezza nel settore per ridurre al minimo le minacce in superficie, rendendo più sicure le organizzazioni grazie al supporto dei più recenti algoritmi di crittografia e cifrari. SMA di SonicWall consente agli amministratori di fornire un accesso mobile sicuro e privilegi basati sulle identità in modo che gli utenti finali ottengano un accesso semplice e veloce alle applicazioni, ai dati e alle risorse aziendali di cui hanno bisogno. Allo stesso tempo, le aziende possono definire criteri di BYOD sicuro per proteggere le proprie reti e i dati aziendali da accessi non autorizzati e dal malware.

Il passaggio al cloud

Per le aziende che si apprestano a compiere la migrazione verso il cloud, SMA offre un'infrastruttura Single Sign-On (SSO) che utilizza un singolo portale Web per autenticare gli utenti in un ambiente informatico ibrido. L'esperienza di accesso è coerente e trasparente, indipendentemente dal fatto che la risorsa aziendale si trovi in sede, nel web o in un cloud in hosting. SMA inoltre si integra con le principali tecnologie di autenticazione multifattoriale attualmente disponibili in campo industriale per garantire una maggiore sicurezza.

Fornitori di servizi gestiti

SMA propone una soluzione chiavi in mano per offrire un elevato grado di continuità e modularità aziendale sia alle organizzazioni con proprie infrastrutture, sia ai provider di servizi gestiti. SMA è in grado di supportare fino a 20.000 connessioni simultanee su una singola apparecchiatura, con una modularità verticale fino a centinaia di migliaia di utenti tramite un clustering intelligente. I data center possono ridurre i costi con il clustering attivo/attivo e con un bilanciatore di carico dinamico integrato, che consente di riallocare il traffico globale verso il data center più ottimizzato in tempo reale e in base alle esigenze dell'utente. Gli strumenti SMA mettono le aziende specializzate in condizione di fornire servizi con tempi di indisponibilità zero, consentendo loro di soddisfare i requisiti più esigenti dei Service Level Agreement (SLA).

SMA fornisce ai reparti informatici la migliore esperienza e l'accesso più sicuro possibile a seconda dello scenario d'uso. Disponibile come apparecchiatura fisica hardened o potente apparecchiatura virtuale, SMA si inserisce senza soluzione di continuità nelle infrastrutture interne o nel cloud esistenti. Le organizzazioni possono scegliere tra una gamma di soluzioni per l'accesso sicuro basato sul web completamente clientless per terzi o dipendenti tramite dispositivi personali, oppure un più tradizionale accesso completo a tunnel VPN basato su client per i dirigenti da qualsiasi tipo di dispositivo. SonicWall SMA ha una soluzione sia per le organizzazioni che devono fornire un accesso sicuro e affidabile a cinque utenti da un'unica postazione, sia per le imprese che necessitano di modularità fino a migliaia di utenti in reti distribuite globalmente.

SonicWall SMA consente alle organizzazioni di adottare mobilità e BYOD senza timori, e passare più facilmente al cloud. SMA consente più autonomia ai lavoratori, mettendo a loro disposizione modalità di accesso valide per tutti.

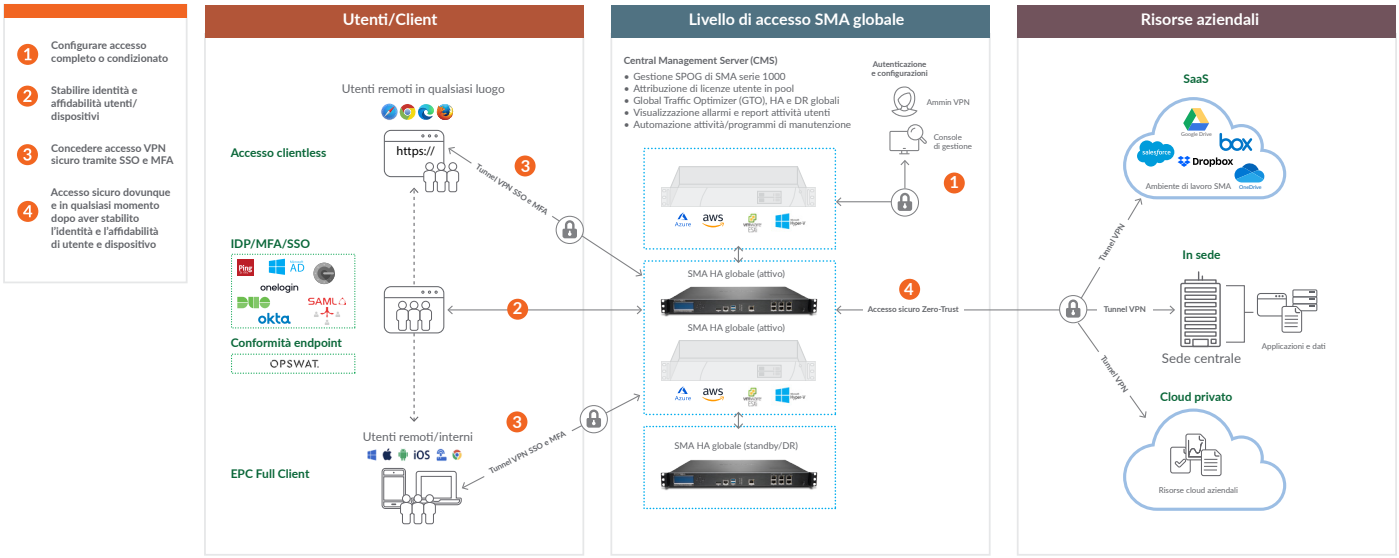
Vantaggi:

- Accesso sicuro unificato a tutte le risorse di rete e nel cloud "in qualsiasi momento, per qualsiasi dispositivo e per qualsiasi applicazione"
- Controllare chi accede a quali risorse definendo politiche granulari tramite il robusto engine di controllo degli accessi
- Aumentare la produttività consentendo il Single Sign-On federato a qualsiasi applicazione SaaS o locale con un singolo URL
- Ridurre il costo totale della proprietà e la complessità della gestione degli accessi consolidando le componenti delle infrastrutture in un ambiente informatico ibrido
- Sapere quali dispositivi cercano di collegarsi e concedere l'accesso sulla base delle politiche e dello stato di salute degli endpoint
- Impedire le violazioni da parte del malware scansionando tutti i file caricati in rete tramite la sandbox Capture ATP
- Proteggersi contro gli attacchi basati sul web e garantire la conformità PCI con l'add-on Web Application Firewall
- Bloccare gli attacchi DDoS e zombie tramite il rilevamento Geo IP e la protezione Botnet
- Disporre della funzionalità sicura con agente nativo tramite accesso clientless HTML5 basato su web browser senza l'impegno di dover installare e mantenere agenti sui dispositivi endpoint
- Ottenere informazioni approfondite fruibili per prendere le decisioni giuste con il monitoraggio in tempo reale e la reportistica completa
- Installare sotto forma di apparecchiature fisiche o virtuali in cloud privati su ESXi o Hyper-V, o in ambienti cloud pubblici AWS o Microsoft Azure
- Abilitare l'emissione dinamica delle licenze di accesso basate sulla domanda in tempo reale, con indirizzamento automatico dell'endpoint alla connessione più performante e dalla latenza più bassa
- Riduzione dei costi iniziali grazie al bilanciamento del carico integrato senza hardware o servizi aggiuntivi, senza alcun impatto per l'utente sul failover dell'apparecchiatura
- Assicurazione contro le interruzioni di servizio o i picchi stagionali grazie all'immediata modularità della capacità

Installazione SMA

Un gateway dalla sicurezza potenziata per l'accesso sicuro, sempre e ovunque, da qualsiasi dispositivo

I gateway SMA mettono a disposizione un accesso remoto sicuro end-to-end completo alle risorse aziendali che si trovano in sede, nel cloud e in data center ibridi. Si tratta di apparecchiature che utilizzano controlli di accesso basati sulle politiche e sull'identità, autenticazione contestuale dei dispositivi e VPN a livello di applicazioni per consentire l'accesso a dati, risorse e applicazioni dopo aver stabilito l'identità e l'affidabilità dell'utente, dell'ubicazione e del dispositivo. Vengono installate in modo flessibile sotto forma di apparecchiature Linux hardened o di apparecchiature virtuali in cloud privati su ESXi o Hyper-V, o in ambienti cloud pubblici AWS o Microsoft Azure



Installazione SMA nel cloud / in sede

Installazione flessibile con apparecchiature fisiche e virtuali

SonicWall SMA può essere installato come apparecchiatura hardened ad alte prestazioni o come apparecchiatura virtuale, sfruttando le risorse di calcolo condivise per ottimizzare l'utilizzo, facilitare la migrazione e ridurre i costi di investimento. I dispositivi hardware sono basati su un'architettura multi-core ad elevate prestazioni che offre accelerazione SSL, throughput VPN e potenti proxy per garantire un accesso sicuro e affidabile. Per le organizzazioni regolamentate e per quelle federali, SMA è disponibile anche con certificazione FIPS 140-2 Level 2. Le apparecchiature virtuali SMA offrono le stesse caratteristiche avanzate di accesso sicuro delle principali piattaforme virtuali o del cloud, come Microsoft Hyper-V, VMware ESX e AWS.

Licenze d'uso utilizzabili da diverse apparecchiature

Le organizzazioni che dispongono di apparecchiature distribuite su scala globale possono beneficiare dell'oscillazione della domanda di licenze d'uso legata ai fusi orari. Indipendentemente dal fatto che un'organizzazione utilizzi licenze VPN complete o licenze ActiveSync di base, la gestione centralizzata di SMA riassegna le licenze alle apparecchiature gestite nelle aree geografiche in cui si sono avuti picchi di domanda dalle applicazioni di altre zone geografiche, nelle quali l'uso è diminuito per via dell'assenza dal lavoro degli utenti nelle ore notturne.

Visibilità di rete con profilatura dei dispositivi sulla base delle situazioni contingenti

Il sistema di autenticazione di fascia alta, che tiene conto delle situazioni contingenti, consente l'accesso solo ai dispositivi affidabili e agli utenti autorizzati. Anche i portatili e i PC vengono analizzati per rilevare la presenza o l'assenza di software di sicurezza, certificati client e ID dei dispositivi. Prima di consentire l'accesso i dispositivi mobili vengono analizzati per verificare le informazioni di sicurezza essenziali come jailbreak o stato della root, ID del dispositivo, stato dei certificati e versione del sistema operativo. Ai dispositivi che non soddisfano i requisiti della politica non viene concesso l'accesso alla rete e l'utente viene avvisato della mancata conformità.

Esperienza coerente da un unico portale web

Gli utenti non devono ricordarsi tutti gli URL delle singole applicazioni o conservare segnalibri dettagliati. SMA dispone di un portale di accesso centralizzato che fornisce agli utenti un URL per accedere a tutte le applicazioni fondamentali da un browser web standard. Quando l'utente ha effettuato l'accesso da un browser, nella finestra del browser viene visualizzato un portale web personalizzabile destinato agli utenti, con un unico punto di controllo per accedere a qualsiasi applicazione SaaS o locale. Il portale visualizza solamente i collegamenti e i segnalibri personalizzati relativi a un gruppo, a un utente o a un dispositivo endpoint specifico. Il portale è una piattaforma agnostica e supporta tutte le principali piattaforme, compresi i dispositivi Windows, Mac OS, Linux, iOS e Android, oltre a supportare numerosi browser per tutti questi dispositivi.

Single Sign-On federato alle applicazioni SaaS e a quelle locali

Eliminare l'esigenza di password multiple e porre fine alle cattive prassi di sicurezza come il riutilizzo delle password. SMA consente un SSO federato alle applicazioni SaaS ospitate nel cloud e a quelle ospitate nel campus. SMA si integra con diversi server di autenticazione, autorizzazione e contabilità e tecnologie leader nel campo dell'autenticazione multifattoriale per una maggiore sicurezza. Il Single Sign-On sicuro viene fornito solo ai dispositivi endpoint autorizzati dopo che SMA verifica l'integrità e la conformità degli endpoint. L'engine della politica di accesso garantisce che gli utenti possano visualizzare solo le applicazioni autorizzate e concedere l'accesso previa autenticazione andata a buon fine. La soluzione supporta un SSO federato anche quando si utilizzano client VPN, mettendo

a disposizione dei clienti un'esperienza di autenticazione senza soluzione di continuità indipendentemente dal fatto che utilizzino un accesso sicuro basato su client o clientless.

Prevenire le violazioni e le minacce avanzate

SonicWall SMA aggiunge un livello di sicurezza d'accesso per migliorare la sicurezza e ridurre la superficie di accesso per le minacce.

- SMA si integra con la sandbox multi-engine basata su cloud SonicWall Capture ATP per effettuare la scansione di tutti i file caricati dagli utenti con endpoint non gestiti o da quelli fuori dalla rete aziendale. Ciò garantisce che gli utenti abbiano lo stesso livello di protezione dalle minacce avanzate, come ransomware o il malware zero-day, quando sono in viaggio come se fossero in ufficio[1].
- Il servizio SonicWall Web Application Firewall mette a disposizione delle aziende una soluzione affidabile e integrata per rendere sicure le applicazioni interne basate sul web. Ciò consente ai clienti di garantire la riservatezza dei dati e che i servizi web interni non vengano compromessi in presenza di accessi da parte di utenti malintenzionati o fraudolenti.
- Il rilevamento di Geo-IP e Botnet protegge le organizzazioni dagli attacchi DDoS e zombie e dagli endpoint compromessi che funzionano come botnet.

Accesso clientless sicuro basato sul browser senza soluzione di continuità

La natura "clientless" di SonicWall SMA significa che gli amministratori non devono installare manualmente componenti fat client sui computer da utilizzare per l'accesso remoto. In questo modo si elimina qualsiasi dipendenza da Java e l'impegno per il reparto informatico, aumentando di conseguenza in modo notevole la possibilità di accesso remoto. Ciò significa che, in assenza di requisiti di pre-installazione o di pre-configurazione, i telelavoratori autorizzati possono utilizzare qualsiasi computer, in qualsiasi parte del mondo, ed accedere in modo sicuro alle risorse aziendali. Nella sua forma più pura, l'accesso sicuro è basato rigorosamente sul browser tramite HTML5, il che offre agli utenti un'esperienza senza soluzione di continuità e unificata.

Offrire un'esperienza "Always On"

Per consentire agli utenti un'esperienza senza soluzione di continuità, SMA mette a disposizione una Always On VPN per i dispositivi Windows gestiti. Gli amministratori possono configurare le impostazioni in modo che venga stabilita automaticamente una connessione VPN ogniqualvolta un client endpoint autorizzato rileva la presenza di una rete pubblica o non affidabile. Ogni accesso al dispositivo Windows mette a disposizione dell'utente una connessione sicura con le risorse aziendali. Gli utenti non devono effettuare l'accesso sui loro client VPN né gestire ulteriori password. Ciò consente un'esperienza senza soluzione di continuità per gli utenti mobili per accedere alle risorse critiche esattamente come se si trovassero in ufficio e consente agli amministratori dei sistemi informatici di mantenere il controllo sui dispositivi gestiti, migliorando la sicurezza dell'organizzazione.

Gestione intuitiva e reportistica completa

SonicWall offre una piattaforma di gestione intuitiva basata sul web, Central Management Server (CMS), per semplificare la gestione delle apparecchiature e fornire ampie funzionalità di reportistica. L'interfaccia utente grafica di facile uso agevola la gestione di apparecchiature e politiche singole o multiple. Ogni pagina mostra come sono configurati i parametri di tutte le macchine in gestione. La gestione unificata delle politiche consente di creare e monitorare le politiche e le configurazioni di accesso. Un'unica politica può controllare l'accesso da parte di utenti, dispositivi e applicazioni, a dati, server e reti. I responsabili informatici possono automatizzare le attività di routine e quelle pianificate, liberando i team addetti alla sicurezza dai compiti ripetitivi affinché si concentrino su attività di sicurezza strategiche, come la risposta agli eventi imprevisti. Essi, inoltre, acquisiscono utili indicazioni sulle tendenze d'accesso degli utenti e sullo stato di salute dell'intero sistema attraverso una reportistica di facile uso e la funzione di log centralizzata.

Consentire la disponibilità dei servizi 24x7

Le organizzazioni hanno l'esigenza di mantenere i servizi forniti attivi e funzionanti con un elevato grado di affidabilità per consentire l'accesso sicuro alle applicazioni critiche in qualsiasi momento. Le apparecchiature SMA supportano la modalità tradizionale attivo/passivo ad alta disponibilità (HA) per organizzazioni che dispongono di un unico data center, o la modalità attivo/attivo HA globale o il clustering attivo/standby per i data center locali o distribuiti. Entrambi i modelli HA consentono agli utenti un'esperienza uniforme con failover a impatto zero e persistenza di sessione.

Implementazione del client VPN in base alle esigenze dell'utente

È possibile scegliere tra un'ampia gamma di client VPN per fornire un accesso remoto sicuro e vincolante a vari endpoint, compresi portatili, smartphone e tablet.

Client VPN	SO supportato	Modello SMA supportato	Caratteristica principale
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	Tutti i modelli	Fornisce l'autenticazione biometrica, tramite VPN app e implementazione del controllo degli endpoint
Connect Tunnel (Thin Client)	Windows, Mac OS e Linux	6200, 6210, 7200, 7210, 8200v, 9000	Fornisce un'esperienza completa "come in ufficio" con un solido controllo degli endpoint
NetExtender (Thin Client)	Windows e Linux	210, 410, 500v	Implementa politiche di accesso granulari ed estende l'accesso alla rete tramite client nativi

Ridurre i costi iniziali grazie alla funzione integrata di bilanciamento del carico

La funzione di bilanciamento del carico integrata nelle apparecchiature SMA consente la modularità dei livelli prevista per le installazioni nelle PMI e nelle grandi aziende. Alcuni modelli delle apparecchiature SMA sono dotati della funzione di bilanciamento dinamico del carico per assegnare in modo intelligente i carichi delle sessioni e attribuire le licenze d'uso in tempo reale sulla base della domanda. Le organizzazioni non devono investire in sistemi di bilanciamento del carico esterni, riducendo in tal modo i costi iniziali.

Un'assicurazione contro gli eventi imprevisti

Una soluzione completa di continuità aziendale e recupero in caso di disastri deve essere in grado di gestire un picco significativo nel traffico di accesso remoto, continuando a mantenere la sicurezza e il controllo dei costi. I pacchetti di licenze SonicWall Spike per SMA sono licenze aggiuntive che consentono alle aziende distribuite di modulare il conteggio degli utenti e raggiungere la massima capacità istantaneamente, garantendo una continuità aziendale ininterrotta. Le licenze Spike funzionano come una polizza assicurativa nei confronti di eventuali picchi futuri previsti o meno da parte di decine o centinaia di ulteriori utenti rispetto a quelli correnti.

Funzioni

Autenticazione avanzata

Single Sign-On federato[2]	SMA utilizza l'autenticazione SAML 2.0 per consentire un SSO federato tramite un unico portale sia alle risorse in sede sia nel cloud, mentre impone l'autenticazione multifattoriale stacked per una maggiore sicurezza.
Autenticazione multifattoriale	Certificati digitali X.509 Certificati digitali lato server e lato client RSA SecurID, Dell Defender, Google Authenticator, Duo Security e altri token di autenticazione a password monouso/a due fattori Common Access Card (CAC) Autenticazione doppia o stacked Supporto captcha, nome utente/password
Autenticazione SAML	SMA può essere configurato come SAML Identity Provider (IdP), SAML Service Provider (SP) o proxy di un IdP esistente in sede per consentire un SSO federato utilizzando l'autenticazione SAML 2.0.
Repository di autenticazione	SMA offre semplici integrazioni con repository standard nel settore per una facile gestione degli account utente e delle password. I gruppi di utenti possono essere popolati dinamicamente in base a repository di autenticazione come RADIUS, LDAP o Active Directory, compresi i gruppi nidificati. È possibile interrogare attributi LDAP comuni o personalizzati per una specifica autorizzazione o verifica della registrazione di un dispositivo.
Proxy di applicazione layer 3-7	SMA fornisce opzioni proxy flessibili; ad esempio, l'accesso dei fornitori può essere concesso tramite proxy diretto, l'accesso degli appaltatori tramite reverse proxy e l'accesso a Exchange dei dipendenti tramite ActiveSync.
Reverse proxy	Il servizio avanzato di reverse proxy con autenticazione consente agli amministratori di configurare il portale e i segnalibri di offload delle applicazioni, consentendo agli utenti di collegarsi senza problemi ad applicazioni e risorse remote tra cui RDP e HTTP. Questa funzione supporta tutti i browser, compresi IE, Chrome e Firefox.
Delega vincolante Kerberos	SMA fornisce il supporto di autenticazione utilizzando un'infrastruttura Kerberos esistente, che non ha bisogno di affidarsi a servizi front-end per delegare un servizio.

Gestione degli accessi

Access Control Engine (ACE)	Gli amministratori concedono o negano l'accesso in base alle politiche organizzative e adottano azioni di rimedio durante la quarantena delle sessioni. La politica ACE basata sugli oggetti utilizza elementi di rete, risorsa, identità, dispositivo, applicazione, dati e tempo.
End Point Control (EPC)	L'EPC consente all'amministratore di applicare le regole di controllo granulare degli accessi in base allo stato di salute del dispositivo di connessione. Con l'integrazione profonda nel sistema operativo, vengono combinati molti elementi per la classificazione dei tipi e la valutazione dei fattori di rischio. L'interrogazione EPC semplifica la configurazione dei profili dei dispositivi mediante un elenco esaustivo e predefinito di soluzioni anti-virus, personal firewall e anti-spyware per le piattaforme Windows, Mac e Linux, comprese la versione e l'applicabilità dell'aggiornamento dei file di firme.
App Access Control (AAC)	Gli amministratori possono definire le specifiche applicazioni mobili che sono autorizzate ad accedere alle risorse della rete attraverso singoli tunnel per app. Le politiche AAC sono applicate sia sul client sia sul server, fornendo una solida protezione perimetrale.

Sicurezza superiore

SSL VPN Layer 3	La serie SMA offre funzionalità di tunneling layer 3 ad alte prestazioni per una vasta gamma di dispositivi client in esecuzione in qualsiasi ambiente.
Supporto della crittografia	Durata della sessione configurabile Cifrari: AES 128 + 256 bit, Triple DES, RC4 128 bit Hash: SHA-256 Elliptic Curve Digital Signature Algorithm (ECDSA)
Supporto cifrari avanzati	Le apparecchiature SMA forniscono un solido approccio alla sicurezza, sono pronte all'uso, conformi e dotate di cifrari di configurazione predefiniti, e gli amministratori possono perfezionarle ulteriormente per prestazioni, grado di sicurezza e compatibilità.
Certificati di sicurezza	Certificati FIPS 140-2 Livello 2, ICSA SSL-TLS, in fase di certificazione Common Criteria, UC-APL
Condivisione file sicura	Blocco degli attacchi sconosciuti di tipo zero-day, come il ransomware a livello di gateway con rimedio automatizzato. I file caricati utilizzando endpoint non gestiti con accesso sicuro alle reti aziendali sono ispezionati dal nostro Capture ATP multi-engine basato sul cloud.
Web Application Firewall (WAF)	Prevenzione degli attacchi basati su protocolli e sul web, per aiutare le attività finanziarie, sanitarie, nel settore dell'e-commerce e altre aziende ad ottenere la conformità OWASP Top 10 e PCI.
Rilevamento Geo IP e protezione Botnet	Rilevamento Geo IP e protezione Botnet offrono ai clienti un meccanismo per consentire o limitare l'accesso degli utenti da diverse località geografiche.
Supporto TLS 1.3	Miglioramenti in termini di sicurezza e di prestazioni riducendo le complessità rispetto ai modelli precedenti.

Esperienza utente intuitiva

Always On VPN	Creazione automatica di una connessione sicura alla rete aziendale da dispositivi Windows forniti dall'azienda per migliorare la sicurezza, ottenere visibilità sul traffico e rispettare la conformità.
Secure Network Detection (SND)	Il client VPN di SMA riconosce la presenza di rete quando il dispositivo è fuori dal campus e ricollega automaticamente la VPN, disattivandola nuovamente quando il dispositivo ritorna all'interno di una rete affidabile.
Accesso clientless alle risorse	SMA offre un accesso clientless sicuro alle risorse tramite gli agent browser HTML5 che forniscono protocolli RDP, ICA, VNC, SSH e Telnet.
Portale Single Sign-On	Il portale WorkPlace offre una visualizzazione semplice, personalizzabile, a pannello singolo per un accesso sicuro con Single Sign-On (SSO) a qualsiasi risorsa in un ambiente informatico ibrido. Non sono necessari ulteriori accessi o VPN.
Tunneling layer 3	Gli amministratori possono scegliere lo Split-Tunneling o applicare la modalità Redirect-All con tunneling SSL/TLS e backup ESP opzionale per ottenere le massime prestazioni.
HTML5 file explorer[1]	Il moderno browser di file consente agli utenti di accedere alle condivisioni dei file da qualsiasi browser web.
Integrazione di sistemi operativi mobili	Mobile Connect è supportato su tutte le piattaforme di sistemi operativi in modo da offrire agli utenti la massima flessibilità nella scelta dei dispositivi mobili.

Resilienza

Global Traffic Optimizer (GTO)	SMA offre agli utenti il bilanciamento del carico di traffico globale a impatto zero. Il traffico viene indirizzato al data center più ottimizzato e performante.
Alta disponibilità dinamica[2]	SMA è dotato di supporti attivo/passivo e offre una configurazione attiva/attiva per un'elevata disponibilità, implementata sia in un unico data center sia in più data center geograficamente lontani.
Persistenza di sessione universale[1]	Offre agli utenti un'esperienza uniforme con failover a impatto zero. In caso di offline dell'apparecchiatura, il clustering intelligente di SMA ridistribuisce gli utenti assieme ai relativi dati di sessione senza la necessità di una nuova autenticazione.
Prestazioni modulabili	Le apparecchiature SMA consentono la modularità esponenziale delle prestazioni tramite l'implementazione di più apparecchiature, eliminando così la presenza di un unico punto soggetto a guasti. Il clustering orizzontale supporta completamente la presenza mista di apparecchiature SMA fisiche e virtuali.
Licenze dinamiche	Le licenze utente non devono più essere applicate alle singole apparecchiature SMA. Gli utenti possono essere distribuiti e riassegnati dinamicamente tra le apparecchiature gestite, in base alle loro esigenze.

Gestione e monitoraggio centralizzati

Central Management System (CMS)	CMS offre la gestione centralizzata basata sul web per tutte le funzionalità SMA.
Avvisi personalizzati	Gli avvisi possono essere configurati per generare trappole SNMP monitorate da qualsiasi Network Management System (NMS) dell'infrastruttura informatica. Gli amministratori possono anche configurare avvisi relativi a file analizzati da Capture ATP e all'uso del disco per consentire reazioni immediate.
Pannello di controllo in tempo reale	Il pannello di controllo personalizzabile in tempo reale consente all'amministratore informatico di diagnosticare in modo semplice e rapido problemi di accesso, acquisendo preziose informazioni per la risoluzione dei problemi.
Integrazione SIEM	L'output in tempo reale ai sistemi di raccolta dati SIEM centrali consente ai team di sicurezza di correlare le attività basate sugli eventi, in modo da comprendere il flusso di lavoro end-to-end di un particolare utente o applicazione. Si tratta di un aspetto fondamentale durante la gestione degli eventi di sicurezza imprevisti e per le analisi forensi.
Pianificatore	Il pianificatore consente agli utenti di pianificare le attività di manutenzione come l'implementazione delle politiche, la replica delle impostazioni di configurazione e il riavvio dei servizi, senza intervento manuale.

Estensibilità

API di gestione	Le API di gestione consentono un completo controllo amministrativo programmatico su tutti gli oggetti di un unico ambiente SMA o CMS globale.
API per utenti finali	Le API per utenti finali forniscono un controllo completo sull'intera procedura di accesso, autenticazione e degli endpoint.
Autenticazione a due fattori (2FA)	SMA fornisce l'autenticazione 2FA tramite integrazione con le principali soluzioni basate su password monouso a tempo (TOTP) come Google Authenticator, Microsoft Authenticator, Duo security etc.
Integrazione MDM	SMA si integra con i principali prodotti di gestione mobile aziendale (EMM) come Airwatch e Mobile Iron.
Ulteriori integrazioni di terzi	SMA si integra con produttori leader del settore come OPSWAT per fornire una protezione avanzata dalle minacce.

[1]*Disponibile con sistema operativo SMA 12.1 o superiore*

[2]*Migliorata in SMA 12.1*

Riepilogo delle funzioni (confronto per modello)

Categoria	Funzione	210	410	500v	6210	7210	8200v
Installazione	Sistema operativo	v9.0 e versioni successive	v9.0 e versioni successive	v9.0 e versioni successive	v12.1 e versioni successive	v12.1 e versioni successive	v12.1 e versioni successive
	Hypervisor supportati	–	–	VMware ESXi / Microsoft Hyper-V	–	–	VMware ESXi / Microsoft Hyper-V
	Piattaforme cloud pubbliche supportate	–	–	AWS/Azure	–	–	AWS/Azure
Throughput	Sessioni utente in contemporanea max	200	400	250	2.000	10.000	5.000
	Throughput SSL/TLS max	560 Mb/s	844 Mb/s	265 Mb/s	800 Mb/s	5,0 Gb/s	1,58 Gb/s
Accesso client	Tunnel layer 3	•	•	•	•	•	•
	Split-tunnel e redirect-all	•	•	•	•	•	•
	Always On VPN	•	•	•	•	•	•
	Incapsulamento ESP automatico	–	–	–	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•
	Secure Network Detection	–	–	–	•	•	•
	File browser (CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•
	Tunnel on demand	–	–	–	•	•	•
	Estensioni Chrome/Firefox	–	–	–	•	•	•
	Supporto tunnel CLI	–	–	–	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•
	Net Extender (Windows, Linux)	•	•	•	–	–	–
	Connect Tunnel (Windows, Mac OSX, Linux)	–	–	–	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•
Accesso mobile	Tramite VPN app	–	–	–	•	•	•
	Implementazione controllo app	–	–	–	•	•	•
	Convalida ID app	–	–	–	•	•	•
Portale utenti	Branding	•	•	•	•	•	•
	Personalizzazione	–	–	–	•	•	•
	Localizzazione	•	•	•	•	•	•
	Segnalibri definiti dagli utenti	•	•	•	•	•	•
	Supporto URL personalizzato	•	•	•	•	•	•
	Supporto applicazione SaaS	–	–	–	•	•	•
Sicurezza	FIPS 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	•	•	•	•	•	•
	Cifrari Suite B	–	–	–	•	•	•
	Interrogazione EPC dinamica	•	•	•	•	•	•
	Controllo degli accessi basato sul ruolo (RBAC)	–	–	–	•	•	•
	Registrazione endpoint	•	•	•	•	•	•
	Condivisione sicura dei file (Capture ATP)	•	•	•	•	•	•
	Quarantena endpoint	•	•	•	•	•	•
	Convalida OSCP CRL	–	–	–	•	•	•
	Selezione cifrario	–	–	–	•	•	•
	Certificati PKI e client	•	•	•	•	•	•
	Filtro Geo IP	•	•	•	–	–	–
	Filtro Botnet	•	•	•	–	–	–
	Forward proxy	•	•	•	•	•	•
	Reverse proxy	•	•	•	•	•	•
Servizi di autenticazione e identità	SAML 2.0	–	–	–	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	SAML Identity Provider (IdP)	•	•	•	•	•	•
	Supporto per dispositivi biometrici	•	•	•	•	•	•
	Supporto Face ID per iOS	•	•	•	•	•	•
	Autenticazione a due fattori (2FA)	•	•	•	•	•	•
	Autenticazione multifattoriale (MFA)	–	–	–	•	•	•

Riepilogo delle funzioni (confronto per modello cont.)

Categoria	Funzione	210	410	500v	6210	7210	8200v
Servizi di autenticazione e identità cont.	Autenticazione concatenata	–	–	–	•	•	•
	One Time Passcode (OTP) tramite e-mail o SMS	•	•	•	•	•	•
	Supporto CAC (Common Access Card)	–	–	–	•	•	•
	Supporto certificati X.509	•	•	•	•	•	•
	Integrazione captcha	–	–	–	•	•	•
	Cambio password in remoto	•	•	•	•	•	•
	SSO basato su moduli	•	•	•	•	•	•
	SSO federato	–	–	–	•	•	•
	Persistenza di sessione	–	–	–	•	•	•
	Accesso automatico	•	•	•	•	•	•
Controllo accessi	AD di gruppo	•	•	•	•	•	•
	Attributi LDAP	•	•	•	•	•	•
	Politiche di geolocalizzazione	•	•	•	–	–	–
	Monitoraggio continuo degli endpoint	•	•	•	•	•	•
Gestione	Interfaccia di gestione (ethernet)	–	–	–	•	•	•
	Interfaccia di gestione (console)	–	–	–	•	•	•
	Amministrazione HTTPS	•	•	•	•	•	•
	Amministrazione SSH	–	–	–	•	•	•
	SNMP MIBS	•	•	•	•	•	•
	Syslog e NTP	•	•	•	•	•	•
	Monitoraggio dell'uso	•	•	•	•	•	•
	Ripristino configurazione	•	•	•	•	•	•
	Gestione centralizzata	–	–	–	•	•	•
	Reportistica centralizzata	–	–	–	•	•	•
	Gestione API REST	–	–	–	•	•	•
	Autenticazione API REST	–	–	–	•	•	•
	Contabilità RADIUS	–	–	–	•	•	•
	Attività pianificate	–	–	–	•	•	•
	Licenze di sessione centralizzate	–	–	–	•	•	•
	Audit guidato dagli eventi	–	–	–	•	•	•
Connettività di rete	IPv6	•	•	•	•	•	•
	Bilanciamento del carico globale	–	–	–	•	•	•
	Bilanciamento del carico su server	•	•	•	–	–	–
	Replicazione stato TCP	•	•	•	•	•	•
	Failover stato cluster	–	–	–	•	•	•
	Alta disponibilità attivo/passivo	–	•	•	•	•	•
	Alta disponibilità attivo/attivo	–	–	–	•	•	•
	Modularità orizzontale	–	–	–	•	•	•
	FQDN singoli o multipli	–	–	–	•	•	•
	Proxy smart tunnel L3-7	•	•	•	•	•	•
	Proxy di applicazione L7	•	•	•	•	•	•
Integrazione	Supporto 2FA TOTP	•	•	•	•	•	•
	Supporto prodotti EMM e MDM	–	–	–	•	•	•
	Supporto prodotti SIEM	–	–	–	•	•	•
	Deposito password TPAM	–	–	–	•	•	•
	Supporto hypervisor ESX	–	–	•	–	–	•
	Supporto hypervisor Hyper-V	–	–	•	–	–	•
Opzioni di licenza	Licenza in abbonamento	–	–	–	•	•	•
	Licenza senza scadenza con supporto	•	•	•	•	•	•
	Web Application Firewall (WAF)	•	•	•	–	–	–
	Licenze Spike	•	•	•	•	•	•
	Licenze multilivello	–	–	–	•	•	•
	Virtual Assist	•	•	•	–	–	–

** Per ulteriori informazioni sui client VPN visitare: https://www.sonicwall.com/en-us/products/remote-access/vpn-client*

Vantaggi dell'upgrade ad apparecchiature di fascia alta

Prestazioni superiori | Aumento throughput | Funzioni avanzate | Migliore modularità

Specifiche delle apparecchiature

È possibile scegliere tra una gamma di apparecchiature di accesso mobile sicuro (SMA) appositamente costruite.
Sono disponibili opzioni di implementazione flessibili con apparecchiature virtuali e fisiche.

Specifiche delle apparecchiature fisiche

Prestazioni	SMA 210	SMA 410	SMA 6210	SMA 7210
Sessioni/Utenti concomitanti	Fino a 200	Fino a 400	Fino a 2.000	Fino a 10.000
Throughput* SSL VPN (a CCU max)	560 Mb/s	844 Mb/s	Fino a 800 Mb/s	Fino a 5,0 Gb/s
Fattore di forma	1U	1U	1U	1U
Dimensioni	16,92 x 10,23 x 1,75 in (43 x 26 x 4,5 cm)	16,92 x 10,23 x 1,75 in (43 x 26 x 4,5 cm)	17,0 x 16,5 x 1,75 in (43 x 41,5 x 4,5 cm)	17,0 x 16,5 x 1,75 in (43 x 41,5 x 4,5 cm)
Peso dell'apparecchiatura	5 kg	5 kg	8 kg	8 kg
Accelerazione dati crittografia (AES-NI)	NO	NO	SÌ	SÌ
Porta gestione dedicata	NO	NO	SÌ	SÌ
Accelerazione SSL	NO	NO	SÌ	SÌ
Memorizzazione	4GB (memoria flash)	4GB (memoria flash)	2 x 1TB SATA; RAID 1	2 x 1TB SATA; RAID 1
Interfacce	(2) GB Ethernet, (2) USB, (1) console	(4) GB Ethernet, (2) USB, (1) console	1GE a (6) porte, (2) USB, (1) console	1GE a (6) porte, 10Gb SFP+ a (2) porte, (2) USB, (1) console
Memoria	4GB	8GB	8GB DDR4	16GB DDR4
Chip TPM	NO	NO	SÌ	SÌ
Processore	4 core	8 core	4 core	4 core
MTBF (a 25°C) in ore	61.815	60.151	70.127	129.601
Funzionamento e conformità	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
Alimentazione	Alimentazione fissa	Alimentazione fissa	Alimentazione fissa	Doppia alimentazione, hot swap
Tensione d'ingresso	100-240VCA, 50-60MHz	100-240VCA, 50-60MHz	100-240 VCA, 1,1 A	100-240 VCA, 1,79 A
Potenza assorbita	26,9 W	31,9 W	77 W	114 W
Dissipazione di calore totale	92 BTU	109 BTU	264 BTU	389 BTU
Condizioni ambientali	RAEE, RoHS UE, RoHS Cina			
Tolleranza agli urti (non operativo)	110 g, 2 msec			
Emissioni	FCC, ICES, CE, C-Tick, VCCI; MIC			
Sicurezza	TUV/GS, UL, CE PSB, CCC, BSMI, schema CB			
Temperatura di funzionamento	da 0 °C a 40 °C			
Certificazione FIPS	NO	NO	FIPS 140-2 Livello 2 con protezione antimanomissione	

** Le prestazioni di throughput possono variare in base all'implementazione e alla connettività. I valori numerici pubblicati si basano su condizioni interne di laboratorio*

Specifiche delle apparecchiature virtuali

Specifiche	SMA 500v (ESX/ESXi/Hyper-V)	SMA 8200v (ESX/ESXi/Hyper-V)
Sessioni in contemporanea	Fino a 250 utenti	Fino a 5000
Throughput SSL-VPN* (a CCU max)	Fino a 186 Mb/s	Fino a 1,58 Gb/s
Memoria allocata	2GB	8 GB
Processore	1 core	4 core
Accelerazione SSL	NO	SÌ
Dimensioni disco	2GB	64 GB (predefinito)
Sistema operativo installato	Linux	Linux hardened
Porta gestione dedicata	NO	SÌ

** Le prestazioni di throughput possono variare in base all'implementazione e alla connettività. I valori numerici pubblicati si basano su condizioni interne di laboratorio. SMA 8200v su Hyper-V è modulabile fino a 5000 sessioni in contemporanea con una velocità massima SSL-VPN di 1,58 Gbps quando è in esecuzione su SO SMA 12.1 con Windows Server 2016*

Informazioni per l'ordinazione

SKU	APPARECCHIATURA SONICWALL SECURE MOBILE ACCESS (SMA)
02-SSC-2800	SMA 210 con licenza per 5 utenti
02-SSC-2801	SMA 410 con licenza per 25 utenti
01-SSC-8469	SMA 500v con licenza per 5 utenti
02-SSC-0978	SMA 7210 con licenza di prova amministratore
02-SSC-0976	SMA 6210 con licenza di prova amministratore
01-SSC-8468	SMA 8200v (apparecchiatura virtuale)
SKU	**LICENZE UTENTI SMA SONICWALL**
01-SSC-9182	SMA 500V altri 5 utenti (Disponibile anche per SMA 210)
01-SSC-2414	SMA 500V altri 100 utenti (Disponibile anche per SMA 410)
01-SSC-7856	Licenza SMA 5 utenti - stackable per 6210, 7210, 8200v
01-SSC-7860	Licenza SMA 100 utenti - stackable per 6210, 7210, 8200v
01-SSC-7865	Licenza SMA 5000 utenti - stackable per 6210, 7210, 8200v
SKU	**CONTRATTO DI SUPPORTO SMA SONICWALL**
01-SSC-9191	Supporto 24X7 per SMA 500V fino a 25 utenti 1 anno (Disponibile anche per SMA 210 e 410)
01-SSC-2326	Supporto 24X7 per SMA 6210 100 utenti 1 anno - stackable
01-SSC-2350	Supporto 24X7 per SMA 7210 500 utenti 1 anno - stackable
01-SSC-8434	Supporto 24X7 per SMA 8200V 5 utenti 1 anno - stackable (Disponibile anche per SMA 6210, 7210)
01-SSC-8446	Supporto 24X7 per SMA 8200V 100 utenti 1 anno - stackable (Disponibile anche per SMA 6210, 7210)
01-SSC-7913	Supporto 24X7 per SMA 8200V 5000 utenti 1 anno - stackable (Disponibile anche per SMA 6210, 7210)
SKU	**GESTIONE CENTRALE PER 6210, 7210, 8200V**
Licenze apparecchiature CMS	
01-SSC-8535	Base CMS + 3 licenze apparecchiatura (Gratis - per le prove e l'uso con licenze utente in abbonamento)
01-SSC-8536	CMS 100 licenza apparecchiatura 1 anno (per l'uso con licenze utente in abbonamento)
01-SSC-3369	Base CMS + 3 apparecchiature (Gratis - per l'uso con licenze utente senza scadenza)
01-SSC-3402	CMS 100 licenza apparecchiatura 1 anno (per l'uso con licenze utente in abbonamento)
Licenze utente centrali (abbonamento)	
01-SSC-2298	Licenza CMS in pool 10 utenti 1 anno
01-SSC-8539	Licenza CMS in pool 1000 utenti 1 anno
01-SSC-5339	Licenza CMS in pool 50000 utenti 1 anno
Licenze utente centrali (senza scadenza)	
01-SSC-2053	Licenza CMS senza scadenza 10 utenti
01-SSC-2058	Licenza CMS senza scadenza 1000 utenti
01-SSC-2063	Licenza CMS senza scadenza 50000 utenti
Supporto per licenze utente centrali (senza scadenza)	
01-SSC-2065	Supporto CMS 24x7 1 anno 10 utenti
01-SSC-2070	Supporto CMS 24x7 1 anno 1000 utenti
01-SSC-2075	Supporto CMS 24x7 1 anno 50000 utenti
Licenze ActiveSync centrali (abbonamento)	
01-SSC-2088	Licenza CSM in pool e-mail 10 utenti 1 anno
01-SSC-2093	Licenza CSM in pool e-mail 1000 utenti 1 anno
01-SSC-2087	Licenza CSM in pool e-mail 50000 utenti 1 anno

Informazioni per l'ordinazione cont.

SKU	GESTIONE CENTRALE PER 6210, 7210, 8200V
Licenze Spike centrali	
01-SSC-2111	CMS Spike 1000 utenti 5 giorni
01-SSC-2115	CMS Spike 50000 utenti 5 giorni
Capture add-on (abbonamento)	
Contattare il rivenditore ** Le licenze in abbonamento comprendono il supporto 24X7 incluso*	
SKU	**ADD-ON SMA SONICWALL**
01-SSC-2406	Add-on SMA 7210 FIPS
01-SSC-2405	Add-on SMA 6210 FIPS
01-SSC-9185	SMA 500V Web Application Firewall 1 anno (Disponibile anche per SMA 210 e 410)
SKU	**UPGRADE SICUREZZA SMA SONICWALL**
02-SSC-2794	SMA 210 Secure Upgrade Plus, 5 utenti in bundle con supporto 24X7 fino a 25 utenti 1 anno
02-SSC-2795	SMA 210 Secure Upgrade Plus, 5 utenti in bundle con supporto 24X7 fino a 25 utenti 3 anni
02-SSC-2798	SMA 410 Secure Upgrade Plus, 25 utenti in bundle con supporto 24X7 fino a 100 utenti 1 anno
02-SSC-2799	SMA 410 Secure Upgrade Plus, 25 utenti in bundle con supporto 24X7 fino a 100 utenti 3 anni
02-SSC-2893	SMA 6210 Secure Upgrade Plus, supporto 24X7 fino a 100 utenti 1 anno
02-SSC-2894	SMA 6210 Secure Upgrade Plus, supporto 24X7 fino a 100 utenti 3 anni
02-SSC-2895	SMA 7210 Secure Upgrade Plus, supporto 24X7 fino a 250 utenti 1 anno
02-SSC-2896	SMA 7210 Secure Upgrade Plus, supporto 24X7 fino a 250 utenti 3 anni
02-SSC-0860	SMA 8200V Secure Upgrade Plus, supporto 24X7 fino a 100 utenti 1 anno
02-SSC-0862	SMA 8200V Secure Upgrade Plus, supporto 24X7 fino a 100 utenti 3 anni
02-SSC-2807	SMA 500V Secure Upgrade Plus, supporto 24X7 fino a 100 utenti 1 anno
02-SSC-2808	SMA 500V Secure Upgrade Plus, supporto 24X7 fino a 100 utenti 3 anni
SKU	**LICENZA SPIKE PER SMA (INCREMENTALE NECESSARIO PER RAGGIUNGERE LA CAPACITÀ)**
01-SSC-2240	Licenza Spike SMA 210 10 giorni 50 utenti (Disponibile anche per SMA 410 e 500v)
01-SSC-7873	Licenza Spike SMA 8200v 10 giorni 5-2500 utenti (Disponibile anche per SMA 6210 e 7210)
02-SSC-4490	LICENZA SPIKE SMA 500V 30 GIORNI 250 UTENTI
02-SSC-4489	LICENZA SPIKE SMA 500V 60 GIORNI 250 UTENTI
02-SSC-4488	LICENZA SPIKE SMA 200/210 30 GIORNI 50 UTENTI
02-SSC-4487	LICENZA SPIKE SMA 200/210 60 GIORNI 50 UTENTI
02-SSC-4486	LICENZA SPIKE SMA 400/410 30 GIORNI 250 UTENTI
02-SSC-4485	LICENZA SPIKE SMA 400/410 60 GIORNI 250 UTENTI
02-SSC-4471	LICENZA AGGIUNTIVA SPIKE CMS SMA 100 UTENTI 30 GIORNI
02-SSC-4473	LICENZA AGGIUNTIVA SPIKE CMS SMA 500 UTENTI 30 GIORNI
02-SSC-4475	LICENZA AGGIUNTIVA SPIKE CMS SMA 1.000 UTENTI 30 GIORNI
02-SSC-4477	LICENZA AGGIUNTIVA SPIKE CMS SMA 5.000 UTENTI 30 GIORNI
02-SSC-4479	LICENZA AGGIUNTIVA SPIKE CMS SMA 10.000 UTENTI 30 GIORNI
02-SSC-4481	LICENZA AGGIUNTIVA SPIKE CMS SMA 25.000 UTENTI 30 GIORNI
02-SSC-4483	LICENZA AGGIUNTIVA SPIKE CMS SMA 50.000 UTENTI 30 GIORNI
02-SSC-4472	LICENZA AGGIUNTIVA SPIKE CMS SMA 100 UTENTI 60 GIORNI
02-SSC-4474	LICENZA AGGIUNTIVA SPIKE CMS SMA 500 UTENTI 60 GIORNI
02-SSC-4476	LICENZA AGGIUNTIVA SPIKE CMS SMA 1.000 UTENTI 60 GIORNI

Informazioni per l'ordinazione cont.

SKU	LICENZA SPIKE PER SMA (INCREMENTALE NECESSARIO PER RAGGIUNGERE LA CAPACITÀ)
02-SSC-4478	LICENZA AGGIUNTIVA SPIKE CMS SMA 5.000 UTENTI 60 GIORNI
02-SSC-4480	LICENZA AGGIUNTIVA SPIKE CMS SMA 10.000 UTENTI 60 GIORNI
02-SSC-4482	LICENZA AGGIUNTIVA SPIKE CMS SMA 25.000 UTENTI 60 GIORNI
02-SSC-4484	LICENZA AGGIUNTIVA SPIKE CMS SMA 50.000 UTENTI 60 GIORNI

** Sono disponibili anche SKU e contratti di supporto pluriennali. Per un elenco completo degli SKU rivolgersi al rivenditore o al rappresentante di fiducia*

Servizi attivati dai partner

Serve aiuto per pianificare, installare od ottimizzare la soluzione SonicWall? I SonicWall Advanced Services Partner hanno seguito corsi di formazione per fornire servizi professionali di livello mondiale. Ulteriori informazioni sul sito www.sonicwall.com/PES.

SonicWall

SonicWall fornisce soluzioni di cibersicurezza illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. SonicWall salvaguarda le organizzazioni che si mobilitano per la nuova normalità aziendale con una protezione senza soluzione di continuità che blocca i ciberattacchi più evasivi in tutti i punti di esposizione esterni e che colpiscono un organico che lavora in misura sempre maggiore in remoto, in mobilità e in ambienti cloud. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune di cibersicurezza per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare www.sonicwall.com o seguirci su Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per ulteriori informazioni consultare il nostro sito web.
www.sonicwall.com

Datasheet-SecureMobileAccess-US-COG-2157