SonicWall TZ-serien

Fenomenal säkerhet och superprestanda till häpnadsväckande låg total ägandekostnad

SonicWall TZ-seriens UTM-brandväggar är perfekta för alla företag som är ute efter nätverksskydd i företagsklass.

SonicWall TZ-seriens brandväggar ger omfattande säkerhet tack vare avancerade säkerhetstjänster med både program på enheten och molnbaserade program mot skadliga koder, antispionprogram, programkontroll, system för förebyggande av intrång (IPS) och URL-filtrering. För att motverka krypterade attacker, som har blivit allt vanligare, har TZ-serien processorkraft nog att inspektera krypterade SSL- och TLS-anslutningar mot de senaste hoten. I kombination med switchar i Dell X-serien kan utvalda TZ-brandväggar hantera säkerheten direkt hos de ytterligare portarna.

Med hjälp av SonicWall-nätverket Global Response Intelligent Defense (GRID) levererar SonicWall TZ-serien regelbundet uppdateringar för att försvaret mot cyberbrottslingar ska fortsätta att vara stabilt. SonicWall TZ-serien kan skanna varje byte i varje paket på alla portar och protokoll så gott som helt utan fördröjning, oavsett filstorlek.

SonicWall TZ-serien har Gigabit Ethernet-portar, integrerad trådlös 802.11ac-anslutning* som tillval, IPSec och SSL VPN, redundans genom inbyggt 3G/4G-stöd, belastningsutjämning och nätverkssegmentering. SonicWall TZ-seriens UTM-brandväggar ger också snabb och säker mobil åtkomst för Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS X och Linux.
SonicWall Global Management System (GMS) möjliggör centraliserad distribution och hantering av SonicWall TZ-seriens brandväggar från ett enda system.

Hanterad säkerhet för distribuerade miljöer

Skolor, detaljhandeln, avsides belägna kontor, filialer och utlokaliserade verksamheter behöver en lösning som kan integreras med företagsbrandväggen. SonicWall TZ-seriens brandväggar har samma kodbas – och samma skydd – som brandväggarna hos våra oerhört populära, nya generationens SuperMassive-brandväggar. Detta underlättar förvaltningen av fjärranslutna kontor, eftersom alla administratörer har tillgång till samma användargränssnitt. Med GMS kan nätverksadministratörerna konfigurera, övervaka och hantera SonicWalls fjärrbrandväggar från ett och samma ställe. Genom att tillföra snabb och säker trådlös anslutning utökas skyddsområdet till att även omfatta kunder och gäster som ofta besöker detaljhandelsbutiken eller det avsides belägna kontoret.

** I nuläget finns inte 802.11ac på SOHO-modellerna; SOHO-modellerna stöder 802.11a/b/g/n.*

SonicWall TZ600-serien

Tillväxtföretag, detaljhandelsbutiker och filialer som är ute efter prisvärd säkerhet får ett säkert nätverk med SonicWall TZ600-seriens brandvägg, med funktioner i företagsklass och utan att behöva tumma på prestandan.

Specification	TZ600 series
Firewall throughput	1.5 Gbps
Full DPI throughput	500 Mbps
Anti-malware throughput	500 Mbps
IPS throughput	1.1 Gbps
IMIX throughput	900 Mbps
Max DPI connections	125,000
New connections/sec	12,000

SonicWall TZ500-serien

För filialer samt små och medelstora företag under tillväxt ger SonicWall TZ500-serien ett högeffektivt skydd utan kompromisser, med nätverksproduktivitet och integrerat trådlöst 802.11ac dualband som tillval.

Specification	TZ500 series
Firewall throughput	1.4 Gbps
Full DPI throughput	400 Mbps
Anti-malware throughput	400 Mbps
IPS throughput	1.0 Gbps
IMIX throughput	700 Mbps
Max DPI connections	100,000
New connections/sec	8,000

SonicWall TZ400-serien

För småföretag, detaljhandelsverksamhet och filialer är SonicWall TZ400-serien ett perfekt nätverksskydd i företagsklass. Flexibel trådlös distribution genom endera externa åtkomstpunkter via SonicPoint, eller trådlöst 802.11ac integrerat i enheten.

Specification	TZ400 series
Firewall throughput	1.3 Gbps
Full DPI throughput	300 Mbps
Anti-malware throughput	300 Mbps
IPS throughput	900 Mbps
IMIX throughput	500 Mbps
Max DPI connections	90,000
New connections/sec	6,000

SonicWall TZ300-serien

SonicWall TZ300-serien är en helhetslösning som skyddar nätverk från attacker. Till skillnad från konsumentprodukter kombinerar SonicWall TZ300-seriens brandvägg effektiva system för förebyggande av intrång, program mot skadlig kod och innehålls-/URL-filtrering med integrerad trådlös 802.11ac-anslutning som tillval och ett brett stöd för säkra mobila plattformar för bärbara datorer, smarttelefoner och surfplattor.

Specification	TZ300 series
Firewall throughput	750 Mbps
Full DPI throughput	100 Mbps
Anti-malware throughput	100 Mbps
IPS throughput	300 Mbps
IMIX throughput	200 Mbps
Max DPI connections	50,000
New connections/sec	5,000

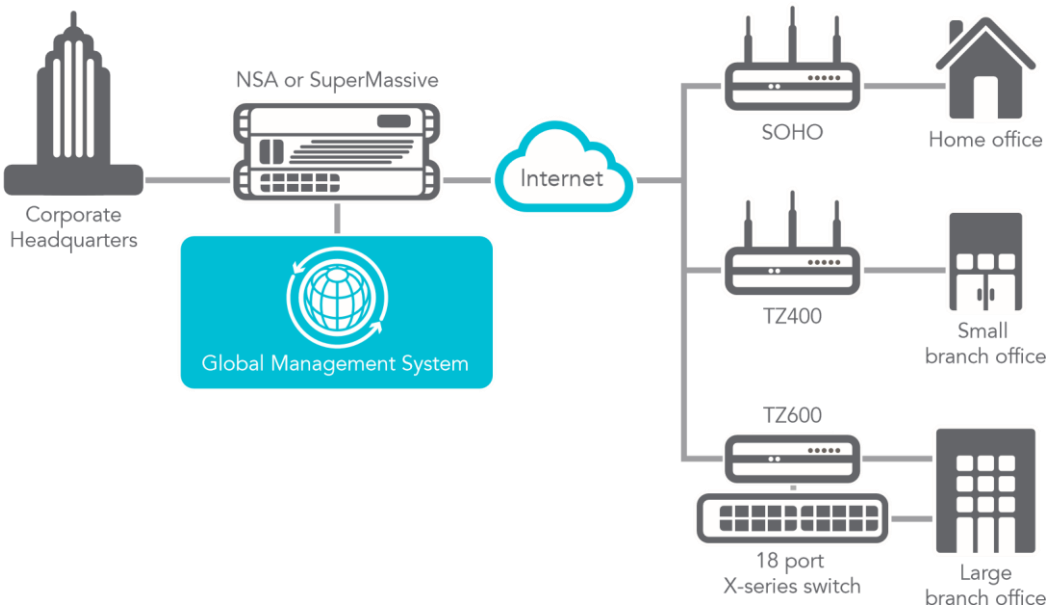
SonicWall SOHO-serien

SonicWall SOHO-serien ger kabelanslutna och trådlösa småföretagsmiljöer och hemmakontor samma skydd i företagsklass som stora organisationer kräver, men till ett mer överkomligt pris.

Specification	SOHO series
Firewall throughput	300 Mbps
Full DPI throughput	50 Mbps
Anti-malware throughput	50 Mbps
IPS throughput	100 Mbps
IMIX throughput	60 Mbps
Max DPI connections	10,000
New connections/sec	1,800

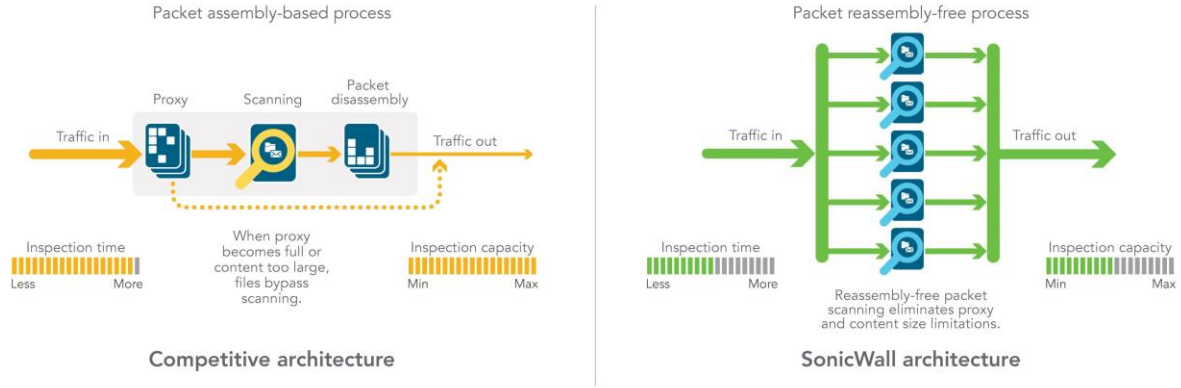
Utbyggbar arkitektur för fenomenal skalbarhet och prestanda

RFDPI-motorn är konstruerad från grunden med fokus på genomsökning med höga prestanda så att den kan hantera den ständigt ökande, parallella nätverkstrafiken. I kombination med system med flerkärniga processorer skalanpassas denna i grunden parallella programvaruarkitektur perfekt och kan hantera de krav som ställs på djup paketinspektion vid hög trafikbelastning. På SonicWall TZ-seriens plattform används processorer som till skillnad från x86-processorerna är optimerade för paket-, krypterings- och nätverksbehandling med bibehållen flexibilitet och programmerbarhet på fältet – som är en svag punkt hos ASIC-systemen. Denna flexibilitet är nödvändig när uppdateringar av kod och nya beteenden krävs för att skydda mot nya angrepp som kräver uppdaterade och mer raffinerade identifieringstekniker.



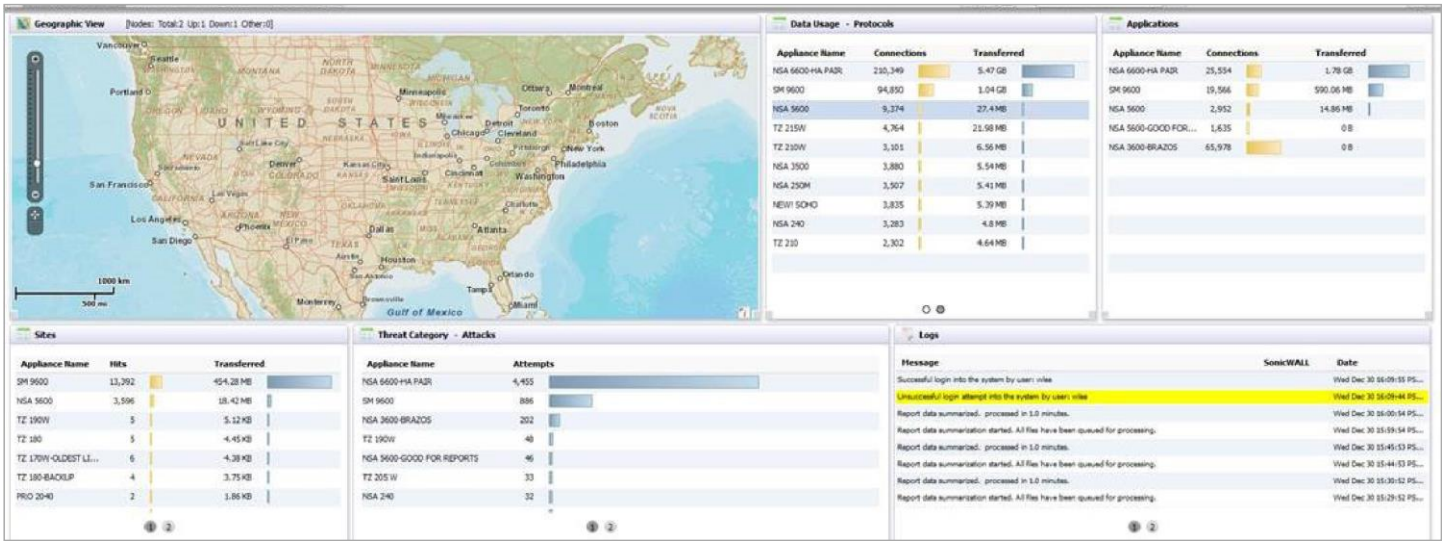
RFDPI-motor (Reassembly-Free Deep Packet Inspection)

RFDPI-motorn ger överlägset skydd och programkontroll utan att du behöver tumma på prestandan. Denna patenterade motor inspekterar nätverkstrafiken för att upptäcka hot i skikten 3–7. RFDPI-motorn kör nätverksströmmar genom omfattande och upprepade normaliserings- och dekrypteringsprocesser för att neutralisera avancerade sätt att komma runt och förvirra identifieringsmotorerna och smyga in skadlig kod i nätverket. När ett paket väl har förbehandlats, bland annat med SSL-dekryptering, analyseras det mot en enda intern minnesrepresentation av tre signaturdatabaser: intrång, skadlig kod och program. Sedan flyttas anslutningsstatusen fram för att representera nätverksströmmens position i förhållande till dessa databaser, tills den påträffar en attack eller annan ”matchande” händelse, varvid en förinställd åtgärd vidtas. Om skadlig kod identifieras avbryter SonicWall-brandväggen anslutningen innan något intrång sker, och loggar händelsen. Datorn kan dock även konfigureras för enbart inspektion eller, i händelse av programidentifiering, för att tillhandahålla bandbreddhantering för skikt 7 för den resterande programströmmen, så snart som programmet har identifierats.



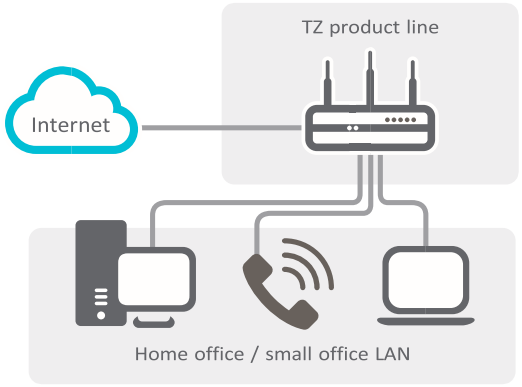
Global hantering och rapportering

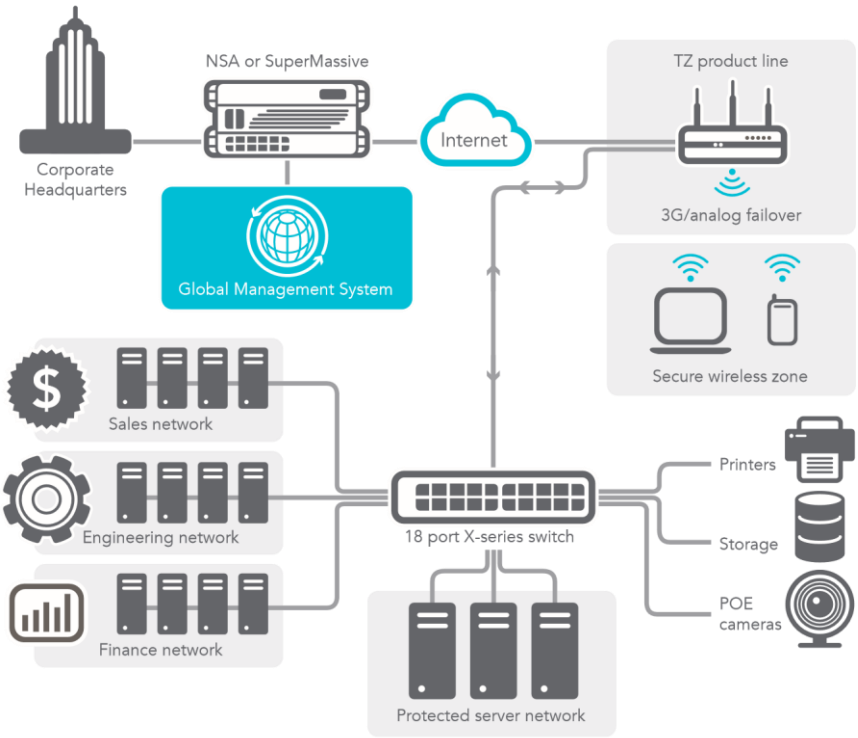
Vid större spridning, till utlokaliserade verksamheter, ger tillvalet SonicWall Global Management System (GMS) administratörerna en enhetlig, säker och utbyggbar plattform för att hantera SonicWalls säkerhetslösningar och switchar i Dell X-serien. Med det systemet kan företagen lätt sammanföra hanteringen av säkerhetslösningar, minska komplikationer i samband med administration och felsökning samt styra alla driftaspekter av säkerhetsinfrastrukturen, däribland en centraliserad policyhantering och -tillämpning, händelseövervakning, analys och rapportering i realtid, med mera. GMS uppfyller också företagens krav för hantering av nätverksbrandväggsändringar, tack vare en funktion för automatisering av arbetsflödet. GMS gör det lättare att hantera nätverkssäkerheten med verksamhetsprocesser och servicenivåer, som verkligen förenklar livscykelhanteringen av alla säkerhetsmiljöer jämfört med att sköta det enhet för enhet.



Säkerhet och skydd

Den engagerade interna SonicWall-gruppen som forskar om hot arbetar med att undersöka och utveckla motåtgärder att använda i brandväggarna för att alltid erbjuda ett aktuellt skydd. Forskargruppen utnyttjar över en miljon sensorer runtom i världen för att samla in exempel på skadlig kod och för att kunna få telemetrisk återkoppling om den senaste hotinformationen, som i sin tur matas in i lösningarna mot intrång och skadlig kod och för programidentifiering. Skyddet som de kunder har som i nuläget prenumererar på en SonicWall-brandvägg uppdateras regelbundet, och vid alla tider på dygnet, och uppdateringarna träder i kraft direkt, utan omstarter eller avbrott. Signaturerna på produkterna skyddar mot många typer av attacker och täcker upp till tiotusentals enskilda hot med en enda signatur. Utöver motåtgärderna på enheten har alla SonicWall-brandväggar tillgång till tjänsten SonicWall CloudAV, som utökar den inbyggda signaturinformationen med över 17 miljoner signaturer, vilket håller på att bli fler. CloudAV-databasen nås via ett prestandasnålt, företagsinternt protokoll vid brandväggen som förbättrar inspektionen av enheten. Med geo-IP- och botnet-filtreringsfunktioner kan nya generationens SonicWall-brandväggar blockera trafik från farliga domäner eller hela geografiska områden, för att minska riskprofilen för nätverket.





application traffic analytics provide with SonicWall next-generation

Programinformation och -kontroll

Genom programinformationen får administratörerna kännedom om programtrafiken i nätverket så att de kan schemalägga programkontroller utifrån affärsprioritet, begränsa improduktiva program och blockera potentiellt farliga applikationer. Med visualisering i realtid identifieras avvikelser i trafiken när de sker, vilket gör det möjligt att omedelbart vidta motåtgärder mot eventuella inkommande och utgående attacker eller prestandaflaskhalsar. SonicWalls analys av programtrafik ger en detaljerad insyn i programtrafik, utnyttjande av bandbredd samt säkerhetshot, liksom kraftfulla funktioner för felsökning och intrångsanalys. Dessutom förbättrar enkel inloggning (SSO) användarupplevelsen, ökar produktiviteten och minskar antalet supportsamtal. Ett intuitivt nätbaserat gränssnitt underlättar hanteringen av programinformation och -kontroll. För en flexibel och säker trådlös anslutning finns den trådlösa höghastighetsanslutningen 802.11ac* som tillval. I kombination med nya generationens SonicWall-brandväggar får du en trådlös nätverkssäkerhetslösning som ger ett omfattande skydd åt kabelanslutna och trådlösa nätverk.
Denna trådlösa lösning i företagsklass gör att wifi-förberedda enheter kan kopplas upp från större avstånd och använda bandbreddsintensiva mobilappar, som video- och röstappar, i miljöer med högre densitet utan att signalen blir sämre.
* I nuläget finns inte 802.11ac på SOHO-modellerna; SOHO-modellerna stöder 802.11a/b/g/n.

Fördelar:

- Nätverksskydd i företagsklass
- Djup paketinspektion av all datatrafik oavsett filstorlek och protokoll
- Säker trådlös 802.11ac-anslutning med integrerad trådlös styrenhet eller extern, trådlös anslutning genom SonicPoint
- Mobil anslutning via SSL VPN för Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS och Linux
- Över 100 ytterligare portar kan hanteras säkert med TZ-konsolen när den används tillsammans med en Dell X-switch