SonicWall Network Security Appliance (NSA) Series

Beprövad säkerhet och prestanda för medelstora nätverk

SonicWall Network Security Appliance (NSA) series erbjuder avancerad säkerhet och prestanda för medelstora företag, filialkontor och distributörsföretag. Med hjälp av innovativ deep learning-teknik i SonicWall Capture Cloud-plattformen, levererar NSa-serien automatiserad intrångsdetektering i realtid och tillgodoser organisationers behov.

Toppmodernt skydd med förstklassig prestanda

Dagens hot mot nätverk är mycket svårare att identifiera med hjälp av traditionella metoder för detektering. Att hålla sig steget före sofistikerade attacker kräver ett mer modernt tillvägagångssätt som kraftigt utnyttjar säkerhetsinformationen i molnet. Utan molnbaserad intelligens, kan inte gateway-lösningarna hålla takten med dagens komplexa hot. NSA serien levererar nästa generations brandväggar (NGFW) genom att kombinera två olika avancerade säkerhetstekniker för att leverera toppmodernt förebyggande av hot som håller ditt nätverk ett steg före. SonicWall's Capture Threat Protection (ATP) har förbättrats tack vare vår patenterade Real-Time Deep Memory Inspection-teknik (RTDMI™).

RTDMI upptäcker och blockerar på förhand zero day-attacker och okända sabotageprogram genom att inspektera direkt i minnet. Tack vare realtidssystemet är SonicWall RTDMI-teknologin exakt, minimerar falska hot och identifierar och mildrar sofistikerade attacker där sabotageprogrammet inte är exponerat i mer än 100 nanosekunder. Sonics Walls patenterade* Reassembly-Free Deep Packet Inspection (RFDPI) tittar på all trafik och kontrollerar alla bytes i varje paket, och inspekterar både inkommande och utgående trafik. Genom att utnyttja SonicWall Capture Cloud-plattformen utöver funktionerna i boxen, som inkluderar skydd mot dataintrång, antisabotageprogram och webb-/webbadressfiltrering, blockerar NSa-serien även de mest lömska hoten vid gatewayen.

Vidare ger SonicWall-brandväggar fullständigt skydd genom att utföra full dekryptering och inspektion av TLS/SSL och SSH-krypterade anslutningar såväl som icke-proxyprogram, oavsett överföring eller protokoll. Brandväggen tar sig djupt in i varje paket (rubrik och data) och söker efter brister på överensstämmelse med protokoll, hot, zero-days-attacker, dataintrång och till och med definierade kriterier. DPI detekterar och förhindrar dolda attacker som utnyttjar kryptografi, blockerar hämtade krypterade sabotageprogram, upphör med spridningen av datavirus och förhindrar kommando och kontroll (C & C) kommunikation och data exfiltration. Regler för inklusion och exklusion tillåter total kontroll i att anpassa vilken trafik som är föremål för dekryptering och inspektion baserat på specifika organisatoriska överensstämmelser och/eller rättsliga krav.

När organisationer aktiverar deep packet inspection-funktioner som IPS, antivirus- och antispionprogram, TLS/SSL-dekryptering/inspektion och andra på sina brandväggar,

Fördelar:

Förstklassigt skydd och prestanda

- Patenterad real-time deep memory inspection-teknik
- Patenterad reassembly-free deep packet inspection-teknik
- On-box och molnbaserat skydd
- TLS/SSL-dekryptering och inspektion
- Beprövad, effektiv säkerhet
- Flerkärnig hårdvaruarkitektur
- Dedicerat Capture Labs forskningsteam

Nätverkskontroll och flexibilitet

- Kraftfullt SonicOS-operativsystem
- Applikationsintelligens och kontroll
- Nätverkssegmentering med VLAN
- Trådlös säkerhet i hög hastighet

Enkel implementering, installation och löpande hantering

- Tätt integrerad lösning
- Centraliserad förvaltning
- Skalbarhet genom flera hårdvaruplattformar
- Låg total kostnad

*U.S. Patent 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

blir ofta nätverkets prestanda långsammare, ibland till och med dramatiskt långsammare. NSA-seriens brandväggar har dock en flerkärnig hårdvaruarkitektur som nyttjar specialiserade säkerhetsmikroprocessorer. Kombinationen mellan RTDMI och RFDPI gör att nätverkets prestanda inte försämras lika mycket som med andra brandväggar.

Nätverkskontroll och flexibilitet

Kärnan i NSa-serien är SonicOS, SonicWalls funktionsrika operativsystem. SonicOS ger organisationer den nätverkskontroll och flexibilitet de behöver genom applikationsintelligens och kontroll, visualisering i realtid, intrångsskydd (IPS) med avancerad teknik, virtuellt privat nätverk i hög hastighet och andra robusta säkerhetsfunktioner.

Med hjälp av applikationsintelligens och kontroll kan nätverksadministratörer identifiera och kategorisera produktiva applikationer från de som är icke produktiva eller potentiellt farliga, och kontrollera trafiken genom kraftfulla policyer för applikationsnivå, både per användare och per grupp (tillsammans med scheman och undantagslistor). Affärskritiska applikationer kan prioriteras och tilldelas mer bandbredd medan icke-väsentliga applikationer är bandbreddsbegränsade. Övervakning och visualisering i realtid ger en grafisk representation av applikationer, användare och bandbreddsanvändning för detaljerad inblick i trafiken över nätverket.

För organisationer som kräver avancerad flexibilitet i sitt nätverk erbjuder SonicOS verktyg för att segmentera nätverket genom användning av virtuella LAN (VLAN). Detta gör det möjligt för nätverksadministratörer att skapa ett virtuellt LAN-gränssnitt som tillåter indelning av nätverk i en eller flera logiska grupper. Administratörer skapar regler som bestämmer graden av kommunikation med enheter på andra VLAN.

I varje brandvägg inom NSa-serien finns en inbyggd trådlös access controller som gör det möjligt för organisationer att säkert utöka nätets omkrets genom användning av trådlös teknik. Tillsammans skapar SonicWall-brandväggar och SonicWave 802.11ac Wave 2 trådlösa accesspunkter en trådlös nätverkssäkerhetslösning som kombinerar branschledande nästa generations brandväggsteknik med trådlös överföring med hög hastighet för nätverkssäkerhet och prestanda i företagsnätet över det trådlösa nätverket.

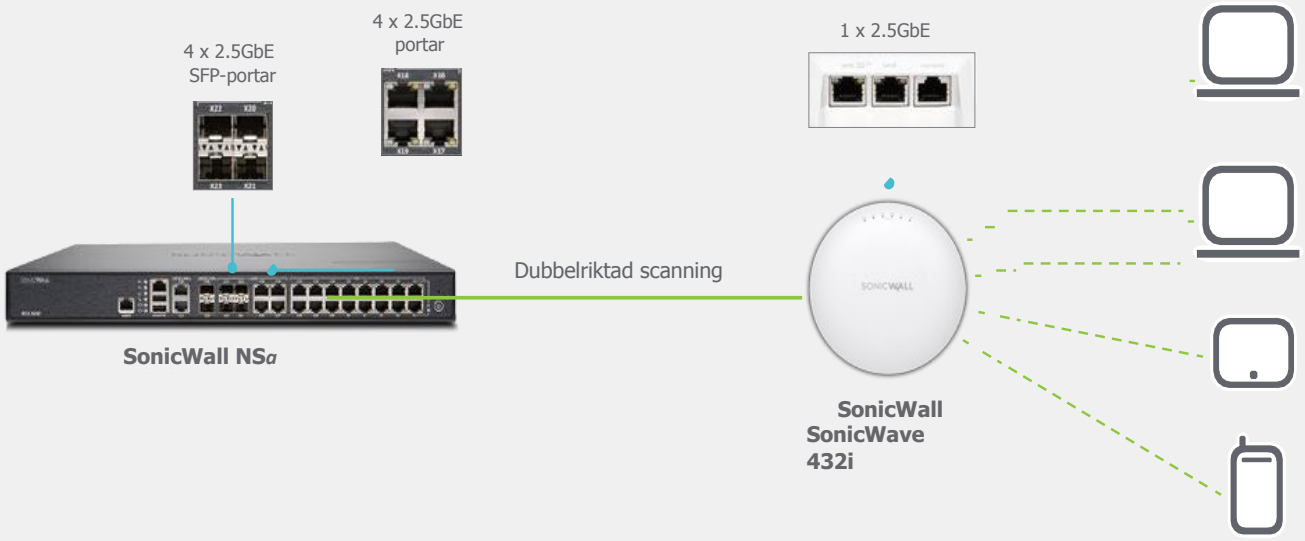
Enkel implementering, installation och enkelt underhåll

I likhet med alla SonicWalls brandväggar, integrerar NSa-serien viktiga tekniker för säkerhet, uppkopplingsmöjlighet och flexibilitet i en enda heltäckande lösning. Detta inkluderar SonicWave trådlösa accesspunkter och SonicWall WAN Acceleration Appliance (WXA)-serien, vilka båda upptäcks automatiskt och tillhandahålls av administratören för NSa-brandväggar. Genom att flera funktioner erbjuds behöver du inte köpa flera olika produkter som inte alltid passar ihop. Detta minskar behovet av att installera lösningar i nätverket och konfigurera dessa, vilket sparar både tid och pengar.

Hantering, övervakning och rapportering av säkerheten i nätverket hanteras centralt genom brandväggen eller via SonicWall Capture Security Center, vilket gör att nätverksadministratörerna kan ha koll på hela nätverket från ett ställe. Snabb och enkel installation tillsammans med enkel hantering gör det möjligt att sänka kostnaderna för ägandeskapet och gör så att ägaren får mycket tillbaka på investeringen.

Säker, trådlös uppkoppling med hög hastighet

Kombinera nästa generationens NSa-brandvägg med en SonicWave 802.11ac Wave 2 trådlös accesspunkt för att skapa en trådlös säkerhetslösning med hög hastighet. NSA-seriens brandväggar och SonicWave accesspunkter har båda 2,5 GbE-portar som möjliggör flera gigabits trådlöst dataflöde genom Wave 2-tekniken. Brandväggen scannar all trådlös trafik som kommer in och ut ur nätverket med hjälp av DPI-tekniken och raderar sen skadliga sabotageprogram och förhindrar dataintrång, även över krypterade anslutningar. Ytterligare säkerhets- och kontrollfunktioner som innehållsfiltrering, applikationskontroll och intelligens samt Capture Advanced Threat Protection kan köras på det trådlösa nätverket för att tillhandahålla ytterligare skyddsklasser.



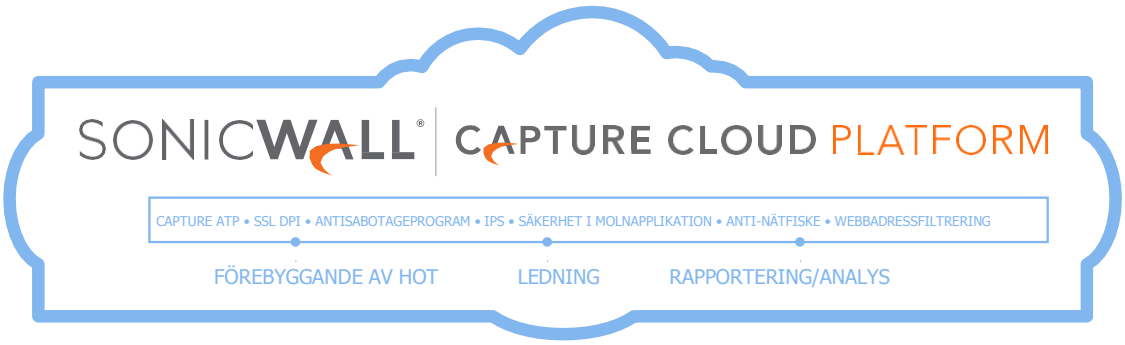
Capture Cloud

SonicWalls Capture Cloud-plattform levererar molnbaserat skydd och nätverkshantering samt rapportering och analys för organisationer av alla storlekar. Plattformen konsoliderar information om hot som hämtats från flera källor, inklusive vår prisbelönta sandboxing nätverkstjänst, Capture Advanced Threat Protection, samt mer än 1 miljon SonicWall sensorer som ligger utplacerade runt om i världen.

Om inkommande data i nätverket innehåller en tidigare osynlig skadlig kod, utvecklar SonicWalls dedicerade Capture Labs forskningsteam signaturer som lagras i Capture Cloud-plattformens databas och distribueras till kundens brandväggar så ett uppdaterat skydd kan skapas. Nya uppdateringar träder i kraft omedelbart utan omstart eller avbrott. Signaturerna som finns på apparaten skyddar mot många typer av attacker, och täcker tiotusentals enskilda hot med en enda signatur.

Utöver motåtgärderna erbjuder NSa-brandväggar kontinuerlig åtkomst till Capture Cloud-plattformens databas, som utökar informationen om signaturen ombord med tiotals miljoner signaturer.

Förutom att erbjuda förebyggande skydd erbjuder Capture Cloud-plattformen allt på ett ställe så att ledningen och administratörerna enkelt kan skapa både historiska rapporter om nätverksaktiviteter och rapporter i realtid.

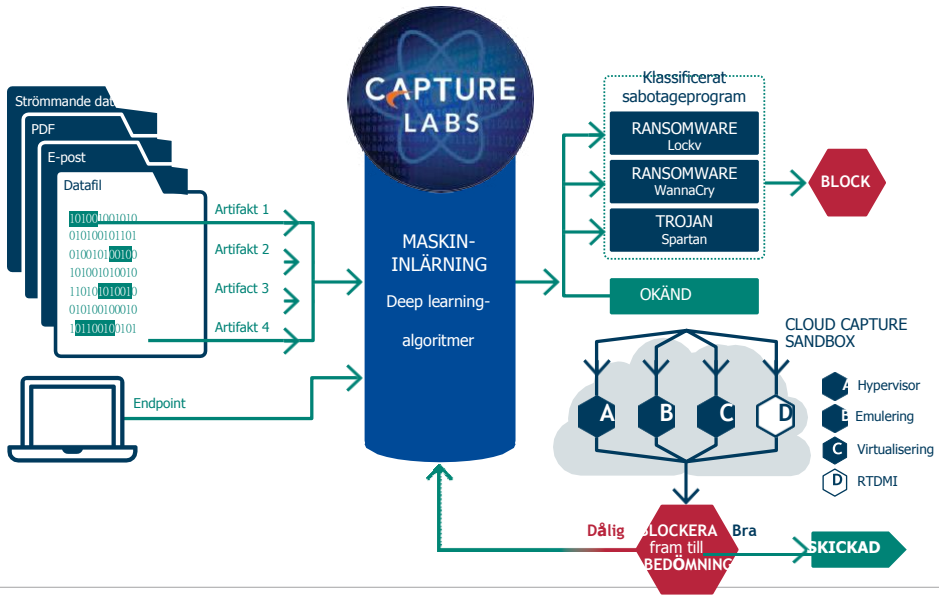


Advanced threat protection

I blickpunkten för SonicWalls automatiserade intrångsskydd av data i realtid står SonicWalls tjänst Capture Advanced Threat Protection, en molnbaserad flermotorig sandbox, som utökar brandväggens skydd mot hot för att detektera och förebygga zero-day attacker. Misstänkta filer skickas till molnet där de analyseras med hjälp av deep learning-algoritmeter med möjlighet att hålla dem kvar vid nätporten tills en bedömning fastställts. Plattformen med flermotorig sandbox, som inkluderar RTDMI i realtid, virtualiserad sandboxing, full systememulering och teknik för nivåanalys av hypervisor, exekverar misstänkt kod och analyserar beteende. När en fil identifieras som skadlig, blockeras den och en # skapas omedelbart inom Capture ATP. Kort därefter, skickas en signatur till brandväggarna för att förhindra efterföljande attacker.

Tjänsten analyserar ett brett spektrum av operativsystem och filtyper, inklusive körbara program, DLL, PDF-filer, MS Office-dokument, arkiv, JAR och APK.

För komplett endpoint-skydd kombinerar SonicWall Capture Client nästa generations antivirusteknik med SonicWalls molnbaserade flermotoriga sandbox.

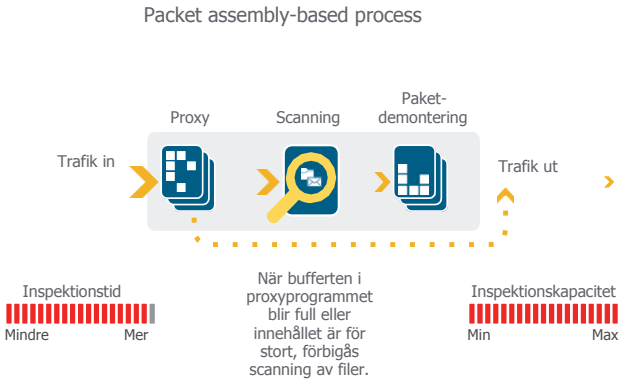


Reassembly-Free Deep Packet Inspection engine (RFDPI)

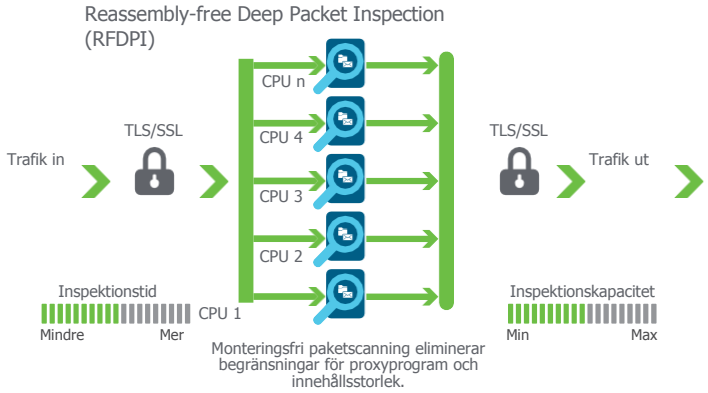
SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) är ett single-pass inspektionssystem med låg latent som utför strömningsbaserad, dubbelriktad trafikanalys med hög hastighet utan proxyprogram eller buffring för att effektivt detektera försök till dataintrång och hämtningar av skadliga program samtidigt som programmet identifierar trafik oavsett nätport och protokoll. Detta patenterade verktyg bygger på strömning av trafikens nyttolast för att upptäcka hot på layer 3-7 och tar nätverksflöden genom omfattande och upprepad normalisering och dekryptering för att neutralisera avancerade avvikande tekniker som försöker förvirra detektionstekniker och smyga in skadliga koder i nätverket.

När ett datapaket genomgår nödvändig förbehandling, inklusive TLS/SSL-dekryptering, analyseras den mot en enda ägande minnesrepresentation bestående av tre signaturdatabaser: intrångsattacker, sabotageprogram och applikationer. Anslutningstillståndet avanceras sedan för att representera strömningens position i förhållande till dessa databaser tills det stöter på ett tillstånd av angrepp eller annan ”matchande” händelse då en förinställd åtgärd vidtas.

I de flesta fall avslutas anslutningen och korrekt loggnings- och meddelandehändelser skapas. Verktyget kan emellertid också konfigureras för inspektion eller, vid applikationsdetektering, för att tillhandahålla layer 7 bandbreddshantering för resten av strömningen för applikationen, så snart applikationen har identifierats.



Konkurrenskraftig proxybaserad arkitektur



SonicWall strömbaserad arkitektur

Global hantering och rapportering

För hårt reglerade organisationer som vill uppnå en fullständigt samordnad säkerhetsstyrning, överensstämmelse och strategi för riskhantering, erbjuder SonicWall en enhetlig, säker och utbyggbar plattform för att hantera SonicWall brandväggar, trådlösa accesspunkter och switches fråb Dell X-Series växlar genom en korrelerad och redovisningsbar workstream-process. Företag kan enkelt stärka säkerheten, minska det administrativa arbetet och problemen vid felsökning samt hantera alla operativa aspekter av säkerhetsinfrastrukturen. Plattformen erbjuder bland annat centraliserad policyhantering och tillsyn, händelseövervakning i realtid, användaraktiviteter, applikationsidentifieringar, flödesanalys och flow forensics, compliance- och audit-reporting med mer. Tack vare workflow-automatisering kan företag med GMS dessutom effektivt hantera alla ändringar i sina brandväggar.

Med hjälp av GMS-workflow-automatiseringen kan alla företag implementera lämpliga brandväggsregler flexibelt och konfidentiellt vid rätt tidpunkt och i överensstämmelse med compliance-reglerna. GMS erbjuder ett sammanhängande sätt att hantera nätverkssäkerhet genom affärsprocesser och servicenivåer. Lösningen adresserar hela säkerhetsmiljön istället för att använda en enhetsbaserad strategi, vilket förändrar livscykelhanteringen.