SonicWall-Produktüberblick: Auf einen Blick

Next-Generation-Firewalls

High-End: NS*sp* 15700/12800/12400

Die Multi-Instance-Firewall für große, verteilte Konzerne, Rechenzentren und MSSPs sorgt für schnellen Schutz, hohe Portdichte und echte Mandantenisolation durch Unified Policy.

Mid-Range: NS*a* Series
NS*a* 9650/9450/9250/ 6650/5650/4650/3650/2700/2650

Branchenweit bewährte Effektivität und Leistung für mittelgroße Netzwerke, Zweigstellen und verteilte Konzerne.

Einstiegslevel: TZ Series
TZ670/TZ570/TZ470/TZ370/TZ270/ TZ600/TZ500/TZ400/TZ350/TZ300/ SOHO 250

Integrierter Bedrohungsschutz und SD-WAN-Plattform für zu Hause, kleine bis mittelständische Unternehmen sowie SD-Branch-Implementierungen.

Virtuell: NSv Series
NSv 10/25/50/100/200/270/300/ 400/470/800/870/1600

Virtuelle Firewalls mit flexiblen Lizenzierungsmodellen, die alle kritischen Komponenten Ihrer Public und Private-Cloud-Infrastruktur schützen.

WLAN-Sicherheit

SonicWave Series
SonicWave 432e/432i/432o/ 231c/224w/231o

Via Cloud oder Firewall verwaltete Sicherheit und Leistung für die nächste Generation von Wireless-Geräten.

Sicherer mobiler Zugriff

SMA Series SMA 8200v/7210/ 6210/500v/410/210

Einfacher, regelbasierter, sicherer Zugriff auf Netzwerk- und Cloud-Ressourcen.

Access Switch

SWS12-8/SWS12-8POE/SWS12-10FPOE/ SWS14-24/SWS14-24FPOE/SWS14-48/ SWS14-48FPOE

Liefert intelligente Switchfunktionalität für sichere Konnektivität der nächsten Generation für KMU und SD-Branch-Implementierungen.

E-Mail Security Series

ESA 9000/7000/5000/ VM Software/Cloud Service

Eine mehrschichtige Lösung zum Schutz vor raffinierten E-Mail-Bedrohungen.

Capture Security Appliance (CS*a*)

On-Prem-Dateiprüfungen und Malware-Schutz.

Verwaltung und Analyse

Capture Security Center
Global Management System (GMS)
Network Security Manager

Kontrolle und umfassender Überblick über Ihr Netzwerk.

Capture Client

Eine einheitliche Client-Plattform mit globalem Dashboard und mehreren Funktionen für die Endpunktsicherheit, einschließlich hoch entwickeltem Malware-Schutz, Sandboxing, Informationen über Anwendungsschwachstellen und im Infektionsfall Rücksetzung in den zuletzt bekannten unbeschadeten Zustand.

Cloud Edge Secure Access

Eine leistungsstarke SaaS-Anwendung mit einfachem Network-as-a-Service für Site-to-Site- und Hybrid Cloud-Konnektivität mit AWS, Azure und Google Cloud. Dabei werden Zero-Trust und Least-Privilege Sicherheitsansätze in einem integrierten Angebot kombiniert.

Cloud App Security

Eine Cloud-native Lösung liefert Sicherheit der nächsten Generation für SaaS-Anwendungen wie Office 365 und G Suite. Damit werden E-Mail, Daten und Anmeldedaten vor komplexen Bedrohungen geschützt, während gleichzeitig für Konformität in der Cloud gesorgt wird.

Next-Gen-Firewall-Aboservices

Threat Protection Service Suite liefert die grundlegenden Security-Dienste, die zur Sicherstellung des Schutzes Ihres Netzwerks vor Bedrohungen notwendig sind, in einem preiswerten Bündel. Dieses Bündel ist nur für die TZ270/370/470 Series erhältlich und beinhaltet Gateway Anti-Virus, Intrusion Prevention und Application Control, Content Filtering Service, Network Visibility sowie 24/7 Support.

Essential Protection Services Suite bietet alle wichtigen Sicherheitsdienste, die zum Schutz vor bekannten und unbekannten Bedrohungen notwendig sind. Dazu gehören Capture Advanced Threat Protection mit RTDMI Technologie, Gateway Anti-Virus, Intrusion-Prevention und Anwendungskontrolle, Content-Filtering-Service, Comprehensive Anti-Spam Service, Netzwerktransparenz und 24/7 Support.

Advanced Protection Services Suite bietet erweiterte Sicherheit für das Netzwerk. Dieses Bündel beinhaltet die Services des Essential-Abos sowie Cloud-Management und 7 Tage Cloud-basiertes Reporting.

Die Advanced Gateway Security Suite (AGSS) ist als Add-on-Service für alle physischen und virtuellen SonicWall-Firewalls erhältlich und schützt vor komplexen und unbekannten Bedrohungen.

In der Advanced Gateway Security Suite (AGSS) enthalten; mit Next-Generation-Firewall in der TotalSecure Advanced Edition kombiniert

- Capture Advanced Threat Protection (ATP): Cloud-basiertes Multi-Engine-Sandboxing
- Gateway-Anti-Virus- und Anti-Spyware-Schutz
- Intrusion Prevention Service
- Anwendungskontrolle
- Content-/Web-Filtering-Service
- 24/7-Support

Security as a Service (SECaaS)

Outsourcen Sie Ihre Netzwerksicherheit mit unserer sofort einsatzbereiten Lösung.

Weitere Informationen finden Sie auf sonicwall.com

Evaluierungsfragen

Next-Generation-Firewalls

- Können Sie mit dem steigenden Bandbreitenbedarf, der Gigabit- oder Multi-Gigabit-Leistung erfordert, Schritt halten?
- Ist Ihre aktuelle Firewall in der Lage, eine Bedrohungsprüfung mit der Geschwindigkeit eingehender Bedrohungen durchzuführen?
- Was sind Ihre Kriterien bezüglich der Leistungsanforderungen?
- Wie hoch ist die Gesamtzahl der Benutzer/Netzwerke hinter der Firewall?
- Wie hoch ist die Gesamtzahl der Sitzungen/Verbindungen während der Spitzenzeiten?
- Wie viele Remote-Standorte und -Benutzer werden mit der Firewall verbunden?
- Wie messen Sie die Effektivität Ihrer Sicherheitskontrollen?
- Welche Art von Internetverbindung haben Sie? Und wie schnell ist sie?
- Wie schützen Sie Ihre Organisation vor neuen Bedrohungen wie Zero-Day-Angriffen?
- Kann Ihre Sandbox Bedrohungen, die sich tief im Speicher verbergen, erkennen und blockieren?
- Wie viele Engines umfasst Ihre Sandbox?
- Kann Ihre Sandbox Dateien am Gateway zurückhalten, bevor sie freigegeben werden?
- Wissen Sie, ob Ihre Unternehmensfirewall HTTPS-Datenverkehr überprüft?
- Kam es in Ihrer Organisation bei der Prüfung von HTTPS-Verkehr zu Netzwerkunterbrechungen oder -ausfällen?
- Ist Ihre virtuelle Firewall genauso robust wie Ihre physische Firewall?
- Wie schützen Sie Ihre Public- oder Private-Cloud-Umgebungen?
- Können Sie angemessene Sicherheitszonen und Mikrosegmentierung in Ihrem virtuellen Netzwerk anwenden?
- Haben Sie eine umfassende Einsicht in Ihren virtuellen Datenverkehr sowie die volle Kontrolle darüber?
- Würden Sie gerne Kosten reduzieren, indem Sie MPLS mit SD-WAN für Secure Private Networking ersetzen?

Capture Client

- Benötigen Ihre Endgeräte einen durchgängigen, erweiterten Schutz vor Ransomware und verschlüsselten Bedrohungen?
- Wie einfach können Sie Regelkonformität und Lizenzmanagement über alle Endgeräte hinweg durchsetzen?
- Fehlt es Ihnen an Transparenz für Ihre Endgeräte und bereitet Ihnen die Verwaltung Ihrer Sicherheitsplattform Probleme?
- Ermöglicht Ihr Endpunktsicherheitsprodukt eine Verbindung zu einer Sandbox-Umgebung?
- Können Sie die an Endpunkten installierten Anwendungen katalogisieren und bestimmen, wie viele Schwachstellen darin enthalten sind?
- Überwacht Ihre aktuelle Lösung kontinuierlich den Zustand Ihrer Systeme?
- Können Sie im Fall eines Ransomware-Angriffs auf einen zuletzt bekannten unbeschadeten Zustand zurücksetzen?
- Wie schnell können Sie Richtlinien für Mandanten hinzufügen oder ändern?

Cloud App Security

- Verwenden Sie O365 oder G Suite?
- Setzen Sie Proofpoint oder Mimecast für die Sicherung Ihrer O365/G Suite ein?
- Scannen Sie interne E-Mail in O365?
- Wie viele genehmigte SaaS-Anwendungen werden in Ihrer Organisation verwendet?
- Ist es für Sie schwierig, die Konformität der in SaaS-Anwendungen gespeicherten Daten durchzusetzen?
- Wie erkennen Sie, ob Anmeldedaten Ihrer Benutzer kompromittiert sind?
- Verfügen Sie über die notwendige Transparenz, um zu erkennen, wer von wo und wann auf Ihre Daten zugreift? (BYOD)

Deep-Memory-Erkennung

Die zum Patent angemeldete SonicWall Real-Time Deep Memory Inspection (RTDMI™) Engine erkennt und blockiert unbekannte Massenmalware proaktiv mittels Deep Memory Inspection in Echtzeit. Die jetzt mit dem SonicWall Capture Advanced Threat Protection (ATP)-Cloud-Sandbox-Service verfügbare Engine identifiziert und stoppt selbst die gefährlichsten modernen Bedrohungen einschließlich künftiger Meltdown-Exploits.

WLAN-Sicherheit

- Klagen Ihre Mitarbeiter/Partner/Kunden über eine langsame WLAN-Leistung?
- Was ist die maximale Anzahl gleichzeitiger Wireless-User in Ihrem Netzwerk?
- Haben Sie Bedenken hinsichtlich der Kosten für eine neue sichere Wireless-Lösung in Ihrem Netzwerk?
- Wie gut kennen Sie sich mit dem 802.11ac-Wave-2-Wireless-Standard aus?
- Brauchen Sie mehr Flexibilität bei der Verwaltung Ihrer Access Points - ob via Cloud oder Firewall?
- Haben Sie Ihr WLAN-Netzwerk effektiv geplant?
- Haben Sie APs, die nicht an Firewalls gebunden sein sollten?
- Machen Sie sich Gedanken über die Bereitstellung komplexer Sicherheitsfunktionen auf Ihrem WLAN-Netwerk?
- Sind Gastservices für Sie wichtig?
- Benötigen Sie ein personalisiertes Gäste-Login-Portal für das Onboarding von Gästen?

Access Switch

- Benötigen Sie Gigabit-fähige Access Switches für PoE-fähige Geräte?
- Ist Ihnen ein einheitliches Sicherheitslevel mit einheitlicher Transparenz und Verwaltung wichtig?
- Stehen Sie vor Lösungsproblemen mit Switches von Drittanbietern, die mit dem SonicWall-Ökosystem funktionieren?

Sicherer mobiler Zugriff

- Was ist Ihre derzeitige Strategie für den Zugriff Ihrer Remote-Mitarbeiter?
- Was halten Sie von einem Zero-Trust-Netzwerkzugang?
- Wie bieten Sie Benutzern sicheren Zugriff auf Unternehmensressourcen und Anwendungen, die On-Prem und in der Cloud gehostet werden?
- Verfügen Sie über eine ausreichende Transparenz, um zu sehen, welche Benutzer und Geräte auf Ihr Netzwerk zugreifen?
- Wie schützen Sie momentan Ihre geschäftskritischen Websites und Webserver?

E-Mail-Sicherheit

- Bereiten Ihnen E-Mail-Bedrohungen wie Ransomware, Spear-Phishing und Business-E-Mail-Compromise Kopfzerbrechen?
- Bietet Ihre aktuelle E-Mail-Sicherheitslösung Schutzfunktionen gegen hoch entwickelte Bedrohungen?
- Befürchten Sie, dass E-Mails mit vertraulichen Informationen nach außen dringen könnten?
- Wie halten Sie Vorgaben wie DSGVO, Sarbanes-Oxley, GLBA oder HIPAA ein?
- Möchten Sie Ihren Kunden verwaltete E-Mail-Security-Services bereitstellen? (MSSPs)

Verwaltung und Analyse

- Welche Probleme könnten Sie beheben, indem Sie Ihre Sicherheitslösungen in einer einzigen zentralen Verwaltungsplattform zusammenführen?
- Welche betrieblichen Vorteile erhalten Sie, wenn Sie alle Ihre Firewalls, APs und Switches zentral über eine Cloud-Konsole von jedem Standort aus verwalten können?
- Wie zuversichtlich sind Sie, dass Sie in der Lage sind, die Einhaltung von Cybersicherheitsvorgaben wie PCI, HIPPA und DSGVO nachzuweisen?
- Wie würde sich Ihr Sicherheitskonzept verändern, wenn Sie in der Lage wären, Bedrohungen und Risiken besser, schneller und genauer zu identifizieren und darauf zu reagieren?
- Welchen Nutzen würden Sie und Ihr Führungsteam erzielen, wenn Sie einen vollen Einblick in die Cyberbedrohungen und Risiken für Ihr Unternehmen hätten?

Cloud Edge Secure Access

- Verfügen Sie über viele sensible Daten? Bereiten Ihnen überprivilegierte Benutzer Kopfzerbrechen?
- Sind Sie besorgt wegen der zunehmenden Auflagen für Datenschutz und Informationssicherheit?
- Müssen Sie die Zusammenarbeit zwischen Mitarbeitern und externen Geschäftspartnern sowie den Umgang mit sensiblen Ressourcen kontrollieren?
- Wie viele Zweigstellen haben Sie? Wie effizient können Sie eine neue einbinden?
- Wie lange dauert das sichere Onboarding eines Remote-Benutzers?

Datasheet-SonicWallProductLineAtAGlance-US-VG-2877

SONICWALL®