SonicWall-Produkte auf einen Blick

Next-Generation-Firewalls

High-End: NS*sp* Series
Diese Firewalls sind für große, verteilte Konzerne, Rechenzentren und MSSPs ausgelegt. Sie bieten einen schnellen Schutz, eine hohe Portdichte und einen Firewall-Inspection-Durchsatz von bis zu 100 GBit/s.

Mid-Range: NS*a* Series
Branchenweit bewährte Effektivität und Leistung für mittelgroße Netzwerke, Zweigstellen und verteilte Konzerne.

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

Virtuell: NS*v* Series
Virtuelle Firewalls mit flexiblen Lizenzierungsmodellen, die alle kritischen Komponenten Ihrer Public- und Private-Cloud-Infrastruktur schützen.

Die SonicWall-Firewalls umfassen DNS sowie eine reputationsbasierte Content-Filterung, um schädliche Websites und Anwendungen zu blocken. Sie unterstützen darüber hinaus Reputation-Scores zur Steuerung der Richtlinien für Webinhalte. Ein erweiterter Speicher für Auditdateien, die Integration der Netzwerkzugangskontrolle (NAC) sowie automatisierte Updates sorgen für eine höhere Benutzerfreundlichkeit.

SonicWave Series

Verbesserte Sicherheit, Performance und Skalierbarkeit dank Wi-Fi-6-Unterstützung, verwaltet über die Cloud mit SonicWall Wireless Network Manager oder Network Security Manager.

SMA Series

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

SonicWall-Switch

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

E-Mail-Sicherheit

ESA Series
Eine mehrschichtige Lösung zum Schutz vor raffinierten E-Mail-Bedrohungen; bereitgestellt in Form einer Appliance, VM oder Cloud-SaaS-Lösung.

Capture Security Appliance (CS*a*)

On-Prem-Dateiprüfungen und Malware-Schutz.

Verwaltung und Analyse

Global Management System (GMS)
Network Security Manager
Wireless Network Manager
Zentrale Verwaltung, Risikosteuerung und Einhaltung von Vorschriften. Ermöglichen Sie Reporting und gewinnen Sie Einblicke in Datenverkehr und Bedrohungen. Automatisieren Sie Workflows und Updates.

Capture Client

Eine einheitliche Client-Plattform mit globalem Dashboard und mehreren Funktionen für Endpoint-Security, 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-Konzept 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-Sicherheit

Eine cloudnative 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 Services Suite liefert die grundlegenden Security-Dienste, die zur Sicherstellung des Schutzes Ihres Netzwerks vor Bedrohungen notwendig sind, in einem preiswerten Bundle. Dieses Bundle 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 Bundle beinhaltet die Services des Essential-Abos sowie Cloud-Management und 7 Tage cloudbasiertes Reporting.

Weitere Informationen finden Sie auf sonicwall.com

Evaluierungsfragen

Next-Generation-Firewalls

- Wie verhindern Sie den Zugriff auf bösartige Websites oder die Anzeige unangemessener Inhalte?
- Haben Sie unterschiedliche Lösungen für DNS und Content-Filterung?
- 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 im Deep Memory verborgene Bedrohungen erkennen und blockieren?
- Wie viele Engines umfasst Ihre Sandbox?
- Kann Ihre Sandbox Dateien am Gateway festsetzen, 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 Visibilität 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-Sicherheit

- Verwenden Sie O365 oder G Suite?
- Setzen Sie Proofpoint oder Mimecast für die Sicherung Ihrer O365/G Suite ein?
- Scannen Sie interne E-Mails 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 patentierte 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.

SonicWave Series

- 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 Secure-Wireless-Lösung in Ihrem Netzwerk?
- Wie gut kennen Sie sich mit dem 802.11ax-Wireless-Standard aus?
- Brauchen Sie mehr Flexibilität bei der Verwaltung Ihrer Access-Points an verschiedenen Standorten?
- 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?

SonicWall-Switch

- Benötigen Sie gigabitfähige 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?
- Sollten Ihre Switches unabhängig von den Firewalls laufen?

Secure Mobile Access

- 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 Email Security Services bereitstellen (MSSPs)?

Verwaltung und Analyse

- Wie bleiben Sie im Hinblick auf Firmware-Updates aktuell?
- Wie setzen Sie organisationsweit Sicherheitsrichtlinien durch?
- 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, HIPAA 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?
- Benötigen Sie integriertes Wireless- und Switch-Management in einem einzigen Dashboard?

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?