SONICWALL-PRODUKTÜBERBLICK: AUF EINEN BLICK

Next-Generation-Firewalls

High-End: NS*sp* 12000
Series NS*sp* 12800/12400
Skalierbare Sicherheit nach dem neusten Stand der Technik für große, verteilte Konzerne, Rechenzentren und Diensteanbieter, die die Vorteile der Cloud-Intelligence nutzen

Mid-Range: NS*a* Series
NS*a* 9650/9450/9250/
6650/5650/4650/3650/2650
Branchenweit bewährte Effektivität und Leistung für mittelgroße Netzwerke, Zweigstellen und verteilte Konzerne

Einstiegslevel: TZ Series
TZ600/TZ500/TZ400/ TZ350/
TZ300/ SOHO 250/SOHO
Integrierter Bedrohungsschutz und SD-WAN-Plattform für kleine bis mittelständische sowie große verteilte Konzerne

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

Wireless Security

SonicWave Series
SonicWave 432e/432i/432o/
231c/224w/231o
Via Cloud oder Firewall verwaltete Sicherheit und Leistung für die nächste Generation von Wireless-Geräten

Weitere Informationen: www.sonicwall.com/de-de/products

Secure Mobile Access

SMA Series SMA
EX9000/8200v/7200/
6200/500v/400/200
Einfacher, regelbasierter, sicherer Zugriff auf Netzwerk- und Cloud-Ressourcen

E-Mail Security Series

ESA 9000/7000/5000/
VM Software/Cloud Service
Eine mehrschichtige Lösung zum Schutz vor raffinierten E-Mail-Bedrohungen

Verwaltung und Analyse

Capture Security Center
Global Management System (GMS)
Analysen
Kontrolle und umfassender Überblick über Ihr Netzwerk

WAN Acceleration Series

WXA 6000 (SW)
WXA 5000 (VM)/500 (SW)
Erheblich verbesserte Performance bei der Anwendungsübertragung und höhere Mitarbeiterproduktivität

Capture Client

Eine einheitliche Client-Plattform mit mehreren Funktionen für die Endpunktsicherheit, einschließlich hoch entwickeltem Malware-Schutz, Sandboxing, Gerätekontrolle und im Infektionsfall Zurückversetzung in den zuletzt bekannten unbeschadeten Zustand

Web Application Firewall (WAF)

Sicherheit für Webanwendungen, Schutz vor Datenlecks und Einhaltung gesetzlicher Vorgaben, lokal oder in der Cloud

Cloud App Security

Diese CASB-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

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)

Sourcen Sie Ihre Netzwerksicherheit mit unserer sofort einsatzbereiten Lösung aus

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.

Evaluierungsfragen

Next-Generation-Firewalls

- Wie messen Sie die Effektivität Ihrer Sicherheitskontrollen?
- Wie gehen Sie vor, wenn Sie Sicherheitslücken identifiziert haben?
- Wie reduzieren Sie das Risiko, dass Ihre Benutzer auf ungeschützte Webanwendungen zugreifen?
- Welche Art von Internetverbindung haben Sie? Und wie schnell ist sie?
- Müssen Sie bei der Performance Abstriche machen, um die Sicherheit in Ihrem Netzwerk zu verbessern?
- Wie schützen Sie Ihre Organisation vor neuen Bedrohungen wie Zero-Day-Angriffen?
- Kann Ihr Team innerhalb von 12 Stunden nach der Veröffentlichung eines Patches Schwachstellen beseitigen?
- 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 festsetzen, bevor sie freigegeben werden?
- Wissen Sie, dass die meisten Websessions verschlüsselt sind? Und wissen Sie, ob Ihre Firewall diese entschlüsseln und prüfen kann?
- 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?
- Verfügt Ihre aktuelle Firewall über PoE-/PoE+-Unterstützung oder müssen Sie Ihre PoE-fähigen Geräte mittels Switch mit Strom versorgen?
- Würden Sie gerne Kosten reduzieren, indem Sie MPLS mit SD-WAN für Secure Private Networking ersetzen?
- Benötigen Sie abobasierte Lizenzierung für virtuelle Firewalls?

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?
- Überwacht Ihre aktuelle Lösung kontinuierlich den Zustand Ihrer Systeme?
- Können Sie im Fall eines Ransomware-Angriffs auf einen zuletzt bekannten unbeschadeten Zustand zurücksetzen?
- Haben Sie die Möglichkeit, die Verbindung unbekannter oder möglicherweise infizierter Geräte mit Endpunkten zu verhindern?

Web Application Firewall

- Wie schützen Sie momentan Ihre geschäftskritischen Websites und Webserver?
- Welche Sicherheitsmaßnahmen treffen Sie, um die PCI-Sicherheitsanforderungen einzuhalten?

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)

Wireless Security

- 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 effektiv geplant?
- Haben Sie APs, die nicht an Firewalls gebunden sein sollten?
- Machen Sie sich Gedanken über die Bereitstellung komplexer Sicherheitsfunktionen auf Ihrem WLAN?

Secure Mobile Access

- Plant oder führt Ihre Organisation gerade die Verlagerung Ihrer Geschäftsanwendungen und -ressourcen in die Cloud durch?
- Bieten Sie Ihren Benutzern Single-Sign-On für lokale und Cloud-Anwendungen?
- Verwenden Ihre Mitarbeiter Dropbox oder private E-Mail-Accounts für die Weitergabe von Dateien?
- Müssen Ihre Mitarbeiter mehrere URLs und Passwörter verwalten?
- Wie sieht Ihre aktuelle Mobility-/BYOD-Strategie aus?
- Haben Sie einen Überblick, welche Geräte auf Ihr Netzwerk zugreifen?

E-Mail Security

- 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 wirtschaftlichen und operativen Herausforderungen verursacht die Verwaltung Ihrer Sicherheitsinfrastruktur?
- 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?

WAN-Beschleunigung

- Verfügt Ihre Organisation über mehrere Außenstellen? Wie viele?
- Sind die Büros über ein VPN oder eine dedizierte WAN-Verbindung (MPLS) angeschlossen?
- Nutzen Ihre Mitarbeiter Anwendungen wie Microsoft Windows File Sharing, SharePoint, Office oder FTP?
- Möchten Sie den Bandbreitenverbrauch und die Kosten reduzieren, statt in den Ausbau der Netzwerkkapazität zu investieren?

Weitere Informationen: www.sonicwall.com/de-de/products

Datasheet-SonicWallProductLineAtAGlance-US-VG-MKTG5159

SONICWALL®