# ENTSCHLÜSSELUNG UND PRÜFUNG VON VERSCHLÜSSELTEM VERKEHR

## High-Performance-Schutz vor verschlüsselten Bedrohungen

Dem 2018 SonicWall Cyber Threat Report zufolge macht verschlüsselter Verkehr heute fast 70 Prozent der gesamten Webkommunikation in Organisationen aus. Zwar bietet die Verschlüsselung von Internetsitzungen viele Vorteile – zum Beispiel werden die Integrität und die Vertraulichkeit persönlicher Informationen während der Übertragung sichergestellt. Ein Nachteil ist aber, dass immer mehr Malware-Autoren diese Verschlüsselungsmethoden nutzen, um ihre Angriffe vor Firewalls zu verstecken. So können Angreifer Firewalls umgehen und über Schwachstellen Malware einschleusen, die in der Lage ist, einen direkten Zugang in jedes Netzwerk zu schaffen. Darüber hinaus nutzen sie auch TLS/SSL, um Command-and-Control-Verkehr zu verbergen und infizierte Systeme von praktisch jedem beliebigen Ort aus zu manipulieren. Organisationen, die darauf verzichten, den verschlüsselten Verkehr zu prüfen, nutzen nicht das gesamte Potenzial ihrer Firewallsysteme. Sie sind nicht in der Lage, den Datenverkehr zu durchleuchten, bösartige Dateien zu identifizieren oder das Einschleusen von Malware und das unerlaubte Versenden vertraulicher Informationen auf externe Systeme zu bemerken.

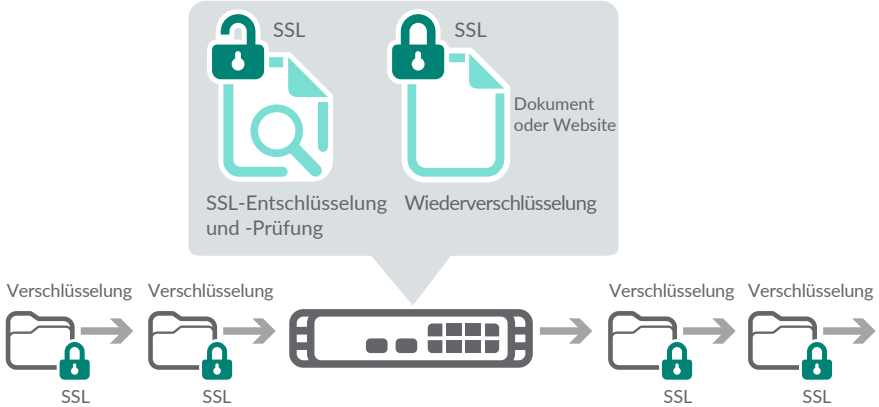
Mit der SonicWall Deep Packet Inspection-Prüfung für TLS/SSL-verschlüsselten Verkehr (DPI-SSL) können Organisationen ihre Netzwerke zuverlässig vor diesen Sicherheitsrisiken schützen. Unsere DPI-SSL-Technologie ist als Add-on-Service auf allen Next-Generation-Firewalls und Unified Threat Management(UTM)-Netzwerksicherheitsappliances von SonicWall verfügbar. Der erweiterte DPI-SSL-Schutz für verschlüsselte Bedrohungen basiert auf der patentierten Reassembly-Free Deep Packet Inspection-Engine von SonicWall, die eine große Bandbreite an Verschlüsselungsprotokollen – u. a. HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS und POPS – unabhängig vom verwendeten Port durchleuchtet.

Der Service entschlüsselt TLS-/SSL-Verkehr, überprüft ihn auf Bedrohungen, verschlüsselt ihn erneut und leitet ihn – sofern keine Bedrohungen oder Schwachstellen gefunden werden – an den Zielort weiter. DPI-SSL ist ein unverzichtbarer Service, um Datenlecks zu vermeiden, eine robuste Anwendungskontrolle zu implementieren und höchste Sicherheit für geschäftskritische Systeme zu gewährleisten.

Dieser Service bietet wichtige Funktionen zur Sicherheits- und Anwendungskontrolle sowie zur Vermeidung von Datenlecks für die Analyse von HTTPS- und anderem TLS-/SSL-verschlüsseltem Verkehr.

**Vorteile:**

- Besserer Einblick in den TLS-/SSL-verschlüsselten Verkehr
- Blockieren versteckter Malware-Downloads
- Möglichkeit, C&C-Kommunikation sowie das Ausschleusen vertraulicher Daten zu verhindern
- Anpassung von Auswahl-/Ausschlusslisten gemäß Compliance-Anforderungen oder rechtlichen Vorgaben



## Systemanforderungen

| Die TLS/SSL-Prüfung ist für folgende SonicWall-Firewalls verfügbar: |
|---|
| SOHO / SOHO W |
| TZ300 / TZ300 W / TZ300P |
| TZ400 / TZ400 W |
| TZ500 / TZ500 W |
| TZ600 / TZ600P |
| NSa 2650 |
| NSa 3650 |
| NSa 4650 |
| NSa 5650 |
| NSa 6650 |
| NSa 9250 |
| NSa 9450 |
| NSa 9650 |
| SuperMassive 9800 |
| NSsp 12400 |
| NSsp 12800 |
| NSv 10 |
| NSv 25 |
| NSv 50 |
| NSv 100 |
| NSv 200 |
| NSv 300 |
| NSv 400 |
| NSv 800 |
| NSv 1600 |

**Partner Enabled Services**
Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Unsere SonicWall Advanced Services Partner bieten Ihnen erstklassige Professional Services. Weitere Infos erhalten Sie unter www.sonicwall.com/PES.

## Funktionen

**Hohe Performance und große Anzahl an Verbindungen** – die Next-Generation-Firewalls von SonicWall nutzen eine hoch entwickelte Prozessorarchitektur und eine sehr große Anzahl an Verbindungen. Auf diese Weise werden sowohl die DPI-SSL-Performance als auch die Sicherheit über alle vernetzten Geräte hinweg optimiert.

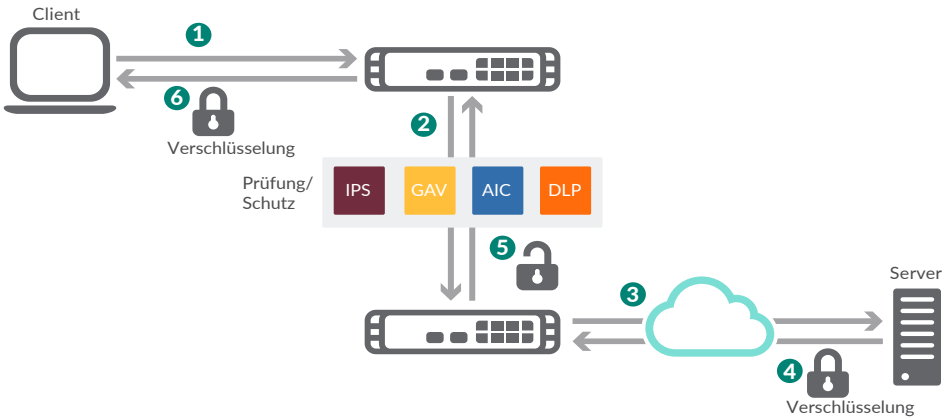
**Sichere und einfache Einrichtung** – die DPI-SSL-Entschlüsselung und -Prüfung schützt Benutzer im Netzwerk zuverlässig und verursacht dank ihrer Einfachheit einen minimalen Konfigurationsaufwand.

**Auswahl-/Ausschlusslisten** – bei Implementierungen mit hohem Verkehrsaufkommen können Administratoren vertrauenswürdige Quellen ausschließen, um die Netzwerkleistung zu steigern. Darüber hinaus können Administratoren eine TLS-/SSL-Prüfung auf Teile des Datenverkehrs anwenden. Dazu müssen sie eine Liste mit Adressen, Services oder Benutzerobjekten oder -gruppen gemäß Datenschutzbestimmungen oder rechtlichen Vorgaben erstellen.

**Client-Implementierungsmodus** – dieser Modus ermöglicht die Prüfung von TLS-/SSL-Verkehr, wenn der Client sich im LAN der Firewall befindet und auf Inhalte im WAN zugreift. Nachdem die Appliance den verschlüsselten Verkehr entschlüsselt und geprüft hat, schreibt sie das vom Remote Server gesendete Zertifikat um und unterzeichnet das neu generierte Zertifikat mit dem benutzerspezifischen Zertifikat. Standardmäßig handelt es sich hier um die Appliance-Zertifizierungsstelle, obwohl ein anderes Zertifikat ausgewählt werden kann.

**Server-Implementierungsmodus** – dieser Modus ermöglicht die Prüfung von TLS-/SSL-Verkehr, wenn Remote Clients eine Verbindung über das WAN herstellen, um auf Inhalte zuzugreifen, die sich im LAN der Firewall befinden. Auf diese Weise kann der Administrator Kopplungen eines Adressobjekts und eines Zertifikats konfigurieren. Wenn die Appliance TLS-/SSL-Verbindungen zum Adressobjekt entdeckt, legt sie das gekoppelte Zertifikat vor und handelt die TLS-/SSL-Verbindung mit dem sich verbindenden Client aus. In diesem Szenario besitzt der Eigentümer der SonicWall-Next-Generation-Firewall die Zertifikate und privaten Schlüssel des ursprünglichen Content-Servers.

**Umfassender Support** – zu den unterstützenden Funktionen gehören Anwendungskontrolle, Content-/URL-Filtering sowie Schutz vor Eindringlingen, Malware und durch Malware veranlasste Command-and-Control-Kommunikation.




### TLS-/SSL-Prüfung – Client-Implementierungsmodus

1. Der Client startet einen TLS-/SSL-Handshake mit dem Server.
2. Die Next-Generation-Firewall fängt die Anfrage ab und stellt eine Sitzung mit eigenen Zertifikaten anstelle des Serverzertifikats her.
3. Die Next-Generation-Firewall startet einen TLS-/SSL-Handshake mit dem Server im Auftrag des Clients, wobei sie ein vom Administrator definiertes TLS-/SSL-Zertifikat verwendet.
4. Der Server schließt den Handshake ab und baut einen sicheren Tunnel zwischen sich selbst und der Next-Generation-Firewall auf.
5. Die Next-Generation-Firewall verschlüsselt den Datenverkehr erneut und leitet ihn an den Client weiter.
6. Die Next-Generation-Firewall entschlüsselt den gesamten Verkehr zum oder vom Client und prüft ihn auf Bedrohungen und Regelverstöße.

## Systemanforderungen

Die TLS-/SSL-Prüfung ist für folgende SonicWall-Next-Generation Firewalls verfügbar:

| FIREWALL | EINMALLIZENZ |
|---|---|
| SOHO / SOHO W | 01-SSC-0723 |
| TZ300 / TZ300 W / TZ300P | Im Sicherheitsservice-Abo enthalten |
| TZ400 / TZ400 W | Im Sicherheitsservice-Abo enthalten |
| TZ500 / TZ500 W | Im Sicherheitsservice-Abo enthalten |
| TZ600 / TZ600P | Im Sicherheitsservice-Abo enthalten |
| NS*a* 2650 | Im Sicherheitsservice-Abo enthalten |
| NS*a* 3650 | Im Sicherheitsservice-Abo enthalten |
| NS*a* 4650 | Im Sicherheitsservice-Abo enthalten |
| NS*a* 5650 | Im Sicherheitsservice-Abo enthalten |
| NS*a* 6650 | Im Sicherheitsservice-Abo enthalten |
| NS*a* 9250 | Im Sicherheitsservice-Abo enthalten |
| NS*a* 9450 | Im Sicherheitsservice-Abo enthalten |
| NS*a* 9650 | Im Sicherheitsservice-Abo enthalten |
| SuperMassive 9800 | Im Sicherheitsservice-Abo enthalten |
| NS*sp* 12400 | Im Sicherheitsservice-Abo enthalten |
| NS*sp* 12800 | Im Sicherheitsservice-Abo enthalten |
| NS*v* 10 | Im Sicherheitsservice-Abo enthalten |
| NS*v* 25 | Im Sicherheitsservice-Abo enthalten |
| NS*v* 50 | Im Sicherheitsservice-Abo enthalten |
| NS*v* 100 | Im Sicherheitsservice-Abo enthalten |
| NS*v* 200 | Im Sicherheitsservice-Abo enthalten |
| NS*v* 300 | Im Sicherheitsservice-Abo enthalten |
| NS*v* 400 | Im Sicherheitsservice-Abo enthalten |
| NS*v* 800 | Im Sicherheitsservice-Abo enthalten |
| NS*v* 1600 | Im Sicherheitsservice-Abo enthalten |

## Über uns

Seit über 27 Jahren bekämpft SonicWall Cyberkriminalität, um kleinen, mittleren und großen Unternehmen weltweit Schutz zu bieten. Mit unseren Produkten und Partnern können wir eine automatisierte Echtzeitlösung zur Erkennung und Prävention von Sicherheitslücken für die individuellen Anforderungen von mehr als 500.000 Organisationen in über 215 Ländern und Regionen bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.



SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Information erhalten Sie auf unserer Website.
www.sonicwall.com


DataSheet-DecryptionAndInspection-US-VG-MKTG4095