ENTSCHLÜSSELUNG UND PRÜFUNG VON VERSCHLÜSSELTEM VERKEHR

High-Performance-Schutz vor verschlüsselten Bedrohungen

Dem SonicWall Annual Threat Report 2017 zufolge macht verschlüsselter Verkehr heute mehr als 60 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.

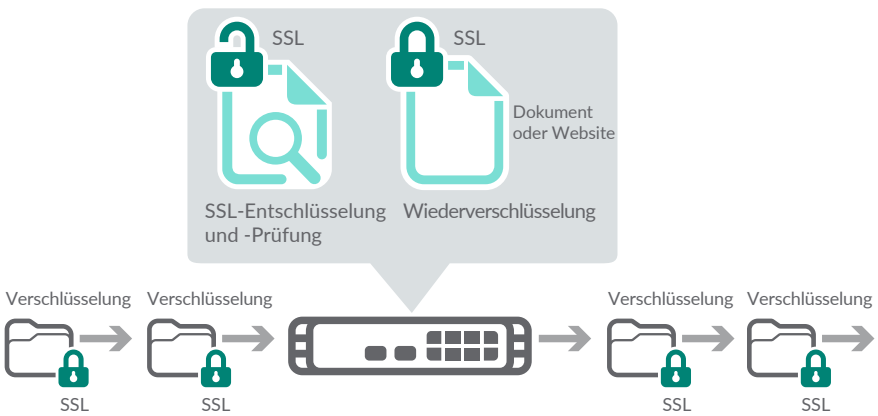
Mit der SonicWall Deep Packet Inspection-Prüfung für SSL-verschlüsselten Verkehr (DPI-SSL) können Organisationen ihre Netzwerke zuverlässig vor diesen Sicherheitsrisiken schützen. Unsere DPI-SSL-Technologie ist als Add-on-Service auf allen Next-Generation-Firewalls und Unified Threat Management(UTM)-Netzwerksicherheitsappliances von SonicWall verfügbar. Der erweiterte DPI-SSL-Schutz für verschlüsselte Bedrohungen basiert auf der patentierten Reassembly-Free Deep Packet Inspection-Engine von SonicWall – einer Full-Stack-Stream-Inspection-Technologie, 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 SSL-verschlüsseltem Verkehr.

Vorteile:

- Einblick in den SSL-/TLS-verschlüsselten Verkehr
- Blockieren verschlüsselter 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 SSL-Prüfung ist für alle Appliances der TZ, Network Security Appliance und SuperMassive Series verfügbar.
Die SSL-Prüfung ist für folgende SonicWall-Firewalls verfügbar:
SonicWall SOHO / SOHO W
SonicWall TZ300 / TZ300 W
SonicWall TZ400 / TZ400 W
SonicWall TZ500 / TZ500 W
SonicWall TZ600
NSA 2600
NSA 3600
NSA 4600
NSA 5600
NSA 6600
SuperMassive 9200
SuperMassive 9400
SuperMassive 9600
SuperMassive 9800
SuperMassive E10200
SuperMassive E10400
SuperMassive E10800

Funktionen

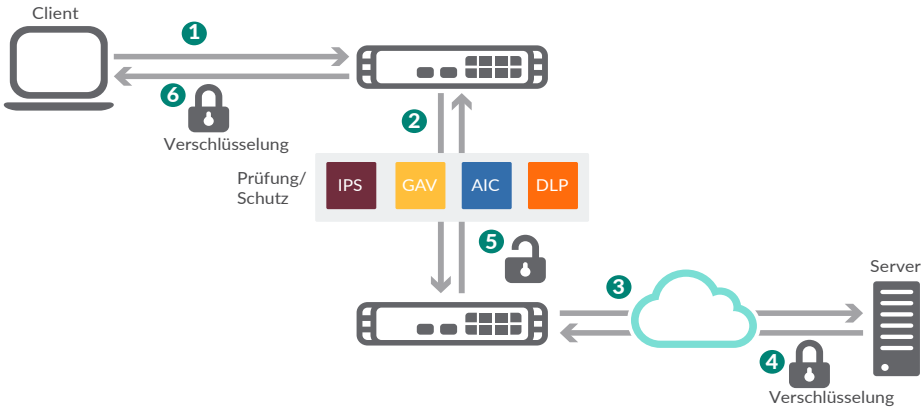
Sichere und einfache Einrichtung – die DPI-SSL-Entschlüsselung und -Prüfung schützt Benutzer im Netzwerk zuverlässig und verursacht dank seiner Einfachheit einen minimalen Konfigurationsaufwand.

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.



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

FIREWALL	EINMALLIZENZ
SOHO / SOHO W	01-SSC-0723
TZ300 / TZ300 W	Im Sicherheitsservice-Abo enthalten
TZ400 / TZ400 W	Im Sicherheitsservice-Abo enthalten
TZ500 / TZ500 W	Im Sicherheitsservice-Abo enthalten
TZ600	Im Sicherheitsservice-Abo enthalten
NSA 2600	Im Sicherheitsservice-Abo enthalten
NSA 3600	Im Sicherheitsservice-Abo enthalten
NSA 4600	Im Sicherheitsservice-Abo enthalten
NSA 5600	Im Sicherheitsservice-Abo enthalten
NSA 6600	Im Sicherheitsservice-Abo enthalten
SuperMassive 9200	Im Sicherheitsservice-Abo enthalten
SuperMassive 9400	Im Sicherheitsservice-Abo enthalten
SuperMassive 9600	Im Sicherheitsservice-Abo enthalten
SuperMassive 9800	Im Sicherheitsservice-Abo enthalten
SuperMassive E10200	Im Sicherheitsservice-Abo enthalten
SuperMassive E10400	Im Sicherheitsservice-Abo enthalten
SuperMassive E10800	Im Sicherheitsservice-Abo enthalten

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

- NSA 220 / NSA 220 W
- NSA 250M / NSA 250MW
- NSA 240
- NSA 2400
- NSA 2400MX
- NSA 3500
- NSA 4500
- NSA 5000
- NSA E5500
- NSA E6500
- NSA E7500
- NSA E8500
- NSA E8510

Über SonicWall

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, Kalifornien 95054, USA
Weitere Information erhalten Sie auf unserer Website.
www.sonicwall.com

DataSheet-SSLinspection-EU-IMAG-23904