Ob aus technischer oder kommerzieller Sicht: Die SSL VPN Appliances von Watchguard vermögen rundum zu überzeugen.

Sicherer Remote-Zugriff dank SSL VPN Appliances von Watchguard

Dass Mitarbeitende im Aussendienst oder im Homeoffice jederzeit einen sicheren Zugang zum Firmennetzwerk, zu Daten und Applikationen erhalten – dafür sorgen die SSL VPN Appliances von Watchguard.

Auf die Bedürfnisse von mobilen Usern und Aussenbüros zugeschnitten sind die SSL VPN Appliances «SSL 100» und «SSL 560» von Watchguard. Die All-in-one-Lösungen verschaffen bis zu 500 Anwendern einen gleichzeitigen Remote-Zugriff auf das Firmennetzwerk sowie auf wichtige Unternehmensressourcen (Daten und Applikationen). Die intuitiv bedienbaren, in wenigen Minuten installierten Plattformen basieren auf der erprobten SSL-VPN-Technologie von Watchguard und gewähren dank sicher verschlüsselten SSL-Tunnels eine maximale Kommunikationssicherheit. Sie ermöglichen via Web-Browser oder über spezielle Clients einen sicheren Zugriff auf individuell freigegebene Ressourcen und unterstützen dabei Funktionen wie SSH (Secure Shell), RDP (Remote Desktop), Anbindung von File Shares/Home Directories sowie bidirektionale Tunnels. Externe Mitarbeitende sind somit in der Lage, weltweit zuverlässig und sicher mit ihren gewohnten Programmen zu arbeiten – als wären sie im Büro vor Ort.

Einfache Handhabung

Die SSL VPN Appliances beeindrucken durch ein einfaches Handling. Nach erfolgter Anmeldung übermitteln sie ein Web-Portal mit den individuellen Applikationen des jeweiligen Users. Web-Anwendungen werden direkt im Browser angezeigt. Nicht webbasierte Applikationen hingegen werden mittels Zugangs-Client, der sich selbst auf dem jeweiligen Endgerät installiert, freigegeben.

Nebst der Anmeldung mit Username und Passwort bietet die Integration einer Zwei-Faktoren-Authentisierung zusätzlichen Schutz. Dabei generiert die Appliance automatisch Zugangsschlüssel und Einmal-Passwörter (OTP) und schickt diese via SMS an den entsprechenden User. Dieser kann sich alsdann durch die Eingabe der erhaltenen Zugangsdaten authentisieren. Komfortabel präsentiert sich ferner die Einbindung der PKI-Lösung (Public Key Infrastructure) SuisseID. Wird ein SuisseID-Stick am USB-Port des Rechners angeschlossen, erfolgt die Authentisierung des Anwenders automatisch.

Nach erfolgter Anmeldung bleibt der Zugriff auf die individuell freigegebenen Ressourcen erhalten. Dank dieser Single-Sign-on-Funktionalität (SSO) entfällt beim Wechsel von einer zur anderen Applikation eine erneute Authentisierung – und somit auch die Übermittlung der einzelnen Passwörter.

Nebst der Gewährung eines sicheren Remote-Zugriffs sowie der geschützten Datenkommunikation via SSL-Tunnel bieten die Appliances zusätzliche Security-Funktionen wie etwa Netzwerk- und Applikationskontrolle, Session-Time-out und Activity Tracking. Zudem erlauben weitreichende Integritätsprüfungen («Deep Device Examination»/Assessment der End-User-Devices) die Einhaltung individueller Sicherheitsregeln. So lässt sich beispielsweise die Anmeldung von Geräten unterbinden, die keine Firewall oder keinen aktuellen Virenschutz besitzen.

Weiter sorgen die Appliances nach Ablauf der jeweiligen Session für einen maximalen (Daten-)Schutz. So werden beispielsweise alle Endpunkt-Zugriffsdaten sowie Dateien und Cache-Speicher nach abgeschlossener Sitzung automatisch gelöscht. Datenlecks und unerlaubte Zugriffe auf Netzwerkressourcen werden so vermieden.

Die Appliances von Watchguard vermögen auch aus kommerzieller Sicht zu überzeugen. Die Lizenzkosten basieren auf der Anzahl gleichzeitiger User – unabhängig davon, wie vielen Benutzenden der gesicherte Remote-Zugriff zur Verfügung steht. Die Appliances bewegen sich im Preisbereich ab 2500 Franken.

Kontakt

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60
info@boll.ch
www.boll.ch