SDoT
Security Gateway Express

Sicherer Informationsaustausch in Echtzeit zwischen Netzen mit unterschiedlichem Schutzbedarf bis GEHEIM

Grundlagen

Das Produkt SDoT Security Gateway Express ist ein Sicherheitsgateway, das einen sicheren, kontrollierten und bidirektionalen Datentransfer zwischen zwei unterschiedlichen Sicherheitsdomänen ermöglicht. Das Produkt ist eine Variante des SDoT Security Gateways, welches vom BSI für eine Nutzung in Netzen zugelassen ist, die staatliche Verschlusssachen bis zum Geheimhaltungsgrad GEHEIM verarbeiten.
Das SDoT Security Gateway Express (kurz „SDoT Express") ist auf Einsatzszenarien optimiert, die eine möglichst latenzarme Übertragung von Daten erfordert. Es kann damit in so genannten „Echtzeitszenarien" eingesetzt werden.

Merkmale

Mit SDoT Express ist es möglich, hochfrequente Datenpakete mit sehr niedriger Latenz und hohem Datendurchsatz zwischen unterschiedlichen Sicherheitsdomänen auszutauschen. Insbesondere die Filtermechanismen wurden auf die Prüfung von typisch militärischen bzw. von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) verwendeten Nachrichtenformaten (z.B. XML, Link 16, ASTERIX, ADatP-3, ADEXP, NMEA, DIS, etc.) optimiert. Diese Nachrichten sind meist nur wenige Kilobyte groß, werden aber in sehr schneller Folge, d.h. mit einer hohen Frequenz, übertragen. Dabei muss die durch das Gateway in der Signalkette hinzugefügte Latenz möglichst gering sein.
Mit dem SDoT Express steht ein Produkt zur Verfügung, bei dem nun Echtzeitanwendungen über Domänengrenzen möglich sind, wie z. B. die extrem zeitkritische Kommunikation zwischen Sensoren und Effektoren mit dem jeweiligen Feuerleit- oder Führungssystem oder der Austausch von sensiblen personenbezogenen Informationen zwischen unterschiedlichen Behörden zur Generierung eines vollständigen Gefährdungslagebilds.

Funktionsweise

SDoT Express filtert zu übertragende Daten anhand vorkonfigurierter Regelwerke und führt für jedes einzelne Datenelement der zu übertragenden Nachricht eine strenge inhaltliche Kontrolle durch. Informationen, die nicht dem Regelwerk entsprechen, werden entweder abgelehnt und damit blockiert oder sanitarisiert, d.h. bestimmte Teile der Daten werden durch vorgegebene Werte ersetzt. Damit kann sichergestellt werden, dass aus der höher eingestuften Sicherheitsdomäne (HIGH) keinerlei sensible Informationen in die niedriger eingestufte Sicherheitsdomäne (LOW) abfließen können.
SDoT Express verfügt über eine Reihe von evaluierten und zugelassenen Parsern, die in der Lage sind, unterschiedliche, strukturierte Datenformate zu „verstehen". Die Regelwerke werden im Vorfeld einer Nutzung erstellt und beschreiben die erlaubten Daten eindeutig.
Es ist möglich verschiedene Regelwerke gleichzeitig zu betreiben und diese verschiedenen Regelwerke unterschiedlichen Protokollen zuzuordnen. Damit ist ein flexibler Einsatz von SDoT Express in allen Szenarien von Behörden und Organisationen mit Sicherheitsaufgaben, inkl. der Echtzeit-Kopplung von unterschiedlichen Sicherheitsdomänen innerhalb von Waffensystemen der Streitkräfte, möglich. Eine Aktualisierung und Änderung der Regelwerke im operativen Betrieb ist natürlich ebenso möglich.

Sicherheitsarchitektur

Die interne Sicherheitsarchitektur des SDoT Express basiert auf dem mit dem SDoT Security Gateway 6.0 eingeführten und mehrfach vom BSI bis GEHEIM zugelassenen SDoT Security Framework.
Daneben liefert die Hardware einen entscheidenden Beitrag zur Sicherheit des Gesamtsystems. SDoT Express wird als Security Appliance ausgeliefert und benötigt lediglich eine Höheneinheit in Standard-19 Zoll-Racks. Die Hardware wurde dabei so konzipiert, dass sie die sicherheitsrelevanten Eigenschaften des SDoT Security Framework optimal unterstützt und gleichzeitig extrem schock- und vibrationsresistent ist. Sie ist herkömmlicher Server-Hardware deutlich überlegen.
Die Entwicklung der Hard- und Software der gesamten SDoT-Produktfamilie folgt strikt dem Grundsatz „Security by Design". Angriffe, falsche Benutzereingaben und technische Fehlfunktionen sind von Anfang an berücksichtigt und die Produkte sind so konzipiert und gehärtet, dass Sicherheitsfunktionen zu keinem Zeitpunkt außer Kraft gesetzt werden können.

Basisfunktionen

- Unterstützte Kommunikationsprotokolle: HTTP, SMTP, TCP, UDP
- Beschränkung auf zulässige IP-Ziele
- Umfassende Protokollierungs- und Auditfunktionalitäten
- Alarmierung bei Sicherheitsverstößen und Störungen
- Fernadministration aller Komponenten mittels komfortablem, leicht verständlichem WebInterface
- Optional: Hochverfügbarkeitsvariante mit Failover

Datentransfer von HIGH nach LOW

- Unterstützte Formate bei automatisierter Freigabe: XML, ADEXP, NMEA0183, ADatP3, ASTERIX, Link 16 sowie praktisch alle Arten von stark strukturierten Daten
- Online Zugriff auf Web Services
- Download von „schwarzen" Daten in den „roten" Bereich
- Latenz und Durchsatz von HIGH nach LOW : < 3 ms und bis zu 200 MB/s

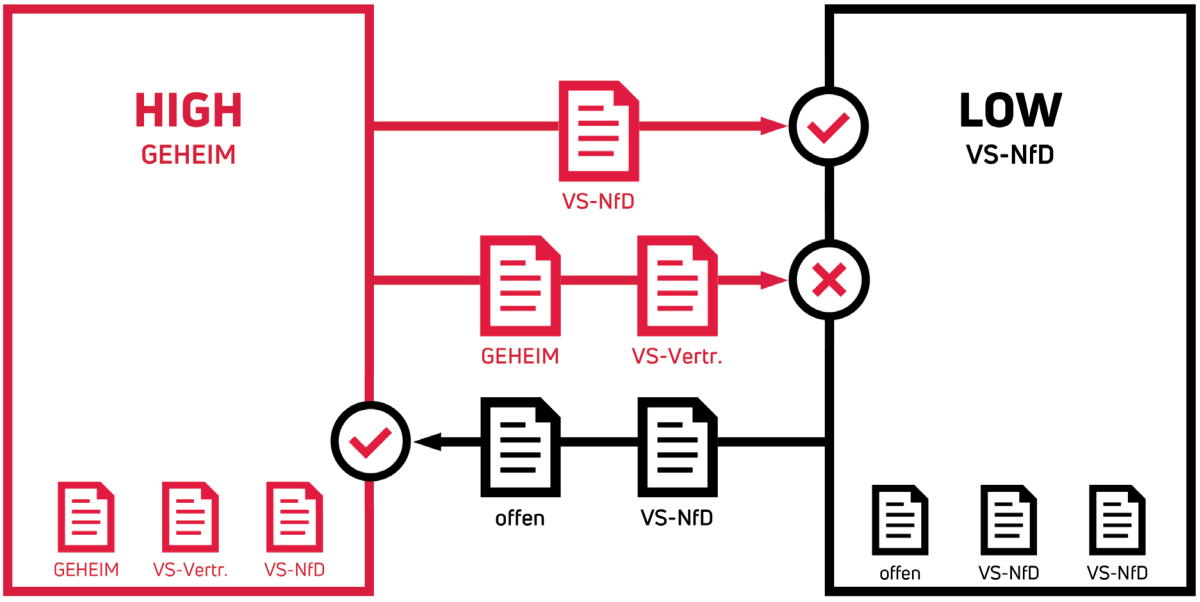
Datentransfer von LOW nach HIGH

- Übertragung aller Arten von Daten mittels der unterstützten Protokolle (auch SNMP)
- Optional: Filterung möglich analog zu HIGH nach LOW
- Latenz und Durchsatz von LOW nach HIGH*: < 1 ms und bis zu 800 MB/s

Zusammenfassung

Die INFODAS GmbH stellt mit dem SDoT Security Gateway Express ein sicheres und extrem leistungsstarkes Sicherheitsgateway vor, um eine vertrauenswürdige und performante Datenkommunikation zwischen verschiedenen Sicherheitsdomänen für Echtzeitanwendungen zu ermöglichen.

*) Angaben zu Latenz und Durchsatz sind abhängig vom individuellen Anwendungsfall



Datenübertragung aufgrund des Geheimhaltungsgrades - mit dem SDoT Security Gateway Express in Echtzeit

infodas
Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
Rhonestraße 2
50765 Köln
T +49 221 70912-0
F +49 221 70912-86
vertrieb@infodas.de
www.infodas.de