SDoT®
SecureDomainTransition

infodas®
Cologne IT Solutions & Services

SDoT® Security Gateway 6.0

Sicherer Informationsaustausch zwischen Netzen mit unterschiedlichen Schutzbedarfen mit allgemeiner Zulassung des BSI

Grundlagen

Themen wie Führungsunterstützung, Informationsmanagement und vernetzte Operationsführung sind von zentraler Bedeutung für alle militärischen Bereiche.
Erst die verzugslose Verfügbarkeit von relevanten Informationen auch und gerade über Netzgrenzen hinweg ermöglicht ein umfassendes Lagebild und beeinflusst den Führungsprozess entscheidend.
Dabei ist unbedingt sicherzustellen, dass an den Netzübergängen die strikten Vorgaben des Geheimschutzes eingehalten werden. Es muss also eine exakte Prüfung der zu übertragenden Informationen stattfinden.

SDoT® verbindet Netze

Das Produkt „Secure Domain Transition **SDoT®** Security Gateway“ bietet hierfür die passende Lösung. Es wird an der hochsensiblen Schnittstelle zwischen zwei unterschiedlich klassifizierten Netzen eingesetzt. **SDoT®** Security Gateway garantiert als „sicherer Netzübergang“, dass nur diejenigen Daten zwischen den Netzen fließen können, die aus Sicht des Geheimschutzes übertragen werden dürfen.
Wird beispielsweise ein GEHEIM klassifiziertes Netz mit einem VS-NfD klassifizierten Netz mittels **SDoT®** Security Gateway verbunden, so sorgt der sichere Filtermechanismus dafür, dass aus dem GEHEIM klassifizierten Netz nur solche Informationen abfließen, die die Einstufungen „VS-NfD“ oder „offen“ aufweisen. Gleichzeitig können, bei Bedarf, auch Daten aus dem VS-NfD-Netz problemlos in das GEHEIM klassifizierte Netz übertragen werden. Eine zusätzliche Firewall schützt dabei das höher klassifizierte Netz vor potenziellen Angriffen aus dem niedriger klassifizierten.
SDoT® Security Gateway ermöglicht also einen bidirektionalen Datenaustausch zwischen Netzen unterschiedlichen Schutzbedarfs.

Zulassung bis GEHEIM

An den hochsensiblen Netzübergängen dürfen nur absolut zuverlässige Sicherheitssysteme eingesetzt werden. Die Verlässlichkeit und Sicherheit des Produkts **SDoT®** Security Gateway wurde bereits mehrfach für die unterschiedlichen Einsatzszenarien vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Einsatz bis GEHEIM bestätigt. Die entsprechenden Einzelzulassungen wurden seitens des BSI auf der Basis von erfolgreich durchgeführten Evaluationen (Wehrtechnische Dienststelle 81) erteilt.
Nach mehrjähriger gemeinsamer entwicklungsbegleitender Evaluierung hat nun das BSI im April 2017 die „allgemeine“ Zulassung für GEHEIM erteilt. Das **SDoT®** Security Gateway 6.0 basiert nunmehr auf einem speziell angepassten, vollständig evaluierten Microkernel-Betriebssystem und ist damit das erste und einzige Sicherheitsgateway am Markt, für welches eine Vollzulassung für GEHEIM ausgesprochen wurde.
Das Produkt steht **ab sofort** allen Bedarfsträgern in Bundeswehr und öffentlicher Verwaltung zur Verfügung. Ein projektspezifischer Zulassungsantrag ist fortan nicht mehr notwendig. Das nächste erklärte Ziel ist es, eine allgemeine Zulassung für NATO SECRET und EU SECRET zu erhalten.

Generallizenz für die Bundeswehr

Die Bundeswehr verfügt über eine Generallizenz zur Nutzung des Produktes **SDoT®** Security Gateway der Firma INFODAS GmbH. Diese Generallizenz erstreckt sich auch auf die neueste Version von **SDoT®** Security Gateway. Damit steht **SDoT®** 6.0 Security Gateway teilstreitkraftübergreifend allen Projekten und Vorhaben zur Verfügung und kann dadurch einen wesentlichen Beitrag zur Verbesserung der NetOpFü-Fähigkeit der Bundeswehr leisten.

Content Filtering made in Germany

Das **SDoT®** Security Gateway führt eine exakte inhaltliche Kontrolle und Steuerung des Datenflusses am Netzübergang durch. Die Inhaltskontrolle kann dabei sowohl automatisiert als auch manuell erfolgen. Bei der automatisierten Kontrolle prüft ein Parser alle Daten, die über das Gateway transportiert werden sollen hinsichtlich ihrer Struktur und ihres Inhalts. Beispiele sind Statusinformationen und Standort-Koordinaten in XML-Dateien, nautische Daten im Format NMEA 0183, Radardaten im ASTERIX-Format oder Meldungen im Link 16-Format.

Filterung anhand von Sicherheitslabeln

Für Daten, die nicht durch ein Regelwerk automatisiert geprüft werden können, bietet das **SDoT®** Security Gateway die Prüfung eines extern erzeugten Sicherheitslabels an. Dabei werden statt der inhaltlichen Prüfung der Daten nun der im Sicherheitslabel angegebene Geheimhaltungsgrad sowie die Gültigkeit der Signatur geprüft. Durch eine starke, kryptographische Bindung ist eine unerlaubte Manipulation an den Daten oder dem Sicherheitslabel nicht möglich.
SDoT® Security Gateway unterstützt NATO-konforme XML Security Label. INFODAS GmbH bietet darüber hinaus mit dem Produkt **SDoT®** Labelling Service einen netzwerkbasierten Dienst zum Erzeugen von solchen Sicherheitslabeln an.

SDoT®
SecureDomainTransition

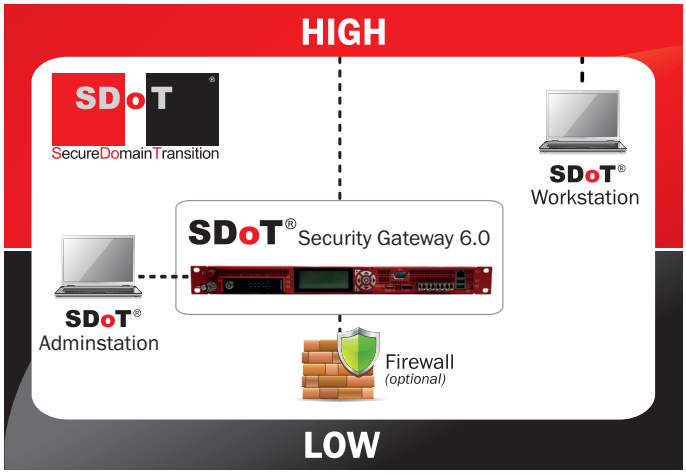
infodas®
Cologne IT Solutions & Services

Verbesserte Sicherheitsarchitektur

Das **SDoT®** Security Gateway 6.0 nutzt zur weiteren Verbesserung der Sicherheit eine nochmals (im Vergleich zur Version 5.0) überarbeitete Architektur, die auf einem neuen Betriebssystem mit starker Separierung aufsetzt. Die sicherheitskritischen Filtermechanismen des **SDoT®** Security Gateway werden durch so genannte „Kompartments“ wirksam und nachweisbar von den nicht-sicherheitskritischen Funktionen, abgeriegelt. Die neue Architektur basiert dabei auf einer vollständig evaluierten Version des Microkernel-Betriebssystems L4, das speziell für den SDoT-Anwendungsfall umfangreich und in Abstimmung mit dem BSI modifiziert wurde.

Neben der gesamten Filterlogik werden auch alle kryptographischen Funktionen durch die Separierungsfunktionen des Betriebssystems von den Netzwerkschnittstellen zu beiden Netzen getrennt. Alle sensiblen Funktionen sind somit vor einem Direktzugriff eines potenziellen Angreifers sowohl aus dem niedriger als auch dem höher klassifizierten Netz effektiv geschützt.

Durch die Verwendung des Microkernel Betriebssystem wird einerseits eine Evaluierung der Plattform überhaupt erst möglich, andererseits reduziert sich der Hardwareaufwand erheblich. Eine mit **SDoT®** Security Gateway 6.0 neu eingeführte Spezialhardware ermöglicht dabei sogar die Nutzung eines Servers mit einer sehr geringen Bauhöhe von nur einer Höheneinheit in Standard-19-Zoll-Racks.



Neue kryptographische Komponente

SDoT® Security Gateway verfügt seit Version 5.0 über eine dedizierte HW-Komponente zur Bereitstellung von kryptographischen Funktionen und zugriffsgeschützten Speicherbereichen. Ab der Version 6.0 kommt ein speziell für **SDoT®** angepasstes, so genanntes S-HSM (**SDoT®** Hardware Security Module), zum Einsatz. Das S-HSM stellt über eine minimalisierte und gehärtete Schnittstelle alle kryptographischen Sicherheitsfunktionen und einen zugriffsgeschützen Speicher zur Verfügung. Das S-HSM wird im Rahmen der entwicklungsbegleitenden Evaluation den gleichen Prüfungen wie das Gesamtsystem unterzogen.

Übersicht der Funktionen

Basis-Funktionalitäten

- Unterstützte Kommunikationsprotokolle: HTTP, SMTP, TCP, UDP, FTP (mit **SDoT®** Data Store)
- Beschränkung auf zulässige IP-Ziele
- Schutz vor Angriffen aus dem schwarzen Netz durch Einsatz einer Firewall
- Virenprüfung der per SMTP, HTTP und FTP übertragenen Daten, Filterung aktiver Inhalte durch zusätzliche Firewall
- Umfassende Protokollierungs- und Auditfunktionalitäten
- Alarmierung bei Sicherheitsverstößen und Störungen
- Fernadministration aller Komponenten mittels komfortablem, leicht verständlichem Web-Interface
- Schutz vor Fehlkonfiguration, Fehlbedienung und Fehlfunktionen: Der ungewollte Abfluss von eingestuften Informationen wird auch im Fehlerfall wirksam verhindert
- Hochverfügbarkeitsvariante mit Failover optional erhältlich
- Bandbreitenkontrolle
- Separierung durch evaluierten Microkernel

Datentransfer von HIGH nach LOW

- Unterstützte Formate bei automatisierter Freigabe: XML, ADEXP, NMEA0183, ADatP-3, ASTERIX, Link 16 sowie praktisch alle Arten von stark strukturierten Daten
- Unterstützte Formate bei manueller Freigabe mittels des Viewers der **SDoT®** Workstation: ASCII, XML, ADatP-3, monochrome Bitmaps, RTF mit eingeschränktem Befehlssatz; weitere Formate auf Anfrage
- Unterstütze Formate bei automatischer Freigabe basierend auf extern erzeugten Sicherheitslabeln (z.B. mit dem **SDoT®** Labelling Service): alle Dateitypen
- Veröffentlichung freigegebener Dokumente auf dem **SDoT®** Data Store zum Abruf durch andere Systeme im niedriger klassifizierten Netz (HTTP oder FTP)
- Online-Zugriff auf Web Services
- Download von „schwarzen“ Daten in den „roten“ Bereich

Datentransfer von LOW nach HIGH

- Übertragung von allen Arten von Daten mittels der unterstützten Protokolle (auch SNMP)
- Kontrollierter Download über HTTP (**SDoT®** Data Store)
- Kontrollierter Datenaustausch über HTTP (HTTP-Response wird geprüft)
- Automatische Erzeugung von Sicherheitslabeln basierend auf der Klassifizierung des niedriger eingestuften Netzes: Damit ist ein späterer Rücktransport nach LOW möglich, sofern die Daten unverändert geblieben sind.

Zusammenfassung

Die INFODAS GmbH stellt heute mit **SDoT®** Security Gateway eine flexible, zulassungsfähige Lösung zum Datenaustausch zwischen Domänen mit unterschiedlichem Schutzbedarf mit allgemeiner Zulassung des BSI bereit.

INFODAS – Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
Rhonestr. 2
50765 Köln
Telefon (0221) 709 12 - 0
Fax (0221) 709 12 - 86
vertrieb@infodas.de
www.infodas.de