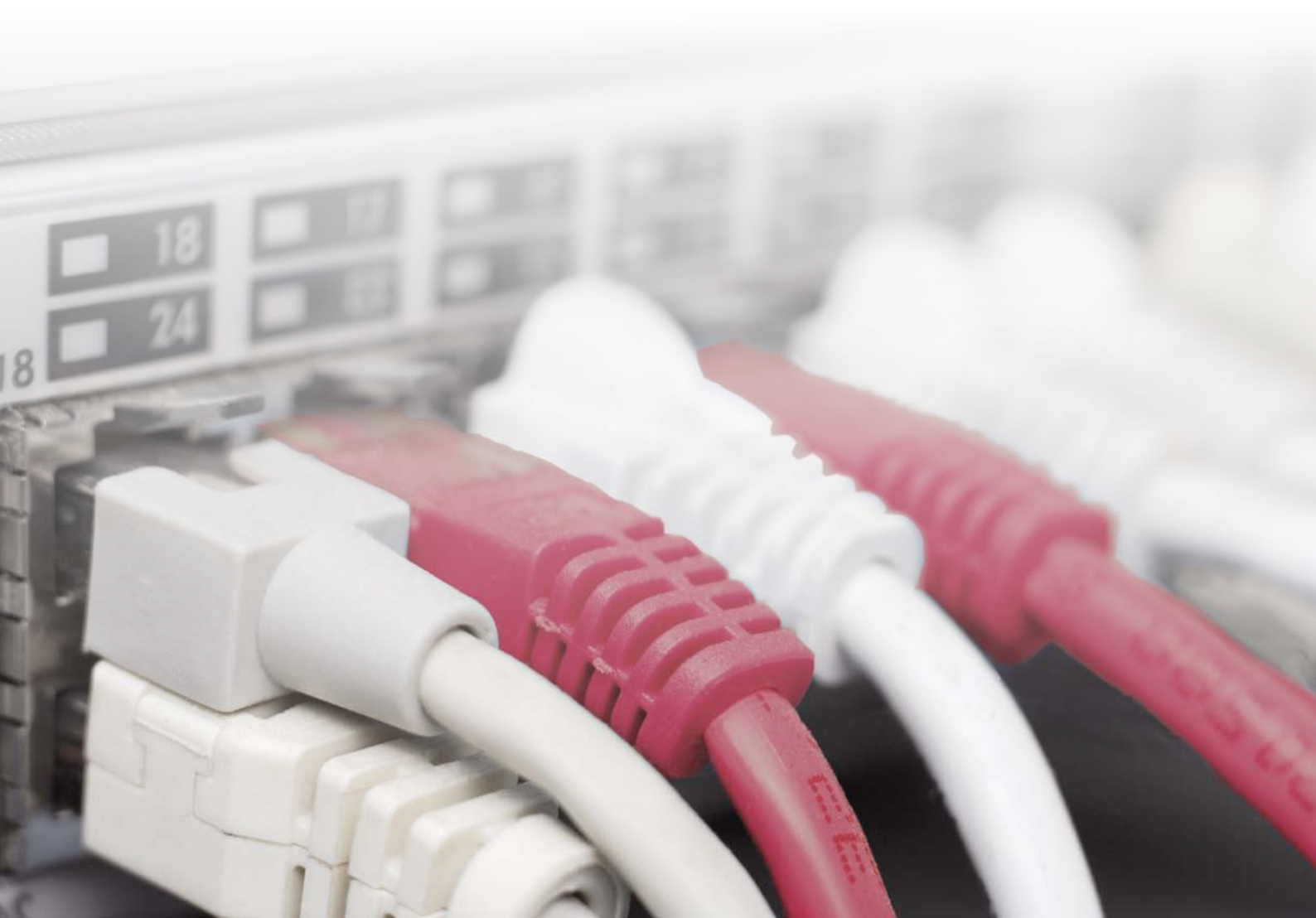


Der richtige Riecher

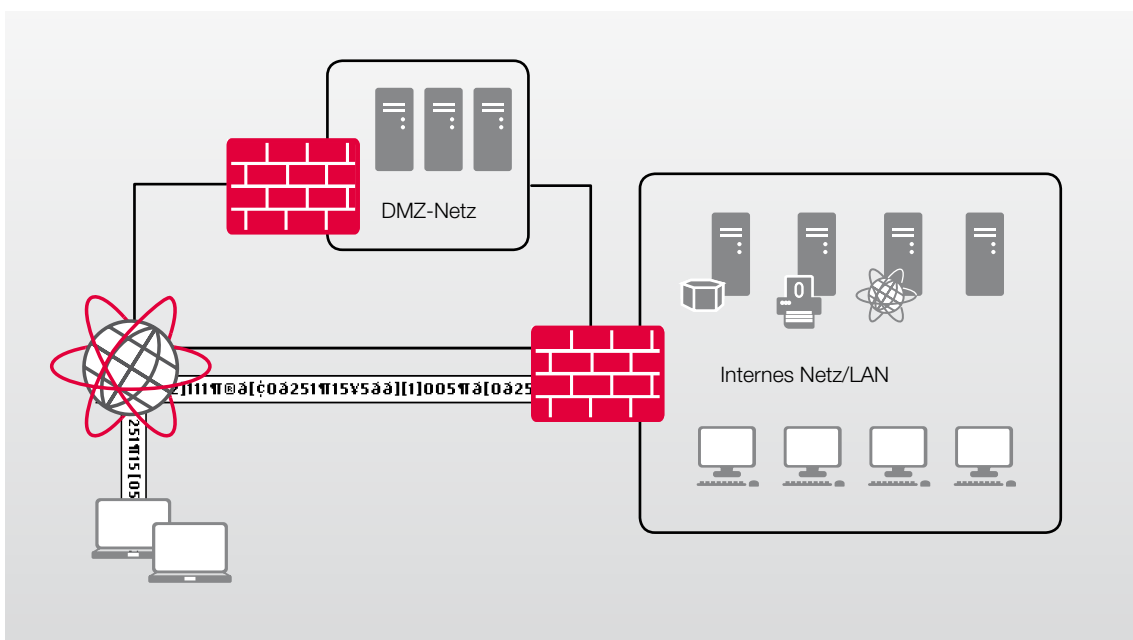
Sicherheit im Netz mit Intrusion Detection
und Intrusion Prevention



Ein beliebtes Ziel für Angriffe: Unternehmens- und Behördennetzwerke

Globale Kommunikation, mobile Arbeitsplätze und IT-gestützte Geschäftsprozesse gehören in den meisten Organisationen von heute zum Standard. Ein störungsfreier und reibungsloser Betrieb der IT-Infrastruktur ist damit mehr denn je ein wichtiger Erfolgsfaktor. Andererseits ist die Bedrohungslage für die global vernetzte Gemeinschaft vielfältiger und professioneller geworden. Erfolgreiche Angriffe vermindern die Produktivität, verletzen Betriebsgeheimnisse und gefährden so letztlich die Substanz von Organisationen. Investitionen in IT-Sicherheit sind deshalb eine notwendige Voraussetzung für den Erhalt von Image, Marktposition und Wettbewerbsfähigkeit. Der Beitrag von secunet sind modernste Lösungen, die bewährt, vertrauenswürdig und zugleich offen für zukünftige Anforderungen sind.

Zur Absicherung von Netzwerken sind Firewalls und Virens Scanner heute zwar eine gute Basis, für den zuverlässigen Schutz von komplexen Unternehmensnetzwerken reichen sie allein aber bei Weitem nicht aus. Um über alle im Netzwerk ablaufenden Vorgänge den Überblick zu behalten und Angriffe zu vereiteln bzw. zu analysieren, sind Intrusion Detection Systeme (IDS) eine unverzichtbare Erweiterung der IT-Sicherheitsinfrastruktur. Eine der wohl bekanntesten IDS-Anwendungen ist das Open-Source-Tool Snort, welches sich als de facto Standard im Markt etabliert hat.



Typische Segmente in einem Netzwerk

secunet snort schützt moderne Unternehmens- und Behördennetzwerke zuverlässig vor Cyber-Attacken und internen Angriffen

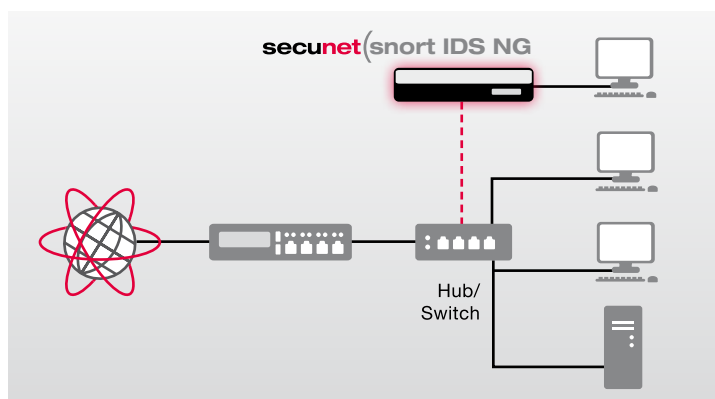
Besonders für komplexe IT-Infrastrukturen und solche mit besonderen Sicherheitsanforderungen ist eine umfassende Cyber Security-Strategie mit einer flexiblen und gleichzeitig zuverlässigen Angriffserkennung unverzichtbar. Genau das bietet secunet snort, eine bewährte wie technisch ausgereifte und skalierbare Lösung zur Erkennung und Abwehr von Netzwerkangriffen. Mit secunet snort minimieren Sie deutlich das Risiko von Angriffen und verbessern gleichzeitig die Sicherheit Ihrer Organisation.

Sie können secunet snort wahlweise als Intrusion Prevention System (IPS) oder als Intrusion Detection System einsetzen (IDS). Beide Produktvarianten – secunet snort IDS NG und secunet snort IPS NG – haben durch ihre technologische Entstehung viele Gemeinsamkeiten in den grundlegenden Funktionen. Viele der nachfolgend beschriebenen Features sind in beiden Produktvarianten zu finden.

secunet snort IDS NG: Intrusion Detection Systeme

Sensible Infrastrukturen mit hohen Sicherheitsanforderungen benötigen eine zuverlässige Angriffserkennung, die weder die Verfügbarkeit noch die Performance beeinträchtigt. Hier sind die secunet snort-Systeme erste Wahl. Unmerklich, im „Sniffing-Modus“, liest das System alle am Sensor vorbeifließenden Daten mit.

Das secunet snort IDS NG-System erkennt auch Angriffe in internen Netzwerksegmenten und ist Spezialist für High Performance-Angriffserkennung.

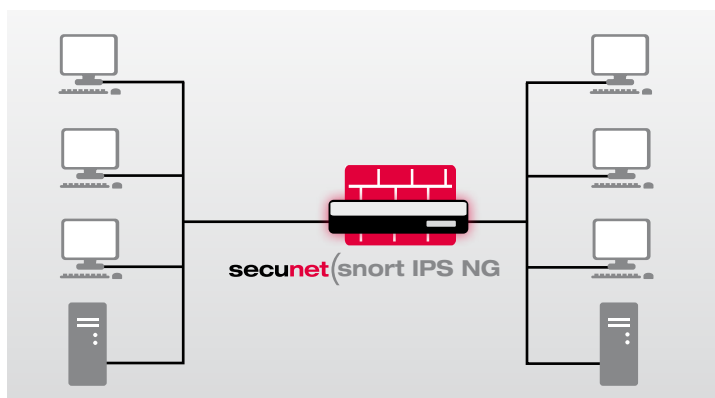


Intrusion Detection System im Sniffing-Modus: Überwachung des gesamten Netz-Datenverkehrs ohne Performance-Verluste oder Reduktion der Verfügbarkeit

secunet snort IPS NG: Intrusion Prevention Systeme

secunet snort IPS NG eignet sich speziell für die Überwachung von Netzwerkübergängen und wird im Bridging Mode auf Layer 2 installiert. So kann das System ohne langwierige und kostenintensive Umstellung der IP-Adressen oder Netzwerk-Topologien einfach und transparent vor den internen Systemen installiert werden.

Werden Angriffe und Bedrohungen auf die zu schützenden Systeme erkannt, können diese automatisch geblockt und aus dem Datenstrom herausgefiltert werden.



Intrusion Prevention System im Inline-Modus: Höchste Sicherheit mit integrierter Firewall- und Blocking-Funktion

secunet snort IDS NG: High Performance Intrusion Detection Systeme

Aktuellen Studien zufolge kommen rund 60-80% aller Angriffe aus dem internen Netzwerk und bleiben deshalb für viele Gateway-Sicherheitsprodukte unsichtbar. Das secunet snort IDS NG erkennt auch diese Angriffe zuverlässig; es kann an zentralen Stellen implementiert werden und damit die gesamte interne Daten-Kommunikation überprüfen. Unsichtbar im Sniffing-Modus eingesetzt, wird der Datenstrom durch secunet snort nicht beeinflusst – das garantiert höchste Verfügbarkeit.

Keine andere Technologie ermöglicht die Echtzeit-Überwachung und Angriffserkennung der Kommunikation in kompletten Netzwerksegmenten – speziell hierfür ist secunet snort konzipiert. Durch die bewährte Scan- und Detection-Technologie sowie die Sensor-/Manager-Architektur liefert secunet snort IDS NG ein Höchstmaß an Performance und Skalierbarkeit.

» **secunet snort ist als modulares System vielseitig einsetzbar. Die bewährte Scan- und Detection-Technologie sowie die Sensor-/Manager-Architektur liefern ein Höchstmaß an Performance und Skalierbarkeit.**

Die intelligente Korrelation zwischen gefundenen Angriffen und den Systemattributen der Netzwerkobjekte ermittelt in Echtzeit, welche Angriffe tatsächlich relevant und gefährlich für das Netzwerk sind. In der Datenausgabe werden alle Störfälle angezeigt und in übersichtlichen Reports ausgegeben. Dies hilft dem Administrator, wichtige Informationen von unwichtigen zu trennen, und schafft damit mehr Sicherheit bei geringem Administrationsaufwand.

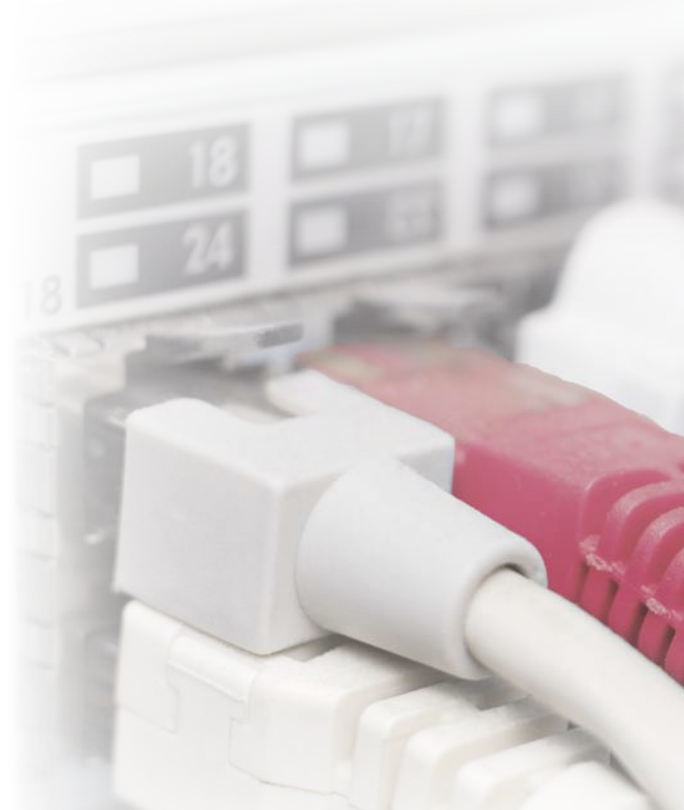
Sichere Überwachung, sicheres Management

secunet snort IDS NG kann standardmäßig mit mehreren Interfaces gleichzeitig sniffen, also mehrere Netzwerksegmente parallel überwachen. Die Sniffing-Interfaces besitzen keine eigene IP-Konfiguration und sind daher nicht angreifbar.

Das Management Interface kann problemlos in einem z.B. durch eine Firewall geschützten Segment platziert werden. Der Management-Zugriff kann auf bestimmte IP-Adressen beschränkt werden. Die Kommunikation zwischen Browser und Manager sowie zwischen Manager und Sensor ist durchgängig verschlüsselt.

Intrusion Prevention im Sniffing Modus

Wird die Intrusion Prevention Engine aktiviert, kann secunet snort IDS NG auf Angriffe reagieren und sie mittels TCP Reset oder Firewall Hardening verhindern.



secunet snort IPS NG: High Performance Intrusion Prevention Systeme

Reine Firewall-Systeme ohne ein integriertes IPS werden den aktuellen Anforderungen an Netzwerksicherheit nicht mehr gerecht: Zu vielfältig und intelligent sind heute Würmer, Trojaner, Hacker und Co. Besser, Sie setzen auf die Strategie von secunet snort: Statt Kommunikationsmöglichkeiten abzuschalten oder einzuschränken, werden sämtliche IP-Pakete eingehend untersucht. Kern des IPS-Systems ist die Intrusion Prevention Engine. Als die der Firewall nachgeschaltete Kontrollinstanz bestimmt sie, ob Datenpakete passieren dürfen oder aussortiert werden. Angriffspakete werden direkt am Gateway abgeblockt, bevor sie in das Netzwerk eindringen können.

Das Intrusion Prevention System secunet snort IPS NG wird im Bridging-Modus auf Layer 2 betrieben. Obwohl es damit „unsichtbar“ direkt in der Kommunikation sitzt, sind Firewall und Intrusion Prevention Engine stets aktiv. So kann secunet snort IPS NG auch vor WLAN-Hotspots, Serverfarmen oder einzelnen Servern eingesetzt werden – an der Netzwerkkonfiguration muss nichts geändert werden. DHCP, BootP, NT-Domain-Anmeldungen oder andere Broadcast-Kommunikation laufen weiter, ohne dass ein Administrator eingreifen muss.

Layer2/Layer3 Firewall

secunet snort IPS NG hat eine Layer 2/Layer 3 Firewall integriert. Sie ist die erste „Kontrollstation“ und untersucht in Echtzeit detailliert alle Datenpakete zwischen den Netzwerksegmenten. Nur der tatsächlich erwünschte und regelkonforme Datenverkehr wird ungehindert zugelassen. Die Regeln der Firewall lassen sich bequem und einfach konfigurieren.

Intrusion Prevention

Die Intrusion Prevention Engine verfügt über mehr als 6000 Regeln und Signaturen zur Erkennung von Angriffen. Das System greift aktiv in den Datenverkehr ein und blockt Angriffe, bevor sie in das Netzwerk eindringen können.

» **Das automatische Regel-Update von secunet snort schützt Sie schneller gegen neue Angriffe als andere Systeme.**

Auto Prevention-Funktion

Die Auto Prevention-Funktion vereinfacht die Konfiguration und erlaubt eine schnelle Klassifizierung der Regeln oder Regelgruppen an die individuellen Sicherheitsanforderungen für Ihr System. Diese Funktion gibt es nur bei den secunet snort NG-Systemen. Mit dem automatischen Regel-Update sind Sie schneller gegen neue Angriffe geschützt als mit anderen Systemen.

secunet snort next Generation: Analyse- und Report-Funktionen

Event-Korrelation reduziert die Gefahr von Fehlalarm

Über die Event-Korrelation überprüfen die secunet snort NG-Systeme bei entdeckten Angriffen, ob diese auf dem Zielsystem tatsächlich ausgeführt werden könnten. Dies wird anhand des integrierten Regelwerks und den definierten Systemattributen entschieden. Jede Übereinstimmung erhöht die Wahrscheinlichkeit, dass es sich um einen gefährlichen Angriff handelt. Bei der Ausgabe können die Angriffe mit niedriger Gefährdungswahrscheinlichkeit herausgefiltert und Fehlalarm so vermieden werden. Die Ergänzung eigener Systemattribute ist problemlos möglich. Administratoren können ebenso individuelle Korrelationen zwischen Regeln und Attributen bilden und festlegen, um welchen Grad sich die Wahrscheinlichkeit der Gefährdung dadurch erhöht oder verringert.

secunet snort kann Events in Echtzeit mit anderen Informationen korrelieren und unterstützt die Übernahme von externen Korrelationsdaten. Die von den secunet snort NG-Systemen erkannten Events können an externe Auswertungssysteme übergeben werden.

Individuelle Signaturen, einfach erstellt

Die secunet snort NG-Systeme bieten die Möglichkeit, einfach und schnell eigene Signaturen über die Managementoberfläche zu erstellen. Die Regeln können

auch in Kombination z. B. nach Source- oder Destination-Adresse, Ports, Pakettyp, Paketgröße oder Inhalt und Häufigkeit des Auftretens innerhalb einer definierten Zeitspanne erstellt werden. Mit secunet snort können Sie somit individuelle Verbindungen festlegen, die zum Alarm führen.

Anomalie-Erkennung als zusätzliche Warnfunktion

Angriffe haben in der Regel spürbare Auswirkungen auf den Datenverkehr: Ein abrupter Anstieg der Datenmenge oder aber das völlige Erliegen eines Internetdienstes können auf einen Angriff hindeuten. Mittels der Anomalie-Erkennung zeigen die secunet snort NG-Systeme Abweichungen von der definierten Regel an und melden diese. Welche Datenmenge „normal“ ist, lernt das System selbstständig. Alternativ kann dieser Wert auch manuell vom Administrator eingestellt werden.

Anomalien können für Netze, einzelne Maschinen und sogar einzelne Ports auf Maschinen definiert werden. Eine Meldung erfolgt, wenn über eine definierte Zeitdauer eine bestimmte prozentuale Über- oder Unterschreitung eines üblichen Wertes festgestellt wird.

» Mit secunet snort können Sie individuelle Verbindungen festlegen, die zum Alarm führen.

Optimales Monitoring, forensische Analyse und Auto Reporting

Die secunet snort NG-Systeme erlauben eine übersichtliche und dennoch detaillierte forensische Analyse aller Angriffe auf das Netzwerk. In der Datenausgabe werden alle Störfälle angezeigt und direkt verschiedenen Kategorien zugeordnet (High, Medium, Low, Info). secunet snort stellt Angriffe gebündelt nach Angriffsziel und Angreifer dar, und verschafft so einen optimalen Überblick über attackierte Systeme. Sämtliche Daten, die für eine Analyse typischerweise benötigt werden, lassen sich schnell und flexibel aus dem System exportieren. Über die Auto-Report-Funktion werden die wichtigsten Angriffe und Regelverstöße in frei konfigurierbaren Reports übersichtlich zusammengefasst – Auswertungen können täglich, wöchentlich oder monatlich erfolgen. Auch die Ausgabediagramme und -tabellen können nach individuellen Wünschen zusammengestellt werden.

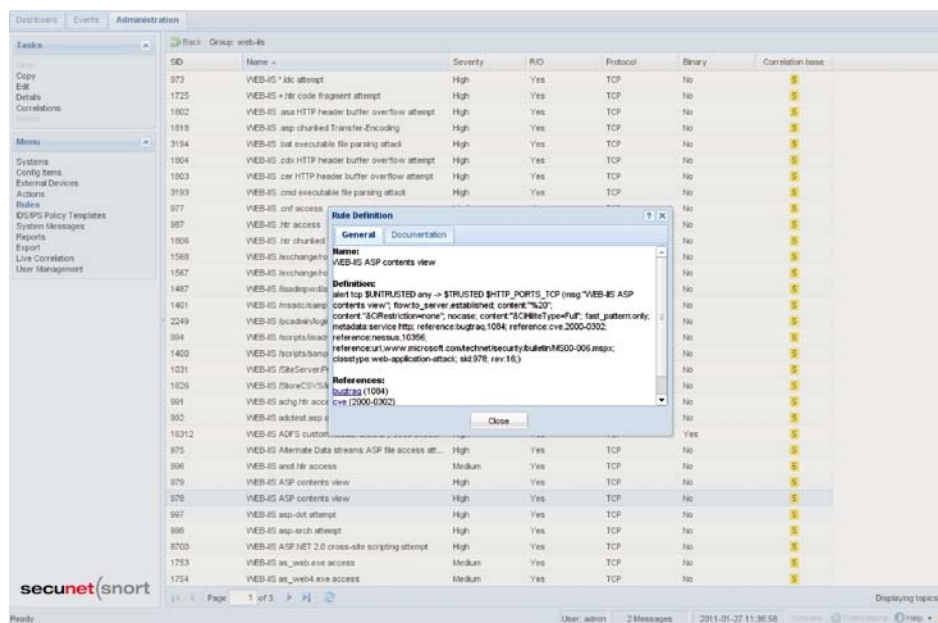
Automatisches Software-Update

Durch das automatische Software- und Pattern-Update sind die secunet snort NG-Systeme stets auf dem aktuellsten Stand.

SNMP-Schnittstelle

Die secunet snort NG-Systeme verfügen über eine integrierte SNMP-Schnittstelle, mit der Daten von allen Systemen abgerufen werden können. Informationen über CPU-Auslastung und Festplattenkapazität beispielsweise sind damit auf Knopfdruck verfügbar.

» Auswertungen können mit secunet snort täglich, wöchentlich oder monatlich erfolgen. Management, IT-Leiter und Administratoren können sich in übersichtlichen Reports jeweils genau die Daten anzeigen lassen, die für sie von Bedeutung sind.



secunet snort NG Grafische Benutzeroberfläche

Die neue grafische Benutzeroberfläche der Next Generation-Systeme: Administration intuitiv, anwenderfreundlich, flexibel

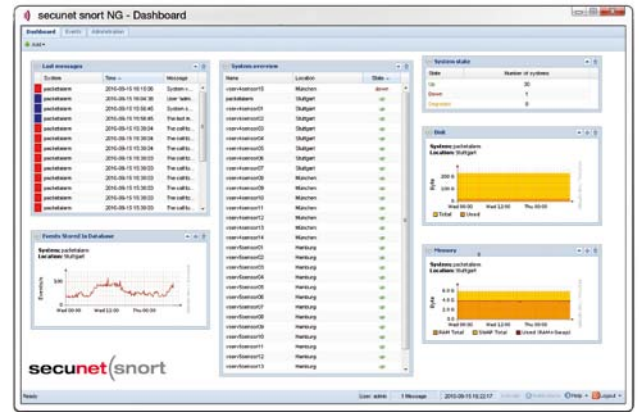
Die neue Generation der secunet snort-Systeme hat eine deutlich verbesserte Administrationsoberfläche (GUI), die sich durch intuitive Bedienung und Übersichtlichkeit bis ins letzte Detail auszeichnet. Dies ist insbesondere für den Betrieb in großen Netzwerken mit vielen IDS- bzw. IPS-Sensoren und Managern von großem Vorteil.

Das neue Dashboard erlaubt eine individuelle Gestaltung, damit die jeweils wichtigsten Informationen individuell auf einen Blick verfügbar sind.

Die Teamorientierung des Bedienerkonzeptes hilft Ihnen bei der Administration großer Netzwerke. Ein granulares Rollenkonzept für die Benutzerrechte ist darin ebenso verwirklicht wie ein „Read Only“-Modus, der Konflikte, die durch eine doppelte Administration entstehen können, vermeidet. Selbst für einzelne Benutzergruppen können Rechte auf Aktionsebene definiert werden.

Selbstüberwachung für optimale Einsatzsicherheit

Alle Appliances der secunet snort Next Generation sind mit einer Hardware-Überwachungsfunktion ausgestattet, damit Sie jederzeit über Verfügbarkeit und Zustand Ihrer IDS/IPS-Installation bestens informiert sind.



» Die Teamorientierung des Bedienerkonzeptes von secunet snort unterstützt Sie optimal bei der Administration großer Netzwerke.

Administration und Management in komplexen Netzwerken

Zentrales Management durch Sensor-Manager-Betrieb

Angriffe können in verteilten Unternehmensnetzwerken oder landesweiten Behörden- und Regierungsnetzwerken an verschiedenen Stellen ansetzen. Für eine zuverlässige Angriffserkennung und -abwehr müssen in solchen Netzwerkstrukturen demzufolge viele Sensoren großflächig verteilt werden. Das ist kein Problem mit den secunet snort NG-Systemen:

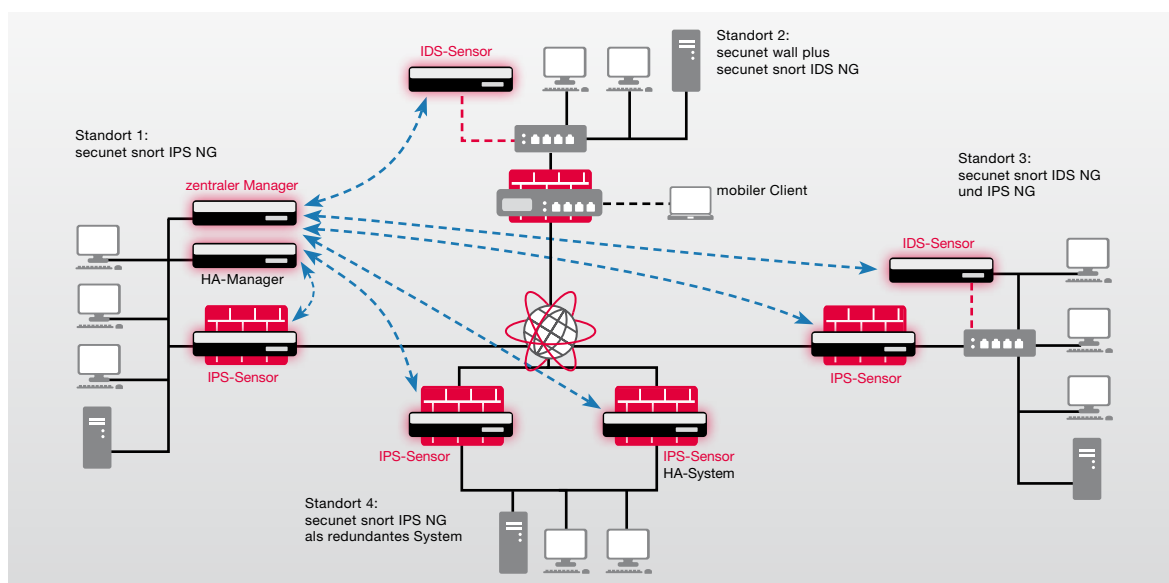
Sie lassen sich in beliebiger Anzahl als verteiltes System betreiben; einzelne Sensoren werden dazu über die gesamte IT-Infrastruktur verteilt und über einem Manager zentral konfiguriert, administriert und überwacht. Die Sensoren können auch dann, wenn sie dezentral positioniert sind, über das Internet oder Virtual Private Networks mit dem zentralen Manager kommunizieren. Die Kommunikation der secunet snort-Systeme untereinander erfolgt über ein verschlüsseltes Protokoll auf TLS-Basis. Für die Kommunikation mit externen Systemen stehen verschlüsselte Protokolle wie HTTPS, SMTP via TLS, SNMP v.3 und SCP zur Verfügung.

Administration von Sensoren – neue Features bei secunet snort NG

Alle Einstellungen zum Scannen von Netzwerkpaketen und zur Erkennung von Angriffen werden auf dem neuen secunet snort NG-Manager über ein webbasiertes User Interface vorgenommen.

Neben den umfassenden Konfigurations- und Auto-Reporting-Funktionen haben Administratoren zudem ein einfach zu handhabendes und anwenderfreundliches Updateverfahren zur Hand. Dies erlaubt beispielsweise, mehrere Updates automatisiert einzuspielen oder beim Betrieb mehrerer Sensoren ein Update auch auf einzelnen, dedizierten Sensor-Systemen durchzuführen. Auch die Software-Distribution ist beim secunet snort NG-Manager besonders einfach. Software-Updates werden auf dem Manager bereitgestellt und damit von zentraler Stelle auf die Sensoren verteilt und installiert. Die Möglichkeit, Updates parallel auszuführen, reduziert Aktionszeiten.

Für die Administration vieler Sensoren können gleichartige Signaturen und Regeln in Templates zusammengefasst werden. Eine Distribution dieser Templates für IDS-/IPS-Policies kann wiederum auf die jeweiligen Sensoren übertragen werden.



secunet snort: Netzwerksicherheit für Netze jeder Art und Größe

secunet snort NG-Appliances

secunet snort NG: optimiert auf Einsatzzweck und Geschwindigkeit

In die neue Generation der secunet snort NG-Systeme haben wir unsere Erfahrungen aus vielen Jahren Produktentwicklung für die Absicherung von mittleren bis großen IT-Infrastrukturen eingebracht:

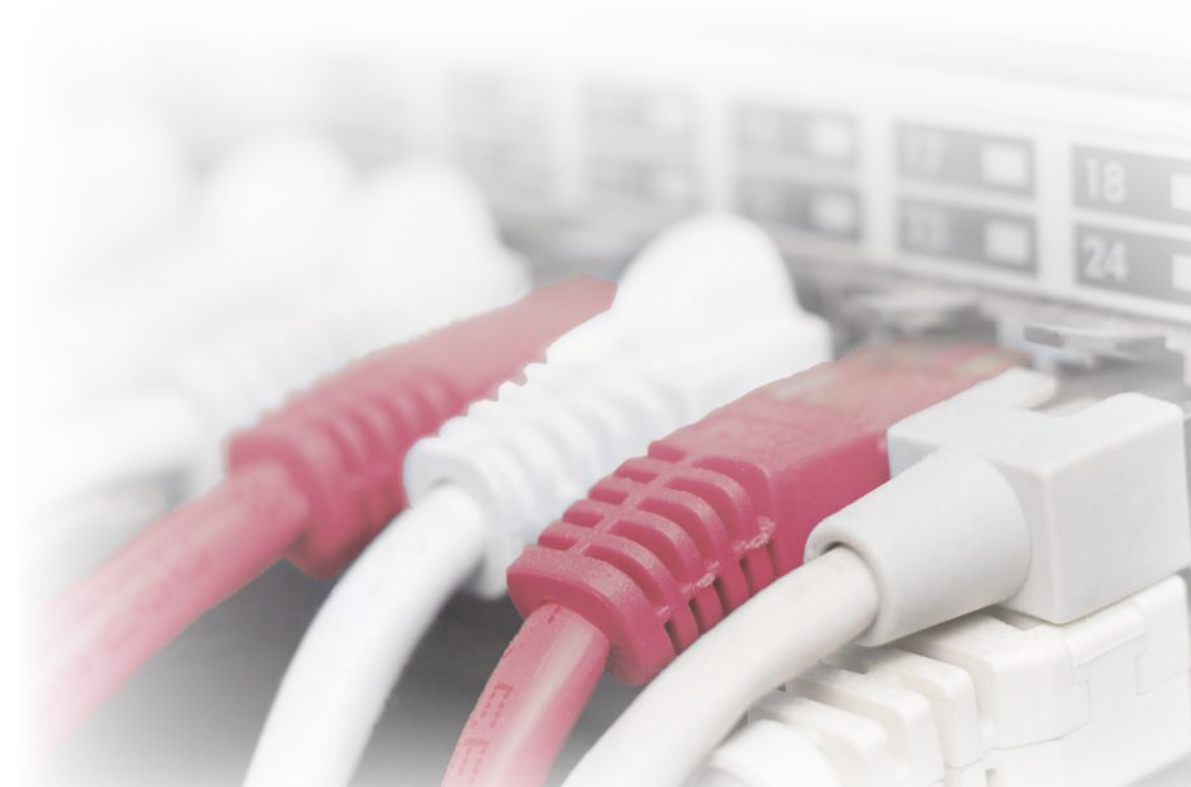
- Alle Produkte sind noch besser auf die Bedürfnisse der jeweiligen Einsatzumgebung abgestimmt und können optimal skaliert werden.
- Die secunet snort NG-Sensoren und Sensor/Manager wurden für die schnelle Verarbeitung von hohen Datenaufkommen entwickelt.
- Die secunet snort NG-Manager sind speziell auf die Speicherung vieler Events und einer schnellen Verarbeitung der anfallenden Daten ausgelegt.
- Die Betriebssoftware der gesamten Appliance-Modellreihe beinhaltet eine Fehlerdiagnose für alle Hardware-Komponenten.
- Die Appliances der Modellreihe 500 NG und höher sind mit RAID sowie redundant ausgelegten Lüftern und Festplatten ausgestattet.

High Speed-Sensoren

Für den Einsatz in großen Netzwerken mit entsprechend hohem Datenaufkommen sind die secunet snort IDS 1000 NGx-Sensoren gedacht. Die speziell entwickelte secunet snort NG-Stream Distribution Technology garantiert die zuverlässige Verarbeitung höchster Datenmengen. Durch parallele Nutzung mehrerer „IDS-Kerne“ kann die Verarbeitung und Analyse der Daten nochmals beschleunigt werden.

High Availability

Alle Sensoren, Sensor/Manager und Manager der secunet snort Next Generation verfügen über High Availability-Funktionalitäten und können redundant ausgelegt werden. Das HA-Feature hält dafür ein paralleles, redundantes System bereit, das im Falle einer Störung automatisch und unverzüglich sämtliche Aufgaben des Hauptsystems übernimmt. Die redundante Auslegung ist auch bei einer räumlichen Trennung zum Hauptsystem möglich.



secunet snort Modellübersicht

Modell		Empfohlene Bandbreite und Hardware-Redundanz	RAID integr.	Sensor	Sensor/Manager	Manager	IDS	IPS
200 NG		Bis zu 200 MBit/s* Speicherung bis 55 Mio. Events**	—	■	■	—	■	■
500 NG		Bis zu 500 MBit/s* Speicherung bis 55 Mio. Events** Redundante Lüfter und HDD	■	■	■	—	■	■
1000 NGx		Bis zu 2.000 MBit/s* Speicherung bis 55 Mio. Events** Redundante Lüfter und HDD Konsequente Auslegung auf die Verarbeitung extrem großer Datenmengen durch die gleichzeitige Nutzung mehrerer IDS-Kerne	■	■	■	—	■	—
Manager								
Manager NG		Speicherung bis 55 Mio. Events** Redundante Lüfter und HDD	■	—	—	■	■	■
Ultra Manager NG		Speicherung bis 195 Mio. Events** Redundante Lüfter und HDD, Hot Spare HDD Konsequente Auslegung zur Speicherung großer Datenmengen und Management großer Netzwerke	■	—	—	■	■	■

*) Die Leistung kann in Abhängigkeit von der Konfiguration variieren

**) Die tatsächliche Anzahl gespeicherter Events kann in Abhängigkeit von der Konfiguration variieren

secunet snort Leistungsmerkmale

	IDS NG	IPS NG
Integration		
Layer 2 (Bridging Mode)	—	■
Passiv (Sniffing Mode)	■	—
Dynamic Intrusion Detection und Intrusion Prevention		
IDS-/IPS-Signaturen	> 6000	> 6000
Individuelle Signaturen	■	■
Korrelation	■	■
Auto Prevention	■	■
Forensische Analyse	■	■
Anomalie-Erkennung	■	■
Traffic Trace	■	■
Port Scans	■	■
DoS	■	■
Buffer Overflow	■	■
Packet Fragmentation-Angriff	■	■
UDP-Angriff	■	■
Application Anomaly-Angriff	■	■
Application Protocol-Analyse	■	■
RFC Compliance-Prüfung	■	■

	IDS NG	IPS NG
System Management		
Sensor-Management	■	■
Anzahl Sensoren	unlimitiert	unlimitiert
Monitoring via SNMP	■	■
Hardware-Diagnostik via SNMP (v1, v2, v3)	■	■
High Availability	■	■
Logging		
Interne Festplatte	■	■
Log an entferntem Syslog-Server	■	■
Log an SNMP-Server	■	■
E-Mail-Aussendung bei Angriffen	■	■
Administration		
Auto-Reporting	■	■
Automatisches Echtzeit-Update	■	■
Konsolen-Interface	■	■
Web-GUI (HTTPS)	■	■
Firewall-Modi und -Features		
Layer 2/Layer 3 Firewall	—	■
NAT, PAT	—	■
Threshold Analyse	■	■
Stateful Pattern Matching	■	■

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

Tel: +49-201-54 54-0

Fax: +49-201-54 54-1000

E-Mail: info@secunet.com

www.secunet.com