Administratorfreundliche Industriefirewall

Dr. Götz Güttich

Industrielle Anlagen sind heutzutage viel größeren Risiken ausgesetzt als früher. In der Vergangenheit war es üblich, dass die Anlagen nicht oder bestenfalls lokal vernetzt waren. Wenn überhaupt kommunizierten sie über industrielle Bus-Technologien und verfügten über keinen Internet-Anschluss. Dies hat sich in den letzten Jahren gewandelt, da sich der TCP/IP-Standard immer mehr auch für die Vernetzung von Industriesystemen und -computern durchgesetzt hat. Abgesehen davon wurden aus den verschiedensten Gründen immer mehr Anlagen an das Internet angeschlossen. Aufgrund dieser Entwicklung gewinnt die Frage nach der Absicherung dieser Netzwerkverbindungen zunehmend an Bedeutung. Oft müssen sich die IT-Administratoren der Unternehmen jetzt auch um diesen Aufgabenbereich kümmern, deswegen werden viele froh sein, wenn sie für den Industriebereich eine Lösung einsetzen können, die sie aus der Absicherung ihrer IT-Netze bereits kennen. Stormshields SNi40 ist ein solches Produkt.

Industriesysteme sind heute nicht nur Angriffen von außen, sondern auch schädlichen Aktionen von innen ausgesetzt. Werden sie kompromittiert, führt das zu kritischen Situationen, die im Zweifelsfall sogar Produktionsausfälle mit sich bringen. Deswegen benötigen die Administratoren im industriellen Umfeld eine Appliance, mit der sie ihre industriellen Aktivitäten absichern können.

Eine "normale" Next-Generation-Firewall reicht hier nicht aus, da die Sicherheitslösung sämtliche im Industriebereich verwendeten Protokolle verstehen muss, nicht nur den klassischen IT-Netzwerkverkehr. Gleichzeitig sollte sie den IT-Sicherheitsprodukten aber vom Look-and-Feel des Konfigurationsinterfaces möglichst ähnlich sein, damit jeder Administrator ohne zusätzliche Schulung dazu in der Lage ist, mit seinem Produkt zu arbeiten.

Stormshield bietet für die genannte Problematik eine Lösung an. Das Unternehmen liefert nicht nur Firewall-Produkte für den IT-Bereich, sondern hat nun mit der SNi40 auch eine Industriefirewall im Angebot, die in einem Industriehardwareformat kommt und neben den IT-Protokollen auch viele Industrieprotokolle unterstützt.

Mit der SNi40 sind die zuständigen Mitarbeiter folglich unter anderem dazu in der Lage, Programmable Logic Controller (PLCs) zu schützen. Das Managementwerkzeug ist bei allen Firewall-Lösungen identisch, so dass sie sich alle auf die gleiche Art verwalten lassen. Damit eignen sich die Produkte nicht nur für die Verwaltung durch die eigene IT-Abteilung, sondern auch durch externe Dienstleister. Umfangreiche Überwachungswerkzeuge zeigen die Vorgänge im

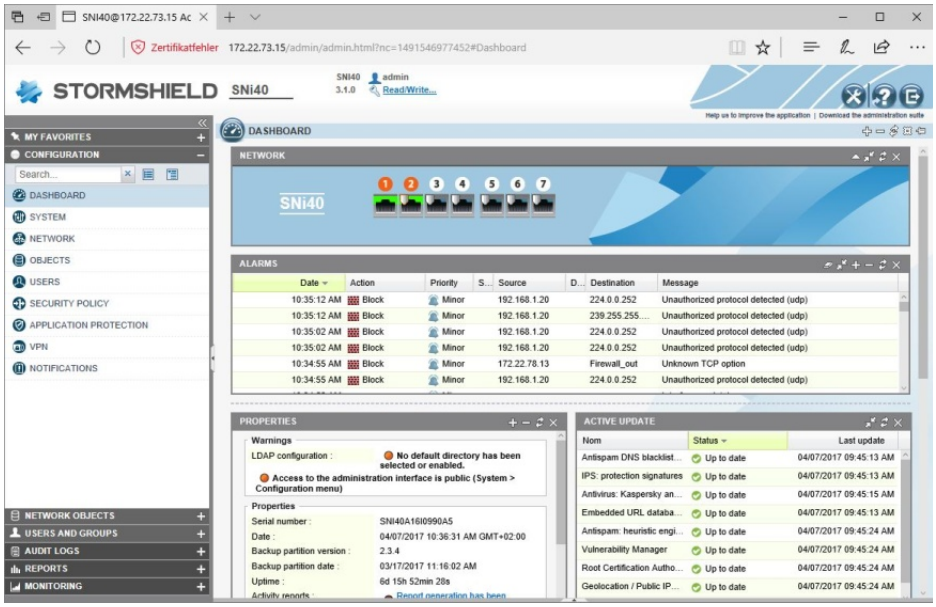
Netz in Echtzeit und machen die Verwaltung der gesamten Umgebung einfach.

Die Hardware

Was die SNi40-Hardware angeht, so wurde die Firewall speziell

entwickelt, um den schwierigen Bedingungen in industriellen Umgebungen standhalten zu können. Sie ist stoßsicher, lässt sich durch elektromagnetische Interferenzen nicht aus der Ruhe bringen, das Gehäuse hält Staub von der Elektronik fern (hierfür wurde das Produkt IP30 zertifiziert) und die Lösung verkraftet extreme Temperaturen von minus 40 bis plus 75 Grad Celsius sowie eine relative, nicht kondensierte Luftfeuchtigkeit von fünf bis 95 Prozent. Außerdem hat der Hersteller einen Hardware-Bypass zwischen den Ports eins und zwei implementiert. Insgesamt 18 verschiedene Überwachungsmethoden kommen zum Einsatz, um den Zustand der Firewall im Auge zu behalten. Melden diese ein Problem, so wird bei Bedarf über ein Relais eine physikalische Verbindung zwischen den beiden genannten Ports hergestellt, so dass der Datenverkehr weiterlaufen kann. In diesem Fall findet zwar keine Sicherheitsüberprüfung mehr statt, es wird aber garantiert, dass das Netz bei einem Firewall-Ausfall nicht zum Erliegen kommt, was insbesondere in Produktionsumgebungen von großer Bedeutung sein kann. Im Test ergaben sich bei der Verwendung des Hardware-Bypass keine Schwierigkeiten.

Abgesehen davon bringt die Hardware noch weitere Besonderheiten mit sich. Das Produkt verfügt über zwei Glasfaseranschlüsse und erlaubt an seinen USB-Ports den Einsatz generischer LTE-Modems. Es lassen sich also auch drahtlose Netzwerkverbindungen herstellen.



Das Dashboard warnt die Administratoren vor potentiellen Konfigurationsfehlern, wie hier einem über den externen Netzwerkanschluss erreichbaren Konfigurationswerkzeug

Als Datenspeicher wurde eine 32 GByte große SSD implementiert, so dass genug Speicherplatz zur Verfügung steht, um lokal Logs aufzuzeichnen, was sehr sinnvoll ist, da in Industrieumgebungen oft kein Syslog-Server oder ähnliches zur Verfügung steht. Ein redundantes Netzteil schließt den Lieferumfang der Lösung ab.

Der Test

Im Test integrierten wir die SNi40-Appliance, die uns Stormshield zu diesem Zweck zur Verfügung gestellt hatte, in unser Netzwerk, brachten sie auf den neuesten Stand – zum Testzeitpunkt war die Version 3.1 aktuell – und konfigurierten sie entsprechend unserer Anforderungen. Dabei machten wir uns auch gleich mit dem Leistungsumfang sowie den Analyse- und Alert-Funktionen der Lösung vertraut. Anschließend ließen wir sie ein paar Wochen lang laufen und wickelten normalen Datenverkehr darüber ab.

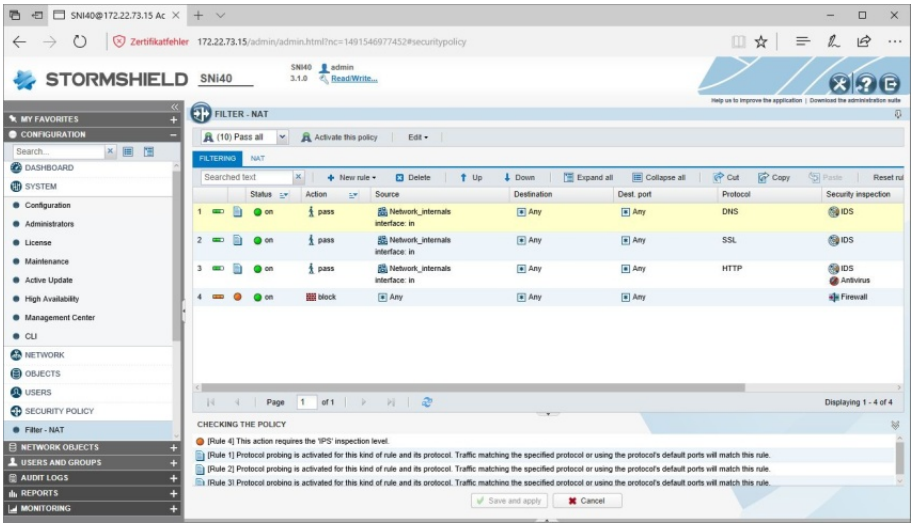
Zum Schluss nahmen wir die internen und externen Interfaces der SNi40 mit diversen Sicherheitsprodukten wie Nmap, Nessus und Metasploit unter die Lupe und führten zudem mehrere Angriffe auf die genannten Netzwerkanschlüsse aus, beispielsweise DoS-Attacken. Dabei analysierten wir, ob sich die Appliance aus dem Tritt bringen ließ und ob sie irgendwelche überflüssigen Informationen, die einem Angreifer helfen könnten, im Netz bereitstellte.

Installation

Um die SNi40 in unser Netz zu integrieren, schlossen wir sie zunächst an einen Netzwerk-Switch an und fuhren sie hoch. Danach verbanden wir uns von einem Client aus mit dem Web-Interface der Appliance, das über den internen Netzwerkanschluss unter der Adresse https:// 10.0.0.254 / admin erreichbar war. Hier nahmen wir die Erstkonfiguration vor, die im Wesentlichen darin bestand, die Netzwerkkonfiguration an unsere Gegebenheiten anzupassen.

Konkret konfigurierten wir das externe Interface als DHCP-Client, da dieses später über den Router, der unseren Internetzu-

gang übernahm, mit einer IP-Adresse versorgt werden sollte. Außerdem richteten wir eine feste, private IP-Adresse für das interne Interface ein und aktivierten den DHCP-Server, damit die Clients im LAN später ihre IP-Adressen von der SNi40 beziehen konnten.



Die Regeldefinition der Stormshield-Lösung

Nachdem das erledigt war, schlossen wir die Appliance zwischen unserem LAN-Switch und dem Internet-Router ans Netz an und fuhren sie hoch. Danach griffen wir wieder auf das Konfigurations-Tool der Lösung zu und erlaubten zunächst einmal testweise sämtlichen Datenverkehr. Dann aktivierten wir die Lizenz und spielten die aktualisierte Firmware mit der Version 3.1 ein, die uns der Hersteller ebenfalls für den Test zur Verfügung gestellt hatte.

Zum Schluss aktualisierten wir die Daten sämtlicher auf der Firewall vorhandenen Dienste, wie Anti-Virus-Pattern, Anti-Spam, IPS, URL-Blocker und Vulnerability Manager. Sobald das erledigt war, änderten wir noch das Standard-Passwort, blockierten eingehenden Verkehr und gaben ausgehend nur die von uns benötigten Dienste frei. Danach war das Produkt einsatzbereit.

Das Web-Interface

Loggt sich ein Administrator während der Arbeit beim Konfigurationswerkzeug der SNi40 ein, so landet er in einem Dashboard, das ihm eine Übersicht über die Schnittstellen der Appliance, die aktuellen Alarme, die Ressourcenauslastung mit der aktuellen Temperatur und die Systemeigenschaften bietet. Letztere umfassen unter anderem die Seriennummer, das Datum, die Uptime und den VPN-Status.

Außerdem weist das Dashboard auf vorhandene Konfigurationsprobleme hin, beispielsweise wenn das Konfigurationsinterface über die externe Schnittstelle erreichbar ist. Zusätzlich umfasst es auch noch Daten über den Zustand der Active Update-Funktion, die die auf der Firewall vorhandenen Dienste wie Anti-Virus, Anti-Spam und ähnliches auf dem aktuellen Stand hält.

Generell wurde das Konfigurationswerkzeug so gestaltet, dass sich auf der linken Seite eine Menüstruktur findet, über die sich sämtliche Funktionen der Lösung erreichen lassen. Diese wurde in verschiedene Bereiche unterteilt. Der erste befasst sich mit der Konfiguration des Systems und er ist bei weitem am umfangreichsten.

Neben dem Dashboard enthält er Funktionen zum Verwalten der Administratorkonten, zum Managen der Lizenz, zum Einspielen von Updates, zum Sichern und Wiederherstellen der Konfiguration, zum Aktivieren des ebengenannten Active Update, zum Einrichten einer Hochverfügbarkeitskonfiguration und zum Aufrufen einer Kommandozeile über die die Administratoren direkt über ihren Browser CLI-Befehle auf der Appliance ausführen können. Darüber hinaus lassen sich an dieser Stelle auch die Systemzeit, das Datum, die Sprache, die Tastaturbelegung und ähnliches festlegen, ein SSH-Zugriff auf die Lösung einrichten und DNS-Server sowie die IPv6-Konfiguration angeben.

Im Unterpunkt "Netzwerk" konfigurieren die zuständigen Mitarbeiter die vorhandenen Schnittstellen, beispielsweise als Bridge oder internes beziehungsweise externes Interface. Außerdem richten sie virtuelle Schnittstellen für IPSec, GRE und Loopback ein, nehmen die DHCP-Konfiguration vor, verwalten das Routing und aktivieren bei Bedarf einen DNS Cache.

Der Eintrag "Objekte" erlaubt das Management aller im Netz vorkommenden Netzwerkobjekte, wie Hosts, Internet, Protokolle, IP-Adressbereiche, Ports und Zeitobjekte (wie etwa "Arbeitsstunden"). Sie wurden der besseren Übersichtlichkeit wegen in Gruppen zusammengefasst. An

gleicher Stelle finden sich auch Zertifikate (beispielsweise für die SSL-Kommunikation) und Web-Objekte, die dazu dienen, den SSL- und URL-Filterfunktionen mitzuteilen, welche Daten sie nicht untersuchen sollen. Es lassen sich bei Bedarf jederzeit eigene Objekte hinzufügen. Über die Benutzerverwaltung legen die Verantwortlichen Konten an, die definieren, was die User im Unternehmen dürfen und was nicht. Stormshield unterstützt an dieser Stelle nicht nur die Zusammenarbeit mit Active Directory- und LDAP-Servern, sondern auch die Authentifizierung über Radius und Kerberos. Außerdem haben die zuständigen Mitarbeiter Gelegenheit, temporäre Anwenderkonten mit einer vorher definierten Gültigkeitsdauer sowie automatisch erzeugten Passwörtern zu erzeugen und das Captive Portal, über das die Anwender die Internetzugangsbedingungen annehmen und sich anmelden müssen, zu definieren.

In diesem Zusammenhang ergibt es Sinn, noch kurz auf eine weitere Möglichkeit, Benutzern Zugriff auf das Netz zu geben, einzugehen, das so genannte Sponsoring. Wurde das Sponsoring aktiviert, so landen die User, die einen Zugang erhalten möchten, auf einer Seite, auf der sie neben ihren Benutzerdaten auch die E-Mail-Adresse eines "Sponsoren" eingeben müssen. Die Firewall sendet daraufhin eine Mail an diesen Sponsoren – in der Regel einen Unternehmensmitarbeiter – und schaltet den Netzzugang frei, sobald dieser die Anfrage genehmigt hat.

Die Regeln

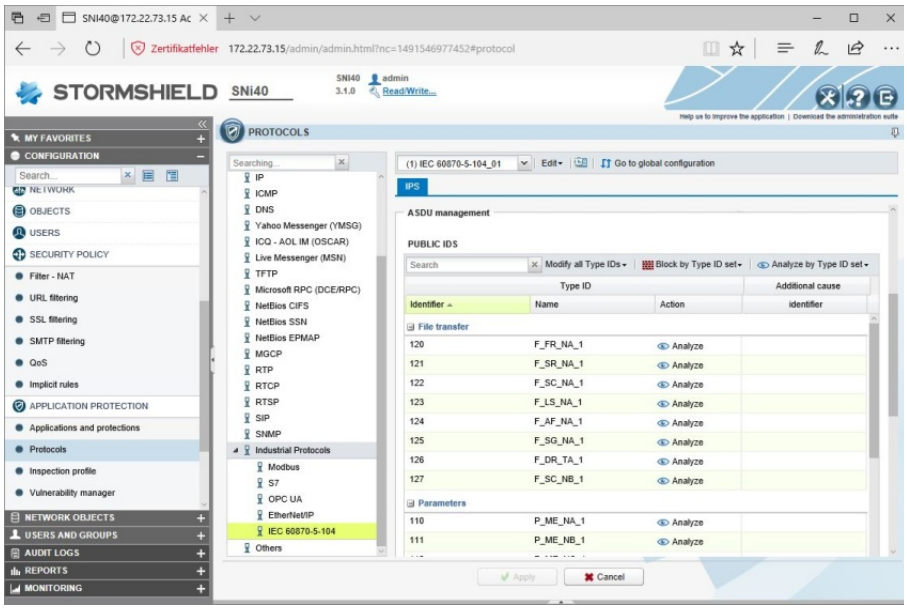
Der Bereich "Sicherheitsrichtlinie" stellt das Herzstück der Lösung dar, da hier die Regeln für den Datenverkehr festgelegt werden. An erster Stelle findet sich hier der Eintrag "Filter/NAT". Die Filterregeln dienen dazu, den Web-Verkehr durchzulassen oder zu blockieren.

Ihre Abarbeitung erfolgt über eine Liste, das heißt, Regeln die sich in der Liste an einer tieferen Position befinden, berücksichtigt das System nur dann, wenn ihre Inhalte nicht bereits durch eine höherplatzierte Policy abgedeckt worden sind. Uns fiel im Test positiv auf, dass das Konfigurationswerkzeug selbstständig auf solche Sachen achtet und den zuständigen Mitarbeiter über Konfigurationsprobleme informiert, beispielsweise durch den Hinweis "Diese Regel wird nicht angewendet, weil sie bereits von der Regel 4 abgedeckt wird."

Wie bei den meisten Firewall-Lösungen üblich, erfolgt die Regeldefinition nach Status (Ein, Aus), Aktion (Blockieren, Durchlassen, Entschlüsseln, Loggen, etc.), Quelle, Ziel, Zielport und Protokoll. Darüber hinaus haben die Verantwortlichen aber auch Gelegenheit, für einzelne Regeln festzulegen, welche Sicherheitsfunktionen aktiviert werden sollen, beispielsweise Antivirus, IPS, Anti-Spam, Sandbox, URL-Filter, HTTP-Caching, SMTP-Filter, FTP-Filter und SSL-Filter. So ist es beispielsweise möglich, HTTP-Übertragungen nur mit aktiviertem Antivirus und IPS zuzulassen.

Die Definition der NAT-Regeln erfolgt ebenfalls mit Quelle, Ziel, Zielport und so weiter. Neben der Regeldefinition finden sich unter den Sicherheitsrichtlinien auch noch Punkte zum Einrichten der URL-Filterung (mit den zu blockierenden Kategorien), der SSL-Filter, der SMTP-Filter und der Quality of Service (QoS). Im Test traten bei der Konfiguration dieser Funktionen keine Probleme zu Tage.

Im Menü zum Anwendungsschutz haben die zuständigen Mitarbeiter Gelegenheit, bestimmte Applikationen oder Befehle wie beispielsweise "Bittorrent" oder "EtherNet/IP: unaut-



Bei den Industrieprotokollen, deren Überwachung die SNi40 über Plugins umsetzt, unterstützt das System auch Custom Pattern

horized command in UDP traffic" zuzulassen oder zu blockieren. Außerdem können sie Schutzfunktionen gegen eine Vielzahl verschiedener Angriffsarten aktivieren. Beispielsweise "DNS ID Spoofing", "Bash Shellshock Vulnerabilities" oder auch "HTTP Redirects auf lokale Dateien".

Ebenfalls zum Anwendungsschutz gehört eine Liste mit den Protokollen, die die Lösung absichern kann. Diese lässt sich an gleicher Stelle auch bearbeiten. So ist es beispielsweise möglich, beim SSL-Protokoll anzugeben, ob die Appliance nicht unterstützte Encryption Methods zulassen soll, wie hoch die Verschlüsselungsstufe sein muss und ob das System unverschlüsselte Daten erkennt. Abgesehen davon können die zuständigen Mitarbeiter auch das IPS für SSL deaktivieren und alle SSL-Anfragen protokollieren. Entsprechende Einstellungsmöglichkeiten gibt es logischerweise auch für alle anderen Protokolle.

Industrieprotokolle

In diesem Zusammenhang ist es sinnvoll, einmal auf die von der SNi40 unterstützten Industrieprotokolle einzugehen. Dazu gehören OPC UA, EtherNet/IP, Modbus, S7 und IEC 60870-5-104. Wichtig in diesem Zusammenhang ist, dass das Stormshield-Produkt für all diese Protokolle so genannte Custom Pattern unterstützt. Mit diesen verfügen die Administratoren über die Option, Grenzwerte zu hinterlegen, mit denen sich bei Bedarf bestimmte Funktionen blockieren lassen, ohne dabei den Datenverkehr an sich zu unterbinden. Es ist auf diese Weise zum Beispiel möglich, normale Datenübertragungen aufrecht zu erhalten, aber keine Werte weiterzuleiten, die über einem Limit, wie etwa sechs liegen.

Drückt ein Mitarbeiter zwölf Mal auf einen Füllknopf und versucht so fälschlicherweise zwölf Liter in ein System einzufüllen, das nur sechs Liter fasst, so erkennt die Firewall das Überschreiten des Schwellwertes und blockiert den dazugehörigen Befehl an die Füllmaschine, ohne dass die anderen Datenübertragungen dadurch beeinträchtigt werden. Bei Bedarf können die IT-Mitarbeiter hierzu auch Bereiche definieren, beispielsweise von minus acht bis plus 16. Die genannte Funktion ist sehr mächtig und versetzt die Verantwortlichen dazu in die Lage, jedes Detail zuzulassen oder zu blockieren und so ihre Anlagen genau abzusichern.

Die Protokolle werden im Betrieb mit Plugins analysiert. Damit sorgt Stormshield dafür, dass die Firewall einen Alarm auslöst, wenn die Rahmenbedingungen, beispielsweise des IEC-Standards nicht erfüllt werden. Die Analyse geht folglich deutlich über eine reine Signaturerkennung hinaus.

Wenden wir uns nun aber wieder dem Anwendungsschutz zu. Über die "Prüfprofile" legen die Administratoren fest, welche IPS-Profile zum Analysieren des ein- und des ausgehenden Verkehrs zum Einsatz kommen sollen. Der "Vulnerability Manager" analysiert installierte und benutzte Applikationen auf den Hosts und überprüft sie auf Angreifbarkeiten, wie beispielsweise eine veraltete Perl-Version. Arbeitet im Netz zum Beispiel ein PLC mit veralteten Diensten, die Sicherheitslücken mit sich bringen, so erkennt der Vulnerability Manager dies und übernimmt den Schutz der Datenübertragungen. So kann er die betroffene Komponente auf Wunsch automatisch in Quarantäne verschieben, was im Test erwartungsgemäß funktionierte.

Die "Host Reputation" lässt sich im Gegensatz dazu einsetzen, um auf dynamische Veränderungen im Verhalten einzugehen. Überschreitet ein Client wie ein PLC oder ein Rechner im Betrieb bestimmte Schwellwerte, zum Beispiel, wenn das IPS meldet, dass der Client auf ungewöhnliche Art kommuniziert, so lässt sich die Host Reputation verwenden, um nicht den gesamten Verkehr zu dem betroffenen System zu unterbinden, sondern nur seinen Zugang zu bestimmten Diensten. Im Test lief das einwandfrei ab. In Produktionsumgebungen bringt es den Vorteil, dass die Produktion weiterlaufen kann und das Netz trotzdem geschützt ist, da etwa der LAN-Zugang einer infizierten Komponente geblockt wird, nicht aber die Steuerung eines Produktionssystems. Die Host Reputation stellt also eine Verkehrssteuerung auf Basis des angezeigten Fehlverhaltens dar. Mit ihr verhindert die Sicherheitslösung schädliche Aktionen und weist auf Probleme hin. Konfigurationsoptionen für die Anti-Virus- (Kaspersky oder Clam-AV) und Anti-Spam-Funktionen schließen den Anwendungsschutz ab.

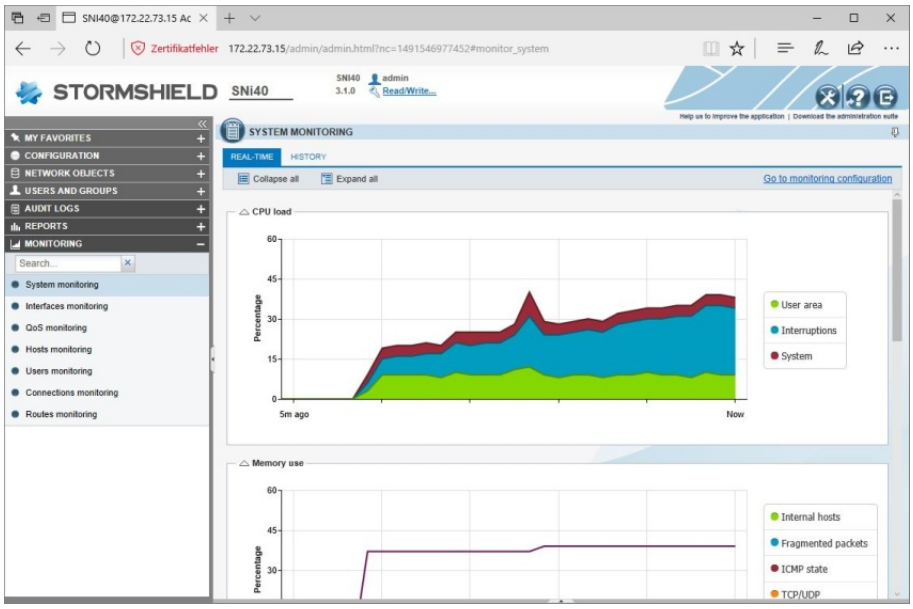
Ansonsten finden sich unter den Konfigurationsoptionen nur noch Menüeinträge zum Definieren der SSL- und IPSec-VPNs und der Benachrichtigungen über lokale Protokolle, Syslog-Server oder IPFIX-Einträge. Bei den

Benachrichtigungen existieren auch noch Punkte zum Konfigurieren des SNMP-Agenten, der E-Mail-Alarme und ähnliches.

Überwachung und Protokollierung

Die restlichen Menüpunkte des Konfigurationswerkzeugs befassen sich mit der Überwachung und der Protokollierung. In Bezug auf die Protokollierung unterscheidet die Appliance zwischen Ansichten, die Korrelationen über mehrere Log-Files hinweg enthalten (beispielsweise alles was mit E-Mail, Systemereignissen und VPN-Verbindungen zu tun hat) und Protokollen. Bei letzteren handelt es sich um die Logs, die die Firewall auf ihre SSD schreibt, zum Beispiel das Admin-Log, das aus Zwecken des Auditings alle auf der Lösung durchgeführten Konfigurationsschritte enthält. Weitere Protokolle gibt es unter anderem zu den Netzwerkverbindungen, den Alarmen, dem SSL-Proxy und ähnlichem.

Die Überwachungsfunktion stellt schließlich Grafiken und Verlaufskurven für Daten wie die CPU- und Speicherlast, die Temperatur, den über die einzelnen Schnittstellen abgewickelten Datenverkehr und die Routen zur Verfügung. Außerdem gehören eine QoS-Überwachung, eine Monitoring-Funktion für Verbindungen (mit Datum, Quelle, Benutzer, Ziel, Zielport, etc.), eine Host-Überwachung und ein User Monitoring zum Leistungsumfang der Lösung. Die beiden letzteren liefern auf Host- beziehungsweise User-Basis Informationen über die benutzte Bandbreite, die Pakete und Verbindungen sowie die Gefährdungen, Anwendungen, Services und so weiter.



Die SNi40 während eines DoS-Angriffs

Sicherheits-Test

Wie bereits angesprochen, nahmen wir im Test das interne und das externe Interface der SNi40 mit diversen Security-Tools wie Nessus, Metasploit, Nmap und dem Greenbone Security Manager unter die Lupe. Außerdem führten wir auch Angriffe mit DoS-Tools und ähnlichem durch, um die Firewall aus dem Tritt zu bringen. Dabei kamen wir zu der Erkenntnis, dass die Stormshield-Lösung praktisch keine überflüssigen Dienste und Informationen im Netz bereitstellte. Nmap fand immerhin heraus, dass auf dem Produkt FreeBSD lief. DoS-Angriffe ließen die ordnungsgemäß konfigurierte SNi40 ebenfalls kalt. Während unserer Analyse traten folglich keinerlei Sicherheitslücken zu Tage.

Fazit

Die SNi40 von Stormshield stellt eine leistungsstarke Firewall-Appliance für Industrieumgebungen mit. Sie bietet nicht nur eine große Zahl an "klassischen" Sicherheitsfunktionen wie Anti-Virus, IPS, Sandbox, Anwendungskontrolle und Anti-Spam, sondern "versteht" auch viele Industrieprotokolle wie Modbus, S7 und IEC 60870-5-104. Da das Benutzerinterface genauso funktioniert, wie bei den anderen Lösungen des gleichen Herstellers und sich vom Aufbau her auch nicht besonders von den Konfigurationswerkzeugen anderer Sicherheitsprodukte für den IT-Bereich unterscheidet, sollte kein Administrator bei der Konfiguration der Lösung vor besondere Hindernisse gestellt werden.

Die Überwachungsfunktionen des Produkts mit den Dashboards, Alerts und Reports sind umfangreich und intuitiv zu bedienen. Auch die Hardware, die stoßsicher, staubabweisend und mit einem verhältnismäßig kleinen Gehäuse mit redundanter Stromversorgung daherkommt, konnte uns überzeugen. Hochverfügbarkeitskonfigurationen lassen sich mit der Lösung ebenfalls realisieren. Administratoren, die sich mit der Aufgabe konfrontiert sehen, auch industrielle Anlagen absichern zu müssen, sollten auf jeden Fall einen Blick auf das Produkt werfen.