Hochverfügbare Next Generation-Firewall für verteilte Netze

Dr. Götz Güttich

Mit den Appliances der Eagle- und der Wolf-Serie bietet Clavister Next Generation-Firewalls an, die sich vor allem für Umgebungen eignen, in denen mehrere Firewalls zum Einsatz kommen, beispielsweise in verteilten Netzen. Ein zentrales Verwaltungstool sorgt dabei dafür, dass die zuständigen Mitarbeiter stets den Überblick behalten. Die Appliances sind in verschiedenen Hardware-Ausstattungen erhältlich, das bedeutet die Unternehmen können in jeder Niederlassung genau die Appliance einsetzen, die am besten auf die Leistungsanforderungen im jeweiligen Umfeld abgestimmt ist. Da sich die Hardware-Lösungen nur in ihrer Leistungsfähigkeit unterscheiden – von der Funktionalität her sind alle Produkte identisch – gilt dieser Test, der mit zwei Clavister W30 durchgeführt wurde, gleichermaßen auch für die anderen Next Generation-Firewalls des gleichen Herstellers.

Die Clavister W30, die für den Einsatz in Zweigstellen,entfernten Niederlassungen und kleinen Rechenzentren konzipiert wurde, bringt – wie bei modernen Next Generation-Firewalls (NGFs) üblich – neben der eigentlichen Firewall-Funktionalität mit Deep Packet-Inspection auch VPNs (IPSec, L2TP, PPTP und SSL), erweitertes Routing (auch auf Policy-Basis) und Anti-Spam-Features mit. Dazu kommen noch Anti-Virus-Funktionen (von Kaspersky), ein IPS, Load-Balancing, Bandwidth-Management, Link-Aggregation, ein Web Filter und Funktionen zur Anwendungskontrolle. Die Appliance verfügt über sechs GBit-Ethernet-Schnittstellen und einen Expansion Slot und unterstützt Hochverfügbarkeit, um die NGF-Installation ausfallsicher zu machen.

Der Test

Im Test richteten wir zunächst eine der W30-Lösungen als Internet-Gateway in unserem Netz ein. Dazu verbanden wir das Produkt mit Netzwerk-Switch und DSL-Modem und fuhren es hoch. Anschließend griffen wir mit einem Browser auf das Web-basierte Management-Interface der Appliance zu und führten die Erstkonfiguration durch. Alternativ steht auch eine Kommandozeile zur Verfügung, über die sich beispielsweise Batch-Dateien ausführen lassen, was Sinn ergibt, wenn viele neue Geräte automatisch konfiguriert werden sollen.

Nachdem die Erstkonfiguration erfolgt war, setzten wir uns im Detail mit dem Konfigurationswerkzeug auf Browser-Basis (das laut Hersteller am besten für die Verwaltung von einzelnen Appliances geeignet ist) auseinander und lernten dabei den Funktionsumfang der Lösung kennen. Zudem passten wir die Konfiguration genau an unsere Anforderungen an.

Im nächsten Schritt bauten wir diverse VPN-Verbindungen zu externen Netzen und Geräten auf. Sobald das erledigt war, installierten wir auf einer Windows 7-Workstation das zentrale Management-Werkzeug Clavister InControl, das nach Herstellerangaben mehrere tausend Gateways verwalten kann, und fügten unseren Gateway zur InControl-Konfiguration hinzu. Anschließend nahmen wir uns InControl selbst

vor und analysierten den Leistungsumfang der Lösung.

Als dieser Vorgang abgeschlossen war, analysierten wir die internen und externen Interfaces der Appliance mit diversen Sicherheitstools wie Nessus, Nmap und Metasploit. Das externe Interface hatten wir zu diesem Zweck mit einer festen IP-Adresse versehen.

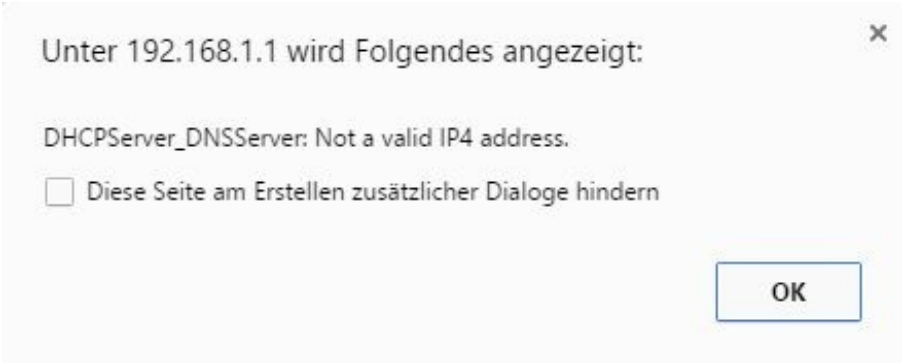
Unser Ziel dabei war, herauszufinden, ob Sicherheitslücken existierten oder ob die Lösung überflüssige Informationen preisgab, die Hackern bei Angriffen helfen könnten. Darüber hinaus verwendeten wir auch etliche Angriffs-Tools, um beispielsweise DoS-Attacken auf die Appliance durchzuführen und zu testen, wie sie darauf reagierte.

Zum Schluss bauten wir unsere Testinstallation so um, dass wir die Hochverfügbarkeitsfunktion der Produkte (HA) unter die Lupe nehmen konnten. Da das HA-Feature nicht mit dynamisch zugewiesenen externen IP-Adressen und PPPoE-Anschlüssen zurechtkommt, schlossen wir zu diesem Zweck beide Appliances hinter einem Router, der den Internet-Zugang übernahm, als Custer zusammen. Dabei behielten wir die Konfiguration mit der festen externen IP-Adresse bei. Im Cluster übernahm das ursprünglich von uns konfigurierte System die Rolle des Masters, die zweite Appliance, die wir zuvor noch nicht angefasst hatten, kam als Slave zum Einsatz, der seine Konfiguration vom Master erhielt.

Inbetriebnahme

Die Inbetriebnahme der W30 gestaltet sich verhältnismäßig einfach. Es genügt, das Produkt auszupacken, und den beiliegenden Quick Start-Guide abzuarbeiten. Dieser empfiehlt, das erste Interface als LAN-Schnittstelle zu verwenden und das zweite für den WAN-Anschluss zu nutzen. Sobald alle Kabel angeschlossen sind, lassen die zuständigen Mitarbeiter die Appliance hochfahren und können sich dann über die Default-IP-Adresse https://192.168.1.1 mit dem Web-Interface des Produkts verbinden.

Daraufhin landen sie auf der Übersichtsseite des Verwaltungswerkzeugs. Diese bietet an, den "Setup Wizard" zu starten, der bei der Erstkonfiguration der Lösung behilflich ist.



Der Setup-Wizard mach die Benutzer auf Fehler in der Konfiguration aufmerksam

Nachdem wir diesen Schritt durchgeführt hatten, präsentierte uns das System einen Willkommensbildschirm, der uns darüber informierte, welche Schritte der Assistent durchführen würde. Zunächst einmal ging es daran, ein neues Passwort für das Administratorkonto zu setzen, was Sinn ergibt, da dadurch sichergestellt wird, dass keine Clavister-Appliances mit Standard-Passwörtern im Netz arbeiten.

Der nächste Schritt befasste sich mit dem Einstellen der richtigen Uhrzeit und der Konfiguration der Zeitzone. Danach kam die Konfiguration des WAN-Interfaces an die Reihe. Wie bereits angesprochen, verwendeten wir die Appliance zu Beginn als Internet-Gateway an einem DSL-Anschluss der Telekom.

Deswegen wählten wir für die WAN-Konfiguration die Option "PPPoE". Alternativ arbeitet die Lösung auch mit festen und per DHCP zugewiesenen IP-Adressen oder PPTP. Für die PPPoE-Konfiguration reichte es, den Benutzernamen sowie das Passwort anzugeben und dem Dienst einen Namen zu geben, damit war die Einrichtung der WAN-Schnittstelle abgeschlossen.

Jetzt ging es daran, einen DHCP-Server für das LAN anzulegen. Dabei vertippten wir uns und stellten bei dieser Gelegenheit fest, dass der Wizard auf fehlerhafte Konfigurationsangaben hinweist und eine Korrektur verlangt. Man kann sich also darauf verlassen, dass die Erstkonfiguration im Großen und Ganzen korrekt abläuft.

Zum Schluss möchte der Assistent noch wissen, welche Zeitserver die Systemzeit auf dem neuesten Stand halten und welche Syslog-Server zum Einsatz kommen sollen, um Daten von der

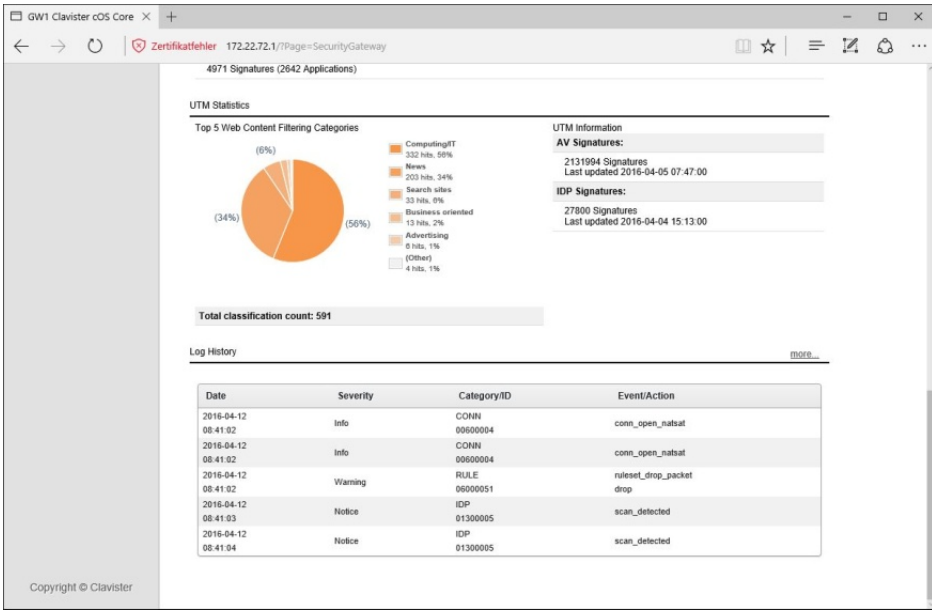
Appliance zu empfangen. Damit ist die Erstkonfiguration beendet und die Änderungen werden übernommen. Üblicherweise gehört die Lizenzierung des Produkts auch mit zum Funktionsumfang des Wizards, dieser Schritt entfiel bei uns aber, da unsere Test-Appliances bereits mit einer installierten Lizenz kamen.

Das Anpassen der LAN-Adresse erfolgt dann manuell über das Web-basierte Konfigurationswerkzeug. Dieser Schritt wird im auf der Clavister-Webseite zum Download angebotenen "Getting Started Guide" zwar genau beschrieben, so dass sich im Test dabei keine Probleme ergaben, unserer Meinung nach gehört er aber ebenfalls zur Erstkonfiguration und sollte deshalb innerhalb des Assistenten abgearbeitet werden.

Das gleiche gilt für die Definition der Regeln für den Internet-Zugang. Standardmäßig erlaubt Clavister nach der Erstkonfiguration die Dienste DNS und HTTP für den Zugriff auf das externe Netz. Dies lässt sich über das Verwaltungswerkzeug natürlich jederzeit ändern, trotzdem wäre es schön, wenn der Wizard zumindest beim Erstellen einer rudimentären, etwas genauer an die Unternehmensanforderungen angepassten, Internetzugriffs-Policy helfen würde.

Das Web-basierte Konfigurationswerkzeug

Nachdem wir die Initialkonfiguration abgeschlossen hatten, loggten wir uns über unsere neue LAN-Adresse bei der NGF ein und definierten zunächst einmal am dritten Interface der Appliance ein Gäste-LAN. In diesem



Die Statusseite bietet unter anderem auch Content Filter-Statistiken an

platzierten wir einen WLAN-Access-Point, über den Besucher über unseren Internet-Anschluss surfen konnten, ohne unsere LAN-Komponenten zu sehen. Im Wesentlichen kopierten wir dazu am dritten Interface unsere LAN-Konfiguration mit einem zusätzlichen DHCP-Server und einem anderen Subnet. Das Gäste-WLAN funktionierte anschließend wie erwartet.

Als wir auf diese Weise sichergestellt hatten, dass alle Anwender in unserem Netz über die Clavister-Appliance Zugriff auf das Internet erhielten, gingen wir dazu über, uns mit dem Konfigurationswerkzeug selbst und damit dem Funktionsumfang der Lösung auseinanderzusetzen, und passten dabei unser Setting gleich genau an unsere Anforderungen an. Zunächst aktualisierten wir dazu die Firmware der Appliance auf das zum Testzeitpunkt aktuelle cOS Core 11.02.01.03, um sicher zu stellen, dass wir mit der neuesten Version arbeiteten.

Nach dem Login beim Web-Interface findet sich der Administrator auf einer Statusseite wieder, die ihn über den aktuellen Zustand der NGF informiert. Am oberen Rand des Fensters erscheint eine Menüleiste und auf der linken Seite befindet sich eine Baumstruktur, die die zu dem jeweils aufgerufenen Menü gehörenden Einträge enthält.

Die eben genannte Statusseite enthält eine Systemübersicht mit Durchsatz, Verbindungen, CPU-Last, Speichernutzung, Systemzeit, den Top fünf Anwendungen, den Top fünf Web Content Filter Kategorien und ähnlichem. Direkt darunter lassen sich diverse Log-Dateien einsehen und durchsuchen. Dazu gehören das System Log, das Antivirus Log, das Log zur Anwendungskontrolle, das Intrusion Detection Log und das Content Filter Log.

Unter "Sub Systems" sehen die Administratoren die aktuelle Blacklist ein und haben die Option, bestehende Blockierungen aufzuheben. Außerdem besteht die Möglichkeit, die vorhandenen Verbindungen in Listenform unter die Lupe zu nehmen. Darüber hinaus lassen sich an gleicher Stelle die DHCP-Server konfigu-

rieren, die Hardware überwachen (beispielsweise die CPU-Temperatur) und die Aktivitäten der Interfaces anzeigen. Die Interface-Übersicht umfasst auch grafische Informationen zur Send- und Receive-Rate. Zusätzlich präsentiert das System unter Sub Systems auch noch die Routing-Table, Daten zum Server Load Balancing und ähnliches.

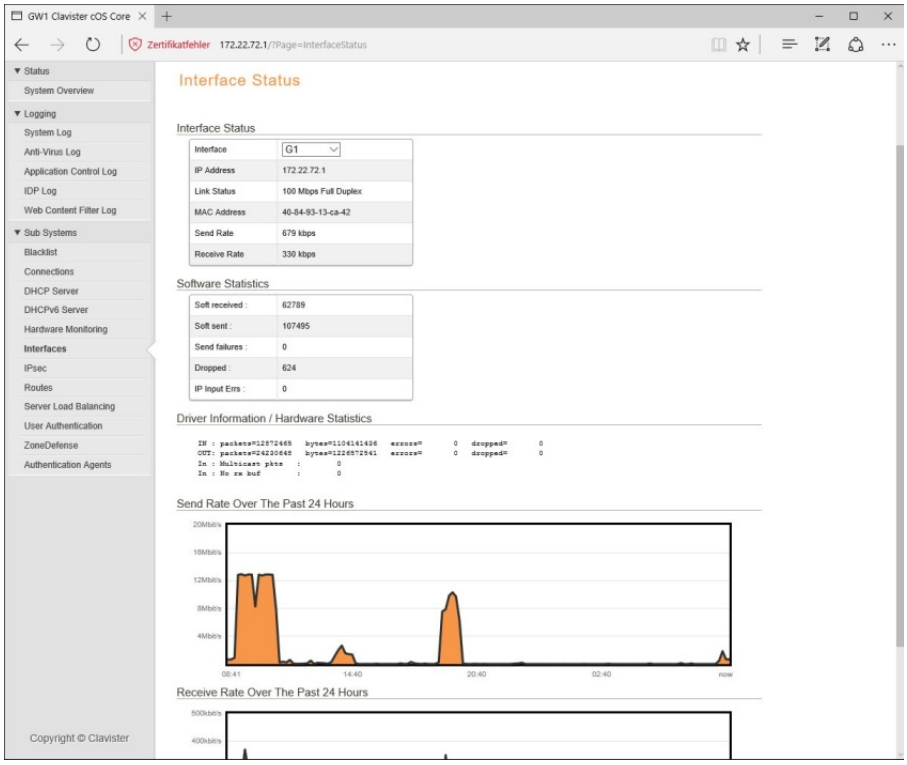
Das Submenü "Maintenance" bietet den Anwendern die Möglichkeit, die Konfiguration und die Core Binaries zu sichern und wiederherzustellen. Außerdem können sie auch eine neue Lizenz einspielen, einen Reset durchführen, oder die Appliance auf Factory-Default-Werte zurücksetzen.

Zusätzlich lassen sich auch Benachrichtigungen aktivieren, die die zuständigen Mitarbeiter über neue Firmware-Releases informieren und automatische Updates für das Antivirus- und das Intrusion-Protection-System einrichten. Der genannte Bereich wurde logisch strukturiert und sollte keinen Administratoren vor unüberwindbare Hürden stellen.

Optionen zum Einspielen neuer Firmware-Dateien und ein Support-Bereich, der eine Diagnose-Konsole mit Systemmeldungen und die Möglichkeit zum Download eines Support-Files mit Systeminformationen bietet, schließen zusammen mit einem Tools-Menü die Übersicht über den Systemstatus ab. Das Tools-Menü umfasst Funktionen wie Ping, einen SSH-Key-Generator und ein Packet-Capture-Werkzeug.

Mit letzterem lassen sich die die über einzelne Interfaces übertragene Daten erfassen und in einem CAB-File zur weiteren Analyse – beispielsweise mit einem Sniffer – auf den PC herunterladen. Übersichten über IDP-Signaturen gehören ebenfalls zu den Tools, genau wie eine Anwendungs-Library, die eine große Zahl von Applikationen (wie AOL, Sophos AV, Google Play und vieles mehr) umfasst und die Benutzer darüber informiert, was die jeweilige Anwendung macht und welches Gefahrenniveau damit verbunden ist.

Da die Application Library später beim Festlegen der Regeln für die Anwendungsüberwachung zum Einsatz kommt, ergibt es Sinn, sich vorab schon einmal damit auseinander zu setzen.



Der Interface-Status umfasst auch grafische Darstellungen des übertragenen Datenverkehrs

Die Systemeinstellungen

Im Hauptmenü "System" finden sich alle Einstellungen zum Konfigurieren der Appliance selbst. Dazu gehören zunächst einmal die Settings für die Systemzeit, die Zeitzone, die Timeserver und den DNS-Client. Zudem legen die Verantwortlichen hier auch fest, welche Benutzer über welche Netze auf das Management-Interface der Appliance zugreifen dürfen, welche Systeme im Netz von der NGF Logs und Events erhalten (über Dienste wie Syslog und SNMP) und wie die Hochverfügbarkeitskonfiguration aussieht, auf die wir später noch genauer eingehen werden.

Ein wichtiger Bestandteil der Systemverwaltung ist das Monitoring. In diesem Zusammenhang spielt zunächst einmal die Überwachung der Hardware eine Rolle. Standardmäßig hat Clavister zu diesem Zweck einen Sensor für die CPU-Temperatur eingerichtet, es besteht aber auch die Möglichkeit, andere Sensoren, die beispielsweise die Stromspannung, den Lüfter und ähnliches im Auge behalten, zu nutzen. Allerdings hängen die verfügbaren Sensoren immer von der gerade verwendeten Hardware ab.

Der "Link-Monitor" dient im Gegensatz dazu zum Überwachen von Objekten wie Hosts oder Netzwerken. Sollten diese aus irgendwelchen Gründen nicht erreichbar sein, so ist die Appliance dazu in der Lage, automatisch vordefinierte Aktionen, wie Failovers und Neukonfigurierungen, vorzunehmen.

Die Real Time Monitor Alerts überwachen schließlich bestimmte Werte wie etwa die CPU-Last, den Durchsatz, die Zahl der Spam-Meldungen oder auch die Zahl gedroppter Pakete. Die zuständigen Mitarbeiter können für diese Grenzwerte setzen und die NGF erzeugt Log-Einträge, falls diese Thresholds überschritten werden.

Ansonsten gehören zu den Systemeinstellungen unter anderem noch eine Benutzerverwaltung für die lokale User-Datenbank, eine White List, die Einträge enthält, die nicht von IDP- und ähnlichen Regeln blockiert werden können und die Definition der HTTP Banner-Files, die das Aussehen der Authentifizierungs- und der Application Level Gateway-Restrictions-Seiten festlegen.

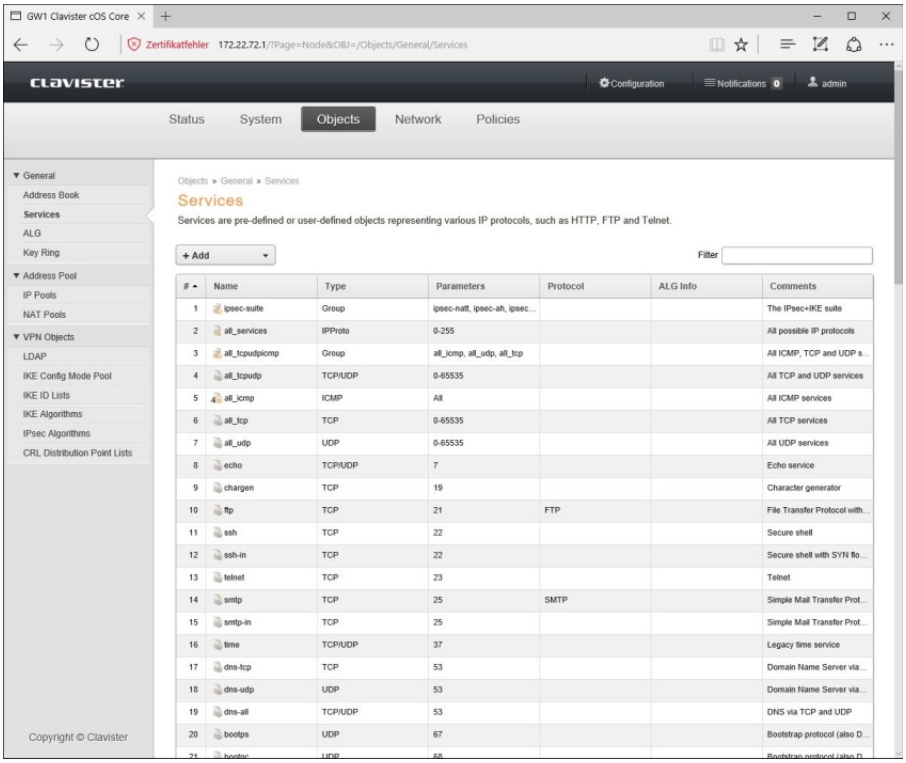
Diverse Geräteeinstellungen schließen das System-Menü ab. Dazu gehören IP Settings wie die Default TTL, das Loggen von Checksummenfehlern und vieles mehr genauso wie TCP Einstellungen wie beispielsweise zur Validierung von Sequence Numbers.

Wenn die Administratoren mit der Maus über einen Eintrag fahren (Hover-Funktion), dann zeigt die W30 zu jeder Konfigurationsoption eine kurze Erklärung an, was sehr sinnvoll ist, weil sich hier auch Einstellungen finden, die selbst IT-Mitarbeitern, die sich mit Netzwerkprotokollen gut auskennen, nicht immer präsent sind. Zusätzlich zu den genannten Protokollen lassen sich übrigens auch noch Settings zu ICMP, PPP, Connection Timeouts, Legth Limits sowie zur Fragmentierung und zur lokalen Reassembly vornehmen.

Das gleiche gilt für Einstellungen zu SSL, der State Engine, der maximalen Zahl der Pipe-Benutzer und zur Diagnose. Im Betrieb fiel uns auf, das die Appliance standardmäßig so eingestellt ist, dass sie anonymisierte Benutzerstatistiken automatisch an Clavister schickt. Das lässt sich zwar hier verhindern, unserer Meinung nach sollte dieser Konfigurationsschritt aber auch im Rahmen des Assistenten zur Erstkonfiguration vorgenommen werden. Settings zur Anwendungskontrolle wie die maximale Zahl unklassifizierter Pakete und unklassifizierter Bytes schließen die Systemkonfiguration ab.

Objekte

Die Objekte sind die Grundlage für die Definition der Policies. Sie umfassen zunächst einmal das Adressbuch, das IP-, Netzwerk- und MAC-Adressen enthält. Bei Bedarf haben die Administratoren auch Gelegenheit, hier neue Host- und Netzwerkadressen hinzuzufügen.



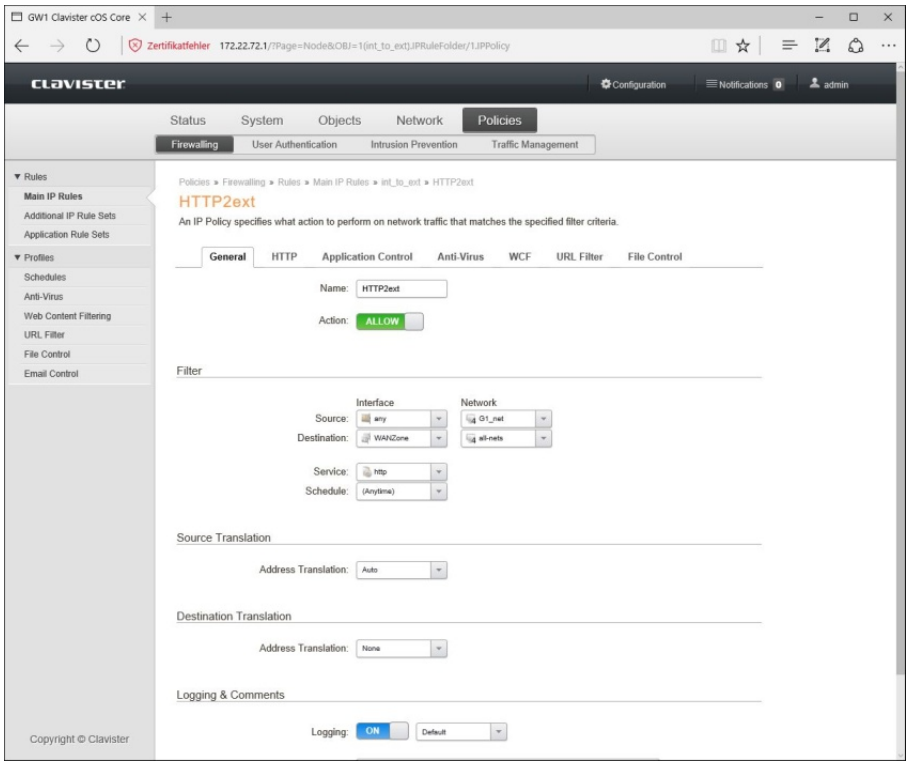
Clavister hat alle relevanten Dienste bereits vordefiniert

Die Services stellen im Gegensatz dazu die im Netz verwendeten Protokolle dar. Clavister hat hier bereits eine große Zahl vordefiniert, wie zum Beispiel "all_icmp", "ssh", "ipsec_suite", "igmp" oder auch "ping". Auch hier gilt wieder, dass die zuständigen Mitarbeiter jederzeit eigene Einträge hinzufügen können.

Unter "ALG" finden sich die Einträge zu den Application Level Gateways. Vordefiniert wur-

den ALGs für H.323 und SIP, es lassen sich bei Bedarf aber auch eigene einfügen, beispielsweise für HTTP, POP3, PPTP und so weiter. An gleicher Stelle sehen die IT-Verantwortlichen auch den Key-Ring ein und legen bei Bedarf neue Schlüssel – etwa zum Absichern von Verbindungen – an.

Ebenfalls von Interesse: die Adress-Pools. Hier finden sich IP-Pools (dynamische Objekte mit IP-Leases) und NAT-Pools, die in NAT-Regeln Anwendung finden können.



Die Definition einer Firewall-Regel

Die VPN-Objekte dienen zur Definition von Virtual Private Networks. Die VPN-Konfiguration erlaubt zunächst einmal das Definieren von LDAP-Servern, von denen die NGF bei Bedarf Zertifikate und Certificate Revocation Lists (CRLs) herunterladen kann.

Der "IKE Config Mode Pool" weist den VPN-Clients dann im Betrieb IP-Adressen, sowie DNS- und WINS-Server zu. Abgesehen davon lassen sich im Rahmen der VPN-Settings unter anderem auch noch die zu verwendenden Algorithmen definieren.

Netzwerk-Settings

Der Hauptpunkt "Network" dient im Wesentlichen zur Konfiguration der Interfaces, VPNs und Routen. Hier lassen sich folglich die Einstellungen für die Ethernet-Adapter mit Adresse, Netzwerk und virtuellem Routing vornehmen. Auch die Link-Aggregation kann an dieser Stelle eingerichtet werden, genau wie PPPoE-Schnittstellen, VLANs und ähnliches.

Ebenfalls interessant: die VPN-Konfiguration. Die Clavister-Lösung unterstützt IPSec, SSL, GRE sowie 6in4 und kann nicht nur mit PPTP- und L2TP-Servern und -Clients kommunizieren, sondern auch mit PPTP V3- und L2TP V3-Komponenten. Im Test stellten wir IPSec-Verbindungen zu einem Lancom-Router vom Typ 1781A und dem aktuellen NCP VPN-Client für Windows her. Dabei kam es zu keinen Schwierigkeiten.

Damit nicht genug, unterstützen die Netzwerkeinstellungen auch "Interface Groups", in denen sich mehrere Schnittstellen für einfacheres Policy-Management zusammenfassen lassen. Was das Routing angeht, so können die zuständigen Mitarbeiter nicht nur statische Routen setzen, sondern auch Routing Tables auf Policy-Basis realisieren. Abgesehen davon besteht auch die Möglichkeit, Load Balancing mit Hilfe verschiedener Routen zu verwirklichen.

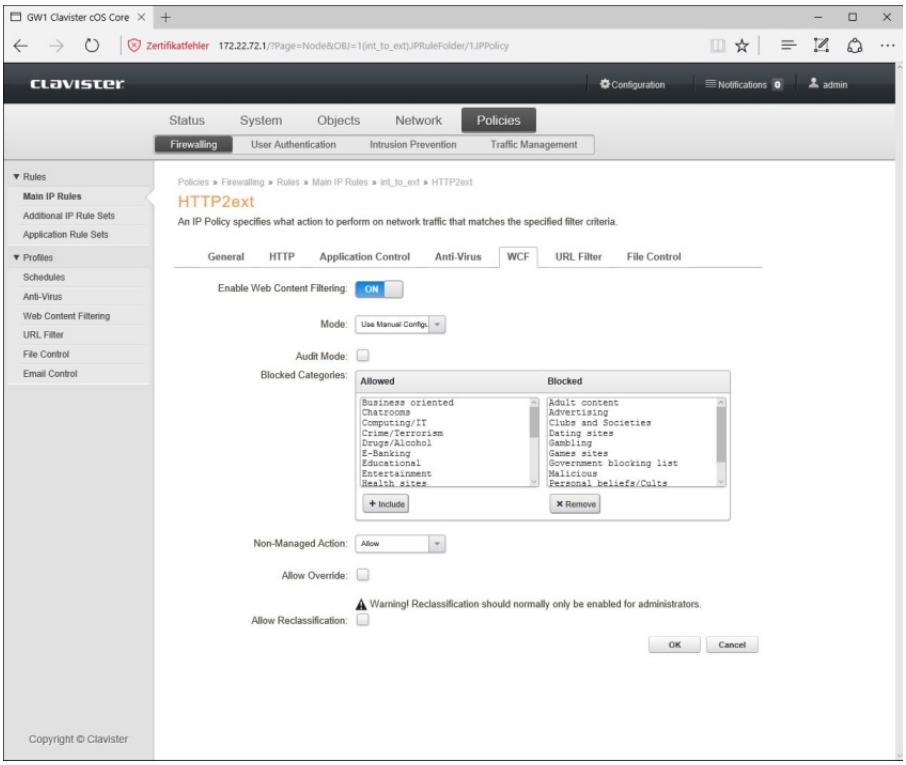
Ebenso unterstützt: dynamisches Routing mit Hilfe von OSPF, virtuelles Routing und Multicast-Routing. Unter "Network Services" konfigurieren die Administratoren schließlich DHCP-Server und -Relays, Radius-Relays, DynDNS und so weiter.

Die Regeln

Der Bereich "Policies" stellt das Herzstück der NGF dar, denn hier richten die zuständigen Mitarbeiter die Regeln ein, die dazu dienen, die Datenübertragungen abzusichern. An erster Stelle sind in diesem Zusammenhang die "Main IP Rules" zu nennen.

Diese lassen sich in Gruppen zusammenfassen, um die Übersichtlichkeit und Verwaltbarkeit zu erhöhen. Es ist so beispielsweise möglich, alle Regeln einer Gruppe auf einmal zu deaktivieren. Die einzelnen Regeln funktionieren – wie bei den meisten Firewalls üblich – mit Parametern wie Quelle und Ziel der Datenübertragung (Netzwerk, Host und ähnliches), dem betroffenen

Dienst (wie "FTP" oder "all_ip"), dem Zeitraum (in dem die Regel gültig ist) und der durchzuführenden Aktion (Drop, Allow, Deny, Reject). Außerdem haben die Administratoren auch die Möglichkeit, den Policies Dienste wie die Application Control, den Web Content Filter oder auch die Antivirus-Funktion hinzufügen, die dann für die jeweiligen Protokolle aktiv werden. Im Test ergaben sich dabei keinerlei Schwierigkeiten.



Die Konfiguration des Web Content-Filters

An dieser Stelle noch ein Wort zur eben genannten Application Control. Mit ihr haben die zuständigen Mitarbeiter die Option, Regeln zu erstellen, die nur für den von einer bestimmten Anwendung generierten Verkehr gelten.

Das funktioniert mit Signaturen, die in einer Datenbank abgelegt wurden. Mit Hilfe der Application Control lassen sich sehr fein abgestufte Policies erzeugen, beispielsweise ist es möglich, einer bestimmten Nutzergruppe eine bestimmte Bandbreite für die Nutzung von Bittorrent zuzuweisen. Damit lässt sich der Datenverkehr im Netz exakt an die Vorgaben des Unternehmens anpassen.

Unter "Profiles" legen die zuständigen Mitarbeiter die Zeitpläne fest, während denen bestimmte Regeln Gültigkeit haben. Außerdem lassen sich unter anderem auch Rahmenbedingungen für Dienste wie den Antivirus (zum Beispiel vom Scan ausgeschlossene Dateitypen oder der Umgang mit komprimierten Dateien) und den Web Content Filter (wie die zu blockierenden Kategorien wie etwa "Advertising", "Gambling", "Swimsuit", etc.) setzen. Auch die E-Mail-Kontrolle mit White- und Blacklist sowie Anti-Spam wird hier konfiguriert.

Was die Benutzerauthentifizierung angeht, so unterstützt das System neben der lokalen Datenbank externe LDAP- und Radius-Server. Die Intrusion Prevention arbeitet mit Signaturen, die sich mit Hilfe von Policies nutzen lassen, um den Datenverkehr auf Angriffe zu überwachen und Abwehrmaßnahmen zu treffen.

Diese Policies setzen sich aus einem Namen, dem betroffenen Dienst, einem Zeitplan, den genannten Signaturen und ähnlichem zusammen. Die "Zone Defense" kommt wiederum zum Einsatz, um Hosts und Netzwerke mit Hilfe von Switches beim Auftreten von IPS- und Threshold Rule-Verletzungen zu blockieren. Last but not least verfügt die W30 auch noch über umfassende Traffic Shaping-Funktionen.

InControl-Installation

Nachdem wir uns durch das Konfigurationswerkzeug durchgearbeitet und unsere Konfiguration optimiert hatten, installierten wir auf einem Test-Client unter Windows 7 im LAN die Management-Software "InControl". Diese eignet sich – wie bereits angesprochen – zum Verwalten großer Installationen mit vielen NGFs.

Die Software besteht aus einer Client/Server-Kombination, auf diese Weise ist es möglich, sie im Netz sinnvoll zu verteilen und von mehreren Clients aus darauf zuzugreifen. Die Installation läuft über einen Wizard ab und sollte keinen Administratoren vor irgendwelche Schwierigkeiten stellen. Sofort nach dem Abschluss des Setups (für den Test installierten wir alle Komponenten auf einem System) konnten wir den Client aufrufen und uns mit den Default-Zugangsdaten "admin" und "admin" beim Server anmelden.

Im nächsten Schritt mussten wir unsere Gateways zu der InControl-Konfiguration hinzufügen. Dazu war es erst einmal erforderlich, auf den einzelnen Gateways einen Key zum Absichern der Verbindung zu erzeugen und diesen über den Key Ring für Managementverbindungen freizugeben.

Anschließend können die IT-Mitarbeiter die IP-Adressen der Gateways in InControl angeben und die jeweils gültigen Keys für die einzelnen Appliances eintragen. Danach meldet sich InControl bei den NGFs an und sie erscheinen im Arbeitsbereich der Software. Das klingt jetzt kompliziert, die genannten Arbeitsschritte waren aber schnell erledigt und da die gesamte Prozedur in der Dokumentation genau beschrieben wurde, sollte es auch hier nirgendwo zu Schwierigkeiten kommen.

Die Arbeit mit InControl

Nach dem Login mit der Konsole landet der User zunächst unter "Home". Hier zeigt die Lösung erstmal die "Global Domain" an. Dieser fügen die Administratoren entweder wie eben beschrieben ihre vorhandenen Gateways hinzu, oder legen eigene Domains oder HA Cluster an.

Zu den Clustern kommen wir später. Aus Performancegründen empfiehlt Clavister, wo möglich die Global Domain zu nehmen, in großen Umgebungen kann es aber durchaus Sinn ergeben, eigene Domains zu erzeugen, da das Policy-Management bei Bedarf auf Domänenbasis erfolgt.

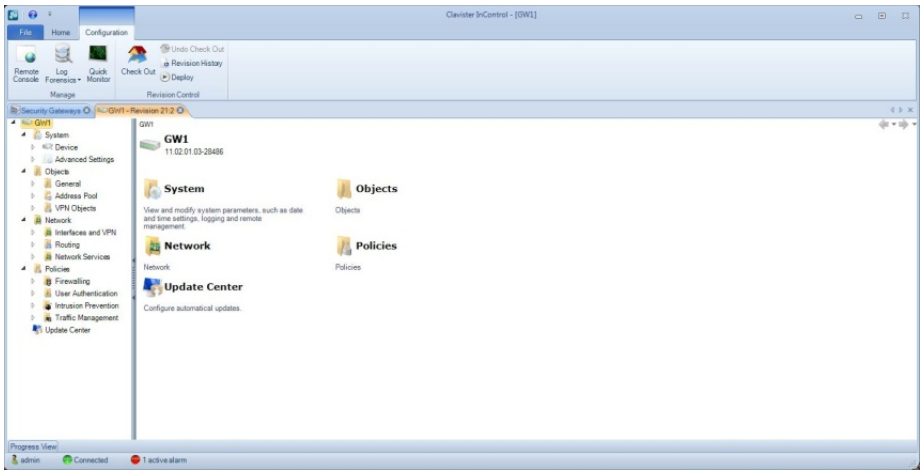
InControl bietet am oberen Bildschirmrand diverse Reiter, darunter befindet sich eine Ribbon-Leiste, die Icons enthält, mit denen sich zum jeweils ausgewählten Kontext passende Funktionen aufrufen lassen. Der Arbeitsbereich der Lösung erinnert also ein wenig an Microsoft Office, was die Einarbeitung in das Tool sehr erleichtert.

Der erste Reiter – "File" – dient dazu, Daten zu im- und exportieren, den SMTP-Server für E-Mail-Alerts zu definieren und ähnliches. Interessanter ist der Reiter "Home", der – wie eben erwähnt – auch direkt nach dem Login angezeigt wird.

Hier finden sich die angemeldeten Security Gateways, Listen mit Alarmen und Lizenzdetails und der Library Browser, mit dem die Benutzer Zugriff auf die Interface-Nutzung und so weiter informieren können.

Zusätzlich besteht an gleicher Stelle auch die Option, Monitoring Dashboards zu konfigurieren, die den zuständigen Mitarbeitern die für sie interessanten Parameter in Form von Gauges, Grafiken und ähnlichem anzeigen, die Benutzer zu verwalten, die entweder als Administrator oder als Auditor auf InControl zugreifen dürfen und Gruppen sowie Audit Trails zu managen. Letztere umfassen die Konfigurationsänderungen auf den Gateways und diverse andere Aktionen.

Wählt ein IT-Mitarbeiter einen Gateway aus, so wird das Icon "Configure" aktiv. Über dieses



Der Konfigurationsdialog von InControl

Einträge wie die Traffic Summary, die Top App Usage, die Top Rule Usage, die Top Talkers und ähnliches haben. Außerdem bietet "Home" auch einen Log Explorer (der Queries durchführen kann), Reporting-Funktionen (die sich bei Bedarf mit einem Zeitplan automatisieren lassen, es ist auch der Versand von Reports per E-Mail möglich) und einen Log Analyzer, mit dem sich die Administratoren über die Anwendungsnutzung, die Top Talker, lassen sich die Appliances einrichten. Auf der linken Seite findet sich eine Baumstruktur, die den betroffenen Gateway und die Einträge "System", "Objects", "Network", "Policies" und "Update Center" enthält. Über diese haben die Verantwortlichen Zugriff auf die Funktionalität der NGFs.

Da der Funktionsumfang der Lösungen ja bereits vorgestellt wurde, gehen wir an dieser Stelle

nicht noch einmal auf die ganzen Details ein. Es reicht, zu sagen, dass die Baumstruktur sehr übersichtlich gestaltet wurde und dass die Konfigurationsarbeit mit InControl flott von der Hand ging.

Uns gefiel das InControl-Interface im Test sogar besser, als das Web-Interface und wir würden es

Der "Quick Monitor" im Betrieb

selbst Anwendern, die nur eine Clavister-Firewall in Betrieb haben, empfehlen, InControl zu installieren und die Konfiguration über diese Software durchzuführen. Das ist allerdings mit Sicherheit Geschmackssache.

Wie oben bereits erwähnt, kann die Konfiguration auch auf Domänenbasis ablaufen. Wählt ein Administrator eine Domäne statt eines Gateways aus, so erhält er die Option, Objekte, Dienste, NAT-Pools, Profile und vieles mehr auf Domänenebene an seine Anforderungen anzupassen.

Nach dem Rechtsklick auf einen Gateway stehen ihm noch diverse weitere Funktionen zur Verfügung. Dabei handelt es sich um eine Remote Console, eine Revision Control für die Konfigurationen, Device Maintenance-Funktionen (mit Upload Firmware, Download Tech Support-File, Restart, etc.) und ähnliches.

Erwähnenswert ist in diesem Zusammenhang noch das "Quick Monitor"-Feature, dass sich ebenfalls über einen Rechtsklick aufrufen lässt. Dabei handelt es sich um ein vordefiniertes Monitoring-Dashboard, das Informationen zu Durchsatz, CPU- und Buffer-Nutzung, der CPU-Temperatur, Verbindungen sowie Interface-Statistiken liefert. Alle über den Rechtsklick erreichbaren Funktionen stehen auch über Icons in der Ribbon-Leiste zur Verfügung.

Der "Progress View" zeigt den aktuellen Status, beispielsweise beim Verteilen von Konfigurationen an. Eine Übersicht über die aufgelaufenen Fehlermeldungen schließt den Leistungsumfang von InControl ab.

Die Sicherheit

Als wir uns durch die Verwaltungswerkzeuge durchgearbeitet hatten, machten wir uns daran, die Appliance mit diversen Hacking- und Security-Lösungen in Bezug auf Sicherheitslücken unter die Lupe zu nehmen. Dabei scannten wir immer die externen und internen Interfaces (die zu diesem Zweck beide mit fixen IP-Adressen versehen wurden).

Konkret kam dabei heraus, dass Nmap am internen Interface wie zu erwarten die für unsere Konfiguration geöffneten Dienste wie HTTP, SSH und ähnliches erkannte. Außerdem vermutete das Tool, dass es sich bei der Appliance um ein D-Link-Gerät handele, gab aber gleich an, dass diese Aussage nicht zuverlässig sei. Am externen Interface waren alle Ports gefiltert, deswegen konnte Nmap nicht viele Informationen erlangen. Immerhin stellte der Scanner anhand der MAC-Adresse fest, dass es eine Clavister-Lösung war.

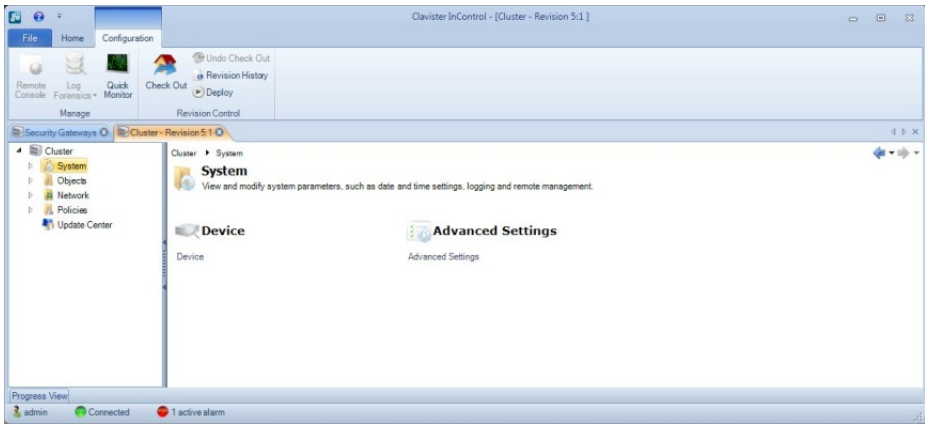
Nessus erkannte am internen Interface ebenfalls die freigegebenen Dienste, sogar mit der Version der verwendeten Server, und bemängelte das auf der Appliance installierte Zertifikat. Das war nur folgerichtig, da wir das selbstgenerierte Originalzertifikat von Clavister auf der Appliance belassen hatten und stellt somit kein Sicherheitsrisiko dar. Außerdem gab Nessus an, dass es sich um eine Clavister-Lösung handele. Am externen Interface fand Nessus nichts. Metasploit war genau wie nmap nach dem Scan des internen Interfaces der Meinung, es handele sich um eine D-Link-Appliance. Außerdem erkannte die Sicherheitslösung wie zu erwarten die freigegebenen Dienste. Am externen Interface konnte sie ebenfalls nichts finden.

Weder an internen noch am externen Interface konnte eines unsere Angriffs-Tools die Clavister-Lösung in Verlegenheit bringen. Sie blieb von den Attacken völlig unbeeindruckt und überstand den Sicherheitstest somit unbeschadet.

Hochverfügbarkeit

In nächsten Schritt verwendeten wir InControl, um mit unseren beiden NGFs einen Cluster aufzusetzen. Dazu kamen wieder fixe IP-Adressen auf den WAN-Interfaces zum Einsatz.

Zunächst fügten wir unsere beiden Gateways zu dem InControl-System hinzu und konfigurierten den späteren Master-Gateway so, dass er unsere Anforderungen erfüllte. Im Wesentlichen übernahmen wir dazu unsere alte Konfiguration, wir wiesen parallel dazu den Interfaces aber noch diverse IP-Adressen hinzu.



Cluster lassen sich im Betrieb genau wie einzelne Gateways verwalten

Damit die Cluster-Konfiguration funktioniert, müssen alle Interfaces der Appliances nämlich sowohl eine Shared IP-Adresse, als auch eine Private IP-Adresse (bei ungenutzten Interfaces kann das Loopback sein) haben. Sobald das erledigt war, genügte es, in InControl einen Cluster zu definieren, zwei Interfaces der Gateways als Synchronisierungs-Interfaces zu verbinden und zuerst den Master und dann den Slave zu dem Cluster hinzuzufügen.

Sobald das geschehen war, fragte InControl nach dem Modus, in dem der Cluster betrieben werden sollte. Hier stehen drei verschiedene Optionen zur Auswahl. Zunächst einmal "Synced". Dabei wird die gesamte Konfiguration von InControl verwaltet und erst auf den ersten und nach einer Pause auf den zweiten Knoten hochgeladen. In diesem Modus ist es nicht mehr möglich, den Cluster parallel über das Web-Interface zu verwalten, es muss zum Management InControl zum Einsatz kommen. Im Modus "Auto" lädt das Werkzeug die Konfiguration nur auf den ersten Node hoch und der Cluster übernimmt den Sync-Vorgang. Die dritte Möglichkeit nennt sich schließlich "manuell". Hier bleibt alles dem Administrator überlassen.

Hat man sich für einen Modus entschieden, wir wählten im Test die zweite Option (da wir weiterhin parallel das Web-Interface nutzen wollten), fragt InControl, welche Netzwerkschnittstellen für die Synchronisierung zum Einsatz kommen. Nachdem wir diese Frage beantwortet hatten, lud das Tool die Konfiguration auf den ersten Node hoch, die Synchronisierung fand statt und der Cluster ging in Betrieb.

Im Test traten beim Failover keine Schwierigkeiten auf. Laut Hersteller nimmt der Failover übrigens weniger als 800 Millisekunden in Anspruch. Cluster lassen sich – wie bereits erwähnt – auch über das Web-Interface erzeugen. Dazu steht ein Wizard zur Verfügung, der die erforderlichen Parameter abfragt.

Fazit

Im Test hinterließ die Clavister W30 einen hervorragenden Eindruck. Die Lösung verfügt über alle Sicherheitsfunktionen, die im Unternehmensumfeld erforderlich sind. In diesem Zusammenhang seien exemplarisch nur die Next-Generation-Firewall, das IPS, der Web Filter, die Anwendungskontrolle sowie die Antivirus- und Anti-Spam-Features genannt. Das zentrale Verwaltungstool ist vorbildlich, die Routingfunktionen wurden leistungsstark gestaltet und mit dem Web-Interface und der CLI stehen Administratoren umfassende Alternativwerkzeuge zum Verwalten der Appliances zur Verfügung, die falls erforderlich auch parallel zueinander Verwendung finden.

Für Anwendungsbereiche, in denen Hochverfügbarkeit benötigt wird, stellt Clavister zudem einfach zu bedienende Funktionen bereit, mit denen sich Cluster schnell und einfach implementieren lassen. Wir können die Lösungen damit rundherum empfehlen.

Dr. Götz Güttich leitet das IAIT in Korschenbroich.