siedl networks
Enterprise Open Source Technology Solutions

SUCCESS STORY

Ausfallsichere OPNsense-Firewall für Koller International Group

Erneuerung der Hardware und Implementierung eines redundanten OPNsense Clusters über die Landesgrenzen hinaus.

Die Firma Koller International Group mit Hauptsitz in Vitis, Österreich, ist in verschiedenen Geschäftsbereichen tätig, wie der Produktion von Whirlpool-Komponenten, Metall- und Kunststofftechnik sowie Holzprodukten für Geschäfts- und Privatkunden. Die neueste Innovation von Koller International Group sind Outdoor Spa`s  und Hot Tub`s für eine wohlige Entspannung im Außenbereich. Neben dem Stammwerk in Vitis gibt es zwei weitere Niederlassungen: in Wien und in Jindrichuv Hradec (Tschechische Republik).

Die bestehende Firewall-Lösung war in die Jahre gekommen, und deren Hersteller hatte für die eingesetzten Geräte End of Support bzw. End of Life angekündigt. Koller International ist langjähriger Kunde von Siedl Networks und beauftragte den IT-Dienstleister aus Krems an der Donau im April 2022 mit der Planung und Implementierung einer neuen Firewall-Lösung.

Die Herausforderung…

Gewünscht war eine leistungsfähige State-of-the-Art-Firewall auf Multi-GBit-Niveau, ausfallsicher vom Internet bis zum Client. Im Anforderungskatalog standen die Punkte „Redundanz und Kontinuität“ an oberster Stelle: Bei einer Störung oder einem kompletten Ausfall der Internetleitung sollten alle wichtigen Dienste wie E-Mail, VPN, etc. weiter funktionieren.

Alle Niederlassungen, auch die Außenstandorte in Wien und Tschechien, müssen redundant angebunden sein. Das Failover muss im Störungsfall schnell und automatisch mit minimalen Umschaltzeiten erfolgen, um einen unterbrechungsfreien Betrieb des Netzwerkes zu gewährleisten.

***Philipp Sprung**, Sales & Account Manager bei Siedl Networks GmbH und **Helmut Hieß**, Leiter IT bei Koller International Group*

Natürlich sollte das Zurückschalten in den Normalbetrieb auch automatisch erfolgen, sobald die Störung behoben ist.

Auf der Wunschliste stand ebenfalls eine sichere VPN-Verbindung für Remote Worker. Die Mitarbeitenden sollen von zu Hause oder unterwegs sicher auf das Unternehmensnetzwerk zugreifen und vertrauliche Informationen geschützt übermitteln können.

Die Lösung…

Siedl Networks realisiert digital souveräne IT-Infrastrukturen mit Open-Source-Technologien und in diesem Fall empfahlen die Techniker aufgrund der erfolgreichen Erfahrungen in mehreren Kundenprojekten eine Open-Source-Lösung: OPNsense.

OPNsense ist eine auf FreeBSD basierende Firewall-Distribution mit Unterstützung für Firewall-Regeln, VPN, Intrusion Detection und Prevention System (IDPS), Proxy-Server, Load Balancing, Traffic Shaping und mehr. Die benutzerfreundliche grafische Oberfläche vereinfacht die Administration. OPNsense kann durch Plugins erweitert werden, hat eine aktive Entwicklergemeinschaft und eine engagierte Community.

Nach einer ausführlichen Recherche entschieden sich die Techniker von Siedl Networks, an jedem Standort zwei Geräte mit OPNsense einzurichten. Am Standort Vitis kommunizieren die beiden Geräte miteinander – fällt eines aus, übernimmt das andere automatisch, ohne dass ein Administrator manuell eingreifen muss. In Wien und Tschechien waren Cold Standby Lösungen gewünscht. Im Fehlerfall muss der Administrator manuell die 2. Firewalls in Betrieb nehmen.

Bei der Planung stellte sich heraus, dass neben den OPNsense® Rack Security Appliances auch neue Core-Switches am Standort Vitis erforderlich waren. Bei den bisher eingesetzten Switches gab es nicht nur Kompatibilitätsprobleme, sondern die älteren Geräte unterstützten nicht alle benötigten Protokolle.

Das WAN-seitige Routing, um die Kommunikation zwischen verschiedenen Standorten und Netzwerken zu ermöglichen, stellte sich als komplex heraus.

Damit eine WAN-seitige Redundanz hergestellt werden konnte, wurden zwei Glasfaseranschlüsse von unterschiedlichen Providern und auch Netzbetreibern (eine A1 Leitung und eine Nögig Leitung) eingesetzt.

Damit im Falle eines Ausfalles der primären Internetleitung dennoch alle Services zur Verfügung stehen, wird nun ein via BGP (Border Gateway Protocol) geroutetes Subnetz verwendet, welches im Fehlerfall über den Backup-Provider gerouted werden kann.

Was ist BGP?
BGP ist das Protokoll, das die besten Wege für den Datenverkehr zwischen den Autonomen Systemen im Internet findet und sorgt für die Stabilität des Netzes, indem es garantiert, dass sich Router an Routenausfälle anpassen können: wenn ein Pfad ausfällt, wird schnell ein neuer Pfad gefunden. BGP trifft Routing-Entscheidungen auf der Grundlage von Pfaden, die durch Regeln oder Netzwerkrichtlinien definiert sind, die von Netzwerkadministratoren festgelegt wurden.

Weiters war die Gestaltung eines voll vernetzten (Full-meshed), ausfallsicheren VPN sehr anspruchsvoll. Hier waren im Vorfeld umfangreiche Tests und einige Entwicklungsarbeit notwendig. IPsec war für das geplante Setup unbrauchbar, OpenVPN bot zu wenig Bandbreite, und Wireguard war zu diesem Zeitpunkt noch nicht gut genug in OPNsense integriert.

Die Techniker entschieden sich daher für tinc VPN (Full Meshed auf Layer 2, d.h. das VPN simuliert die gesamte Netzwerkschicht und die verschiedenen Geräte und Standorte erscheinen als Teil eines einzigen lokalen Netzwerks). tinc VPN ist effizient und ressourcenschonend, was die Netzwerklatenz minimiert und sicherstellt, dass die VPN-Kommunikation effizient und mit minimalen Auswirkungen auf die Netzwerkressourcen stattfindet.

Die Umsetzung ...

Nachdem die Planungsphase abgeschlossen war, begannen die Techniker von Siedl Networks im Juli 2022 mit den Tests im eigenen Labor.
Sie stellten die Kundennetzwerke nach, konfigurierten die Hardware und führten zahlreiche Ausfalltests durch. Das ist effizient und verkürzt die Installationszeit. Nach rund 10 Tagen waren alle zufrieden – jetzt konnte die Implementierung bei Koller International beginnen. Innerhalb weniger Tage stellten die Techniker die Standorte in Tschechien, Wien und Vitis um.

Die OPNsense-Cluster mit Session Sync ermöglichen ein Stateful Failover bei einem Hardwareausfall.Jede Firewall ist redundant über das Link Aggregation Control Protocol (LACP) an einen neuen Switch-Stack (2 mal 10 GBit) angebunden, und jeder Server ist ebenfalls redundant über LACP mit dem Switch-Stack verbunden. Die Client-Switches sind in einem RSTP-Ring mit dem Switch-Stack verbunden. Diese Ringtopologie ermöglicht redundante Verbindungen, die den Datenverkehr auch dann weiterleiten können, wenn eine der Verbindungen oder ein Switch ausfällt.

Als Intrusion Detection and Prevention System (IDPS) kommt Suricata zum Einsatz, eine der Kernkomponenten von OPNsense. Das Netzwerküberwachungstool analysiert den Netzwerkverkehr in Echtzeit, kann Bedrohungen und Angriffe erkennen und darauf reagieren. Suricata kann den Netzwerkverkehr filtern, bestimmte Verbindungen blockieren oder Alarme auslösen, um Administratoren über verdächtige Aktivitäten zu informieren. Dazu kommen Funktionen wie Traffic Logging, Protocol Analysis, Flow Monitoring etc.

Über Koller International Group:

KOLLER INTERNATIONAL GROUP

Der Name Koller steht für technisches Know-how, eine hochmoderne Produktion und Innovationsgeist aus Österreich. Die Koller Unternehmensgruppe ist in verschiedenen Geschäftsbereichen erfolgreich tätig: Als eines der weltweit führenden Unternehmen in der Wassertechnik entwickelt und produziert die Firma Koller am Standort in Vitis Komponenten für Whirlpoolsysteme. Zusätzlich ist Koller ein anerkannter Partner für Unternehmen, wenn es um die Produktion und die Galvanisierung von Metallteilen geht. Sämtliche Produkte werden in höchster Qualität und ausschließlich in der EU hergestellt. Koller Holz bietet Holzprodukte für Geschäfts- und Privatkunden.

Die neueste Innovation von Koller International Group sind Outdoor Spa`s und Hot Tub`s für eine wohlige Entspannung im Außenbereich.

Website: https://www.rkoller.com

Das Fazit ...

Die neue Firewall mit OPNsense ist leistungsstark und ausfallsicher. Sie ermöglicht den reibungslosen Betrieb aller Standorte auch bei einer Unterbrechung der Internetleitung. Auch das vollautomatische Failover erfüllt alle Ansprüche. Alles ist so konfiguriert, dass Ausfallzeiten auf ein Minimum reduziert werden können. Dank der intelligenten Konfiguration schaltet die Firewall automatisch in den Normalbetrieb zurück, sobald eine Störung behoben ist.

Siedl Networks hat die Herausforderung gemeistert – durch die neue State-of-the-Art Lösung ist die Koller International Group nun optimal geschützt und kann ihre Geschäftsprozesse ohne Sicherheitsbedenken fortsetzen.

Über Siedl Networks GmbH:

siedl networks
Enterprise Open Source Technology Solutions

Siedl Networks ist seit 2002 ein IT-Systemhaus aus Krems an der Donau und erbringt mit 16 Mitarbeitern IT-Dienstleistungen österreichweit für Unternehmen, Schulen und Non-Profit-Organisationen. Die Spezialisierung liegt bei Enterprise Open Source Systemen, welche nicht nur installiert und in Berieb genommen werden, sondern von Siedl Networks auch betreut und gewartet werden.

Website: www.siedl.net