

Skalierbarer Ansatz

Zentrale Infrastruktur für Fernwartung über Internet



Beitrag als PDF auf
www.AuD24.net

Fernwartung über Internet ist zukünftige Standardtechnik. Während kleine Szenarien mit wenigen Verbindungen leicht aufzubauen sind, erfordern skalierbare Lösungen für viele hundert Tunnel geeignete Konfigurationen und Produkte.

■ Lutz Jänicke



Dr. Lutz Jänicke

ist CTO bei Innominate Security Technologies in Berlin

T +49/30/921028-0

ljaenicke@innominate.com

Die traditionelle Fernwartung über Modem wird absehbar durch VPN-Verbindungen (Virtual Private Network) über Internet ersetzt. Für eine erfolgreiche Fernwartung über VPN ist die Appliance an der Maschine nur ein Teil des Puzzles. Das zentrale VPN-Gateway und die Managementlösung sind genauso wichtig. Dabei muss die verwendete Lösung mit der Zahl zu wartender Maschinen skalieren. Die Maximalzahl von Maschinen unter Wartung ergibt sich dabei aus der Zahl der Maschinen pro Jahr und der typischen Laufzeit von Wartungsverträgen. Es gilt also, auf die Fernwartung von hunderten oder tausenden Maschinen vorbereitet zu sein.

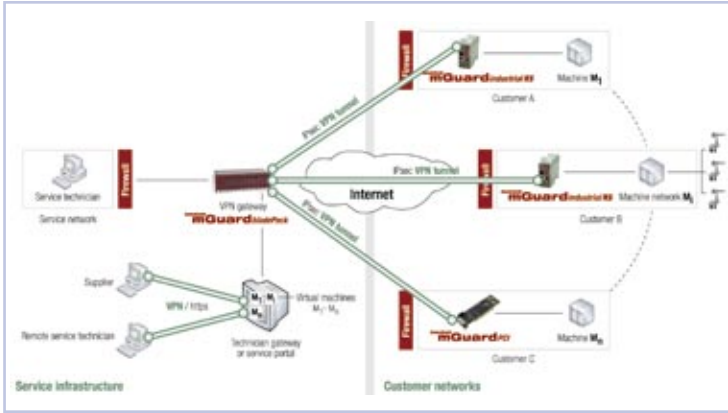
Fernwartung über Internet

Fernwartung über das Internet erfordert eine sichere Verbindung, wobei Verschlüsselung und Authentifikation durch VPN-Tunnel erzielt werden. Diese Tunnel werden zwischen dezentralen Appliances an den einzelnen Maschinen und dem zentralen Service-Gateway (meist im

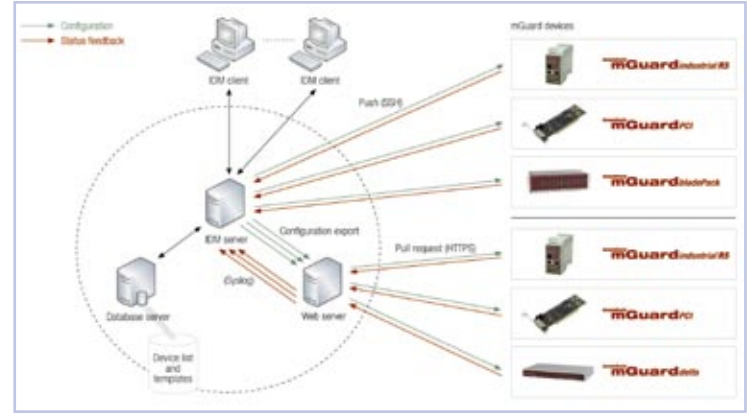
Rechen- oder Servicezentrum des Maschinenbauers) aufgebaut.

Für Angebote wie Predictive Maintenance oder Fernüberwachung müssen die VPN-Tunnel ständig aktiv sein. Werden sie nur im Fernwartungsfall aktiviert, muss nur eine kleine Zahl aktiver Tunnel gleichzeitig unterstützt werden, die Konfiguration einer großen Zahl von Tunneln muss aber möglich sein.

Bei der Konzeptionierung einer Fernwartungslösung mit VPN ist schon bei den ersten Planungsschritten der Endausbau zu berücksichtigen. Erfahrungen mit Modemlösungen lassen sich nicht sinnvoll übertragen. Es ergibt sich ein Wachstum der zu verwaltenden VPN-Verbindungen entsprechend der ausgelieferten Zahl von Maschinen. Ein Maschinenbauer, der 20 Systeme pro Monat ausliefert und Wartungsverträge über die ersten vier Jahre nach Auslieferung abschließt, muss also für etwa $20 \times 12 \times 4 \approx 1000$ Tunnel planen. Dabei muss nicht bereits zum Start die volle Tunnelzahl vorliegen, das Konzept sollte aber über entsprechende Skalierbarkeit verfügen. Viele Angebote im Markt sprechen den Kunden mit einer einfachen In-



Fernwartungsszenario mit zentralem Gateway und dezentralen Appliances



Auf Skalierung ausgelegte Architektur des Device Managers von Innominate

betriebsnahme des ersten Tunnels an. Sie bauen darauf, dass der Kunde später auch bei Skalierungsproblemen nicht mehr abspringt, wenn die ersten Systeme ausgerollt sind.

Skalierbares Konfigurationsmanagement

Im Idealfall werden die maschinenseitigen VPN-Appliances nach der Inbetriebnahme nie mehr umkonfiguriert. Bei einer Nutzungsdauer von mehreren Jahren sollte allerdings die Notwendigkeit von Konfigurationsänderungen eingeplant werden. Die meisten industriellen Lösungen werden über eine WEB-GUI konfiguriert. Änderungen an mehreren Appliances müssen dann durch manuelle Interaktion durchgeführt werden. Dies ist für bis zu etwa 20 Appliances umsetzbar, darüber hinaus wird ein zentrales Management-Tool benötigt. Im benannten Beispiel von etwa 1000 Systemen ergibt sich bei 1000 Konfigurationsvariablen pro System eine Menge von einer Million Parametern, welche bei 100 Byte pro Parameter eine Gesamtgröße von 100 MB haben.

Es könnten also im ungünstigsten Fall die Konfigurationen von 1000 Systemen gleichzeitig einer Änderung bedürfen. Da es sich dabei um eine systematische Änderung handeln würde, ist es sinnvoll, einen Template-basierten Ansatz zu verwenden, der aus einer oder wenigen Grundkonfigurationen die individuellen Konfigurationen ableitet. Muss eine Grundeinstellung geändert werden, erfolgt dies nur an einer Stelle. Die Änderung in den individuellen Konfigurationen und die Aktivierung auf den Zielsystemen übernimmt das zentrale Management. Entsprechend der großen Zahl von Systemen muss der Erfolg der Konfigurationsänderung zentral erfasst und gemeldet werden.

Tunnelaufbau und Identifikation

Bevor ein VPN-Tunnel aufgebaut wird, müssen sich die Kommunikationspartner gegensei-

tig authentifizieren. Stand der Technik ist dabei die Verwendung von Public-Key-Verfahren unter Verwendung von X.509-Zertifikaten. Das Zertifikat enthält dabei den öffentlichen Schlüssel zusammen mit Informationen über das System wie eine Geräteerkennung.

Während für eine kleine Installation die Verwaltung durch individuelle Konfiguration eines jeweiligen Zertifikats für einen Tunnel erfolgen kann, ist dies bei einer großen Installation nicht mehr sinnvoll. Die Verwendung einer Public Key Infrastructure mit Certificate Authority (CA) erlaubt die Konfiguration unter Verwendung spezifischer Zertifikatseinträge.

Der Device Manager von Innominate erlaubt nicht nur die Konfiguration der dezentralen Appliances, sondern konfiguriert auf Wunsch auch automatisch das zentrale Gateway mit den notwendigen Tunnelparametern. Noch einfacher ist die Verwendung von Tunnelgruppen, bei denen alle von einer CA ausgestellten Zertifikate akzeptiert werden. Dann muss nur noch ein Sammeltunnel konfiguriert werden, welcher hunderte echte Tunnel abdeckt.

Skalierbarkeit des zentralen Gateways

Zur Terminierung von 1000 VPN-Tunneln ist ein zentrales Gateway entsprechender Leitungsfähigkeit und eine entsprechende Bandbreite der Internet-Anbindung notwendig. Einmal aufgebaut, sind die Tunnel ohne Nutzdaten aktiv: Zur Erkennung von Verbindungsstörungen werden in kurzen Abständen Dead-Peer-Detection-Pakete verschickt, bei 1000 Tunneln sind dies etwa 10 Pakete pro Sekunde. Typischerweise einmal pro Stunde werden alle Sitzungsschlüssel erneuert, bei 1000 Tunneln also mindestens alle drei Sekunden ein neuer Schlüssel. Neben der Hardware-Performance ist hier insbesondere die Qualität der Software von Bedeutung. Sowohl die interne Struktur der verwendeten VPN-Applikationen als auch die Einbindung in die Steuerungs-Soft-

ware entscheiden über die Skalierbarkeit: Ungünstig geschachtelte Schleifen, welche n^2 folgen, bleiben meist unbemerkt und funktionieren sehr gut bei wenigen Tunneln, zerstören aber die Gesamtleistung bei sehr vielen Tunneln.

Nach Neustart des zentralen Gateways verbinden sich die dezentralen Appliances automatisch wieder mit der Zentrale. Es werden also extrem viele Tunnelanfragen in kurzer Zeit eintreffen. Das zentrale Gateway muss also über eine hohe Rechenleistung und über die Ablaufstrukturen zur Bewältigung dieser Belastung verfügen.

Speicherlecks in der Software erfordern besondere Beobachtung hinsichtlich der ständig vorhandenen Systemaktivität. Verliert eine Applikation etwa nur einige Byte pro Tunnel und Operation (DPD; Re-Keying), summiert sich dies sehr schnell zu großen Speicherbereichen auf, welche dann zu Funktionsstörungen führen können. Leider sind viele populäre OpenSource-Komponenten mit diesem Problem behaftet.

Mit dem mGuard centerport bietet Innominate eine leistungsfähige Hardware für mindestens 1000 VPN-Tunnel. Die x86-basierte Hardware verfügt über einen Mehrkernprozessor, welcher über ausreichende Leistungsreserven auch für große VPN-Installationen verfügt. Die neue Firmware mGuard 7.0 unterstützt die neue Hardware ebenso wie die bereits am Markt eingeführten Appliances. Ein besonderes Augenmerk wurde dabei auf die Skalierbarkeit gelegt.

Zusammenfassung

Zu einer vollständigen Fernwartungslösung für Maschinenbauer gehört weit mehr als eine VPN-Appliance für industrielle Umgebungen. Eine skalierbare Managementlösung und ein leistungsfähiges zentrales Gateway sind unverzichtbare Bestandteile des Gesamtkonzepts. ■

Weiterführende Infos auf AuD24.net:

more @ click **AD109911**