

Zentrale Infrastruktur ermöglicht die Fernwartung vieler Anlagen

Fernwartung über das Internet kann die zukünftige Standardtechnik werden. Zu einer Fernwartungslösung für Maschinenbauer gehört jedoch mehr als eine Kommunikationsschnittstelle: Eine skalierbare Managementlösung und eine zentrale Datenübergabestelle sind unverzichtbare Bestandteile des Gesamtkonzepts.

LUTZ JÄNICKE

Die traditionelle Fernwartung über Modem wird absehbar durch VPN-Verbindungen über das Internet ersetzt. Die große Zahl neu vorgestellter VPN-Router für Industrieanwendungen zeigt, dass der Markt in Bewegung ist. Für den erfolgreichen Einsatz von Fernwartung über VPN ist aber die VPN Appliance an der Maschine nur ein Teil des Puzzles. Das zentrale VPN-Gateway und die Managementlösung sind genauso wichtig für den Betrieb.

Die eingesetzte Fernwartungs-Lösung muss mit der Zahl zu wartender Maschinen korrelieren. Die maximale Zahl von Maschinen unter Wartung ergibt sich aus der Zahl der Maschinen pro Jahr und der typischen

Dr. Lutz Jänicke ist Chief Technology Officer bei der Innominate Security Technologies AG in 12489 Berlin, Tel. (0 30) 92 10 28-0, Fax (0 30) 92 10 28-0 20, contact@innominate.com

Laufzeit von Wartungsverträgen. Es gilt also, auf die Fernwartung von hunderten oder sogar tausenden Maschinen vorbereitet zu sein.

Fernwartung über das Internet erfordert eine sichere Verbindung, wobei Vertraulichkeit (Verschlüsselung) und Authentifikation durch VPN-Tunnel erzielt werden. Die VPN-Tunnel werden zwischen dezentralen Appliances wie dem Innominate Mguard an den einzelnen Maschinen und dem zentralen Servicegateway aufgebaut, das sich typischerweise im Rechen- oder Servicezentrum des Maschinenbauers befindet.

Für Angebote wie die vorbeugende Instandhaltung oder Fernüberwachung müssen die VPN-Tunnel ständig aktiv sein; teilweise werden sie auch nur deswegen ständig betrieben, um die Verfügbarkeit der Verbindung sicherzustellen. Werden die VPN-Tun-

nel 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 (Bild 1).

Bei der Konzeption einer Fernwartungslösung mit VPN ist schon bei den ersten Planungsschritten der Endausbau zu berücksichtigen. Die Erfahrungen mit schon vorhandenen Modemlösungen, von denen nur wenige gleichzeitig aktiv sind, lassen sich nicht sinnvoll übertragen.

Fernwartung reduziert die Kosten beim Maschinenbauer

Soll die Fernwartung zukünftig ausschließlich über VPN erfolgen, müssen alle ausgelieferten Systeme dies unterstützen. Es ergibt sich ein Wachstum der zu verwaltenden Verbindungen entsprechend der ausgelieferten

Die Fernwartung von Anlagen dient der Kostenreduktion. Erfolgt sie über das Internet, wird eine sichere Verbindung benötigt.



Bild: Innominate Security Technologies

Erläuterungen

Abkürzungen zur Netzwerktechnik

- ▶ VPN – Virtual Private Network: Kommunikationsschnittstelle in einem Netzwerk, die verschiedene Geräte aus ihrem ursprünglichen Netz heraus an ein benachbartes Netz bindet, ohne dass die beiden Netzwerke zueinander kompatibel sein müssen
- ▶ GUI – Graphical User Interface: Software-Komponente, die dem Benutzer eines Computers die Interaktion mit der Maschine über grafische Symbole ermöglicht
- ▶ PKI – Public Key Infrastructure: ein System, das digitale Zertifikate zur Absicherung rechnergestützter Kommunikation ausstellen, verteilen und prüfen kann
- ▶ CA – Certificate Authority: Bestandteil einer PKI, der digitale Zertifikate beglaubigt
- ▶ DPD – Dead Peer Detection: erkennt, ob eine IP-Sec-Verbindung unbeabsichtigt oder unvorhergesehen abgebrochen wurde, und sorgt für den automatischen Wiederaufbau im Fehlerfall
- ▶ X.509 – Standard für eine PKI
- ▶ IP-Sec – Internet Protocol Security: Sicherheitsprotokoll, das für die Kommunikation über IP-Netze die Schutzziele Vertraulichkeit, Authentizität und Integrität sicherstellen soll und zum Aufbau von VPN verwendet wird
- ▶ SA – Security Association: Vereinbarung zwischen zwei kommunizierenden Einheiten in Rechnernetzen, die beschreibt, wie die beiden Parteien die Sicherheitsdienste anwenden werden, um sicher miteinander kommunizieren zu können

Zahl von Maschinen. Die Fernwartung dient der Kostenreduktion beim Maschinenbauer (Gewährleistung) oder Betreiber und wird über mehrere Jahre benötigt. Ein Maschinenbauer, der 20 Systeme pro Monat ausliefert und Wartungsverträge über die ersten vier Jahre nach Auslieferung abschließt, muss also für etwa 1000 Tunnel planen. Dabei ist es nicht notwendig, bereits zum Start für die volle Tunnelzahl ausgestattet zu sein, das Konzept sollte aber die entsprechende Skalierbarkeit haben. Pilotprojekte sollten so ausgelegt sein, dass sie die Skalierbarkeit mit bewerten. Viele Angebote im Markt zielen darauf, den Kunden mit einer einfachen Inbetriebnahme des ersten Tunnels anzusprechen, und bauen darauf, dass der Kunde

dann später auch bei Skalierungsproblemen nicht mehr abspringen wird, wenn die ersten Systeme aufgebaut sind.

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 VPN-Appliances werden über eine Web-GUI konfiguriert. Änderungen an mehreren Appliances müssen dann durch manuelle Interaktion durchgeführt werden. Dies ist bei maximal 20 Appliances machbar, darüber hinaus wird ein zentrales Managementtool benötigt. Im genannten Beispiel von etwa 1000 Systemen

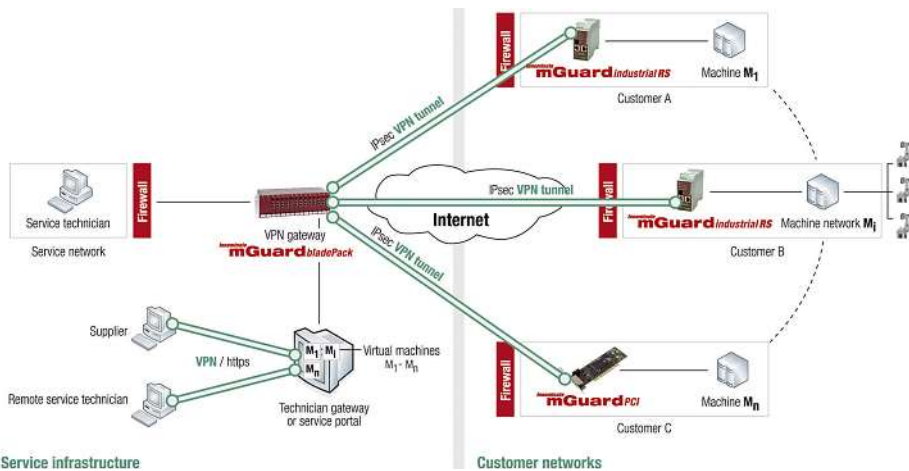


Bild 1: Die Abbildung zeigt ein Fernwartungsszenario mit zentralem Gateway und dezentralen Geräten. Für die Fernwartung oder die vorbeugende Instandhaltung muss die Möglichkeit bestehen, eine große Zahl von Tunneln zu konfigurieren.

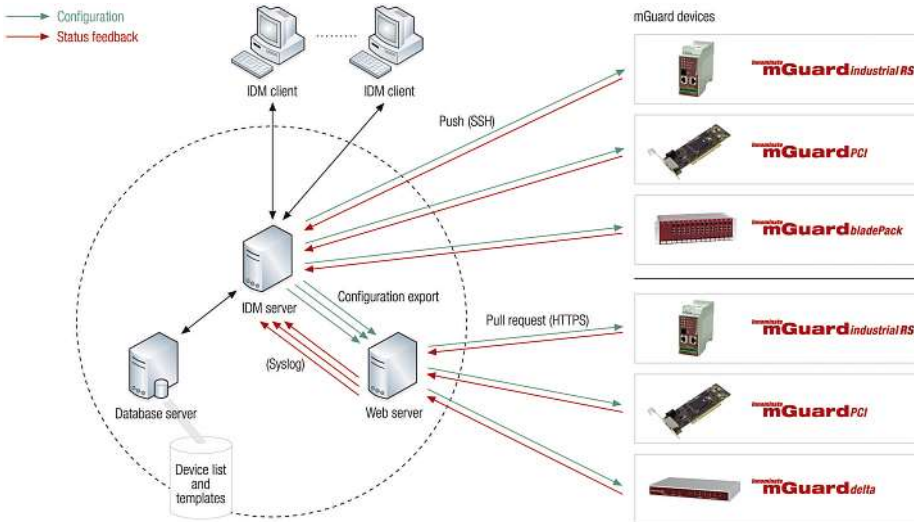


Bild 2: Die Architektur des Innominate Device Managers ist auf Skalierung ausgelegt.



Bild 3: Der Mguard Centerport mit Mehrkernprozessor hat ausreichend Leistungsreserven für große VPN-Installationen.

ergibt sich bei 1000 Konfigurationsvariablen pro System eine Menge von 1 Mio. Parametern, welche bei 100 Byte pro Parameter eine Gesamtgröße von 100 MByte haben. Es wird deutlich, dass ein entsprechendes Managementtool von Anfang an für große Datenbestände entwickelt worden sein muss, wie etwa der Innominate Device Manager (IDM) als Client-Server-Architektur mit einer relationalen Datenbank (Bild 2).

Beim oben genannten Beispiel eines Maschinenbauers könnten im ungünstigsten Fall die Konfigurationen von 1000 Systemen gleichzeitig einer Änderung bedürfen. Dabei wird es sich um eine systematische Änderung handeln.

Änderungen der Grundkonfiguration erfolgen nur an einer Stelle

Es erweist sich als sinnvoll, einen Template-basierten Ansatz zur Verfügung zu haben, welcher aus einer oder wenigen Grundkonfigurationen die individuellen Einstellungen ableitet. Muss eine Grundkonfiguration geändert werden, erfolgt dies nur an einer Stelle. Die Anwendung der Änderung in den individuellen Konfigurationen und die Aktivierung auf den Zielsystemen übernimmt dann das zentrale Management. Entspre-

chend der großen Zahl von Systemen muss der Erfolg der Konfigurationsänderung zentral erfasst und gemeldet werden.

Bevor ein VPN-Tunnel aufgebaut wird, müssen sich die Kommunikationspartner gegenseitig authentifizieren. Stand der Technik ist dabei die Verwendung von Public-Key-Verfahren unter Verwendung von X.509-Zertifikaten. Das Zertifikat enthält dabei den nicht geheimen, öffentlichen Schlüssel zusammen mit Informationen über das System.

Während für eine kleine Installation die Verwaltung der Tunnel durch individuelle Konfiguration eines jeweiligen Zertifikats für einen Tunnel erfolgen kann, ist dies bei einer großen Installation nicht mehr sinnvoll. Die Verwendung einer PKI mit CA ermöglicht die Konfiguration unter Verwendung spezifischer Zertifikatseinträge.

Der IDM ermöglicht 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, so dass nur noch ein „Sammeltunnel“ konfiguriert werden

muss, welcher für hunderte echte Tunnel reicht. Dabei entfällt aber die Möglichkeit, individuelle Firewall-Regeln für jeden Tunnel zu konfigurieren.

DPD-Funktion stellt die fehlerfreie Verbindung der Tunnel sicher

Zur Terminierung von 1000 VPN-Tunneln ist ein zentrales Gateway mit entsprechender Leitungsfähigkeit notwendig. Auch muss die Internet-Anbindung über eine entsprechende Bandbreite verfügen. Sind die Tunnel aufgebaut, sind sie ohne Nutzdaten aktiv: Zur Erkennung von Verbindungsstörungen werden in kurzen Abständen von beispielsweise 90 Sekunden DPD-Pakete verschickt, bei 1000 Tunneln sind dies etwa 10 Pakete pro Sekunde. Einmal pro Stunde werden in der Regel alle Sitzungsschlüssel erneuert, bei 1000 Tunneln also mindestens ein neuer Schlüssel alle 3 Sekunden.

Außer der Leistung der Hardware ist insbesondere die Qualität der Software von Bedeutung.

► Sowohl die interne Struktur der verwendeten VPN-Applikationen wie auch die Einbindung in die Steuerungssoftware entscheiden über die Skalierbarkeit: Ungünstig geschachtelte Schleifen bleiben meist unmerkelt und funktionieren sehr gut bei wenigen Tunneln, zerstören aber die Gesamtleistung bei sehr vielen Tunneln.

► Nach einem Neustart des zentralen Gateways verbinden sich die dezentralen Appliances automatisch wieder mit der Zentrale. Es werden also extrem viele Tunnelanfragen in kurzer Zeit eintreffen. Neben einer entsprechend hohen Rechenleistung muss das zentrale Gateway auch die Ablaufstrukturen haben, um diese Belastung zu bewältigen.

► Speicherlecks in der Software erfordern besondere Beobachtung hinsichtlich der ständig vorhandenen Systemaktivität. Verliert eine Applikation etwa nur einige Byte pro Tunnel und Operation, summiert sich das sehr schnell zu großen Speicherbereichen auf, welche nach einer absehbaren Zeit zu Funktionsstörungen und schließlich zum Absturz führen können.

Mit dem Mguard Centerport (Bild 3) ergänzt das Unternehmen sein Angebot um eine Hardware für mindestens 1000 VPN-Tunnel. Die x86-basierte Hardware mit Mehrkernprozessor hat genügend Leistungsreserven für große VPN-Installationen.

Die Firmware Mguard 7.0 unterstützt die neue Hardware ebenso wie die bereits am Markt eingeführten Appliances. Bei der Entwicklung wurde besonderes Augenmerk auf die Skalierbarkeit gelegt.

Bilder: Innominate Security Technologies