

Sonderdruck für Innominat

Geräte für sichere Industrienetze

Auswahlkriterien für den Router-Kauf

Die Sicherheit im industriellen Ethernet hängt stark von der eingesetzten Hardware ab. Welche Details bei der Anschaffung und beim Betrieb von Netzwerkequipment zu beachten sind, klärt der folgende Ratgeber.

Mit dem Einzug von Ethernet und TCP/IP in die industrielle Vernetzung reift auch das Bewusstsein für Verwundbarkeiten und Sicherheitsrisiken vernetzter Steuerungs- und Automatisierungssysteme. Industrial Network Security ist ein Wachstumsmarkt, für den das gängige Office-Equipment nicht taugt, und der ein entsprechend zunehmendes Angebot an industrietauglichen Produkten hervorbringt. Viele dieser als Firewall-, VPN- und Security-Router oder Network Security Appliance bezeichneten Geräte ähneln sich auf den ersten Blick. Dies verleitet schnell dazu, für eine Auswahl nur noch auf den Preis zu schauen. Doch Vorsicht: Der Teufel steckt im Detail und hier zusätzlich in der Frage nach leistungsfähigen Managementwerkzeugen. Es geht nicht darum, welches Produkt am

meisten kann, sondern welches exakt das liefert, was Kunden wirklich brauchen, und ihnen dafür eine „runde“ Lösung bietet.

Bauformen und Schnittstellen

Geräte zur Hutschienenmontage für den Einsatz im Schaltschrank mit 24V-Stromversorgung sind die bevorzugte und vorherrschende Bauform. Ein Gehäuse mit Schutzklasse IP 20 ist dabei meist ausreichend. Will man Security-Technik flexibel auch in Industrie-PCs integrieren oder im Netzverteilteraum zum Einsatz bringen, sollte man auf die Verfügbarkeit anderer Bauformen, also etwa PCI-Karten oder 19-Zoll-Chassis, achten. Zu bedenken ist auch, über welche Schnittstellen und Medien die internen Ethernet-Netzwerke der Maschinen oder Anlagen mit ex-

ternen Netzen kommunizieren sollen. Genügt die Einbindung über Ethernet in das umgebende LAN? Ist zur direkten Internetanbindung über ein DSL-Modem eine PPPoE-Unterstützung gefragt? Für schmalbandige Fern- oder Condition-Monitoring-Applikationen kommen auch serielle Wählverbindungen über Analogmodem und ISDN oder Mobilfunkverbindungen über GSM/GPRS in Betracht. Anspruchsvolleren Fernwartungsaufgaben werden diese in puncto Bandbreite und Antwortzeiten heute allerdings nicht mehr gerecht. Für diese sollte es schon eine Ethernet-basierende oder zumindest breitbandigere Mobilfunkverbindung (EDGE/UMTS/HSDPA) geben.

Netzwerkintegration und Routing

Häufiger Einsatzzweck von Routern ist die Anbindung von Maschinen und Anlagen an ein umgebendes Betreibernetz. Die Maskierung des internen Maschinennetzes durch Network Address Translation (NAT) und die Weiterleitung bestimmter Datenpakete durch Port-Forwarding gehören dabei zum Standardrepertoire. Weit weniger häufig zu finden, aber äußerst nützlich, ist das so genannte 1:1-NAT oder Virtual Mapping. Es erlaubt, Subnetze aus Anlagen mit identischem internem IP-Adressraum elegant auf eindeutige externe Adressen abzubilden, sodass sie über diese virtuellen Adressen von außen erreichbar werden.

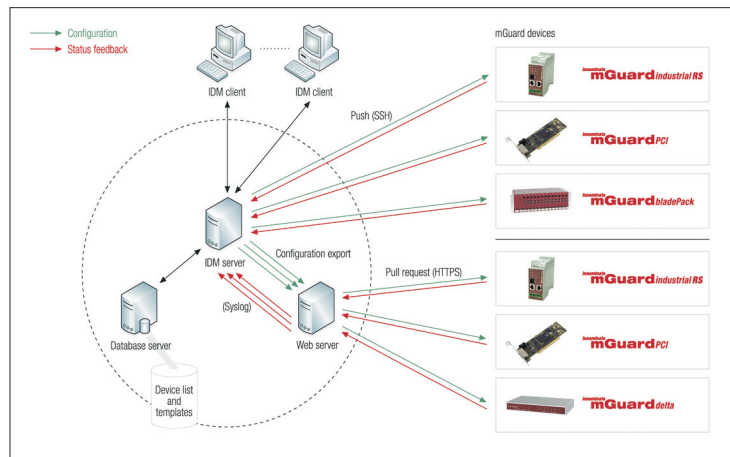
Falls dies relevant ist, gilt es auch darauf zu achten, dass sich zusätzliche interne und externe Routen in weitere Netze definieren lassen und VLANs (Virtual LANs) unterstützt werden. Zu prüfen ist ferner, ob benötigte Netzwerkdienste von den Geräten bereitgestellt werden: DHCP-Client und -Server zur dynamischen Konfiguration des Routers oder angebundener Hosts, DNS-Forwarding/Caching und lokale Auflösung von Host-Namen, DynDNS-Registrierung eines Host-Namens für dynamisch wechselnde externe IP-Adressen (etwa bei DSL) sowie NTP-Client und -Server für eine synchronisierte Systemzeit.

Firewall-Sicherheit und Performance

Wichtigstes Sicherheitsinstrument zur Kontrolle und Beschränkung des Netzwerkverkehrs auf zulässige Verbindungen ist die in einer Appliance integrierte Firewall. Einfache Paketfilter sind dafür längst nicht mehr Stand der Technik. Den stellen so genannte Stateful Inspection Firewalls dar, die auch die zulässige Richtung der Initialisierung von Verbindungen überwachen und Antwortpakete automatisch bestehenden Verbindungen zuordnen können (Connection Tracking). Die Firewall sollte ferner grundlegende Schutzmechanismen gegen IP Spoofing, SYN Flooding und Denial-of-Service-(DoS-)Angriffe aufweisen. Besonders wenn es gilt, Sicherheit in bestehende Systeme und Netze nachzurüsten, ohne eine weitere Segmentierung einzuführen und damit zur Rekonfiguration der Systeme gezwungen zu sein, ist es wichtig, dass die Security-Appliances nicht nur als Router, sondern auch in transparenten Stealth oder Bridge Modes betrieben werden können. Im Idealfall ist zum Management der Geräte dabei nicht einmal eine eigene IP-Adresse nötig, sondern jene übernehmen stattdessen automatisch die Netzwerkidentität (MAC- und IP-Adresse) des geschützten Systems. Neben derart flexiblen Appliances sind auch solche auf dem Markt, die ausschließlich als Router oder nur als Bridge fungieren können. Sehr nützlich ist bisweilen auch eine User Firewall, die bestimmte Verbindungen nur

für definierte Benutzer nach deren vorheriger Authentisierung freischaltet. Ein Beispiel hierfür sind Techniker, die sich per Notebook an ein LAN anschließen und dort per DHCP eine dynamisch wechselnde IP-Adresse erhalten, um dann mit einer Projektierungssoftware an der Programmierung

VPN-Verfahren mit breiter Unterstützung durch kommerzielle Hersteller und die Open-Source-Community. IPSec ist im Kern eines jeweiligen Betriebssystems wie zum Beispiel Linux implementiert. Sofern CPU-seitig verfügbar, kommt es dadurch in den Genuss einer hardwarebeschleunigten



Device-Management: Die Fähigkeit zum effizienten zentralen Management verbunden mit gezielter Delegation von administrativen Rechten an lokales Personal (im Bild die Architektur des Device Managers für Mguard-Geräte von Innominate) ist der Schlüssel zum erfolgreichen Rollout großer Mengen von Security-Appliances.

von Steuerungen zu arbeiten, die sich hinter Security Appliances in geschützten Produktionszellen befinden. Der Zugriff auf die Projektierungs-Ports der Steuerungen bleibt so autorisierten Personen vorbehalten. Nicht zuletzt sollte man ein Auge auf die zugesicherte Leistung der Geräte werfen. Gerade Produkte im unteren Preissegment basieren häufig auf schwächeren Prozessoren, mit denen sie nur einen Datendurchsatz von wenigen MBit/s erreichen und die so schnell zum Flaschenhals im Netzwerk werden. Gute Security-Router leisten als Firewall bidirektional „Wire Speed“, also 2 x 99 MBit/s in einem 100-MBit/s-Ethernet-Netzwerk.

VPNs für den Internet-Teleservice

Sicherheit für Ferndiagnose, Fernwartung und Condition Monitoring von Maschinen und Anlagen über das Internet ist heute das häufigste Motiv für den Einsatz von Network Security Appliances. Dazu dienen Virtual Private Networks (VPNs), die durch Verschlüsselungstechnik die Authentisierung, Vertraulichkeit und Integrität des Datenverkehrs gewährleisten. Die Security-Architektur IPSec ist das heute weltweit mit Abstand meistgenutzte

Verschlüsselung und erreicht so eine gut zehnmal höhere VPN-Leistung als reine Softwarelösungen. Stand der Technik bei Verschlüsselung mit auf absehbare Zeit ausreichender Sicherheit sind die Verfahren 3DES und AES-256. Für den VPN-Zugriff entscheidend sind der IPSec Tunnel Mode und die Unterstützung von NAT Traversal (NAT-T), weil meist zwei Subnetze (nicht nur einzelne Knoten) über ein VPN verknüpft sein sollen, die sich wiederum selbst hinter weiteren Firewall-/NAT-Gateways befinden, also etwa ein Maschinennetz mit dem Netz eines Remote-Service-Centers. Nützlich sind ferner IKE-Fragmentation-Support, um auch über „schlechte“ Internetstrecken mit UDP-Fragmentverlusten zuverlässig Verbindung zu bekommen, sowie eine Dead Peer Detection (DPD) und Überwachung von VPN-Gegenstellen mit DynDNS-Host-Namen, um nach Unterbrechung oder Wechsel der IP-Adresse eine Verbindung automatisch wiederherzustellen. Zunehmend finden sich auf dem Markt auch Geräte, die eine OpenVPN-Implementierung nutzen. Anders als IPSec läuft diese quelloffene Software nicht im Kernel, sondern im User Space des Betriebssystems, was sie für einen Hersteller leichter

auf seine Plattform portierbar macht, ihr aber die Performance-Vorteile hardwarebeschleunigter Verschlüsselung vorenthält. Dies wird besonders für die Skalierbarkeit einer zentralen Gegenstelle schnell zum Problem. Außerdem ist OpenVPN im Gegensatz zu IPSec kein Internetstandard.

Ferner gibt es noch Lösungen mit SSH/SSL-Tunnelung. Diese stellen keine VPN-Kopplung von IP-Netzen her. Vielmehr muss die Tunnelung für jede benötigte Verbindung einzeln konfiguriert werden und ist auf TCP-Protokolle mit statischen Ports beschränkt. UDP-basierende Dienste wie die IP-Telefonie (VoIP) oder Video-Streaming lassen sich damit also nicht übertragen.

Zur Authentisierung der VPN-Partner sollten bevorzugt digitale Zertifikate anstelle von Preshared Keys verwendet werden. Man sollte darauf achten, dass die Geräte eine vollwertige Unterstützung für eine Public-Key-Infrastruktur (PKI) bieten und eine Managementsoftware verfügbar ist, die den sonst eher mühsamen Umgang mit Certificate Authorities (CAs) und Zertifikaten komfortabel erleichtert.

Besondere Aufmerksamkeit verdient erneut das Thema Nachrüstung: Fast alle heute marktgängigen Security-Appliances unterstützen VPNs nur im Router-Betrieb. Gilt es, eine sichere Fernwartbarkeit über das Internet gewissermaßen in eine bestehende Anlage nachzurüsten, gelingt dies transparent für das umgebende Netzwerk nur mit einer Appliance, die auch im Stealth- oder Bridge-Modus VPN-Verbindungen etablieren kann. Zu achten ist zudem darauf, dass die Appliance Firewall-Regeln auch innerhalb von VPN-Tunneln anwenden kann.

Manche Fernwartungs-Router sind nur für Punkt-zu-Punkt-VPN-Verbindungen vom einzelnen Technikerarbeitsplatz zu einer einzelnen Maschine gedacht oder geeignet. Dies ist kaum noch zeitgemäß: Verbindungsdaten zu jeder Maschine müssen beim Techniker lokal vorgehalten und ihm damit bekannt gemacht werden und die Maschinen über öffentliche IP-Adressen erreichbar sein. Sinnvoller ist die Anbindung der Maschinen über ausgehende VPN-Verbindungen zu einem zentralen

Service-Gateway oder Serviceportal. Praktisch unverzichtbar ist dazu die Fähigkeit, das oben beschriebene 1:1-NAT auch in VPN-Tunneln anwenden zu können. Nur so lassen sich Maschinen bei einer Vielzahl von Kunden mit real gleichem oder überlappendem Adressraum aus Sicht der Servicezentrale über eindeutige (virtuelle) Adressen ansprechen. Ferner sollte die Appliance über einfache Softwareschnittstellen und/oder digitale I/Os zum Schalten und Überwachen von VPN-Verbindungen verfügen, da fast alle Betreiber die Kontrolle über Teleserviceverbindungen an ihrem Ende behalten wollen.

Sollen verschiedene Dienste zeitgleich über eine Fernverbindung mit begrenzter Bandbreite genutzt werden, erweisen sich QoS-Funktionen (Quality of Service) als nützliche Helfer. Ihr Bandbreitenmanagement kann zum Beispiel dafür sorgen, dass ein VoIP-Telefonat verständlich und die Antwortzeiten beim Remote Desktop Sharing akzeptabel bleiben, während sich ein File-Transfer im Hintergrund mit der verfügbaren Restbandbreite begnügen muss.

Device-Management und Monitoring

Wer plant, mehr als 100 Security-Appliances einzurichten und zu betreiben, für den kommt jetzt der wichtigste Abschnitt: Es gilt nämlich, diesen Zoo von kleinen, aber komplexen Geräten zu beherrschen, ohne dass einem der Aufwand dafür über den Kopf wächst.

Zunächst sollte es möglich sein, Einzelgeräte ohne spezielle weitere Hilfsmittel in Betrieb zu nehmen. Dies geschieht meist über eine integrierte Weboberfläche (Web-GUI). Um den Rollout oder das Konfigurations-Update von Geräten etwa durch Skripte automatisieren zu können, sollte ferner ein umfassendes Command Line Interface (CLI) zur Verfügung stehen. Diese Zugänge sollten sichere Benutzerauthentisierungen und Protokolle verwenden (HTTPS statt HTTP, SSH anstelle von Telnet, optional mit Zertifikaten) und sich auf definierte Netze beschränken lassen. Eine Security-Appliance, die ungesichert administriert werden kann,

ist nichts wert. Hilfreich ist es ferner, Konfigurationsprofile vom und zum Gerät laden, dort speichern und wieder aktivieren zu können, besonders auch ein gegenüber den Werkseinstellungen kundenspezifisch anpassbares Grundprofil.

Verfügt das Security-System über ein effizientes zentrales Management, sollte damit auch ein Rollout großer Mengen von Security-Appliances ohne große Probleme möglich sein. Das Managementsystem stellt dafür zum Beispiel Konfigurationsvorlagen zur Verfügung, die sich hierarchisch strukturieren und auf Geräte vererben lassen, und steigert damit die Produktivität bei Inbetriebnahme und Pflege der Geräte enorm. Ein Rollen- und Rechtemodell sollte erlauben, ganz bestimmte Parameter von einem Techniker vor Ort noch lokal auf dem Gerät einstellen zu lassen (zum Beispiel externe Router-IP-Adresse, Netzmaske und Default Gateway, die vom Kunden erst in letzter Minute bereitgestellt werden), ohne dass sicherheitsrelevante, zentral vorgenommene Einstellungen dabei manipuliert werden können. Ein Firmware-Update der Geräte sollte inkrementell und über das Netz im laufenden Betrieb möglich sein.

Im Fernwartungskontext ist es typischerweise nicht möglich, Konfigurationen vom zentralen Management auf hinter Kunden-Firewalls liegende Geräte aufzuspielen (Push-Verfahren). Die Geräte müssen diese dann vielmehr selbst, etwa über HTTPS und gegebenenfalls Proxy-Server, bei einem zentralen Server abrufen können (Pull-Verfahren) und auch über VPN administrierbar sein.

Ist eine Einbindung der Geräte in Netzwerkmanagement- und -Monitoring-Systeme beabsichtigt, sollten sie SNMP in der sicheren Version 3 unterstützen, lesend und schreibend mit umfassender Management Information Base (MIB), sowie SNMP Traps und Syslog-Meldungen für relevante System- und Firewall-Ereignisse an einen zentralen Server schicken können.

Torsten Rössel/jos

Torsten Rössel ist Director Business Development bei Innominate Security Technologies.