Excellence in Digital Security.

genua.

genubox

Hochsichere Fernwartungslösung

Technische Informationen

Inhalt

1. genubox: hochsichere Fernwartungslösung mit breitem Einsatzspektrum

Diese Informationsbroschüre richtet sich an Personen und Unternehmen, die sich mit der Fernwartung beliebiger Systeme beschäftigen, wie Betriebstechniker, Maschinenbauer und Systemintegratoren.

Sie bietet Ihnen einen kompakten Überblick, wie Sie mit Hilfe der Fernwartungslösung genubox umfangreiche Fernwartungsdienste ermöglichen können und dabei gleichzeitig das Netzwerk des Anlagenbetreibers zuverlässig schützen.

1.1. Problemstellung

Zeit ist Geld. Dabei spielt es keine Rolle, ob es sich um zu berechnende Anfahrtskosten eines Service-Teams oder um die Arbeitsunterbrechung im Unternehmen handelt. Ein Maschinenstillstand in der Produktion oder ein Ausfall von Serversystemen verursacht erhebliche Probleme und muss unbedingt vermieden werden. Mit typischen Industrieprotokollen wie z. B. S7 von Siemens lassen sich beispielsweise Industrieanlagen ständig überwachen. Probleme können so schnell erkannt und behoben werden, um Ausfallzeiten zu vermeiden oder möglichst kurz zu halten.

Vertreibt ein Hersteller seine wartungsintensiven Industrieanlagen, Fertigungsmaschinen oder Antriebssysteme weltweit, sind Fernwartungsmöglichkeiten via Internet aus diesem Grund meist implementiert. Damit sind Informationen über den Zustand der Anlage rund um die Uhr abrufbar und Fernzugriffe durch das Service Center des Herstellers grundsätzlich jederzeit möglich.

Allerdings muss für die Fernwartung das IT-Netz des Kunden gegenüber dem Wartungsunternehmen teilweise geöffnet werden. Diese Öffnung kann generell nicht vermieden werden, sollte aber aus Sicherheitsgründen so gering wie möglich ausfallen. Hier stoßen die üblichen Implementierungen des Fernwartungszugriffs häufig auf Bedenken des Kunden, da sie unnötig große Teile des IT-Netzes offenlegen. Zudem sind Identifizierung und Authentisierung des zugreifenden Dienstleisters meist unzureichend gelöst.

Ein weiterer kritischer Punkt sind fehlende Kontrollmöglichkeiten: Ein Fernwartungskunde möchte nachvollziehen können, welche Arbeiten ein Dienstleister am Fernwartungsobjekt durchführt.

Nicht zuletzt befürchten Unternehmen, dass Fernwartung Produktionsprozesse komplizierter gestaltet und spezialisiertes IT-Personal zur Betreuung der Lösung benötigt wird.

1.2. Möglichkeiten und Grenzen herkömmlicher Fernwartungsverfahren

In diesem Abschnitt betrachten wir unterschiedliche Lösungen zur Öffnung eines IT-Netzes für Fremdzugriffe und zeigen deren Vor- und Nachteile auf.

1.2.1. Öffnung der Firewall oder Zugriff per Modem/ISDN

Um den Fernwartungszugriff zu ermöglichen, öffnet der Kunde die Firewall für die Absender-IP-Adresse des Fernwarters und die Ziel-IP-Adresse des Wartungsobjektes. Weitgehend analog dazu kann auch ein Zugriffsweg per Modem oder ISDN an der Firewall vorbei eingerichtet werden.

Diese Standardlösung birgt folgende Risikofaktoren:

1. Es gibt keine Authentifizierung des Fernwarters und keine Prüfung der Autorisierung des Zugriffs. Damit besteht die Gefahr des Zugriffs durch Drittparteien, insbesondere wenn die Öffnung der Firewall nach Abschluss der Arbeiten unbeabsichtigt länger als nötig bestehen bleibt.
2. Der Fernwartungszugriff kann abgehört und gegebenenfalls durch Angreifer übernommen werden.
3. Eventuell vorhandene Implementierungsfehler in der Firewall können einen direkten Zugriff auf andere Bereiche des Kundennetzes ermöglichen.
4. Es existiert keine Trennung auf Netzebene.
5. Durch fehlende Aufzeichnung bzw. unzureichende Protokollierung des Zugriffs können der Wartungsvorgang und mögliche Probleme im Nachhinein nicht nachvollzogen werden.
6. Ohne die Möglichkeit, die Einwahl nur nach Absprache freizugeben, besteht bei Fehlfunktion der Haupt-Firewall eine permanente Gefährdung der Netzwerksicherheit.

1.2.2. Zugriff via VPN

Gelegentlich wird vorgeschlagen, den Fernwartungszugriff durch das VPN-Protokoll IPsec abzusichern. Dadurch werden tatsächlich die Risikofaktoren 1 und 2 behoben.

Allerdings birgt diese Methode ein neues Risiko: Da IPsec einen vollkommen transparenten und gerouteten Netzzugriff implementiert, besteht jetzt die Möglichkeit, dass die IT-Netze verschiedener Kunden, die gleichzeitig über IPsec gewartet werden, unbeabsichtigt miteinander kommunizieren können. Angesichts der Spezialisierung von Wartungsunternehmen auf branchentypische Systeme besteht die reale Gefahr, dass dabei Netze konkurrierender Unternehmen miteinander in Kontakt geraten und auf diese Weise auch unberechtigte Personen Zugriff auf die War-

tungsobjekte erhalten können. Aus diesem Grund ist es wichtig bei einer Fernwartungslösung darauf zu achten, dass es nicht zu einer Netzkopplung kommt.

2. Die Lösung: Sichere Fernwartungszugriffe mit genubox

Die Fernwartungslösung genubox basiert auf dem flexiblen und hochsicheren Betriebssystem OpenBSD. Dieses verfügt über einen auf Sicherheit optimierten TCP/IP-Stack, Routing-Funktionen, Paketfilter, Authentisierungsmethoden sowie umfangreiche kryptografische Funktionen. Im Folgenden erfahren Sie, wie diese wirkungsvoll zur Absicherung eines Fernwartungszugriffs eingesetzt werden können.

Die Fernwartungslösung genubox auf Industrie-Hardware

2.1. genubox als Rendezvous Server und Application Level Gateway

Durch den Einsatz zuverlässiger Methoden zur Verschlüsselung, Authentifizierung und Autorisierung werden die Risikofaktoren 1 und 2 ausgeschlossen. Gegenüber dem im vorstehenden Abschnitt genannten IPsec-Verfahren bietet es den Vorteil einer flexibleren und individuelleren Identifizierung des Fernwarters. Die Gefahr einer unerwünschten Kopplung verschiedener Kundennetze wird vermieden, da SSH nur die benötigten Applikationen und nicht ganze Netze verbindet (Eliminierung Risikofaktor 4).

Durch die zusätzliche Filterfunktion wird das Kundennetz in zwei Bereiche unterteilt. Dabei ist der eine Bereich mit dem Wartungsobjekt für den Fernwarter erreichbar, während für ihn das restliche Kundennetz nicht zugänglich ist. Dabei ist vorteilhaft, dass die Filterung auch auf OSI-Schicht 2 (im Bridging-Modus) erfolgen kann. Bei der üblichen Filterung auf OSI-Schicht 3 (im Routing-Modus) wäre zusätzlich eine Restrukturierung des Kundennetzes in zwei eigenständige Subnetze erforderlich, die durch den Bridging-Modus vermieden wird. Eine Filterfunktion auf OSI-Schicht 3 ist aber auch jederzeit möglich.

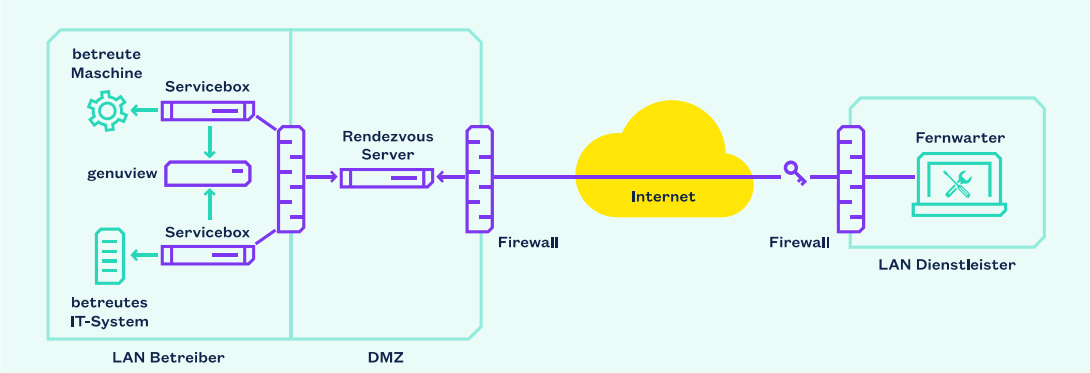
Der Fernwarter baut zunächst einen SSH-Tunnel zu genubox auf und wird dort authentisiert. Durch den Tunnel kann er dann mit beliebigen TCP-basierten Anwendungen auf das Wartungsobjekt zugreifen.

genubox bietet darüber hinaus die Leistung eines vollständigen Industrial Firewall-Systems. Dessen Paketfilter-Funktion wird so konfiguriert, dass bestehende Zugriffsmöglichkeiten anderer Kundensysteme auf das Wartungsobjekt nicht beeinträchtigt werden. Dagegen unterbindet der Filter unerlaubte Verbindungen, die der Fernwarter wissentlich oder unwissentlich vom Wartungsobjekt zu anderen Kundensystemen aufzubauen versucht. Damit beschränkt sich die Gefährdung durch den Fernwartungszugriff auf den Bereich des Wartungsobjekts (Eliminierung Risikofaktor 3).

genua folgt der BSI-Empfehlung für sichere Fernwartung und bietet auf der Servicebox ein Application Level Gateway für Remote-Desktop- und SSH-Zielsystem-Zugriffe an. Dadurch gibt es auch auf Applikationsebene keine durchgehende Datenverbindung vom Fernwarter zum Zielsystem. Das Application Level Gateway agiert als Vermittler zum Zielsystem.

2.2. Einrichtung einer Rendezvous-Lösung

Als Restrisiko bleibt eine Gefährdung des Kundennetzes nur beim Vorliegen einer Fehlfunktion der Haupt-Firewall. Dieses kann schließlich vermieden werden, indem eine direkte Einwahl des Fernwarters in das Kundennetz unterbunden wird (Eliminierung Risikofaktor 6).



Rendezvous in der DMZ als sichere Lösung

Stattdessen wird ihm lediglich die Verbindung zu einem Rendezvous-Server erlaubt, der in der Cloud oder einer Demilitarisierten Zone (DMZ) neben der Haupt-Firewall steht.

Damit

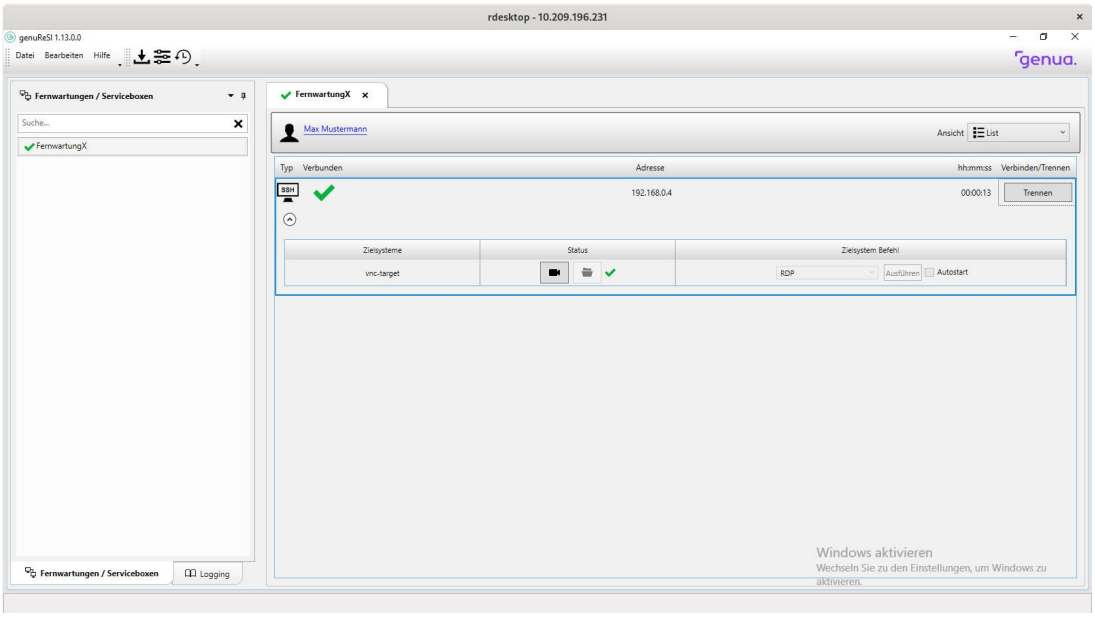
- entscheidet der Operator, ob der Wartungszugriff erlaubt wird oder nicht
- ist die vollständige Kontrolle des Wartungszugriffs gewährleistet

Zusätzlich wird er Fernzugriff protokolliert. genubox bietet zudem die Möglichkeit einer Video-Aufzeichnung und Live-Übertragung des Wartungsvorgangs (Eliminierung Risikofaktor 5).

Fazit: genubox bietet zusammen mit einem Rendezvous-Server maximale Kontrolle und Sicherheit für Fernwartungslösungen. Dabei bedarf es keinerlei Anpassungen der Firewall oder anderer Systeme im Kundennetz.

2.3. Hoher Komfort durch Fernwartungs-App

Mit Hilfe der Fernwartungs-App wird ein hochsicherer Fernwartungszugriff so einfach und komfortabel wie nie zuvor: Die Fernwartungs-App ist eine Windows-Anwendung, die es sowohl dem Fernwarter als auch dem Kunden (Operator/Maschinenführer/Maschinen-Administrator) ermöglicht, mit einigen wenigen Mausklicks Fernwartungsbeziehungen (Konfigurationen) zu verwalten und mit einem Mausklick zu starten und zu beenden.



Die Fernwartungs-App von genua für einfache Bedienung

Die Fernwartungs-App steht auf unserer Website zum kostenlosen Download zur Verfügung. Sie bedarf zum Betrieb auf einem Windows-Rechner lediglich Nutzerrechte und kann somit problemlos verwendet werden. Die einzelne Fernwartungskonfiguration wird zentral auf der Central Management Station genucenter erzeugt und verschlüsselt und lässt sich per API Call auslesen, um z. B. via E-Mail versendet zu werden. Spätere Änderungen am zentralen Management, wie z. B. ein neues Wartungsobjekt, werden automatisch von der App übernommen. Damit ist diese Lösung sehr wartungsarm: Der Fernwarter muss lediglich diese Konfiguration in seiner App öffnen und ist bereit zur Fernwartung.

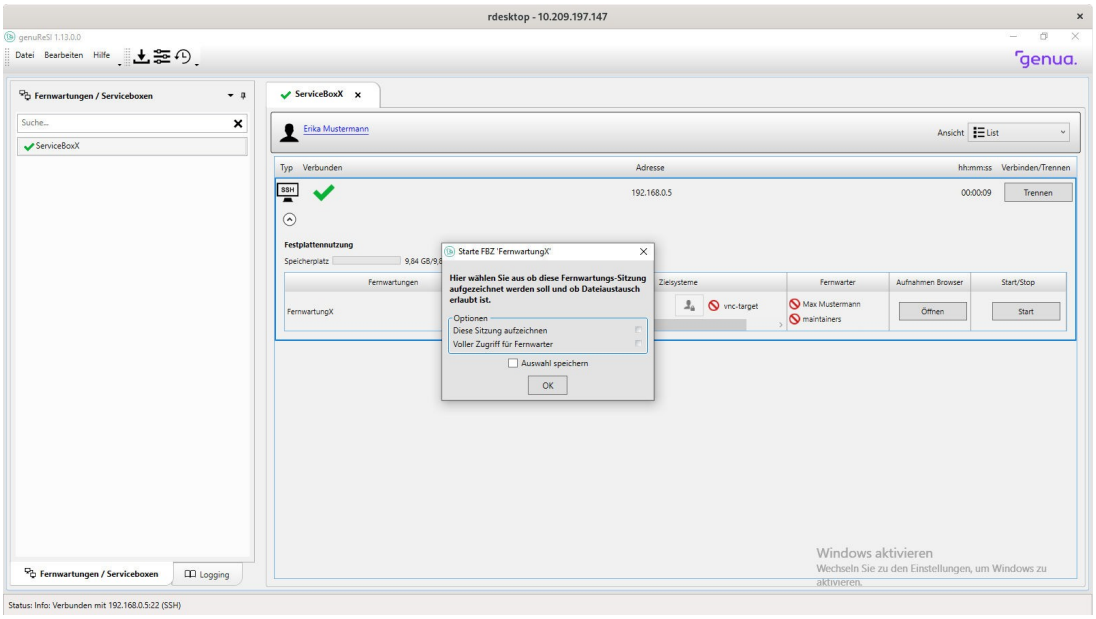
2.4. Webbrowser-basierte Fernwartung

Zusätzlich zur Windows App bietet die Rendezvous-Lösung jetzt die Möglichkeit der Fernwartung per Standard-Webbrowser. So können Service-Mitarbeiter eine Wartungsverbindung flexibel mit allen gängigen Endgeräten wie z. B. Windows-/Linux-PC, Apple MacBook oder Tablet initiieren.

Durch die plattformunabhängige Lösung per Standard-Webbrowser ist die Kompatibilität sichergestellt und die Aktualität der zugrundeliegenden Anwendung durch System-Updates stets gewährleistet. Die Bedienung ist benutzerfreundlich gestaltet und setzt kein technisches Fachwissen voraus. Für die sichere Verbindung zwischen Service-Mitarbeiter und Rendezvous Server sorgt eine Zwei-Faktor-Authentifizierung sowie eine geschützte Datenübertragung per Hypertext Transfer Protocol Secure (HTTPS).

2.5. Nachvollziehbarkeit durch Aufzeichnung und Monitoring

Um zusätzliche Sicherheit sowie die Nachvollziehbarkeit des Fernwartungszugriffes zu gewährleisten, kann genubox sämtliche Fernwartungszugriffe aufzeichnen und/oder live übertragen.



Mit der Fernwartungs-App einfach per Mausklick Fernwartungszugriffe aufzeichnen

Dabei kann der Operator den Zugriff durch den Fernwarter auch auf bestimmte Aktionen einschränken. Sowohl Operator als auch Fernwarter verwenden die komfortable Fernwartungs-App unter Windows. Fernwartungs-Sessions, z. B. via RDP,

VNC oder SSH werden für den Anlagenbetreiber als Video auf der genubox hinterlegt.

2.6. Option: genuview

genua bietet mit genuview zusätzlich eine Access- und Storage-Management-Lösung für Remote-Desktop-Aufzeichnungen an.

Nach erfolgtem Fernwartungszugriff wird die Aufzeichnung im Raw-Format unkomprimiert an einen genuview-Server weitergeleitet und dort speichersparend archiviert. Der Zugriff auf die Aufzeichnungen kann über ein zentrales Rechte-Managementsystem komfortabel verwaltet werden.

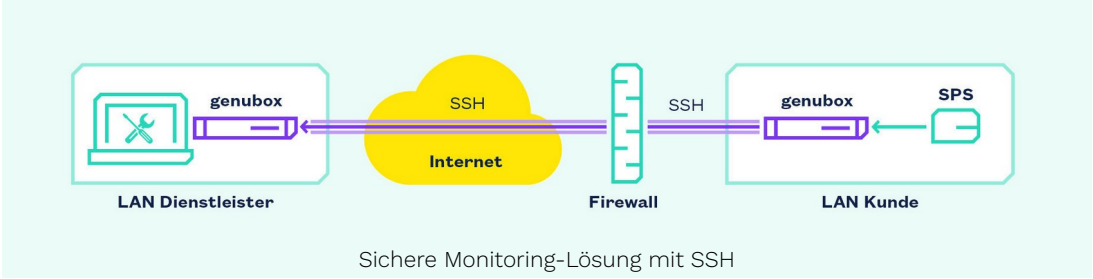
2.7. Option: Fernzugriff mittels L2TP-IPsec-VPN

Neben einer ausschließlichen Verwendung von SSH kann – alternativ oder parallel – die Verbindung zwischen Dienstleister und Rendezvous Server über ein L2TP-IPsec-VPN erfolgen, während das Zielsystem im LAN des Kunden wie gehabt nur über den SSH-Tunnel der Servicebox erreichbar ist. Dabei werden nur zulässige Pakete von der integrierten Firewall des Rendezvous Servers in den SSH-Tunnel weitergereicht. Wie in der oben beschriebenen Lösung ist eine Netzkopplung ausgeschlossen und der Kunde behält weiterhin volle Zugriffskontrolle.

Ein weiterer Vorteil ergibt sich für den Dienstleister aus einer vereinfachten Konfiguration des VPNs: Die Notwendigkeit von Hilfsprogrammen wie PuTTY entfällt, da L2TP-IPsec-VPN von den meisten aktuellen Betriebssystemen wie Windows (ab XP), Mac OS X sowie iOS (iPhone, iPad) und Android nativ unterstützt wird. Auch für Linux sind passende Clients verfügbar. L2TP wird ebenfalls durch die Fernwartungs-App von genua unterstützt.

2.8. Fernzugriff mittels SSH-VPN

Der Fernzugriff mittels SSH-VPN ist ein weiteres typisches Einsatzszenario von genubox.



Sichere Monitoring-Lösung mit SSH

Diese Lösung kommt beispielsweise zum Einsatz, wenn Industrieanlagen permanent Sensordaten zur Auswertung an einen Leitstand senden sollen. Dabei sorgt

eine genubox beim Anlagenbetreiber und eine genubox beim Dienstleister bzw. Anlagenhersteller für Datensicherheit. Aufgrund der permanenten Übertragung kommt bei dieser Monitoring-Lösung kein Rendezvous-Server zum Einsatz.

3. genubox im Überblick

Die Möglichkeiten der Fernwartungslösung genubox gehen weit über die einer herkömmlichen VPN-Lösung hinaus. Sie bietet neben kryptografischen Grundfunktionen (Basismodul) eine Anwendungsplattform (Applikationsmodul), auf der eine für den jeweiligen Einsatz passende Anwendung integriert werden kann. Aufgrund verschiedener Schnittstellen sowie flexibler Kommunikationsmöglichkeiten ist genubox für alle Einsatzfelder geeignet.

3.1. Das Basismodul

3.1.1. Krypto-Tunnel für TCP-Sessions

Zwischen genuboxen oder zwischen genubox und Application Server lassen sich Verschlüsselungstechniken auf verschiedenen Netzwerkebenen realisieren. Diese können so genannte Remote Bridges zur verschlüsselten Kopplung von zwei Teilnetzbereichen (Layer 2), IPsec-Gateways zur Verschlüsselung von IP-Paketen (Layer 3) oder dienstspezifische Tunnel mittels SSH oder SSL (Layer 4) sein.

Zur Verschlüsselung werden ausschließlich starke Algorithmen verwendet. Insbesondere durch den Einsatz von Applikations-Tunnels für TCP-Verbindungen können genuboxen in undefinierten IP-Umgebungen eingesetzt werden, z. B. für Dial-Up- und DSL-Zugänge oder hinter Firewalls und NAT-Routern. Damit lassen sich auch Zugänge zu privaten Adressbereichen realisieren, die durch Proxys oder NAT-Router abgetrennt sind – selbst wenn mehrere solcher Bereiche identische IP-Adressen benutzen.

3.1.2. Industrial Firewall im Bridging Mode

genubox verfügt über eine leistungsfähige Stateful Industrial Firewall, mit der alle Verbindungen, die über die genubox vermittelt oder von ihr verarbeitet werden, bis zum OSI-Layer 4 überwacht werden können. Da genubox sowohl Routing (Layer 3) als auch Bridging (Layer 2) beherrscht, lassen sich diese Sicherheitsfunktionen auf beiden Ebenen nutzen. So kann genubox im Falle von Bridging als unsichtbare Firewall zur Abtrennung eines Systems oder ganzen Netzwerks eingesetzt werden.

3.1.3. IPsec-Gateway

Mit dieser Applikation lassen sich genuboxen als reguläre Layer 3-basierte IPsec-Router einsetzen. Auch wenn sich genubox hinter einem NAT-Router befinden sollte, stellt dieses dank NAT-Support kein Hindernis dar.

Ein weiterer Vorteil ist die Skalierbarkeit von IPsec-VPNs durch die Zusammenlegung von Tunneln. Dadurch ist es möglich, sehr komplexe IPsec-VPNs mit vielen Netzen zu betreiben, ohne einzelne Gateways zu überlasten. Darüber hinaus werden On Demand-Funktionen unterstützt, die das VPN nur bei Bedarf aufbauen.

Zusätzlich können durch das DPD-Protokoll (Dead Peer Detection) ausgefallene Verbindungspartner schnell identifiziert werden.

3.1.4. Das Applikationsmodul

Bei Projekten ist häufig der Einsatz individueller Anwendungen gefordert. Diese lassen sich in genubox integrieren. Bei Bedarf steht genua als kompetenter Entwicklungspartner zur Verfügung, der die Anwendung nach den Vorgaben des Kunden implementieren oder dabei assistieren kann.

Als individuelle Applikationen sind Maschinenüberwachung, Ferndiagnose, Remote Management Access, komplexe Applikations-Tunnel für ASP-Anwendungen sowie Präventiv-Wartungssysteme denkbar.

Ein konkretes Beispiel bilden Anwendungen, die Sensordaten von Industrieanlagen aufzeichnen, verpacken und in bestimmten Zeitabständen an ein Wartungsunternehmen versenden.

4. Anwendungsfälle

Bereits zahlreiche Unternehmen und Behörden setzen auf genubox, wenn es um sichere Remote-Anwendungen geht. Im Folgenden zeigen wir Ihnen mögliche Einsatzszenarien auf.

Bei allen Szenarien bietet genua den Vorteil einer zentralen Management-Lösung, die eine Überwachung aller Hardware-Komponenten und Software-Stände bietet. Durch die zentrale Distribution von Patches ist das gesamte System stets aktuell und auf dem Stand der Technik abgesichert. Die Möglichkeit, sämtliche Vorgänge innerhalb der Lösung aufzuzeichnen, gewährleistet Transparenz, Nachvollziehbarkeit und Auditfähigkeit.

4.1. Anlagenwartung mit Rendezvous

Bei der Rendezvous-Lösung laufen alle Wartungsverbindungen über einen Rendezvous Server, der in der Cloud oder einer Demilitarisierten Zone (DMZ) neben der Firewall installiert ist – beim Dienstleister oder bei Kunden. Hierhin bauen sowohl der Wartungs-Service als auch der Kunde zum verabredeten Zeitpunkt Verbindungen auf. Erst mit dem Rendezvous auf dem Server entsteht die durchgängige Wartungsverbindung. Über diese kann der Service die Maschinenanlage oder das IT-System im Kundennetz mit freigeschalteten Applikationen ansprechen. So behält

der Kunde die vollständige Kontrolle über die Wartungszugriffe in seine Netze. Die Rendezvous-Lösung gewährleistet zuverlässige IT-Sicherheit, zeichnet alle Aktionen des Services revisionsoptimiert auf, ist in verschiedenen Umgebungen flexibel einsetzbar und per Fernwartungs-App einfach zu bedienen.

Durch die Möglichkeit, einen Virenscanner an den Rendezvous Server oder die Servicebox anzubinden, lassen sich die vom Wartungs-Service gesendeten Daten auf Schadcode überprüfen. Diese Option bietet zusätzlichen Schutz vor Angriffen und sichert die Anlagenverfügbarkeit. Typische Wartungsobjekte sind Industriemaschinen, IT-Infrastrukturen, Automationssysteme, Dokumenten-Managementsysteme usw.

So greift ein Techniker beispielsweise mit dem Siemens Simatic Manager via sicherer Fernwartungsverbindung auf ein Automationssystem einer Produktionsstraße zu. Dank Fernwartungs-App von genua braucht er bei einem späteren Vor-Ort-Termin beim Kunden keine Anpassungen an seiner Projekt-Software vornehmen.

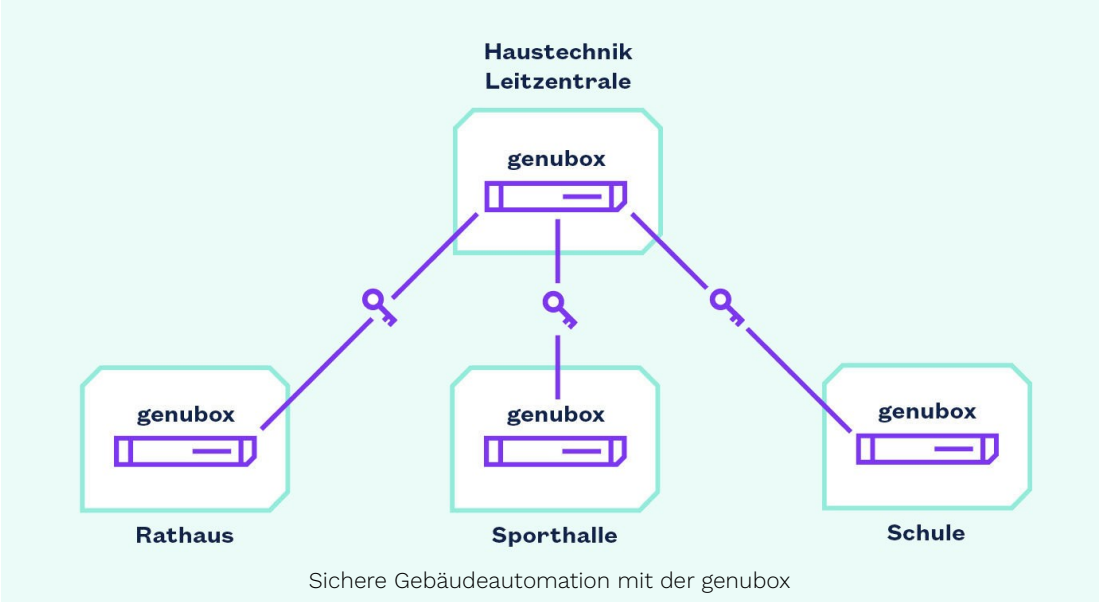
4.2. Sichere VPN-Strecken über SSH oder IPsec

Eine häufige Anwendung von genubox liegt in der Bereitstellung verschlüsselter, authentisierter Verbindungen. Die Besonderheit von genubox in diesem wettbewerbsintensiven Markt: genubox ist eine Produktvariante der für VS-NFD-Kommunikation zugelassenen und nach CC EAL 4+ zertifizierten genuscreen. Ihre Architektur entspricht den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), das genuscreen dazu regelmäßig aufwändigen Sicherheitsprüfungen unterzieht.

Da genubox über ein Applikationsmodul und damit über eine Schnittstelle für individuelle Anwendungen verfügt, ist sie nicht zertifizierbar. Aufgrund ihres hohen Sicherheitsniveaus ist sie jedoch besonders für kritische Anwendungsbereiche geeignet, in denen VPN-Lösungen, die eine geringere Transparenz aufweisen, nicht zum Einsatz kommen sollten.

4.3. Kundenspezifische Lösungen

Zusammen mit Kunden entwickelt genua maßgeschneiderte Lösungen: Individuelle Software-Anwendungen des Kunden – oder von genua für den Kunden entwickelt – werden über das Applikationsmodul von genubox mit der VPN-Lösung von genua kombiniert.



Sichere Gebäudeautomation mit der genubox

Zuverlässiger und schneller Hersteller-Service sowie die Sicherheit der VPN-Anbindung stehen bei unseren Auftraggebern im Vordergrund. Bewährte Einsatzbeispiele sind u. a. Anwendungen der Gebäudeautomation im öffentlichen und privatwirtschaftlichen Bereich.

4.4. Sichere Anbindung von Mobilanwendungen an das Netzwerk einer Organisation

Die Anbindung mobiler Devices wie Smartphones oder Tablets ist ein zunehmend wichtiges Thema in Unternehmen. Auch in diesem Bereich stellt genubox eine mögliche Lösung mit gehobenem Sicherheitsniveau dar: Als Gateway auf Basis der für VS-NFD-Kommunikation zugelassenen und nach CC EAL 4+ zertifizierten genuscreen ermöglicht sie verschlüsselte, authentisierte Verbindungen zwischen mobilen Mitarbeitern und dem Netzwerk einer Unternehmenszentrale. Datentransfers sind jederzeit zuverlässig geschützt.

5. Schnittstelle zu SIEM-Systemen

genubox verfügt über eine Schnittstelle zu SIEM-Systemen (Security Information and Event Management) zur zentralen Erfassung aller sicherheitsrelevanten Meldungen der Fernwartungslösung. Damit lassen sich diese mit Meldungen weiterer Systeme intelligent verknüpfen und Angriffsversuche nachvollziehen, die bei isolierter Betrachtung einzelner Systeme unerkannt bleiben.

6. Support von Zero-Trust-Konzepten

Beim Zero-Trust Networking wird das Vertrauen in die Sicherheit des Gesamtnetzes durch das Vertrauen in die Sicherheit spezifischer Kommunikationsendpunkte ersetzt, d. h. in Geräte, Dienste und Anwendungen. Eine Kompromittierung einzelner Endpunkte ist damit auf die erlaubten Kommunikationsbeziehungen beschränkt und gefährdet nicht mehr das Gesamtnetz. Dieses Vorgehen gibt dem Betreiber die Kontrolle über seine Anlagen zurück und verringert proaktiv die Angriffsfläche.

Die Fernwartungslösung von genua unterstützt Zero-Trust-Konzepte. In diesem Zusammenhang übernimmt der Rendezvous Server die Rolle des Software-defined Perimeter und erlaubt authentisierten externen Anwendern den Zugriff nur auf spezifische Dienste. Hierhin verbindet sich das Zielsystem von innen. Der Fernwarter wiederum baut ebenfalls eine verschlüsselte Kommunikation zu diesem Perimeter auf. Nach erfolgreicher Authentisierung wird ein Zugriff ausschließlich auf spezifisch benötigte Dienste ermöglicht, wie z. B. auf den Desktop der zu wartenden Maschine, das Terminal oder auf ausgewählte Ports.

Das geschieht nach dem Principle of Least Privileges: Nur das gewünschte Protokoll der Software bestimmt also die Verbindung, alle anderen Anwendungen oder gar beide Netze werden nicht gekoppelt.

7. Anbindung an eine zentrale Benutzer- und Rechteverwaltung

Eine Schnittstelle zu Identitäts- und Zugriffsmanagementsystemen ermöglicht die flexible Anbindung der Fernwartungslösung an eine zentrale Benutzer- und Rechteverwaltung. genubox unterstützt OKTA, Keycloak, Azure Active Directory, Microsoft Active Directory und RADIUS (Remote Authentication Dial-In User Service).

8. Zentrales Management mit genucenter

Ein wesentlicher Vorteil der Fernwartungslösung von genua ist die zentrale Administrationsmöglichkeit. Dabei dient die Central Management Station genucenter als effektives und ressourcensparendes Werkzeug zur Konfiguration, Überwachung und Administration von genubox. Sie bietet eine Übersicht über die jeweilige Installation und stellt sicher, dass alle Systeme auf dem aktuellen Stand sind und einwandfrei funktionieren.

Änderungen und Updates lassen sich über komfortable Gruppierungs-Funktionen gleichzeitig auf beliebig viele Systeme übertragen. Damit ist die konsequente Umsetzung von Policies im gesamten Netzwerk möglich. In wachsenden Installationen

werden die zusätzlichen Systeme ganz einfach in die Central Management Station integriert und von hieraus gleich mit bewährten Konfigurationen ausgestattet.

9. Produktvarianten

genubox ist in verschiedenen Ausführungen erhältlich:

genubox XS: Dieses Modell verfügt über einen Smartcard-Reader. Es ist mit drei Netzwerkschnittstellen ausgestattet und für den Einbau in 19" Rack-Schränke ausgelegt.

genubox XSo: Dabei handelt es sich um die Basisversion für den Office-Einsatz.

genubox Xsi: Diese robuste Hardware-Variante ist mit drei Netzwerkschnittstellen ausgestattet und eignet sich für die Hutschienenmontage. Sie ist insbesondere für den Einsatz in Schaltschränken geeignet.

genubox S, M und L: Diese Server-Modelle gewährleisten die Abdeckung unterschiedlich hoher Performance-Anforderungen. Die Bauformen sind ausschließlich für den Betrieb in 19" Rack-Schränken geeignet und werden vor allem als leistungsfähige Rendezvous Server verwendet.

Darüber hinaus ist genubox auch als Software-Version zum Betrieb auf kundeneigenen Systemen oder in Public Clouds (Virtualisierer Microsoft Hyper-V, Linux KVM, VMWare ESXi und VMWare vSphere) in unterschiedlichen Leistungsklassen verfügbar.

10. Kundenservice

Den Kundenservice zu genubox erhalten Sie direkt vom Hersteller genua, einem führenden Spezialisten für Netzwerkadministration und IT-Sicherheit. Auf Wunsch übernehmen wir das komplette Management Ihrer Fernwartungslösung. Dann haben unsere Spezialisten Ihr System ständig über stark verschlüsselte Internetverbindungen im Blick und erledigen die gesamte Administration, so dass Sie sich stets auf einen reibungslosen Betrieb verlassen können.

Wir bieten aber auch eine Support Hotline, die Ihnen bei allen Fragen per Telefon und E-Mail zur Seite steht, sowie einen regelmäßigen Update-Service. Gerne schnüren wir Ihnen ein maßgeschneidertes Service-Paket. Sprechen Sie uns an – wir bieten Ihnen eine umfassende Beratung.

11. Training

Beim Produkt-Training zu genubox werden Aufbau und Funktionsweise anschaulich dargestellt, um anschließend Schritt für Schritt die Installation, das Management über genucenter/Stand-Alone-GUI sowie das Einspielen von Updates kennenzulernen. Einen wichtigen Punkt bilden natürlich auch interessante Einsatzszenarien. Weitere Informationen zu Inhalten und Terminen finden Sie unter:

https://www.genua.de/trainings

Unser Trainings-Team steht Ihnen für Anfragen gerne zur Verfügung:

T +49 89 991950-902 , E training@genua.de

GB-WP-0923-21-D

So erreichen Sie uns:

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München

T +49 89 991950-0, F +49 89 991950-999, E info@genua.de, www.genua.de