Zentrales Monitoring in verteilten Netzwerken

Whitepaper

Autor: Daniel Zobel, Dokumentation und Support bei der Paessler AG

Erstveröffentlichung: August 2010 – Stand: Januar 2012

Inhalt

Einleitung

Unternehmen mit mehreren Standorten sind auf eine performante IT-Infrastruktur angewiesen. Reibungslos ablaufende IT-Prozesse und eine zuverlässige Kommunikation, sowohl intern (zwischen einzelnen Firmenstandorten), als auch extern (mit Kunden und Partnern) sind Schlüsselfaktoren für den sicheren Geschäftsbetrieb. Um die örtlich verteilten Netzwerke und deren Verfügbarkeit sowie Bandbreitenauslastung jederzeit im Blick zu haben, ist ein zuverlässiges Monitoring unerlässlich. Es liefert wichtige Informationen über den Zustand der Netzwerke und warnt vor dem Erreichen kritischer Werte das IT-Personal.

Anhand der Software PRTG Network Monitor zeigt dieses Whitepaper im Folgenden auf, wie mit so genannten Remote Probes („Fern-Sonden“) die Netzwerküberwachung auf zusätzliche Standorte erweitert werden kann.

Vielseitige Anwendungsgebiete mit dem Probe-Prinzip

PRTG Network Monitor überwacht ein Netzwerk „out-of-the-box“: Direkt nach Installation und Auto-Discovery stehen erste Monitoring-Ergebnisse zur Verfügung. Dafür werden keine weiteren Remote-Installationen und keine Agenten auf den Zielsystemen benötigt, denn PRTG nutzt die gängigen Protokolle der Hardwarehersteller, um Informationen abzufragen.

Neben diesem Standard-Szenario gibt es eine Vielzahl von Einsatzbereichen, die eine erweiterte Netzwerküberwachung erfordern. Hierfür kann eine zentrale Installation von PRTG in Zusammenarbeit mit zusätzlichen „Remote Probes“ (Fern-Sonden) eingesetzt werden. Diese Probes kann man sich als kleine Programme vorstellen, die auf einem Computer an beliebiger Stelle im Netzwerk betrieben werden. Sie stehen mit der zentralen PRTG-Serverinstallation in ständiger Verbindung und leiten die Überwachungsergebnisse weiter. Falls die physikalische Verbindung zwischen Remote Probe und PRTG-Server einmal unterbrochen werden sollte, kann die Probe Monitoring-Daten zwischenspeichern und sie senden, sobald die Verbindung wiederhergestellt ist.

Diese Konfiguration ist für alle Unternehmen interessant, deren Netzwerk sich über mehrere Standorte, VPNs oder mit Firewalls abgetrennte Netzwerksegmente erstreckt und die auf ein zentrales Netzwerk-Monitoring über verschiedene lokale oder verteilte Netze (LANs/WANs) abzielen. Auch für IT-Servicedienstleister, die ihren Kunden einen höheren Service-Level bieten und eine Netzwerküberwachung direkt beim Kunden einrichten möchten, sind Remote Probes eine bequeme und effiziente Lösung.

Für eine Reihe technischer Speziallösungen hat die Remote-Probes-Architektur ebenfalls einen großen Mehrwert.

- Zur einfachen Lastverteilung der Überwachungsaufgaben auf mehrere Einzelrechner (dies ist z.B. für das langsame WMI-Protokoll in großen Netzen empfehlenswert).
- Zum Herstellen einer generell verschlüsselten Verbindung zur Übermittlung von Überwachungsdaten zwischen zwei gesicherten Standorten über das offene Internet.
- Für ein Monitoring komplett gekapselter Dienste wie Mail- oder Webserver.
- Mit der Probe-Technik kann der Administrator in einem Netzwerk ohne weitere Hilfsmittel Quality-of-Service (QoS) Messungen durchführen. Die notwendige Teststrecke wird dabei zwischen zwei PRTG-Probes hergestellt.

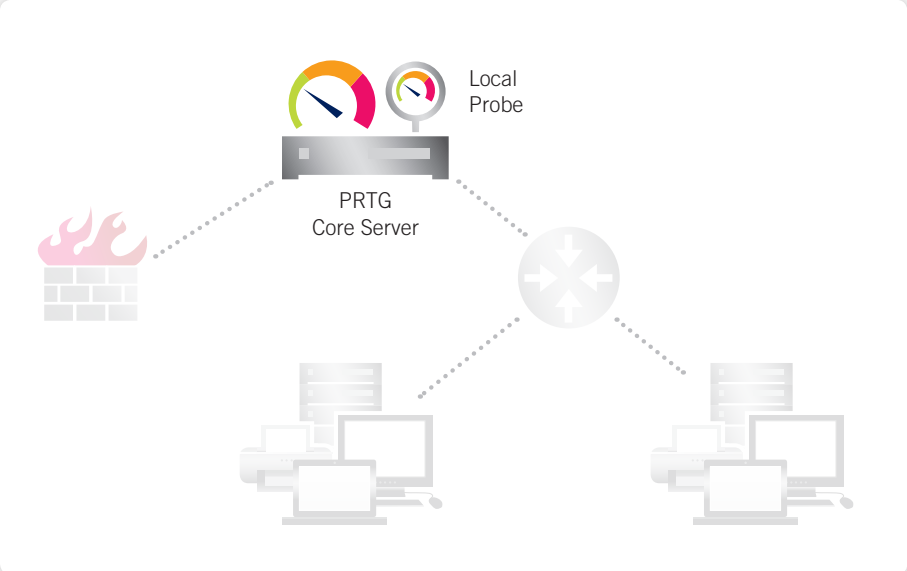


Abbildung:
Eine Standardinstallation von PRTG besteht aus Server und Local Probe

Die PRTG-Probe-Architektur

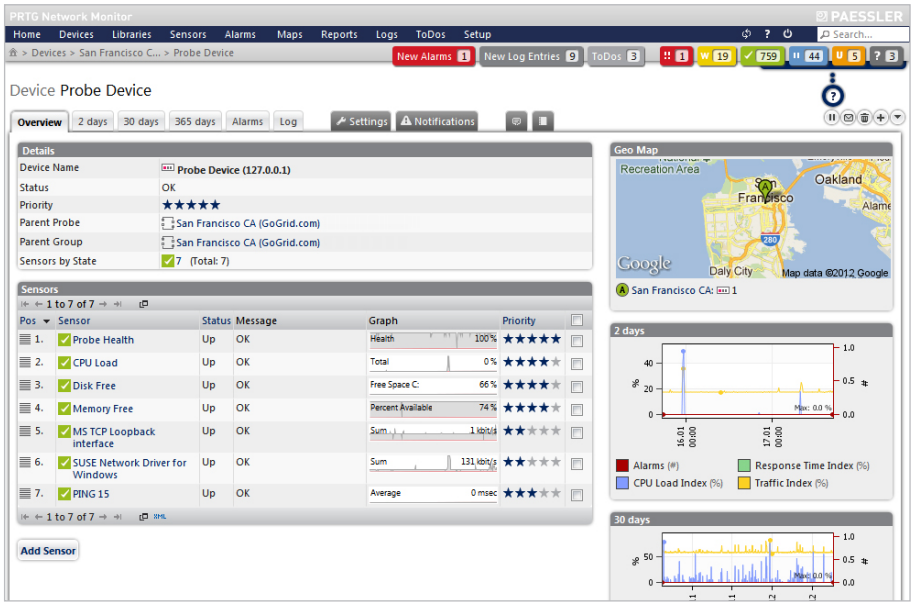
Die Softwarearchitektur von PRTG ist leistungsstark und sehr einfach zu integrieren. Eine Standardinstallation von PRTG besteht zunächst aus einem zentralen Server und einer „Local Probe“ (direkt auf dem Rechner), die beide jeweils als Dienst auf einem beliebigen Windows-Rechner im Netzwerk laufen. Der Server enthält die Konfiguration und übernimmt die Verwaltung der Überwachungsdaten, erstellt Berichte und versendet Benachrichtigungen. Er stellt auch den Webserver für das Benutzerinterface zur Verfügung, worüber der Benutzer Einstellungen tätigen und die Überwachungsdaten einsehen kann. Die eigentliche Netzwerküberwachung findet mittels der Local Probe statt. Diese kommuniziert über gängige Protokolle mit den Geräten sowie Rechnern und leitet die empfangenen Daten an den PRTG-Server weiter. Für das Monitoring kommen beispielsweise SNMP, WMI oder WBEM zum Einsatz; zur Traffic-Analyse auch NetFlow-Protokolle oder Packet Sniffer. Alle Daten fließen zentral in der Überwachungslösung zusammen, unabhängig davon, auf welchem Weg sie empfangen werden. Dort erfolgt die Auswertung und Analyse. Verschiedene „Trigger“ lösen Nachrichten oder Aktionen aus, beispielsweise beim Überschreiten festgelegter Grenzwerte oder wenn ein Gerät nicht mehr auf einen Ping reagiert. Sogar ein automatischer Neustart eines überwachten Rechners kann so ausgelöst werden.

Lösungen für Unternehmen mit verteilter Infrastruktur

Daten aus unterschiedlichen Protokollen werden zentral erfasst.

Diese Architektur mit einer Local Probe wird bei Bedarf um Remote Probes erweitert, die auf einem anderen Rechner installiert sind und dort im Hintergrund laufen. Auch sie kommunizieren mit den Geräten im Netzwerk und senden Monitoring-Daten an den PRTG-Server. Anders als die lokale kann sich eine Remote Probe aber in einem ganz anderen Netzwerk und hinter einer Firewall befinden. Sie ist in der Lage, das Netz, in dem sie installiert ist, „von innen“ zu überwachen und von dort aus eine verschlüsselte Verbindung zum PRTG-Server herzustellen. So kann auf einfache Weise die Netzwerküberwachung erweitert werden, ohne dass die Sicherheit des Netzwerkes nach außen gefährdet wird. Die Einbindung dieser externen Standorte erfolgt in der Monitoring-Lösung nahtlos; der Administrator hat alle Netzwerke zentral im Blick.

Abbildung:
Paessler-Probe in San Francisco in Aktion (PRTG Web-Interface)



Mehrere Standorte

Ein Unternehmen mit verteilter Infrastruktur kann mit der Probe-Funktionalität seine eigenen Außenstellen in ein zentrales Netzwerk-Monitoring einbinden, auch wenn sich diese hinter Firewalls befinden und eigene Netzwerke betreiben. Hierfür ist lediglich die einmalige Installation eines zentralen PRTG-Servers und mehrerer Probes notwendig – jeweils eine in jeder Außenstelle. Für die Verbindung zwischen den Außenstellen und der Firmenzentrale werden die bestehenden Netzwerkverbindungen des Unternehmens verwendet, beispielsweise eine vorhandene VPN-Anbindung.

Sicherheitsrisiken minimieren durch SSL: Die Verbindung zwischen Server und Probe ist grundsätzlich verschlüsselt.

Beim Monitoring werden mitunter sensible Daten gesammelt, die im Datenstrom zwischen Probe und Server ausgetauscht werden. Darüber hinaus empfängt die Probe vom Server über diese Verbindung die komplette Konfiguration mit allen notwendigen Zugangsdaten zu den Systemen, die überwacht werden sollen. Oft sind dies Passwörter mit Administrator-Rechten, um Zugang zu sehr systemnahen Informationen zu erhalten. Deshalb erfolgt die Kommunikation zwischen PRTG-Server und den Probes immer SSL-verschlüsselt, damit sensible Informationen nicht in falsche Hände geraten können. Selbst eine Server-Probe-Verbindung über das offene Internet stellt so kein Sicherheitsrisiko dar.

Probes binden auch externe Mailserver bei Hosting-Providern in das Monitoring ein.

Firmeneigene Mailserver bei einem Hosting-Provider und andere Bestandteile der IT-Infrastruktur, die nicht von außen über eine HTTP-Verbindung zugänglich sind, können mit Probes bequem in eine Netzwerküberwachung eingebunden werden. So ist die IT-Abteilung jederzeit über Störungen informiert und kann Statistiken zur Auslastung abfragen.

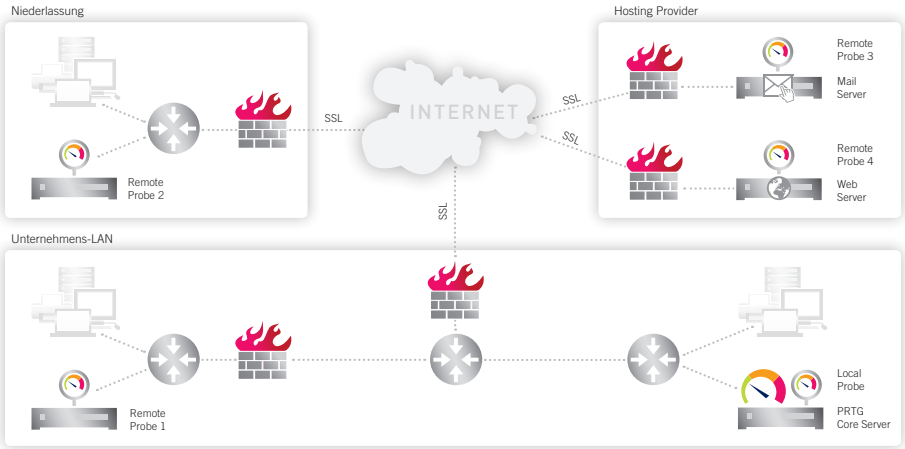


Abbildung:
Einsatz von Remote Probes zur Anbindung von Außenstandorten und zur Netzwerküberwachung „gekapselter“ Dienste. Die Probes überwachen ihr jeweiliges Sub-Netz und übermitteln die Ergebnisse an den zentralen Server.

Einfache Lösung für „Managed Service Provider“

Dienstanbieter in der IT-Branche, sogenannte „Managed Service Provider“ (MSP) sind in der Lage, mit Hilfe eines Setups aus einem zentralen Server und vielen Remote Probes ihren Kunden ein intelligentes Monitoring direkt vor Ort anzubieten. Netzwerküberwachung als Service lässt sich so auf einfache Weise realisieren. Der MSP benötigt dafür selbst nur ein einziges zentrales System, das die Auswertung der Daten, die Benachrichtigung im Fehlerfall (an den MSP selbst oder direkt an den Kunden) und sogar eine umfangreiche Komponente zur Berichterstellung enthält. Für jeden Kunden können einzeln Berichte erstellt werden – beispielsweise über Verfügbarkeit (Uptime) und Auslastung bestimmter Geräte oder den Verbrauch von Internet-Traffic. Der Service-Provider muss so nicht für jeden Kunden einen eigenen (virtuellen) Server betreiben und instandhalten, sondern nur eine einzige zentrale Installation konfigurieren und mit Software-Updates versorgen. Dies spart Zeit und Kosten.

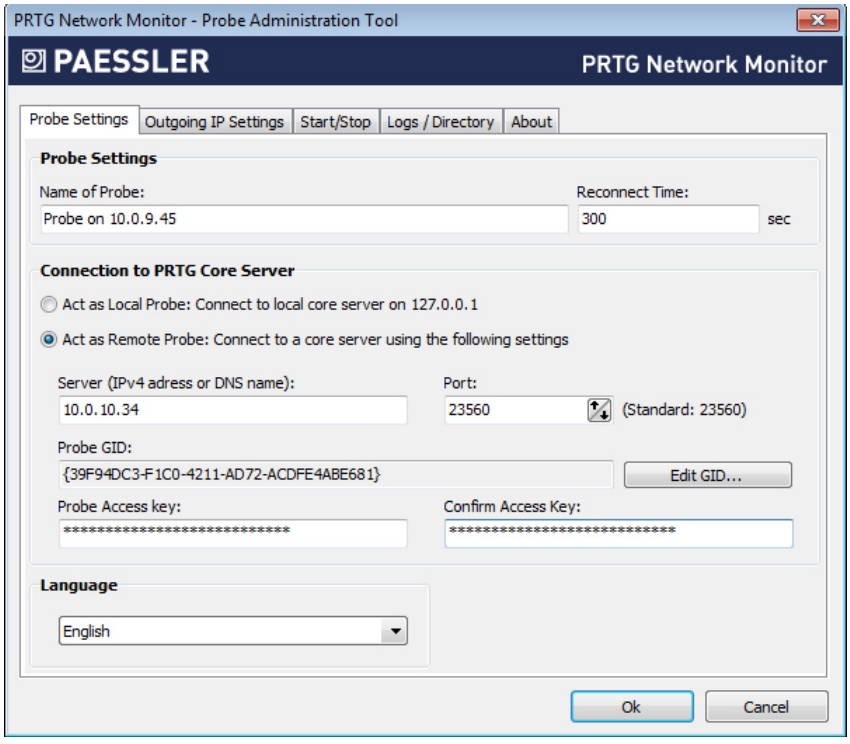
Auf Kundenseite wird lediglich eine Remote Probe installiert, die das Kundennetzwerk „von innen“ monitort und die Ergebnisse in einer verschlüsselten Verbindung zum Server des MSPs überträgt. Dies geschieht über die ohnehin vorhandene Breitband-Internetverbindung des Kunden.

Ein MSP benötigt lediglich eine Probe im Netzwerk seines Kunden.

Der Aufwand für die Umsetzung ist hierbei minimal; wenn vorhandene Server benutzt werden können, muss beim Kunden nicht einmal eigene Hardware aufgestellt werden. Falls doch ein eigener PC benötigt wird, genügen bei einem kleineren Netzwerk schon sehr preisgünstige Geräte (etwa ein Thin-Client oder ein Netbook), da die Probe-Software keine hohen Systemanforderungen stellt. Alternativ lässt sich die Probe auch auf einer virtuellen Maschine (VMware, Hyper-V, XEN) betreiben.

Besteht das Kundennetzwerk aus mehreren Sub-Netzen, wird in jedem einzelnen eine eigene Probe eingesetzt. Diese baut selbstständig eine Direktverbindung zum PRTG-Server auf; dabei verwenden alle den gleichen Port, wodurch der Konfigurationsaufwand bei der Firewall überschaubar bleibt. Die Identifizierung und Authentifizierung der einzelnen Probes beim PRTG-Server erfolgt über eindeutige Kennungen, die sicherstellen, dass nur berechtigte Probes eine Verbindung aufbauen können.

Abbildung:
Ein eindeutiger Probe-Schlüssel dient der Authentifizierung



Bei Bedarf kann der MSP eine Migration zu einem eigenen virtuellen Kunden-Server durchführen.

Die mögliche Anzahl der eingesetzten Probes wird von PRTG technisch nicht limitiert, sodass ein MSP eine Vielzahl von Kunden bedienen und das Monitoring beständig erweitern kann.

Ist die Monitoring-Lösung erst einmal eingerichtet, steigt auf Kundenseite oft das Interesse an zusätzlichen Überwachungsdaten bzw. Szenarien. Mit einer daraufhin erweiterten Netzwerküberwachung wachsen dann schnell die Anforderungen. Wünscht der Kunde später seine eigene, unabhängige Installation, kann ihm der MSP bequem einen virtuellen oder realen Server installieren. Das Monitoring erfolgt dabei weiterhin über Remote Probes. Bereits vorhandene Probes im Netz des Kunden können einfach weiter verwendet werden, ohne dass zusätzliche Hardware integriert werden muss. Der MSP erbringt weiterhin die Dienstleistung und kümmert sich um den Betrieb des Servers.

Schnelle Einrichtung: Der Konfigurationsaufwand beim Kunden bleibt überschaubar.

Die Firewall beim Kunden wird dabei nicht „durchlöchert“, denn für die Verbindung zur Probe muss lediglich ein einziger Port geöffnet werden. Da so eine Verbindung von der Probe im Inneren des Netzwerks zum Server nach außen hergestellt wird, ist auf Kundenseite oft auch gar keine Änderung in den Sicherheitseinstellungen erforderlich. Dies minimiert den Konfigurationsaufwand.

Spezielle Lösungen für spezielle Szenarien

Besondere Konfigurationen benötigen oft auch spezielle Monitoring-Lösungen. Remote Probes bieten in diesem Bereich eine Reihe von Einsatzmöglichkeiten, die über die zentrale Netzwerküberwachung in externen Netzwerken hinausgehen.

Lastverteilung

Soll in einem Netzwerk ein sehr detailliertes Monitoring eingerichtet werden, kann dies je nach Anzahl der eingesetzten Sensoren und der verwendeten Überwachungstechnik zu Performance-Einschränkungen führen – abhängig von der eingesetzten Hardware und Beschaffenheit des Netzwerks. Beispielsweise werden beim Einsatz von Packet-Sniffern typischerweise mehr CPU-Leistung und Arbeitsspeicher benötigt als etwa bei einem einfachen SNMP-Monitoring, denn beim Packet-Sniffing wird eine sehr viel größere Menge von Daten verarbeitet. Auch der intensive Einsatz des WMI-Protokolls erfordert zusätzliche Ressourcen.

Überwacht der Administrator sein Netzwerk in großem Umfang mit diesen Techniken, ist unter Umständen leistungsfähigere Hardware notwendig, um das Datenvolumen in angemessener Zeit zu verarbeiten. Alternativ kann er die Netzwerküberwachung aber auch auf mehrere Probes im Netzwerk verteilen, die jeweils einen Teil des Monitorings übernehmen und den zentralen Server entlasten. Jede Probe kann dabei auf einem eigenen System installiert werden. Die gesammelten Daten laufen zentral beim PRTG-Server zusammen und stehen dort zur Auswertung bereit.

Sicherstellen einer verschlüsselten Übertragung

Vor allem bei SNMP hat sich bis heute der verschlüsselte Standard in der Version 3 kaum durchgesetzt, sodass viele moderne Geräte lediglich SNMP v1 mit einer sehr einfachen Authentifizierung und Klartextübertragung der Daten anbieten. Während dies z.B. bei einer Überwachung des Druckertoner-Füllstandes meist kein Problem darstellt, könnten beim Monitoring eines Routers sensiblere Daten übertragen werden, die beispielsweise Rückschlüsse über das Surfverhalten bestimmter Benutzer ermöglichen würden.

Remote Probes können die Sicherheitsrisiken veralteter Hardware kompensieren.

Oft gibt es hardwareseitig keine Alternative zu SNMP v1. Um sicherzustellen, dass auf dem Übertragungsweg zum zentralen Server sensible Informationen nicht mitgelesen werden, kann der Administrator eine Remote Probe im Netzwerk dieser Geräte einrichten und diese von dort aus überwachen. Die gesammelten Daten werden dann über die SSL-verschlüsselte Server-Probe-Verbindung übermittelt.

Gekapselte Dienste

Probes können – wie erwähnt – auch in Systemen eingesetzt werden, deren Systeminformationen grundsätzlich von außen nicht zugänglich sein sollen. Windows Web- oder ein Mailserver sind Beispiele solcher Anwendungsgebiete. Installiert der Administrator auf dem Server eine Probe, können von dort aus – etwa mit WMI-Sensoren – Prozessorlast, Arbeitsspeicher- und Festplattenverbrauch überwacht, aber auch der aktuelle Status der Mail-Queue abgefragt werden. Dafür müssen auf dem Server keine Ports für eingehende Verbindungen geöffnet werden, und die Systeme werden nicht verwundbar gemacht. Die Monitoring-Daten stehen trotzdem ständig zur Verfügung, da die Probe von innen heraus die Verbindung zum zentralen PRTG-Server herstellt. Tritt eine Störung auf, informiert das Nachrichtensystem des PRTG-Servers sofort den Verantwortlichen.

Monitoring aus unterschiedlichen Perspektiven

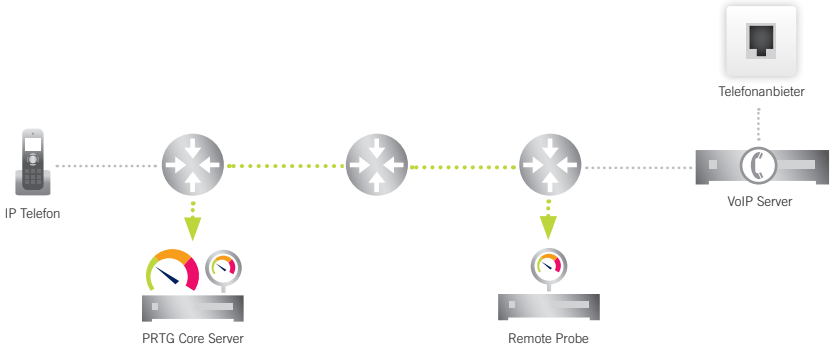
Die Webseite eines Unternehmens oder gar der eigene Webshop sind ein wichtiger Teil der Unternehmenspräsentation und machen oft einen beträchtlichen Teil des Umsatzes aus. Schon kurze Ausfälle können sich negativ auf die Umsatzzahlen auswirken. Ein Monitoring der eigenen Internetpräsenz ist deshalb unverzichtbar. Vor allem Firmen, die international agieren, setzen vermehrt auf ein Content Distribution Network (CDN), das die Web-Inhalte auf verschiedene Server rund um den Globus spiegelt und dem Besucher die Inhalte von dem jeweils (topologisch gesehen) „nächsten“ Server liefert. Dies führt zu kürzeren Antwortzeiten (Ping) und einem schnelleren Seitenaufbau.

Weltweite Perspektiven: Probes können eine Webseite von jedem Kontinent aus überwachen.

Mit PRTG können Administratoren jeweils eine Probe für das Überwachen von Servern auf jedem Kontinent installieren und ihre Internetpräsenz so aus verschiedenen Perspektiven monitoren.[1] Auf diese Weise können sie leicht die Ladezeiten von Webseiten in den unterschiedlichen Ländern vergleichen, beispielsweise in den USA, Europa oder Asien. Dazu überprüft jede Probe via separate Netzwerkverbindung die Ladezeiten und sendet die Daten anschließend an den zentralen Server. Dort kann der Administrator dann überprüfen, ob die gemessenen Werte den Wünschen der Geschäftsleitung entsprechen, ob das CDN-Netz erweitert oder Systeme aufgerüstet werden sollten.

Wenn ein Unternehmen bei einem Internetprovider für einen gewissen Service-Level bezahlt, kann der Administrator auf diese Weise auch überprüfen, ob die Service-Level-Vereinbarungen eingehalten werden. Dazu installiert er eine Probe mit einem QoS-Sensor auf einem beim Provider gehosteten Server. So lässt sich die Leitungsqualität zwischen dem Host-Server und dem Unternehmensstandort ermitteln.

Abbildung:
QoS-Monitoring



[1] Ein entsprechendes „Cloud“-Monitoring finden Sie beispielsweise auf http://www.cloudclimate.com/

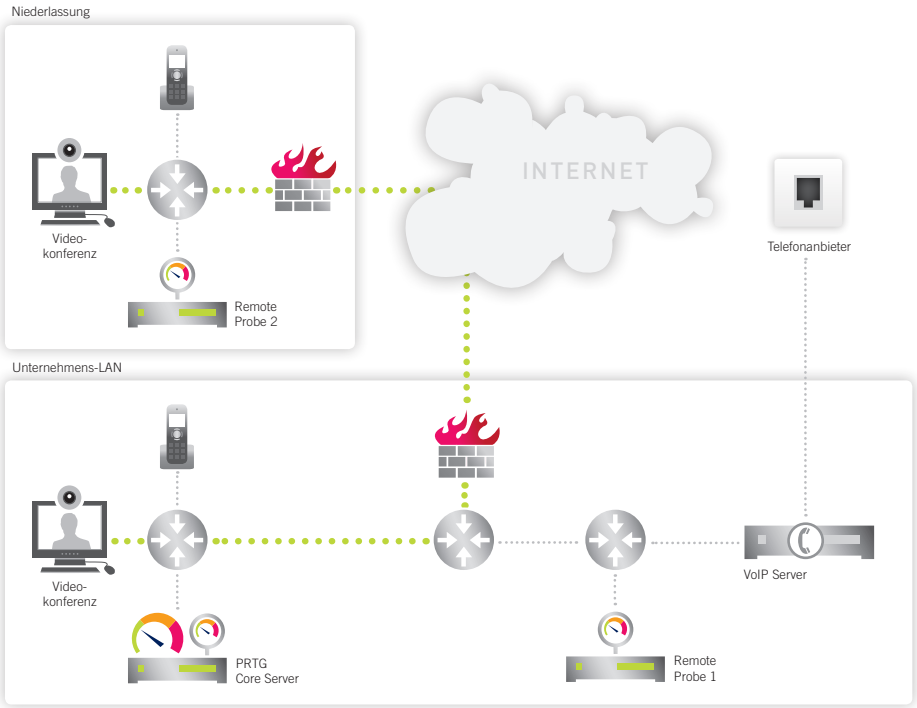
Quality-of-Service-Messungen

Probes ermöglichen QoS-Messungen ohne kostspielige Hardware.

Eine hohe Servicequalität im Netzwerk ist ein wichtiges Kriterium für einen reibungslosen Geschäftsbetrieb. Aber nicht nur im „normalen“ Betrieb eines Netzes, sondern gerade bei der Integration von Voice over IP (VoIP), ist eine Sicherung der Quality of Service (QoS) unerlässlich. Denn die UPD-Paket-basierende Sprachkommunikation reagiert besonders empfindlich auf Störungen wie Paketverlust, Jitter oder größere Verzögerungen bei der Paketübertragung. Professionelle Geräte, beispielsweise höherpreisige Cisco-Router, unterstützen eine Servicequalität-Messung der Netzwerkstrecke zwischen zwei Geräten mit dem Protokoll IP-SLA. PRTG kann diese Daten auslesen und verarbeiten.

Ist solche Hardware nicht vorhanden, kann der Administrator mit Hilfe von Probes eine eigene Messstrecke aufbauen und mit den QoS-Sensoren von PRTG die Servicequalität bestimmen. Dafür wird entweder eine Verbindung zwischen dem PRTG-Server und der Probe hergestellt, oder es kommen zwei Probes zum Einsatz, die auf beliebigen Servern im LAN oder auch im Internet installiert werden. Die „Messstationen“ können also flexibel aufgestellt werden. Eine der beiden Probes in diesem Aufbau übernimmt dabei die Sammlung der Daten und sendet die gemessenen Werte an den Server, die diese weiter auswertet. Mit diesem Setup monitort PRTG in Echtzeit die Verbindung und alarmiert beim Erreichen kritischer Werte. So ist der Verantwortliche permanent hinsichtlich der gewünschten VoIP-Mindestqualität auf dem Laufenden.

Abbildung:
VoIP-Monitoring



Ein einfaches Konzept für viele Möglichkeiten

Die Möglichkeit, das Monitoring mit PRTG durch Remote Probes im Netzwerk zu verteilen, eröffnet viele Anwendungsgebiete. Unabhängig vom Einsatzzweck der Probes laufen stets die gesammelten Daten zentral auf einem Server zusammen. Nach Auswertung dieser Informationen erhält der Verantwortliche einen Überblick über alle Einsatzstandorte. Unternehmen profitieren somit von einem zentralen Monitoring all ihrer Außenstellen. IT-Servicedienstleister können auf einfache Weise ein Monitoring beim Kunden direkt vor Ort anbieten, bei minimalen Eingriffen in dessen Netzwerk und ohne die Notwendigkeit, einen eigenen virtuellen Server für jeden Kunden zu betreiben. Die Probes eignen sich auch für technische Speziallösungen: zur Lastverteilung bei sehr großen oder rechenintensiven Installationen, als zusätzlicher Sicherheitsaspekt beim Monitoring oder bei gekapselten Diensten, wie Mail- oder Webserver. Durch die Flexibilität des Setups lassen sich Probes auch sehr gut zur Netzwerküberwachung aus unterschiedlichen Blickwinkeln einsetzen (wie etwa bei CDN-Netzen) oder zum Aufbau einer eigenen Messstrecke für die QoS-Sicherung im Netzwerk. Wichtig ist hierbei, dass die Daten zwischen den einzelnen Komponenten der PRTG-Software stets verschlüsselt übertragen werden.

Der Administrator benötigt nur eine Serverinstallation mit einer Lizenz. Mehrere Probes sind in allen PRTG-Lizenzen bereits enthalten, lassen sich schnell installieren und werden vom Server aus konfiguriert. Das Unternehmen spart auf der Serverseite Kosten durch den niedrigeren Wartungsaufwand einer zentralen Installation, denn Hardware und Betriebssystem werden nur einmal benötigt.

Über die Paessler AG

Die Paessler AG mit Sitz in Nürnberg entwickelt Software für die Bereiche Netzwerküberwachung und Webserveranalyse seit 1997. Weltweit setzen mehr als 150.000 Administratoren, Webseitenbetreiber, Internet Service Provider und andere IT-Verantwortliche Paessler Software ein. Freeware und Testversionen aller Produkte können unter www.de.paessler.com heruntergeladen werden.

Paessler AG
Bucher Straße 79a, 90419 Nürnberg, Deutschland
www.paessler.com, info@paessler.com

UST#: DE 217564187
Steuer#: FA Nürnberg 241/120/60894
Eintragung: Amtsgericht Nürnberg HRB 23757

Vorstand: Dirk Paessler, Christian Twardawa
Vors. d. Aufsichtsrats: Dr. Marc Rössel