La surveillance centralisée dans les systèmes distribués

Livre blanc

Auteur : Daniel Zobel, du service Documentation et Support de Paessler AG
Date de publication : août 2010 – Dernière révision : janvier 2012

Sommaire

Introduction

Les entreprises multi-sites doivent pouvoir compter sur une infrastructure informatique hautes performances, à même d'assurer l'exécution transparente de leurs processus informatiques et une communication fiable, en interne (entre les différents sites) comme en externe (avec les partenaires et clients). Cela exige une surveillance continue de la disponibilité des ressources et de l'utilisation de la bande passante des réseaux localement distribués. Cette méthode confère en effet aux entreprises des informations critiques sur l'état de leurs réseaux et informe le personnel informatique des éventuels problèmes rencontrés par les différentes ressources du réseau.

Ce livre blanc illustre les possibilités d'extension de la surveillance réseau offertes par PRTG Network Monitor, une solution basée sur des sondes distantes appelé aussi « Remote Probe » (le mot « sonde » a été remplacé par le mot « Probe » dans la version française du logiciel PRTG).

Les sondes au service d'applications polyvalentes

PRTG Network Monitor est une solution de surveillance réseau prête à l'emploi. Elle donne des résultats dès l'installation après l'activation de son outil d'auto-détection. Exploitant les protocoles standard des équipements en place pour collecter des informations, elle ne nécessite aucune installation distante supplémentaire, ni d'agents sur les systèmes surveillés.

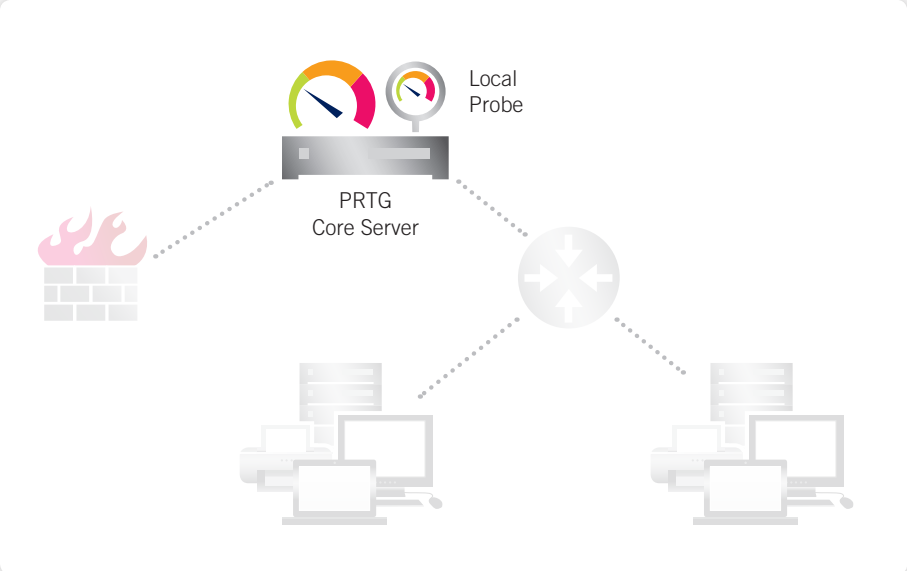
PRTG peut également surveiller des réseaux étendus, installée de façon centrale et combinée à des sondes distantes, autrement dit de petits programmes exécutés sur n'importe quel ordinateur du réseau, qui collectent en permanence les données de surveillance et les communiquent à l'installation PRTG centrale. En cas d'interruption de la connexion physique entre une sonde distante et le serveur central, la sonde inscrit les données de surveillance en mémoire tampon afin de les envoyer au serveur dès le rétablissement de la connexion.

Cette configuration est idéale pour les entreprises exploitant un même réseau pour plusieurs sites, des VPN ou des segments de réseau séparés par un pare-feu, et qui souhaitent centraliser la surveillance de leurs différents réseaux locaux ou distribués (LAN/WAN). Les sondes distantes conviennent également aux fournisseurs de services informatiques voulant optimiser la qualité de leurs services en surveillant les réseaux directement depuis l'infrastructure de leur client.

L'architecture à sondes distantes répond à plusieurs besoins techniques spécifiques :

- répartition des tâches de surveillance entre plusieurs ordinateurs (par exemple, en cas d'utilisation intensive du protocole WMI, particulièrement lent, sur des réseaux étendus) ;
- établissement d'une connexion sécurisée pour la transmission des données de surveillance entre deux sites sécurisés sur l'Internet public ;
- surveillance de services encapsulés, de type service de messagerie ou serveur Web ;
- évaluation de la qualité de service d'un réseau sans outils supplémentaires (par simple liaison mesurée entre deux sondes PRTG).

Illustration :
Installation standard de PRTG, avec serveur central (PRTG Core Server) et sonde locale (Local Probe)



L'architecture de la solution PRTG à base de sonde

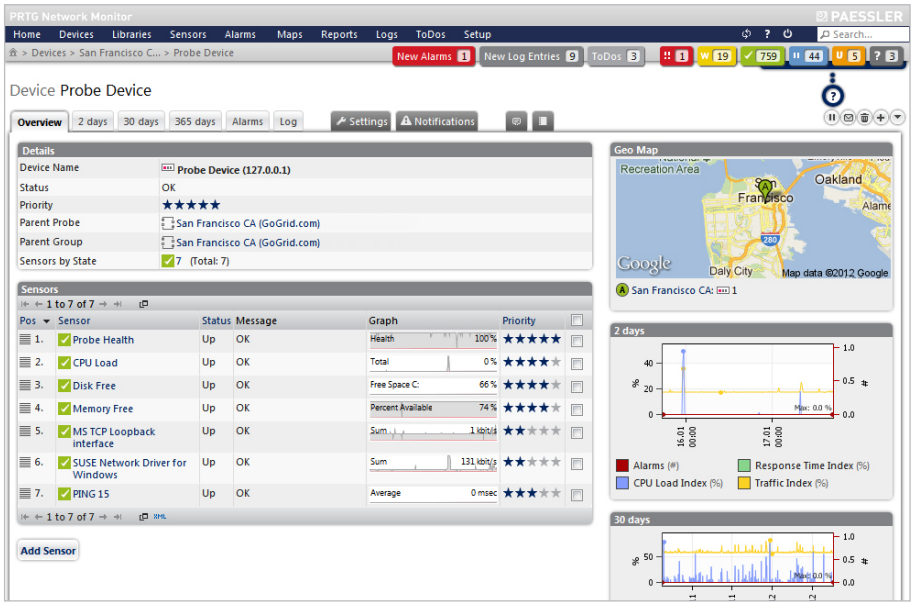
L'architecture logicielle de PRTG est à la fois unique et extrêmement simple. Une installation PRTG standard comprend un serveur central et une sonde locale, chacun exécutable comme un service sur n'importe quel ordinateur sous Windows du réseau. Le serveur stocke la configuration et gère les données de surveillance, rapports et notifications. Il héberge également l'interface permettant aux utilisateurs de modifier les paramètres et de consulter les données de surveillance. La sonde locale se charge quant à elle de la surveillance du réseau. Elle communique avec les périphériques et ordinateurs via des protocoles standard et transmet les données collectées au serveur central de PRTG. La surveillance peut ainsi être effectuée par SNMP, WMI ou WBEM. Des protocoles NetFlow et renifleurs de paquets servent à analyser le trafic. Toutes les données, quel que soit leur mode de transfert, convergent vers la solution de surveillance centrale pour être évaluées et analysées. Divers « déclencheurs » activent des notifications ou des actions spécifiques, au dépassement de certains seuils, par exemple, ou lorsqu'un dispositif ne répond plus aux requêtes ping. Ils peuvent même déclencher le redémarrage automatique d'un ordinateur surveillé.

Des solutions pour les entreprises à l'infrastructure distribuée

Les données issues de différents protocoles sont gérées de manière centralisée.

L'architecture de base, qui ne comprend qu'une sonde locale, peut être complétée par des sondes distantes. Ces dernières sont alors installées sur d'autres ordinateurs et s'exécutent en coulisses. Elles communiquent avec les périphériques de leur réseau et envoient les données de surveillance collectées au serveur central de PRTG. Contrairement à la sonde locale, les sondes distantes peuvent être situées sur un réseau différent et derrière un pare-feu. Elles peuvent surveiller le réseau sur lequel elles sont installées « de l'intérieur » et établir une connexion cryptée avec le serveur central de PRTG. Il est ainsi extrêmement simple d'étendre la surveillance réseau sans exposer le réseau aux risques extérieurs. Cette configuration garantit une sécurité optimale. Les sondes distantes s'intègrent en toute transparence à la solution de surveillance, permettant aux administrateurs de superviser tous les réseaux depuis une même interface.

Illustration :
Sonde Paessler en action à San Francisco (interface Web de PRTG)



La surveillance de plusieurs sites

Grâce aux sondes, le système de surveillance réseau central peut couvrir les succursales d'une entreprise à l'infrastructure distribuée, même si celles-ci utilisent des réseaux distincts, protégés par un pare-feu. Il suffit en effet d'installer un seul serveur central PRTG et une sonde dans chaque filiale. Les données collectées au niveau des filiales sont alors transmises au siège par le biais des connexions réseau disponibles (une connexion VPN existante, par exemple).

SSL : la connexion entre le serveur et chaque sonde est cryptée par défaut.

Les données de surveillance les plus sensibles peuvent également être collectées et transmises via la liaison de données reliant la sonde au serveur central. Cette connexion sert aussi à la configuration des sondes, lesquelles reçoivent tous les droits d'accès nécessaires pour surveiller chaque système couvert depuis le serveur. Il s'agit généralement de mots de passe avec droits d'administrateur qui donnent accès à des informations très orientées machine. Afin que ces informations ne tombent pas entre de mauvaises mains, la communication entre le serveur central de PRTG et les sondes est systématiquement cryptée en SSL. Le serveur et les sondes peuvent ainsi communiquer via l'Internet public sans risque.

Les serveurs de messagerie externes hébergés par des fournisseurs peuvent être surveillés par le serveur central grâce aux sondes distantes.

Les sondes facilitent en outre la surveillance des serveurs de messagerie des entreprises, exécutés par un hébergeur, et d'autres composants de l'infrastructure informatique non accessibles de l'extérieur par une connexion HTTP. Elles informent par ailleurs les techniciens informatiques des éventuels problèmes et leur permettent d'obtenir en permanence des statistiques sur la charge de travail.

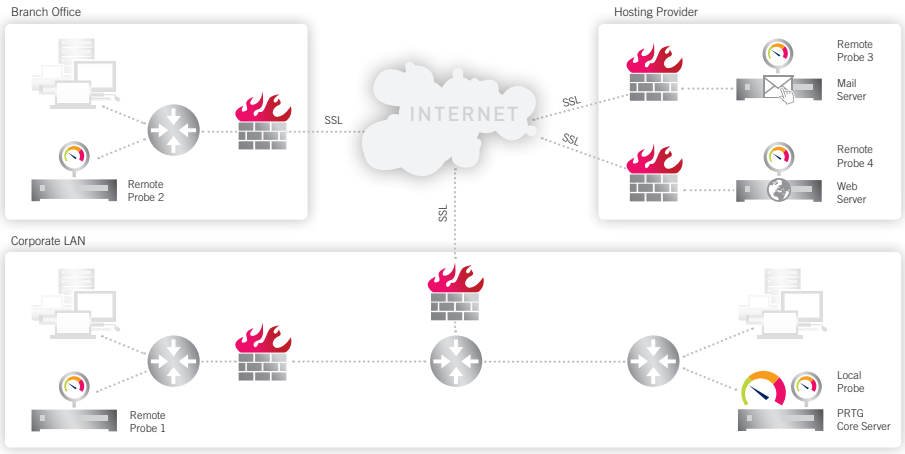


Illustration :
Utilisation de sondes distantes pour la surveillance de succursales et de services « encapsulés ». Chaque sonde surveille son sous-réseau et transmet ses données au serveur central.

Des solutions simples pour les fournisseurs de services gérés

PRTG permet aux fournisseurs de services informatiques de proposer facilement à leurs clients des services intelligents de surveillance sur site, en configurant un serveur central et autant de sondes distantes qu'ils le souhaitent. Un simple système central leur suffit en effet pour analyser les données, recevoir des notifications de panne (ou les envoyer directement au client) et produire des rapports détaillés. Ils peuvent également créer des rapports individuels pour chaque client, sur la disponibilité, la charge de travail de périphériques particuliers ou le trafic Internet, par exemple. Inutile ainsi d'exécuter et de maintenir un serveur (virtuel) par client, ce qui se traduit par des gains importants de temps et d'argent.

Le client, quant à lui, n'a besoin que d'une sonde distante, qui surveille son réseau « de l'intérieur » et transmet les résultats cryptés au serveur du fournisseur via la connexion haut débit existante.

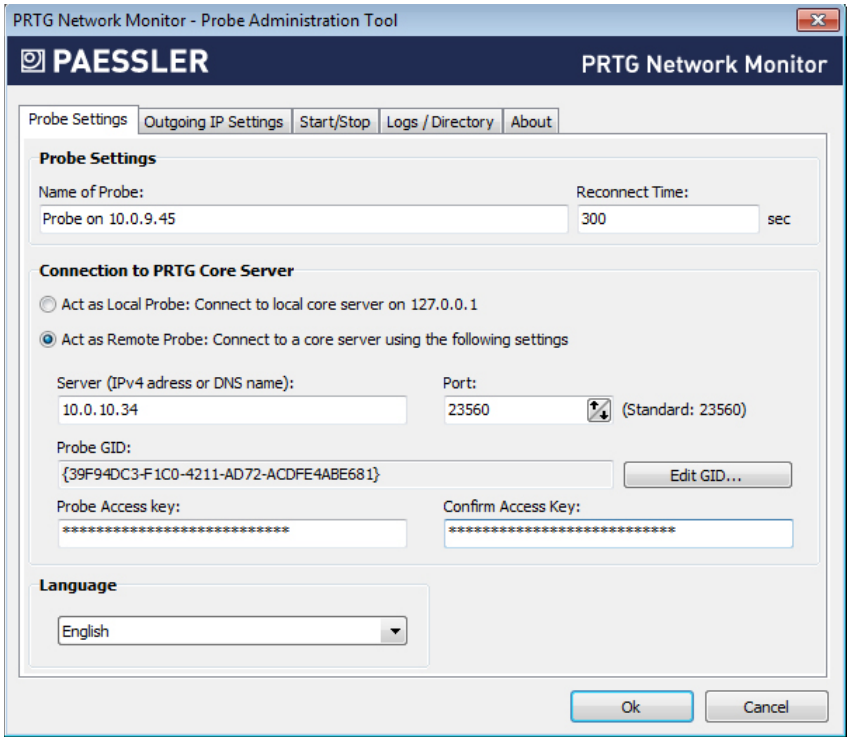
Les fournisseurs peuvent étendre leur portefeuille de services simplement en installant une sonde distante sur le réseau de leurs clients.

Cette configuration représente un coût d'intégration minime, surtout si l'on peut exploiter les serveurs existants, ce qui dispense d'installer du matériel supplémentaire chez le client. Et même s'il faut dédier un PC, la sonde logicielle mobilise si peu de ressources système que des équipements bon marché suffisent pour les petits réseaux, un client léger ou un ordinateur portable par exemple. La sonde peut aussi être exécutée sur une machine virtuelle (ex. VMware, Hyper-V ou XEN).

Lorsque le réseau du client compte plusieurs sous-réseaux, chacun doit avoir sa propre sonde. Toutes établissent une connexion directe avec le serveur central PRTG via le même port. La configuration des pare-feux reste ainsi simple à gérer. Chaque sonde est détectée et authentifiée par le serveur central PRTG grâce à son identifiant unique de sorte que seules les sondes autorisées puissent établir une connexion.

La solution PRTG peut être combinée à un nombre illimité de sondes et par conséquent étendue à loisir pour divers besoins.

Illustration :
Chaque sonde se voit attribuer un identifiant unique



Simplicité de migration vers un serveur virtuel individuel, au besoin.

Généralement, dès qu'un client se dote d'une solution de surveillance, il souhaite rapidement obtenir davantage de données de surveillance, pour d'autres scénarios. La surveillance réseau avancée permet de répondre aisément à ces nouveaux besoins. S'il souhaite une installation indépendante, il suffit que le client demande à son fournisseur de services de configurer un serveur physique ou virtuel. Le cas échéant, la surveillance se fera toujours par les sondes distantes. Le client continuera à utiliser les sondes installées sur son réseau, sans même devoir investir dans de nouveaux équipements. Le fournisseur de service continuera à veiller au bon fonctionnement du serveur.

Configuration rapide : efforts minimes pour le client.

Le pare-feu du client reste intact, la connexion de la sonde ne nécessitant l'ouverture que d'un seul port. Cette connexion est établie par la sonde depuis le réseau jusqu'au serveur externe. Cette configuration dispense la plupart des clients de modifier la configuration de leur système de sécurité.

Des solutions spécifiques pour les scénarios particuliers

Qui dit configurations spécifiques dit souvent solutions de surveillance sur mesure. Les sondes distantes conviennent justement à de nombreuses applications, au-delà de la simple surveillance centralisée de réseaux distants.

Equilibrage de la charge de travail

Une solution de surveillance réseau granulaire peut grever les performances d'un réseau, selon le nombre de capteurs requis, la technique de surveillance appliquée, le matériel de surveillance utilisé et la topologie du réseau. Par exemple, l'utilisation de renifleurs de paquets mobilise généralement davantage de capacité de traitement et de mémoire RAM que la simple surveillance SNMP car elle suppose d'analyser davantage de données. De même, l'utilisation intensive du protocole WMI exige davantage de ressources.

Répartition de la charge de travail : l'ajout de sondes allège la charge de travail de la sonde locale du serveur central.

Ces techniques de surveillance réseau nécessitent donc des équipements performants pour garantir le traitement suffisamment rapide des données collectées. PRTG permet en revanche de répartir les tâches de surveillance réseau entre plusieurs sondes afin d'alléger la charge de travail du serveur central. Chaque sonde peut être installée sur un système distinct. Les données collectées sont transmises au serveur central PRTG, prêtes à être évaluées.

Transmission cryptée

La version 3 de la norme de cryptage SNMP est encore peu démocratisée. Quantité de dispositifs récents ne proposent encore que SNMP v1, un mécanisme d'authentification extrêmement simple qui transmet les données en texte clair, n'offrant donc pas des garanties de sécurité optimales. Ce protocole convient à la transmission de données non sensibles, comme le niveau d'encre des imprimantes, par exemple. Mais la surveillance d'un routeur exige la communication d'informations plus critiques, qui pourraient notamment révéler les habitudes de navigation de certains utilisateurs.

Les sondes distantes peuvent compenser l'exposition aux risques d'équipements obsolètes.

Peu d'équipements proposent actuellement des alternatives à SNMP v1. Pour veiller à ce que les données sensibles ne soient pas interceptées durant leur transfert vers le serveur central, l'administrateur peut installer une sonde de surveillance à distance sur le réseau des périphériques concernés. Les données collectées seront alors transmises via la connexion cryptée en SSL entre la sonde et le serveur.

Services encapsulés

Comme nous l'avons mentionné précédemment, les sondes peuvent également servir à la surveillance des systèmes généralement inaccessibles de l'extérieur, comme les serveurs Web ou de messagerie sous Windows. Il suffit en effet aux administrateurs d'installer une sonde sur l'un de ces serveurs pour collecter des informations ; au moyen de capteurs WMI, ils peuvent s'informer sur la charge de travail du processeur, l'utilisation de la mémoire et des disques ou le statut actuel des e-mails en attente, par exemple. Les connexions entrantes ne nécessitant pas l'ouverture de ports, cette configuration préserve la sécurité du système. Les données de surveillance restent néanmoins disponibles en permanence, la sonde établissant une connexion avec le serveur central de PRTG depuis l'intérieur du réseau. Le système de notification de PRTG informe immédiatement les administrateurs des éventuels problèmes.

La surveillance sous différentes perspectives

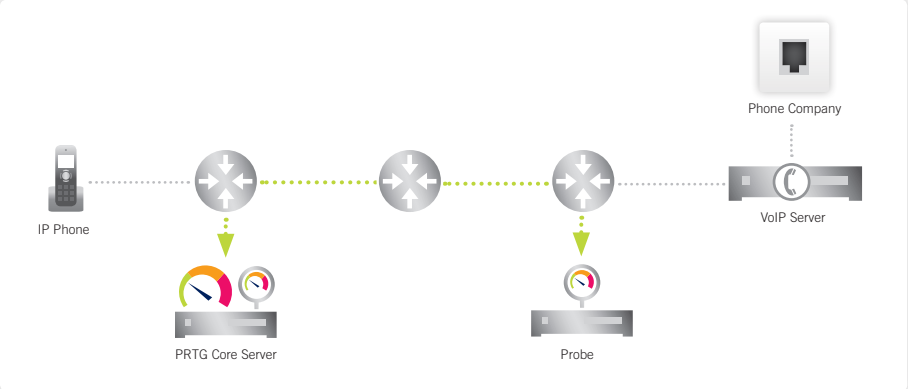
L'image de marque et la réputation de certaines entreprises, voire leur chiffre d'affaires, dépendent grandement de leur site Web ou de commerce en ligne. La moindre panne peut alors faire dégringoler les ventes, d'où la nécessité absolue de surveiller la présence en ligne de l'entreprise. Les multinationales, notamment, sont de plus en plus nombreuses à exploiter un réseau de distribution de contenus, lequel crée une image miroir du contenu Web sur différents serveurs aux quatre coins du globe, de sorte que c'est le serveur le plus proche de l'internaute (dans la topologie réseau) qui lui communique les informations. Cette stratégie permet d'obtenir des temps de réponse (aux requêtes ping) plus courts et le chargement plus rapide des pages.

PRTG permet aux administrateurs d'installer une sonde pour surveiller chaque serveur et leur site Web depuis différentes perspectives.[1] Ils peuvent ainsi comparer aisément les délais de chargement du site sur différents continents, en Europe, en Asie ou en Amérique. Chaque sonde vérifie le temps de chargement via une connexion réseau distincte et transmet ses données au serveur central. L'administrateur peut alors vérifier si les mesures correspondent à celles fixées par la direction et déterminer s'il faut étendre le réseau de distribution de contenus ou procéder à une mise à niveau des systèmes.

Perspectives globales : les sondes permettent de surveiller un site Web sur tous les continents

Et si l'entreprise paie un FAI en contrepartie de garanties de niveau de service, l'administrateur peut contrôler si les niveaux de service contractuels sont respectés. Il suffit d'installer une sonde avec capteur de qualité de service sur le serveur hébergé par le FAI pour analyser la qualité du réseau entre le serveur hôte et le lieu où se situe l'entreprise.

Illustration :
Surveillance de la qualité de service



[1] Une illustration de la surveillance Cloud est disponible à l'adresse http://www.cloudclimate.com/

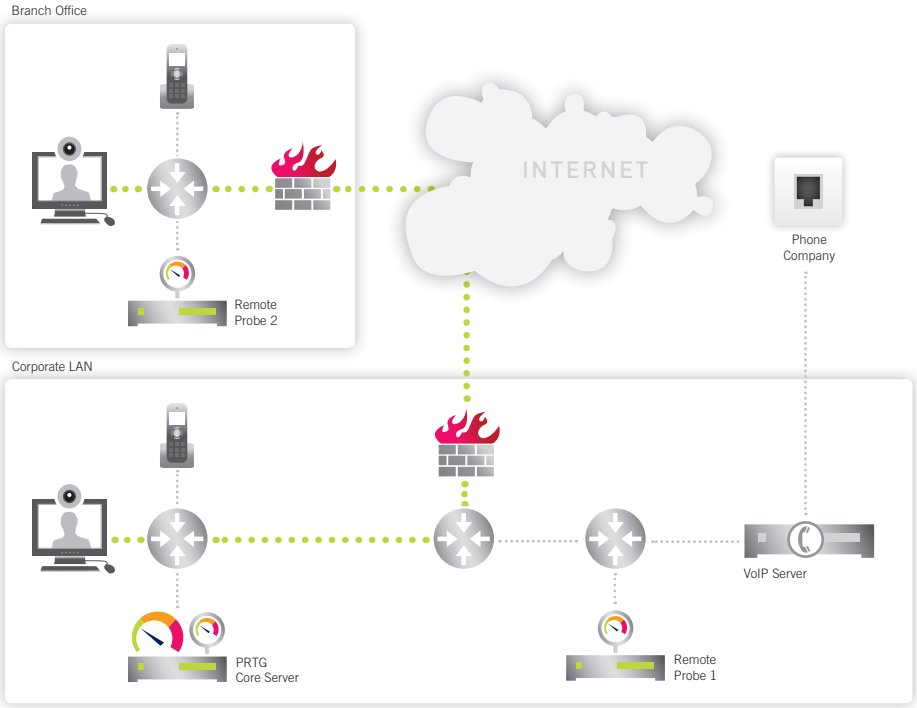
Evaluation de la qualité de service

La qualité de service est déterminante pour le bon déroulement des opérations en réseau, ainsi que pour l'intégration de solutions Voice over IP (VoIP). Les communications vocales basées sur des paquets UDP sont en effet particulièrement sensibles aux perturbations de type perte de paquets, instabilité ou retard de transmission de paquets. Des équipements professionnels, comme les routeurs haut de gamme de Cisco, permettent d'évaluer la qualité de service du réseau entre deux périphériques via le protocole IP-SLA. PRTG peut justement lire et analyser ces données.

Les sondes permettent d'évaluer la qualité de service d'un réseau sans équipement coûteux.

A défaut de ce type d'équipement dans l'entreprise, l'administrateur peut installer des sondes pour concevoir sa propre ligne de mesure de la qualité de service via les capteurs de qualité de service intégrés à PRTG. La connexion peut aussi bien s'effectuer entre le serveur PRTG et une sonde qu'entre deux sondes, qui pourront être installées sur n'importe quel serveur du LAN, voire via Internet. Les possibilités sont donc multiples. L'une des sondes gère alors la collecte des données et envoie les valeurs mesurées au serveur pour qu'il les évalue plus en détail. Quant au système PRTG, il surveille la connexion en temps réel et avertit l'administrateur en cas de dépassement des seuils critiques. L'administrateur peut ainsi déterminer si le réseau offre la qualité minimale requise par la solution VoIP.

Illustration :
Surveillance d'une solution VoIP



Un concept simple aux applications multiples

La surveillance distribuée d'un réseau au moyen de sondes distantes permet d'envisager de multiples applications. Quels que soient les systèmes surveillés, les sondes transmettent en permanence toutes les données au serveur central. L'administrateur dispose ainsi, en un clin d'œil, d'une parfaite visibilité sur toutes les installations surveillées.

En installant plusieurs sondes à distance, les entreprises peuvent centraliser la surveillance de toutes leurs succursales. Quant aux fournisseurs de services informatiques, ils peuvent proposer des services de surveillance sur site à leurs clients, avec la garantie d'interventions minimales sur le réseau et sans avoir à configurer un serveur virtuel distinct pour chaque client. Les sondes conviennent également à des besoins techniques spécifiques, notamment d'équilibrage de la charge de travail dans les installations étendues ou intensives en capacité de traitement, de renforcement de la sécurité ou de surveillance de services encapsulés, tels que des serveurs Web ou de messagerie. Et grâce à leur flexibilité de configuration, les sondes permettent de surveiller un réseau sous différentes perspectives (comme dans le cas des réseaux de distribution de contenus) ou d'évaluer la qualité de service d'un réseau. Les données transitant entre les différents composants du logiciel PRTG sont systématiquement transmises via une liaison cryptée en SSL, pour garantir une sécurité optimale en permanence.

L'installation sur un serveur et une licence suffisent : toutes les licences PRTG couvrant d'office plusieurs sondes, rapides à installer et configurables via l'interface du serveur. L'entreprise n'a ainsi plus qu'à se charger de la maintenance du seul serveur central et de son système d'exploitation, ce qui réduit considérablement ses coûts.

À propos de Paessler AG

La société Paessler, fondée en 1997 et basée à Nuremberg en Allemagne, est spécialisée dans le développement de logiciels de surveillance réseau et d'analyse de serveur Web.

La solution Paessler est déjà utilisée à travers le monde par plus de 150.000 administrateurs réseau, opérateurs de site Web, fournisseurs de services Internet et autres professionnels de l'informatique.

Des versions gratuites et d'évaluation de tous les produits peuvent être téléchargées sur www.fr.paessler.com.

Paessler AG
Bucher Str. 79a, 90419 Nuremberg, Allemagne
www.fr.paessler.com, info@paessler.com

N° d'identification de T.V.A. : DE 217564187
N° d'identification fiscale : FA Nürnberg 241/120/60894
Immatriculation au Registre du Commerce : Tribunal d'instance (Amtsgericht) Nuremberg, HRB 23757

Comité directeur : Dirk Paessler, Christian Twardawa
Président du conseil de surveillance : Dr. Marc Rössel