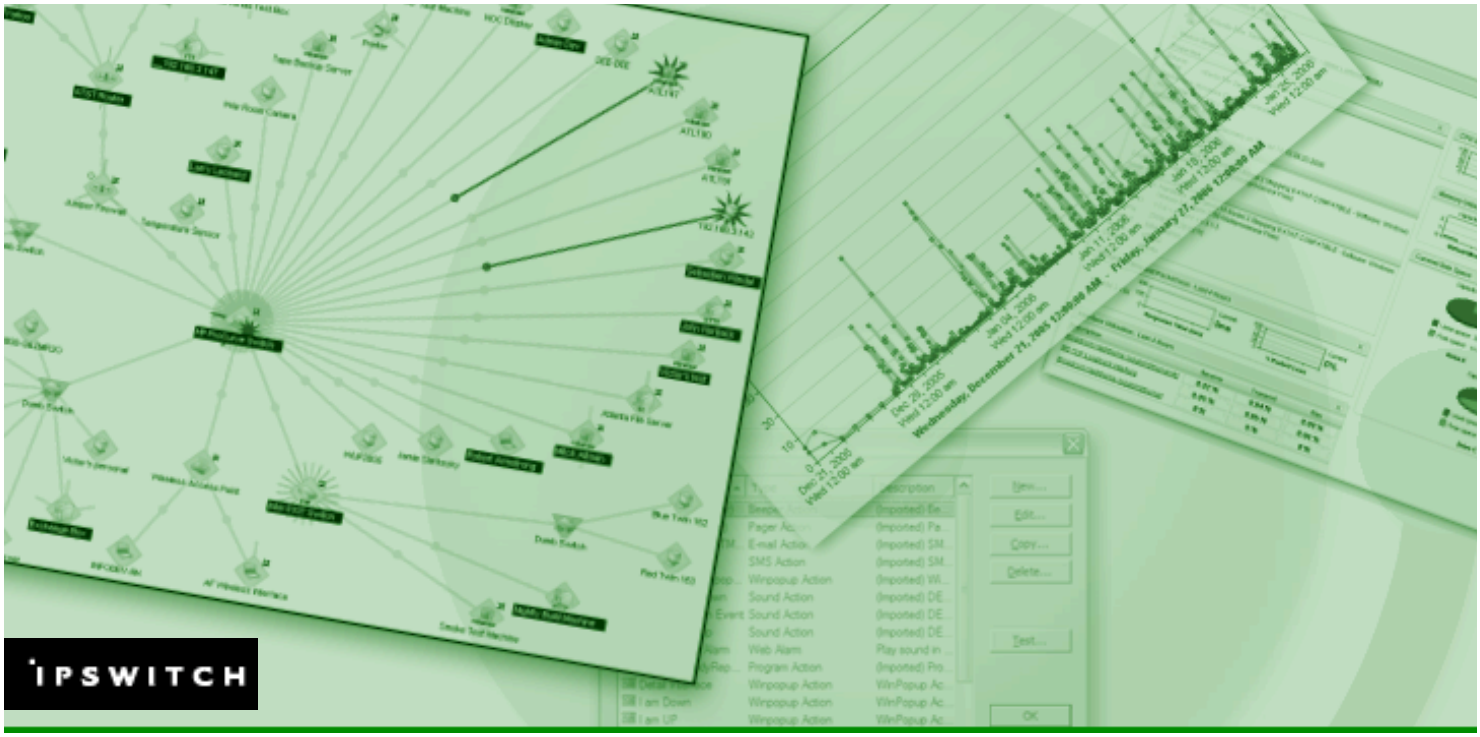


MSP-Funktionalität in WhatsUp Professional 2006

Managed Service Provider (MSP) überwachen dezentrale Unternehmensnetze - ein Markt, der stark wächst. Dieser Überblick beschreibt, wie WhatsUp Professional von einem MSP, oder auch von Firmen mit Niederlassungen außerhalb ihres WAN, eingesetzt werden kann.

IPSWITCH WhatsUp Professional 2006

Wie kann ein MSP dezentrale Netzwerke von Kunden überwachen?

Beim traditionellen Netzwerkmonitoring wird die Überwachungssoftware auf einem Server konfiguriert, der an das LAN oder WAN angeschlossen ist und einen Teil des Netzes bildet. Sobald Probleme auftauchen, kann der Prozess der Fehlersuche und –beseitigung schnell gestartet werden. Meist geschieht das durch jemanden, der vor Ort oder aus unmittelbarer Nähe agieren kann. Ein MSP jedoch muss nicht im selben Gebäude, derselben Stadt oder auch nur demselben Land sitzen wie der Kunde, dessen Netze überwacht werden.

Da die Kunden sich bei der Funktionsfähigkeit ihrer Systeme auf ihren MSP absolut verlassen, muss der MSP ein Problem so schnell wie möglich diagnostizieren und bewältigen. Wenn ein Fehler auftritt, muss dieser aus der Ferne gefunden und beseitigt werden können – am besten bevor der Kunde ihn bemerkt. Eine langwierige Reise zum Kunden ist oft nicht akzeptabel.

Sie haben die Wahl!

Mit einem durchdachten Einsatz von WhatsUp Professional können MSPs Zugriff auf dezentrale Kundennetzwerke erhalten und dabei eine Vielfalt an Verbindungsarten und Sicherheitseinstellungen nutzen. Das sorgt dafür, dass der MSP eine große Bandbreite an Kunden und Kundensituationen erreichen und verwalten kann; zugeschnitten auf die vorhandene Technik, auf spezielle Netzwerkmanagement-Lösungen, die dem Kunden am besten dienen und nicht zuletzt auf die technischen Fähigkeiten des Personals beim Kunden.

So gelingt der Start

Die Basis der Überwachungslösung bildet die zentrale Installation von WhatsUp Professional. Diese kann auf unterschiedliche Weise genutzt werden - ganz nach Typus der Kunden - und ist unbedingt erforderlich für eine reibungslose Anbindung der überwachten Netze.

Sobald die zentrale Installation von WhatsUp erfolgt ist, können Sie für jeden Kunden die Geräte, die Sie überwachen möchten, hinzufügen. Spezielle Konfigurationshinweise für unterschiedliche Unternehmenstypen behandeln wir weiter unten.

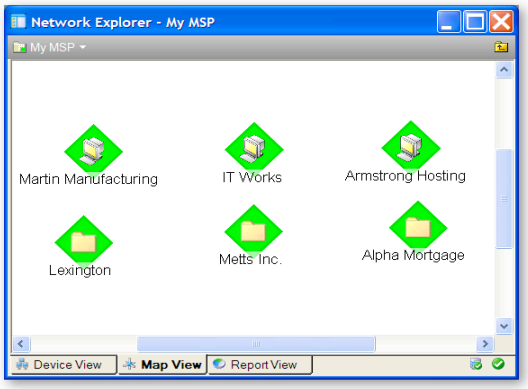


Schaubild 1 – MSP-Ansicht von Kundennetzen

Aufbau eines Kundennetzwerks

Bevor Sie als MSP den Aufbau des Netzwerks eines Kunden starten, sollten Sie einige Punkte klären. Die folgenden Fragen helfen Ihnen herauszufinden, was alles möglich und was praktisch umsetzbar ist:

- Möchte der Kunde Reports in Echtzeit?
- Gibt es ein VPN zwischen Kunde und MSP?
- Hat der Kunde eine große Anzahl an Netzwerkgeräten, die überwacht werden sollen?
- Möchte der Kunde, dass Administrationsaufgaben in seinem Netzwerk ausgeführt werden?
- Möchte der Kunde Polling auch ohne VPN-Verbindung erlauben?
- Möchte der Kunde, dass der MSP nur öffentlich zugängliche Netzwerkkomponenten überwacht?
- Muss der MSP SNMP-Traps des Kunden an ein zentrales, übergeordnetes Überwachungssystem senden?

Schaubild 1 zeigt die MSP-Installation von WhatsUp Professional mit 6 überwachten Kunden. Die oberen drei Situationen stellen die Überwachung entfernter WhatsUp-Installationen und die unteren drei die Überwachung interner oder externer Netzelemente dar.

Schaubild 2 zeigt jede der vier Unternehmenstypen, die wir in diesem Überblick behandeln. Auch wenn es noch weitere Abstufungen geben mag, sollten diese die meisten Kundenanforderungen treffen.

A - Kleines Netzwerk mit VPN

B - Großes Netzwerk mit VPN

C - Großes Netzwerk ohne VPN **D** - Überwachen öffentlich zugänglicher Netzkomponenten

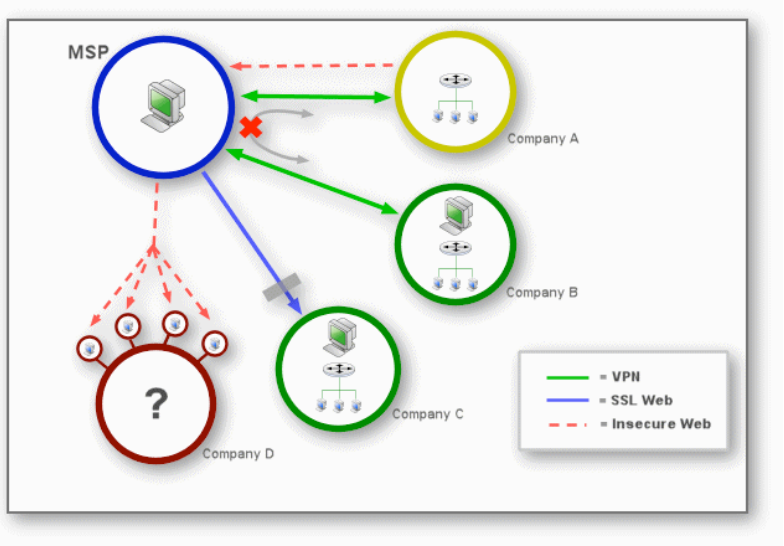
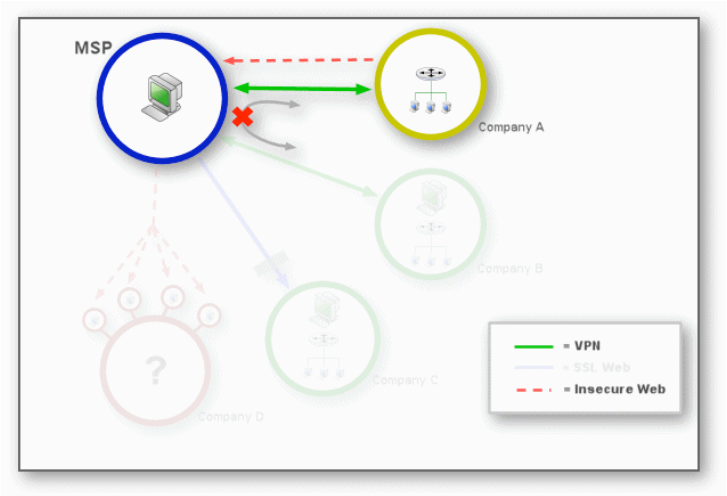


Figure 2 - Typisches Kundennetz

Der folgende Abschnitt liefert einen Abriss jedes dieser Unternehmenstypen und ihre Einbindung in eine MSP-Installation mit WhatsUp Professional. Die Legende unten rechts zeigt die Verbindungsart, die der MSP für die spezifische Firmenart verwendet.

Unternehmenstyp A



Bei dieser Konfiguration betreibt der MSP eine VPN-Verbindung zum Kunden und übernimmt die komplette Überwachung des Netzwerks . In WhatsUp wird in einer einzigen Gerätegruppe das vollständige Kundennetz angezeigt. Der Kunde hat nur wenige zu überwachende Geräte, so dass die Datenlast sehr gering ist.Die Firewall des MSP ist so eingestellt, dass die Daten von einem Kunden nicht von anderen Kunden eingesehen werden können

.Reporting

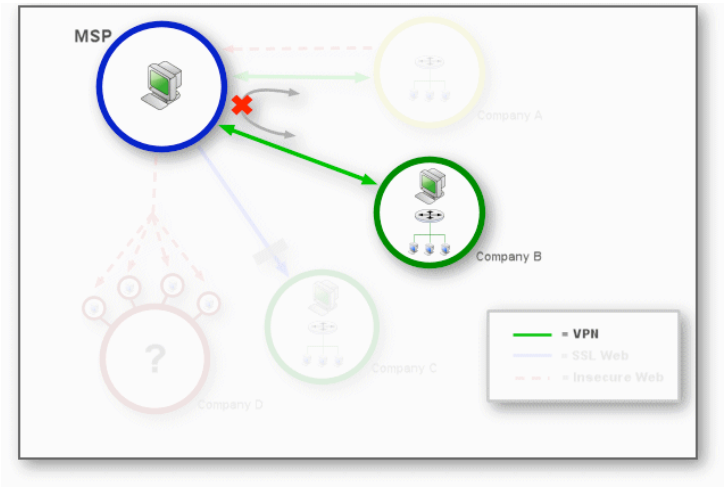
Der Kunde sieht seine WhatsUp Professional-Reports über eine Web-Anbindung zum öffentlichen Webserver des MSP. Über ein Nutzerkonto wird der Zugriff auf Geräte- und Gruppenreports beschränkt. Die WhatsUp Web-Schnittstelle ist auf Port 80 eingestellt und die Firewall des MSP ist so konfiguriert, dass nur bestimmte IP-Adressen von Kunden auf den Port zugreifen können.

Benachrichtigungen

Da die MSP-Funktionalität von WhatsUp alle Benachrichtigungsarten für diesen Unternehmenstyp übernimmt, können die Einstellungen einfach über die Action Policy erledigt werden. Gehen Sie in der WhatsUp-Konsole auf “Action Policy Library” und legen Sie Parameter für Ihren Kunden fest. Da es unwahrscheinlich ist, dass von Kundenseite Probleme gelöst werden, brauchen Sie nur MSP-Mitarbeiter zu benachrichtigen. Nach Erstellung der Action Policy können Sie die “Bulk Field Change”-Funktion nutzen, um die Einstellung für alle Geräte der Gerätegruppe des Kunden zu übernehmen.

Die gewünschte Aktion kann eine Reihe von Abfolgen - speziell zugeschnitten für diesen Kunden - beinhalten. Zum Beispiel können E-Mail-Nachrichten verschickt werden, die den Kundennamen in der Betreffzeile führen.

Unternehmenstyp B



Genau wie bei Unternehmenstyp A erlaubt auch der Typ B dem MSP eine VPN-Verbindung zu seinem Netzwerk. Hier ist der MSP nur damit befasst, die dezentrale WhatsUp-Installation so zu konfigurieren, dass das Kundennetz vor Ort überwacht werden kann. Der MSP nutzt die VPN-Verbindung, um die Funktionsfähigkeit von WhatsUp zu prüfen und um Zugriff auf das Web-Interface zu bekommen, ohne dies für das öffentliche Internet zu öffnen.

Die Firewall des MSP ist so konfiguriert, dass Daten eines Kunden nicht von einem anderen eingesehen werden können.

Diese Konfiguration ist speziell geeignet für Kunden, die ein relativ großes Netz haben oder aktive Gerätegruppen besonders intensiv überwachen möchten. Da der Hauptteil der Überwachung lokal erfolgt, ist die VPN-Datenlast gering.

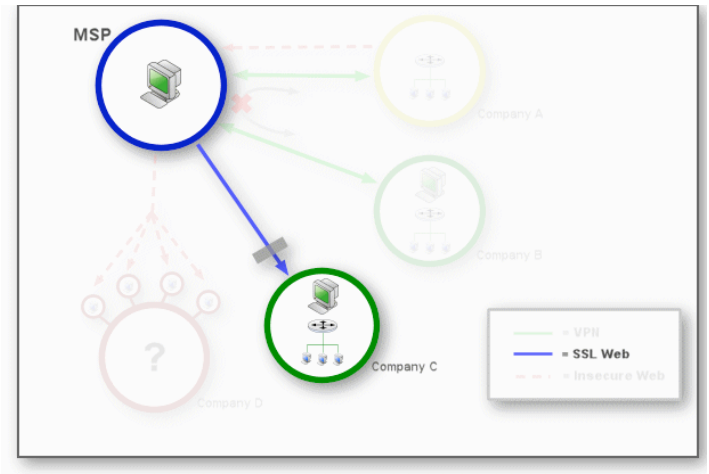
Reporting

Das Reporting besorgt die dezentrale WhatsUp-Installation. Der Kunde kann die Berichte lokal einsehen, der MSP durch ein VPN-gesichertes Web-Interface.

Benachrichtigungen

Aktionen werden beim Kunden definiert und können so eingerichtet werden, dass nur der MSP benachrichtigt wird oder auch ein Techniker beim Kunden vor Ort.

Unternehmenstyp C



Bei diesem Unternehmenstyp installiert der MSP WhatsUp Professional dezentral beim Kunden und nutzt eine sichere SSL-Verbindung zur Konfiguration und Überwachung über das Web-Interface.

Auf Kundenseite wird die Firewall so eingestellt, dass nur die IP-Adresse des MSP Verbindung zu dem Port bekommt, auf dem der SSL-Webserver läuft.Die zentrale WhatsUp-Installation überwacht die Verbindung zum sicheren Web-server, erledigt jedoch nicht den Hauptteil des Netzwerkmonitorings.

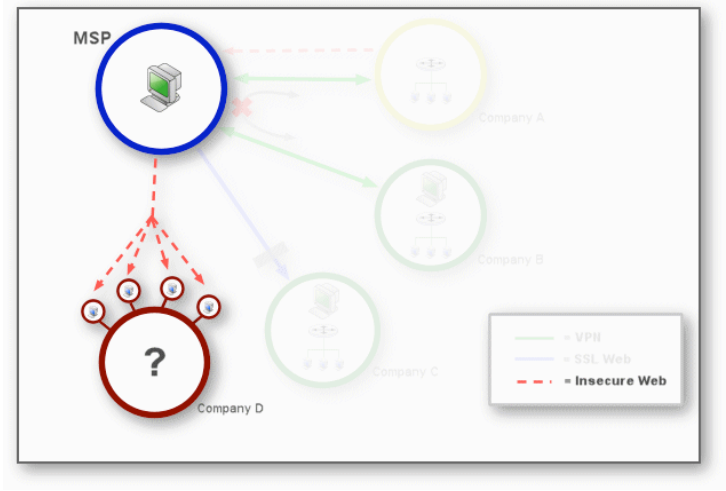
Reporting

Das Reporting übernimmt die dezentrale WhatsUp Professional-Installation und kann vom Kunden lokal eingesehen werden, vom MSP über das sichere SSL-Webinterface.

Benachrichtigungen

Aktionen werden beim Kunden definiert und können so eingerichtet werden, dass nur der MSP benachrichtigt wird oder auch ein Techniker beim Kunden vor Ort.

Unternehmenstyp D



Der Unternehmenstyp D unterscheidet sich von den anderen. Bei diesem Einsatz wird der MSP nur benötigt, um die öffentlich zugänglichen Netzwerkelemente des Kunden zu überwachen: öffentliche FTP-Server, Websites, Mailserver etc. Das Netzwerk des Kunden wird hierbei nicht überwacht und der MSP kümmert sich auch nicht darum, was hinter der Unternehmens-Firewall passiert Das wird durch das Fragezeichen in der Grafik symbolisiert.

Dieser Einsatztyp kann die Erweiterung zu einer Überwachung des internen Netzes durch einen MSP darstellen.

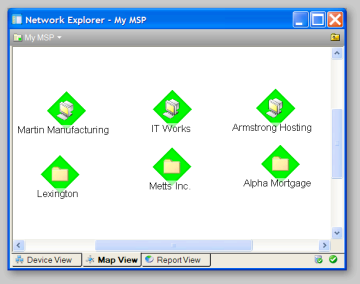
Reporting

Das Reporting kann wie beim Typ A erfolgen, doch dürfte hier in den meisten Fällen nicht das Personal und Know-how vorhanden sein, um die Netzwerkfunktion sicherzustellen. Deshalb sollte der MSP für die Fehlerbehebung zuständig sein und den Kunden mit periodischen Reports regelmäßig über den Status der öffentlich zugänglichen Netzkomponenten unterrichten.

Benachrichtigungen

Aktionen und Benachrichtigungen können genauso festgelegt werden wie für Unternehmenstyp A beschrieben.

Verbindung über WhatsUp Professional



Wenn Sie eine dezentrale Instanz von WhatsUp überwachen (siehe die oberen 3 Geräte in der linken Grafik), können Sie einfach auf das Icon klicken, um das zugehörige Kontextmenü zu starten.

1. Wählen Sie in dem Menü “Remote Desktop”, um sich mit dem Rechner, auf dem WhatsUp läuft, zu verbinden.
2. Wählen Sie “Browse” um einen Web-Browser für das WhatsUp Web-Interface für das spezielle Gerät zu öffnen. Eventuell müssen Sie dafür die Einstellungen bei “Device Properties” anpassen.

Entscheidungsmatrix

Wir haben die unterschiedlichen Unternehmenstypen vorgestellt und kommen nun zu den oben angemerkten Vorüberlegungen. Das Diagramm zeigt alle wichtigen Ausgangsfragen und den Unternehmenstyp, der dafür in Frage kommt. Ein Feld ohne “X” bedeutet, dass der Punkt nicht zum Unternehmenstyp passt. Bitte beachten Sie, dass wir hier nur allgemeine Grundregeln aufstellen können und dass manche Firmen eine Mischung aus den definierten Typen bilden.

Ausgangspunkt	A	B	C	D
Kunde möchte Reports in Echtzeit	X	X	X	
Kein VPN verfügbar			X	X
Kunde möchte >10 Geräte überwachen lassen (begrenzte Bandbreite)		X	X	
Kunde möchte Administrationsaufgaben für sein Netzwerk selbst übernehmen		X	X	*
Polling sollte auch ohne VPN.-Anbindung weiter laufen		X	X	
Kunde möchte nur öffentliche Netz-Angebote überwachen lassen				X
MSP muss SNMP-Traps des Kunden zurück an die zentrale Konsole senden	X	X		
WhatsUp soll in jeder Niederlassung installiert werden		X	X	

* MSP ist nicht befasst mit diesem Teil des Netzwerks.

Zusammenfassung

Mit etwas Planung und Kundenanalyse kann ein MSP mit den bestehenden Funktionen von Ipswitch WhatsUp Professional 2006 ein effizientes Netzwerkmonitoring für seine Kunden aufsetzen. Mit diesem Überblick liefern wir Ihnen einige Ansatzpunkte, wie ein MSP die Überwachung dezentraler Systeme angehen kann. Neben dieser Kurzanalyse werden tiefer gehende Fragen zu WhatsUp in der Online-Hilfe, dem Handbuch und in der Knowledge-Base unter www.ipswitch.com beantwortet.
Einstellungen von Firewalls und VPN sollten zusätzlich untersucht werden, da diese von der beim Kunden eingesetzten Hard- und Software abhängen.