Be Proactive, Not Reactive!

Installation Examples

for Sentry-go *v6*

March, 2014

http://www.Sentry-go.com

Sentry-go is an easy to use monitoring solution that allows you to monitor what you want, when you want. Whether you're monitoring desktops or servers, either directly or indirectly as a 3rd party, Sentry-go provides the features you need at a price you'll like!

Setting up a Sentry-go monitored environment

Sentry-go is a quick & easy to use monitoring solution for the Windows platform, allowing you to monitor what you want, when you want! Its flexibility means that you can install it within different environments in a way that's determined by your specific needs and the needs of the target environment.

In this paper, we will consider how to use Sentry-go in a number of different environments and how you might set it up to maximise benefit whilst minimising the amount of external configuration needed.

Although your environment may differ slightly from these, the ideas put forward can be modified to suit most installations.

Firewalls

Today, most organisations, even smaller ones use a firewall to protect their network and access to data. This may be the Windows Firewall running locally on each server, or a dedicated system protecting your internal network or sub-networks. When accessing monitored information, such as that provided by Sentry-go from outside the local server or outside your own Windows domain, you will need to have permission to do so by allowing TCP/IP traffic through this firewall to and from the appropriate tools & software.

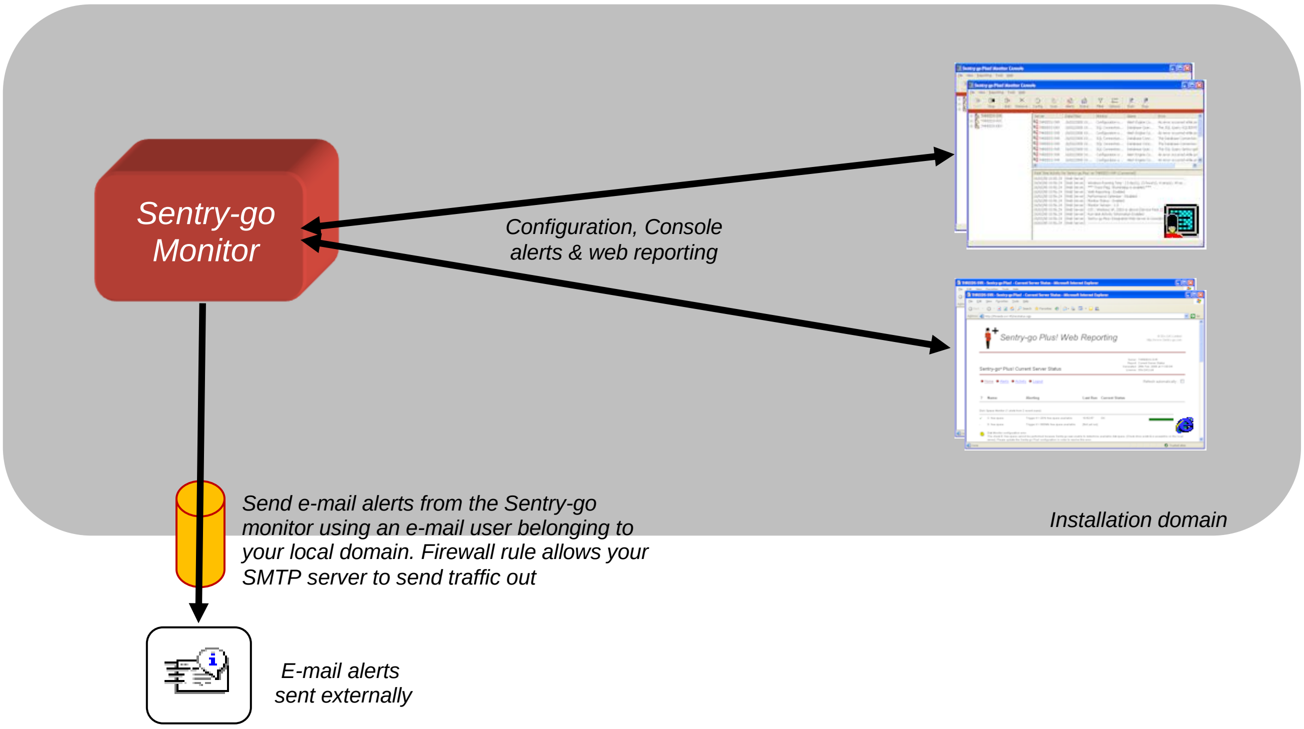
Depending on your organisation's rules and procedures, this may be relatively easy or harder to achieve. Sentry-go provides ways for you to gain access to information in a number of different ways in order to take into account rthese rules and these are highlighted in the sections that follow.

Installation Scenarios

In the examples that follow, we will show and discuss a number of environments and how Sentry-go information can be accessed from them. We will also consider the role of 3rd party support teams and how they can access information from different domains/customers at the same time.

Single machine with internal access & external e-mail alerting

In this simple model, a single Sentry-go server monitor is running on a single server. Access from client tools or web browsers to the monitor is made solely internally, and alerts such as e-mail alerts are being sent externally.


Sentry-go Monitor
Configuration, Console alerts & web reporting
Installation domain
E-mail alerts sent externally

Send e-mail alerts from the Sentry-go monitor using an e-mail user belonging to your local domain. Firewall rule allows your SMTP server to send traffic out

Configuration

In this case, everything is internal within your network domain, except the ability to send e-mail alerts. Assuming you already have external e-mail access from your desktops, configure the monitor to use the same e-mail & SMTP settings and use a local sender's e-mail address – e.g. Sentry-go@<Your Company Domain>. This should allow access without the need for any firewall configuration changes.

Firewall Changes

None.

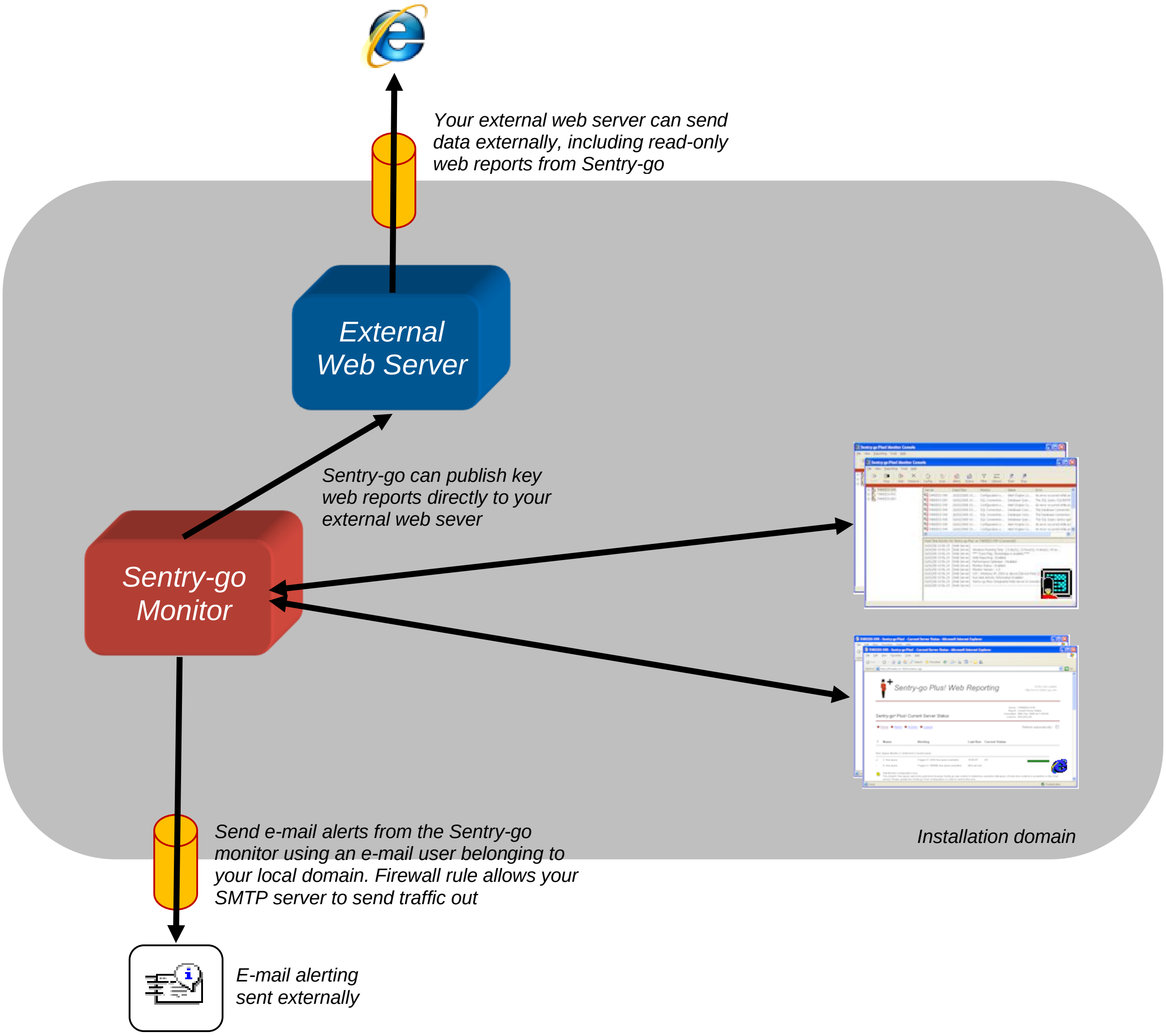
Pros & Cons

This scenario is ideal when you don't need external access to monitored information through the web. Alerts are triggered and can be sent externally via your standard e-mail gateway. If alerts are received you can access the monitor either locally or remotely (e.g. using Remote Desktop/Terminal Services etc.) in order to investigate further.

Access via client tools & web browser is limited to internal machines only. Alerting is limited to standard methods such as e-mail, which can be slowed depending on network conditions etc.

Single machine with internal access, published web reporting and external e-mail alerting

In this next option, we've added the ability to review key web reports from the monitor, using your existing web server. All other options remain the same.



Your external web server can send data externally, including read-only web reports from Sentry-go

Sentry-go can publish key web reports directly to your external web sever

Send e-mail alerts from the Sentry-go monitor using an e-mail user belonging to your local domain. Firewall rule allows your SMTP server to send traffic out

E-mail alerting sent externally

Configuration

By enabling Sentry-go's web publishing feature (available with all server monitors), the system will periodically copy or FTP key Sentry-go web reports to your existing web server. As this already has access through our firewall (or may be external to our network completely), no changes are required.

Firewall Changes

None.

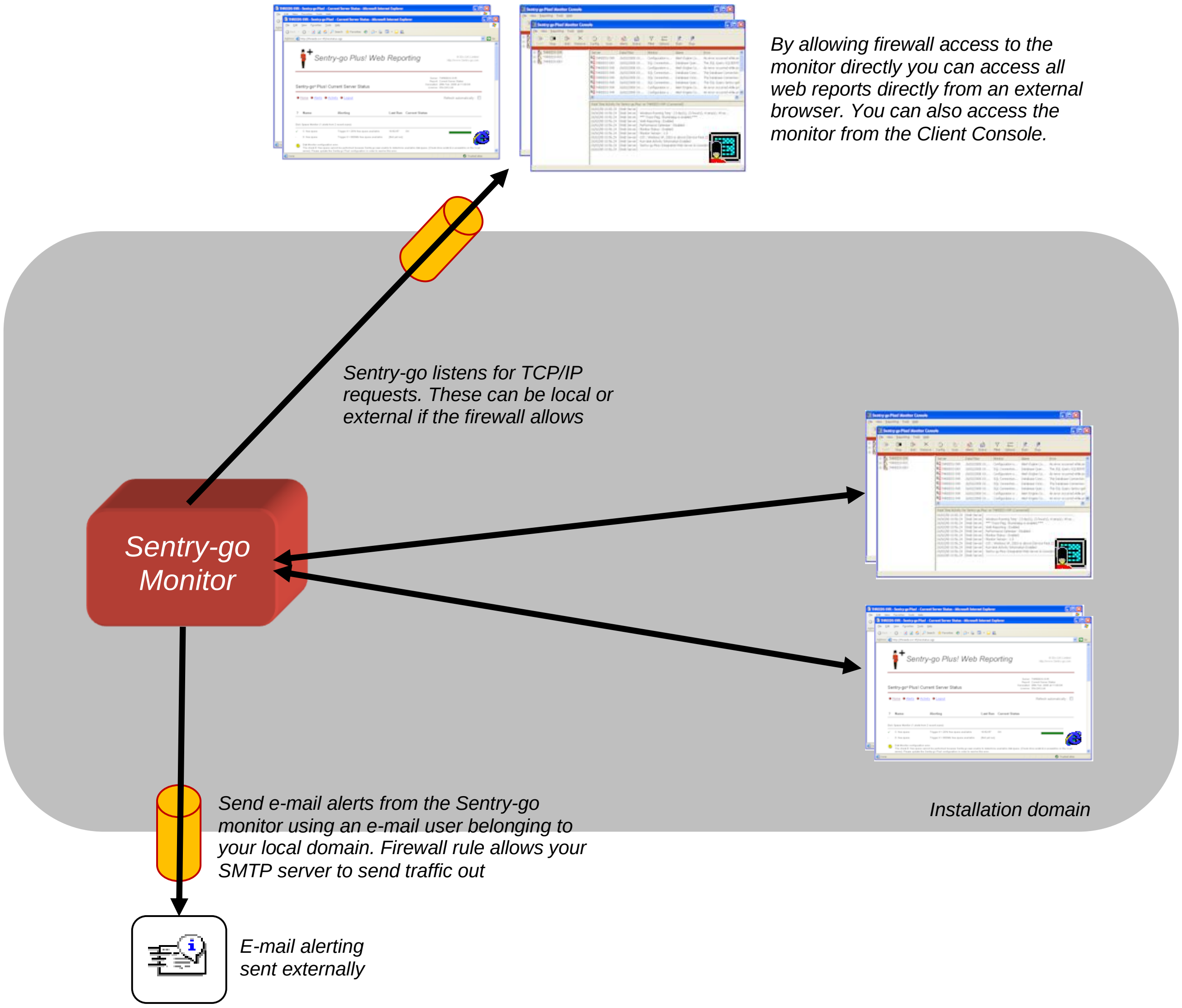
Pros & Cons

In addition to the above, we can access key monitored information (such as recent status) from a web browser using a standard URL, without needing to configure our firewall or provide access to the monitor itself from the outside world.

More detailed information & configuration settings etc. are still only available internally.

Single machine with full access, full external reporting and external e-mail alerting

Although we still only have a single server environment, this is one of the more flexible configurations. With it, you have complete control over the monitor and its web reports from within or outside your own network.



By allowing firewall access to the monitor directly you can access all web reports directly from an external browser. You can also access the monitor from the Client Console.

Sentry-go listens for TCP/IP requests. These can be local or external if the firewall allows

Send e-mail alerts from the Sentry-go monitor using an e-mail user belonging to your local domain. Firewall rule allows your SMTP server to send traffic out

E-mail alerting sent externally

Configuration

In this configuration, we have full external access to the monitor. To enable this, we must configure the firewall to allow traffic in/out of the monitor’s configured listen port (which company procedures may or may not allow). Access can still be made locally and alerts are triggered as before, through your SMTP server.

Firewall Changes

Add rules to allow the monitor to receive and send TCP/IP traffic externally. See later for more information.

Pros & Cons

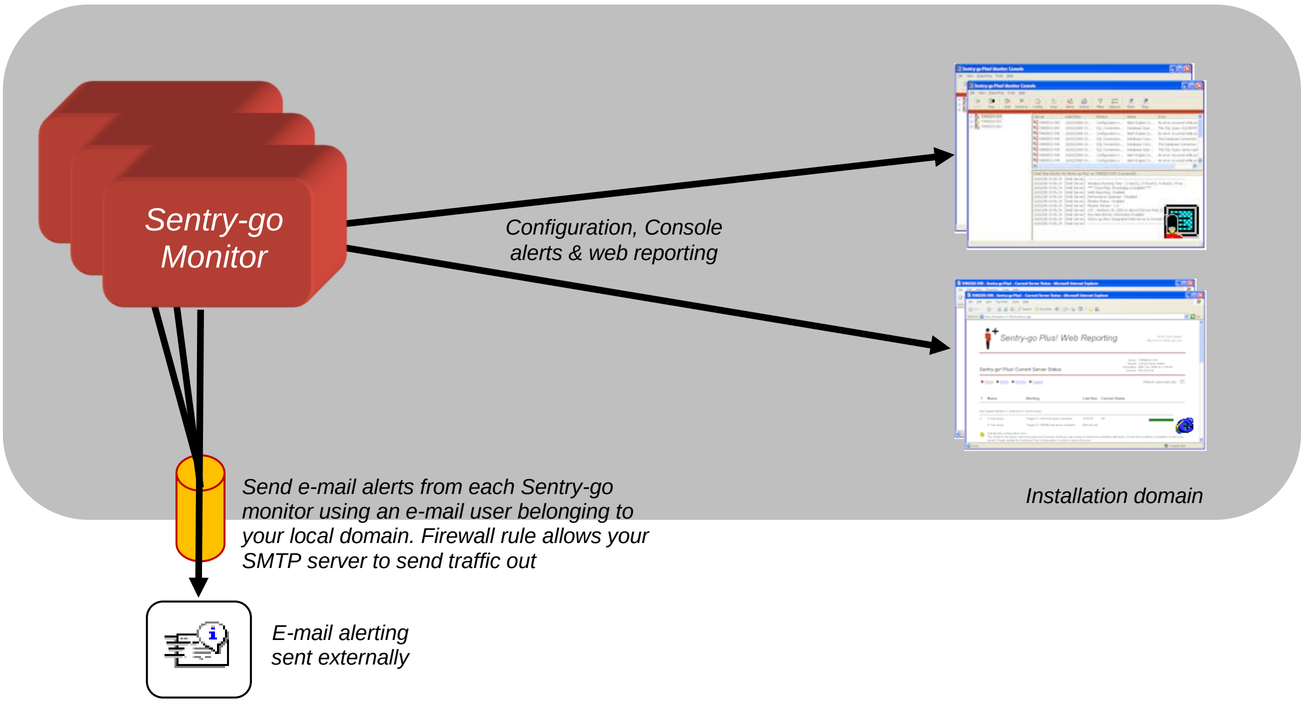
Full access is now available, internally or externally from both web browsers & client tools. Real-time alerts & configuration settings are also accessible internally or externally.

Security-wise, this option requires careful planning – e.g. to set a password for web access/configuration settings, limit access to specific IP-addresses etc.

See "Firewall Rules" later for more information.

Multiple machines, internal access, external e-mail alerting

We now have a number of Sentry-go monitors running within your environment. Access from client tools or web browsers to each monitor is made internally, whilst alerts such as e-mail can be sent externally, again from each monitor.


Sentry-go Monitor
Configuration, Console alerts & web reporting
Send e-mail alerts from each Sentry-go monitor using an e-mail user belonging to your local domain. Firewall rule allows your SMTP server to send traffic out
Installation domain
E-mail alerting sent externally

Configuration

Each monitor is accessible internally and each can send e-mail alerts through your SMTP server.

Firewall Changes

None.

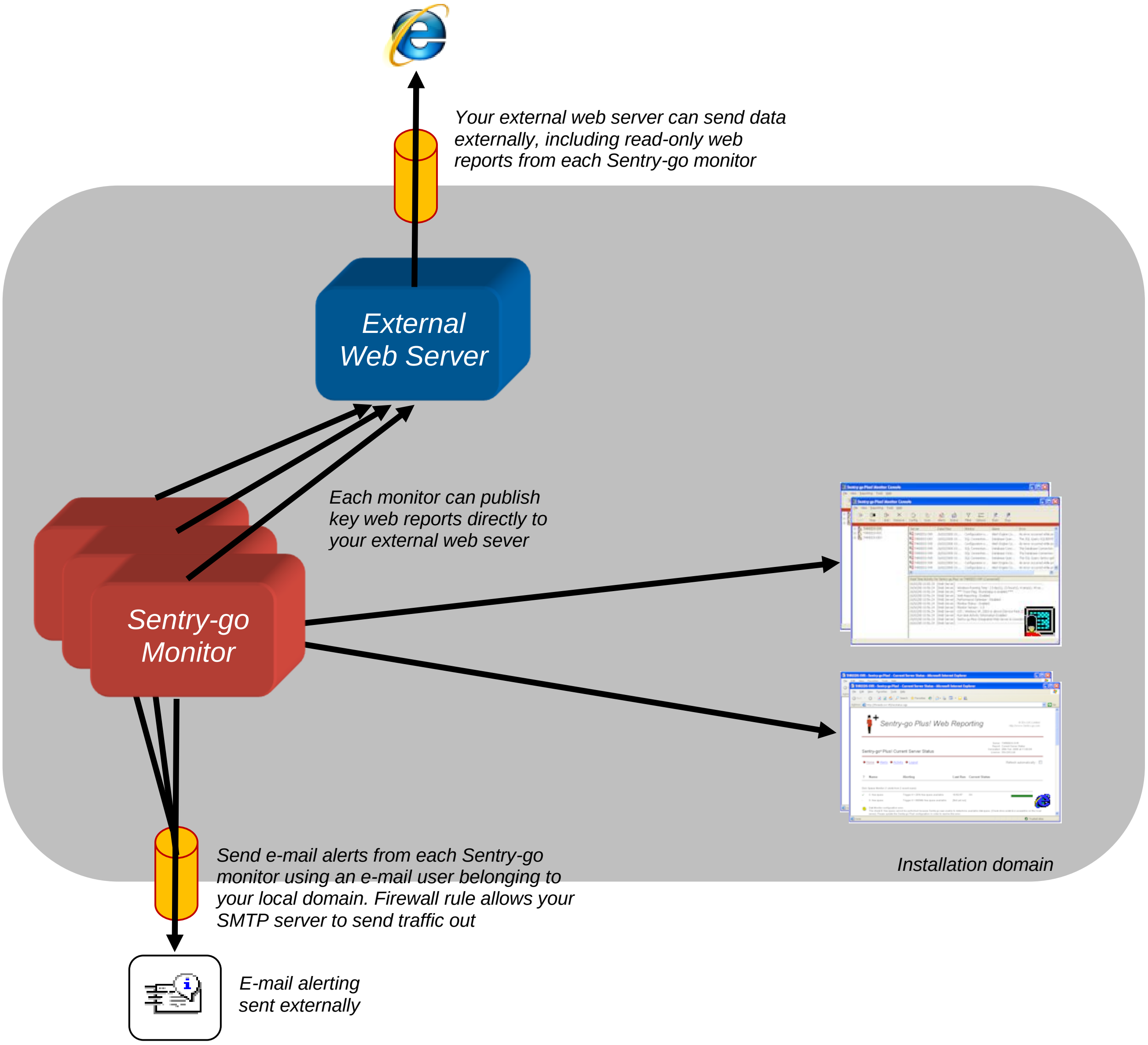
Pros & Cons

As before, this scenario is ideal when you don't need external access to monitored information through the web. You can still access reports locally or using Remote Desktop/Terminal Services etc. Alerts are triggered and can be sent externally via your standard e-mail gateway.

Access to each server via client tools & web browser is limited to internal machines only. Alerting is limited to standard methods such as e-mail, which can be slowed depending on network conditions etc.

Multiple machines with internal access, published web reporting and external e-mail alerting

Here, we have a number of Sentry-go monitors, each of which publish key web reports to your existing web server (or web provider). Access from client tools or web browsers to each monitor is made internally within your network, whilst alerts such as e-mail can be sent externally, again from each monitor.



Your external web server can send data externally, including read-only web reports from each Sentry-go monitor

Each monitor can publish key web reports directly to your external web sever

Send e-mail alerts from each Sentry-go monitor using an e-mail user belonging to your local domain. Firewall rule allows your SMTP server to send traffic out

E-mail alerting sent externally

Configuration

In this configuration, we’ve enabled Sentry-go’s web publishing feature for each monitor. Periodically, the monitor will copy or FTP key Sentry-go web reports to your existing web server, which already has access through your firewall (or may be external to our network completely).

Firewall Changes

None.

Pros & Cons

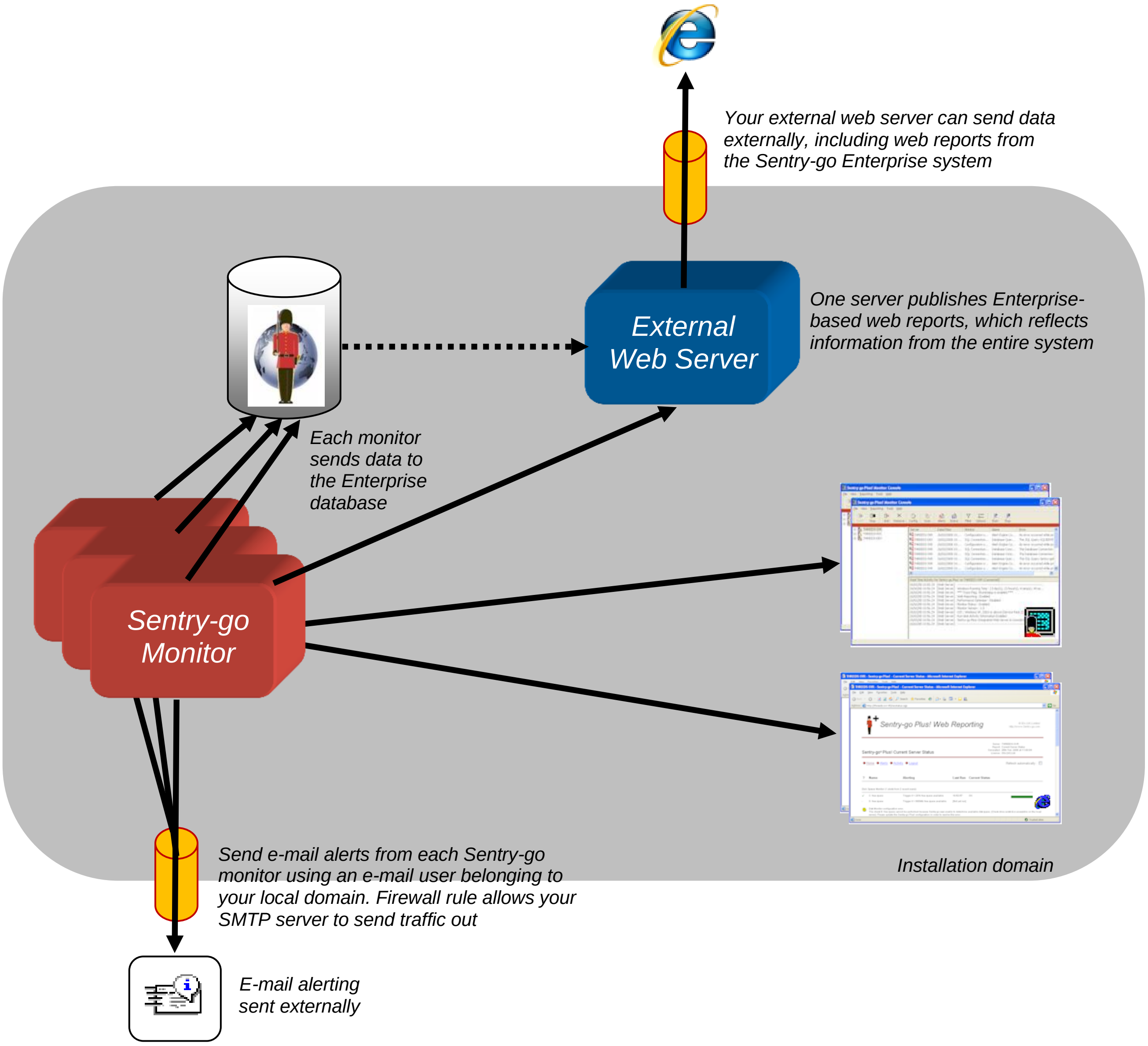
This means we can access key monitored information (such as recent status) from a desktop browser from each monitor, without needing to configure our firewall or provide access to the monitor itself from the outside world.

More detailed information & configuration settings etc. are still only available internally and reports can only be accessed individually for each server/monitor.

Multiple machines, internal access, published Enterprise reporting, external e-mail alerting

In this scenario, we've installed the Sentry-go Enterprise Option, a separate feature that allows information from your monitors to be collated centrally in a SQL Server database. It also allows additional "enterprise" web reports to be accessed, giving combined details from all monitors within the environment.

Access from client tools or web browsers to each monitor is made internally within your network only, whilst alerts such as e-mail can be sent externally, again from each monitor.



Your external web server can send data externally, including web reports from the Sentry-go Enterprise system

One server publishes Enterprise-based web reports, which reflects information from the entire system

Each monitor sends data to the Enterprise database

Send e-mail alerts from each Sentry-go monitor using an e-mail user belonging to your local domain. Firewall rule allows your SMTP server to send traffic out

Installation domain

E-mail alerting sent externally

Configuration

The Enterprise Option is an optional component that can be purchased and used with Sentry-go server monitors. It uses a SQL Server database to collate monitoring information from all monitors within your domain. Using these details, Sentry-go can periodically publish web reports to your existing web server, as before, but it can now publish single “enterprise” reports, showing details from all monitors combined. These reports can then be accessed from your external web server (or provider) without the need to change your firewall settings.

Firewall Changes

None.

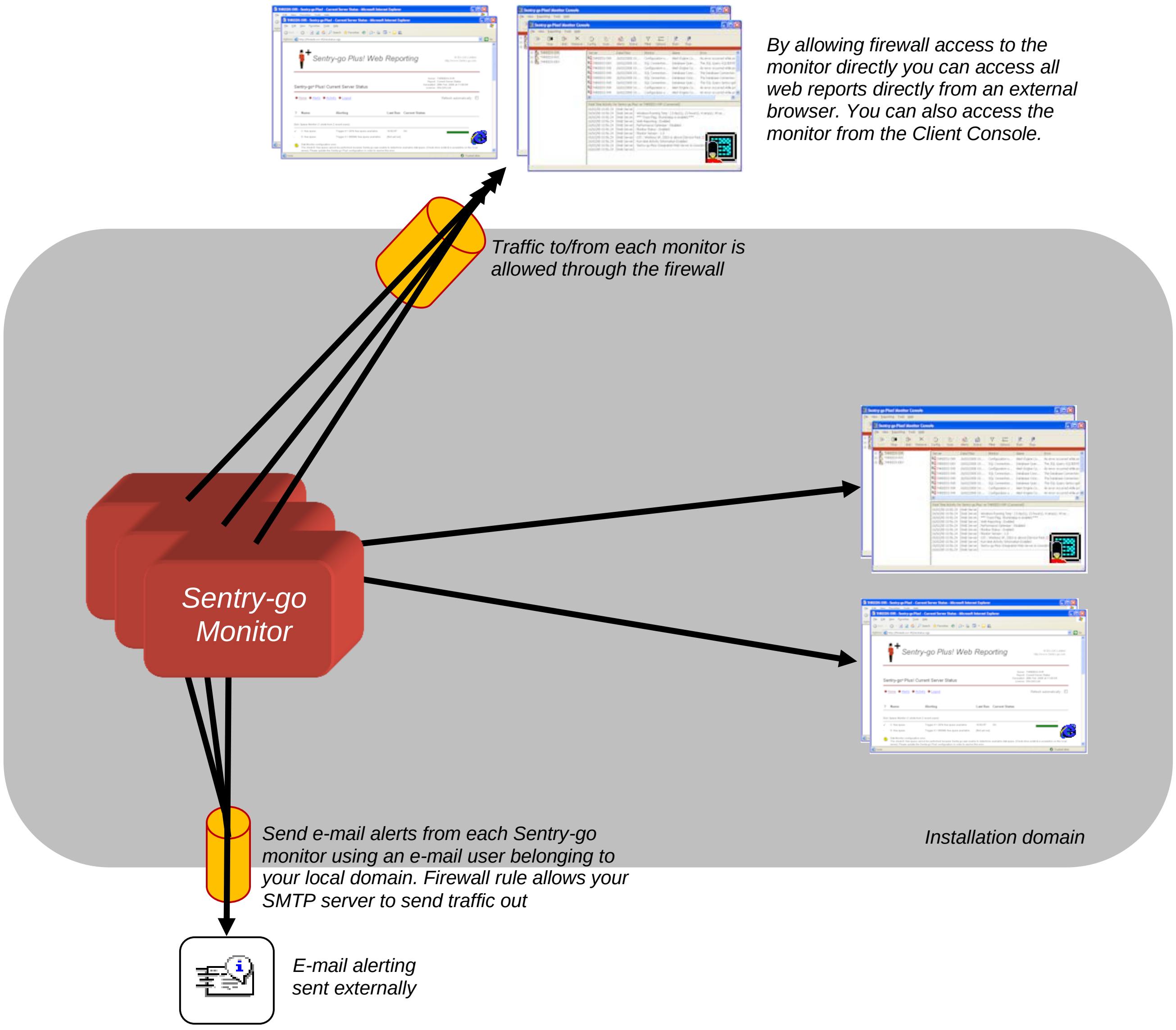
Pros & Cons

This option allows combined reports from the entire monitored environment to be accessed from a desktop browser easily through your existing web server.

It requires the “Enterprise Option” component and a SQL Server database. More detailed information & configuration settings etc. are still only available internally and reports can only be accessed individually for each server/monitor.

Multiple machines with full access

This is arguably the most flexible & comprehensive option. With it, you have complete control over each Sentry-go monitor and its web reports, either internally or externally.



By allowing firewall access to the monitor directly you can access all web reports directly from an external browser. You can also access the monitor from the Client Console.

Traffic to/from each monitor is allowed through the firewall

Send e-mail alerts from each Sentry-go monitor using an e-mail user belonging to your local domain. Firewall rule allows your SMTP server to send traffic out

Installation domain

E-mail alerting sent externally

Configuration

This setup gives you full internal & external access to each Sentry-go monitor. To enable it, the firewall must be configured to allow traffic in/out for each monitor (which company procedures may or may not allow). Access can still be made locally and alerts are triggered as before, through your SMTP server.

Firewall Changes

Add rules to allow the monitor to receive and send TCP/IP traffic externally. See later for more information.

Pros & Cons

This option is the most flexible as it allows full access internally or externally. Real-time alerts & configuration settings are also accessible internally or externally from all monitors.

However, this brings with it additional security issues which need careful consideration – e.g. setting a password for web access/configuration settings, limit access to specific IP-addresses etc.

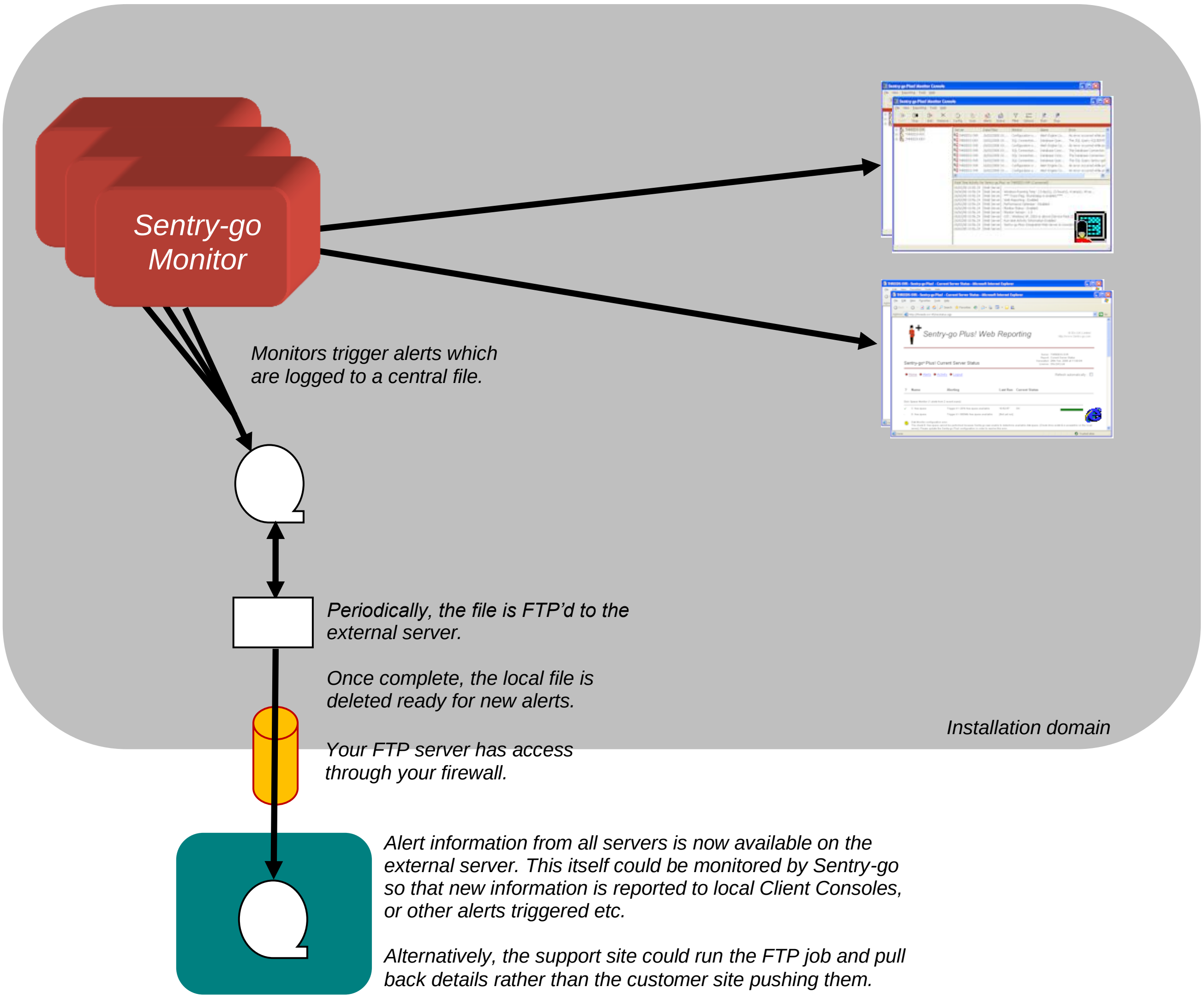
Security-wise, this option requires careful planning – e.g. to set a password for web access/configuration settings, limit access to specific IP-addresses etc.

See “Firewall Rules” later for more information.

Multiple machines, with central logging & periodic (semi real-time) alerting

This option uses the monitor’s ability to log triggered alerts to a file and is useful when companies do not wish to configure firewalls as described above.

We have a number of Sentry-go monitors, each recording alerts to a central network file. Access from client tools remains internal, but a scheduled job periodically sends (FTPs) the alerts to a central source, accessible by support technicians or the helpdesk. This could be an external server – e.g. at a 3rd party outsourcing company etc., and could be used in conjunction with other alerting options.



Monitors trigger alerts which are logged to a central file.

Periodically, the file is FTP’d to the external server.

Once complete, the local file is deleted ready for new alerts.

Your FTP server has access through your firewall.

Alert information from all servers is now available on the external server. This itself could be monitored by Sentry-go so that new information is reported to local Client Consoles, or other alerts triggered etc.

Alternatively, the support site could run the FTP job and pull back details rather than the customer site pushing them.

Configuration

This setup gives you semi real-time alerting through the logged file information which itself could be monitored by Sentry-go running on the 3rd party server.

Firewall Changes

None.

Pros & Cons

Although this option is a compromise over the previous one, it allows semi real-time alert information to be accessed without the need to change or compromise any firewall settings. Alert details are FTP’d to the remote server/3rd party and so only FTP access needs to be configured from a single server.

3rd Party Remote Support

If you provide 3rd party support to your customers, you may be wondering how Sentry-go can fit in to and help your organisation monitor your customers sites/servers ? If you've already considered the above sections, you'll know the short answer is *"in a number of ways".*

To discuss these options further, we've extended some of the examples below to show how a 3rd party support scenario could work.

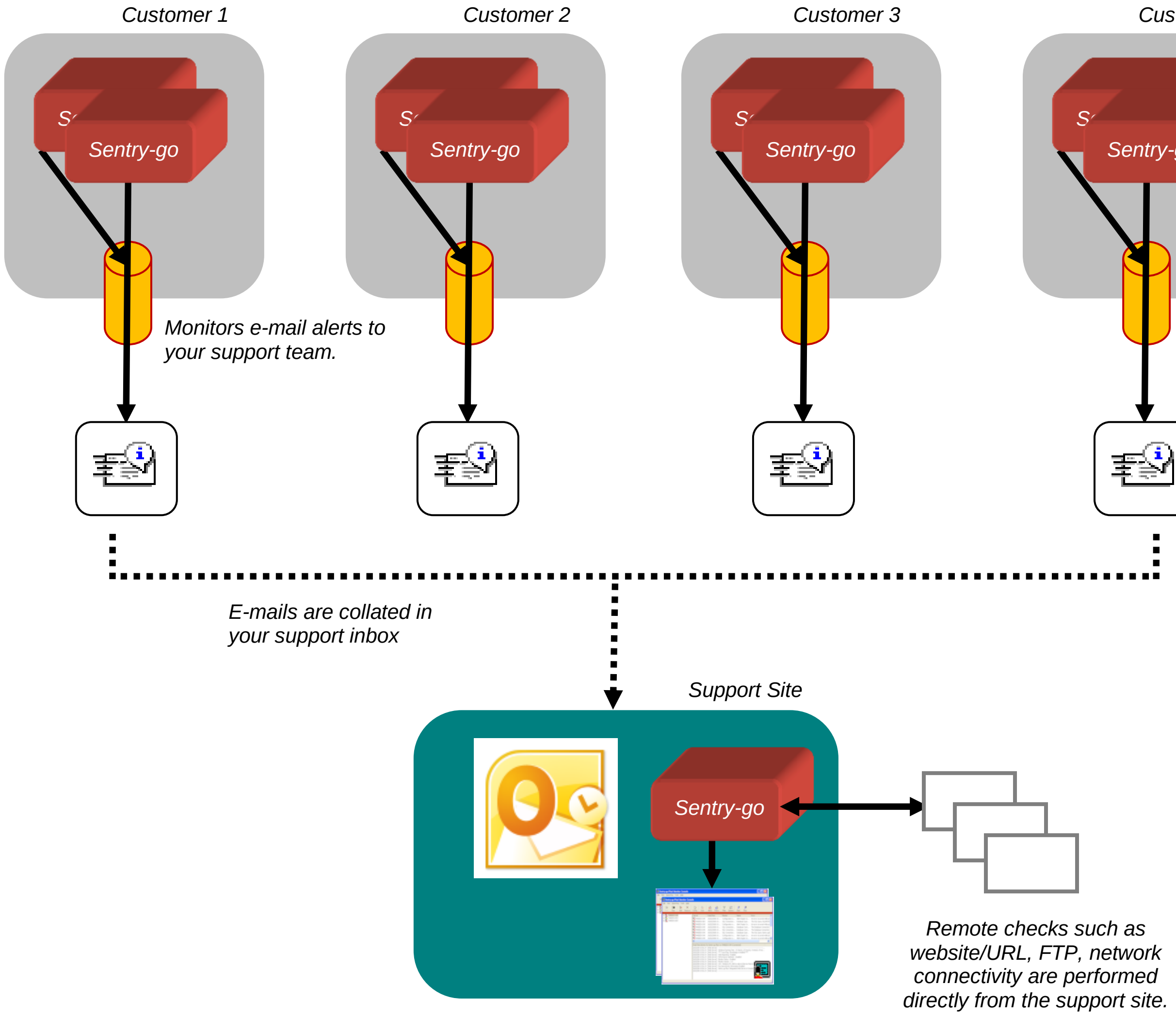
Remote vs Local Monitoring

Sentry-go server monitoring is, where possible, carried out locally. This minimises network overhead, removes any single point of failure and puts the monitor in a much better position to perform automatic responses where they're possible.

However, some monitoring tasks are, by their nature, network-based – for example, web page access, FTP, network connectivity etc. As these are to be remotely verified, the easiest way to monitor this type of task for a support company is to run a single Sentry-go monitor directly from their own site (& shown in the diagrams below). This will automatically feed into the local Client Console (on their site) or trigger alerts in your preferred way.

Remote support using e-mail alerting

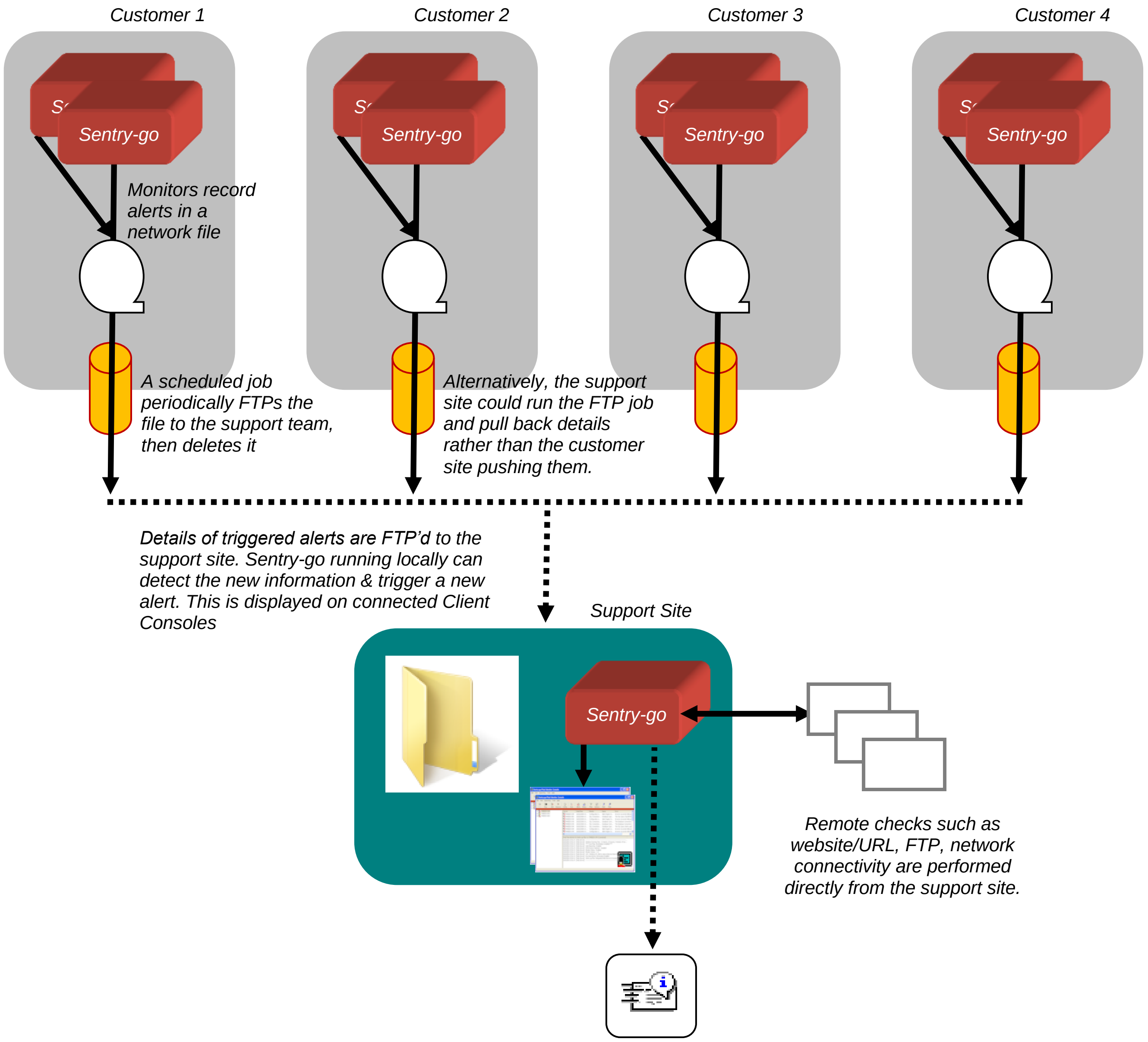
In this scenario, customer sites are configured to e-mail any alerts and optionally summary e-mails. E-mails are sent using the customer's SMTP server and sent to a dedicated support e-mail. Allowing for network issues, alerts are sent in near real-time and collated in the support mailbox from where they can be accessed and coordinated as required. Effectively the mailbox acts as the Sentry-go Client Console with alerts typically arriving in chronological order.


Customer 1
Customer 2
Customer 3
Customer 4
Sentry-go
Sentry-go
Sentry-go
Sentry-go
Monitors e-mail alerts to your support team.
E-mails are collated in your support inbox
Support Site
Sentry-go
Remote checks such as website/URL, FTP, network connectivity are performed directly from the support site.

Remote support using FTP-based alerting

With FTP alerting, the monitors at each customer site are configured to record their alerts locally to a network file. Periodically a server at each site forwards alerts to the support team using FTP.

With Sentry-go also running at the support site, any changes brought in through FTP are detected automatically and highlighted as alerts on connected Client Consoles. They can also be forwarded as new alerts using other methods, such as e-mail.



Monitors record alerts in a network file

A scheduled job periodically FTPs the file to the support team, then deletes it

Alternatively, the support site could run the FTP job and pull back details rather than the customer site pushing them.

Details of triggered alerts are FTP'd to the support site. Sentry-go running locally can detect the new information & trigger a new alert. This is displayed on connected Client Consoles

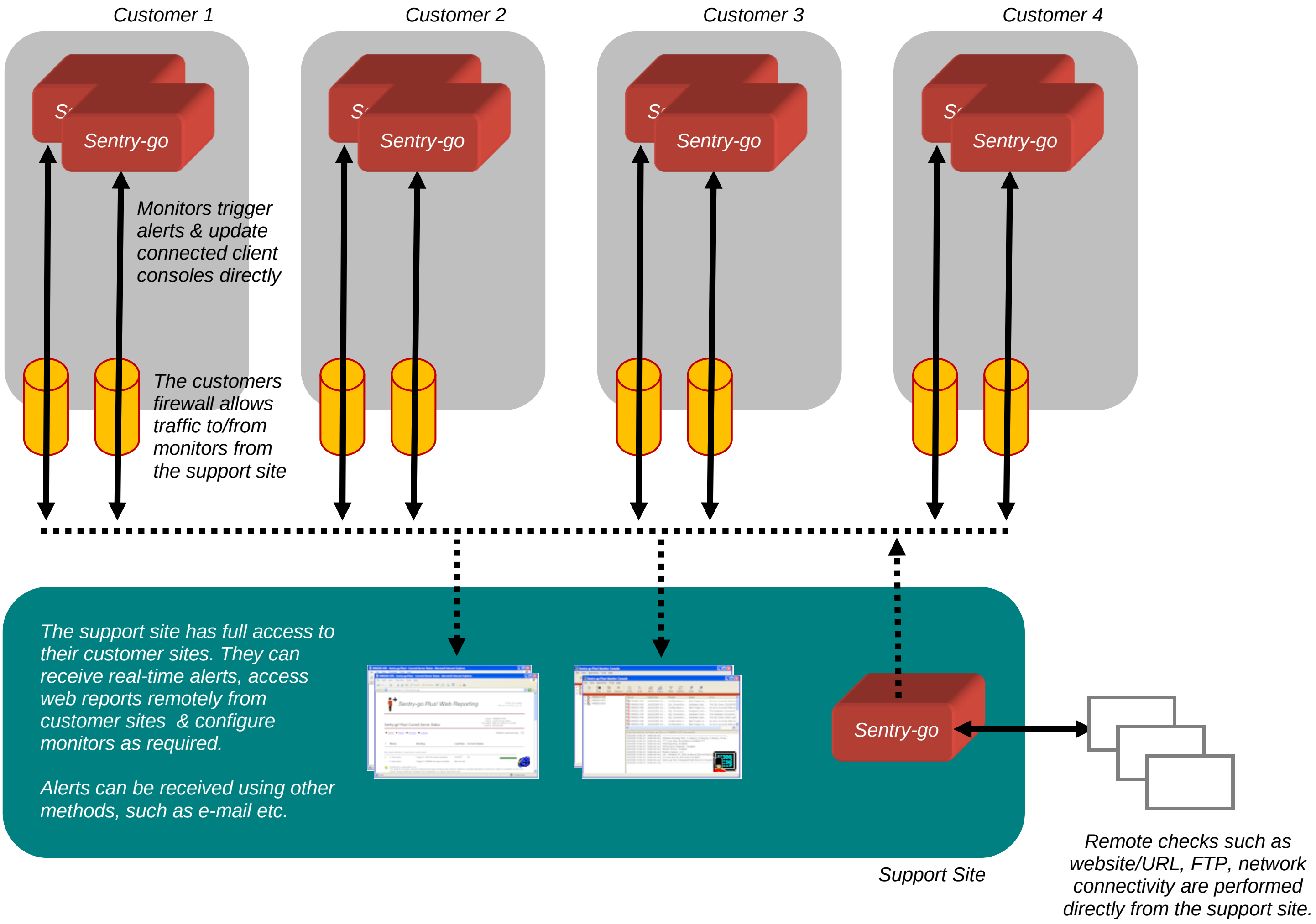
Remote checks such as website/URL, FTP, network connectivity are performed directly from the support site.

Forwarded alerts can also be triggered, using your preferred alerting methods.

Remote support with full access

If available, this is the most flexible solution, though it does require the most planning and agreement with customers. With it, firewalls at customer sites are configured to allow direct access to Sentry-go monitors from the support site. Assuming good network conditions, real-time alerts as well as web reporting can now be achieved directly from support site desktops.

Customers are now accessed in exactly the same way as a local Sentry-go monitor, through client tools and/or web browsers.



Monitors trigger alerts & update connected client consoles directly

The customers firewall allows traffic to/from monitors from the support site

The support site has full access to their customer sites. They can receive real-time alerts, access web reports remotely from customer sites & configure monitors as required.

Alerts can be received using other methods, such as e-mail etc.

Remote checks such as website/URL, FTP, network connectivity are performed directly from the support site.

Firewall Rules

A number of Sentry-go monitoring components, client tools and the web server communicate using TCP/IP. Therefore you need to ensure TCP/IP traffic is allowed through your firewall when …

- They need to communicate
- You wish to access them using TCP/IP.

Although firewalls can differ from site to site, the follow applies ...

- To check which port a Sentry-go monitor is listening for inbound client & web requests, configure the monitor locally, select the "Settings" tab and check the port number value. *By default, the Setup Wizard will configure port 1000.*

- To receive real-time notifications, you may need to allow firewall access to your client PC. The Sentry-go Client Console uses TCP/IP port 100 and above (e.g. 100-105) to receive notifications.

- To allow the monitoring service to stopped/started from within client tools, you would need to allow firewall access to the system’s SCM (which controls Windows services). Although you could do this, it is not recommended. Instead, we recommend that you stop/start the monitoring service locally, or using a Remote Desktop/Terminal Services connection.

More information, help & support

More information on the Sentry-go monitoring software range is available online at http://www.Sentry-go.com. Alternatively …

- For sales advice, please e-mail Sales@Sentry-go.com.
- For technical support, please e-mail Support@Sentry-go.com.