HOW CENTRALISED UNIFIED THREAT MANAGEMENT (UTM) CAN HELP COMPANIES CONTROL SECURITY AT REMOTE OFFICES, SIMPLIFY ADMINISTRATION AND CUT COSTS

Submitted by: Annabelle Brown

Thursday, 5 June 2008

WICK HILL/WATCHGUARD WHITE PAPER

5th June 2008

BULLET POINT SUMMARY OF WHITE PAPER

• In today's distributed computing environment, it is becoming increasingly important to control security at remote locations from the centre.

• Companies such as WatchGuard are now providing unified threat management (UTM) solutions with strong centralised control.

• The problems when centralised control is not strong include -

- difficulty implementing company security policies across the whole network

- no clear visibility of what is happening across the network

- branches failing to carry out all security updates and procedures

- difficulty in providing audit logs

- lack of availability of skilled staff at remote sites

- higher costs to support remote sites.

• Looks at the centralised management features provided by WatchGuard in its UTM solutions, which give tight, centralised control of security across the network.

• Features include drag and drop VPN tunnel creation; and an easy to use real time monitoring system with clear, intuitive graphical interface

• Two typical scenarios of how a unified threat management system with centralised control makes controlling remote security easier and more cost-effective.

INTRODUCTION

In today's modern, distributed computing network, where companies and organisations need to secure IT not just for the head office, but for remote locations as well, the ability to control security for multiple sites from one single location is becoming increasingly important.

With some security systems, the tasks of configuration, updating, rebooting, etc. for remote sites might all have to be done separately and repeated for each location. Administrators could be faced with managing remote security appliances individually, possibly having to send someone out to a remote site to carry out certain tasks, such as configuration or establishing VPN tunnels. This can be difficult, time consuming, costly and complex and, in some cases, it is practically or financially impossible

It can be further complicated if there are multiple appliances, delivering multiple levels of security, such as firewall, VPN, spam blocking, gateway anti-virus, web content management and intrusion detection/prevention.

However vendors, such as WatchGuard Technologies, have now responded to the need for strong centralised control with their range of Firebox UTM (unified threat management) security appliances, which make controlling security for multiple sites quick, easy and cost-effective.

THE NEED FOR STRONG CENTRALISED MANAGEMENT

Many problems arise when strong centralised management is not available for extended networks with multi-site locations. Critically, the lack of good centralised management takes control away from the administrator, making it more difficult to implement and report on company security policies throughout an organisation, and increasing the likelihood of security lapses.

Administrators have no clear visibility of what is happening across the network and if problems do occur, it’s harder to resolve them quickly and effectively throughout the company. Additionally, without proper centralised management, it is more likely that branches will fail to carry out all necessary updates and security procedures. And, of course, the lack of centralised reporting means that organisations are unable to provide audit logs confirming that they have met their security and staff protection responsibilities.

The availability of skilled staff at remote sites is another issue. There simply may not be enough of them to do all the necessary updates, configuration, etc. Or the level of understanding of security issues may not be high enough to maintain the required level of security. It will also be harder for administrators to manage security services such as anti-virus, spam blocking, web blocking and intrusion prevention.

Some specific functions, such as setting up VPN tunnels between locations, can be very complex and prone to error, as well as time-consuming and costly if tackled without central control. A centralised management system, such as one which can set up VPNs from a central location and can do it in a simple way, such as by using ‘drag and drop’ techniques, can save an enormous amount of time, effort and money.

Cost is an important issue. Having to deal separately with each remote site, and possibly having to visit sites, is time consuming and consequently expensive. The lack of control can lead to errors at remote sites, or security lapses which can be costly. Or, it may be felt necessary to employ skilled staff to suitably manage remote site security, again another cost to an organisation.

The key benefit of a centralised management system is control for the network administrator and the more remote sites a company has, the greater the potential benefit. A good centralised management system empowers the network or security administrator to flexibly mange the whole network in real time. It saves a huge amount of time, effort and cost. And it allows corporate policies to be easily deployed across the network.

CENTRALISED MANAGEMENT FROM WATCHGUARD

Security vendor WatchGuard, one of the world's leading providers of unified threat management appliances (UTMs), has focused strongly on providing administrators with centralised management systems that bring maximum control of security across the network, while being flexible, cost-effective and easy to use.

Centralised management within the WatchGuard System Manager (WSM) feature, found on all WatchGuard Firebox X UTM appliances, provides administrators of simple or complex network environments with a powerful, intuitive interface to centrally manage multiple Firebox X UTM appliances, including firewall, VPN, various security applications, and appliance software updates.

WatchGuard System Manager allows administrators to -

- view all security appliances at a glance and launch monitoring or configuration tools for pinpoint control of any device or UTM service.

- immediately see and understand what's happening on the network and take instant pre-emptive and corrective action with interactive real time monitoring.

- send simultaneous global firmware and configuration updates to multiple Firebox X appliances with one management action, either immediately or as an automatic scheduled task.

- make configuration changes immediately or work offline for convenience.

- create secure site-to-site VPN tunnels with just three steps, saving time and frustration.

- manage security services such as gateway anti-virus/intrusion prevention, spamblocker or web blocker with no separate management software to purchase or maintain.

- easily tailor systems to business needs by using flexible objects, simplified service configurations and customisable reports

- use drag and drop management to lessen the time and effort needed to create centrally managed security configurations and branch office VPN tunnels between WatchGuard appliances.

- view, edit, and create security policies and tunnels across the enterprise from a single management console.

- make use of secure, centralised logging and comprehensive reporting on remote devices, with no extra logging or reporting modules to buy.

SPECIAL FEATURES

An easy to use real time monitoring system with clear, intuitive graphical interface

Users of WatchGuard’s centralised management system often comment on the value of the real time nature of the management function and its ease of use, which allow them to get going straight away and perform the kind of routine tasks that every administrator has to perform - only faster and more efficiently. They also appreciate the overall visibility gained into the network, thanks to the intuitive graphical interface.

WSM has a suite of utilities which collectively provide ‘interactive real time monitoring’. These are graphical tools which show what is going on in the system in real time. This brings the whole network alive in front of the administrator, making it very easy to see exactly what is happening in terms of network events or security events, and to understand just what users are doing.

WatchGuard calls these facilities interactive because many of them allow administrators to act on the data that’s being shown right in front of them. For example, in ‘host watch’ or ‘traffic monitor’, administrators can right click the IP address that’s shown and then do a diagnostic. They can try and ping that IP address, or actually stop the connection right there.

If they see a connection and decide there’s something wrong, they can stop it, cut it off, take a look at what’s going on and decide if it should be prevented permanently, with a rule change. Or, if it turns out to be OK, it can be allowed again.

The system gives a real immediacy to the connection between the administrator and the Firebox. The configuration tools are visually oriented and thoughtfully laid out, based on common tasks. Smart defaults provide strong security right from the start, saving valuable configuration time and effort, while advanced, granular controls empower the expert user.

Policy creation can be streamlined with optional time-savers such as wizards, aliases, and QoS objects. Configurations can be created offline and deployed when most convenient, or quick changes can be saved to the box immediately.

The interactive real time monitoring system provides clear, visually driven interfaces and plain-English log messages, making it easy to validate the security policy and to make changes or adjustments as desired. Interactive tools help administrators take instant preventive or diagnostic action directly from the monitoring interface, without the need to open separate configuration screens. Compared to some other systems, this can be a major benefit.

Ease of VPN tunnel creation

A key feature of the system is the ease, speed and accuracy with which branch office VPN tunnels can be created using drag-and-drop techniques. A branch office tunnel is initiated by dragging one branch office VPN device to another - a fast, easy and virtually foolproof method. Creating those tunnels, without a feature like this, would normally be very detailed and demanding, taking considerable time and being sensitive to all kinds of errors. The WatchGuard system gives flexible, granular control of the centrally managed tunnels.

The VPN facility is also extremely helpful when working with dynamic IP devices. It very easily accommodates locations with dynamic IP addresses. When you tell WSM that a device is dynamic, then it will always know the IP address of that device, without the administrator having to get on the phone to check. Whenever the IP address changes, the device contacts the server to report the new address.

Offline configuration

Within the Policy Manager function, on Firebox Core and Firebox Peak devices, is an offline configuration tool which is unique. When the administrator is creating a policy for a device, it can be created offline, acting on a file instead of acting directly on the Firebox. This allows administrators to make policies just as immediately as with a web based interface, which is what most competitive products use. However, with WatchGuard the offline configuration tool allows administrators to do a variety of useful things.

They can save local copies of the file, which provides back-up security and peace of mind. And they can use one configuration file as a template, which can be used to set up another Firebox in the same way. Or a few changes can be made for the second device. This method saves a great deal of time when it comes to setting up subsequent devices.

Another way this feature can be used is to make a configuration file, save it as a file and then save another copy. Minor tweaks can be made on the second copy, and both files can be tried as a quick and easy experimentation to find out which is most suitable. The first file is always available as a back-up. Or the two files can be swapped around. The first file also serves as a permanent back-up in case of disaster.

Logging and Reporting

Secure, centralised logging and comprehensive reporting are included in WatchGuard System Manager, bundled with all Firebox X Core and Peak models, with no extra logging or reporting modules to buy. XML-based, human-readable logging is easy to understand, allows integration with third party reporting tools, and is sent over a reliable, encrypted connection for security and continuity of log data. The full-featured reporting available on WSM facilitates the in-depth analysis of network activity, security threats, and user behaviour.

Comprehensiveness

WSM is an extremely comprehensive package. It comes bundled with every Firebox Core and Firebox Peak device. The only extra which companies need to buy is additional licensing when the number of remote

devices goes above four (except with Firebox 550E Core model).
With competing products, companies often must buy the centralised management software itself, as well as the extra remote device licenses. With many competitive products, there are also separate functional models to buy, such as reporting, unlike WatchGuard WSM which includes a complete set of reporting modules.

There are many different types of organisation where WatchGuard Firebox UTMs, with centralised management, can provide a high level of security across the whole network.

Following are two scenarios illustrating how the system might be used:

SCENARIO 1

Company
A major clothing retailer with a head office in London and 100 branches around the UK. Good, uninterrupted communications on a daily basis between head office and the branches is essential for sending stock, financial and administrative data.

Aims
To provide an ultra-reliable security system, which is always available. Any downtime can mean serious financial loss. If stock information is not passed to head office, for example, stock replenishment could be adversely affected, resulting in a fall in retail sales.
With such a large network of branch offices, managing security throughout the network could become extremely complex, time-consuming, prone to error and potentially very expensive.

The company needs a solution that is easy to use, easy to understand, fast and keeps costs down. With so many branches, it becomes more difficult to implement, report on and maintain corporate standards in every single branch. The company needs a system which provides an easy method of rolling out updates and changes throughout the organisation and provides for strong centralised control.

System used
In this scenario, a typical system would be Firebox X Peak at head office, with 100 Firebox X Edge wireless UTMs at branches. Centralised management is achieved by the use of WSM on the Firebox X Peak. All UTMs have deep packet inspection firewalls with a VPN, zero day protection, gateway anti-virus, intrusion prevention, anti-spyware, anti-spam and URL filtering available.

Benefits
- Huge savings are made in time, manpower and cost by building a master configuration template that is sent out, in one move, to all 100 branches.

- Any changes made to the master template are again instantaneously sent to all 100 branches through simply hitting one button, saving time and making a very large network manageable.

- The corporate security policy is easily applied throughout the company. The interactive monitoring system makes it easy for the administrator to check that the corporate policy continues to be upheld and to easily remedy any situations where divergence occurs.

- Establishing VPN tunnels with all the branches is accomplished very quickly and easily with WatchGuard's simple drag-and-drop procedure. Without this, the whole process of establishing VPN links could have taken weeks and been much more prone to error and potential problems. And, of course, making changes is similarly easy with the WatchGuard drag and drop process.

- Managing such a huge network is greatly simplified and aided by the intuitive graphical user interface which gives a clear overall view of the whole network and allows the administrator to take action centrally to deal with any problems at the branches. A high level of control is obtained.

- Costs are minimised by not having to deploy skilled staff at the remote sites.

- The company wanted to provide free Internet access via a wireless hot spot in the stores, as an incentive to shoppers. The 100 Firebox Edge wireless UTMs installed in the stores have a feature called 'wireless guest services', which is used to provide this facility. 'Guest services' ensures that hotspot access is completely and securely separated from the corporate network.

- Security services on the systems (gateway anti-virus, intrusion prevention, anti-spyware, anti-spam and URL filtering) are all managed centrally, including updates. This proves cost-effective, compared to some competitive products, as there is no separate management software needed for this.

- Cost savings are made on the reporting for the 100 remote branches, because the reporting modules are included in the system price.

SCENARIO 2

Company
An international finance company with one head office in the City of London, three offices in Europe and two in the Far East. As the company is in the financial sector, security is particularly important.

Aims
Being in the financial sector, a very high level of security is sought.
With branches abroad being geographically remote, using different languages and being in different time zones, it can be difficult for head office to ensure control and implement corporate policies throughout the network. A system which gives the company strong but flexible control from head office is needed.

System used
The City of London head office has a top of the range Firebox X Peak UTM and the branches have Firebox X Core UTMs. Features on both models include deep packet inspection firewalls with a VPN, zero day protection, gateway anti-virus, intrusion prevention, anti-spyware, anti-spam and URL filtering.

Benefits

- The ease of use and clarity of the graphical interface coupled with interactive real time monitoring make it very easy to carry out all network administration from the head office console. The company achieves a very high level of control.

- Tasks such as updates, firmware upgrades and configuration changes can be prepared offline and scheduled in to take place at the remote sites during an off-time maintenance window in each of the overseas offices.

- Implementing the same security policies throughout the network is simplified by using the offline configuration feature within Policy Manager. When the overseas offices are set up, a central configuration file is created, providing the essence of the security policy. This is used for all the branches, with only minimal extra work needed, such as adjustments for factors like as local IP addresses. The policy can be distributed to all the branches with one touch.

- The interactive real time monitoring proves very useful for troubleshooting. When someone in one of the remote locations reports any issues with the network, or when the administrator becomes a little concerned about one of the branches, it is very easy to use the monitoring tools to diagnose the problem and to correct it remotely.

- The comprehensive logging and reporting facility makes it easier to keep track of what is happening at the geographically distant remote locations.

ENDS

For reader queries, please contact: Wick Hill T: 01483 227600; W: www.wickhill.com. For further press information, please contact Annabelle Brown on 0191 252 8548, email abpublicrelations@btinternet.com