



Network security for the smaller business

Clavister White Paper

Network security best practice

- Implement an effective password policy and ensure that passwords are regularly changed
- Install and maintain firewalls and virus protection applications
- Ensure the physical security of your environment
- Create backups for important data
- Ensure software applications are regularly updated
- Limit access to sensitive and confidential data
- Be sure to remove all content from equipment that is being sold or scrapped
- Remove unused software and defunct user accounts
- Conduct frequent security self assessments
- Run regular education sessions so all staff are aware of policies
- Test business continuity and disaster recover planning

Overview

Recent estimates reveal that small to mid-sized businesses (SMB) employ 300 million people world-wide. In developed countries they account for approximately 95 to 99 per cent of all enterprises, employ 66 per cent of the workforce and generate 55 per cent of national turnover.

SMBs face many challenges which are made worse by recession but one which they experience in both good times and bad is the need to secure their IT. It's a big problem because industry reports show that while 75 per cent of SMBs place great importance on IT security; more than half are struggling to implement adequate security measures.

Implementing effective IT and network security is a challenge for all businesses because large or small, they all rely on business critical applications for their day to day survival. However, while larger enterprises have greater financial resources which enable them to employ their own skilled staff or outside consultants, these options are not generally available to the SMB.

Many smaller businesses lack budget for security as well as dedicated, skilled IT staff and this prohibits the implementation of an effective security policy.

To identify threats and effectively combat them, SMBs need to adopt a logical approach that first assesses the risks then audits current infrastructures before going on to put in place best practices supported by appropriate security solutions.

Threats

The increasingly networked environment in which SMBs operate creates tremendous opportunities but it also introduces great risks. The biggest challenge of all for SMBs is the complexity of security and the speed of change which makes it very difficult for an SMB security or IT administrator to keep up.

The Internet is an important part of our lives and accessibility to the worldwide web is crucial for many SMBs who rely on its swift interchange of data. However, just as reliance on that swift network traffic increases, so do the threats that it can bring.

The Internet presents many security pitfalls for any business small or large, and if industry pundits are to be believed, the dangers will continue to increase. Data can be corrupted by viruses or exploited by cyber criminals. Malicious Distributed Denial of Service (DDoS) attacks can be launched when intruders attempt to hijack access to network services. Threats such as *Viruses, Worms,*

Trojans, Sniffers, Spam and *Phishing* are now well-known computing terminology and spam is one of the most common threats to the network. In fact, a leading search engine provider has identified more than three million unique URLs on more than 180,000 websites that automatically install malware on visitors' machines. Spam is often used to drive traffic to these sites where the malware is installed for later use.

Evolving communication needs also leave SMBs vulnerable to security attacks. Remote working and home working are becoming more commonplace, with employees using remote laptops or handheld devices to access company networks. To reduce overheads such as telephone costs, the SMB may look at Skype or other software which results in increased use of the Internet and increased vulnerability.

A before and after look at UTM shows how multi-function devices can help reduce the total number of boxes and therefore the cost of hardware and administration.

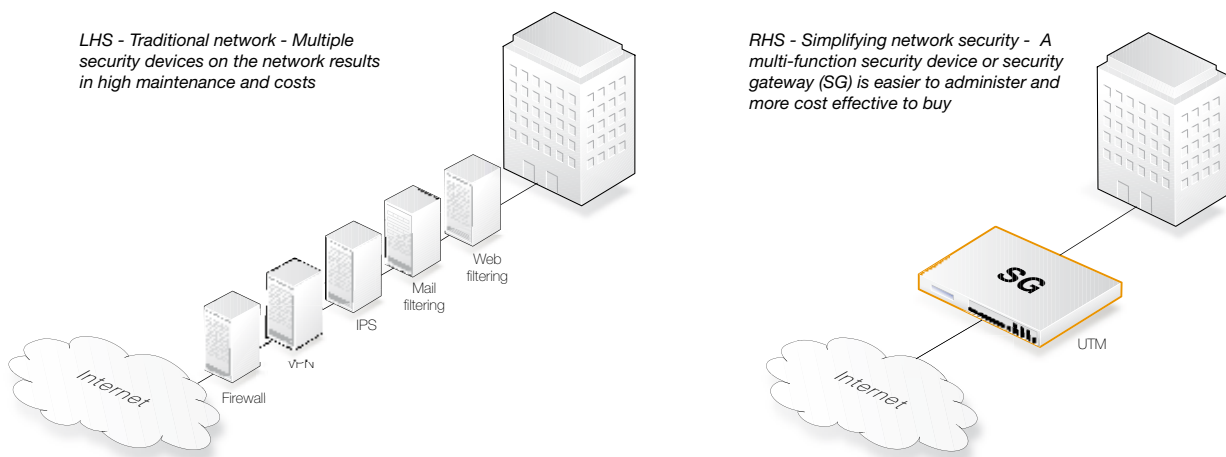


Figure 1: A before and after look at how unified threat management (UTM) can lower the cost of network security

The bottom line is that network attacks cost SMBs money. If a Trojan Horse or a virus is introduced to your network then the result can be catastrophic with complete data loss a real possibility. Computers will lose performance and the business can grind to a halt and while SMB owners may feel that they are too small to be a target for hackers, this is not the case – everyone is a target. SMBs can become part of larger attacks and as larger organizations have more sophisticated security solutions, SMBs can be seen as more vulnerable targets. There is also the possibility that security breaches may come from within their organization.

Fortunately, as cyber threats have evolved, so have the methods of defense. Increasingly sophisticated firewalls offer effective protection and anti-spam products can filter out up to 99% of unsolicited mail. But as quickly as solutions to known threats are found, the threats change and security challenges change with them.

The growth of new community driven technologies introduces new security challenges. Previously, it was 'straightforward' to keep on top of security because it was quite segmented. If SMBs needed to filter incoming data, they purchased a firewall; if they needed to scan for viruses they purchased anti-virus software but today the situation is much more complex due to more and more business applications being used online or via the company network. They have to cope with intrusion detection, manage encryption policies and cater for remote and roaming users, peer-to-peer networking and instant messaging. There are now so many technologies working hand-in-hand that they start to interact with each other and in a small company, it is just too much for one single administrator to manage, particularly since most IT people in SMBs tend to be generalists rather than security specialists.

So how should the SMB set about implementing effective security?

Risk assessment

Assessing risk is the first step towards improving network security for the SMB. Whether it is related specifically to network security and the Internet or to any other aspect of the business, an effective risk assessment must document potential threats, establish your vulnerability to those threats then evaluate the cost or damage that they could cause. This must then be compared with the cost of implementing protection. Is the investment worth it?

The SMB IT administrator should ask these questions:

- What systems or resources do I need to protect?
- What is the commercial or business value of those resources?
- What are the possible threats that those resources face?
- What is the likelihood of those threats being realized?
- What would be the impact of those threats on my business?

It is then time to investigate technical or procedural remedies that could counteract the risks and compare the cost of each solution against the potential damage the threat could cause. If the cost of the solution is higher than the financial impact of the risk then you must either look for another solution or make the decision to live with part or all of the risk.

If you do not have the resources to address everything at once, what will your priorities be? For the SMB there must be a compromise on what security policies and solutions to put into place.

What SMBs need to do is to recognize that security does not stand still and today's solution may not meet tomorrow's threats. They need to establish the specific risks that the company faces and develop an IT security strategy that meets this unique risk profile.

Today's content-based threats which bypass conventional firewalls, spread faster and do more damage.

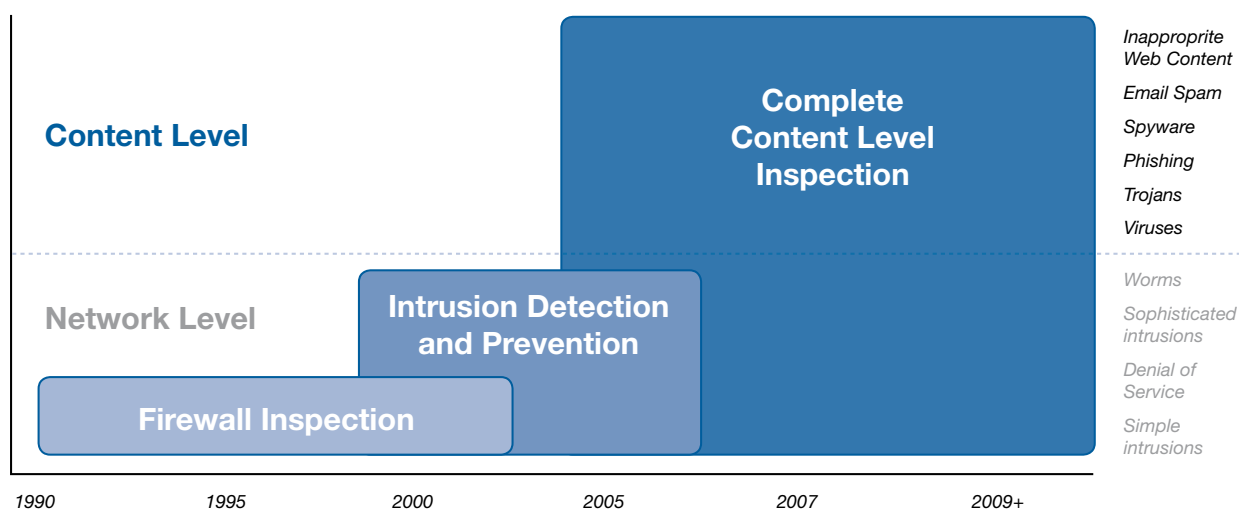


Figure 2: Content-based threats that get through conventional firewalls do more damage, faster

Network security audit

Having assessed the risks and before deciding on suitable security solutions it is sensible and indeed vital for SMBs to carry out a full audit which must cover not only the equipment and devices in use but must also document the existing network security solution and the people and policies that are in place. If you don't know what you've got, how can you protect it?

Yet again, conducting an audit of this kind can be adversely affected by a lack of budget and most SMBs just cannot afford to hire external consultants to do the work. Once more, it is sensible to tailor the work to the budget and prioritize.

In preparation, the auditor must list all the relevant equipment, processes and people and ensure that there are no critical omissions. All the devices must be logged and applications scrutinized to establish version numbers, patch and fix status and which functions have been disabled. It is also useful to look back and learn from any security problems that may have been experienced in the past.

The number of checks that make up a full audit are extensive but mostly they are just common sense! With the network it is logical to start at the edge and work to the core. Are firewalls in place and how is traffic filtered? Are those firewalls and the equipment that supports them regularly upgraded? What are your access controls and are they adequate? How secure are your passwords and if you have Virtual Private Networks (VPN), how are they assigned and secured? How many switches, hubs and routers are there and are the ratios correct? Are new users registered and are any insecure computers denied access?

Wireless networks are particularly vulnerable to security breaches and it is important to audit the security protocols that are in place such as 802.11i or the more powerful 802.11n. Check how access points are managed and secured and look into the security arrangements for Virtual Local Area Networks (VLANs). Is network traffic encrypted, how are users authenticated and is there an internal firewall for wireless users?

There are also many audit checks for desktop computers. Among these, it is important to establish the situation surrounding such things as passwords, personal firewalls, log-in rules and file encryption. The auditor must also check that patches are up-to-date and investigate the existence of external storage devices and back-up policies.

Away from the technicalities of the audit, it is also important to ensure the physical security of computer and networking equipment.

Best practices for network security

Best practices are things you do – steps you take – actions and plans to ensure network security. There are many best practice guidelines that SMBs can use and just two are ISO17799 from the International Standards Organization and CoBIT (Control Objectives for Information and Related Technology).

However, some of these models are designed for larger organizations and may be too complex for the average SMB, so it is important to just remember that good network security always starts with a living security policy. This should be an outline of security practices that every executive in the organization agrees to live by. It should include guidelines for everything from user access and passwords to business continuity and disaster recovery planning.

Some basic rules to follow are:

- Implement an effective password policy and ensure that passwords are regularly changed.
- Install and maintain firewalls and virus protection applications.
- Ensure the physical security of your environment.
- Create backups for important data.
- Ensure software applications are regularly updated.
- Limit access to sensitive and confidential data.
- Be sure to remove all content from equipment that is being sold or scrapped.
- Remove unused software and defunct user accounts.
- Conduct frequent security self assessments.
- Run regular education sessions so all staff are aware of policies.
- Test business continuity and disaster recover planning.

Security solutions for the SMB

IT security specialist Clavister delivers sustained commercial advantage to organizations around the world by protecting them from the business disruption and financial loss that network security breaches can cause.

Based in Sweden, the Clavister team has brought fresh thinking to the security arena by developing a holistic and flexible security service that can be scaled to meet constantly changing business needs and its chief technical officer, John Vestberg, has some useful advice for SMBs.

"SMBs definitely need to put up a firewall and they then need to start managing Virtual Private Network (VPN) connections from people working from home or on the move," he says. "They need to understand the basic principles behind VPN – not necessarily to be experts in encryption but to at least understand why they need to authenticate users and how communication can be secured. They must understand protocols and support issues not only for introducing roaming users but also for maintaining them.

"Anti-virus software is easy to implement and understand. Even a novice can understand it because it is more tangible than many other technologies. However, anti-virus is useless if it is not updated regularly as the threats are continuously evolving. They have to have the mindset that it is not just a one-shot installation."

The use of the network has expanded and so opens up traffic into the company. This in turn opens up an intrusion threat that must be countered by introducing the right security including intrusion protection and intrusion prevention measures.

"Intrusion prevention is not as straightforward to understand and implement as say, anti-virus. It is very specialized," adds Vestberg. "You don't just need to understand the basic principles; you also need to have expertise in networking to be able to tune your system so that the security is working. This is something that a general IT administrator just would not learn overnight. It takes a specialist security person who understands networking, security and network tuning.

"The obvious risk is that you may deploy an Intrusion Detection Solution (IDS) then find that you can't manage it. Either it gives you too many false positives or you strip it down to a level where it doesn't give you any headaches but then it doesn't give you any actual intrusion protection either."

Many IDSs, if improperly configured, will register attacks as legitimate even if those attacks have no bearing on the network. These false positives can quickly swamp the network with constant alerts, eliminating the value of the intrusion prevention tool.

It is important for small businesses to protect their investment in security and it should be seen as an ongoing maintenance cost, not just a one off investment. SMBs may take the short approach and invest in a product then leave it until something goes wrong, by which time the damage can be done.

"At Clavister, we see security as intrinsic to the well being of a company network and no matter the size of the company; the needs for security are basically the same. It might be on different scales but the principles are the same," says Vestberg.

"No matter whether it's for an SMB, an enterprise or a managed security provider, we bring more than a box. If you purchase a security product from some companies, you get a box, you get documentation for that box and that's it. Since we realize that SMBs need more help, we try to see security as a flexible ecosystem. They need proper devices in their networks. They need proper management to enhance the service and to simplify the job of the IT administrator.

"We can provide tools to manage security in the best way, but we cannot empower with the knowledge. However, we can lower the knowledge threshold needed by offering the management systems and centralized management tools that allow him or her to be more productive with the few hours

that are spent administering security. Also we aim to offer the many elements that are needed to manage security without having to go to five different vendors. Clavister solutions mean that the SMB has a lot less to understand and cope with.

"We appreciate that the customer does not have the time to manage a lot of different types of software. We offer a streamlined and simplified management solution with one piece of software that does everything for you. Our management system is really straightforward and intuitive and you don't have to spend a lot of time supporting, upgrading and updating security patches and operating system patches. All of that is history and you can just focus on managing your security, not managing the security product. It also helps you bring total cost of ownership (TCO) down.

"Scalability is also important. As a company grows, so must its security. Clavister's solutions allow users to upgrade by changing software licenses giving them the same functionality but with more capacity."

Clavister's security gateways (SG) are able to cater for businesses of all shapes and sizes – the SG50 is a security solution for companies of up to 50 employees while the SG3200 series of rack mountable products are a good entry level solution for a medium-sized SMB. However, choosing the right solution depends more on the amount of data running over the network than on headcount.

All Clavister products offer Intrusion Detection and Prevention (IDP), bandwidth management, office-to-office VPN, user authentication, deep inspection, content filtering and anti-virus gateway. With the SG10 and SG50 series, the emphasis is on a lower basic cost of ownership with additional options. With the SG3200 series, you can set security policies and filtering for every single user and benefit from extreme scalability ranging from 350 to 1,000 Mbps plaintext and 100 to 250 Mbps VPN throughput.

Conclusion

While the path to success may be daunting, achieving network security is possible and affordable for SMBs. It is also vitally important because just as their use of technology increases, so do the threats and the rate of change is very quick.

To keep pace with this change, it is important for SMBs to look upon security as an ongoing process based on good practices, good advice and the implementation of comprehensive, scalable security solutions.

About Clavister

Since 1997, Clavister has been delivering leading network security solutions, providing commercial advantage to tens of thousands of businesses worldwide. The Clavister family of unified threat management (UTM) appliances and remote access solutions provide innovative and flexible network security with world-class management and control.

Clavister has pioneered virtual network security, and this along with its portfolio of hardware and software appliances gives customers the ultimate choice. Clavister products are backed by Clavister's award-winning support, maintenance and education program.

Headquartered in Sweden, Clavister's solutions are sold through International sales offices, distributors, and resellers throughout EMEA and Asia.

To learn more, visit www.clavister.com.

Contact Information

General Information
info@clavister.com

Sales Information
sales@clavister.com

Technical Support
support@clavister.com

Ordering Information
order@clavister.com

Partner Information
partner@clavister.com

CLAVISTER®

WE ARE NETWORK SECURITY

Clavister AB, Sjöгатan 6 J, SE-891 60 Örnsköldsvik, Sweden

Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com | Email: info@clavister.com