



Enterprise wide Security on the Internet

By

Shad Mortazavi

Nexus Global Technical Manager

Nexus Management Inc

Enterprise wide security on the Internet

1

Published in: <http://newsviews.info/techbytes03.html>

NOTE: The information contained in this document is the property of Nexus Management and is disclosed to you on the condition that you maintain the information strictly confidential. You are hereby warned that the information disclosed is subject to change without notice or the assumption of any liability on the part of Nexus Management.



Enterprise wide security on the Internet

To fully appreciate the challenges of enterprise wide security and to apply an appropriate security model, it is important to understand that enterprise networks have been evolving.

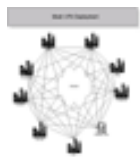
The classic enterprise network (Diagram 1) for most organizations was a hub and spoke arrangement. Global central offices would typically be linked together over leased line connections of some description. These would usually act as your hubs and off these would lie the regional spokes.

Due to the expense of leased lines very few global organizations could afford to deploy fully meshed global networks.

Remote users would access a local node using Remote Access to their local spoke office, or the organization would subscribe to their leased line service provider to provide them with routing back to their private network from a local point of presence.

Home workers were also limited to the same technologies as the remote user.

As applications, operating systems and general data requirements became more sophisticated, the model no longer provided an efficient way for enterprises to operate. The demand for higher bandwidth led to the decrease in the cost of leased lines and the emergence of new technologies, namely Virtual Private Networks (VPN). Remote users demanded and were given a myriad of high speed Internet access.



In the new enterprise model offices can communicate with each other securely over the Internet. It is now possible to mesh offices together removing the need for the hub and spoke. High speed Internet access allows users to work effectively from home utilizing VPN clients to securely connect over the Internet to any portion of the enterprise network.

Wireless networks are again reshaping the way we define an enterprise network. Allowing users to be mobile and to work from a varied number of locations globally.

In the not too distant future enterprise networks themselves may be a virtual concept; where all users are remote, working from any location globally, and the enterprise network is hosted at a co-location establishment at some ISP.

From a security standpoint, in the classic model, it would be fairly easy to control the external flow of traffic in and out of the hub offices, and the spoke offices would come back to the hub offices, to access the Internet. Careful IT managers would take time to deploy measures between hub and spoke offices, to ensure that if one site had been compromised it could easily be isolated and would not compromise the rest of the offices in the enterprise network.

However, the fully meshed network where every office has access to the Internet and all the other offices over the VPN, and remote workers accessing the offices over the Internet, poses an intriguing security challenge.

In all areas of enterprise system/network administration, a reactive approach does not lead to good I.T and a proactive approach is needed.

The second article in the series was on Corporate security on the Internet. This article works through common exploits that can be utilized to gain access to the corporate network. The same exploits can be used to gain access to the enterprise network. However by the nature of the infrastructure the enterprise wide network offers many more access points to the hacker.

A smart hacker or a group of hackers may launch multiple attacks on multiple enterprise locations, in an attempt to find multiple vulnerabilities and to eventually overcome the IT resources. This in return may cause disengagement of your VPN and Internet access, leading to thousands of dollars in lost revenue, and the theft of corporate data. This data may end up strewn across user groups on the Internet for all to see, or sold to a competitor for competitive gain.

If IT resources are remote, and security standards vary from site to site, it can be very difficult and time consuming to track the source of attack(s) and to take the appropriate security measures.

The key to a successful security strategy is central control of all policies and a central repository of security information, with constant monitoring of all security systems and network components.

The same good practices introduced in Article 2 should be deployed in the enterprise network. In addition to these, the following advice is offered to further secure your enterprise wide network.

Enterprise wide security on the Internet

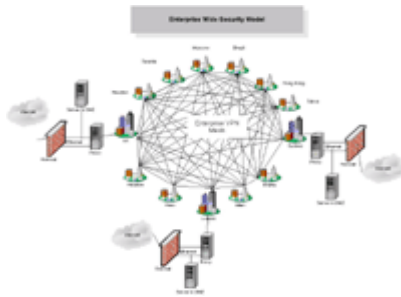
3

Published in: <http://newsviews.info/techbytes03.html>

NOTE: The information contained in this document is the property of Nexus Management and is disclosed to you on the condition that you maintain the information strictly confidential. You are hereby warned that the information disclosed is subject to change without notice or the assumption of any liability on the part of Nexus Management.

1. **Consider not using the full mesh for all your Internet access! : -**
 At first glance this statement may seem to some readers to defeat the object, and a regression back to the classic networks, and to a certain degree it does! Consider deploying the full mesh for your VPN. This gives you the full redundancy that you require for interoffice communication, but unless you have the money and the resources to invest in anti-virus, content scanning and firewalls at each site not to mention the constant auditing and upkeep of the rule set of each edge device, restrict internet access to a few key sites.

In this way you can control the flow of traffic between your enterprise network and the Internet. You can set up the same security infrastructure as described in Article 2, for key locations to access the Internet.



With fault tolerance and load balancing in mind you may want to deploy intelligent routing and set up a number of these structures within your enterprise wide network. This way you have the redundancy of VPN mesh, and the peace of mind that if one of your Internet access points fail another can take its place.

2. **Distributed Security:** This has been the Holy Grail of enterprise wide security. Article 2 introduced the concept of deployment of multiple Intrusion Detection Systems (IDS). However let's say you have 40 IDS devices within your enterprise, how do you manage them, and how do you proactively monitor the systems?

Seems like a large task? Well if you combine the correct technologies together, you may just have the Holy Grail.

3. Last week I introduced the merits of Snort as an IDS product. It would be great to have the 40 IDS's all report their findings to a central system, that in turn could e-mail, SMS, page, and visually alert you to the impending danger within a few minutes of the event occurring.

Let me introduce you to Big Brother. A wonderful product that allows you to monitor a number of systems, and to page, SMS and e-mail you of events, based on rules that you setup.

There is a Snort bridge, [snort2bb](#), allowing Snort to report its findings to Big Brother. In this way all your IDS's will proactively report their findings back to your Big Brother Console, every few minutes. You can even set up a rule that will page you when you are not in the office!

Would it not also be nice to have the same capability with Tripwire, so you could monitor changes on your key systems? Well there is a plug in for Big Brother available for the [tripwire program](#).

Article 2 also introduced [NMAP](#) as a powerful tool to monitor open ports on your network devices. There is a [script](#) that allows you to integrate NMAP and Big Brother. In this way you are aware when maliciously or inadvertently someone opens a port in your firewall, a device in your DMZ or your network.

Big Brother also has an NT/W2K/Unix/Linux agent which can pick up messages from the event viewers, so you can pick up messages about Anti-Virus, authentication, etc.

Big Brother also provides you with a mechanism to write your own plug in. So with a little bit of time and some programming skills, it is possible to integrate your own security products with this tool. Although no small undertaking, it may be far more cost effective to hire an individual with scripting skills than to deploy a full-blown security suite.

You may also want to use a commercial product with similar capabilities. A good suite of products is offered by [Computer Associates](#).

There are many products out on the market, take time to read reviews on these products. Good starting points are [Help Net Security](#), [Security Focus](#), [Eye on Security](#)

4. **Secure all remote VPN Users: -**

This has to be a vital part of your Internet security strategy. You may spend many hours and dollars configuring the perfect enterprise network security infrastructure, scan it with the tools described in [Article 2](#), only to find that a hacker by chance comes across a laptop with a VPN client installed, compromises this laptop and gains access to your enterprise network. [Article 1](#) describes the measures necessary to secure these individuals on the Internet.

5. **Central Management of Users: -**

Consider the central management of all your users. You may wish to

deploy a directory structure such as Novell's e-directory to manage all the authentication that take place on your enterprise network, including remote VPN users. A well-designed directory will ease the administration of users on the enterprise network and allow you easily to administer global users, groups and rights. Be stringent with user names and passwords. It is a good idea to work hand in hand with personnel, to track new users and employees who have left the system.

Members of the IT team should not use the administrative password. In fact although necessary at times for systems maintenance and recovery in the enterprise, there should be no use of the administrative users name and password.

6. Central deployment of Anti-Virus: -

You should invest in anti-virus software for every user, server and gateway device. You should be able to manage the distribution of anti-virus via a central console. Symantec and Trend Microsystems provide excellent products for the enterprise environment.

7. Wireless Networks:-

You should insist that all company business that takes place over a wireless infrastructure is encrypted. There are several ways of achieving this. You may deploy your VPN client on the client system to encrypt the data, or use SSL/TLS to secure transmissions between the user and the DMZ.

If you don't secure transmissions you run the risk of the transmission being intercepted by an individual with a simple packet analysis tool. A recent survey in London using nothing but a crisp/chips packet led to the discovery of 60 wireless networks in the financial districts.

Again as described by Article 1. Make sure that the system on the wireless network is secure. If you are providing a wireless network within a location for customers, consider placing their feed to the outside world on the DMZ.

8. Find your own weaknesses before the hackers: -

It is far less embarrassing and acceptable to find your own security gaps. Use the tools described in Article 2 to monitor your enterprise network and to flush out all security holes, on a regular basis. You would also be wise to run a password audit of all your users using the techniques described in Article 2, again on a regular basis.

9. Update your systems as frequently as possible: - As well as frequent updates for your anti-virus and IDS database, make sure you update BIOS's, Firmware and OS's on a regular basis, as these fix vulnerabilities as they are exposed. You may want to test updates in a test lab to understand the effect of your updates and then to put these updates into place.

Conclusion

All three articles have aimed at highlighting the dangers of living and working on the world's largest network, and to provide you with a set of tools and some guidelines. You may wish to adopt all or some of the suggestions depending on your needs. Take time to research different approaches to the question of security, be it for you personal computer, your corporation or your enterprise wide network, and choose a strategy most appropriate for your needs.

It is important to be vigilant and to be informed. Take time to sign up to news groups and newsletters from respected websites, and follow closely the exploits as they become unveiled. Once understood, apply the correct remedy for your systems.

Above all do not ignore the issue of security.

Shad Mortazavi