Global Information Assurance Certification Paper

SANS GSEC PRACTICAL ASSIGNMENT
Version 1.4b

Network Security issues arising from changing WAN and LAN technologies.

By James Drew

5 June, 2004

Abstract

This paper provides security options and how-to information for managers and network administrators, respectively when implementing a migration from Frame Relay to a Telco provided Multiprotocol Label Switching (MPLS). Security and design considerations required for companies wishing to migrate from a Telco provided Frame Relay wide area network to cheaper services are considered.

This paper proposes that there is there are alternative solutions to implementing Wireless 802.11x simply to provide mobile communications for companies that are primarily office based. Specifically this paper highlights security of the dynamic vlan capabilities of Layer 3 switches combined with other wireless communation strategies to provide a cost effective mobile soultion that a small to medium size enterprise (SME) can implement and keep secure with minimal resources.

Management rational for changing LAN and WAN infrastructure

This section should really be titled “Just because it’s the right solution for them doesn’t mean its right for you”. It is the responsibility of the MIS department to support the business processes in a cost-effective manner. This translates to the constant review of IT product and services used by the MIS department with a view to providing value for money, which in turn will see the MIS department have to migrate to some of these technologies.

It is a recognised business procedure for managers to base their decisions on relative risk and total cost of ownership. MIS infrastructure is no different to any other business procurement in this respect. There are also regulatory guidelines for certain business sectors that may discourage uptake of less secure technologies.

The IT manager also has the responsibility to incorporate security into new developments wherever possible as this is the most cost effective way to implement security. It is important for managers and budget makers to look at all aspects of security, from the physical security of the servers and communications equipment to sufficient resources (both in manpower and test equipment) to be able to keep as current as possible with patches for all IT equipment.

Certain topics such as Wireless and VPN’s dominate the literature with regards to security information for LAN and WAN, if the hype is to be believed then the future is wireless users connecting with laptops and PDA from home via Internet based VPN’s. While undoubtedly VPN’s can provide a very scalable and robust solution for some companies and also can provide a level of connectivity that was simply unaffordable to other companies. For the companies that can afford more expensive WAN connections such as frame relay the choice of what to migrate to requires careful consideration.

Wide Area Network migration from Frame Relay to MPLS

Wide area connections are often implemented on Frame Relay technology. A common implementation of Frame Relay is a set of point to point connections between customer routers. This type of connection allows the customer to use any protocol e.g. IP/IPX and virtually any routing protocol.

Recently Telcos have been offering MPLS based WAN soultions as an upgrade for Frame Relay connections. The business benefits of migrating to a MPLS based Wide Area Network is that the costs are significantly lower for the same bandwidth. The reason that the costs are lower is that MPLS network removes the concept of the Committed Information Rate (CIR). The removal of the CIR allows the Telco to utilise all of its bandwidth for any company rather than have bandwidth go unused as the company this bandwidth has been leased to isn't using it.

MPLS networks do not provide a point to point transparent virtual connection for customer routers. They also require that the only protocol that can be used is IP. Many MPLS networks use the Border Gateway Protocol (BGP) to define the VPN's as per rfc2547 [1].

Routing and Tunnels

In order to route data within an enterprise it is common practice to deploy an Interior Gateway Protocol [IGP]. However virtually all IGP's require the virtual adjacency of particiapating routers (i.e provider routers are transparent to the customer routers, for example Frame Relay). With MPLS and MPLS/VPN's this transparancy is not available. A common method for the enterpise to create this adjacency and thus allow the use of IGP is to create layer 3 tunnel interfaces between routers. A tunnel creates a virtual point to point connection between two devices that do not necessarily need to be adjacent. The use of tunnels simplifies the implementation of MPLS as being able to retain the current routing protocol has advantages in terms of reduced complication cost and risk.

However the use of tunnels interfaces, particularly when IPSEC is used to encrypt all traffic using the tunnel causes latency as each packet must be have its headers changed and the packet encrypted, which causes high CPU utilisation on the routers involved. This latency may be unacceptable for enterprises that utilise latency intolerant systems or searching for maximum performance. It should be noted that a tunnel interface with IPSEC is not the same as IPSEC between routers which is also refered to as a tunnel.

In order to maintain maximum performance an enterpise may well look at changing its current IGP to use a routing protocol which doesn't require provider backbone transparency and thus will not need a layer 3 tunnel. BGP is used by

MPLS/VPN's and can be used by the enterpise to route its traffic over the MPLS/VPN network.

While it should be policy to encrypt all traffic travelling over network which are not under the technical administration of the enterprise, IPSec is not the only way to encrypt data. For Example;

- The Citrix ICA protocol is encrypted and only shows screen-shots of the applications and thus would be hard to derive meaning data from an interception.
- SSL (128 Bit) connections for internal web services.
- SSH and secure FTP should be in use wherever possible.
- Choosing an application that encrypts certain fields so that the information is useless.

IPSec can be used for 'high-value' data or connections to high value devices. Management an make the decision on whether to use IPSec on a case by case basis dependent on the risk and the latency tolerance of the application in question. In such situations of high risk it would be advisable to use IPSec encryption host to host. Where Citrix is used it can be secured from the Citrix server to the high value host.

An IPSec installation between application servers and Citrix servers would be more secure than a distributed installation to provide IPSec from the Servers to the User PC. This is because the servers will be protected by physical security and will not be providing any certificate or key information to the user PC's (as part of a distributed IPSec solution). As this information can be used by an internal attacker (or external attacker who has managed to gain access to a User PC with an unauthorised wireless or modem device attached) to gain information about the security of the high value servers.

Securing BGP routers

BGP is unusual in the routing protocol world in that it uses TCP to communicate routing information. It relies on there being a valid IP connection over which to send routing updates. BGP will try to verify the status of the IP link by default. However due to performance issues that can occur when the routers try to synchronise, which may require link verification being removed.

IGP's such as EIGRP are simple in that they are just configured with the autonomous system number and networks that they will route. BGP has two distinct modes eBGP and iBGP. eBGP is used between autonomous systems (e.g. WAN Links) and iBGP is used within the same autonomous system (e.g. LANs). iBGP requires more configuration work than standard 'automatic' IGPs. This configuration work increases exponentially the more routers are added. In order to overcome such scalability issues iBGP uses route reflectors. Route Reflectors are BGP routers that act as a central database of routes for all BGP

routers in the same autonomous system. The use of route reflectors reduces the configuration work and the amount of overhead on the routers.

Network Administrators will find reviewing the Cymru BGP risk assesment document [2] extremely helpful in understanding the types and risks of Attacks that BGP routers can be sucesptible to and ways to secure the devices against such threats.

Denial of Service (DOS) attacks are relatively easy to do as routing protocols can easily be confused if malicious routing information can be propagated into the routing process. It should be noted that due to the fact that all the BGP routers will be internal to the firewalled permiter the threat vectors will be limited compared to Internet based BGP routers.

The BGP route reflector is the ideal target for attacks as all other iBGP routers will trust information that is provided from this router. This router should be as secure as possible.

There are several additonal configuration stategies that should be employed by the network administrator to increase the security of BGP routers.

1. The use of loopback addresses, which are within the IANA reserved address space for neighbor designation has three security advantages.

    - The Border router / firewall will not pass traffic with these addresses onto the Internet.
    - It increases the stability of the routing process by not slaving BGP to a physical port, which may fail and thus stop BGP routing to and from that device.
    - By having the loopback addresses on a non-physical, then the difficulty to add another device onto this network would not be possible.

2. Access lists should be configured on the VLAN and the ethernet and serial interfaces of the routers to prevent TCP port 179 (BGP) except from other defined BGP routers and telnet, SSH, ftp and tftp from administration devices.
3. The use of Router hardening tools for example Router Audit Tool (RAT) will help to secure the router itself from being compromised due to insecure configuration.
4. Logins to the routers should wherever possible use a centralised authentication server such as Radius, TACACS+ or Kerberos.
5. BGP secure templates [3] can provide a basis for BGP router configuration.

A very useful paper on simple tasks to secure existing BGP is provided by makesecure.com [4]. While it is aimed at securing BGP connections to the Internet, it is also very applicable to private business implementations of BGP as an IGP replacement.

The current US-CERT advisory on TCP vulnerabilities, [5] specifically states the impact of malicious activity on BGP routing processes. Using flaws in TCP sequence generators a hacker can perform a '*Man in the middle attack'* by hijacking a valid TCP connection. By injecting wrong routing information into the routing process the entire BGP network can be halted for as long as the incorrect information is injected.

BGP can be implemented securely if there is encryption of the TCP header, which means the TCP sequence numbers are not visible thus rendering a man-in-the-middle attack useless.

While BGP requires all neighbor routers to be specifically identified and thus is more secure than many IGP's, there is work continuing to provide a secure BGP protocol (SBGP) [6],[7]

Until a secure BGP is ratified and adopted by router manufacturers, the solution is to implement IPSEC on the routers to encrypt only the BGP traffic via a crytpo map. Technical configuration for IPSEC for Cisco routers can be found on their website [8]. This way the BGP routing process is secure and there are no latency issues on general traffic.

Local Area Network solutions

Vlan Membership Policy Service (VMPS)

Cisco promote VMPS as a security tool which allows a business to move machines from switch port to switch port while ensuring that a specific device has the same security privilege (VLAN).

The main advantages from VMPS for the business is the ability to perform office moves with minimal resource and downtime when compared to performing the same move in a switched environment which operates port security.

Some businesses with a high proportion of laptops or a 'hot-desking' policy, which means that static 'port security' is not an option. VMPS is also an option for businesses wishing to implement a hot-desking policy without having to implement wireless, which has its own technical and security issues and may be inappropriate for certain businesses.

VMPS is free with the Cisco 6000 series and is supported by the current range of access layer switches. These benefits make VMPS a very attractive option for MIS managers.

However there are security issues inherent with VMPS, which the network administrator should be aware of before deploying VMPS.

- VMPS provides the ability for a device, which is on a secured vlan protected by physical security, to work on any port on any switch in the vtp domain, even in an unsecured area by default, thus bypassing physical measures.

- Use of port security is incompatible with VMPS. Without port security switches are vulnerable to spoofing attacks.

- VMPS works by loading a plain text file containing the configuration of which devices are connected to what vlan automatically on reboot from a specified tftp server. Poisoning or even reading the VMPS plain text file would be very useful to the hacker as not only does it give information about which vlan's have what MAC addresses, port group information but also information about the VTP domain and the security state of VMPS.

Issue one can be addressed by

- Amending Security Policy to specifically state that devices from secure networks should not be placed on insecure networks without undergoing a process of reimaging and vmps entry change.

- Changing the default configuration to include ‘vmps port groups’, which can tie a set of MAC addresses to a specific access switch. Further information on VMPS configuration is available from Cisco [9].

Issues one and two can be addressed by

- Removing the ability to belong to certain vlan's on certain switches, regardless of VMPS entries.

It is assumed that the users are connected via access layer switches, for example 3500 series switches. These switches are in turn connected to the distribution layer 6000 series switch.

The main reasons for the assumption is that in this configuration the price per port is much less than connecting users straight to the distribution layer switch. Also this configuration allows the use of fibre to connect the access layer switches from a distance which allows the network to overcome the distance limitations of Ethernet.

When access switches that need to be able to connect to multiple vlans are connected to the distribution switch the link between them must be made a trunk link whereby a set of vlans is available to the access switch. All vlans are available by default on trunk links but you can modify the list per trunk, and thus what vlans are available to specific access layer switches. Access layer switches servicing insecure areas should have their trunk links modified on the distribution switch to remove the possibility of any port on the access layer switch being part of the secure vlan. This is true even if the access layer switch is compromised. Information on how to do this can be found on Cisco’s website [10].

- For the secure network access layer switches implement port security, port protection (switch will route all layer 2 traffic via a layer 3 router rather than between ports), remove user vlans from the trunk [11].

Issue three can be addressed by

- Specifying the VMPS server to download the plain text file only from the bootflash of the supervisor routing module.
- Should the routing module have IPSEC then in conjunction with an ACL the file can be pulled via FTP from a single admin PC (which should be on the same vlan as the switch.
- The plain text file should be encrypted while residing on the file server. It should only be unencrypted immediately prior to modification and upload.
- All configuration work regarding the VMPS should be logged for audit purposes.
- Password policy regarding quality and changing rotation should be strictly enforced on the 6000 series switch and router.
- The VMPS admin PC should be connected directly into the 6000 series using port protection and port security, to mitigate packet sniffing.

Wireless Devices

A common theme of security attacks is that the vulnerability has often been identified and the provider has provided a 'fix'. However inadequate patching processes mean that these fixes go unnoticed and thus the network remains vulnerable [12]. The MIS managers should realise that adopting a wireless network will increase the requirement on the patching process, especially as the increased number of threat vectors via access points being accessible from public areas e.g. Wardriving. If the MIS department doesn't have enough expertise to install a Wireless network securely and chooses to outsource the installation the manager should be sure the MIS department has enough expertise and resource to adequately patch such a system.

Wireless development is moving quickly in an effort to become as fast and reliable as wired networks, thus there is a very real situation of being left behind with an expensive system that cannot be secured without moving replacing all the wireless infrastructure e.g. 802.11a Vs 802.11g. This need for upgrades increases the demands of wireless system patching.

Businesses whose offices are pre-cabled with CAT5e can use VMPS to connect desktop; laptop or Ethernet enabled PDA's with minimal expenditure compared to 802.11 wireless installations. PDA's can be connected to the corporate network using several different technologies, so the choice of PDA can be critical to the LAN infrastructure that the MIS department is asked to provide.

- Ethernet wired PDA and laptop cradles utilise standard cabling.
- IR isn't practical due to the slowness of the protocol and the directed beam.
- Bluetooth is practical but the users administer access control (unless access points are provided) and it does have several security issues [13].
- Blackberry (GPRS) based systems are practical and use either GPRS or an Ethernet cradle to connect to the corporate network. The devices are usually purchased / leased from the GPRS service provider and so upgrade costs can be placed on the service provider.
- Other GPRS systems (e.g. Nokia) have similar solutions to Blackberry but use the increased functionality of mobile phones instead of PDA's. A case study is provided on Nokia's website [14].

Any wireless connection solution that doesn't require a distributed infrastructure to be purchased and maintained by the business would be preferable, provided the corporate data travelling over any infrastructure that is not under the businesses technical control is encrypted. However security should not only be applied to the transmission but the security of the information once it has left the corporate network and been delivered to a mobile device.

If the mobile devices have bluetooth in addition to the standard GPRS then the possibility exists that the corporate data can be stolen from the mobile device via bluetooth vulnerabilites or it being stolen. Hard drive encryption is possible on laptop devices but the data security on PDA's and Mobile phones is not as strong. Therefore the choice of mobile device may well depend on the value of the data that an individual is carrying.

While MIS managers can have Bluetooth turned off on mobile devices, it will be difficult to ensure that this continues to be the case once the device has been given to the user. The proper use of user training and an amended security policy should be used to reinforce the importance of Mobile device security to all those who are provided with company devices.

Conclusion

There are many ways for a medium size enterprise to have the benefits of being able to move users and devices around an office space with the minimum of disruption and the minimum of MIS resource. However managers need to review their ability to implement these strategies over a 3-5 year term in a secure and cost effective manner. There are cabled solutions such as VPMS and wireless solutions based on GPRS that can deliver flexibility for the workforce while keeping MIS administration and expenditure to a minimum. Wireless devices do not need to replace a cabled environment; a GPRS solution provides all the flexibility yet doesn't compete with the cheaper more secure cabled infrastructure.

BGP and MPLS can be used to provide the enterprise with maximum performance for latency intolerant applications. BGP routers can be secured with IPSEC just for the routing protocol while not affecting the general traffic. In future an encrypted BGP protocol should be available.

The use of VMPS and port security where necessary allows Network Administrator to maintain a high degree of flexibility when it comes to office moves and still provide high levels of security for certain 'high risk' individuals and departments.

With these systems MIS managers can provide lower cost solutions while not overstretching the maintenance resource required to keep these systems secure.

References

[1] Rosen,E. Rekhter, Y. “RFC 2547 - BGP/MPLS VPNs”. Cisco Systems. March 1999.
URL: http://www.faqs.org/rfcs/rfc2547.html (5 June 2004).

[2] Greene, Barry. “BGPv4 Security Risk Assessment”. Version 0.3.11 June 2002
URL: http://www.cymru.com/Documents/index.html (5 June 2004).

[3] Thomas, Rob. “Secure BGP Template” Version 3.3. 28 April 2004
URL:http://www.cymru.com/Documents/secure-bgp-template.html (5 June 2004).

[4] Kanclirz, Jan. “Make Secure BGP”. 15 Sept 2003
URL: http://www.makesecure.com/makesecure-bgp.pdf (5 June 2004).

[5] US-CERT. “Vulnerabilities in TCP”. 20 April 2004.
URL: http://www.us-cert.gov/cas/techalerts/TA04-111A.html (5 June 2004).

[6] Kent, Stephen. “Securing the Border Gateway Protocol” BBN Technologies. June 2003.
URL: http://www.cisco.com/warp/public/759/ipj_6-3/ipj_6-3_bgp1.html (5 June 2004).

[7] White, R. “Securing BGP through Secure Origin BGP” Cisco Systems. June 2003.
URL: http://www.cisco.com/warp/public/759/ipj_6-3/ipj_6-3_bgp2.html (5 June 2004).

[8] Cisco Systems Documentation. “Configuring IPSec”. Cisco Systems.
URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/config/ipsec.htm (5 June 2004).

[9] Cisco Systems Documentation. “Configuring Dynamic Port VLAN Membership with VMPS”. Cisco Systems.
URL:http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008019f046.html (5 June 2004).

[10] Cisco Systems 6500 Documentation. “Configuring Ethernet VLAN Trunks”. Cisco Systems.
URL:http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007f32c.html#1021347 (5 June 2004).

[11] Cisco Systems 3500 Documentation. “Configuring the Switch Ports”, Cisco Systems

URL:http://www.cisco.com/en/US/products/hw/switches/ps637/products_configuration_guide_chapter09186a00800d9d3d.html (5 June 2004).

[12] Sutherland, Ed."Examining Alternatives to Patching WEP" Wi-Fi Planet 18 January 2002
URL: http://www.wi-fiplanet.com/columns/article.php/958331 (5 June 2004).

[13] Kotadia, Munir. "Nokia admits multiple bluetooth security holes". ZDNet UK. 9 Feburary 2004.
URL:http://news.zdnet.co.uk/communications/wireless/0,39020348,39145886,00.htm (5 June 2004).

[14] Nokia. "Case Study: PPG industries". Nokia. May 2004.
URL:http://www.nokia.com/BaseProject/Sites/NOKIA_MAIN_18022/CDA/Categories/Business/BusinessMobility/MobileEmail/_Content/_Static_Files/ppgcasestudy_04may12.pdf (5 June 2004).