Published on *Jisc community* (https://community.jisc.ac.uk)

Home > Advisory services > Wireless Technology Advisory Service > Case studies > Cross campus virtual private network (VPN) tunnelling

Cross campus virtual private network (VPN) tunnelling

Stephen Moore, *The University of Liverpool*

Abstract

This case study provides a detailed overview of secure cross-campus VPN tunnelling between two collaborating organisations, namely the universities of Liverpool and Edinburgh. Implementation has allowed members of either university visiting the other campus to establish a secure connection to their own organisation using wireless infrastructure. The authentication takes place at the home organisation, and no additional registration for services is needed. This implementation utilised existing wireless infrastructures, VPN server hardware and Bluesocket wireless gateways and incurred no additional infrastructure costs, however, this would clearly be a consideration for a campus without the required infrastructure. Utilising an existing and already maintained infrastructure, there were no additional support or maintenance requirements for either university. Once implemented the project worked successfully as planned and has been shown to be reliable and secure with no performance issues relating to the use of secure encrypted tunnels, however it must be noted that the volume of concurrent use was limited. Success of the project during its first three months of implementation has been positive and has resulted in its expansion to include the London School of Economics (LSE). Visitors from the both Liverpool and Edinburgh have successfully established remote authentication over the LSE wireless infrastructure.

Introduction

It is a requirement that each student and staff member is provided with a username and password for use when accessing university IT facilities. Although not technically complex, the overall volume of logon details to issue is a large administrative task, increased further by the additional process of validating the identity of visitors and issuing temporary authentication details accordingly. As well as presenting an additional administrative burden on IT departments, such steps also bring inherent security risks as temporary logon details can often be misplaced, carelessly discarded or exploited. Furthermore, unless deactivated, such accounts could remain active presenting a potential backdoor into a university campus network.

The aim of this project is to help alleviate such potential problems, and minimise the administrative workload, through the implementation of an alternative method of authentication whereby participating organisations can safely grant network access to visitors. The proposed method allows a visitor to an organisation to authenticate a secure network connection against a local authentication server situated at their *home campus. (*The term *home* is used to refer to the visitors' organisation of origin. Additionally the user will be issued an IP address from their home campus network. This will bind the user to their home campus policies and additionally allow access to IP address restricted services.). Pressures to provide

enhanced accessibility to computing facilities, combined with heightened security awareness, suggests that all opportunities to further enforce and improve upon existing security policies should be openly considered.

Service Requirements and Constraints

The use of wireless technologies is desirable to provide a method of connectivity over which university visitors can establish a connection to their university of origin, as it provides for flexibility in the locations from which the service can be implemented and is a widely used technology, requiring little support from the host university. Bandwidth requirements for the implementation of cross campus VPN tunnelling are minimal and are based solely on the number of simultaneous users and their respective throughput. In comparison to bandwidth both available to, and utilised by, most organisations the impact will in the majority of circumstances be negligible. (In situations whereby multiple simultaneous users introduce a high combined throughput, bandwidth restrictions can be applied at the gateway. A Bluesocket wireless gateway is capable of policing such restrictions.) The project is subject to, and requires no greater service level requirement, than that currently implemented for the existing network infrastructure and VPN server; however successful use of the service will require a working service at both organisations. Cross campus VPN tunnelling requires little additional support or maintenance as it functions using existing infrastructures and services for which, in the majority if not all organisations, maintenance and support will already be available in-house.

Feasibility Study / Site Survey / Cost Comparisons

The cross campus VPN tunnelling project utilised an existing wireless infrastructure and VPN server at both organisations and there was therefore no requirement to conduct a site survey or to take additional costs into consideration. However, if an organisation wished to implement the project without having in place the necessary requirements then extensive feasibility studies, site surveying and cost comparisons should take place when planning and implementing both a wireless infrastructure and VPN service.

Although not implemented specifically for the project, each organisation utilised three key infrastructure components:

- Wireless network infrastructure;
- VPN Server;
- Bluesocket wireless gateway.

Cross campus VPN tunnelling was initially conceived to allow connections to originate from a wireless network, generally regarded as being insecure. In practice the proposed method could be used to allow a VPN tunnel and associated authentication to take place over any infrastructure presuming a default rule is in place to allow *unauthenticated* traffic to reach the target VPN server. With regards to wireless network access three distinct wireless standards currently exist, these being 802.11a (54Mbit/s), 802.11b (11Mbit/s) and 802.11g (54Mbit/s), the main difference between the standards being throughput and range. Any of these wireless standards is suitable; however the implementation in use at both Liverpool and Edinburgh universities is 802.11b. (The wireless access points at The University of Liverpool support both the 802.11b and 802.11g standards. However due to performance drawbacks in allowing the simultaneous use of both standards only 802.11b is presently offered due to this being the

most commonly used standard. The University of Edinburgh are running a combination of 802.11b only and 802.11b/g compatible mode standards.)

If an organisation wishes to participate in cross campus VPN tunnelling they will require a VPN server on campus to which their staff or students can establish a secure tunnel from the organisation that they are visiting. (The organisation being visited must be participating in cross campus VPN tunnelling.) Most organisations have already implemented a VPN server, however if a participating organisation does not have a VPN server they may still participate by permitting visitors' to their organisation access to the VPN server at their *home* organisation. The University of Liverpool uses a Cisco® 3005 VPN Concentrator and Edinburgh a Cisco® 3030 VPN Concentrator.

A Bluesocket wireless gateway is required to follow the guidelines in this case study. However, the concepts could be applied to wireless networks secured using different gateways, including a Linux based computer configured as a NAT/firewall gateway or even a firewall interface onto a demilitarized zone. The Bluesocket gateway recognises all connections to the wireless network and denies them access onto the campus network (and beyond onto the Internet) until successful authentication has taken place. By allowing unregistered users access to their home VPN server only, it is possible to tunnel directly through the Bluesocket wireless gateway and authenticate at their *home* campus without the need to authenticate against the local gateway.

Although the implementation of the case study is feasible over a range of different network infrastructures, there are potential constraints. The largest constraint is the infrastructure used to supply a wireless network within a university. The proposed method requires the use of a gateway to provide firewall and authentication capabilities. This proposed system would not work for universities that provide authentication *within* the wireless access points themselves using static username/password lists or who do not use username/passwords but instead restrict connections based on MAC address. Additionally if Wired Equivalent Privacy (WEP) is used to encrypt the wireless traffic then the WEP encryption key would need to be made available to visitors and would therefore have a potential impact on the overall security. Obviously the service also relies on the VPN server at the target university being available and contactable.

Finally, the performance of the connection will depend on three key factors:

1. The performance of the wireless network connection between the client and the wireless access point will have an impact on the total possible throughput. Although with wireless speeds operating between 11Mbit/s and 54Mbit/s, there are circumstances whereby if a particularly weak signal is established speeds could be as low as 1Mbit/s.
2. The performance and load of the *home* VPN server is likely to have an impact on the performance of the service. If a low capacity VPN server is in operation and experiencing a high load then this will probably have a negative impact on the overall performance.
3. Finally, for completeness, the network infrastructure transporting traffic between the wireless access point and the home VPN server will also be a key consideration in determining performance. However, it is presumed that such an infrastructure will be unlikely to present any performance considerations due to the comparatively low throughput being utilised.

Project Planning

The planning and implementation of the project required collaboration between both

organisations and was broken down into the following:

1. Realisation of the need for *remote* authentication capabilities. (The term 'remote' is used to represent an organisation other than the organisation at which the user is currently located – usually the organisation of origin for a visitor.
2. Investigation into the feasibility aspects of *remote* authentication.
3. Suitability study undertaken on using existing wireless infrastructures, VPN server hardware and wireless gateway technologies.
4. Security, reliability and performance aspects considered.
5. Project scalability and co-ordination assessment.
6. Implementation and initial testing.
7. Real world testing.

Procurement

N/A

Implementation

The implementation guide will presume the following:

- A Bluesocket wireless gateway, running software release V3.0.0.12F or higher, is already physically installed, configured and operational.
- The reader has knowledge of the Bluesocket gateway product; including how to access the Bluesocket administration interface and make configuration changes.
- That a VPN server is installed, configured and in active service. Configuring and implementing a VPN server is outside the scope of this case study.
- Any gateway firewalls controlling access to the Campus network/VPN server will allow connections from the necessary source locations.

The Bluesocket wireless gateway acts as a firewall between an *insecure* wireless network and a *secure* campus network. All users connected to the wireless network are assigned a role by the Bluesocket gateway. Those users who are connected, but yet to authenticate (and therefore have no access past the gateway) are assigned an unregistered role. Authenticated users can be assigned into different roles based on their profile; The University of Liverpool categorises users into undergraduate, postgraduate or staff roles and can control access rights accordingly. As visitors to the university will not have a user account on the local authentication server, it is necessary to allow them access, through the Bluesocket gateway, to their home VPN server destination for remote authentication.

By default a user is assigned the unregistered role when they have established a connection to the wireless network and have received an IP address from the Bluesocket Dynamic Host Configuration Protocol (DHCP) server (or relayed from a central campus DHCP server) but are yet to authenticate to receive network access. Whilst in the unregistered role the

Bluesocket gateway restricts access to DNS lookups only (this is necessary to allow the client to attempt to access a web page which then is redirected to the Bluesocket login page). For the implementation of cross campus VPN tunnelling, additional access to respective VPN servers at remote campus locations must be allowed.

- To configure a Bluesocket wireless gateway the required VPN server destinations must be defined.
  - Log into the Bluesocket administrator interface.
  - Select the *Destinations* tab and sub option *Destinations*.
  - Add a new Destination with an appropriate name and the IP address of the associated remote VPN server [*See Appendix A, Image 1*].
  - Repeat this step for all required VPN servers.
- Unregistered users should be granted access to the VPN server destinations.
  - Select the *Roles* tab.
  - Edit the unregistered role [*See Appendix A, Image 2*].
  - Add extra policy entries to this role allowing *any* service in *bothdirections* to the VPN server destinations [*See Appendix A, Image 3*].
  - Save this once completed.

At this point the destination VPN servers have been created within the Bluesocket gateway and access to them has been granted through the unregistered role.

A visitor to the university should now be able to establish an initial connection to the local wireless network and then, using their own VPN client, establish a secure tunnel to their home VPN server with authentication taking place against their home authentication server. No authentication capability has to be granted locally once the initial configuration has taken place. Furthermore granting unregistered access to remote VPN server introduces few security considerations as VPN servers are, by their nature, generally publicly accessible.

Operational Performance

During the three months since its implementation the service has operated as expected and the results have been encouraging.

The aim of the project was to remove the requirement for obtaining temporary authentication details when visiting the other organisation. Based on this requirement the project has been a resounding success as authentication can now take place using the visitors home authentication credentials. The performance and reliability of the project has been excellent with the use of secure VPN tunnels not showing any notable impact or degradation on the connectivity speeds over the wireless network, though clearly they provide additional security over an insecure wireless medium.

The success of the project has resulted in its expansion to include LSE who, although not having a VPN server, have successfully enabled visitors from both Liverpool and Edinburgh universities to establish secure tunnels back to their home organisations for authentication. LSE do have a Bluesocket wireless gateway and at the time of writing are planning on implementing a VPN server into their network infrastructure in the near future.

Benefits of Project

The benefits of cross campus VPN tunnelling are significant with regards to a reduction in administrative tasks and improvements in security. The effectiveness of the project however is limited by the number of organisations that implement the scheme. Clearly the greater the number of organisations that allow cross campus VPN tunnelling the more useful it will be as a means of remote authentication.

Lessons Learned

Several fundamental issues have risen from the project.

- The scalability of the scheme requires consideration, as each site needs to be specifically configured to allow default access to all other participating sites. With small numbers of participants this poses few problems, however with a large number of sites this could prove unwieldy and would require a central coordination facility. A proposed approach could be a central list of participating universities and their VPN server IP address. If a new organisation wishes to participate in the scheme they must submit their details to the list (to be granted access by all list members) and likewise they must permit access to all existing entries on the list.
- The use of IP addresses could be a potential problem if an organisation changed the IP address of their VPN server. This would require each participating organisation to update their configurations accordingly and could be overcome using a fully qualified domain name. A further improvement on this concept could be made using a 'common format' for domain names that point to a VPN server, for example vpnserver.liv.ac.uk or vpnserver.ed.ac.uk.
- A separate area for consideration is the configuration of end user VPN clients as a user must configure and/or install a VPN client as required for connection to their *home* organisation. (7 Details on the Liverpool and Edinburgh university VPN clients are available online at http://www.liv.ac.uk/CSD/systems/VPN/index.htm [1] and http://www.ed.ac.uk/schools-departments/information-services/computing/c... [2] respectively.) Variations amongst organisations of VPN server manufacturers and configurations result in a range of requirements from client software. Knowing such requirements and associated configuration can create problems for users not based at their 'home' university, for example a distance learning student or staff member working between two organisations. A particular example of this is the use of split-tunnelling to reduce the load on a VPN server by only tunnelling data destined for the target network, all other data destined elsewhere is directed onto the Internet in the normal manner. This configuration poses two problems for cross campus VPN tunnelling, the first being that it requires the use of a specific client with a specific configuration before a session can be established. Secondly, the configuration will only tunnel data destined for the target network, therefore a user can access data from their *home* organisation but all other requests to different destinations are directed over the *local* wireless network which, as the user has not locally authenticated, may be blocked.

Summary

To summarise it is clear that the cross campus VPN case study has put forward a useful concept that has been proven to function as planned. Security can be greatly increased amongst organisations and the administrative burden on IT departments reduced

considerably, especially during the hosting of a large function or seminar. However, the overall success of the deployment of such a scheme would depend largely on the number of participating organisations. Scalability must be considered; as more organisations participate access control filters will become more complex. This can have a detrimental effect on performance. However such performance loss is likely to be insignificant and should not pose

[3]

[4]

Image 2

Policy	Action	Service	Direction	Destination
1	Allow	DNS	Both ways	Any
2	Allow	Any	Both ways	Edinburgh University VPN Server

[5]

Image 3

Trademarks

Cisco is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the US and certain other countries.

Links
[1] http://www.liv.ac.uk/CSD/systems/VPN/index.htm
[2] http://www.ed.ac.uk/schools-departments/information-services/computing/connecting/vpn
[3] http://community.ja.net/system/files/images/wtas-crosscampuscasetudy01.jpg
[4] http://community.ja.net/system/files/images/wtas-crosscampuscasetudy02.jpg
[5] http://community.ja.net/system/files/images/wtas-crosscampuscasetudy03.jpg