

# Gateshead Grid for Learning

## Policies and Guidance

### External Servers & Remote Access

#### Table of Contents

Introduction.....	1
External Servers & Remote Access Policy.....	1
GGFL - VPN.....	2
GGFL – Web/FTP Servers.....	2
GGFL – Mail Servers.....	3
Data Flow.....	3
Incoming Bandwidth.....	4
Glossary.....	5
PPTP.....	5
L2TP.....	5
IPSec.....	5
SSL.....	5
Application for External Servers & Remote Access .....	6

#### Introduction

This document is intended to provide general information and guidance related to connecting school LANs to the broadband Grid for Learning network, and running school systems and servers effectively to deliver a reliable, high performance service. It also provides specific policies adherence to which is necessary for the smooth and effective running of the whole network.

#### External Servers & Remote Access Policy

Schools wishing to forward external addresses to their LAN introduce security flaws and compromise the network integrity. This address forwarding facility is normally associated with web server, mail server, and remote access type connections, other server type connections can be submitted for consideration. It is recommended that schools use the Gateshead Grid Data Centre to house servers such as web or mail servers. Where this is not practical technologies such as reverse proxy, co-location etc should be considered when connecting WAN to LAN. This will mitigate much of the risk associated with forwarding Internet traffic across the WAN directly to school appliances.

Remote access to a site is not recommended by the Grid for Learning as it provides an enormous risk to the integrity of data held on the school LAN. This type of access normally creates a direct tunnel between a third party and the school LAN, effectively joining the network/PCs of the two parties together into a single network. The school must take every precaution to ensure that a remote access connection does not give access to sensitive or private data stored on the school site. Schools may also experience unwanted attention from “Hackers” attempting to infiltrate sites and/or “Denial Of Service (DOS)” attacks which could bring a network to a stand still. The following is an excerpt from a report compiled by NTA Monitor, a company that specialises in the security and audit of IT networks.

“NTA Monitor's 2006 VPN Security Report reveals that the IT industry is the most vulnerable sector to network attacks. Tests were conducted on a variety of sectors - charities, finance, government, IT, manufacturing and utilities.

Of the IT organisations tested, an average of nine vulnerabilities were found per organisation, most of which were classified as low level risks. However, the number of medium risks identified, which may enable external attackers to disrupt VPN services or gain unauthorised network access, was above average, indicating that IT is the most insecure sector.

Overall, the 2006 VPN Security Report findings show that although organisations tested have taken the necessary steps to reduce high risk security vulnerabilities, medium, low and informational level risks are still very common leaving companies and public sector organisations vulnerable.

Of all the risks discovered, 17% were classified as medium level risk while the majority (64%) were of a low criticality level. The lower risk vulnerabilities will allow attackers to gain valuable information, which combined with other vulnerabilities, can lead to a denial of service attack or let hackers view and use confidential data.”

*NTA Monitor, <http://www.nta-monitor.com/posts/2006/04/ipsec-risks.html>*

Schools wishing to allow remote access to their network must complete a form to recognise that they will take the responsibility for breaches in the school network security following the implementation of a remote access solution or the forwarding of ports to a school sited appliance.

Please complete the form on the last page and send an original copy, signed in ink, to

Gateshead Grid for Learning  
ICT Admin  
Unit 6 Keel Row  
The Watermark  
Metro Riverside Park  
Gateshead  
NE11 9SZ

The following document sets out the protocols that can be forwarded to school LANs. This does not effect the ports listed for outgoing connections. Outgoing ports available to schools are listed in “Web Filtering Policy”.

## **GGFL - VPN**

The following types of tunnelling protocol can be forwarded to the school LANs.

Protocols include; PPTP, L2TP, IPSec,SSL

Schools can decide upon any vendor they choose to supply the VPN connection. However, the connection must be made client (external workstation) to host (school appliance). VPN connections made from the school LAN to an outside facility will not be allowed. This type of connection is filtered according to the Gateshead Grid “Filter Categories”, and described in the SLA as a category that can not be requested for whitelisting by schools.

Schools requiring advice on building and configuring such VPNs can purchase consultancy from many third party vendors or ictGateshead. Each type of VPN should be considered on its scalability, security and cost. Some of the above VPN types can be implemented freely on existing network appliances. See Glossary for short description of VPN types.

The following describe the incoming ports that can be opened for schools as requested by the appropriate authority.

## GGFL – Web/FTP Servers

The following protocols can be forwarded to school based web servers.

Protocol	Port
HTTP	TCP IP 80
HTTPS	TCP IP 443
FTP	TCP IP 21

## GGFL – Mail Servers

The following protocols can be forwarded to school based mail servers.

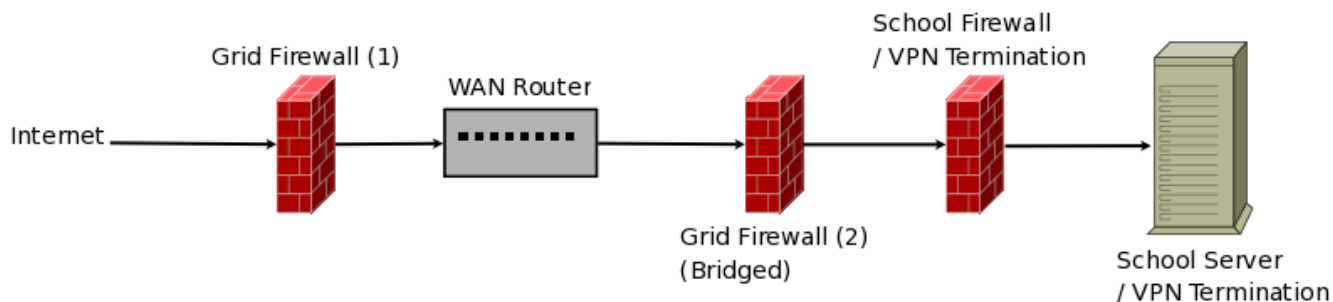
Protocol	Port
SMTP	TCP IP 25
SMTPs	TCP IP 465
POP3	TCP IP 110
POP3s	TCP IP 995
IMAP	TCP IP 143
IMAPs	TCP IP 993

## Data Flow

Internet connections that comply with the above protocol descriptions are forwarded from GF1 via the WAN infrastructure to GF2. GF2 acts as a bridged connection to the school firewall. Schools may terminate a VPN on their firewall or within the school LAN.

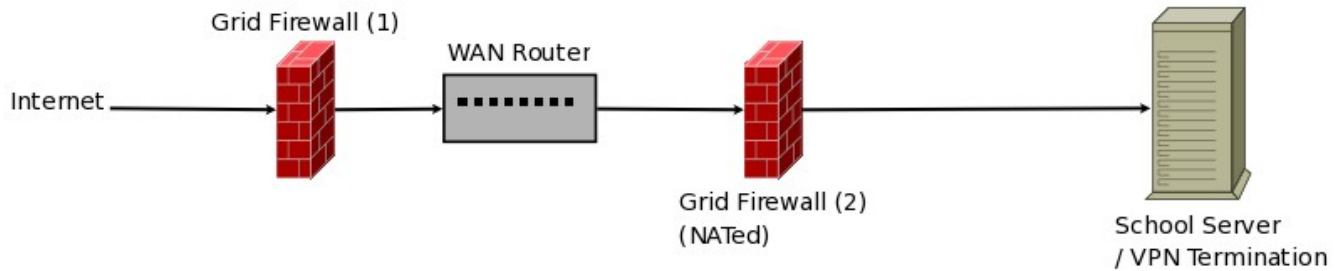
Scene 1 describes a typical secondary school where the firewall is implemented and controlled by the school. The Gateshead Grid's responsibility ends at GF2.

## Scene 1



Scene 2 describes a typical primary school where the firewall is implemented and controlled by ICTGateshead. The Grid's responsibility ends at GF2.

## Scene 2



### Incoming Bandwidth

The Gateshead Grid has a finite quantity of bandwidth available to schools. The Fibre backbone operates at 100Mb. Available bandwidth, after overheads, can be comfortably approximated as 85% of the theoretical 100mb. This bandwidth must be shared equitably (often called a fair usage policy) between all those who access the Grid. Schools are allocated incoming bandwidth from pupil/staff numbers. Incoming bandwidth usage will be monitored at GF2. The allocated bandwidth is not a hard limit. Schools occasionally breaching this total will not have their bandwidth allocation restricted. However, if this allocation is breached for more than 3 days (72 hours) within any 31 day period by more than 15% then the allocation will be enforced through Class of Service (COS) at the appropriate Grid firewall.

Available Incoming Bandwidth (85%) Kb	Total Pupils/Staff Population	Kb per pupil/staff	Pupil/Staff Numbers #	Schools Inbound Bandwidth Kb	Schools Inbound Bandwidth Mb
87040	30000	2.9	2250	6,528	6.4
87040	30000	2.9	2000	5,803	5.7
87040	30000	2.9	1750	5,077	5.0
87040	30000	2.9	1500	4,352	4.3
87040	30000	2.9	1250	3,627	3.5
87040	30000	2.9	1000	2,901	2.8
87040	30000	2.9	900	2,611	2.6
87040	30000	2.9	800	2,321	2.3
87040	30000	2.9	700	2,031	2.0
87040	30000	2.9	600	1,741	1.7
87040	30000	2.9	500	1,451	1.4
87040	30000	2.9	400	1,161	1.1
87040	30000	2.9	300	870	0.9
87040	30000	2.9	200	580	0.6
87040	30000	2.9	100	290	0.3
87040	30000	2.9	50	145	0.1

#Schools will be approximated to the higher Pupil/Staff numbers.

# Glossary

## PPTP

PPTP establishes the tunnel but does not provide encryption. It is used in conjunction with the Microsoft Point-to-Point Encryption (MPPE) protocol to create a secure VPN.

PPTP has been criticized in the past for various security flaws; many of these problems have been addressed in current versions of the protocol. Using EAP authentication greatly enhances the security of PPTP VPNs.

## L2TP

The L2TP client is built into Windows 2000, XP and 2003, but you can download client software for most pre-Windows 2000 operating systems (Windows 98, ME and NT 4.0)

L2TP requires the use of digital certificates. User authentication can be performed via the same PPP authentication mechanisms as PPTP, but L2TP also provides computer authentication.

L2TP has several advantages over PPTP. PPTP gives you data confidentiality, but L2TP goes further and also provides data integrity (protection against modification of the data between the time it left the sender and the time it reached the recipient), authentication of origin (confirmation that the user who claims to have sent the data really did), and replay protection (which keeps a hacker from being able to capture data that is sent, such as the sending of credentials, and then “replay” it to “trick” the server). On the other hand, the overhead involved in providing this extra security can result in slightly slower performance than PPTP.

## IPSec

IPSec in tunnel mode secures packets that are transmitted between two gateways or between a client computer and a gateway. As its name implies, an IPSec VPN works only with IP-based networks and applications. Like PPTP and L2TP, IPSec requires that the VPN client computers have client software installed.

IPSec support is included in Windows 2000/XP/2003, but not in older Windows operating systems. VPN gateway vendors, such as Cisco and CheckPoint, provide client software for their IPSec-based VPNs. Note that you may have to purchase licenses for the client software.

## SSL

SSL VPNs operate at an even higher layer of the OSI model than IPSec VPNs: the session layer. This gives them the ability to control access more granularly. SSL VPNs use digital certificates for server authentication. Other methods can be used for client authentication, but certificates are preferred as the most secure.

# Gateshead Grid for Learning

## Application for External Servers & Remote Access

School name : \_\_\_\_\_

I agree with the following statement:-

Remote access to a school site provides an enormous risk to the integrity of data held on the school LAN. This type of access normally creates a direct tunnel between a third party and the school LAN, effectively joining the network/PCs of the two parties together into a single network. The school must take every precaution to ensure that a remote access connection does not give access to sensitive or private data stored on the school site. Schools may also experience unwanted attention from "Hackers" attempting to infiltrate sites and/or "Denial Of Service (DOS)" attacks which would bring a network to a stand still. The Headteacher and Governing Body accepts all responsibility for any such breaches in network and data security or the denial of ICT services within the school.

### Declaration

I have read and understood the document "Gateshead Grid for Learning Policies and Guidance: External Servers & Remote Access (Version 1.01 - 04/12/08)". I am aware of and have assessed the implications of implementing access to my school network and wish to proceed.

Signed \_\_\_\_\_ (Head Teacher) Date \_\_\_\_\_

Print Name \_\_\_\_\_

Signed \_\_\_\_\_ (Chair of Governors) Date \_\_\_\_\_

Print Name \_\_\_\_\_

Witness \_\_\_\_\_ Date \_\_\_\_\_

Print Name \_\_\_\_\_ Position \_\_\_\_\_

N.B. This must be signed by the Head Teacher or Acting Head Teacher and the Chair of Governors of the school requesting the service.

