

ICT Data Transfer systems within LSICT: IPsec

Context

Under the Data Protection Act of 1998, the LEA is required to ensure that data maintained within its systems is both secure and processed in accordance with the data subject's rights - thus it is the responsibility of Learning Services ICT to protect relevant electronic data from:

- Data modification during transfer;
- Interception, viewing, or copying if intercepted;
- Being accessed by unauthenticated/unauthorised parties.

As a result of the testing and evaluation of appropriate systems, it has been decided that implementation of a secure file server utilising Windows 2000 Internet Protocol Security (IPSec) would provide the most effective return on investment with regard to ease of client use, minimising administrative overheads and increasing data security.

This document aims to provide both an overview of IPSec as implemented in Microsoft Windows 2000 and the considerations necessary for its effective application within the context of Learning Services ICT.

Overview of IPSEC as implemented in Microsoft Windows 2000

IPSec is a framework of open standards for ensuring private, secure communications over IP networks through the use of cryptographic security services. The Windows 2000 implementation of IPSec is based on standards developed by the Internet Engineering Task Force (IETF) IPSec working group.

IPSec has two goals:

- To protect IP data packets;
- To provide a defence against network attacks.

These are met through using a combination of cryptography-based protection services, security protocols, and dynamic security key management.

IPSec is based on an end-to-end security model: the only stations that need to be IPSec-aware are those involved in the sending and receiving of data packets - each station handles security at its respective end, with the assumption that the medium over which the communication takes place is not secure. This implicit assumption both increases data security and reduces financial overheads, as the routers that forward packets between the source and destination are not required to support IPSec.

The end-to-end security model allows IPSec to be successfully deployed for the following scenarios:

- **Local area network (LAN):** client/server, peer to peer.
- **Wide area network (WAN):** router to router.
- **Remote access:** dial-up clients and Internet access from private networks.

Within the above systems, IPSec policies can be used to provide the following:

- **Access control** - connection negotiation and filtering of inbound communications.
- **Integrity** - checksums and message digest algorithms are used to allow detection of tampered packets.
- **Data origin authentication** - ensuring the source of the data is valid.
- **Outbound protocol filtering** - management of data before it leaves the system.

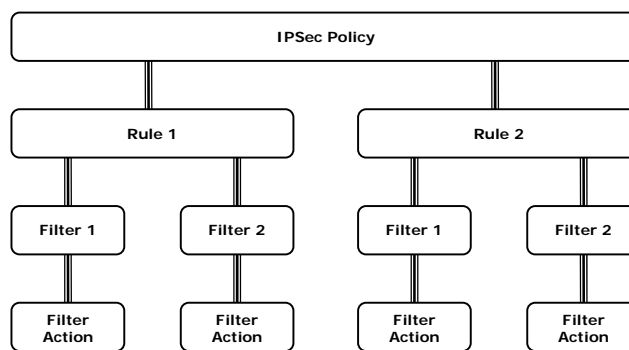
ICT Data Transfer systems within LSICT: IPSec

IPSec policies

IPSec policies are composed of rules that determine how and when the policies are used. These rules, consisting of a list of filters and filter actions, are triggered by source, destination and type of IP traffic: a match between a filter and packet header information triggers the rule, with the subsequent acceptance/rejection of the communication being determined by the filter actions. Each policy can have multiple rules and the rules can all be active simultaneously or singly.

IPSec therefore consists of the following:

- **Filters** - which accept or reject packets.
- **Rules** - determining which filters are to be in effect.
- **Policies** - the administrative unit of rules in effect.



Configuring IPSec for Inter-Network Security

To create secured communications between remote networks, IPSec can be configured for tunnel mode: this enables the authentication and encryption of data flowing within an IP tunnel created between two routers. The advantage of this mode is that data is secure between the two tunnel endpoints, regardless of the ultimate destination: thus all communications between networks are secure, without requiring the configuration of IPSec on each station. However, tunnel mode does not provide security *within* each network: for site-specific network security, IPSec for transport mode is required. Transport mode, the default IPSec mode, authenticates and encrypts data flowing between any two stations running Windows 2000 where communication between these two stations is not required to pass across a router.

Customising IPSec Policies

Customised IPSec policies can be created to select:

- Which stations require encryption;
- The security methods that are used for any encryption.

Levels of station security identified by Microsoft include the following:

- **Minimal** - no sensitive data, no IPSec.
- **Standard** - balanced security using a range of policies including minimal policies (e.g. where policies may be enabled but not required for data transmission).
- **High Security** - highly sensitive data at risk of theft or disruption (i.e. remote dialup access, public network communications).

Policy invocation is governed by rules which provide the ability to initiate and control secure actions based on the source, destination, and type of IP traffic.

ICT Data Transfer systems within LSICT: IPSec

Each IPSec policy may contain one or more rules, any number of which may be active simultaneously - the type of policy can be as follows:

- **Pass-through policy** - IPSec ignores the traffic: utilised when
 - Communication is necessary with a station that cannot be secured;
 - The traffic is not considered sensitive;
 - The traffic provides it own protection (Kerberos, SSL, PPTP).
- **Blocking policy** - this traffic will not be accepted or allowed to pass. This will help stop communication from a rogue station; it can also prevent traffic from leaving a system.
- **Permit policy** - no traffic is allowed to pass unless a filter for it is defined.
- **Negotiated policy** - the policy is negotiated with other IPSec-enabled stations, but allows communication with non-IPSec-enabled stations: enables the control of communications from sensitive stations while also allowing traffic from non-sensitive stations.

Windows 2000 provides three default rules that encompass a variety of client and server-based communications.

Windows 2000 Predefined Policies

Windows 2000 default policies, rules, and filter actions are as follows:

- **Client (Respond Only)** - does not secure communications most of the time;
 - Can respond to requests for secure communications by using default response rule.
 - Only requested port and protocol traffic is secured.
 - An effective policy to set on clients: when the client accesses a secured server, it will respond - otherwise, it uses normal communications.
- **Server (Request Security)** - secures communication most of the time;
 - Allows unsecured communication from non-IPSec-enabled stations.
- **Server (Require Security)** - secured communications required at all times;
 - Unsecured communications from any source are rejected.

The effects of these policies are summarised below:

	No policy	Respond policy	Request policy	Require policy
No policy	Open communication	Open communication	Open communication	No communication
Respond policy	Open communication	Open communication	Communicate only if IPSec matches	Communicate only if IPSec matches
Request policy	Open communication	Communicate only if IPSec matches	Communicate only if IPSec matches	Communicate only if IPSec matches
Require policy	No communication	Communicate only if IPSec matches	Communicate only if IPSec matches	Communicate only if IPSec matches

ICT Data Transfer systems within LSICT: IPsec

IPsec Rule Components

A rule consists of the following components:

- **Tunnel Endpoint:** defines the tunnelling station closest to the IP traffic destination, as specified by the associated IP filter list - there must be two rules to define an IPsec tunnel, one for each direction.
- **Network Type:** applies to connections configured in Network and Dial-up Connections. Select one of the following options:
 - All network connections.
 - Local area network (LAN).
 - Remote access.
- **Authentication method:** defines the method for verifying the identity of a user - three authentication methods are supported by Windows 2000:
 - **Kerberos v5:** the default authentication protocol in Windows 2000, valid for any clients that are running the Kerberos v5 protocol that are located within the same forest or within a trusted Kerberos realm.
 - **Public Key Certificates** - necessary for Internet communications, remote access, external partner access, L2TP (Layer 2 Tunnelling Protocol) communications, and stations that do not use Kerberos v5. To use certificates, at least one trusted Certificate Authority (CA) must be configured: this is usually located on an enterprise level server.
 - **Pre-shared keys:** specifies a secret, shared key that two users agree upon and manually configure prior to use.
- **IP Filter List:** defines which traffic will be secured with this rule: policy-specific filters for certain types of IP traffic or specific subnets can be created, or the following default filters can be used:
 - All ICMP traffic.
 - All IP traffic.
- **Filter Action:** iterates the security actions that will occur when traffic matches an IP filter, where the action specifies whether to permit the traffic, block the traffic, or negotiate the security for the given connection. One or more negotiated filter actions may be specified with the first listed taking priority: if a filter action cannot be negotiated, the next filter action will be attempted. Each filter contains the following:
 - Source and destination address - specific IP addresses, subnets, or networks.
 - Protocol - the default covers all TCP/IP protocols but individual protocols can be specified.
 - Source and destination ports (TCP and UDP) - the default covers all ports, but can be configured to apply only to packets on a particular port. Both inbound and outbound filters must exist and in both inbound and outbound communications, packets are matched with filters.

ICT Data Transfer systems within LSICT: IPsec

IPsec Encryption Schemes

IPsec offers a variety of authentication and data packet encryption algorithms, the use of which varies in accordance with the sensitivity of the information

- **Authentication Encryption:** there are two authentication encryption choices:
 - **Secure Hash Algorithm (SHA):** Federal Information Processing Standards (FIPS) accepted for U.S. government contracts. This high-security method uses a 160-bit key.
 - **Message Digest 5 (MD5):** most widely used method for commercial applications. This high-security method uses a single 128-bit key and has a lower performance overhead.
- **Packet Encryption:** there are three available types of data packet encryption:
 - **56-bit DES:** a method used for most exported applications and low-security business traffic, such as e-mail. This low-security method uses a single 56-bit key.
 - **40-bit DES:** a method supported for application exports to France. This low-security method uses a single 40-bit key. The 40-bit Data Encryption Standard (DES) is not RFC compliant and therefore will not be evaluated for LSICT requirements.
 - **3DES:** the most secure method, 3DES uses three 56-bit keys and processes each block three times, using a unique key each time. This high-security method increases processor utilisation by a factor of about 2.5 compared with other DES encryption types.

Recommended Implementation

IPsec Policies

Windows 2000 default policies have been examined to see whether they meet some or all of the identified needs of the project: at this stage it appears that a combination of the Client (Respond Only) and Server (Require Security) policies will best meet the requirements of LSICT. This combination will ensure server security at all times while allowing client stations to operate in a way whereby security implementation is transparent to the end user. However, due the increasing requirement of SIMS (particularly Assessment Manager) access across curriculum networks, it may become necessary to develop bespoke IPsec policies to facilitate curriculum (i.e. site-local) access at a lower level of security than that needed for site-to-LSICT (i.e. external to site) traffic, to prevent disruption occurring between RM Connect servers and the Admin servers: implementation of the default Server (Require Security) policy on the Admin servers would theoretically prevent access from RM Connect 2.3/2.4 (Windows NT4) servers and may cause disruption to access from RM Community Connect 3 (Windows 2000) servers. Any bespoke policies created will be developed to meet the Microsoft definition of High Security for servers/stations, with all policies whether default or bespoke being implemented and managed through Active Directory Organisational Units.

IPsec Rules and Filtering

- **Tunnel Endpoint:** these will be the client-site admin server and a server at LSICT (this does not have to be the secure server, merely a server through which access to the LSICT network occurs – however, to reduce administrative overhead and maintain the highest possible security, it is recommended that the secure server be the LSICT tunnel endpoint).
- **Network Type:** it is recommended that rules be applied to all network connections.
- **Authentication method:** Public Key Certificates are recommended, with the configuration of a trusted Certificate Authority server at LSICT (the CA server may be the secure server).
- **IP Filter List:** it is recommended that all IP traffic be filtered.
- **Filter Action:** it is recommended that source and destination addresses will identify the client and server respectively (this applies equally to the situation where the site Admin server is the client and the LSICT secure server is the server); source and destination ports will be the default of All Ports.

ICT Data Transfer systems within LSICT: IPSec

Authentication Encryption

The recommended method is Message Digest 5, due to compatibility with DFES secure sites (128-bit keying) and currently implemented protocols/software (e.g. Internet Explorer 6) as well as decreasing the network performance overhead incurred through the use of IPSec.

Packet Encryption

3DES is recommended: the Intel Pro 100S network cards installed in the Stone Admin servers are 3DES compliant.

Resource Requirements

1. The purchase of a server suited to handling heavy data transfer rates in a reliable manner and storing potentially large amounts of data in a secure environment. It is further recommended that, with a view to future-proofing (thereby ensuring a more effective return on investment), any such server be equipped with a 3DES compliant 100/1000Mb network card (e.g. Intel Pro 1000)
2. Windows 2000 requires the installation and configuration of Routing and Remote Access on the Windows 2000 Admin servers and associated LSICT servers to implement tunnel mode for IPSec.
3. 3DES Network cards will need to be implemented in all servers and client workstations: although various manufacturers supply compliant cards, best value considerations lead to the recommendation of the Intel Pro 100 S – this card is already installed in the Stone-sourced Admin servers and a large number of admin workstations.
4. It is recommended that LSICT implement the testing and evaluation of the current Beta/Release Candidate of Windows 2003 Server (available through Microsoft TechNet) to pre-empt any required amendments to IPSec policies that may be necessary upon introduction of this operating system, rather than to incur the administrative overhead of effecting changes on a live system at a later date.
5. It is further recommended that the initial client test site for trialling the IPSec implementation be one where the Internet connectivity is provided through ISDN rather than broadband, thereby enabling a better assessment of the impact upon network traffic in the currently predominant client environment.
6. Allocation of sufficient ICT Technical Support Assistant time to enable:
 - The effective implementation and testing of IPSec Policies, Rules and Filters,
 - The effective implementation and testing of associated Active Directory Group Policies, scripting and data transfer.
 - The effective implementation and testing of points 1 - 5 above.