netSurity Bridge

VERSATILE PRIVATE NETWORK

MANUAL AND CONFIGURATION GUIDE

Copyright

We do not warrant that the Software will meet your requirements or that its operation will be uninterrupted or error free. We exclude and expressly disclaim all express and implied warranties or conditions not stated in this notice (including without limitation, loss of profits, loss or corruption of data, business interruption or loss of contracts, any implied warranties of quality, merchantability, fitness for a particular purpose or ability to achieve a particular result), so far as such exclusion or disclaimer is permitted under the applicable law. The License Agreement does not affect your statutory rights. You assume the entire risk as to the quality and performance of the Software and the Materials. Should the Software or the Materials prove defective you (and not us or any licensed reseller) assume the entire costs of all necessary servicing, repair or correction.

Our liability to you for any losses shall not exceed the amount you originally paid for the Software during the Initial License Period and during the Permanent License Period, shall not exceed the amount of the License Fee.

In no event will we be liable to you for any indirect or consequential damages (excluding but not limited to any lost profits, lost savings, loss or corruption of data or loss of contracts) even if we have been advised of the possibility of such damages. In particular, we accept no liability for any programs or data made or stored with the Software nor for the costs of recovering or replacing such programs or data.

Nothing in this notice limits liability for fraudulent misrepresentation or our liability to you in the event of death or personal injury resulting from our negligence.

Issue Date: 07 July 2004
Version 1.5

netSurity Bridge Installation and Configuration Guide

1. Introduction

netSurity Bridge

What is netSurity Bridge?

netSurity Bridge is a versatile private network, designed to provide a precision encryption solution in order to secure communications.

Bridge is different from most VPN solutions, in that rather than encrypt the entire traffic between two points, Bridge allows for precision targeting of key services, and only applies encryption where it is needed, allowing the remainder of traffic to flow unimpeded.

Where can it be deployed?

netSurity Bridge can be deployed to protect TCP based network sessions – more information about deployment scenarios can be found in section 3 - configuration.

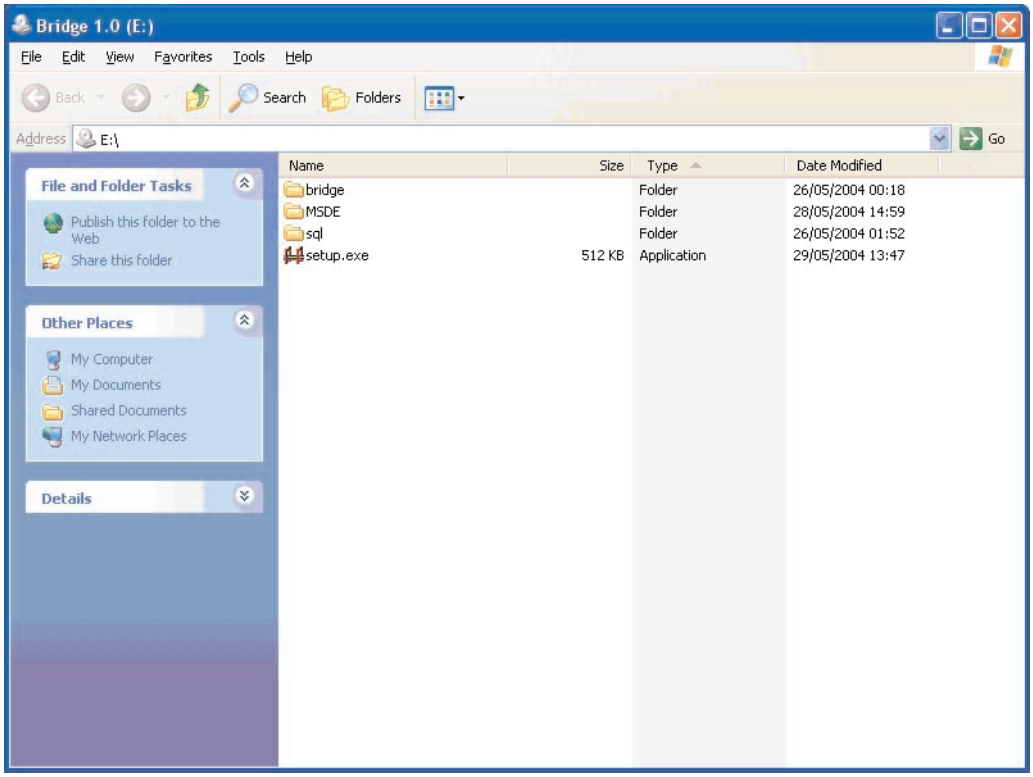
mailto: info@netSurity.com

2. Installation

Installing netSurity Bridge

The following steps are required to install netSurity Bridge.

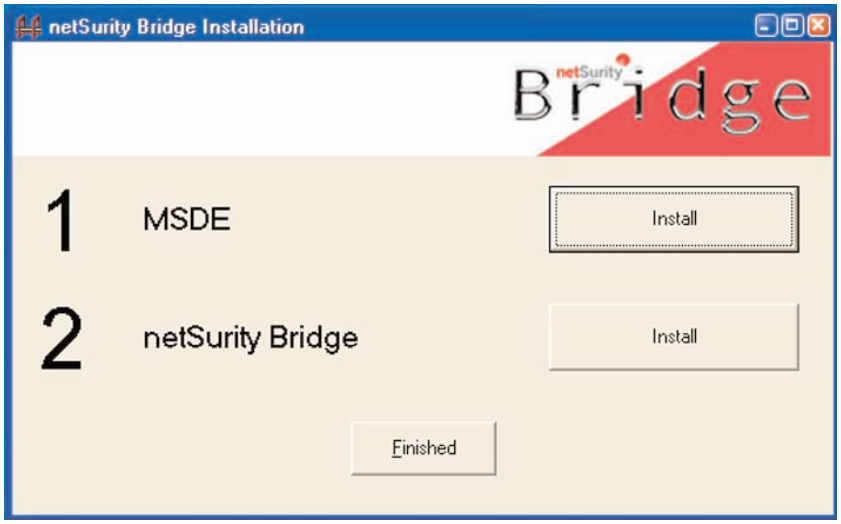
Open the netSurity Bridge CD and double click on the installer application setup.exe to launch it.



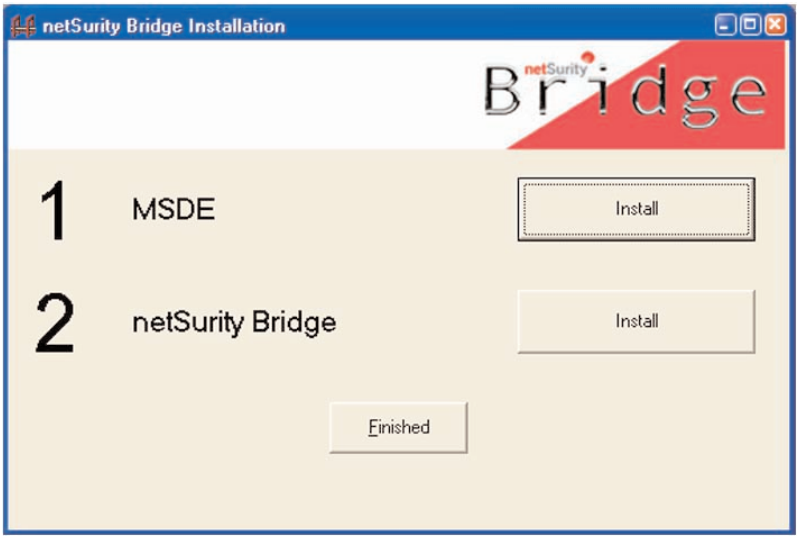
Once the setup application has started, it displays the available installation options.

mailto: info@netSurity.com

netSurity Bridge requires an instance of SQL 2000 or Microsoft SQL Desktop Edition (MSDE). If one of these options is not detected, then MSDE must be installed prior to installation netSurity Bridge setup, by clicking the MSDE Install Button.



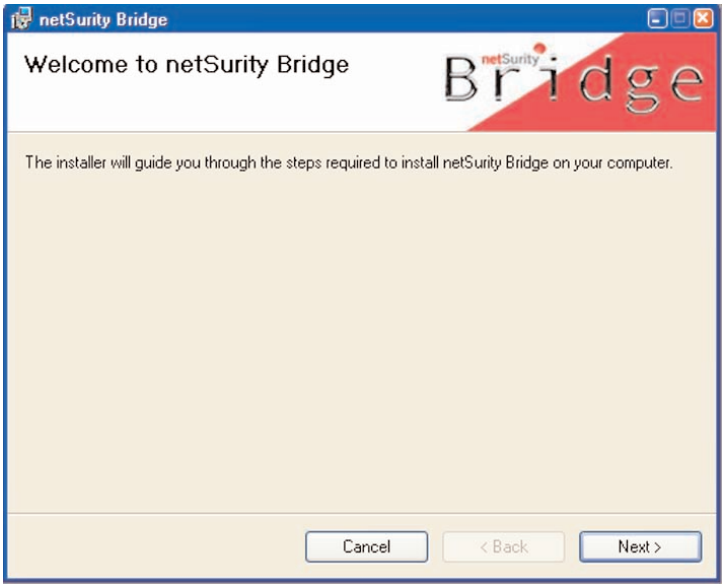
MSDE will automatically be installed. Following installation of MSDE or if an instance of SQL 2000 or MSDE is detected on the system then netSurity Bridge can be installed by clicking the Install Button.



The first part of the netSurity Bridge installation starts the database service and configures it ready for use by Bridge.

mailto: info@netSurity.com

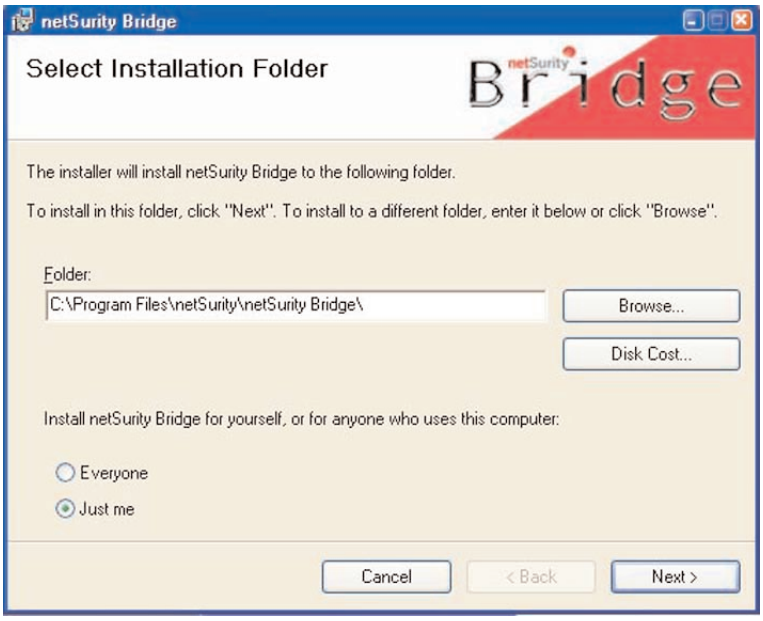
When the “Welcome to the Bridge Setup Wizard” is then displayed, select the next button to proceed.



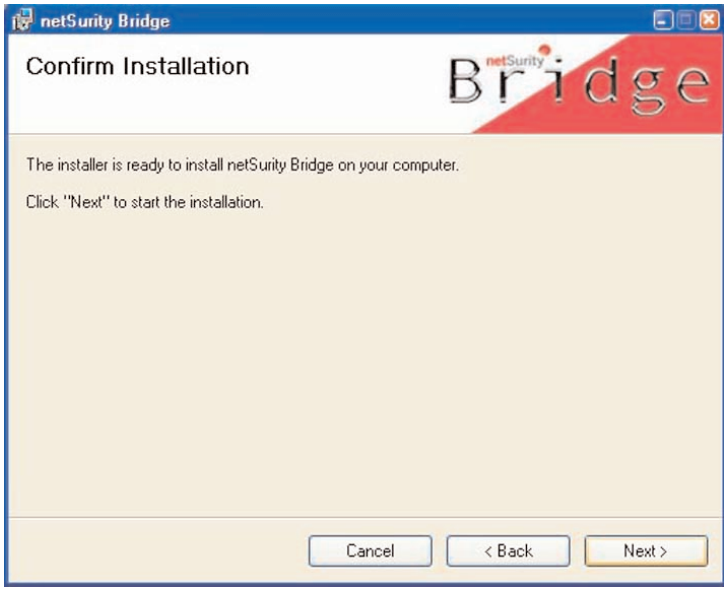
This will display the netSurity Bridge License agreement. You must accept the license to proceed.

Select the Installation Folder for netSurity Bridge and Click the Next Button.

mailto: info@netSurity.com

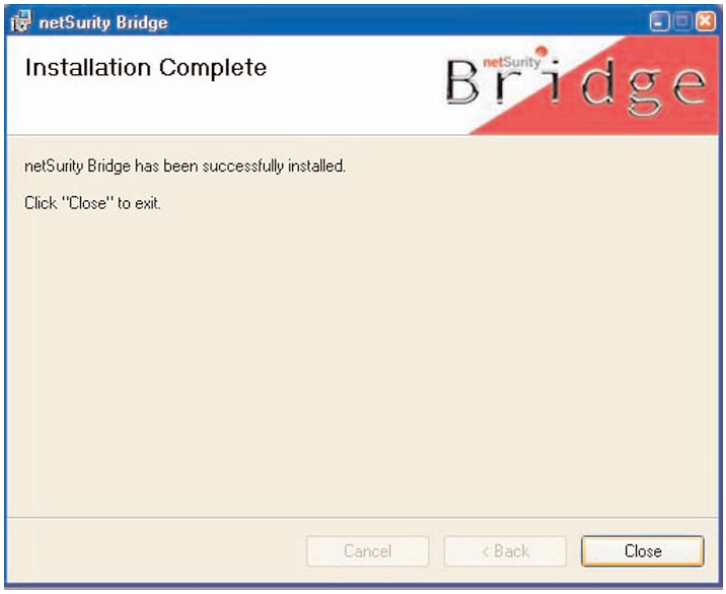


Click the Next Button once more to confirm the installation, and the setup of netSurity Bridge will proceed.

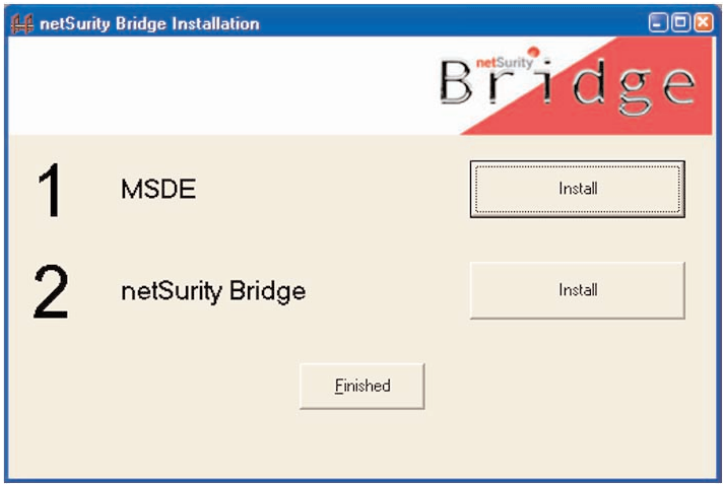


Bridge will now be installed onto your system, and the success dialog displayed.

mailto: info@netSurity.com



Click finish on the netSurity Bridge Installation wizard to complete the setup.



netSurity Bridge has now been successfully installed onto your system, and is ready to be licensed and configured.

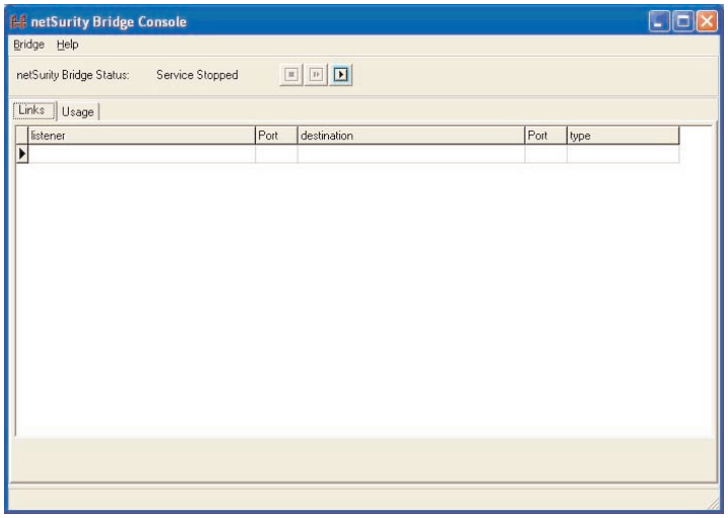
mailto: info@netSurity.com

Configuring netSurity Bridge

The Console Application

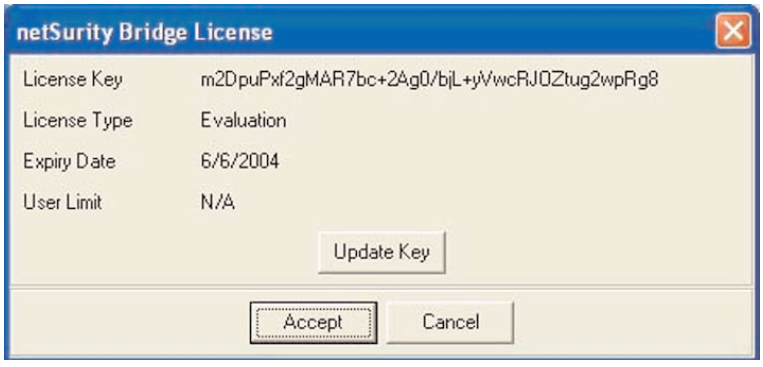
The console application is used to control the activation, licensing and configuration of netSurity Bridge, and to track the number of concurrent sessions managed.

The console can be launched using the menu item found on the start menu under the netSurity heading.



Licensing netSurity Bridge

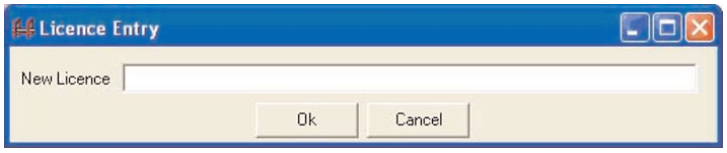
The license for netSurity Bridge is controlled using the Bridge Console. The license dialog is launched using the Manage License item of the Bridge menu.



The license dialog displays the currently active key, along with the type of license, its expiry date and the number of concurrent users allowed by it.

A new key can be entered by clicking the Update Key button, and typing or pasting in the new license key.

mailto: info@netSurity.com



If an invalid key is entered, the currently loaded key will be cleared.

The new key is accepted by clicking the Accept button – the cancel button will discard any changes made to the Bridge key.

To obtain a license email sales@netSurity.com or call 08700 433 748.

Links

netSurity Bridge stores the connections it makes between systems as Links, joining a listening address that accepts incoming connections to a destination address.

Links are made up of a listening address and port, a destination address and port, and the type of connection being made.

There are a number of connection types currently available within Bridge as follows:

Code	Type	Usage
N	Clear Text	All traffic travelling over this link is unencrypted. Does not require a second link to decrypt traffic.
X	Low Encryption	All traffic travelling over this link is encrypted using a non-cryptographically significant link Requires use of a second link to decrypt traffic using an identical connection type.
C	RC4 Client	All Traffic travelling over this link is encrypted using RC4 and RSA asymmetric keys. Requires a matching RC4 Server to decrypt the traffic.
S	RC4 Server	All traffic travelling over this link is decrypted from RC4 and RSA asymmetric keys. Can only accept and decrypt traffic from a linked server employing RC4 Client.

Details of the RC4 Client / Server cryptography can be found in the appendices.

mailto: info@netSurity.com

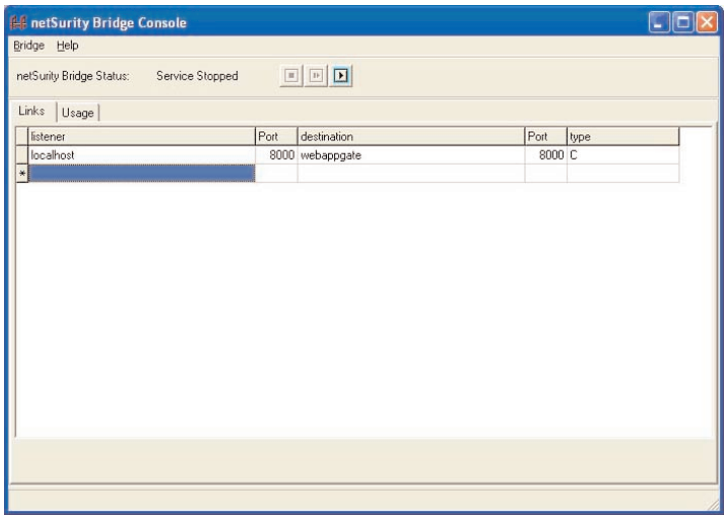
Managing Links

Links are updated using the Links tab in the main Console window.

Link information can be freely typed into the grid structure, and navigated using the cursor and tab keys. Individual cells can be updated by selecting them and entering new information.

Rows can be deleted from the links tab by selecting a row and pressing control and delete.

A new row is automatically added by scrolling to the bottom of the list and pressing the cursor down key to move to the next row. (This only works if the last row is populated).

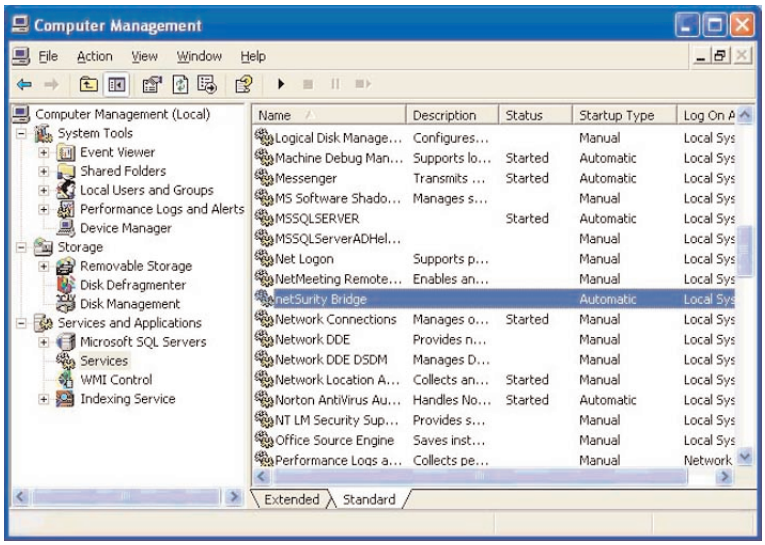


Starting and Stopping netSurity Bridge

netSurity Bridge operates as a Windows Service, and needs to be started before it can function.

netSurity Bridge can be started and stopped within the Console, using the buttons in the top panel, next to the service status notification.

Alternatively, netSurity Bridge can be managed using the Services element of the Windows Computer Management tool.



Changes can be made to netSurity Bridge while it is running, however they will not take effect until the service has been stopped and restarted.

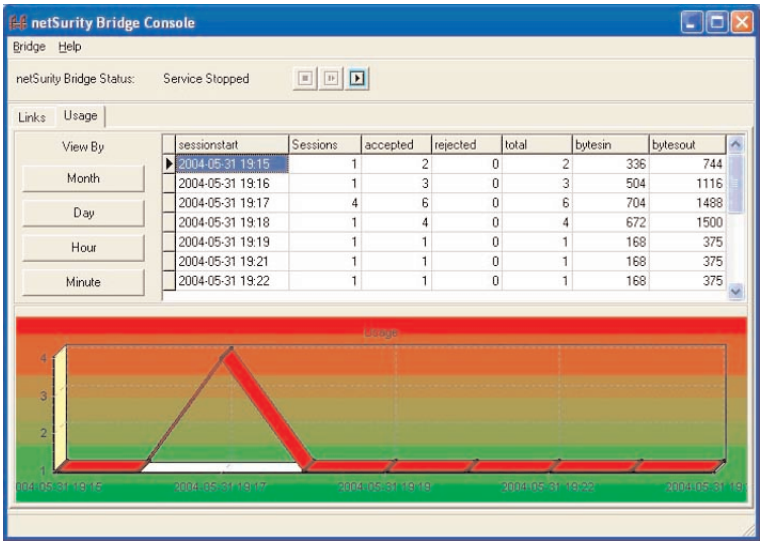
mailto: info@netSurity.com

Monitoring Usage

netSurity Bridge tracks each of the sessions made to it, allowing monitoring and management of the service it provides.

This information is stored in the attached database, and can be accessed graphically with the Usage tab of the Console.

This allows the information to be displayed by a variety of time periods, to assess periods of peak and ongoing usage, by month, day, hour and minute.



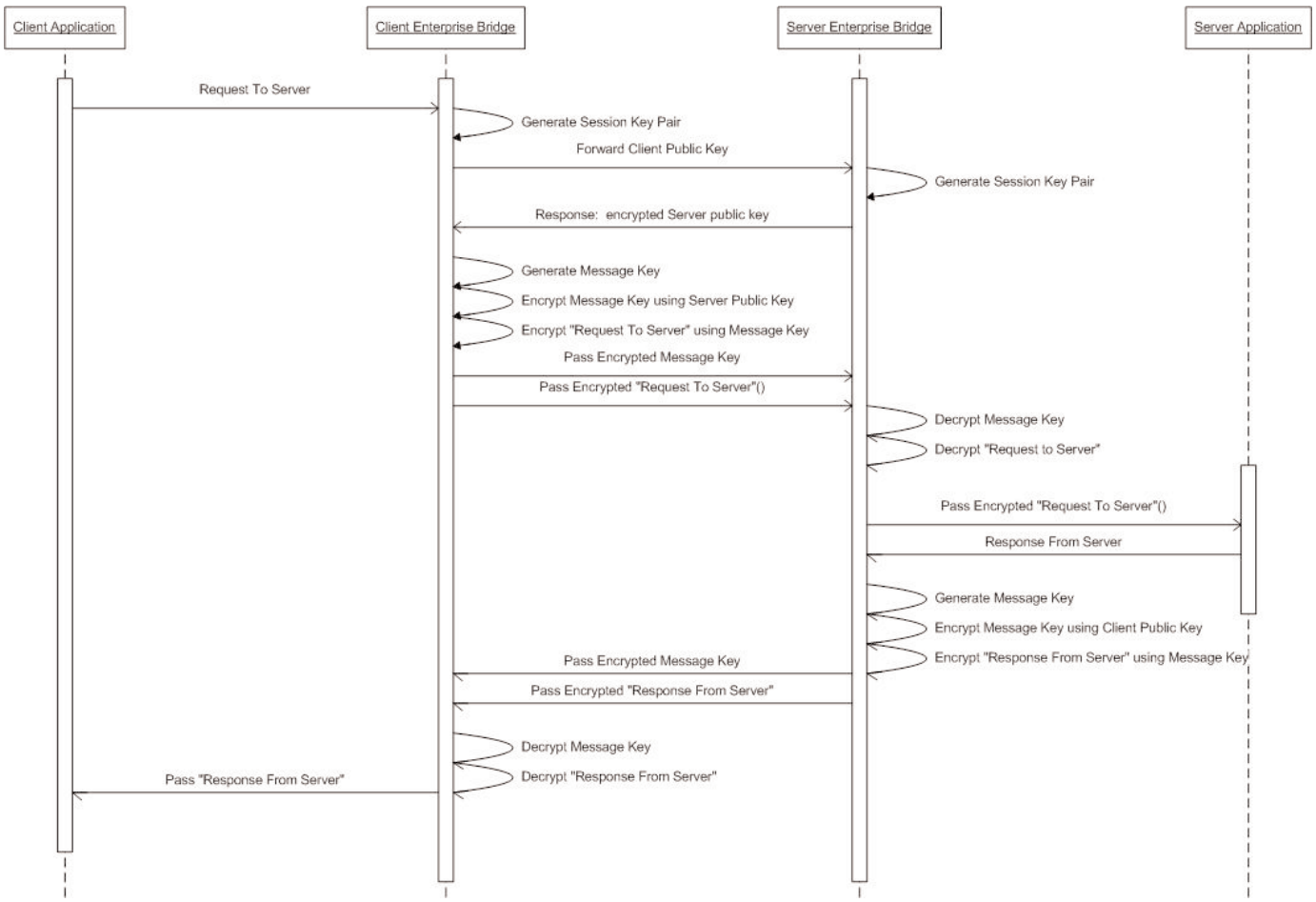
netSurity Bridge will log events in the Windows Event Log when 95% of the license limit is reached, and in the event of a session being rejected when too many sessions are being used.

mailto: info@netSurity.com

Appendix A – Encryption Model

netSurity Bridge uses a combination of RSA PKI and RC4 streaming encryption to ensure that messages passed between the client and server instances of Enterprise Bridge are protected.

The diagram below highlights the key elements of the end-to-end process of communication between a Bridge client and server.



mailto: info@netSurity.com

netSurity Bridge

Configuration guide

NETSURITY BRIDGE - CONFIGURATION GUIDE

Overview

This section describes some of the most common uses of netSurity Bridge, and provides sample configurations that can be adapted for use in your own solutions.

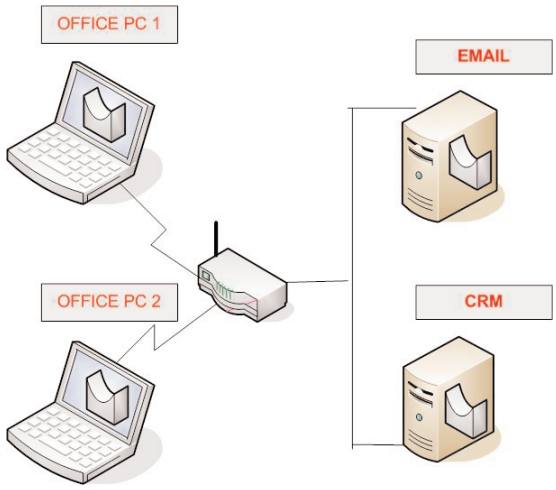
Client-Server Solutions

Client-Server solutions are used to provide privacy locally from one machine to another, thereby removing the risk of protected traffic being intercepted and read during communication over the local network.

Where to deploy

Client-Server based solutions are ideal for:

- Remote Access (RAS, VPN) to secured services.
- Internal Access to sensitive resources.
- Wireless LANs



Example Deployment – Remote Access

SpeedyCo would like their travelling sales force to be able to gain access to their company networks in order to send and receive email and access their Customer Relationship Management (CRM) system. As each individual sales person makes their own arrangements for accessing the internet, SpeedyCo needs a simple solution to ensure that all email communication and access to the company CRM system are protected from disclosure over the Internet.

netSurity Bridge is installed on each salesperson's laptop and behind SpeedyCo's firewall. Each laptop is configured to send and encrypt e-mail and access to the CRM system via the internal Bridge. The internal Bridge decrypts the data and forwards to the mail and CRM server.

On each laptop, the mail program e.g. Microsoft Outlook is re-configured to connect to the local computer i.e. SMTP port 25 to localhost and POP3 port 110 to localhost. A desktop shortcut to the CRM application is created as http://localhost:8080. Using the netSurity Bridge console application on the laptop, netSurity Bridge is now configured to receive the SMPT, POP3 and CRM HTTP connections, encrypt using RC4 and forward to the internal Bridge Server which has been given a URL of "bridge.speedyco.com". Note that each service to be forwarded must be given a destination port as well as address. This will be the port set up on the internal Bridge server to receive inbound connections.

mailto: info@netSurity.com

Laptop Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
Localhost	25	bridge.speedyco.com	8025	C
Localhost	110	bridge.speedyco.com	8110	C
Localhost	8080	bridge.speedyco.com	8080	C

The internal Bridge Server must now be configured to receive inbound connections, to decrypt the RC4 and forward to the destination host.

Internal Bridge Server Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
bridge.speedyco.com	8025	Mailserver	25	S
bridge.speedyco.com	8110	Mailserver	110	S
bridge.speedyco.com	8080	CRM Server	80	S

Now when the laptops connect to e-mail and the CRM server this traffic will be encrypted and protected whatever connection mode, e.g. dial, broadband or wireless access is used.

mailto: info@netSurity.com

Example Deployment – Access to Sensitive Information

SpeedyCo has provided all its line managers with access to the company HR system in order to access and manage information about the staff they are responsible for. SpeedyCo does not want to invest in complex PKI solutions or have to manage certificates on the HR system, but wishes to ensure that sensitive information is not transferred over the company networks in clear text.

netSurity Bridge is installed locally onto each line managers desktop and also onto the HR Server. The HR Application is on a server called HRServer, with a domain name hrserver.speedyco.com and the application listens on port 1433.

netSurity Bridge is configured on each desktop to intercept connections to the HR System, encrypt using RC4 and forward to the HR Server. On the HR Server, netSurity Bridge is configured to listen for incoming encrypted connections, decrypt the RC4 and forward to the application on port 1443.

Desktop Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
Localhost	1433	hrserver.speedyco.com	8443	C

Server Configuration

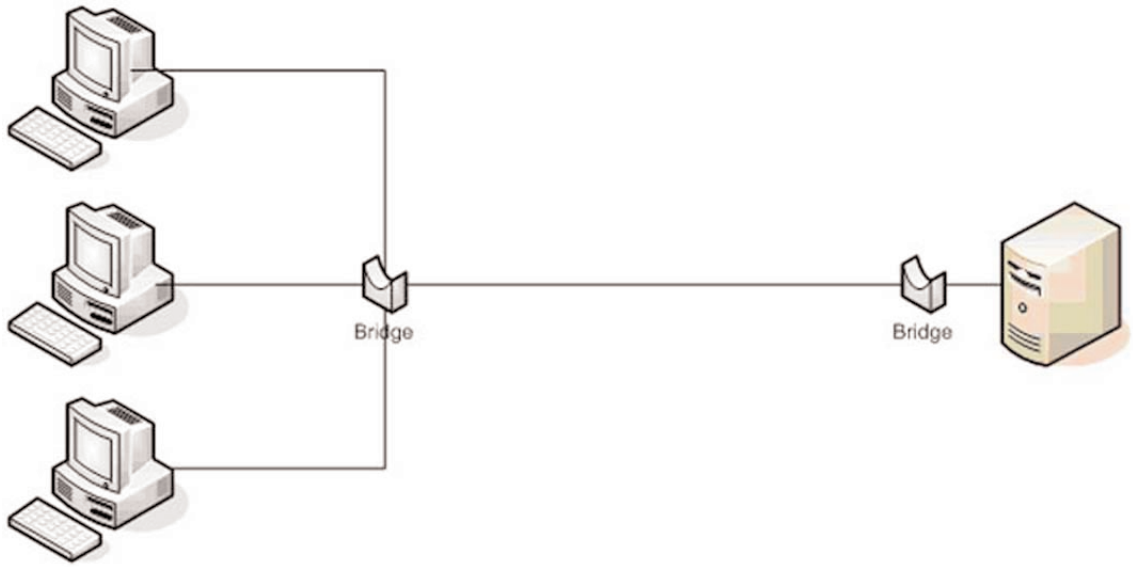
LISTENER	PORT	DESTINATION	PORT	TYPE
HRServer	8443	Localhost	1433	S

mailto: info@netSurity.com

Point to Point Security

Point to Point solutions are used when netSurity Bridge is used by a cluster of machines to connect to another, with all traffic transferred between bridge instances being protected, while internal traffic is unimpeded.

Solution



Where to deploy

Secure Access solutions are ideal for:

* Remote Office (RAS, VPN) to secured services by satellite offices.
* Internal Access to high security resources by group (e.g. Finance and HR Systems).

mailto: info@netSurity.com

Example Deployment – Remote Office Access

SpeedyCo has opened a new office for a small team of product developers, and needs to allow staff working in this office to access services on the main corporate network. It is important that connections to the remote office are secure, however internal traffic can remain unencrypted as it never leaves the site.

To facilitate this, a secure "bridge" is created between the remote office and the central site. A Bridge server is installed in the remote site and another Bridge Server is installed at the central site.

Machines used in the remote office itself, will reference the bridge server as though it were providing the remote services locally. In the example below, the remote office Bridge Server is called OfficeLink and the main office Bridge Server is called CentralLink and the "Bridge" is configured to encrypt e-mail and http traffic.

Remote Office Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
Officelink	25	Centrallink	25	C
Officelink	110	Centrallink	110	C
Officelink	80	Centrallink	80	C

Central Office Configuration

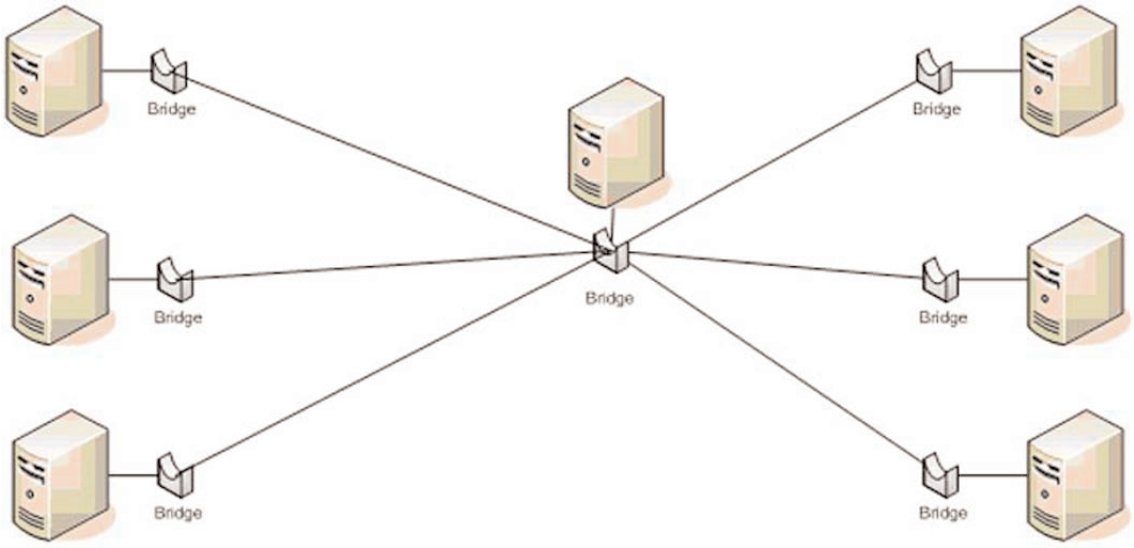
LISTENER	PORT	DESTINATION	PORT	TYPE
Centrallink	25	Mailserver	25	S
Centrallink	110	Mailserver	110	S
Centrallink	80	Portalserver	80	S

mailto: info@netSurity.com

Peer to Peer Solutions

netSurity Bridge can be used to allow secure communication between servers, Bridge either being installed onto each server for strict control of network traffic, or it can provide shared access between servers.

Solution



Where to deploy

Peer to Peer solutions are ideal for:

- Meta Directory and other data synchronisation systems
- Secured access to sensitive information
- Distributed Applications

mailto: info@netSurity.com

Example Deployment – Meta Directory

SpeedyCo uses a Meta directory to manage Active Directory based user and Email accounts, along with managing a PABX to assign and track telephone numbers.

In order to ensure that sensitive information about staff and user accounts are not transferred in clear text, netSurity Bridge is used to secure communication between each of the key servers.

Bridge is installed directly onto the HR machine, an Active Directory Domain Controller, the PABX and the Meta directory itself. The Meta directory server is configured to reference connecting systems via bridge rather than directly and each connecting system is configured to reference the Meta directory via its locally installed Bridge.

Meta Directory Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
Localhost	1433	HRServer	8433	C
Localhost	1389	ADServer	8389	C
Localhost	1434	PABXServer	8433	C

HR Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
HRServer	8433	Localhost	1433	S

Active Directory Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
ADServer	8389	Localhost	389	S

PABX Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
PABXServer	8433	Localhost	1433	S

mailto: info@netSurity.com

Example Deployment – Distributed Application

SpeedyCo's Finance system is a web based application that connects to the main accounts system hosted on another machine. While access to the Finance front end is controlled using Bridge, there is also a need to ensure that information transferred between the two servers is also secured.

Bridge is installed directly onto the server hosting the finance application, and also directly on the accounts server. Each Bridge installation is configured to secure communications between them.

Finance Server Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
Localhost	1433	AccountsServer	8433	C

Accounts Server Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
AccountsServer	8433	Localhost	1433	S

mailto: info@netSurity.com

Bridging Firewalls

netSurity Bridge can be used to join networks through firewalls, allowing them to communicate securely regardless of the choice of vendor and product used in firewall selection.

Solution

Where to deploy

Bridging Firewall solutions are ideal for:

- Linking organisations and groups network infrastructure

Example Deployment – Bridging Firewalls

SpeedyCo has recently purchased a Spanish competitor, Rapido.SP and now needs to link the two company's networks. Rapido.SP has been using a different brand and type of firewall, and there is no common link between SpeedyCo's existing firewall infrastructure and that of Rapido.SP.

In order to allow the two companies to access each others networks, Bridge is installed onto gateways in each network, inside the DMZ and the firewalls are configured to allow access on selected, bridged, network ports.

Each company can now access their local gateway server, in order to utilise the corresponding service in the other companies network.

SpeedyCo Gateway Server Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
InternalHome	80	gateway.rapido.sp	80	C
ExternalHome	80	PortalServer (SpeedyCO)	80	S

Rapido.SP Gateway Server Configuration

LISTENER	PORT	DESTINATION	PORT	TYPE
InternalHome	80	gateway.speedyco.com	80	C
ExternalHome	80	PortalServer (Rapido.SP)	80	S

mailto: info@netSurity.com