netSurity Bridge - Frequently Asked Questions

General

What is netSurity Bridge?

netSurity Bridge is a security tool that allows you to protect network traffic from eavesdroppers attempting to acquire sensitive information by listening on open and insecure networks. It can be deployed in Point to Point, Peer to Peer or Client Server solutions.

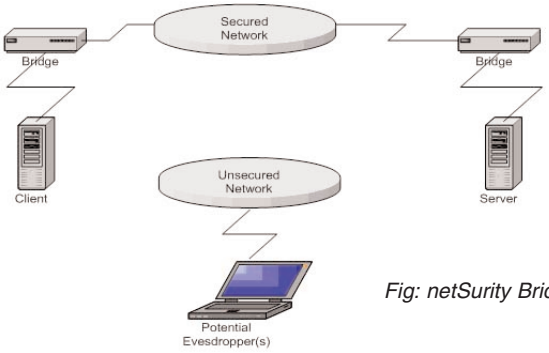


Fig: netSurity Bridge Overview

Where can netSurity Bridge be used?

netSurity Bridge can be used to protect networks where there are well defined client server, point to point or peer-to-peer relationships between systems and there are known network addresses that can be used to access these systems.

netSurity Bridge is provided as a Windows Service, and therefore needs to be installed onto an NT based platform (running Windows NT 4 service pack 6, Windows 2000 or Windows XP professional).

netSurity Bridge requires SQL Server 200 or Microsoft SQL Desktop Edit (MSDE) to be installed in order to monitor configuration, usage and license data. MSDE is provided with netSurity Bridge.

How does netSurity Bridge work?

netSurity Bridge maintains a list of 'connectors' (a pair of network addresses to hold a source and destination address along with a security model) which tell it to listen on a series of selected network addresses, and as network connections are made to monitored addresses, netSurity Bridge forwards anything it receives to the selected target. Once a session has been established, the server is able to reply via the netSurity Bridge mechanism, creating a two way secure communication channel.

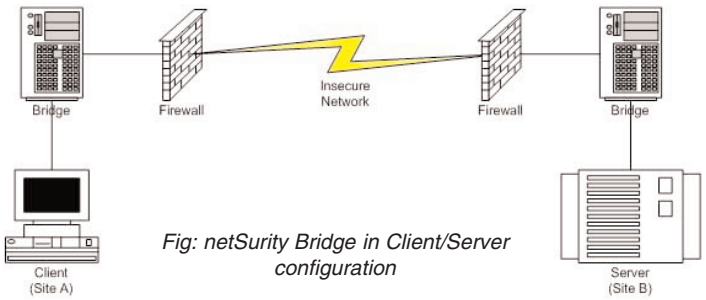


Fig: netSurity Bridge in Client/Server configuration

*For example, for Company B to make one of its internal intranet servers available to Company A, it installs netSurity Bridge at both locations. Site A is configured to connect **server.sitea.com** to **eb.siteb.com**, while Site B is configured to connect **eb.siteb.com** to **server.sitea.com.** Clients at Company A are set up so they treat server.sitea.com as though it were server.siteb.com, and as they make requests of the server they are encrypted at site a, transmitted over the internet, decrypted at site b and then passed on to the actual server.*

mailto: info@netSurity.com

What kind of network traffic can netSurity Bridge protect?

netSurity Bridge protects TCP network traffic where there are known, fixed points on the network infrastructure where netSurity Bridge can be installed. This makes it ideal for protecting client-server, point to point and peer-to-peer network sessions where at least one half (the receiving instance of netSurity Bridge) has a fixed network address.

netSurity Bridge has been developed with particular reference to synchronisation tools such as Meta Directory and Microsoft's active directory connector - however it has also proven to be successful in securing other forms of network services such as web servers, e-mail, and VoIP, and there are no reasons why other forms of TCP based network services can not be protected.

What is 'Zero Maintenance'?

netSurity Bridge is 'Zero Maintenance' in that once it has been installed and configured, then no further user operation is required for its ongoing operation, and it does not require a supporting infrastructure to be made available to ensure its availability.

This is in contrast to many other cryptography based solutions that require certificate authorities, directory services and key management.

How is netSurity Bridge 'Transparent'?

netSurity Bridge doesn't make any requirements on the services it enables other than they are configured to communicate via netSurity Bridge.

In the example here, the Site A Client would be reconfigured in order to communicate with the local netSurity Bridge, rather than with the Site B Server directly. As far as both the client and server are concerned, nothing other than the address used for communication has changed, and both applications are unaware that their exchanges are now secured.

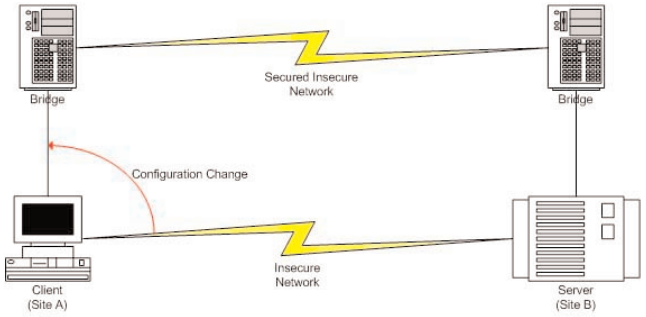


Fig: Client changeover from insecure to secure connection.

SECURITY

What are the 'Security Models'?

netSurity Bridge makes a number of security models available, two of which combine to provide a strong cryptographic protection for bridging insecure networks.

These can be briefly summarised as:

- Clear Text

  Clear Text security provides no cryptographic protection, but does allow network resources to be referenced via the netSurity Bridge rather than directly, and does not require a second instance of netSurity Bridge.

- Low Security or Simple Encryption

  Low Security provides a very simple exclusive or protection for network traffic, and is not recommended for use in live environments. This requires a second instance of netSurity Bridge to decrypt protected network traffic.

mailto: info@netSurity.com

- RC4 Client

  The RC4 Client provides strong encryption using RSA PKI to generate a session based public / private key pair for exchange of individual message keys used by the RC4 streaming algorithm. This security model requires a second instance of netSurity Bridge, using the RC4 Server security model to decrypt protected network traffic.

- RC4 Server

  The RC4 Server provides strong encryption using RSA PKI to generate session based public / private key pairs for exchange of message keys. This security model requires a second instance of netSurity Bridge, using the RC4 Client security model to provide encrypted network traffic.

How are the cryptographic keys used?

Cryptographic keys are kept as volatile as possible, and copies are not kept by netSurity Bridge.

PKI key pairs are created whenever a new session begins, and are destroyed at the end of the session.

Message keys are created for each individual piece of network traffic forwarded between bridges (keys are exchanged using the PKI key pairs), and are discarded after a single use.

Why use RC4 encryption? (Why don't you use DES or AES or ---)

Speed - the RC4 algorithm was selected in order to provide a fast overall process for encryption and decryption, while providing strong and reliable encryption. DES (and its variants), AES and the other potential candidates remain good and reliable tools, however given that netSurity Bridge is protecting a real time environment it was decided that performance was a strong priority providing the overall protection offered was not compromised.

But I need DES (or AES, or ---)

It is understandable that certain environments - particularly those with well defined security protocols will have definite cryptographic requirements.

In these situations, netSurity can offer a bespoke security model as a professional service, and can make dedicated versions of netSurity Bridge available.

If you are interested in pursuing a bespoke netSurity Bridge, please contact us to arrange a consultation to discuss your requirements.

Can netSurity Bridge be combined with other forms of security?

netSurity Bridge is designed to be as transparent as possible, and should work with no problem with additional security systems - you can even stack multiple instances of netSurity Bridge - it is that compatible.

We would also strongly recommend use of firewall and IDS if you're planning to connect your systems to external networks and netSurity Bridge works fine with both of these technologies.

NETSURITY BRIDGE

How do I use netSurity Bridge?

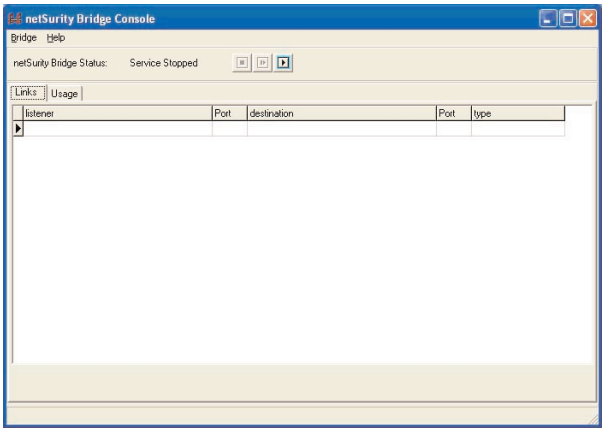
Once netSurity Bridge has been installed, it is provided with an administration tool used to create and manage the netSurity Bridge configuration, and control the operation of the actual bridge software.

mailto: info@netSurity.com

The netSurity Bridge itself operates under a 'zero maintenance' design and normally runs as a windows service and does not need to be employed directly by users.

There is an option to run the service in console mode, which allows an operator to see immediately what the netSurity Bridge application is doing.

How do I configure netSurity Bridge



The netSurity Bridge Administrator is used to create and manage the configuration, and to control the netSurity Bridge service.

To create a new connector, you will need to know the source and destination addresses (including port numbers), and the type of connector being implemented (clear text, low security, RC4 client, or RC4 server).

Note, netSurity Bridge is provided with a comprehensive configuration guide describes most scenarios that you are likely to need.

Fig: netSurity Bridge Administrator (configuration for Example Site A)

Monitoring netSurity Bridge?

netSurity Bridge facilitates monitoring of its activity by recording information into the windows event log. This makes it available not only to operators, but automated monitoring tools, such as Tivoli.

What about internal threats?

When deploying netSurity Bridge to protect data trascending external networks, it is easy to identfy the risks and boundaries than need to be secured. It is easy to forget however that internal networks can be more at risk. Access to sensitive data can be obtained by unauthorised users who have a privilidged access rights to networks.

netSurity Bridge is designed to operate across both internal and external networks. When deploying netSurity Bridge into internal networks, you can ensure that sensitive data is passed safely between systems or bertween clients and servers.

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.

mailto: info@netSurity.com

SUPPORT

Is Training Available?

netSurity Bridge is intended to be simple enough to use that no training is required.

What about support?

Support is available from support@netSurity.com.

If this does not resolve your issues, then netSurity offer a range of support packages ranging from simple email support up to more substantial support arrangements.

How about consultancy?

Consultancy is available to solve a wide range of security issues and to help you get the most from netSurity Bridge - please contact us through info@netSurity.com to discuss your requirements.

LICENSING

How is Bridge Licensed?

Bridge is licensed by concurrent connections, allowing you to scale deployments to suit your needs. On average, we have found that only about 40% of users will actually be using Bridge at any point in time, allowing you to provide for large numbers of potential users without the need to purchase licenses for all of them.

Bridge ships complete with a 30 day 'discovery' key, that allows unlimited usage in order to ensure that you can get a realistic measure of how many licenses you will need, rather than forcing you to purchase licenses speculatively.

After 30 days you should apply for a full license for the number of concurrent connections by emailing sales@netSurity.com or phoning 08700 433 748.

How much does Bridge Cost?

Bridge is priced competitively, based on the number of concurrent users at Bridge server. For a quote, please contact us at sales@netsurity.com or call on +44 8700 433 748.

What other licensing options are there?

As well as our volume licensing, netSurity Bridge is available with an unlimited 'enterprise mode' that allows any number of concurrent users through a selected bridge.

We are happy to discuss enterprise wide license options, allowing you to deploy as many copies and licenses of Bridge within your enterprise as you need without incurring further costs.

Alternatively, apply for access to our 'Diamond Customer Programme' for early editions of all netSurity products, discounted prices and reseller agreements.

mailto: info@netSurity.com