

Linktivity Security

Deploying a Linktivity Collaboration Solution in a Secure Network Environment

Many customers, attracted to the convenience and flexibility that the Linktivity solutions offer, have questions about how using WebDemo and WebInteractive might expose their corporate networks to security risks. In this document we'll explain how Web servers communicate across a network and what risks are associated with those communications. We will overview the differences between the Totally Secure Communications, and Secure Communications networks as well the Linktivity Server and dynamic clients security.

A **firewall** is a set of related software programs, or a hardware device, that protects the resources of a private network from users from other networks. A firewall, working closely with a router program, examines each network data packet to determine whether to forward it to its destination. A firewall is often installed on a specially designated computer to prevent any incoming request from going directly at private network resources.

A **port** is a "logical connection place" that corresponds to a particular server program on a computer in a network.

Applications that use TCP/IP such as http, the Hypertext Transfer Protocol, have ports with pre-assigned numbers. Other application processes are given port numbers dynamically for each connection. When a server program or "service" is started, it is said to bind to its designated port number. Any client program that wants to use that server must also request to bind to the same port number.

Port numbers range from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged services. For the HTTP service, port 80 is defined as a default.

As you'll discover, the nature of the Linktivity solutions and the Linktivity Server is such that neither the Web server nor applications running on it are made vulnerable to outside incursion. More specifically, because WebDemo and WebInteractive have very limited access to the resources of the server where they reside, they do not provide intruders with an opportunity to gain deeper access to your network.

SSL and 128-Bit Encryption

Linktivity relies on industry standard SSL and HTTPS for the encryption of "front-end" transactions, such as user logins and management functions, registrations, scheduling, and other similar transactions. The Linktivity Web Meeting can be fully secured using server certificates and SSL, making all of your Web conferencing and business collaboration data totally secure. In addition, Linktivity provides two other layers of security. First, there is the 128-bit dynamic encryption on the fly for all meetings, which delivers the highest level of protection required for enterprise data communications. Secondly, all meeting have the capability to lock out anyone (close the door after the meeting has started) from joining the meetings.

The Totally Secure Network

Let's start by looking at a scenario in which a security-conscious company has protected their network to provide maximum network protection. Our security-conscious company has decided to eliminate any possibility of intrusion from an outsider into their network by setting up a network firewall and configuring it to block access to all ports on their network (incoming and outgoing) except for certain ports. In this case the security department may have it setup so that internal users can go out port 80 (for Web browser traffic) only and that only return traffic from port 80 is allowed back in. This means that only traffic that was requested from an internal user is allowed back into the network but the internal users could only go to services running on port 80. From a security standpoint, this is a secure network. However, there are some issues with this setup. The first is that users may try to find ways around the security rules to allow them to do work related tasks. The goal of security is to secure the network without causing undo hardship to the

users. If a department sets the rules too secure they may actually hurt the security of the network. The second issue is that only allowing traffic out/in certain ports requires more time from the IS department to add or remove ports as business needs dictate.

Even though this scenario is secure from a communications standpoint, this highly secure scenario is not ideal. In the case of a Web server setup behind this corporate firewall, internal employees can use it to surf the web, but no one outside of the network (including employees with laptop PCs) may have access. A Web server hosting a corporate web site would be able to provide content to internal employees (over an Intranet), but no Internet access to the site would be allowed.

Let's look at a more common security setup. In this case, our security-conscious company has decided to make rules that allow users on the inside of the firewall to initiate connections to the outside world and get information back through the connection they have initiated.

Again, even though this is still considered secure (and is commonly used) it does have limitations.

If a user receives a Trojan horse or back door type program from some other means (e.g. an email attachment), this back door type program can initiate a connection to a predetermined server and receive instructions. At this point, the machine with the back door is compromised and can be used to compromise more machines on the local network or be used in some type of Internet attack. This is why you should also have anti virus software on your corporate machines.

In addition to the added security risk, if our security conscious company wants to setup a Web server on the local network, they still have the problem of having only the internal users access the Web server. Users outside of the company network will not have access to this Web server.

The Communications Network

Let's take our scenario one step further and assume that our high-security company wants to put up a corporate Web page for the world to see. The scenarios described above are now unacceptable because no one from the outside world can connect to the Web server.

Let's assume our security conscious company has decided to open a 'hole' in the firewall in order for people from the outside world to be able to get to the Web site. The company will now have an open 'hole' or port in the firewall. For Web servers, this is typically port 80. So, the company tells the firewall that it is O.K. to allow incoming requests to port 80 to go to the Web server.

Let's pause and look more closely at this scenario before the point at which the company has set up Web service on the exposed machine. The company

has a working TCP/IP network operating behind a firewall. Port 80 is open on the firewall to a single machine. That machine is currently not running. So, at this point, the company is not worried. There is *no* security risk. Why? Because there is nothing listening to port 80. TCP/IP is a protocol for communication. Like all forms of communication, data communication requires a speaker, and a listener.

Now, let's move on to the point at which the company installs a Web server. To extend our metaphor, this is the equivalent of plugging in your telephone. Now people are able to connect to something on port 80, and something will happen. At this point you must worry about security.

The Secure Communications Network

Now, let's go back to our security-conscious company. They have hired a security agent. This agent has completely locked down the Web server, patched the operating system it runs on, and cleaned out any programs that may allow remote users to break into the machine. Now the company can safely show their Web pages in the knowledge that the Web server is no longer a security risk. Or is it? As it sits, there is the possibility of a security breach. There is a 'hole' in the firewall to allow traffic from the outside world into the Web server. That traffic isn't the security problem. The problem is if a new exploit in the operating system is found that allows someone to "take control" of the system. Once something has control of this server (or the server is compromised somehow) the server can be used to attack the rest of the machines on the local network. This is because the Web server is on the same local network.

The better solution is to use a DMZ. A DMZ is an area on the network that isn't quite on the Internet but isn't on the local network. This allows people from the outside world to access machines on the DMZ, which are behind the corporate firewall, but machines on the DMZ cannot get to any machines on the local network. This means local users can access the Web server that is on the DMZ, and users on the Internet can access the Web server that is on the DMZ, but if the Web server were to be compromised, it would not be able to affect machines on the local internal network since it is on the DMZ.

Using a DMZ for your Web server is similar to having your server on the Internet, but at your ISP's location, except the machine is at your own location.

Now our company really likes their Web server, which is installed on the DMZ of their network, and certainly sees the value in it. They also hear about a new product called Linktivity, and feel that, combined with their Web services this will give them a real competitive advantage.

Now, let's look at the security issues. The security problems with our Web server originated from the fact that our Web server was on the local network. With the Web server on the DMZ or at the ISP's location, the Web server won't affect your local network. Web Servers do get attacked, and most

attacks are centered on known issues with the operating system or a sub component of the operating system. This is done because if they can hack into the operating system through a program that is a System service, they now have System level access. Once you have system level access to the system, you can do virtually any thing you want.

Let's now look at what adding the Linktivity Server to your system adds.

The answer, in terms of system access, is very little. The Linktivity Server is limited to the following functions:

1. Linktivity ConnectionPoint *talks to a single, predetermined database*. Linktivity ConnectionPoint's ability to talk to its database is limited to predetermined read and writes operations. ***There is no way to manipulate the Linktivity ConnectionPoint to delete or examine anything other than specific Linktivity ConnectionPoint data.*** Manipulation of Linktivity-specific data by the Linktivity ConnectionPoint itself is limited. For example, Linktivity ConnectionPoint offers no user interface and does not have the capability to do anything other than the few predetermined tasks that have been assigned it.
2. Linktivity **Server talks to other people who have called it**. The key point here is that you or a user *must* call the Linktivity ConnectionPoint. The Linktivity ConnectionPoint *cannot* establish connections to other machines or networks. It can only talk to people who have requested a connection to it.
3. The Web site portion of the Linktivity Server is a Web site that adheres to all of the security protocols setup on the Web server.

The Linktivity ConnectionPoint cannot access, view or manipulate any other device in your network. It can only manage its internal database. The internal database is used to keep track of Linktivity specific information such as who called, when they called, and which conference they joined.

Let's return to our security-conscious company. They have now installed WebDemo or WebInteractive. They can now safely ignore it. The Linktivity Server cannot access the network or launch other programs on the server. From a security standpoint, it really cannot do much at all.

To put to rest any final anxieties about someone accessing the Linktivity Server through an open port, let's review the components of the Linktivity solution.

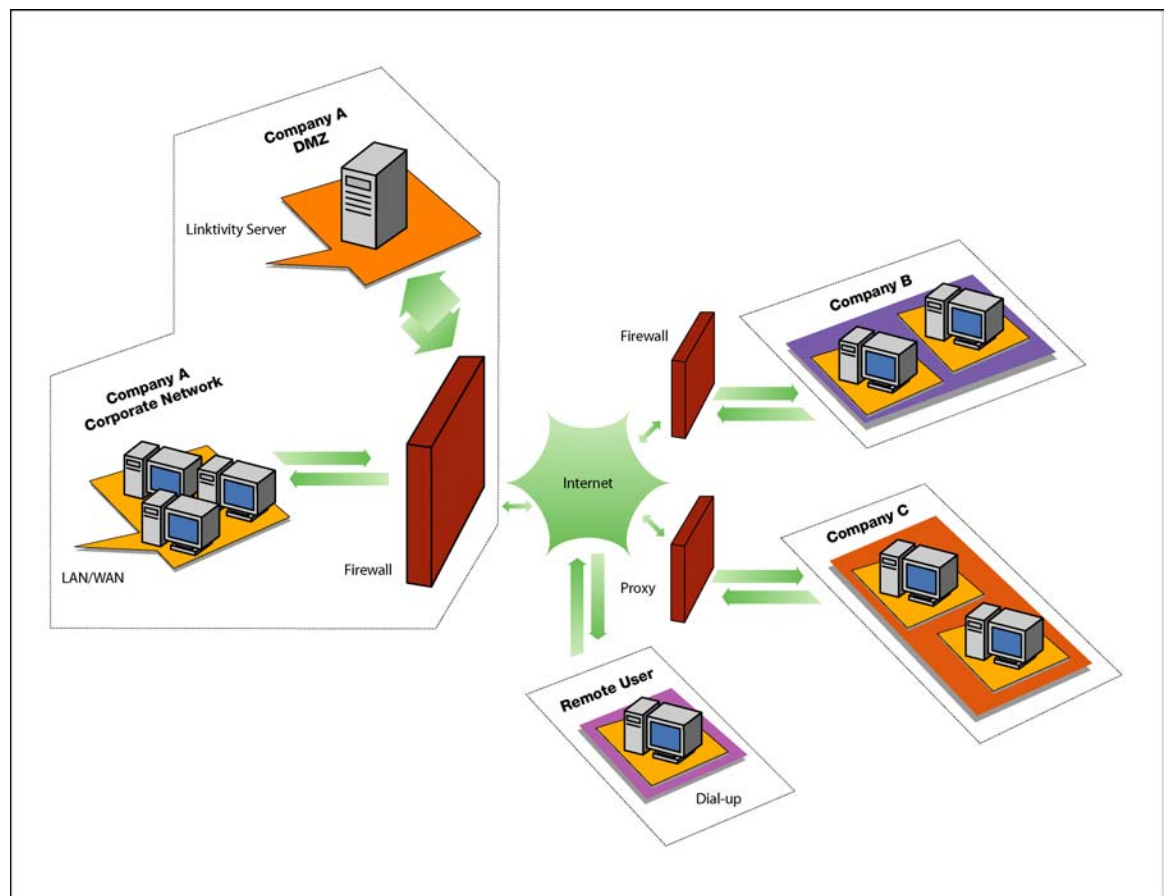
Linktivity Server Architecture and Installation

When you install WebDemo or WebInteractive on a machine, you are installing the Linktivity ConnectionPoint, which is the connection point for all users. The Linktivity ConnectionPoint is a Java application that installs on a Windows 2000/2003 machine. The Linktivity Server communicates with an ODBC-compliant database (such as Microsoft Access or SQL Server) and operates with an http server (Internet Information Services-IIS) for the UI.

How the Linktivity Server works

The key server-side application components of Linktivity Server include:

- Linktivity ConnectionPoint application
- ODBC-compliant database
- An http server
- WebDemo and/or WebInteractive user interface Web pages



Linktivity Server

The center of WebDemo and WebInteractive is the Linktivity ConnectionPoint. The Linktivity ConnectionPoint coordinates all the activity between the Host/Agents and the Participants/Customers when Linktivity collaboration tools are in use. The Linktivity ConnectionPoint manages all connections including any firewall conflicts caused by the Participant's network. Whether you are conducting a meeting, a training session, or helping a customer, the Linktivity ConnectionPoint establishes and maintains the session and allows the Host or Agent to use special functions to facilitate the session. These collaboration tools include Keyboard Chat, Voice Chat, Video, Record and Playback, File Transfer, Application and Desktop Sharing and Remote Control.

The Java based Linktivity ConnectionPoint is the command center of the WebDemo and WebInteractive collaboration tools and has been designed and developed to satisfy a broad range of business applications. The Linktivity ConnectionPoint architecture allows for maximum scalability. During a collaboration session, it is the Linktivity ConnectionPoint's job to create and maintain the session through a computer network, such as the Internet or LAN using an existing TCP/IP or HTTP protocol. The Linktivity Server resides on an HTTP server at a site determined by the owner of the server. When a collaboration tool such as Keyboard Chat is started between the Host and the Participant the Linktivity Server communicates the necessary information to allow the Keyboard Chat function to perform. The Linktivity Server provides the same service for all the WebDemo collaboration tools.

ODBC-Compliant Database

During the standard install, a Jet Engine database driver (MDAC) is automatically installed if it does not already exist on your server (it is already installed on any Windows 2000/2003 platform). The Database Administrator can manage the Jet Engine database by using Microsoft Access. Any ODBC-compliant database can be used to replace the Jet Engine database such as Microsoft SQL Server. With a few simple steps, the Database can be replicated, and the product will use the new database engine within minutes.

IIS (Internet Information Services)

The Web site runs on IIS (Internet Information Services). IIS is part of a Windows 2000/2003 install. This is used for the UI of the Linktivity Products.

Firewalls

The Linktivity ConnectionPoint actively manages all online sessions, providing secure connectivity that will not interfere with network firewalls. With the Linktivity Server, network administrators can spend less time addressing firewall configuration or security issues. For the most part, firewalls block inbound connections. If something or someone is trying to connect to your

machine from the outside (this is called an *inbound* connection), firewalls do a great job at intercepting these connection requests and handling them according to the company's policies. WebDemo and WebInteractive users (host and clients) initiate an outbound connection to the Linktivity Server. Once connected they will get the necessary information to join a session (including downloading the necessary java applets). At this point they make another outbound connection, but this time it is to the ConnectionPoint. The user (host or client) has initiated outbound connection to the Linktivity Server. There are no connections initiated from the Linktivity Server so no holes have to be created on the user's network.

Connection Method

As stated above, the users (host/clients) initiate the connections, not the Linktivity Server. Once the user has the necessary information to join a session, it will download the signed java applets (support files for the connection and controls). If the user has not yet tested their system using the "Test System" feature of the Linktivity server, they will be forced into the "Test System" page. This page will determine which connection method works for this machine along with checking other necessary settings. After the "Test System" is finished it will save a cookie with the connection type that was established. When joining a session, the saved connection type will be attempted first. If the saved connection type will not connect it will follow the same logic it used during the "Test System" to establish a connection.

The java applet follows the following logic to establish a connection: First, a TCP/IP socket connection (Persistent TCP connection) is attempted. If this connection type cannot be established the java applet will check for proxy server settings. If there is proxy server information available it will try making a proxy connection through the proxy server. If this method fails, the applet will then attempt to make an HTTP connection to the ConnectionPoint. It will try the above connections on each port that the ConnectionPoint was installed for, (the owner of the Linktivity Server determines the port) which is normally Port 443 and Port 80.

Security

Security is handled in many ways. There is the security of the data being transferred to the Linktivity clients and the Linktivity Server, the security of the interaction between a Service Representative and customer, and the security overall of a Web Server.

1. Any communication between PCs and the Linktivity Server is never done with clear text. All messages sent across the wire are encoded in a proprietary format and compressed. In addition, due to the architecture of the Linktivity product, having a piece of the information that was sent between the ConnectionPoint and a host/client will not contain useful information.
2. Web Server security is something that everyone is becoming increasingly conscious about as more and more worms and viruses

are created and spread. We recommend that people keep up with the updates from Microsoft for IIS and the updates from their virus protection software.

General Security of a Linktivity Server

The Linktivity ConnectionPoint tools talk to a single, predetermined database. The ConnectionPoint's ability to talk to its database is limited to predetermined read and writes operations. There is no way to manipulate the tools to delete database entries, or to examine anything other than specific ConnectionPoint data. Manipulation of ConnectionPoint specific data by the Linktivity ConnectionPoint itself is limited. For example, the Linktivity Server can change the date on a predefined field to today's date. It does not have the capacity to do anything else. It offers no user interface. It has no flexibility to do anything other than the few predetermined tasks that have been assigned to it. The Linktivity ConnectionPoint only talks to other people who have called them. The key point here is that you or a user must call the Linktivity Server. The Linktivity Server cannot establish connections to other machines or networks. It can only talk to people who have requested a connection to it.

Encryption

The Linktivity Server never sends meeting content in clear text. The Linktivity Server uses an encoded proprietary data format (based on industry standards) for transmitting data to and from the Host and the Participant. For more details on encryption, read the section titled "Security" above.

Client and Participant Interactions

The Linktivity Server extends functional components; such as remote control, file transfer, voice and video conferencing to remote participants by dynamically downloading secure and digitally signed Java-based applets and DLL components and configuring them on the participant's machine the first time they enter a WebDemo or WebInteractive session. The Linktivity applets and DLLs are compressed into small CAB/JAR files to improve the one time download speed.

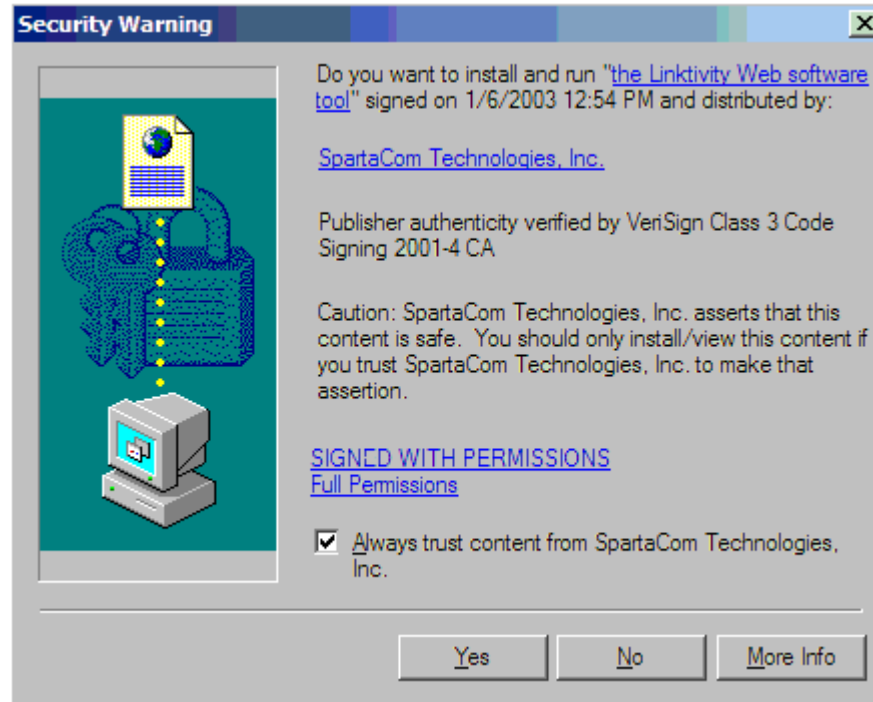
The Java Applets are Java applications embedded on HTML or Active Server Pages that run in the environment of a Web browser. Java Applets and CABs/JARs can run in order to eliminate the potential risk that is associated with running an un-trusted code, applets are executed in the applet *sandbox*, which constitutes safe environment for executing mobile code in which all access to the resources of the underlying system is prohibited. The safety of the applet *sandbox* environment is guaranteed by a proper definition of some core Java system classes.

Linktivity Security 3-18_05.doc

Linktivity | 800-809-1245 | www.linktivity.com

Java Applets are Java applications embedded on HTML or Active Server Pages that run in the environment of a Web browser. Java Applets and CAB can run in order to eliminate the potential risk that is associated with running an untrusted code, applets are executed in the applet *sandbox*, which constitutes safe environment for executing mobile code in which all access to the resources of the underlying system is prohibited. The safety of the applet *sandbox* environment is guaranteed by a proper definition of some core Java system classes.

All Linktivity CABs/JARs are digitally signed to ensure that the applets are from Linktivity and require a connection to a Linktivity ConnectionPoint in order to communicate to another computer. Remember, users must initiate the connection to the ConnectionPoint to establish a connection.



Conclusion

Linktivity solutions are easy to use in-house server software solution that provides you with all the tools necessary to conduct a Web-based highly interactive successful meeting, training sessions, and technical and customer support. Linktivity lets you use the Internet to extend the reach and impact of your ideas to virtually anybody, anywhere in the world. All you need to conduct or join a meeting is a computer and an Internet connection.

The Linktivity products are scalable from two to over 500 concurrent connections and designed with user interfaces are developed to give our customers the flexibility to customize the "look and feel" to better meet their needs within a safe and secure online environment.