Overview - Using ADAMS With a Firewall

Internet security is becoming increasingly important as public and private entities connect their internal networks to the Internet. One of the most popular methods to secure an internal network against unauthorized access from the Internet is through the use of a “firewall.” A firewall allows an administrator to permit access from the internal network to the Internet, while rejecting access from the Internet to the internal network. This arrangement provides the corporation with a direct Internet connection while keeping the internal network secure.

NRC uses Citrix's[1] Internet technology, which allows users to run Citrix sessions over the Internet. This configuration sometimes poses a challenge for maintaining Internet security because Citrix's Independent Computing Architecture (ICA) protocol is a relatively new networking protocol that runs over Transmission Control Protocol/Internet Protocol (TCP/IP) using registered port 1494. Some firewalls do not correctly process ICA because it is not a "well known" networking protocol. In such cases, allowing the ICA protocol to pass through the firewall becomes a configuration challenge. Some types of firewalls can be configured to pass ICA, while others cannot. ICA uses dynamic port allocation much like the File Transfer Protocol (FTP). The initial synchronization between the Citrix client and the Citrix server occurs over TCP port 1494 and User Datagram Protocol (UDP) port 1604, but the actual Citrix session occurs over a dynamically allocated port. For this reason, it might be necessary to allow connections over a range of TCP/IP ports through the given firewall. If required, these connections should be allowed only between the client and the server. Allowing Citrix ICA traffic through a firewall generally entails defining a rule to allow access in the proper direction.

[1] Citrix Independent Computing Architecture (ICA) Client and Server software are products of Citrix Systems, Inc.

Firewall Architecture

Most firewalls use one of four architectures, namely:

- Packet Filter Gateway
- Circuit Level Gateway
- Application Proxy
- Stateful Inspection

These four firewall architectures pose different configuration challenges for passing the ICA protocol. Some firewalls have built-in abilities to allow new protocols such as ICA to be passed, while others require the application of a specific workaround.

Packet Filter Gateway

Packet filter gateways are the easiest to configure for ICA but provide the least security. A packet filter analyzes each IP packet at the network layer and determines whether to pass or block it according to a set of rules. A packet filtering gateway is more of an intelligent router than a firewall. If the packet filter has a rule specified in its rule base that allows communication between two specific addresses, packets are allowed to travel through the firewall to the specified address. If no rule is available for a given address, the packet is rejected and is not allowed to pass through the firewall.

To configure a packet filtering gateway to pass the ICA protocol, insert a rule in the packet filter's rule base that allows communications to the Citrix server over port 1494. Depending on the vendor and the model of the packet filtering gateway, this step could involve defining a rule that allows traffic over port 1494 to and from certain machines or groups of machines inside and outside of the network.

Circuit Level Gateway

Circuit level gateways operate at the session level used by TCP/IP and UDP. A circuit is a logical connection that is maintained for a period of time, then torn down or disconnected. The firewall verifies the circuit when it is first created. Once the circuit is verified, subsequent data transferred over the circuit is not checked. Circuit level gateways can limit which connections can be made through the gateway and can be configured for the ICA protocol. They provide a moderate level of security.

Configuring circuit level gateways to pass the ICA protocol involves allowing circuits to be made through the gateway on port 1494. Once the circuit is allowed, connections to Citrix servers are verified through a circuit that allows Citrix sessions through the gateway.

Application Proxy

Application proxies are probably the most secure firewalls, but a special proxy must be written for each given protocol. Proxy servers provide in-depth knowledge of IP protocols and allow application level analysis. They examine each packet of information as it passes through the gateway. Proxy servers are not designed to allow for new types of protocols. To pass a new protocol through a proxy server, a workaround must be developed.

The most common workaround for proxy servers involves the use of a service called SOCKS. This service is loaded on the proxy server and allows new protocols to be passed through the proxy server without writing a full application proxy for the new protocol. Although this is a workable solution, not all proxy servers support the SOCKS services. Some vendors are currently working on transparent interfaces much like SOCKS that could allow proxy servers to pass new protocols, such as ICA. At the present time, however, no proxies or SOCKS-compatible services are available for ICA.

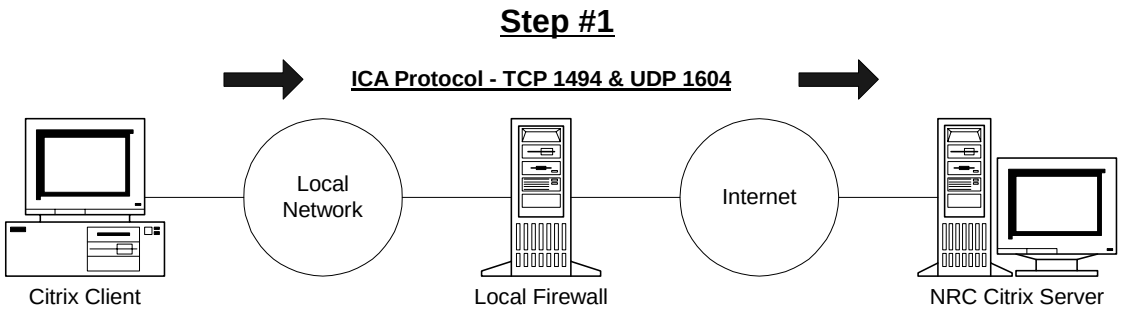
Configuring a proxy server to pass the ICA protocol requires allowing communications to pass through port 1494 to the Citrix server. It should be noted that this configuration may not be supported by all proxy servers. Because opening a port on the firewall can pose a security risk, it is recommended that communication only be allowed to initiate from inside the local network. Allowing access from the Internet over port 1494 could pose a serious security risk. Therefore, it is suggested that only Citrix clients from the local network be allowed to connect to Citrix servers on the Internet.

Stateful Inspection

Stateful Inspection (SI) is a new firewall technology that lends itself to the configuration of new protocols. Stateful inspection expands on packet filtering by adding state information derived from past communications and other applications. Some of the newer SI firewalls allow new protocol definitions to be added to the firewall with minimal work. Much like a packet filtering gateway, SI firewalls can be easily configured to allow new protocols to be passed through the firewall over defined ports. In addition to this ease of configuration, the SI firewalls can provide added security to these new protocols by performing packet inspection as the packets move through the firewall. Some SI firewalls, for example Checkpoint Firewall-1, have a scripting language that allows custom scripts to be written for packet inspection. This scripting adds an extra layer of security above packet filtering while keeping ease of configuration. SI firewalls have the ability to inspect all levels of the TCP/IP packets, allowing inspection scripts to be as simple or as complex as required.

Configuring SI firewalls to pass the ICA protocol requires defining the ICA protocol as a network service. The ICA protocol should be defined on port 1494 with a dynamic source port allocation; that is, above port 1023. Rules can then be added to the rule base to allow users to access Citrix servers. It should be noted that allowing inbound connections from the Internet could pose a security problem. Most SI firewalls do perform some level of packet inspection even without a custom inspection script. This inspection provides an extra level of security above packet filtering; however, it is an issue that should be researched depending on the model of firewall used. Although many firewalls can be configured to pass the ICA protocol, NRC recommends taking measures to ensure a secure environment.

The Citrix Three-Step Connection Process



Overview

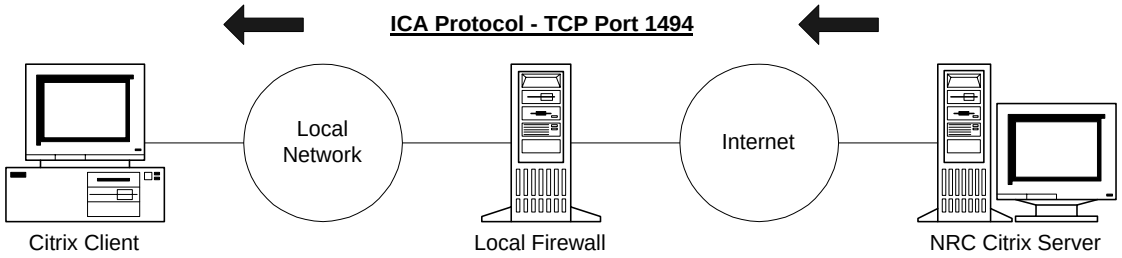
A user starts a Citrix session from the client workstation. The Citrix client software contacts the Citrix server using TCP port 1494 and UDP port 1604.

Details

For local users to access Citrix servers on the Internet, ICA packets must be passed through the firewall in an outbound direction to the Internet. Depending on the type of firewall being used, this option could involve opening up TCP port 1494 and UDP port 1604 on the firewall to allow outbound access to the Internet. Because the local users are considered to be inside the trusted domain, a minimal security risk is involved.

In this configuration, a Citrix client behind the firewall can initiate a Citrix session to a Citrix server anywhere on the Internet. Because TCP port 1494 is only open to outbound access from the local network, there is little security risk involved in this setup.

Step #2



Overview

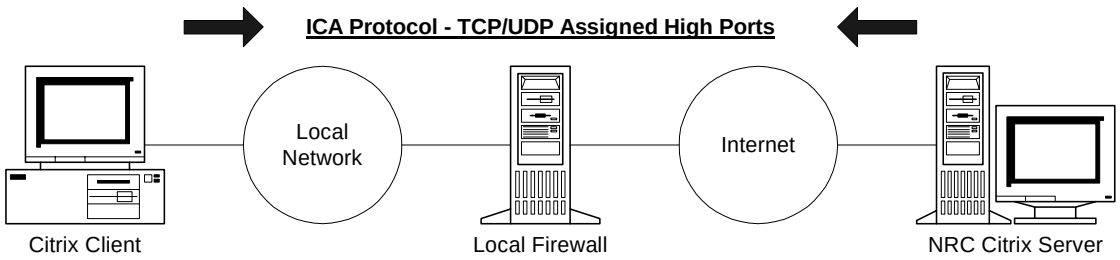
The Citrix server sends a message back to the Citrix client over TCP port 1494 saying "connect using port X" where X is a port number above 1023.

Details

For Internet users to access a Citrix server behind the corporate firewall, Citrix ICA packets must be passed in an inbound direction through the firewall. In this situation, port 1494 should be opened for inbound communication from the Internet.

Caution: If connections are allowed to all machines behind the firewall, a hole is opened that exposes the entire internal network to the Internet. Therefore, for security reasons, inbound communications from the Internet should be allowed to connect only to the Citrix server(s). The IP address of the NRC Citrix server is 148.184.174.242.

Step #3



Overview

Once port X is established in step #2, communications between the Citrix client and the Citrix server will take place using the assigned high TCP and UDP ports, which are 1023 to 65,535.

Details

For Internet users to access a Citrix server behind the corporate firewall, Citrix ICA packets must be passed in an inbound and outbound direction through the firewall. In this situation, TCP and UDP ports 1023 - 65,535 should be opened for inbound and outbound communication to and from the Citrix server on the Internet.

The NT TCP port allocation algorithm is to just index the ports used from minimum user port (1025). A counter is maintained of the last one allocated, and is incremented for each allocation. A check is then made to ensure that no other connection is using this port, and if the port is in use it goes to the next one. So the NT TCP/IP port number is a function of how many other connections have been made to the box, and are not random. MetaFrame does not change this algorithm at all, and uses standard NT TCP/IP. The maximum user port used by default is 5000, but a registry key "MaxUserPort" can allow this to be specified up to the TCP/IP maximum of 65535.

Example

This algorithm is the same as if a MetaFrame were running a HyperText Transfer Protocol (HTTP) server. The remote browser would connect at port 80, and the NT TCP/IP would allocate a new port in the range of 1025-5000 that was not in use. The next user would get Port +1 if this one is also not busy, and so on. MetaFrame ICA does the same thing. The firewalls know about port 80 and will allow the allocation because of the connection. This type of rule needs to be enabled in a firewall-specific manner for ICA. All the information the firewall needs should be in the connection setup messages that flow between the remote client on the other side of the firewall and the host. These are TCP, not ICA, messages, so no knowledge of ICA is needed.