

# Firewall Settings to Access Hosted Environment

Client firewall settings in most cases depend on whether the firewall solution uses a Stateful Inspection process or one that is commonly referred to as an Access Control Method, which simply looks at allowed UDP and TCP port numbers and the direction of packets. We will attempt to cover both types in this document, but please remember, each device has its own way of doing this. Please consult your firewall equipment documentation for the correct commands and procedures.

## Configuration of Firewalls / Routers

For the configuration listed below, please use these addresses in place of the names. Both sets of addresses must be used.

Hosted Environment Networks: 97.65.91.0/24 (Subnet Mask 255.255.255.0)

Hosted Environment DMZs: 207.250.245.64/26 (Subnet Mask 255.255.255.192)

207.250.170.0/26 (Subnet Mask 255.255.255.192)

### For Access Control Method (also known as access lists and usually used on routers)

Type Of Traffic:	From: (Source Address)	To: (Destination Address)	Ports:
<b>Outbound ICA Traffic</b>	Client Network	Hosted Network	TCP 80 TCP 443 TCP 2598 <i>Deprecated:</i> TCP 1494 UDP 1604
<b>Inbound ICA Traffic</b>	Hosted Network	Client Network	None <i>Deprecated:</i> TCP High Ports
<b>Hosted Environment WWW Traffic</b>	Client Network	Hosted Network Hosted DMZ	TCP 80 (HTTP) TCP 443 (HTTPS)

## For Stateful Firewall Method

Type Of Traffic:	From: (Source Address)	To: (Destination Address)	Ports:
<b>Outbound ICA Traffic</b>	Client Network	Hosted Network	TCP 80 TCP 443 TCP 2598 <i>Deprecated:</i> TCP 1494 UDP 1604
<b>Inbound ICA Traffic</b>	Hosted Network	Client Network	None
<b>Hosted Environment WWW Traffic</b>	Client Network	Hosted Network Hosted DMZ	TCP 80 (HTTP) TCP 443 (HTTPS)

## Frequently Asked Questions

- **“Why are ports TCP 1494 and UDP 1604 connections being depreciated?”**  
It is suggested that all customers upgrade to the latest Citrix client in order to take advantage of the better security and session reliability that it offers. These improvements required Citrix to change the default ports that are used to communicate from the client to the server.
- **“Do I need to change any firewall settings right away?”**  
It is highly likely that ports TCP 80 and TCP 443 are already open so that you can browse sites on the Internet with your web browser. In this case, while you may choose to remove ports TCP 1494 and UDP 1604 from your firewall configuration, you should not need to change anything in order to continue to access the Hosted Environment.
- **“Why do I need to open port TCP 2598?”**  
You should be able to use the Hosted Environment without having to open port TCP 2598. In the case that port is not available, ports TCP 80 and TCP 443 will be used exclusively. However, if you open port TCP 2598, you will benefit from the enhanced session reliability that the Citrix client can provide when this port is opened. Please contact support with questions about accessing the hosted environment without port 2598.
- **“What if I can’t get TCP 80 / TCP 443 connections to work?”**  
An alternate link is provided on each Customer Launch Page that can be used in conjunction with an older Citrix client to continue to access the Hosted Environment. You should only need this option if you run certain kinds of proxy servers. Please contact Support if you can only use the depreciated support access via TCP 1494 / UDP 1604.

- **"Why is the range of Hosted Environment addresses so large?"**

The address range listed is entirely in our control; no other entity will use this address space so be assured that it is secure. We deliver your applications using a load balancing methodology so any one of many servers configured on any of these addresses in this range could respond to your request for an application. Although you request application services from two addresses in this range, neither of these ever actually responds - they simply "broker" your request to the address of the appropriate server depending on real time utilization figures. It is required that if you limit by rule to an address range that this entire range be allowed as there is no way to predict which address your application will be served on at any given time.

- **"What are some of the error messages I might see if the firewall or router is not properly configured?"**

Below are some screen shots of some possible messages you might see if your firewall or router is not properly configured.

