

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)

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

Type Of Traffic:	From: (Source Address)	To: (Destination Address)	Ports:
Outbound ICA Traffic	Client Network	Hosted Network	TCP 1494 UDP 1604 TCP 2598
Inbound ICA Traffic	Hosted Network	Client Network	TCP High Ports
Hosted Environment WWW Traffic	Client Network	Hosted Network Hosted DMZ	TCP 80 (HTTP) TCP 443 (HTTPS or SSL)

For Stateful Firewall Method

Type Of Traffic:	From: (Source Address)	To: (Destination Address)	Ports:
Outbound ICA Traffic	Client Network	Hosted Network	TCP 1494 UDP 1604 TCP 2598
Inbound ICA Traffic	Hosted Network	Client Network	None
Hosted Environment WWW Traffic	Client Network	Hosted Network Hosted DMZ	TCP 80 (HTTP) TCP 443 (HTTPS or SSL)

Frequently Asked Questions

- **“Why do I need have all of these unusual ports open?”**

Port 80 and Port 443 are actually very common ports to have open out to the Internet. These ports are used for web browsing and secure web browsing.

TCP 1494 and UDP 1604 may seem unusual, but these are the ports ICA traffic runs on, similar to web browsing on Port 80 and 443. These are required to be open to work in the Hosted environment.

TCP High Ports (1023 – 65535) need to be opened in a non-stateful environment. An excerpt from a Citrix document explains this connection based requirement best:

“A user starts a session from the client. The client contacts the server over TCP Port 1494. The server sends a message back to the client over TCP Port 1494 saying "connect using port X" where X is any port number above 1023. This is called using TCP High Ports. All of the ports under 1023 are reserved for system use and "Well Known" protocols such as FTP, HTTP etc. The MetaFrame server will dynamically (randomly) allocate a specific port above 1023 for each TCP/IP session. This is how we can support multiple sessions at one time. Each one has it's own port.

Once communication is established, the client will send its information to the server on Port 1494 with a destination Port of X. When the server replies, it will be sent on Port X, with a destination Port of 1494. If your router or firewall does not have this port open, the packet will be dropped, hence the opening of TCP High Ports."

- **"Isn't this a security risk to have these extra ports open?"**

It could be a security risk to have the high ports open if you would allow them to come from any IP address. However, you can minimize that risk by making sure that you only accept packets on these ports from the Hosted Network. We highly recommend that you configure your router or firewall in this manner.

- **"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.

