

Check Point Software Technologies LTD

FireWall-1 Version 4.0 Microsoft NetMeeting with Network Address Translation Quick Reference

The purpose of this document is to provide basic guidance on configuration issues when combining the use of Microsoft's NetMeeting application with FireWall-1 security policies, particularly Network Address Translation (NAT).

FireWall-1™ version 4.0 is capable of supporting configurations combining Microsoft's NetMeeting™ (and other H.323 based protocols) with Network Address Translation. NetMeeting utilizes the protocol H.323 which encapsulates the real source address within the data portion of the packet. This has been problematic in the past but version 4.0 of FireWall-1 has been designed to interpret this information and deal with it appropriately.

To enable the multi-point data conferencing portion of NetMeeting (application sharing, whiteboard, chat, file transfer, and directory lookups), the firewall need only pass through primary TCP connections on statically assigned ports which is relatively simple. Supporting these data conferencing features in conjunction with NAT is also relatively simple. However, in order to support the video and audio features of NetMeeting the firewall must understand the calls it makes using secondary TCP and UDP connections on dynamically assigned ports.

NetMeeting uses the ports listed in the table below.

Port	Protocol
389	Internet Locator Server (TCP)
522	User Location Service (TCP)
1503	T.120 (TCP)
1720	H.323 call setup (TCP)
1731	Audio call control (TCP)
Dynamic	H.323 call control (TCP)
Dynamic	H.323 streaming (RTP over UDP)

To establish outbound NetMeeting connections through a firewall, the firewall must be configured to allow the following:

- Pass TCP connections on ports 389, 522, 1503, 1720, and 1731 and,
- Pass TCP and UDP connections on dynamically assigned ports from 1024 to 65535. (Support for dynamic port assignment will occur automatically with Stateful Inspection using the pre-defined NetMeeting service.)

In order to establish audio and/or video connections, H.323 uses a call setup protocol to initiate sessions. This protocol uses TCP port 1720 and is responsible to negotiate a TCP port between hosts for the H.323 Call Control Protocol. Also, both the Audio Call Control Protocol (using TCP port 1731) and the H.323 streaming protocol, referred to as Real Time Protocol (RTP) must dynamically negotiate UDP ports.

NetMeeting requires that two UDP ports be determined on each side of the firewall for audio and video streaming for a total of four ports for inbound and outbound audio and video. These dynamically negotiated ports are selected arbitrarily from all the ports that can be assigned using the protocols described in the paragraph above.

NetMeeting directory services require either TCP port 389 or TCP port 522, depending on the type of server used. Internet Locator Servers (ILS) which support Lightweight Directory Access Protocol (LDAP) for NetMeeting require port 389, and the User Location Service requires (ULS) port 522.

Based on the information above, there are several things to keep in mind when configuring FireWall-1 to securely pass NetMeeting traffic while performing Address Translation:

- Translation for machines on the inside of the firewall must use STATIC translation as HIDE mode is incapable of knowing which machine on the inside is to receive the call setup packets. This is true only if the firewall must be configured to support inbound call connections. If outbound only calls are to be supported (i.e. the internal client initiates the connection) then HIDE mode will work.
- New services must be created for the ULS protocol which uses TCP port 522, the T.120 protocol which uses TCP port 1503, and the Audio Call Control protocol which uses TCP port 1731. (*See note at the end of this paper for details of which protocols are predefined with which FireWall-1 4.0 Service Packs.)
- Make sure in the Service Column of the FireWall-1 GUI to explicitly use the NetMeeting service as well as the new services as the use of 'any' does not allow the H.323 based protocols to operate correctly. This is done by design as FireWall-1 will only support H.323 when explicitly defined.

The Security Policy depicted on the following page shows elements to included in a policy allowing NetMeeting connections to a particular client machine within a protected network. In reality, this object will probably be more than one client so this may be a group of workstations or whatever is applicable in your network. This policy presumes that no authentication is taking place which may not be the case in your security policy. Of course, if you utilize authentication replace the 'accept' action with the appropriate authentication option up to and including SecuRemote.

No.	Source	Destination	Service	Action	Track	Install On
1	Internal_Client	Any	NetMeeting ULS-522 T.120-1503 ACC-1731	accept	Long	Gateways
2	Internal_Client	Any	Any	accept	Long	Gateways
3	External_Client	Internal_Client	NetMeeting T.120-1503	accept	Long	Gateways
4	Any	Any	Any	drop		Gateways

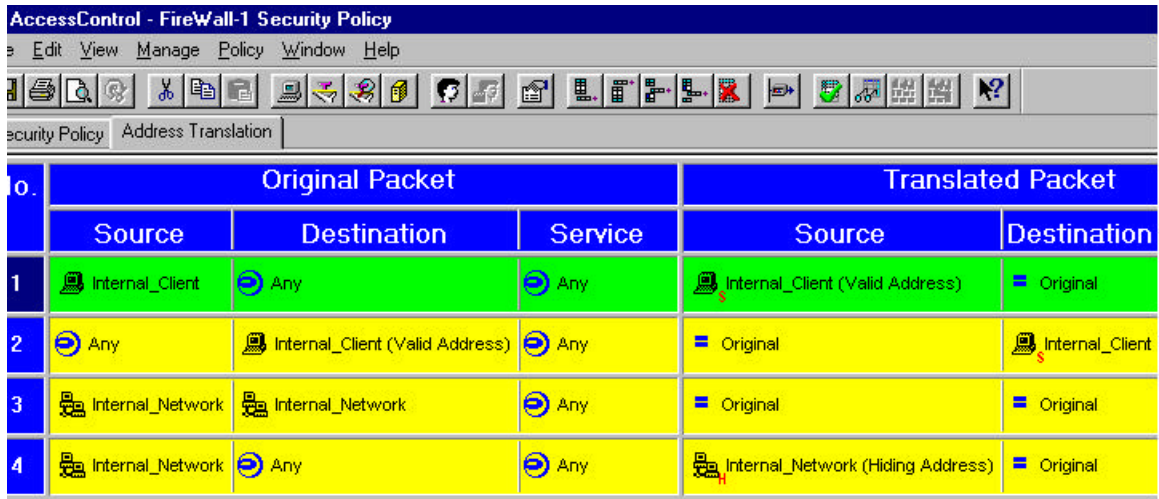
In the Security Policy above Internal_Client is a machine on the protected side of the firewall. Predefined machines on the outside of the firewall can connect to this machine to establish NetMeeting sessions. Rule number 1 allows the internal machine to connect outside the firewall using NetMeeting protocols. Rule number 2 allows the same client outbound communications for any other protocols.

Rule number 3 allows a predefined machine outside the firewall to communicate with the internal machine using NetMeeting protocols.

The above information allows machines to connect through FireWall-1 to establish NetMeeting connections. The next step is the configuration of Address Translation to allow connections in situations where illegal addresses are used on the protected side of the firewall or if address translation is used as an additional security measure.

In short, as indicated above, for connections to be established from outside the firewall to the internal client machine, STATIC address translation must be used. The address translation rule, therefore, will must include a valid, routable, address which represents the 'real' address of the internal client machine. Also, any static rule must appear before any other hide rules as FireWall-1 views address translation rules the same way it views security policy rules – in order of appearance in the rule base. If HIDE mode rules appear first, the firewall will always match this and will not look further for a static rule. (Note that with FireWall-1 version 4.0 the use of the "Add Automatic Address Translation Rules" feature in the definition of network objects will place the address translation rules in the correct order on your behalf.)

The address translation rule base will look like the screen shot below:



No.	Original Packet			Translated Packet	
	Source	Destination	Service	Source	Destination
1	Internal_Client	Any	Any	Internal_Client (Valid Address)	Original
2	Any	Internal_Client (Valid Address)	Any	Original	Internal_Client
3	Internal_Network	Internal_Network	Any	Original	Original
4	Internal_Network	Any	Any	Internal_Network (Hiding Address)	Original

Note that any packet coming into the firewall with the destination of the 'valid' IP Address of the internal client will be translated statically into the client's 'real' IP Address prior to forwarding the packet to the internal network. At the same time, with subsequent rules, the rest of the 'hidden' network can continue to operate with traditional HIDE address translation.

*Note on predefined NetMeeting services with FireWall-1 4.0. This paper was written using FireWall-1 Service Pack 1(SP1). With SP1, several NetMeeting services need to be created by the firewall administrator. Subsequent service packs have included more NetMeeting services in the predefined "NetMeeting" service group.

Specifically, SP3 includes the T.120 service which utilizes TCP port 1503. SP4, although not released at the time of publication of this document will include ULS which utilizes TCP port 522, and ACC which utilizes TCP port 1731.