



We Secure the Internet.

# Check Point® H.323 Security Vulnerability 1/25/04



## Overview

A recent advisory published by NISCC at:

<http://www.uniras.gov.uk/vuls/2004/006489/h323.htm>

reveals several vulnerabilities in H.323 equipment including GateKeepers, endpoints (phones, softphones, video cameras, etc.) and firewalls that enforce H.323 security.

In order to protect FireWall-1 against the attacks described in the above mentioned advisory, all Check Point customers using H.323 are required to install an update. **Even if you are not using H.323**, Check Point still highly recommends that you install an update on all enforcement modules.

The update is available from <http://www.checkpoint.com/techsupport/downloads.jsp> or contact Check Point Support for a fix ([support@ts.checkpoint.com](mailto:support@ts.checkpoint.com)). Check Point also encourages you to contact your other H.323 equipment vendors (especially the GateKeeper) and install any related updates.

## If H.323 is not used

If H.323 is not used you have two methods of providing protection:

### Add a deny all H.323 traffic rule

The best protection against these vulnerabilities is to deny all H.323 traffic to-and-from your protected networks. This method will fully protect FireWall-1 and the network(s) behind it against these vulnerabilities. To deny H.323 traffic, a rule such as the following should be added to the rule base:

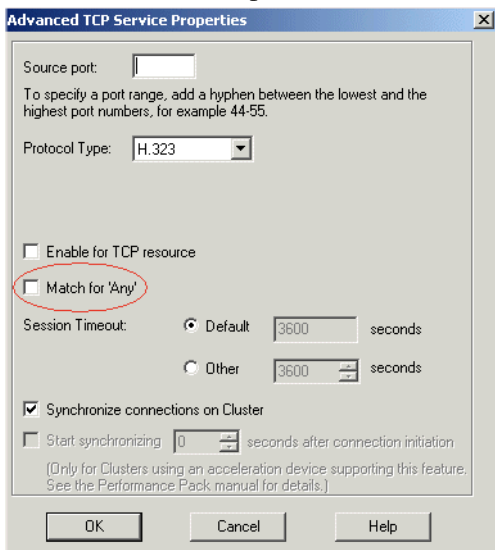
3	* Any	* Any	* Any Traffic	TCP H323	drop	Log	* Policy Targets	* Any	Don't allow any H.323 traffic to/from our network
---	-------	-------	---------------	----------	------	-----	------------------	-------	---

### Disallow automatic H.323 parsing

---

Check Point VPN-1 Pro parses H.323 traffic by default, unless a rule is defined (specific or general) to block H.323 traffic. Automatic parsing allows FireWall-1 to dynamically follow an H.323 session state and allows additional and relevant connections when phone or video calls are made.

To tell FireWall-1 not to parse and enforce H.323 traffic by default, in SmartDashboard, go to **Manage > Services**, select the **H323** service and click **Edit**. In the **TCP Service Properties - H323** window that opens, click **Advanced** and deselect the **Match for 'Any'** option as follows:



## Update Installation Instructions

For installation instructions please refer to the relevant Hotfix Release notes.