

HOW TO CONFIGURE TRAFFIC INSPECTOR

This document describes how to perform the initial Traffic Inspector configuration. The following aspects are described in this tutorial:

- Defining operation mode and networking settings
- Populating the program with user accounts
- Verifying configuration settings and testing user access to the Internet

Defining operation mode and networking settings

Navigate to Console Root | Traffic Inspector[] | Settings |

Locate the **Traffic Inspector settings** group box, select the **Actions** tab and click the **Launch the Advanced Configuration Wizard** link.

	TrafInsp - [Console	Root\Traffic Inspector	[LOCAL]\Settings]	_ D X
<u>a</u> File <u>A</u> ction <u>V</u> iew Fav <u>o</u> rites	<u>W</u> indow <u>H</u> elp			_ & ×
🗢 🔿 🙍 🖬 🙆 👔				
Console Root C	SETTING SETTIN	SS 3/1/16 05:15:05 AM 0.01 0 0		
	View driver statistics			
	View IP routing table			~
Connection to LOCAL user win-8fash	l Ir&rdd\administrator			
Connection to LOCAL, user WIN-blasb	norua (auministrator.			

The first setting we have to define is the operation mode.



Traffic Inspector supports two operation modes:

- Gateway mode
- Single interface mode

Under gateway mode, Traffic Inspector is deployed at the edge of your home or office network and processes all the traffic that flows into and out of it. This is the most feature-rich operation mode.

The Single interface mode requires Traffic Inspector to only have one network interface that is connected to the internal network. The Single interface implies that an Ethernet switch with the port mirroring capability is used to send a copy of network packets to Traffic Inspector. Under Single interface mode Traffic Inspector can only perform traffic accounting. If you plan to implement Web Access Control, gateway-level anti-virus protection, spam filtering, etc., use Gateway mode instead.

The **Windows NAT service** tab is used to select the service that provides the Network Address Translation (NAT) functionality.



On Windows two services can provide NAT functionality:

- Internet Connection Sharing service (ICS)
- Routing and Remote Access Service (RRAS)

RRAS NAT is more capable than ICS NAT. On Windows Server 2012 R2, you have to install the Remote Access role to be able to use RRAS NAT. Instructions on how to do this can found on the Web. For now we will use ICS-based NAT.

Traffic Inspector features a custom firewall which effectively prevents unauthorized access to your network and services from the Internet. We recommend that you disable Windows Firewall on the Traffic Inspector gateway. Using two firewalls concurrently will lead to greater ambiguity.

Thursday .	
Operation Mode Windows Services Current Configuration Windows NAT Service Windows Firewall Acoly Settimas	Windows Firewall is a component of the Windows operating system that provides firewalling and packet filtering. Windows Firewall is enabled by default. Traffic Inspector features an integrated firewall. To simplify configuration, it is recommended that you disable Windows Firewall.
Done	Windows Firewall Do not configure Do not change Windows firewall settings. Disable Disable Disable Windows frewal.
Usla	d Back Maxie Canad

Click **Next** a couple of times to finalize the first part of the configuration process.

The second part of the Configuration Wizard allows you to configure Traffic Inspector services and interfaces. Since, we are only interested in the initial Traffic Inspector configuration, we can ignore the majority of advanced settings. Configure Traffic Inspector as described below.

On the **Features** tab select the **Enable Traffic Inspector firewall** option and the **Enable RAS server support** option (required for remote VPN users).

Configu	ire services and interfaces
E Features	→ Enable Traffic Inspector firewall
Services	Traffic Inspector firewall protects the gateway and internal networks from unauthorized access from external networks (the Internet). Default settings provide the necessary level of protection.
🗐 External Interfaces	Enable Advanced Routing feature
External Firewall	Advanced Routing functionality enhances Windows routing capabilities. It allows to route different types of traffic via different external interfaces based on various criteria.
Anniu Sattinae	Enable RAS server support
Done	Enable support for RAS dial-in interfaces in Traffic Inspector.
	Enable guest networks
	Enable IEEE 802.1Q VLAN support
	Enable support for tagged Ethernet traffic in Traffic Inspector.
	Enable DVB adapter support
Heln	< Back Next > Concel

On the **Internal Interfaces** tab select network interfaces that are used by Traffic Inspector to connect to your home / office network.

Features	
Services	Select internal interfaces:
Internal Interfaces	Ethernet
External Interfaces	Ethernet 2
External Brewall	Ethernet 4
NAT Mode	
DNS Resolution	A de actual stand stand
Apply Settings	Auto-select internal internaces
Done	
	Notice of the second
	Internal internaces are connected to internal networks.
	RAS server dial-in interfaces and loopback interface are
	automatically configured as internal internaces.

On the **External Interfaces** tab select network interfaces that are used by Traffic Inspector to connect the Internet.

Conngare	services and interfaces
Select Action Features Services	Select external interfaces:
Internal Interfaces External Interfaces	Ethernet 4
External Firewall NAT Mode DNS Resolution Apply Settings Done	External interfaces are connected to external networks. Auto-select external interfaces Auto-select interfaces for which default routes exist Interfaces that are used in default routes are automatically configured as external.
	Auto-select dial-up and RRAS demand-dial connections Dial-up and RRAS demand-dial interfaces will be automatically configured as external.

On the **External Firewall** tab select network interfaces for which Traffic Inspector firewall will be enabled.

	The Advanced Configuration Wizard	×
Configur	e services and interfaces	
Features Services Internal Interfaces External Interfaces	The external firewall protects the Traffic Inspector server and internal networks by filtering IP traffic originating on the Internet. Default settings provide the necessary protection. The firewall can be selectively enabled or disabled for specified interfaces.	
External Firewall NAT Mode DNS Resolution Apply Settings Done	Select interfaces for which the external firewall will be enabled:	
Help	< Back Next > Cancel	

he **Interface NAT Mode** tab allows you to configure public / private mode for previously-selected external and internal interfaces. Make appropriate selections, click the **Next** button twice and wait while the new settings are being applied.

must	
Features Services	This tab allows you to configure NAT modes for selected interfaces.
Internal Interfaces	You can review and change these settings using standard Windows administration tools.
External Interfaces	Select private NAT interfaces:
O NAT Mode	Ethemet 2
DNS Resolution	
Done	Configure private NAT mode for RAS dial-in interfaces Select public NAT interfaces:
	₩Ethernet

Importing users

Traffic Inspector is designed to control user access to the Internet. Each user that is going to access the Internet via Traffic Inspector must have a user account. You can create each account manually or use a bulk-import method provided by **the User Import Wizard**.

You can launch **the User Import Wizard** in the final step of **the Configuration Wizard**. Alternatively, you can navigate to *Console Root* |*Traffic Inspector[]*|*Users and Groups*|, then locate the **Users and Groups** group box, select the **Actions** tab and click the **Import Users** link.

TrafInsp - [Console Root\Traffic Inspector [LOCAL]\Users and Groups]	- 🗆 X
Eile Action View Favorites Window Help	_ 8 ×
Console Rot Console Rot Traffic Inspector [LOCAL] Toolbox Wess and Groups Non-group Users Services Noladitistation Settings Activation Users and Groups Ceneral Actions General Actions General Actions On Service Users On Administration Users On Activation Other part of the	2
onnection to LOCAL, user win-8fasb1r8rdd\administrator.	

Select the **Local network scan** option and click **Next**. In case your Traffic Inspector gateway is joined to a windows domain, you can also use the **Active Directory user import** option.

Select Mode Network Scan User Settings Dimporting Users	ers
Done Done	Select user import method Active Directory user import Cal network scan
Help	< Back Next > Cancel

Select the users that you want to add to Traffic Inspector and click **Next**.

Select Mode	Select networ	k:	
Network Scan	192.168.137.	0/255.255.255.0 V	Scan
-	Select devices	E	
User Settings	Name	IP	MAC
Importing Users	PC1	192.168.137.254	08-00-27-AA-DD-31
Done			
	<	III.	>

Define settings for imported users. Set **Authentication type** to **IP address** and **Access type** to **Unlimited**. With IP address authentication, a user is considered to have an authenticated status once he/she turns on their computer. With unlimited access, a user can access the Internet irrespective of their balance.

Select Mode	Group:
Network Scan	<non-group> v</non-group>
User Settings	
Importing Users	Authentication type
Dese	P address
Done	O MAC address
	O IP + MAC
	Access type
	Unlimited
	O Limited

Finish the User Import Wizard by clicking Next and Done.

Verifying configuration settings and testing user access to the Internet

You can now verify your Traffic Inspector setup.

We have configured Traffic Inspector to use ICS-based NAT. When ICS is enabled, the internal Traffic Inspector interface is automatically set to use IP address 192.168.137.1. Unless you change this address to a different one, ICS will also provide a DHCP and DNS service for the 192.168.137.0/24 network. You can now turn on your LAN PC and it will obtain all the necessary networking settings automatically via DHCP. The IP address assigned to your LAN PC via DHCP may change over time.

If you have changed the IP address of the internal Traffic Inspector to a value other than 192.168.137.1, ICS DHCP server will stop working and you will have to assign an IP address to your LAN PC manually. Be sure to assign an IP address that is in the same range as the Traffic Inspector internal interface's IP address.

On your LAN PC, open a browser and access an Internet website. All should be working.

Congratulations, you have configured Traffic Inspector to provide Internet access for you LAN! From here, you may want to think about configuring advanced Traffic Inspector features including:

- Web Access Control
- Kaspersky Gateway Antivirus
- Spam Filtering
- Advanced Routing
- Logs and Reports
- Administrative access to program
- Automatic backup and cleanup