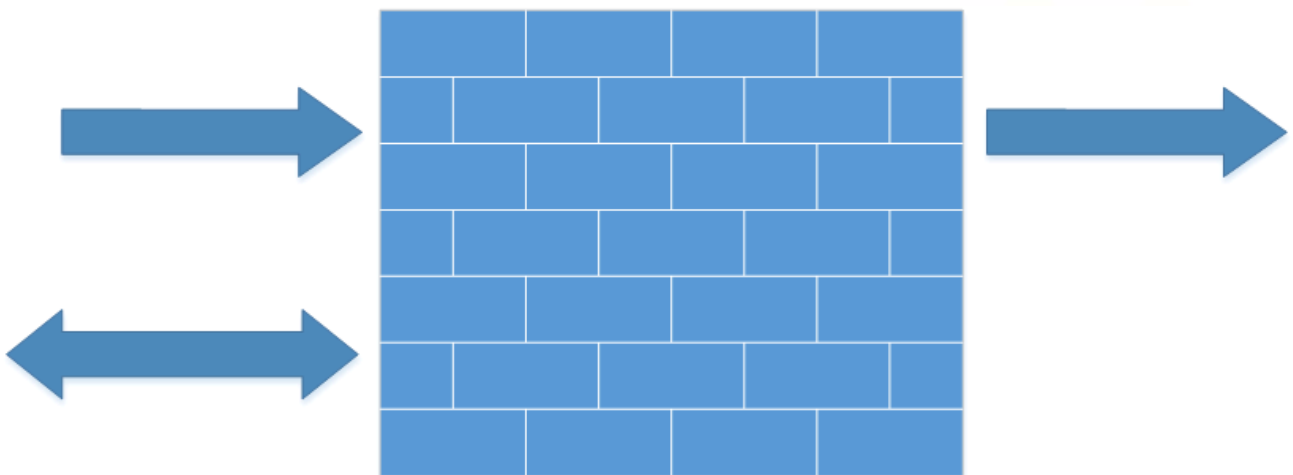


APPLICATION NOTE: AN-005-WUK

Firewall

Access Control, Port Forwarding, Custom NAT and Packet Filtering.

Applies to the xRD and ADSL Range.



FIREWALL

Access Control

The Access Control page allows configuration of the firewall to allow or deny access to internal services of the router. The Access Control element applies to incoming interfaces.

1. WLS: The Wireless 2G / 3G / 4G Interface.
2. VPN: Applies to all supported VPN types. IPSec, SSL, WeConnect, PPTP and L2TP.
3. GRE: The GRE tunnel interface.

By default, the firewall will block all access to all internal services, (e.g. the router’s web configuration pages), through the wireless interface. The exception is if access is via a VPN tunnel, which allows full access to all internal services, because this is deemed as trusted traffic.

The settings can be changed either by allowing or blocking access to all services on each interface, or by using the tick boxes to allow or block access to specific services.

For example, if the SIM card has a fixed public IP address, you might want to allow access to the router’s web server on the Wireless Interface.

Status	System	Wireless	Network	Routing	Firewall	VPN	Serial Server	Management
Setup	Access Control	DoS Filters	Custom Filters	Port Forwards	Custom NAT	MAC Filters		

Logged in as **admin** Host: MRD-455

Access Control

External Access Control	Incoming Interface						
	WLS		VPN		GRE		
Default policy	Deny ▾		Allow ▾		Deny ▾		
Services	Allow	Port	Allow	Port	Allow	Port	
Web Server	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	80	<input type="checkbox"/>	80	
Secure Web Server	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	443	<input type="checkbox"/>	443	
Telnet Server	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	23	<input type="checkbox"/>	23	
SSH	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	22	<input type="checkbox"/>	22	
SNMP	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	161	<input type="checkbox"/>	161	
GRE	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
Dynamic routing	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
DNP3	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
IPsec VPN	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
Serial Server	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
Respond to ICMP (Ping)	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
Reset						Update	

Internal services use the standard port numbers for the service type. For example, port 80 is used for the web server. It is possible to change the port number for a particular service but take care not to create a conflict with the other services.

FIREWALL

Access Control Examples

Firewall > Access Control

Example 1 – Allow access to all internal services on the wireless interface.

At the top of the **WLS** column, set the **Default Policy** to **Allow**.

NB: Note that each service in the WLS column will be given a tick and greyed out.

Status System Wireless Network Routing Firewall VPN Serial Server Management
 Setup Access Control DoS Filters Custom Filters Port Forwards Custom NAT MAC Filters

Logged in as admin Host: MRD-455

Access Control

External Access Control	Incoming Interface					
	WLS		VPN		GRE	
Default policy	Allow ▾		Allow ▾		Deny ▾	
Services	Allow	Port	Allow	Port	Allow	Port
Web Server	<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	80	<input type="checkbox"/>	80
Secure Web Server	<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	443	<input type="checkbox"/>	443
Telnet Server	<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	23	<input type="checkbox"/>	23
SSH	<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	22	<input type="checkbox"/>	22
SNMP	<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	161	<input type="checkbox"/>	161
GRE	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
Dynamic routing	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
DNP3	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
IPsec VPN	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
Serial Server	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
Respond to ICMP (Ping)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
Reset						Update

Example 2 – Allow only web access to all internal services on the wireless interface.

At the top of the **WLS** column, set the **Default Policy** to **Block**.

In the **Allow** column, tick the Web Server option and enter port 80.

Status System Wireless Network Routing Firewall VPN Serial Server Management
 Setup Access Control DoS Filters Custom Filters Port Forwards Custom NAT MAC Filters

Logged in as admin Host: MRD-455

Access Control

External Access Control	Incoming Interface					
	WLS		VPN		GRE	
Default policy	Deny ▾		Allow ▾		Deny ▾	
Services	Allow	Port	Allow	Port	Allow	Port
Web Server	<input checked="" type="checkbox"/>	80	<input checked="" type="checkbox"/>	80	<input type="checkbox"/>	80
Secure Web Server	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	443	<input type="checkbox"/>	443
Telnet Server	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	23	<input type="checkbox"/>	23
SSH	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	22	<input type="checkbox"/>	22
SNMP	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	161	<input type="checkbox"/>	161
GRE	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
Dynamic routing	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
DNP3	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
IPsec VPN	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
Serial Server	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
Respond to ICMP (Ping)	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>	
Reset						Update

Custom NAT

1-to-1 NAT

1-TO-1 NAT enables you to forward **all** IP traffic destined for one IP addresses and translate it to another IP address on the private network behind a router.

For example, if a network has an internal devices on the LAN, 1-to-1 NAT can map your outside IP addresses to provided by your ISP to the IP addresses of the servers.

When you enable 1-to-1 NAT on an interface, the router routes all incoming packets to a specified IP addresses and forwards it to another IP address specified in the NAT rule.

When you select NAT type **1:1** the following options will be available.

Incoming interface

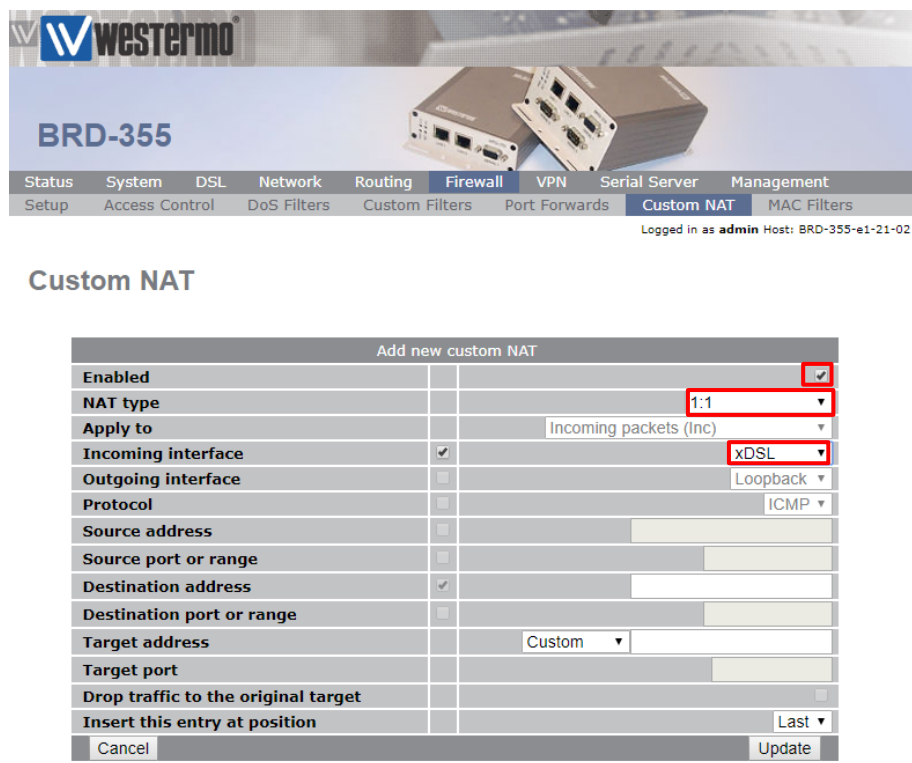
If selected, packets will be matched based on the network interface they have been received on. Note that this can only be applied to a Destination NAT on Incoming packets.

Destination address

Enter a single IP address. Only packets matching this destination address will have the filter applied to them.

Target address

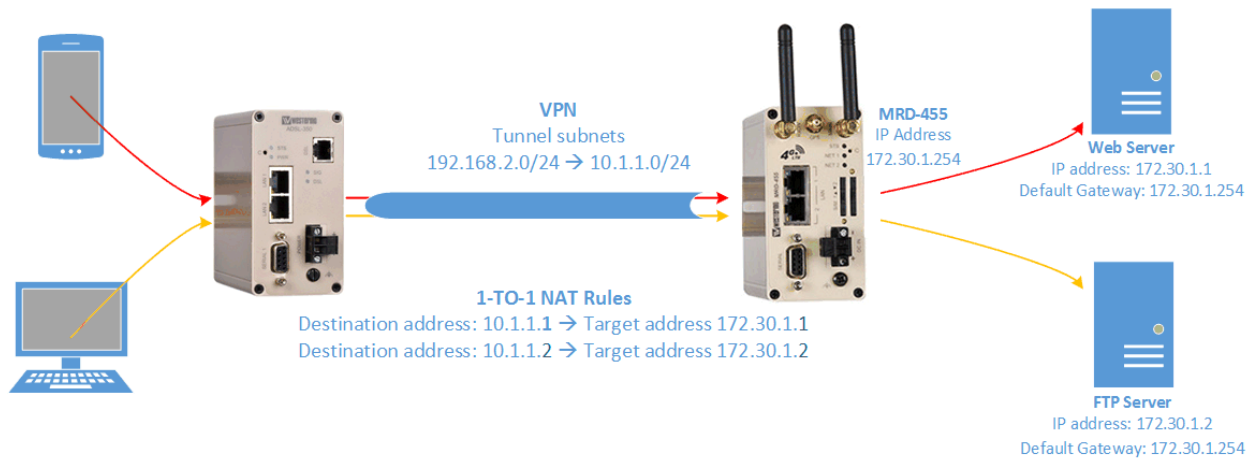
This is the IP address that the NAT rule will apply and forward packets to. When set to Custom, any IP address can be entered in the text box. If an interface is selected from the dropdown box, the current address of that interface will be applied to packets.



Custom NAT Example 1

1-to-1 NAT and IPSec VPN

1-to-1 NAT is useful if you have several remote outstations connected by VPN's, where devices at each outstation have been pre-programmed with the same IP addresses on each site. 1-to-1 NAT enables you receive packets for IP addresses on the VPN subnet and forward them to the real IP addresses on the LAN subnet.



Browse to Firewall → Custom NAT.

NAT type: 1:1



Custom NAT

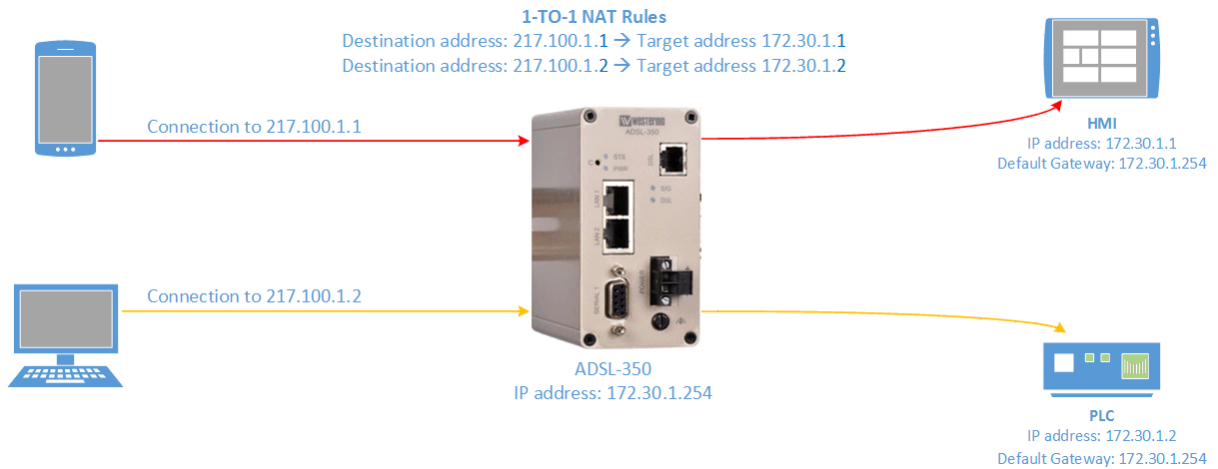
Editing custom NAT 1	
Enabled	<input checked="" type="checkbox"/>
NAT type	1:1
Apply to	Incoming packets (Inc)
Incoming interface	<input checked="" type="checkbox"/> Any IPsec
Outgoing interface	<input type="checkbox"/> LAN
Protocol	<input type="checkbox"/> TCP
Source address	<input type="text"/>
Source port or range	<input type="text"/>
Destination address	<input checked="" type="checkbox"/> 10.1.1.1
Destination port or range	<input type="text"/>
Target address	Custom 172.30.1.1
Target port	<input type="text"/>
Drop traffic to the original target	<input type="checkbox"/>
Insert this entry at position	1
<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

Custom NAT Example 2

1-to-1 NAT

Access to Private Devices from the Internet.

If your broadband link has a static public IP address, or a range of static public IP addresses, you can use your router to terminate the DSL line but use 1-to-1 NAT to forward traffic for each of the public IP addresses to a device, (such as a PLC), on the private LAN subnet. I.e. to give access to a private web server.



Browse to Firewall → Custom NAT.

NAT type: 1:1



Custom NAT

Add new custom NAT	
Enabled	<input checked="" type="checkbox"/>
NAT type	1:1
Apply to	Incoming packets (Inc)
Incoming interface	xDSL
Outgoing interface	Loopback
Protocol	ICMP
Source address	
Source port or range	
Destination address	217.100.1.1
Destination port or range	
Target address	Custom 172.30.1.1
Target port	
Drop traffic to the original target	<input type="checkbox"/>
Insert this entry at position	Last
<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

Custom NAT

Destination NAT

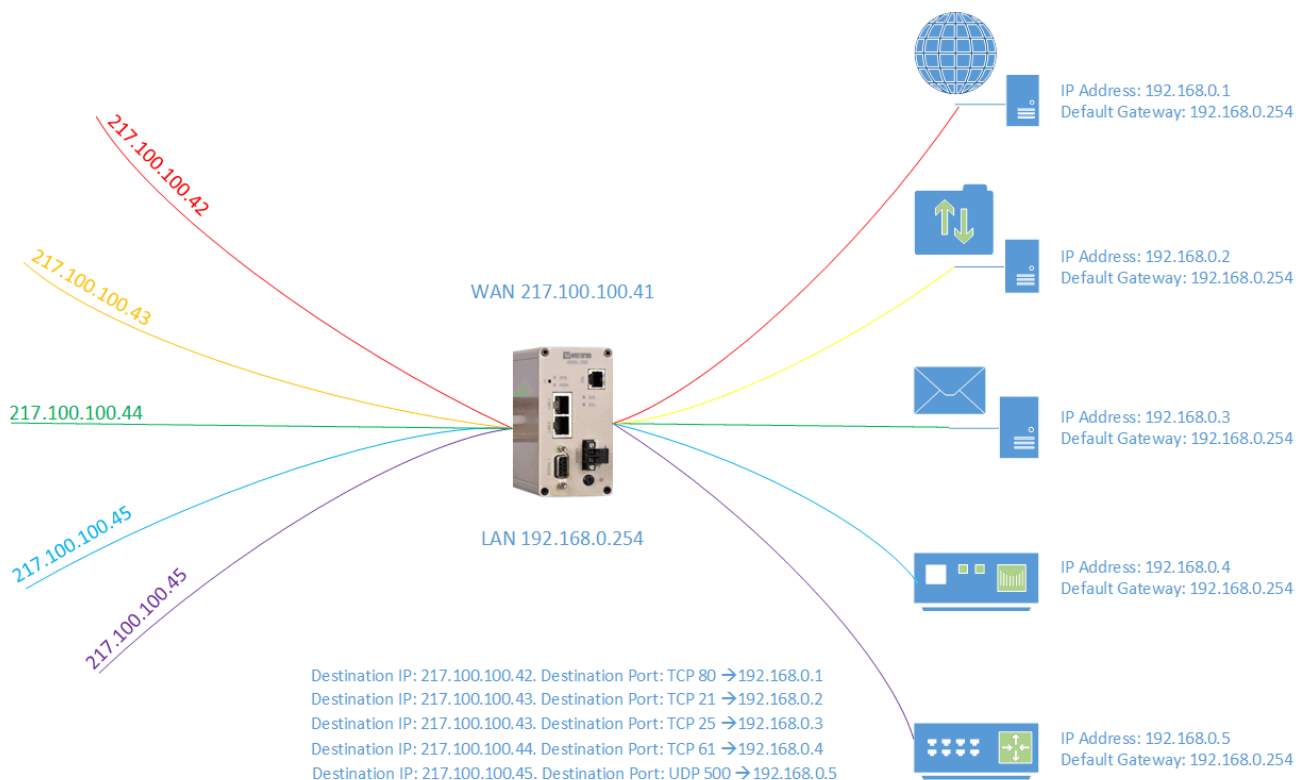
Destination NAT translates traffic to 1 IP address and changes the destination IP address so that the traffic is routed to another device.

Destination NAT is similar to the 1-to-1 NAT except it gives more options when filtering traffic. For instance you can specify that the NAT rule only applies to a certain protocol or traffic to a certain TCP/UDP port.

Example – NAT Public Addresses to Private Addresses.

In this example, the Westermo BRD-355 router holds 6 static BT broadband IP addresses. Using **Destination NAT** rules, traffic will be routed to various devices on the private LAN depending on which broadband IP address (and in some cases which TCP/UDP port), is connected to.

Browse to **Firewall → Custom NAT**.
NAT type: **Destination NAT**.



Custom NAT

Destination NAT

The following settings apply to incoming traffic on the DSL link (xDSL).

The destination NAT rule will translate IKE Packets, (UDP port 500), with an original destination IP address of 217.100.100.45, change the destination IP address and forward the packets to the VPN Concentrator with IP address 192.168.0.5.

NB: See the last link example from the drawing on the previous page.



Custom NAT

Add new custom NAT	
Enabled	<input checked="" type="checkbox"/>
NAT type	Destination NAT ▾
Apply to	Incoming packets (Inc) ▾
Incoming interface	<input checked="" type="checkbox"/> xDSL ▾
Outgoing interface	<input type="checkbox"/> Loopback ▾
Protocol	<input checked="" type="checkbox"/> UDP ▾
Source address	<input type="checkbox"/>
Source port or range	<input type="checkbox"/>
Destination address	<input checked="" type="checkbox"/> 217.100.100.45
Destination port or range	<input checked="" type="checkbox"/> 500
Target address	Custom ▾ 192.168.0.5
Target port	<input type="checkbox"/>
Drop traffic to the original target	<input type="checkbox"/>
Insert this entry at position	Last ▾
<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

Custom NAT

Source NAT

Source NAT is useful where it is not possible to set a Default Gateway in devices connected to the router’s LAN, but you need to have remote access to them.

In this situation we are able to use Source NAT function where the source IP address of incoming packets is changed so that the packets appear as if they are coming from the router’s local LAN interface.

NB: Source NAT only helps with inbound remote access connections to devices on the LAN that don’t have a Default Gateway set. It does not allow these devices to connect in an outbound direction to the internet.

Example 1 – Catch ALL Source NAT

NB: If you are using a **Destination NAT** rule to gain remote access, make sure the **Source NAT** rule comes *after* the destination NAT rule.

This example changes the source IP address to the router’s LAN address for all traffic leaving the LAN interface.

NB: Use this ‘catch all’ rule carefully. If there are any devices on the LAN that are using the router as it’s Default Gateway, it will stop their outbound connections to the internet from working because the reply packets will have their source address changed. If you have a mixture of devices on the LAN with and without Default Gateways set, it is better to use a more selective rule as shown on page 9.

Browse to **Firewall → Custom NAT**.
 NAT type: **Source NAT**.



Custom NAT

Add new custom NAT	
Enabled	<input checked="" type="checkbox"/>
NAT type	Source NAT
Apply to	Incoming packets (Inc)
Incoming interface	Loopback
Outgoing interface	LAN
Protocol	ICMP
Source address	
Source port or range	
Destination address	
Destination port or range	
Target address	LAN
Target port	
Drop traffic to the original target	<input type="checkbox"/>
Insert this entry at position	Last
<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

Custom NAT

Source NAT

Example 2 – Apply Source NAT to Connections to a Specific Device IP Address.

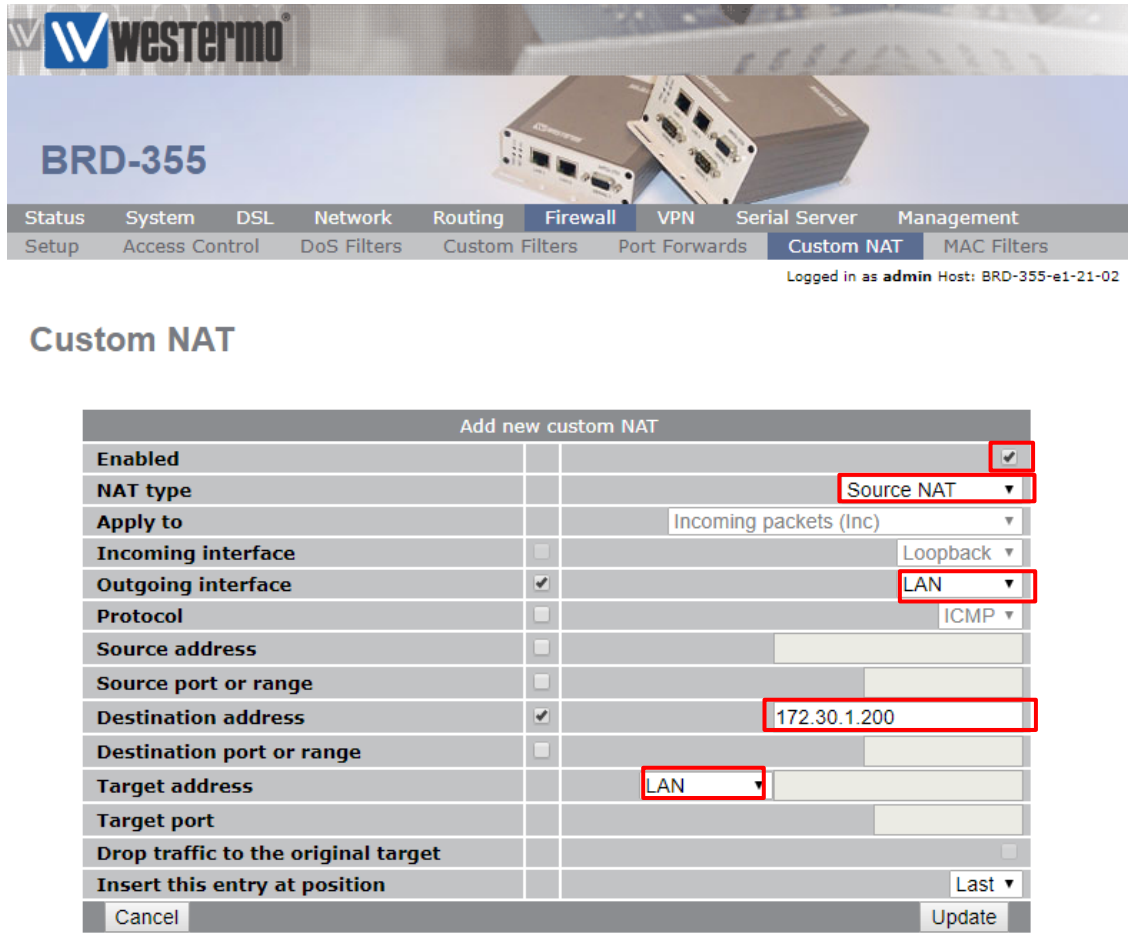
NB: If you are using a **Destination NAT** rule to gain remote access, make sure the **Source NAT** rule comes *after* the destination NAT rule.

This Source NAT example targets traffic to a specific IP address. This is useful when a only a specific device does not have a default Gateway set, or if it uses another Default Gateway for most of it's external traffic.

This rule changes the source IP address of any traffic leaving the LAN port to whichever is the LAN IP address of the router, but only where the destination IP address is 172.30.1.200. Any external traffic to this IP address will appear to originate from the router.

NB: Instead of specifying a destination IP address, you can specify traffic to a specified subnet (e.g. 172.30.1.0/24).

Browse to **Firewall → Custom NAT**.
 NAT type: **Source NAT**.



Port Forwards

Same Port End to End

A port forward is a way of making a device on a private LAN network accessible from the internet, even though they are behind a router or firewall.

It specifically applies to devices running a particular service. For example port forwarding is commonly used for accessing a web server, or for security camera's and for file sharing. Port forwarding is a more secure way of giving limited access to a device or server, as it only allows connections to specified services listening on certain ports.

After you have forwarded a port it is said to have an open port.

Example 1 - The following rule applies to incoming traffic in the DSL interface. It forwards all incoming TCP port 80 traffic to a Web server on the private network.



Port Forwards

Add new port forward	
Enabled	<input checked="" type="checkbox"/>
Protocol	TCP
Incoming interface	xDSL
Source address (blank for any)	
Original destination port or range	80
New destination address	192.168.0.1
New destination port (blank to use original port)	
Insert this entry at position	Last
<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

Port Forwards

Changing the Destination Port.

The port forwarding function allows traffic to be filtered on a certain destination port number as shown in the previous example. But it's also possible to then change the destination port number when forwarding the traffic to an IP address on the private network.

For instance, web servers generally use TCP port 80 for their web service. It's possible to confuse port scanners on the internet searching for a hidden web server by setting the port forwarding rule to listen on an unrelated port number (e.g. 5555). That traffic could then be forwarded using the standard TCP port 80 and sent to the web server on the private LAN.

Example 2 - The following rule applies to incoming traffic in the DSL interface. It forwards all incoming TCP port 5555 traffic to a Web server on the private network but changes the destination port to TCP port 80.



Port Forwards

Add new port forward	
Enabled	<input checked="" type="checkbox"/>
Protocol	TCP
Incoming interface	xDSL
Source address (blank for any)	
Original destination port or range	5555
New destination address	192.168.0.1
New destination port (blank to use original port)	80
Insert this entry at position	Last
<input type="button" value="Cancel"/> <input type="button" value="Update"/>	

Firewall

Custom Filters

The Custom Filter area is where the firewall's packet filter is configured to either allow or deny IP packets based on certain criteria. Packets can be matched based on the router's inbound or outbound network interface, the protocol, the source or destination addresses and ports.

The following options are available for each custom filter.

Enabled: Set the enabled check box to have the rule installed in the firewall. A rule can be temporarily disabled by unchecking this box.

Apply to Custom filters can be applied at three separate points in the router:

- **Forwarded packets:** This filter applies to packets that are received from one network interface and then routed out another network interface.
- **Locally destined packets:** This filter applies to packets destined for the router's internal services.
- **Locally generated packets:** This filter applies to packets generated by one of the router's internal services.

Incoming interface: If selected, packets will be matched based on the network interface they have been received on.

Outgoing interface: If selected, packets will be matched based on the network interface they will be transmitted from.

Protocol: If selected, packets will be matched based on their protocol type. To filter on a specific source or destination ports, the protocol must be set to TCP or UDP.

Source address: If selected, enter either a single address (e.g. 192.168.0.1) or a subnet range (e.g. 192.168.0.0/24). Only packets matching this source address/subnet will have the filter applied to them.

Source port or range: If selected, packets will be matched based on their TCP or UDP source port. Specify either an individual port (e.g. 443) or a port range (e.g. 80-143).

Destination address: Similar to the Source address, but instead matching on the destination address.

Destination port or range: Similar to the Source port or range, but instead matching on the destination port.

Action: Determines what action on packets who meet all of the matching criteria for the filter. If set to Deny, the packet will be dropped. If set to allow, the packet will be passed.

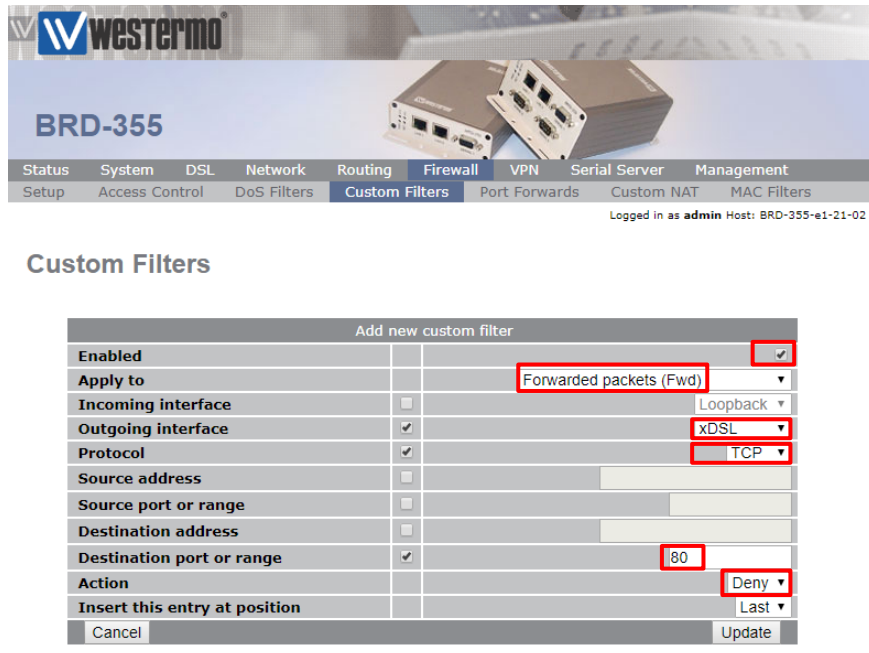
Insert this entry at position: Determines where this entry will be inserted in the list of custom filters. Rules are applied in order from top to bottom.

Firewall

Custom Filters – Block Outbound Traffic

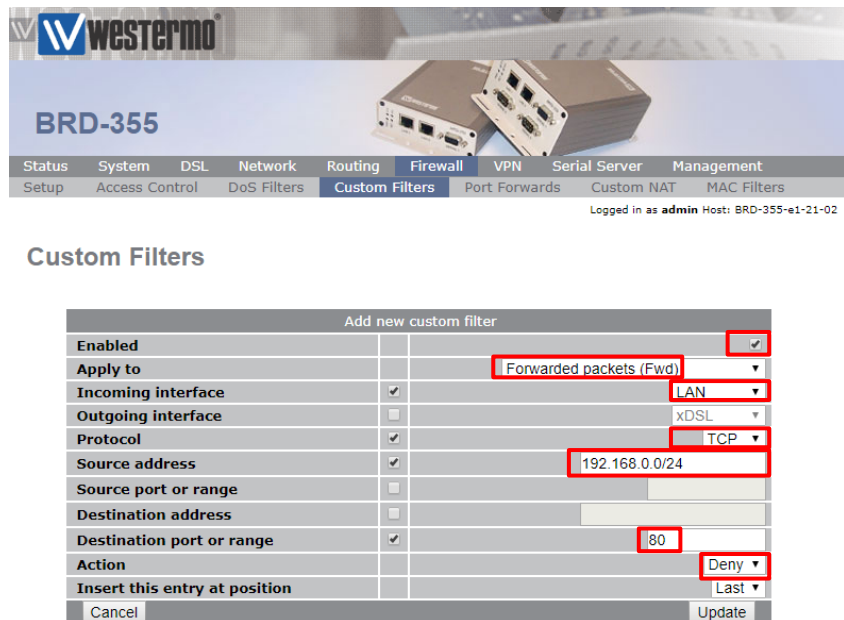
Example 1.

The following packet filter blocks all outbound http traffic by denying port 80 traffic on the outgoing DSL interface.



Example 2.

The following packet blocks all http traffic for any device specifically on the 192.168.0.0/24 network.



NB: Notice that unlike example 1, the packet filter is this time applied to the incoming LAN interface and not the outbound DSL interface. This is because the rule is designed to block web access from PC's on the LAN subnet. The rule can not be applied to the outside interface, because traffic leaving the DSL port will have NAT applied to it which changes the source address to that of the broadband IP address. Therefore to the packets would not match the firewall rule.

Firewall

MAC Address Filtering

All IP (Internet Protocol) enabled devices have a network interface with a unique Media Access Control (MAC) address assigned to it. It is sometimes known as the hardware or physical address.

Using MAC address filtering, the MAC address can be filtered to either allow or deny a device access either to the router itself or access to another network.

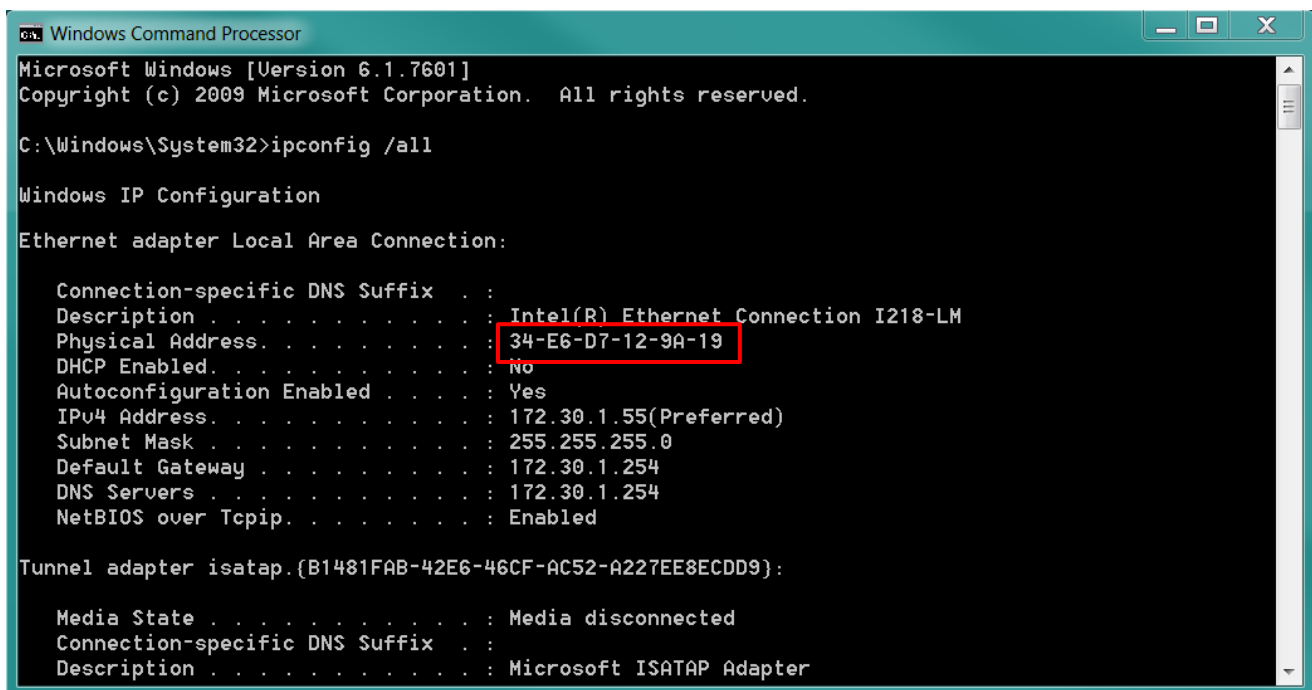
Communications between IP devices on a LAN (Local Area Network), are actually sent between MAC addresses. The IP address on a local network is only used to establish which device's MAC address owns the IP address. Therefore unlike the previous sections, this type of communication is at the Ethernet / Data link level (Layer 2 of the OSI Model) rather than at Network Level (Layer 3).

NB: While providing a certain level of protection, MAC Filtering can be circumvented by an attacker scanning the network for a valid MAC. Someone with sufficient knowledge can then change the MAC address of their device and gain access to the network. Therefore if access to the LAN interface of an ADSL-350 or MRD router is to be restricted, MAC address filtering should not be used as the only form of security.

Locating the MAC address.

On a Windows PC open the Command Line Interface and run the command `ipconfig /all`.

The MAC address (Physical address) will be listed for each of the network interfaces.



```
Windows Command Processor
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>ipconfig /all

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Intel(R) Ethernet Connection I218-LM
    Physical Address. . . . . : 34-E6-D7-12-9A-19
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 172.30.1.55(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.30.1.254
    DNS Servers . . . . . : 172.30.1.254
    NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{B1481FAB-42E6-46CF-AC52-A227EE8ECDD9}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
    Description . . . . . : Microsoft ISATAP Adapter
```

Firewall

MAC Address Filtering – Example

The following example by default allows all passthrough traffic but denies all access to the router interface from the LAN.

The MAC filter however allows local access to the router web interface from a laptop with MAC address **34-E6-D7-12-9A-19**. This is useful if administration of the router should only be possible from certain PC's or Laptops etc.

NB: The MAC address format uses a : (colon) as the delimiter. So if the MAC address is listed as **34-E6-D7-12-9A-19** on your device, the format should be changed to **34:E6:D7:12:9A:19** (not case sensitive).





MAC Filters - LAN

Add new MAC filter	
Enabled	<input checked="" type="checkbox"/>
Source MAC address	34:e6:d7:12:9a:09
Passthrough action	Allow ▾
Local action	Allow ▾
Insert this entry at position	Last ▾
Cancel	Update



MAC Filters - LAN

Default Policy (Apply to undefined MAC Addresses)	
Passthrough action	Allow ▾
Local action	Deny ▾
Update	

Enabled	MAC Address	Passthrough	Local	Edit	Delete
<input checked="" type="checkbox"/>	34:e6:d7:12:9a:09	Allow	Allow		
Add new MAC filter					

Revision history for version 1.1

Revision	Rev by	Revision note	Date
00			
01	JM	Changed ADSL-350 to BRD-355. Also changed incorrect 'allow' rule on the in customer filters section, example 2. Should have read 'Deny'	29/11/18
02			
03			
04			
05			
06			
07			



H E A D O F F I C E

Sweden

Westermo
SE-640 40 Stora Sundby
Tel: +46 (0)16 42 80 00
Fax: +46 (0)16 42 80 01
info@westermo.se
www.westermo.com

Sales Units

Westermo Data Communications

China

sales.cn@westermo.com
www.cn.westermo.com

France

infos@westermo.fr
www.westermo.fr

Germany

info@westermo.de
www.westermo.de

North America

info@westermo.com
www.westermo.com

Singapore

sales@westermo.com.sg
www.westermo.com

Sweden

info.sverige@westermo.se
www.westermo.se

United Kingdom

sales@westermo.co.uk
www.westermo.co.uk

Other Offices



For complete contact information, please visit our website at www.westermo.com/contact or scan the QR code with your mobile phone.