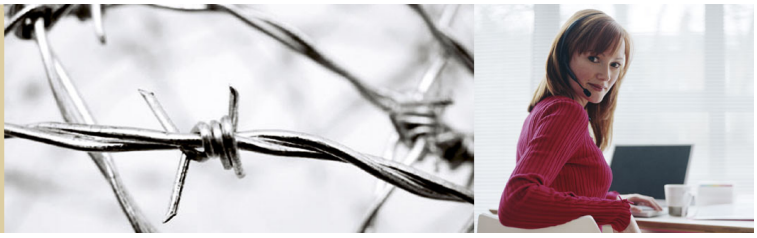
Application Note

Working with Advisory Routing with Dual WAN



2006-09-05

rev.01

Table of Contents:

1 Scope

This document will give you an introduction to Advisory Routing. This feature has been implemented as of release 9.3 / build 6271 for all Dual WAN appliances, such as TrustGate363R and TrustGate5 Model 33.

2 Background

To understand this document you need to be familiar with TrustGate Firewall/VPN appliances, especially the Firewall (Forwarding) and Routing (not least NAT).

3 What is Advisory Routing?

Advisory Routing (Routing > Advisory Routing) lets you specify rules for forwarding packets through a specific interface.

For example, you can make a rule stating that SMTP traffic should be forwarded through the WAN2 interface.

The rules are "advisory" in the sense that the system is free to disregard them for some reason. They are positioned very low in the routing decision hierarchy, just above the default routes, and they only affect forwarded packets (that is, not packets originating from the appliance itself).

Static routes, tunnels, and local networks all have higher priority than advisory routing rules.

In addition, advisory rules are disregarded if their interface is down. For example, if the WAN2 interface (or its link to the ISP) is down, and you've created a rule stating that SMTP should be forwarded through WAN2, that rule will be disregarded, and the packets will be forwarded through the WAN interface. If you don't want that to happen, you can make a forwarding firewall rule blocking SMTP with "Outgoing Interface" = WAN.

The rules are traversed from top to bottom. The first rule to match will terminate the traversal.

4 Scenarios

Why do we need the Advisory Routing in the first place?

If your Dual WAN appliance is using WAN load balancing (*) you won't know what interface (WAN or WAN2) the appliance will send from the next time. That's the whole idea of load balancing – both interfaces are in use.

But if you want to send from one specific interface like WAN2 and not WAN you will need Advisory Routing.

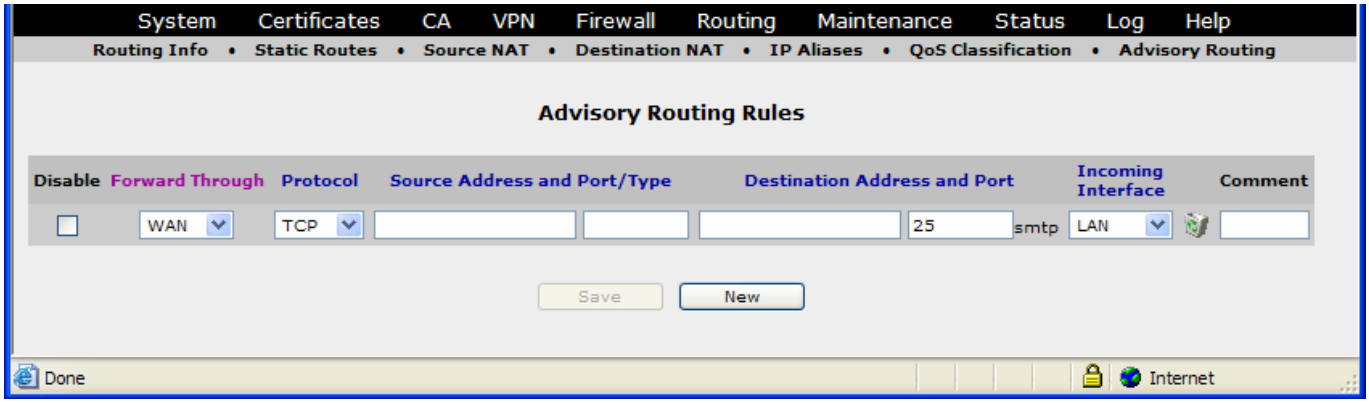
> *(*)-You get the same problem if the appliance is using Failover. You don't know what interface is active. Is it the default WAN interface that is active or has it already fallen over to WAN2?*

4.1 Scenario 1 - Mail restricted to WAN(1)

It is often seen that mails sent from WAN2 is blocked as spam mail on certain services on the internet. This can have several reasons; a common one is that reverse DNS is not supported for the WAN2 IP address (*). An easy way to overcome this problem is to send mail only from the WAN interface.

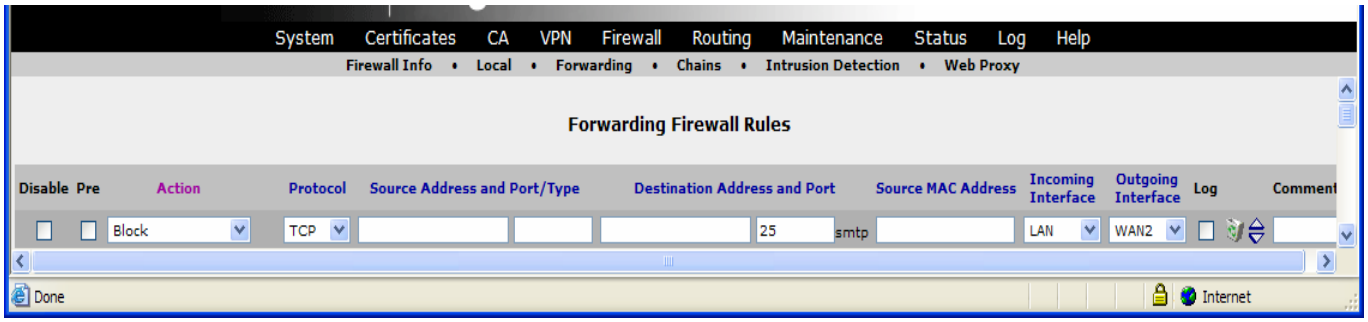
> *(*) -. It is normally your ISP or your IP provider that is responsible for creating an rDNS record for your IP address. For more information, search for rDNS or Reverse DNS on the Internet.*

Figure 1 Mails only from WAN interface:



With this Advisory Routing rule, SMTP (Mail) will only be forwarded on the WAN interface – unless WAN is down, in which case mail traffic will be forwarded on WAN2. If you don't want this to happen, add the following rule to the firewall (forwarding):

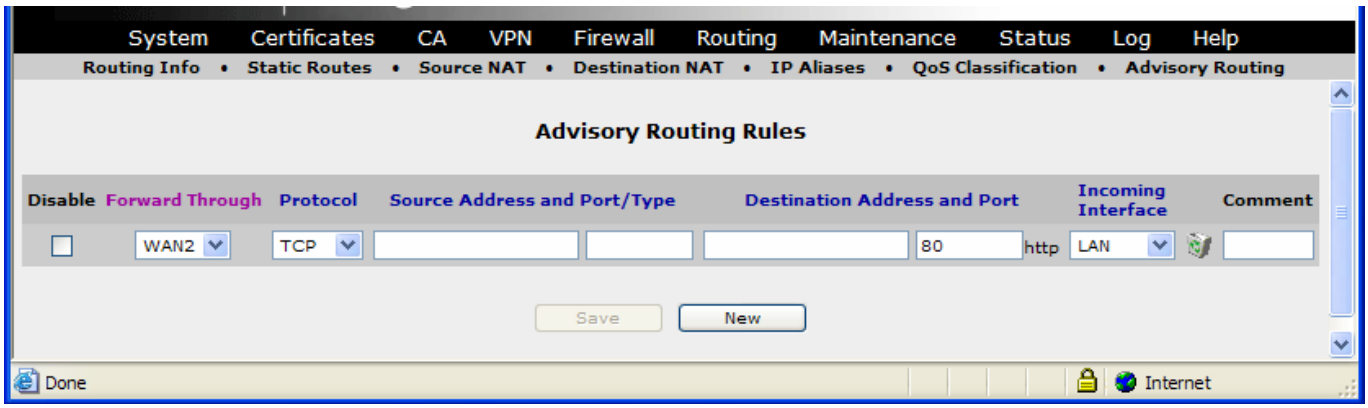
Figure 2 Block all mail traffic on WAN2 if WAN is down



4.2 Scenario 2: Restrict user's Web traffic to WAN2

To restrict Web browsing to WAN2, add the following Advisory Routing rule:

Figure 3 Users' WEB traffic is moved to WAN2



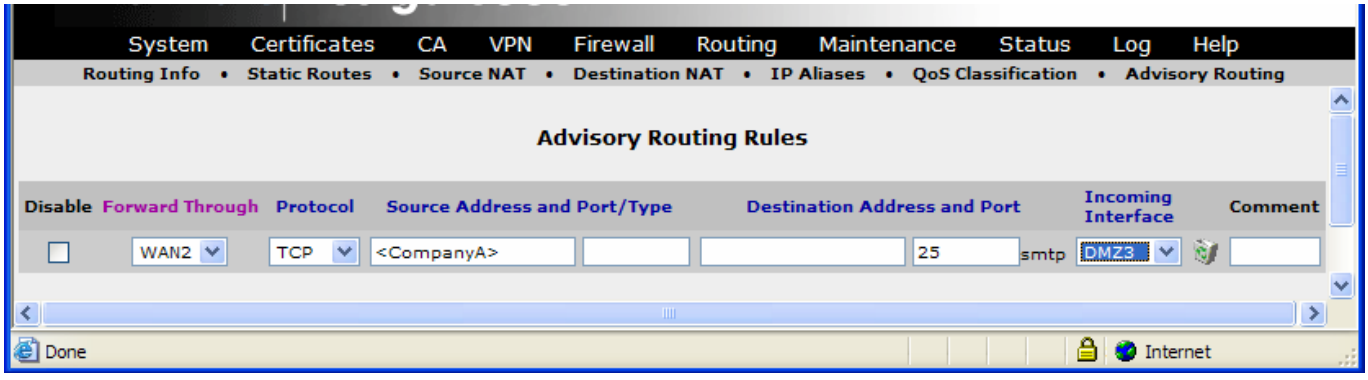
4.3 Scenario 3: Hosting service on IP Alias for WAN2

You are hosting a server for CompanyA and have created an IP-Alias for this company on WAN2. All Web traffic coming from the outside to this IP-Alias will also be responded to using this alias. That is, of course, how it is supposed to be.

But if you also want to do some mail exchange initiated from the hosted CompanyA server, you need to force the server to use WAN2 using an Advisory Routing rule. Normally, outgoing traffic will use WAN (default interface) or both WAN and WAN2 if the TrustGate is using WAN load balancing, and this will make it seem as if the traffic is coming from an unknown IP-address.

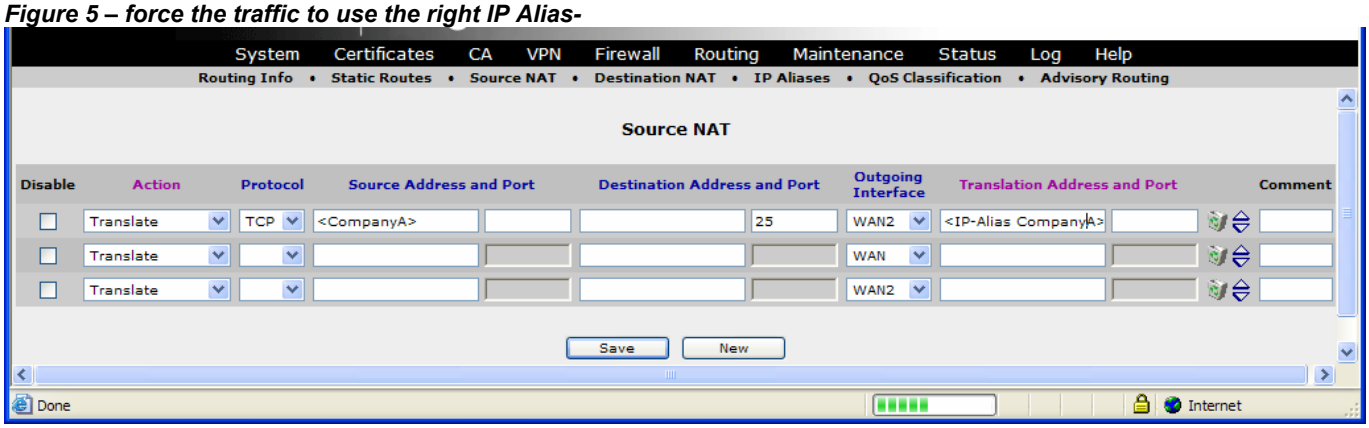
The following Advisory Routing rule ensures that all port 25 (mail) traffic from this server will be advised to use WAN2. With this rule – or a combination of this rule and the Source NAT rule (see below) – we ensure that when mail exchange is sent from local CompanyA server it will use the right IP-address.

Figure 4 CompanyA mail exchange if forced to use WAN2



To complete the configuration, add an additional Source NAT rule that forces traffic to the IP-Alias for CompanyA. (The two default Source NAT rules should be left as they are).

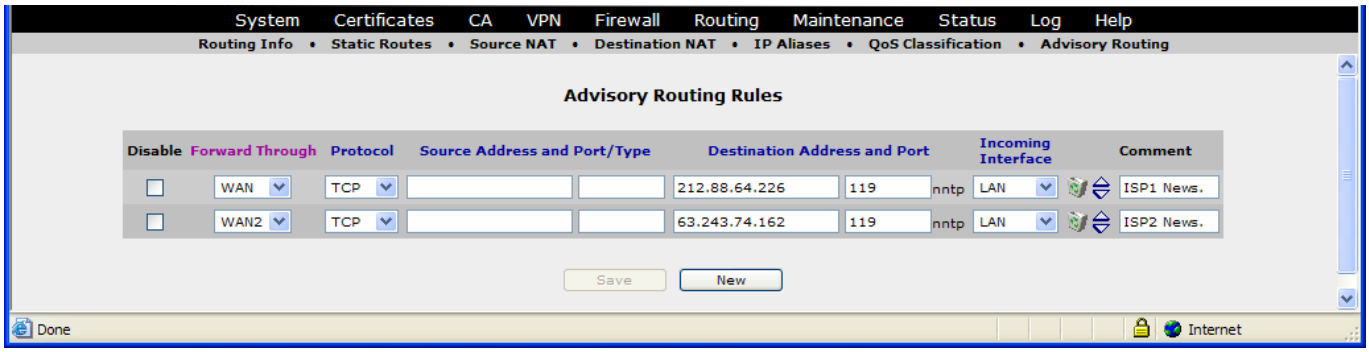
Figure 5 – force the traffic to use the right IP Alias-



4.4 Scenario 4: Additional NEWS provider

You have two different Internet Service Providers, ISP1 on WAN and ISP2 on WAN2. Each provider has a NEWS service, but unfortunately neither of them allows anyone except their own customers to access its NEWS server. That means that if you try to access NEWS server ISP1 from WAN2 you will get access denied. To solve this problem, make an Advisory Routing Rule for each provider's service.

Figure 6 Traffic from each 'NEWS provider is directed to a different WAN interface



5 Notices

5.1 Websites and support

support@secomea.com

Corporate website: www.secomea.com

Product support portal: http://www.secomea.com/Service-and-Support-85.aspx

5.2 Trademarks and copyrights

Trademarks: TrustGate5 and TrustGate363R are trademarks of Secomea A/S.

Other trademarks are the property of their respective owners.

5.3 Disclaimer

Secomea A/S reserves the right to make changes to this document and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S.

Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions.but we can not guarantee that there are none.

The following paragraph does not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

Secomea A/S shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.