

The SpeedTouch™ and Firewalling

Author: Sascha Peckelbeen, Peter Huyge

Date: June 2003

Edition: v1.0

Abstract: This application note provides technical Firewall information and how this relates to the SpeedTouch™ 600 Business DSL Routers. A brief background on the capabilities of the SpeedTouch™ Firewall is presented. The subsequent sections give detailed explanation on example setups clarifying the features and capabilities of the SpeedTouch™ within the context of a secure network.

Applicability: This application note applies to all Release R4.2 SpeedTouch™ 600 Business DSL Routers.

Updates: Due to the continuous evolution of DSL technology, existing products are regularly improved. For more information on the latest technological innovations, software upgrades, and documents, please visit the SpeedTouch™ web site at:

<http://www.speedtouch.com>

1 INTRODUCTION

Network Security is about assuring a chain of well configured security measures. If you want to surf the Internet and don't want to allow peeking eyes at your host system or if you have to setup your extranet Web server to allow specific customers, a good configured firewall should help you with the first steps of that secure environment.

A warning though, security is as weak as the weakest link. So even if you follow the example setups described in this technical paper, the security of your network is something that depends on the security of your OS, Web server, Virus scanner and even your users.

Firewalls come in different flavors and each one has its weaknesses and strengths. The SpeedTouch™ is equipped with a very flexible and performing packet firewall. This paper will guide you through the basic parameters of the SpeedTouch™ Firewall and will discuss some real world examples with basic comments on the choices made for those specific setups.

2 BASIC CONCEPTS

The Packet Firewall has the ability to decide if a certain packet transported through the SpeedTouch™ is allowed to pass a certain boundary. The decisions are made based on a set of rules. Those rules define very rigorous what the Firewall should search for in the packets that pass by.

Lets take a look at the basic information fields that the SpeedTouch™ Firewall can make decisions on. The zones of influence range from the Internet Layer to the Host to host Layer as depicted in the figure and are defined to match certain values in the definition of the Firewall rule.

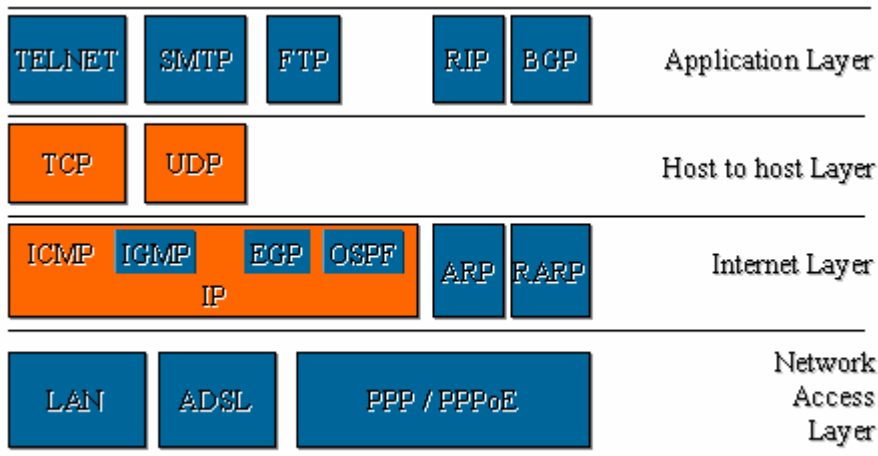


Figure 1 Zones of Influence

So decisions to drop, deny, allow a packet can be based on a combination of TCP, UDP, ICMP, IP or Interface combinations.

The next figure shows all the IP header parameters that the Firewall can search a match for. The Source and Destination address are obvious, but also specific IP protocols can be allowed or dropped because the Protocol field is also inspected. E.g. IP Protocol ICMP could be the target of a specific rule.

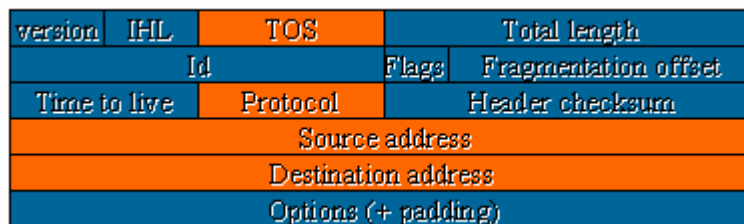


Figure 2 IPv4 Header Zones of Influence

ICMP itself has some extra zone of influence. The best known is the ICMP Echo type that is used by a simple ping. But total freedom is given for defining the best ICMP policy for the firewall. E.g. Allow outgoing ICMP Echo Request and incoming ICMP Echo Reply could be a useful rule for a LAN to Wan rule.



Figure 3 ICMPv4 Header Zones of Influence

The TCP and UDP protocol, the most common IP protocols on the Internet have also a nice list of items that can be combined. The examples that follow in the next chapters will demonstrate the power of good chosen combinations of these parameters.

| | | | |
|------------------------|----------|------------------|--------|
| Source port | | Destination port | |
| Sequence number | | | |
| Acknowledgement number | | | |
| Offset | Reserved | Window | Window |
| checksum | | Urgent pointer | |
| Options | | | |

Figure 4 TCPv4 Header Zones of Influence

| | |
|----------------|------------------|
| Source port | Destination port |
| Message length | checksum |

Figure 5 UDPv4 Header Zones of Influence

One Firewall rule with a certain combination of the previous parameters will probably not be enough to handle the decisions that the Firewall will have to make, even for the configuration of a standard Internet surfer.

Multiple Firewall rules will eventually define a complete Firewall behavior where most users should be comfortable with. These rules will be combined in a specific order in a so-called Firewall rule chain, or in short a chain. Combining these rules in chains makes it easier to manage switching between different configurations using the defined chains. Another reason is also that different points in the Firewall can attach different chains of rules. E.g. different rules act on packets that come into the SpeedTouch™ and other rules act on packets that leave the SpeedTouch™. Those different points are called hook points. The SpeedTouch™ has five off these hook points.

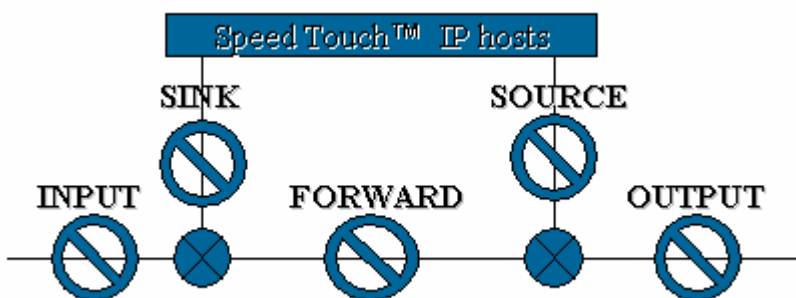


Figure 6 Hook points

To summarize, a rule is a combination of zone of influence parameters combined in a specific order in a chain where that chain is hooked on one of the five hook points, hook points that are strategic located in the SpeedTouch™ IP stack.

3 BASIC DEFAULT FIREWALL

By default following rules and chains are defined in the SpeedTouch™ 610Series:

3.1.1 The sink hook rules

```

:firewall rule create chain=sink index=0 srcintfgrp=!wan action=accept
:firewall rule create chain=sink index=1 prot=udp dstport=dns action=accept
:firewall rule create chain=sink index=2 prot=udp dstport=bootpc action=accept
:firewall rule create chain=sink index=3 prot=udp dstport=sntp action=accept
:firewall rule create chain=sink index=4 prot=icmp icmptype=echo-reply action=accept
:firewall rule create chain=sink index=5 prot=icmp icmptype=destination-unreachable action=accept
:firewall rule create chain=sink index=6 prot=icmp icmptype=time-exceeded action=accept
:firewall rule create chain=sink index=7 prot=udp dstport=snmp log=yes action=count
:firewall rule create chain=sink index=8 prot=udp dstport=rip log=yes action=count
:firewall rule create chain=sink index=9 action=drop

:firewall assign hook=sink chain=sink
    
```

The first rule is very specific for the SpeedTouch™. The first rule indicates the firewall to allow only incoming packets to flow through the sink to the IP host of the SpeedTouch™ if they come from the not WAN interfaces.

The remaining udp rules are added to allow correct functioning of the dns forwarding, dhcp client functionality and the network time protocol. The icmp rules are added to allow correct functioning of the :ip traceroute functionality and to allow the Speedtouch™ to ping hosts on the WAN.

The rules concerning RIP and SNMP only counts packets, this is because those services are disabled for the WAN by default; but by logging incoming messages a wrong network configuration can be spotted by looking at the syslog messages. The user is also reminded in this way that when he activates one of those services on a WAN interface he also has to allow it explicitly by adding a firewall rule.

All other traffic towards the SpeedTouch™ IP host is dropped.

The following command will show the statistics of the packets that passed specific rules in the chains:

```
=>firewall rule stats chain=sink
Chain , index 0, packets 3148, bytes 535352
Chain , index 1, packets 0, bytes 0
Chain , index 2, packets 0, bytes 0
Chain , index 3, packets 0, bytes 0
Chain , index 4, packets 0, bytes 0
Chain , index 5, packets 0, bytes 0
Chain , index 6, packets 0, bytes 0
Chain , index 7, packets 0, bytes 0
Chain , index 8, packets 0, bytes 0
Chain , index 9, packets 0, bytes 0
=>
```

3.1.2 The forward hook rules

```
:firewall rule create chain=forward index=0 srcintfgrp=wan dstintfgrp=wan action=drop
:firewall assign hook=forward chain=forward
```

By default WAN to WAN traffic is not allowed. Spoofed packets arriving from a WAN port that would have been rerouted to a WAN port are dropped with this rule.

In contrast to the sink and source hooks, the default firewall configuration does not inject a drop rule in the forward hook. As a consequence the default firewall permits any traffic from the WAN to the LAN and vice versa. In case this behavior is not desired, a drop rule must be inserted in the forward hook, preceded by additional accept rules for all traffic that should be allowed to pass.

3.1.3 The source hook rules

```
:firewall rule create chain=source index=0 dstintfgrp=!wan action=accept
:firewall rule create chain=source index=1 prot=udp dstport=dns action=accept
:firewall rule create chain=source index=2 prot=udp dstport=bootps action=accept
:firewall rule create chain=source index=3 prot=udp dstport=sntp action=accept
:firewall rule create chain=source index=4 prot=udp dstport=syslog action=accept
:firewall rule create chain=source index=5 prot=icmp icmptype=echo-request action=accept
:firewall rule create chain=source index=6 prot=udp dstport=33434 action=accept
:firewall rule create chain=source index=7 prot=udp dstport=rip log=yes action=count
:firewall rule create chain=source index=8 prot=udp dstport=snmptrap log=yes action=count
:firewall rule create chain=source index=9 prot=udp srcport=snmp log=yes action=count
:firewall rule create chain=source index=10 action=drop
:firewall assign hook=source chain=source
```

The source hook will look at all the packets being generated by the SpeedTouch™ IP Host. By default there is no restriction for the LAN. So everybody from the LAN, if authenticated, should be able to connect to the SpeedTouch™ for administrative configuration.

Again a couple of UDP ports are opened to allow dns, dhcp server, Syslog and ntp functionality; ICMP rules for traceroute and ping functionality. RIP and SNMP are again logged. All other packets will be dropped.

The two following chains are also defined by default but are not attached to any hook. They are there for an easy default firewall configuration if the SpeedTouch™ 610 is used in a VPN setup.

```
:firewall rule create chain=allow_ipsec_sink index=0 prot=udp dstport=ike action=accept
:firewall rule create chain=allow_ipsec_sink index=1 prot=ah action=accept
:firewall rule create chain=allow_ipsec_sink index=2 prot=esp action=accept
:firewall rule create chain=allow_ipsec_sink index=3 srcintfgrp=wan prot=tcp ack=yes action=accept
```

To use this “allow_ipsec_sink” chain it should be inserted before the drop action of the sink chain. The last “allow_ipsec_sink” chain rule maybe needs some explanation. Only IP TCP packets that have the ack flag set will be allowed to the SpeedTouch™ IP Host. So from the TCP 3-way-handshake only the second and third packets are allowed and so a setup of an incoming tcp connection is not allowed. Connection attempts that where initiated by the SpeedTouch™ 610 IP Host are although allowed.

```
:firewall rule create chain=allow_ipsec_source index=0 prot=udp dstport=ike action=accept
:firewall rule create chain=allow_ipsec_source index=1 prot=tcp action=accept
```

A same approach for these rules, they should be inserted before the drop action of the source hook.

To summarize, the complete listing of the default firewall rules with the VPN rules enabled and hooked.

```
:firewall rule create chain=allow_ipsec_sink index=0 prot=udp dstport=ike action=accept
:firewall rule create chain=allow_ipsec_sink index=1 prot=ah action=accept
:firewall rule create chain=allow_ipsec_sink index=2 prot=esp action=accept
:firewall rule create chain=allow_ipsec_sink index=3 srcintfgrp=wan prot=tcp ack=yes action=accept

:firewall rule create chain=allow_ipsec_source index=0 prot=udp dstport=ike action=accept
:firewall rule create chain=allow_ipsec_source index=1 prot=tcp action=accept

:firewall rule create chain=forward index=0 srcintfgrp=wan dstintfgrp=wan action=drop

:firewall rule create chain=sink index=0 srcintfgrp=!wan action=accept
:firewall rule create chain=sink index=1 prot=udp dstport=dns action=accept
:firewall rule create chain=sink index=2 prot=udp dstport=bootpc action=accept
:firewall rule create chain=sink index=3 prot=udp dstport=sntp action=accept
:firewall rule create chain=sink index=4 prot=icmp icmptype=echo-reply action=accept
:firewall rule create chain=sink index=5 prot=icmp icmptype=destination-unreachable action=accept
:firewall rule create chain=sink index=6 prot=icmp icmptype=time-exceeded action=accept
:firewall rule create chain=sink index=7 prot=udp dstport=snmp log=yes action=count
:firewall rule create chain=sink index=8 prot=udp dstport=rip log=yes action=count
:firewall rule create chain=sink index=9 action=drop

:firewall rule create chain=source index=0 dstintfgrp=!wan action=accept
:firewall rule create chain=source index=1 prot=udp dstport=dns action=accept
:firewall rule create chain=source index=2 prot=udp dstport=bootps action=accept
:firewall rule create chain=source index=3 prot=udp dstport=sntp action=accept
:firewall rule create chain=source index=4 prot=udp dstport=syslog action=accept
:firewall rule create chain=source index=5 prot=icmp icmptype=echo-request action=accept
:firewall rule create chain=source index=6 prot=udp dstport=33434 action=accept
:firewall rule create chain=source index=7 prot=udp dstport=rip log=yes action=count
:firewall rule create chain=source index=8 prot=udp dstport=snmptrap log=yes action=count
:firewall rule create chain=source index=9 prot=udp srcport=snmp log=yes action=count
:firewall rule create chain=source index=10 action=drop

:firewall assign hook=forward chain=forward
:firewall assign hook=sink chain=sink
:firewall assign hook=source chain=source
```

4 BASIC REAL-LIFE SCENARIO FIREWALL

The previous discussed firewall configuration is the first step in a good security setup. But this firewall configuration limits its power to the protection of the internal SpeedTouch™ IP Host. Combined with VPN policies this configuration will give the users although a very secure combination.

The example in this chapter will discuss another means to add some extra obscurity to your internal network if it is approached by external attacks/visits. The example will combine a more robust firewall configuration that on its own, so without the help of VPN policies, will allow a safe setup of e.g. a Web server on the internal network.

Lets take the default firewall configuration and add some enhancements step by step.

```
:firewall rule create chain=forward index=0 srcintfgrp=wan dstintfgrp=wan action=drop
:firewall rule create chain=sink index=0 srcintfgrp=!wan action=accept
:firewall rule create chain=sink index=1 prot=udp dstport=dns action=accept
:firewall rule create chain=sink index=2 prot=udp dstport=bootpc action=accept
:firewall rule create chain=sink index=3 prot=udp dstport=sntp action=accept
:firewall rule create chain=sink index=4 prot=icmp icmptype=echo-reply action=accept
:firewall rule create chain=sink index=5 prot=icmp icmptype=destination-unreachable action=accept
:firewall rule create chain=sink index=6 prot=icmp icmptype=time-exceeded action=accept
:firewall rule create chain=sink index=7 prot=udp dstport=snmp log=yes action=count
:firewall rule create chain=sink index=8 prot=udp dstport=rip log=yes action=count
:firewall rule create chain=sink index=9 action=drop
:firewall rule create chain=source index=0 dstintfgrp=!wan action=accept
:firewall rule create chain=source index=1 prot=udp dstport=dns action=accept
:firewall rule create chain=source index=2 prot=udp dstport=bootps action=accept
:firewall rule create chain=source index=3 prot=udp dstport=sntp action=accept
:firewall rule create chain=source index=4 prot=udp dstport=syslog action=accept
:firewall rule create chain=source index=5 prot=icmp icmptype=echo-request action=accept
:firewall rule create chain=source index=6 prot=udp dstport=33434 action=accept
:firewall rule create chain=source index=7 prot=udp dstport=rip log=yes action=count
:firewall rule create chain=source index=8 prot=udp dstport=snmptrap log=yes action=count
:firewall rule create chain=source index=9 prot=udp srcport=snmp log=yes action=count
:firewall rule create chain=source index=10 action=drop

:firewall assign hook=forward chain=forward
:firewall assign hook=sink chain=sink
:firewall assign hook=source chain=source
```

As an internal user the assumption is made that at this point there is no “Trojan Horse” on the internal setup and that all data from the internal network is allowed to go to the external network or the Internet if the internal user initiated the data transfer. The incoming data should be restricted to data that was asked for or to data that is asked to very specific/secured servers.

Practically, in this example the Internet is allowed to connect to our internal FTP server. Combined with the previous requirement of our example setup two rules are added.

```
:firewall rule create chain=forward index=0 dst=a.b.c.d/32 prot=tcp dstport=ftp action=accept
:firewall rule create chain=forward index=1 srcintfgrp=wan prot=tcp syn=yes ack=no action=drop
```

The first rule will allow the forwarding of packets to the public routable IP address a.b.c.d where an FTP server is listening on the standard FTP port. The IP address a.b.c.d is located on our internal network. The second rule will drop all other external initiated TCP connections.

The next step would be to add a first obscurity by disallowing incoming ICMP echo-requests. Allowing other ICMP messages can be useful in detecting the state of external network if some internal processes are trying to reach the outside world. E.g. a destination unreachable message sent back to your browser if that browser was waiting for a response will result in a direct response to the user so that the user doesn't have to wait for the expiration/retransmits of its request.

The rule is simple.

```
:firewall rule create chain=forward index=2 srcintfgrp=wan prot=icmp icmptype=echo-request
action=drop
```

There is however still some unpleasant feeling about this setup. The firewall allows incoming protocols other than TCP or ICMP. An extra security measurement in the chain could be to use the NAPT engine of the SpeedTouch™. This NAPT engine would allow statefull decisions on the incoming connections and would disallow all incoming connections if there is no NAPT entry in its connections table. The forward rules become like this for e.g. an FTP server with IP address a.b.c.d.

```
:firewall rule create chain=forward index=0 dst=a.b.c.d/32 prot=tcp dstport=ftp action=accept
:firewall rule create chain=forward index=1 srcintfgrp=wan prot=tcp syn=yes ack=no action=drop
:firewall rule create chain=forward index=2 srcintfgrp=wan prot=icmp icmptype=echo-request
action=drop
:firewall rule create chain=forward index=3 srcintfgrp=wan dstintfgrp=wan action=drop

:firewall assign hook=forward chain=forward

:nat create protocol=tcp inside_addr=a.b.c.d:ftp outside_addr=0.0.0.0:ftp
```

The added value is that the NAPT engine will filter out Teardrop, Bonk or other Fragment Bomb attacks because the attack fragments will be discarded or reassembled by the SpeedTouch™ and in that way secure the internal IP stacks.

The last addition in this NAPT setup could be to add an extra Spoofing test on the forward hook so that the firewall protects our internal private IP addresses. There should not be any incoming IP packets coming from a WAN interface where the source IP address is from the subnet that is specified on the LAN interface. In our example the firewall doesn't want to see source a.0.0.0/8 IP addresses coming from the WAN.

```
:firewall rule create chain=forward index=0 srcintfgrp=wan src=a.0.0.0/8 action=drop
```

To summarize, lets put all the rules together for this example.

```
:firewall rule create chain=forward index=0 srcintfgrp=wan src=a.0.0.0/8 action=drop
:firewall rule create chain=forward index=1 dst=a.b.c.d/32 prot=tcp dstport=ftp action=accept
:firewall rule create chain=forward index=2 srcintfgrp=wan prot=tcp syn=yes ack=no action=drop
:firewall rule create chain=forward index=3 srcintfgrp=wan prot=icmp icmptype=echo-request
action=drop
:firewall rule create chain=forward index=4 srcintfgrp=wan dstintfgrp=wan action=drop
:firewall rule create chain=sink index=0 srcintfgrp=!wan action=accept
:firewall rule create chain=sink index=1 prot=udp dstport=dns action=accept
:firewall rule create chain=sink index=2 prot=udp dstport=bootpc action=accept
:firewall rule create chain=sink index=3 prot=udp dstport=sntp action=accept
:firewall rule create chain=sink index=4 prot=icmp icmptype=echo-reply action=accept
:firewall rule create chain=sink index=5 prot=icmp icmptype=destination-unreachable action=accept
:firewall rule create chain=sink index=6 prot=icmp icmptype=time-exceeded action=accept
:firewall rule create chain=sink index=7 prot=udp dstport=snmp log=yes action=count
:firewall rule create chain=sink index=8 prot=udp dstport=rip log=yes action=count
:firewall rule create chain=sink index=9 action=drop
:firewall rule create chain=source index=0 dstintfgrp=!wan action=accept
:firewall rule create chain=source index=1 prot=udp dstport=dns action=accept
:firewall rule create chain=source index=2 prot=udp dstport=bootps action=accept
:firewall rule create chain=source index=3 prot=udp dstport=sntp action=accept
:firewall rule create chain=source index=4 prot=udp dstport=syslog action=accept
:firewall rule create chain=source index=5 prot=icmp icmptype=echo-request action=accept
:firewall rule create chain=source index=6 prot=udp dstport=33434 action=accept
:firewall rule create chain=source index=7 prot=udp dstport=rip log=yes action=count
:firewall rule create chain=source index=8 prot=udp dstport=snmptrap log=yes action=count
:firewall rule create chain=source index=9 prot=udp srcport=snmp log=yes action=count
:firewall rule create chain=source index=10 action=drop

:nat create protocol=tcp inside_addr=a.b.c.d:ftp outside_addr=0.0.0.0:ftp
```

5 CONCLUSION

This application note has given a generic overview of how the SpeedTouch™ 610 can help you in securing your local network. The Firewall is a part of the secure chain and combined with the NAT engine it brings us more flexibility on managing the TCP/IP packets. The default firewall configuration should prevent attacks to the IP host of the SpeedTouch™. The most secure setup off course is the use of VPN policies enhanced with a well-chosen firewall configuration.

Visit us at:

www.speedtouch.com

Acknowledgements

All Colleagues for sharing their knowledge.

Coordinates

THOMSON
Prins Boudewijnlaan 47
B-2650 Edegem
Belgium

Email: documentation.speedtouch@thomson.net



Copyright

©2003 THOMSON. All rights reserved.

The content of this document is furnished for informational use only, may be subject to change without notice, and should not be construed as a commitment by THOMSON. THOMSON assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. The information contained in this document represents the current view of THOMSON on the issues discussed as of the date of publication. Because THOMSON must respond to changing market conditions, it should not be interpreted to be a commitment on the part of THOMSON, and THOMSON cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. THOMSON MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.