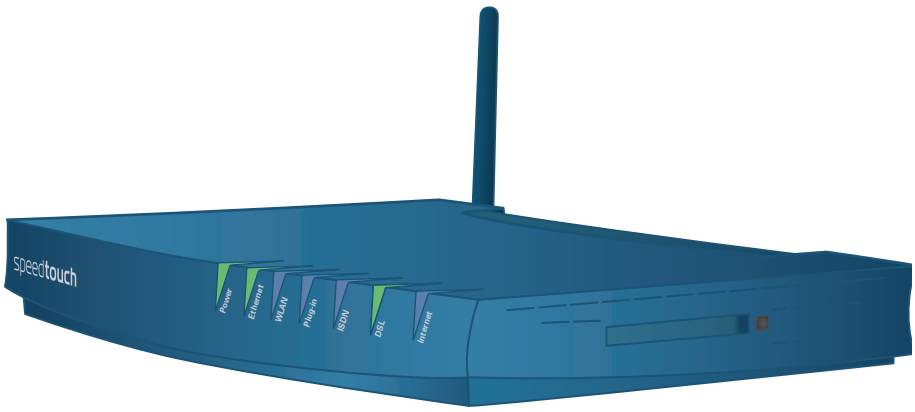
THOMSON

Thomson Gateway

Residential DSL Gateways



Stateful Inspection Firewall Configuration Guide

R7.4 and higher

Thomson Gateway

Stateful Inspection Firewall Configuration Guide

Copyright

Thomson Telecom Belgium
Prins Boudewijnlaan, 47
B-2650 Edegem
Belgium

http://www.thomson-broadband.com

Trademarks

The following trademarks may be used in this document:

- DECT is a trademark of ETSI.
- Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc.
- Ethernet™ is a trademark of Xerox Corporation.
- Wi-Fi®, WMM® and the Wi-Fi logo are registered trademarks of the Wi-Fi Alliance®. "Wi-Fi CERTIFIED", "Wi-Fi ZONE", "Wi-Fi Protected Access", "Wi-Fi Multimedia", "Wi-Fi Protected Setup", WPA", WPA2" and their respective logos are trademarks of the Wi-Fi Alliance®.
- UPnP™ is a certification mark of the UPnP™ Implementers Corporation.
- Microsoft®, MS-DOS®, Windows®, Windows NT® and Windows Vista® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Apple® and Mac OS® are registered trademarks of Apple Computer, Incorporated, registered in the United States and other countries.
- UNIX® is a registered trademark of UNIX System Laboratories, Incorporated.
- Adobe®, the Adobe logo, Acrobat and Acrobat Reader are trademarks or registered trademarks of Adobe Systems, Incorporated, registered in the United States and/or other countries.

Other brands and product names may be trademarks or registered trademarks of their respective holders.

Document Information

Status: v2.0 (June 2008)
Reference: E-DOC-CTC-20071115-0008
Short Title: Config Guide: SIF R7.4 and higher

Contents

Contents

About this Stateful Inspection Firewall Configuration Guide

Used Symbols

A ***note*** provides additional information about a topic.

A ***caution*** warns you about potential problems or specific precautions that need to be taken.

Terminology

Generally, the Thomson TG will be simply referred to as Thomson Gateway in this document.

Typographical Conventions

Following typographical convention is used throughout this manual:

- This sample text indicates a hyperlink to a Web site.

  Example: For more information, visit us at www.thomson-broadband.com.
- This sample text indicates an internal cross-reference.

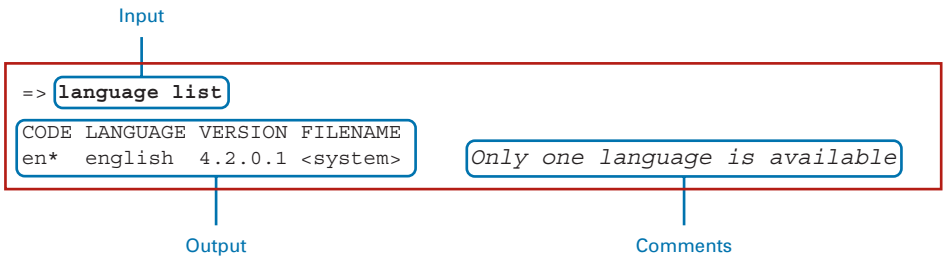
  Example: If you want to know more about guide, see "1 Introduction" on page 7.
- ***This sample text*** indicates an important content-related word.

  Example: To enter the network, you ***must*** authenticate yourself.
- **This sample text** indicates a GUI element (commands on menus and buttons, dialog box elements, file names, paths and folders).

  Example: On the **File** menu, click **Open** to open a file.
- **`This sample text`** indicates a CLI command to be input after the CLI prompt.

  Example: To obtain a list of all available command groups, type **`help`** at the top level.
- **`This sample text`** indicates input in the CLI interface.
- *`This sample text`* indicates comment explaining output in the CLI interface.

Example:



Documentation and software updates

Thomson continuously develops new solutions, but is also committed to improving its existing products.

For more information on Thomson's latest technological innovations, documents and software releases, visit us at http://www.thomson-broadband.com.

1 About Firewalls

Definition

Firewalls are computer network devices that protect a network from other less trusted networks. They are essentially network access control devices that permit and deny different types of traffic to travel into and out of an organization's network. Most often, firewalls are placed at the network boundary to protect an organization from unauthorized or malicious traffic.

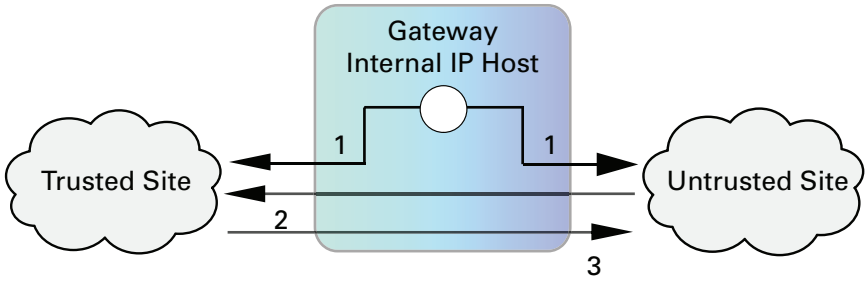
Working

Traffic that passes the firewall can be categorized in three types of traffic flows:

Flow	Function
1	Protection of the Thomson Gateway internal IP host
2	Protection of the Trusted Site, for example the LAN
3	Network policy defined by the Trusted Site

Illustration

The picture below shows the three traffic flows through a firewall:



How firewalls help

A firewall helps to prevent intruders from accessing data on your computer via the Internet or another untrusted network. To do this, it keeps unauthorized data from entering or exiting your system.

1| About Firewalls

2 Firewall Types

About firewall types

Different types of firewall exist. The most common firewalls are IP packet level firewalls which use the IP packet as basic unit for their internal operation. The firewall analyses IP packets beyond their IP headers such as transport headers e.g. TCP and UDP.

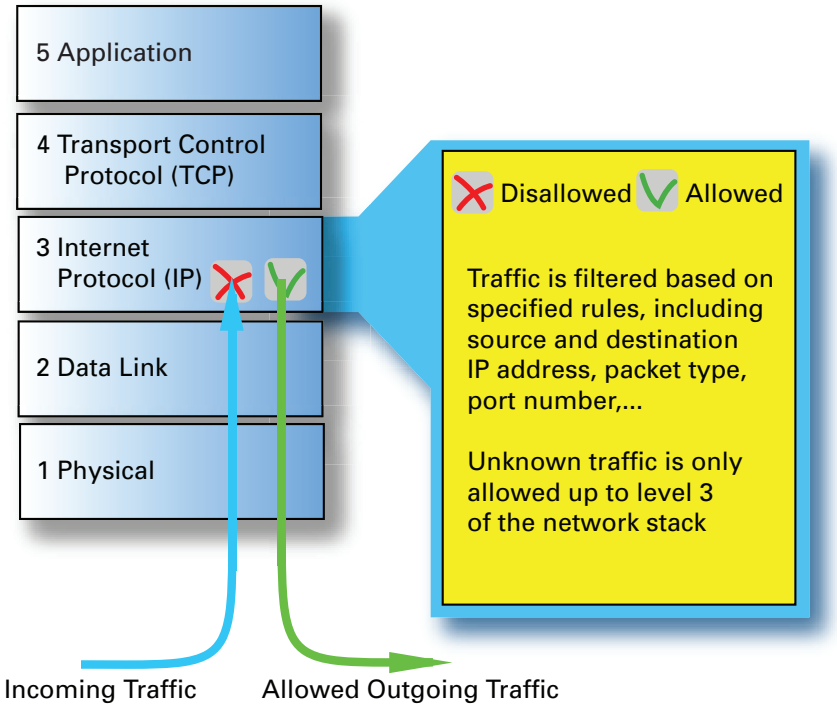
The four basic IP packet level firewalls types are:

- Packet filtering firewall
- Circuit level gateways
- Application level gateways or proxies
- Stateful inspection firewall (SIF)

From Software release R5.3 onwards, the Thomson Gateway uses a SIF instead of a packet filtering firewall.

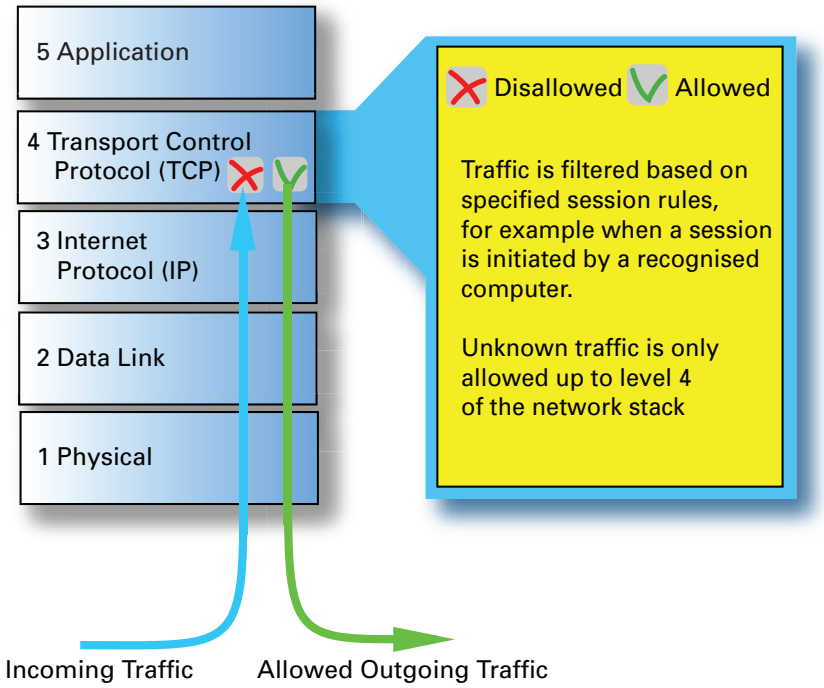
Packet filtering firewall

Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP. They are usually part of a router firewall. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator. Rules can include source and destination IP address, source and destination port number and protocol used.



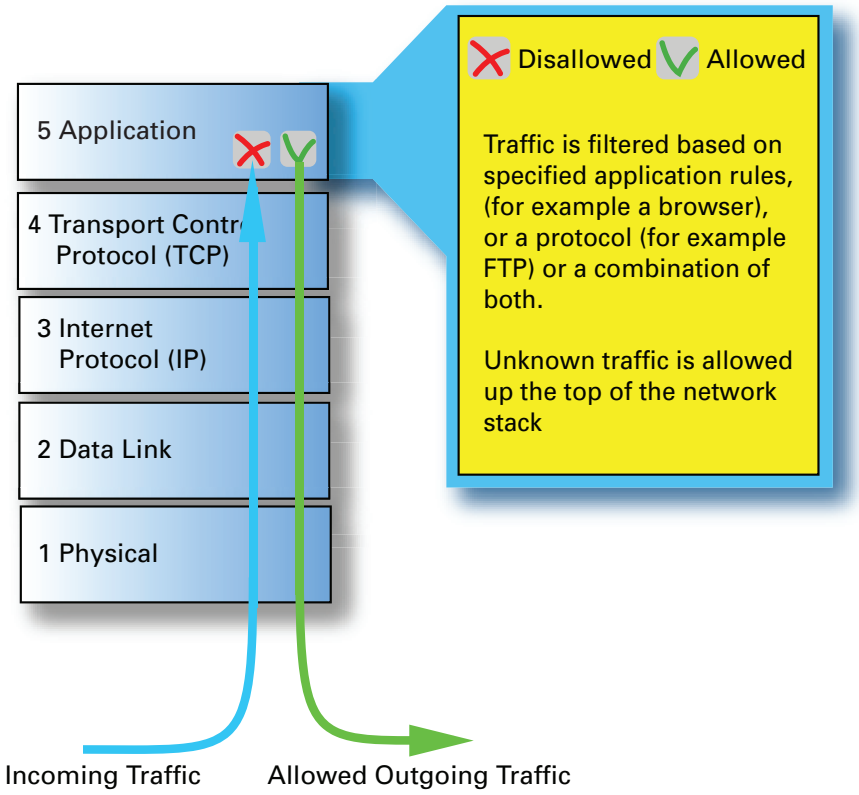
Circuit level gateways

Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to a remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks. Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. However, they do not filter individual packets.



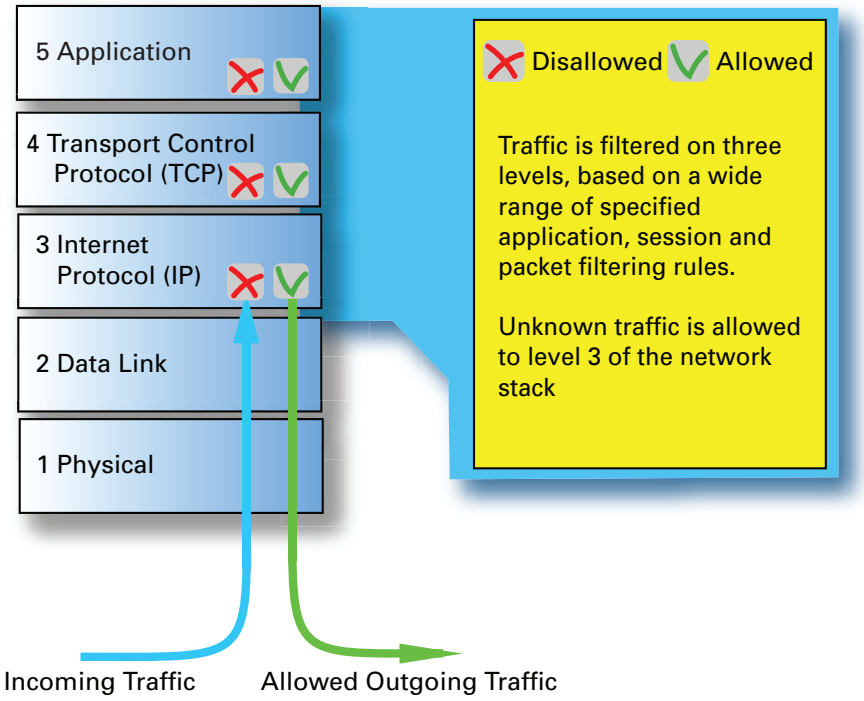
Application level gateways or proxies

Application level gateways, also called proxies, are similar to circuit level gateways except that they are application specific. They can filter packets at the application layer of the OSI model. Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, an application level gateway that is configured to be a web proxy will block allow any ftp, gopher, telnet or other traffic. Because they examine packets at application layer, they can filter application specific commands such as http:post and get. This cannot be accomplished with either packet filtering firewalls or circuit level neither of which know anything about the application level information. Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance. This is because of context switches that slow down network access dramatically. They are not transparent to end users and require manual configuration of each client computer.



Stateful inspection firewall (SIF)

Stateful inspection firewalls (SIF) combine the aspects of the other three types of firewalls. They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer. They allow direct connection between client and host, alleviating the problem caused by the lack of transparency of application level gateways. They rely on algorithms to recognize and process application layer data instead of running application specific proxies. Stateful multi-layer inspection firewalls offer a high level of security, good performance and transparency to end users.



Streams and connections on a SIF

The basic actions a SIF performs are identical compared to a packet filter: either permit or deny traffic. However the rules on which it makes these decisions are far more complicated. The SIF analyses header field values, but also maintains a history of received streams and tries to predict responses.

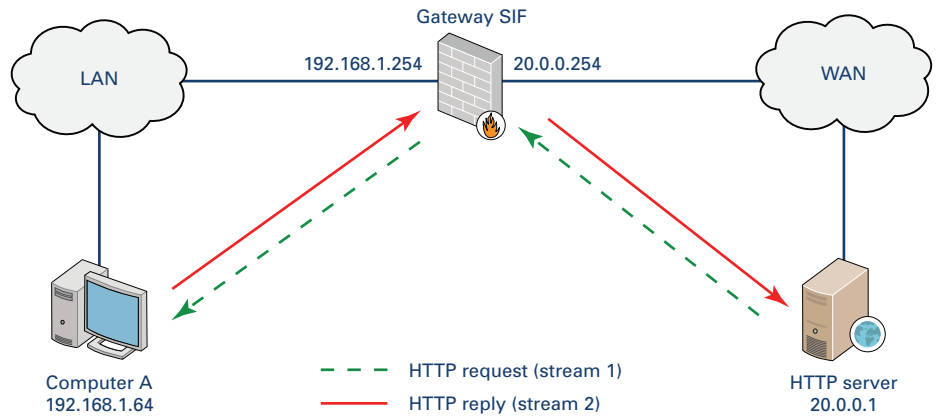
If subsequent streams are not in line with the collected history and if answers are not in line with the predicted responses, streams are dropped.

- A ***stream*** is uni-directional. It's a collection of one or more packets with the same Source and Destination and other common characteristics like protocol type, sequence number, ICMP code,...
- A ***connection*** is bi-directional. It's a combination of related streams, initiator and returning stream.

A SIF maintains a table of active connections. Each entry records the most important parameters of the stream such as source and destination IP address and port numbers, the current TCP sequence number and other characteristics. Entries are created only for those streams that are allowed to pass through, according to the security policy in the firewall rules database.

SIF, an example

The following picture provides an example of the information kept in the stream/connection table when computer A sends a HTTP request to the HTTP server:



Stream/Connection Table

Connection	Streams	Protocol	SRC IP	DST IP	SRC Port	DST Port
Connection 1	Stream 1 Stream 2 (expected)	HTTP HTTP	192.168.1.64 20.0.0.1	20.0.0.1 192.168.1.64	1026 80	80 1026

Note that the source (SRC) port is the port randomly chosen by the client when making a connection to the HTTP server.

Firewall Rules Table

Rules	Protocol	SCR INTF	DST INTF	Action
1 2 3	HTTP (TCP on port 80) ...	LAN	WAN	Accept

Process:

The process of the above example is as follows:

1. Computer A (client) initiates a HTTP connection to the HTTP server.
2. The HTTP traffic is allowed because of rule 1 in the firewall rules table.
3. All the characteristics of stream 1 (src and dst IP, src and dst port, protocol) are added in the stream/connection table.
4. The expected stream is added to the stream/connection table. A returning stream with the same characteristics as the expected stream will be passed through the firewall. This is the stateful behaviour of the firewall.
5. The HTTP server sends the expected reply. This returning stream is allowed because it's mentioned in the stream/connection table as expected stream. When the HTTP server wants to initialize a connection to A, no rule is hit. A packet with no rule match is automatically blocked by the firewall.

Default firewall behaviour

The default behaviour of the firewall is to block all traffic. This means that you can only makes holes in the firewall by adding rules. When a packet doesn't hit a rule it is automatically blocked.

3 Properties of the Thomson Gateway SIF

Overview

This chapter covers the following topics:

3.1 Returning Stream Prediction

Returning stream prediction

Most in- or outgoing packets expect a reply in reverse direction. The firewall does not know whether there will be a reply or not it only checks if an incoming packet belongs to an existing connection. The expected stream is added to the stream/connection table.

Returning stream prediction is used on all layer three and four protocols (IP, ICMP, TCP and UDP).

The firewall knows whether an incoming packet belongs to an existing connection or not thanks to the underlying so called “connection framework”.

Example 1

Below is an example:

1 A ping request is made from 192.168.1.64 to 20.0.0.1

The stream is:

```
stream 1: src ip 192.168.1.64; dst ip 20.0.0.1; protocol=icmp; icmp type = 8; icmp code =
0;
```

2 A reply on the ping request follows from 20.0.0.1 to 192.168.1.64

The stream is:

```
stream 2: src ip 20.0.0.1; dst ip 192.168.1.64; protocol=icmp; icmp type = 0; icmp code =
0;
```

Since stream 2 has the same parameters as stream 1 (the source and destination have been swapped), the connection framework knows that both streams belong to the same connection. It is a reply to a (correct) ping request.

Example 2

Below is another example:

1 A ping request is made from 192.168.1.64 to 20.0.0.1

The stream is:

```
stream 1: src ip 192.168.1.64; dst ip 20.0.0.1; protocol=icmp; icmp type = 8; icmp code =
0;
```

2 An ICMP error is generated from 30.0.0.1 to 192.168.1.64 (embedded: dst 20.0.0.1 unreachable)

The stream is:

```
stream 2: src ip 30.0.0.1; dst ip 192.168.1.64; protocol=icmp; icmp type = 3; icmp code =
1;
```

The embedded header in the ICMP error message has the same parameters as stream 1. The firewall knows that the ICMP error and stream 1 are related to each other.

3.2 Stateful Connection Tracking

About Stateful Connection Tracking (SCT)

Connection tracking refers to the ability to maintain state information about a connection in the stream/connection table, such as source and destination IP address and port number pairs, protocol types, connection state and time-outs.

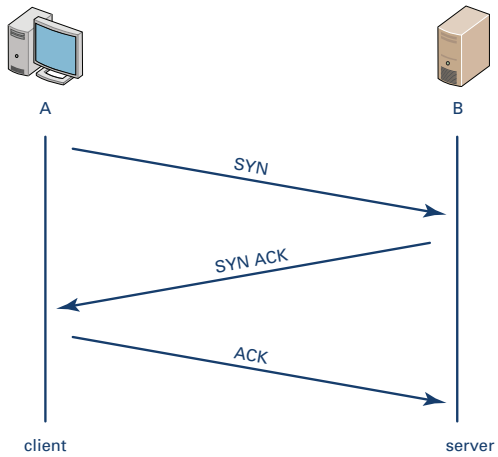
SCT checks

Stateful connection tracking checks whether all traffic is correctly formed. In case of the Thomson Gateway SIF, the following checks can be done:

Check	Description
TCP Sequence Number Checks	The SIF checks whether the TCP sequence numbers follow up or not. This is based on the configurable TCP window size and the last sequence number. By default, TCP checks are not performed. To change this, use the **`:firewall config`** command
TCP Window Size Tracking	The SIF checks the buffer or window size.
ICMP checks	■ ICMP request/reply types ■ Error types The SIF checks whether each ping reply is made to the correct ping request. Refer to " Example 1" on page 16 and " Example 2" on page 16 for more information.
UDP Checks	The SIF checks the header length. This is also for TCP and ICMP.
TCP state/flag combination checks	Refer to the example below.

TCP state/flag combination checks: example

A good example of TCP state/flag check is the three-way handshake:



The SIF controls that the TCP handshake runs properly.

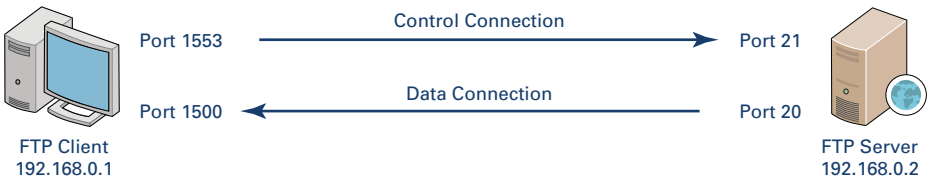
3.3 Application Level Gateway

About Application Level Gateway (ALG)

Certain protocols, such as IPSec, SIP and FTP are hard to track correctly, since they carry low layer IP information within the data payload of the packets, and therefore require special connection tracking support system, in order for the tracking to succeed.

Example: FTP protocol

Below is a diagram for the FTP Protocol:



The process is as follows:

1. The FTP protocol opens a single connection that is called the FTP control connection.

   This connection is used only for issuing commands (get, put, ls).

2. As a result of the command, the system opens another connection (i.e. on another port) to carry the information related to that specific command. To do this, the FTP client sends a port and an IP address to connect to.
3. The FTP client opens the port and the server connects to that specified port from its own port 20 (known as FTP-Data).
4. The FTP Client transfers the data over the data connection.

Problem definition

The problem in the above example is that the firewall does not know about the extra (data) connections, since they where negotiated within the actual payload of the protocol data. Because of this, the firewall will not be able to determine whether or not it should allow the server to connect to the client over these specific connections.

Solution: Application Level Gateway (ALG)

A possible solution to this problem is to add a special support system, the Application Level Gateway (ALG) to the connection tracking module which will scan through the messages sent in the control connection for specific syntaxes and information. When it encounters such information, it will dynamically add that specific information as related, and the server will be able to make the connection, with the related entry.

4 Basic concepts of the Thomson Gateway SIF

Overview

This chapter covers the following topics:

4.1 Hook Points and Flows of the Thomson Gateway

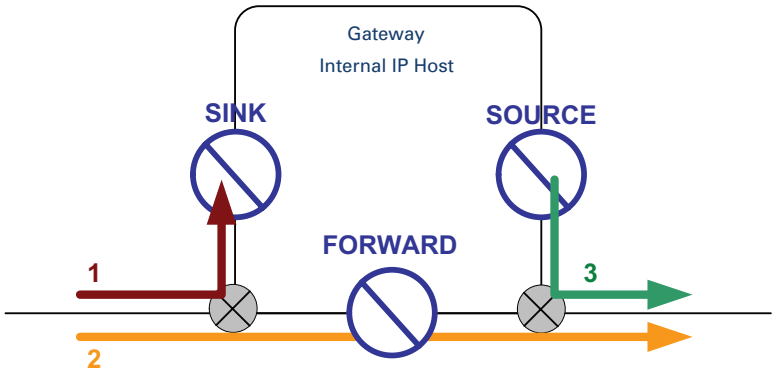
About hook points

Streams are intercepted at certain points in the Thomson Gateway called hook points or ***hooks***. At these points, and only here, the first packet of the connection, is matched against a ***chain***, which contains a hierarchical set of ***rules*** (at least one). These rules determine the type of control implemented on this and all related subsequent packets of the applicable stream.

On CLI level, a chain and a hook are the same object. It is not necessary to assign a chain to a specific hook.

Diagram

The diagram below shows the basic hooks and flows of the Thomson Gateway:



Function of the hook points

The function of the Thomson Gateway hooks:

Hook	Flow	Function
Sink	1	The point of all traffic destined for the Thomson Gateway. At this hook you can determine whether a stream/connection is allowed to address the local IP host.
Forward	2	The point of all traffic to be forwarded through the Thomson Gateway. At this hook you can determine whether a stream/connection is allowed to be handled (i.e. routed) by the local IP host.
Source	3	The point of all traffic sourced by the Thomson Gateway. At this hook you can determine whether a stream/connection is allowed to leave the local IP host.

E-DOC-CTC-20071115-0008 v2.0

Function of the traffic flows

The function of the Thomson Gateway traffic flows is:

Flow	Function
1	The streams/connections exclusively destined for the Thomson Gateway IP host itself.
2	The streams/connections sourced by the untrusted site, forwarded by the Thomson Gateway towards the local network, or vice versa.
3	The streams/connections exclusively sourced by the Thomson Gateway itself.

Additional Hooks/Chains

In addition to the basic hooks and related chains, the system uses a number of other hooks. Use the following CLI command to list them:

```
=>firewall chain list
```

This produces the following output:

```
Chains
======
Name                                                Policy          Description

-------------------------------------------------------------------------------
sink                                                accept          system
forward                                             accept          system
source                                              accept          system
sink_fire                                           accept          system
forward_fire                                        accept          system
source_fire                                         accept          system
forward_timeofday                                   accept          system
forward_custom                                      accept          system
sink_system_service                                 accept          system
source_system_service                               accept          system
forward_level                                       accept          system
forward_host_service                                accept          system
forward_multicast                                   accept          system
forward_level_High                                  accept          system
forward_level_Medium                                accept          system
forward_level_Standard                              accept          system
forward_level_Low                                   accept          system
forward_level_Disabled                              accept          system
forward_level_BlockAll                              accept          system
forward_level_Test                                  accept          system
{Administrator}=>
```

It is also possible to create other chains using the following command:

```
=>firewall chain add chain <name of the chain>
```

4.2 Basic Mode vs Expert Mode

About Web Interface modes

The Web Interface has two modes, a ***Basic Mode*** and an ***Expert Mode.*** On residential Thomson Gateways, only the Basic Mode is available; business Thomson Gateways have both modes.

Differences

The options you can view and configure depend on the used mode. Below is an overview of the differences between the two modes:

Item	Basic Mode	Expert Mode
Set and view the security level	Yes	Yes
Create a new security level	Yes	Yes
View the security level policy	Yes	Yes
View and set the general firewall settings	No	Yes
Create Expressions	No	Yes

4.3 Firewall Security Levels

Overview

The Thomson TG has a number of pre-defined security levels, all designed to provide a specific level of protection for the Thomson Gateway and the local network.

This section covers the following topics:

4.3.1 About Security Levels

How to view the security levels

Via the Web Interface some information on the firewall security levels is provided.

To access the firewall information, do one of the following:

- go to **Expert Mode > Firewall > Policy**.
- go to **Basic > Toolbox > Firewall** and click on **details**.

This overview provides the policy settings for the selected security level.

When using Expert Mode, the page also provides the general security levels.

Pre-defined security levels

Several Security Levels exist, all having influence on the Forward hook only, meaning that these levels do not affect firewalling to or from the Thomson Gateway host itself:

Select...	To...	Available on...
Security level “High”	Block all outgoing connections except well known applications (DNS, HTTP, HTTPS, FTP, TELNET, IMAP, POP) and block all incoming connections.	Business only
Security level “Medium”	Allow all outgoing connections except Windows protocols (Netbios, RPC, SMB) and block all incoming connections. ■ All outgoing connections are allowed, except the Windows protocols. ■ Game & Application sharing is allowed.	Business only
Security level “Standard “	Allow all outgoing connections and block all incoming traffic. ■ All outgoing connections are allowed. ■ Game & Application sharing is allowed by the firewall.	All
Security level “Low “	Allow all outgoing connections and block all incoming traffic except Internet Control Management Protocol (ICMP). ■ All incoming connections are blocked, except ICMP. ■ Game & Application sharing is allowed.	Business only
Security level “Disabled”	Disable the firewall. All traffic is allowed to pass through your SpeedTouch. ■ Any kind of traffic from anywhere is allowed. ■ Game & Application sharing is allowed by the firewall.	All

Select...	To...	Available on...
Security level “BlockAll”	Block all traffic from and to the Internet. ■ Any kind of traffic from anywhere is dropped. ■ Game & Application sharing is not allowed by the firewall.	All

Disable the firewall

Disabling the firewall is not the same as selecting security level **Disabled**. Disabling the firewall means that both packet filtering and stateful tracking are disabled.

You can only disable the firewall via CLI:

```
:firewall config state disabled
```

We highly recommend selecting **Disabled** instead of disabling the firewall. **Disabled** stops filtering packets, but continues stateful tracking behaviour. Stateful tracking will prevent malicious traffic such as:

- ICMP error message on unsent ICMP message
- A ghost reply (replies on non-existent requests)
- ACK or FIN ACK, without TCP SYN

Disabling the firewall means all traffic is allowed, which poses a security risk.

4.3.2 Security Level Settings

Overview

There are two types of settings:

- General security level settings
- Security level policy Settings

General security level settings

Per selected security level following general settings are provided:

Setting	Description
Level name	Name of the security level
Description	Description of the security level
UDP tracking	Two values are possible: ■ **strict:** Only returning UDP streams belonging to the same connection are allowed. ■ **loose:** The source port of the original UDP connection is opened for all hosts which want to connect to this port. This can be configured for example for gaming: to allow the client to receive information from other players of the same on-line game, loose udp tracking should be configured to allow incoming packets on the port that was used to start the communication with the server.
Game & Application Sharing	Allow the firewall level to open ports for "games and application sharing" in order to use applications like Peer-to-Peer file sharing (PtoP), Internet Games, Web serving, FTP serving, WebCams, IRC DDC, and Instant Messaging such as AIM, ICQ, Yahoo and MS Messenger. You need to configure such games or applications if you like to act as a game server or share a server located on your local network with other people. Configuration can be done via **Toolbox > Game & Application Sharing**.
Proxying	Allow or disallow the firewall from acting as a proxy server or not. A proxy server acts both as a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it. For example HTTP Intercept.
Readonly	When selected, does not allow customization of the security level. No firewall rules can be added or deleted. By default all pre-defined levels are read-only. They can only be changed in Expert Mode.

Security level policy Settings

The policy settings provide an overview of all firewall rules. The table below provides a general overview of the different elements in a rule and their function:

Element	Function
Nr	The index of the firewall rule. The firewall will go through the rules, from top to bottom, starting from rule 1. When no rule is hit, the firewall will block the traffic (default behaviour).

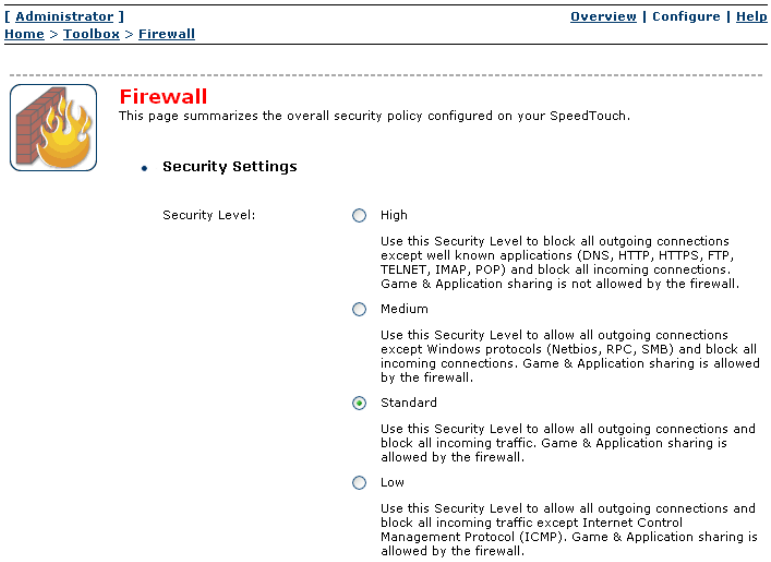
Element	Function
Name	The name of the rule.
Action	The action to be taken for this rule ■ **accept**: the connection is accepted ■ **deny**: send to the sender that the packet could not be delivered ■ **drop**: the packet is silently discarded ■ **reset**: reset of the connection ■ **count**: counts the number of connections that match the rule description. Contrary to other actions this action does not stop further parsing of the firewall rules database; the result is shown in the last column **hits**.
Service	The service or protocol. (e.g. smtp, http, telnet,...)
Src Intf	The source interface. (e.g. _lan1, _wan1, _dmz1,...)
Src IP	The name of the source IP expression.
Dst Intf	The destination interface (e.g. _lan1, _wan1, _dmz1,...)
Dst IP	The name of the destination IP expression.
Log	To log the actions concerning this rule. You can see the result in **Firewall > Log**.
Hits	Shows the number of connections that matched the rule, if the action is **count**.

4.3.3 How to select a Firewall Security Level

How to select of the security level in *Basic Mode*

Proceed as follows:

1. Open a web browser and browse to the Thomson TG Web Interface: **http://dsldevice.lan**.
2. Go to **Basic >Toolbox > Firewall**.
3. Click **Configure**.
4. Select the required security level:



5. Click **Apply**.

In Basic mode, you can only see the four generic security levels. The Security Levels **BlockAll** and **Disabled** are available on business variants (and in Expert mode) only.

Select the security level in Expert Mode

Proceed as follows:

1. Open a web browser and browse to the Thomson TG Web Interface: **http://dsldevice.lan**.
2. Go to **Expert Mode > Firewall > Policy:**
3. Select the required level in the level list:
4. Click **Set Active**.
5. Click **Save All** to save the configuration.

5 Firewall configurations with the Web Interface

Overview

This section covers the following topics:

5.1 How to Create an expression

Types of expressions

Expressions are used in rules for source and destination interfaces, source and destination IP address(es) (ranges) and services.

There are three (3) types of expressions:

- ***Interface related expressions***

  These are expressions related to an interface like: lan, wan, ipoa, pppoe, pppoa etc.

- ***IP related expressions***

  These are expressions related to an IP address or range.

- ***Service related expressions***

  These are expressions related to a service like http, ftp, ike, sip, etc.

You can only create an expression in ***Expert Mode***.

How to create an expression

Proceed as follows:

1. Open a web browser and browse to the Thomson TG Web Interface: **http://dsldevice.lan**.
2. Go to **Expert Mode > Firewall > Expressions**:

   Note Expressions shown in red on the GUI screen are dynamically created by other Thomson TG modules. These are used in **Game & Application Sharing** or **TG Services**, and can be used in firewall rules. They cannot, however, be modified.

3. How to continue depends on the type of expression you want to create:
   - To create an Interface related expression, proceed with "5.1.1 How to Create Interface Related Expressions" on page 31
   - To create an IP expression, proceed with "5.1.2 How to Create IP Related Expressions" on page 32
   - To create a Service related expression, proceed with "5.1.3 How to Create Service Related Expressions" on page 33

5.1.1 How to Create Interface Related Expressions

How to create an interface-related expression

This is only possible in *Expert Mode*. Proceed as follows:

1. If necessary, click the **Interface** tab:
2. Click **New**.
3. Type a name for the expression in the **Name** field.
4. Select the interface group (**any**, **wan**, **lan**, **local**, **dmz**, **guest** or **tunnel**).

   Select **Not** to make the expression negative.

   Example: if you select Interface group **lan**, selecting **Not** means that all traffic not coming from a LAN will be filtered.
5. Select the interface. An interface is the connection between the SpeedTouch™ and one of its attached networks. Possible interfaces are: **Physical interfaces**, **ATM interfaces**, **Ethernet interface**s, **IP interfaces**, or **PPP interfaces**.

   Select **Not** to make the expression negative.
6. Click **Apply** to add the new expression.
7. Click **Save All** to save the configuration.

5.1.2 How to Create IP Related Expressions

How to create an IP-related expression

This is only possible in *Expert Mode*. Proceed as follows:

1. Select the **IP** tab.
2. Click **New**.
3. Type a name for the expression in the **Name** field.
4. Type the IP address (or continuous range) in the **IP address** field.

   Select **Not** to make negative.

   To enter a range of IP addresses, you should create an expression for that range. Refer to "5.1.2 How to Create IP Related Expressions" on page 32.
5. Click **Apply** to add the new IP related expression.
6. Click **Save All** to save the configuration.

5.1.3 How to Create Service Related Expressions

How to create a service-related expression

This is only possible in *Expert Mode*. Proceed as follows:

1. Select the **Service** tab.
2. Click **New**. This opens the following form below the table.
3. Type a name for the expression in the **Name** field.
4. Select the protocol to filter on from the **Protocol** list.
5. If applicable, enter a port number (range) for:
   - **Source port** (from... to)
   - **Destination port** (from... to)

   Select **Not** to make negative.
6. Click **Apply** to add the new service related expression.
7. Click **Save All** to save the configuration.

5.2 How to Create and Modify a Security Level

Overview

This section covers the following topics:

How to create a security level in Basic mode

Proceed as follows:

1. Go to **Basic Mode > Toolbox > Firewall.**
2. Click **Configure**.
3. In the **Pick a Task...** area, click **Create a new Security Level.**
4. Select a security level to be used as basis for the new one.
5. Click **Apply**.
6. To change the rules of the Security Level, proceed with " How to add rules to a security level Using Basic mode" on page 35.

How to create a security level in Expert Mode

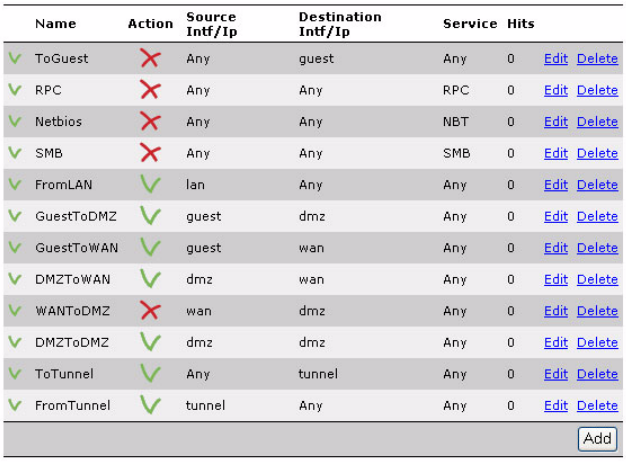
Proceed as follows:

1. Go to **Expert Mode > Firewall > Policy**.
2. Select a security level to be used as basis for the new one.
3. Click **Customize**.
4. Provide a name and description for the new security level and click **Apply.**
5. The new security level, e.g. **MyLevel** is now created and available in the drop-down list.
6. To change or add rules, proceed with " How to add rules to a security level using Expert mode" on page 36
7. Click **Save All** to save the configuration.

How to add rules to a security level Using Basic mode

Proceed as follows:

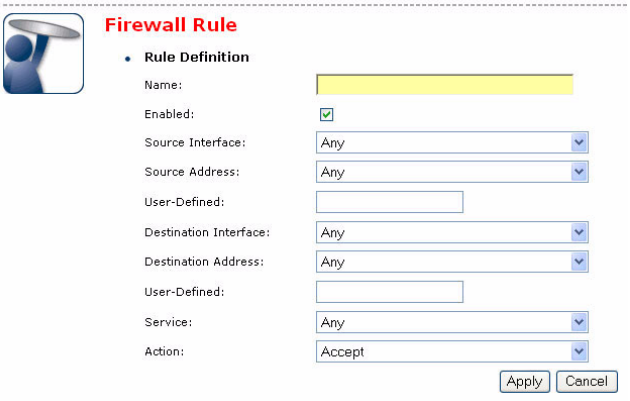
1 After creating a new level, the rule overview table is shown:



	Name	Action	Source Intf/Ip	Destination Intf/Ip	Service	Hits	
✓	ToGuest	✗	Any	guest	Any	0	Edit Delete
✓	RPC	✗	Any	Any	RPC	0	Edit Delete
✓	Netbios	✗	Any	Any	NBT	0	Edit Delete
✓	SMB	✗	Any	Any	SMB	0	Edit Delete
✓	FromLAN	✓	lan	Any	Any	0	Edit Delete
✓	GuestToDMZ	✓	guest	dmz	Any	0	Edit Delete
✓	GuestToWAN	✓	guest	wan	Any	0	Edit Delete
✓	DMZToWAN	✓	dmz	wan	Any	0	Edit Delete
✓	WANToDMZ	✗	wan	dmz	Any	0	Edit Delete
✓	DMZToDMZ	✓	dmz	dmz	Any	0	Edit Delete
✓	ToTunnel	✓	Any	tunnel	Any	0	Edit Delete
✓	FromTunnel	✓	tunnel	Any	Any	0	Edit Delete

Add

2 Click **Add**. The following page appears:



3 Provide a name for the rule.

4 Select:

- **Source interface** (for example _lan1, _wan1, _dmz1,... or Any)
- **Source IP expression** (or type the IP address (range) in the
- **User-Defined** box)
- **Destination interface** (e.g. _lan1, _wan1, _dmz1,...)
- **Destination IP expression** (or type the IP address (range) in the)
- **User-Defined** box)
- **Service** (service or protocol; for example smtp, http, telnet,...)

5 Click **Apply**. To change an existing rule, proceed with " How to change an existing rule in Basic mode" on page 37.

How to add rules to a security level using Expert mode

Proceed as follows:

1. Select a security level e.g. Mylevel in the drop-down list.
2. Click **New**. This opens the following form below the table:
3. Select an Index for the firewall rule and provide a name.

   The firewall goes through the table hierarchically, starting with the first rule. If no rule applies, the firewall blocks the traffic (default behaviour).
4. Select:
   - **Source interface** (for example _lan1, _wan1, _dmz1,... or Any)
   - **Source IP expression** (or type the IP address (range))
   - **Destination interface** (e.g. _lan1, _wan1, _dmz1,...)
   - **Destination IP expression** (or type the IP address (range))
   - **Service** (service or protocol; for example smtp, http, telnet,...)

   Select **Not** to make the rule negative.
5. Specify the flags:
   - **Enable** enables the rule or not.
   - **Log to** logs the actions relating to this rule. To view the result, go to **Firewall > Log**.
6. Select the Action to be taken for this rule:
   - **accept:** the connection is accepted
   - **deny:** send to the sender that the packet could not be delivered
   - **drop:** the packet is silently discarded
   - **reset:** reset of the connection
   - **count:** counts the number of connections that match the rule description. Contrary to other actions this action does not stop further parsing of the firewall rules database; the result is shown in the last column **hits**.
7. Click **Apply** to add the rule to the security level.To change an existing rule, proceed with " How to change an existing rule in Expert mode".
8. Click **Save All** to save the configuration.

How to change an existing rule in Basic mode

Proceed as follows:

1. Go to **Basic Mode > Firewall > Configure**.
2. Select the security level for which you want to change a rule, and click the corresponding **Edit**.
3. Go to the rule you want to change and click **Edit**. For more info on what to change, refer to " How to create a security level in Basic mode" on page 34.

   To remove the rule from the firewall, click **Delete**.
4. Change the settings of the rule and click **Apply**.

How to change an existing rule in Expert mode

Proceed as follows:

1. Go to **Expert Mode > Firewall**.
2. In the drop-down list, select the security level for which you want to change a rule and click **Customize**.
3. Click on the arrow in front of the rule you want to change.
4. Change the settings and click **Modify**. For more info on what to change, refer to " How to create a security level in Expert Mode" on page 34.

   To remove the rule, click **Delete**.

5.3 Scenario 1: Share a server on the trusted site

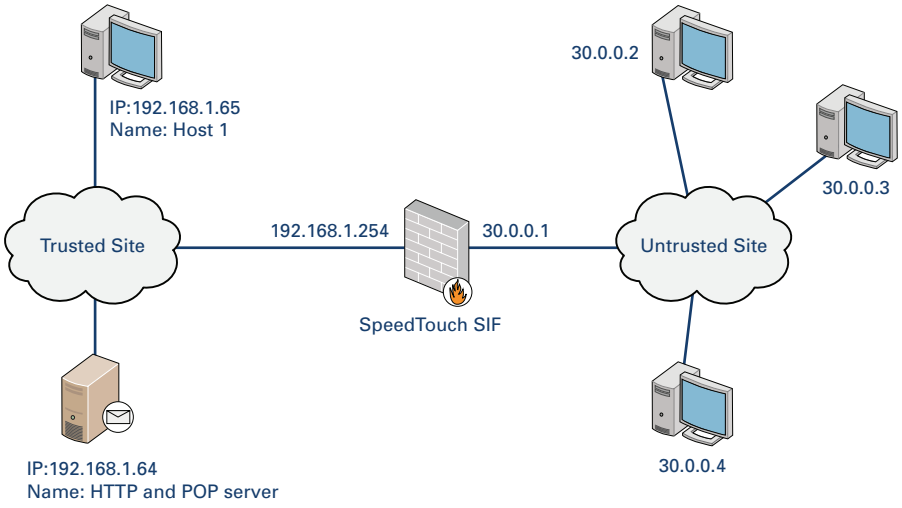
Introduction

This section will explain how to share a server located on your local network with other people.

For this scenario we start with ***security level standard***. Security level standard allows all outgoing connections and blocks all incoming traffic. Game & Application sharing is allowed by the firewall.

Network setup

Following picture shows the network setup.



Overview

This scenario covers the following procedures:

5.3.1 Share the Web server (HTTP) for the WAN

Introduction

This section will explain how to configure the firewall to allow access from ***anybody*** on the untrusted site to the Web server (HTTP) on the trusted site. There are two ways to configure this:

- Via Expert mode
- Via Basic mode

Via Expert mode

Proceed as follows:

1. Go to **Expert Mode > Firewall > Policy**.
2. Create a new security level e.g. **MyLevel**.
3. For more information, see "5.2 How to Create and Modify a Security Level" on page 34.
4. Click **New**. The Policy Rule Properties form opens.
5. Select an index. Note that the lower index has the higher priority.
6. Provide the following information:
   - **Name:** "Share Web Server".
   - **Source Interface**: "wan". This allows traffic from the (untrusted WAN site).
   - **Service:** "http". This allows only http traffic from the WAN site.
7. Select the **Enable** and **Log** flags.
8. Select **accept** as Action to allow the specified kind of traffic.
9. Click **Apply** to add the rule to the security level.
10. Click **Save All** to save the configuration.

Via Basic mode

You can configure the same via the ***Basic Mode***. Proceed as follows:

1. Go to **Basic Mode > Toolbox > Game & Application Sharing**.
2. Click **Configure**.
3. Select **Web Server (HTTP)**.
4. In the drop-down list, select the device **Webserver**.
5. Select the box under **Log** to enable logging.
6. Click **Add**.
7. This rule assigns HTTP to the Webserver (192.168.1.164)
8. When the internet connection comes up, a NAT map is automatically created and the game or application is assigned.

5.3.2 Share the POP3 server for 30.0.0.2 and 30.0.0.3.

Introduction

This section explains how to configure the firewall to allow access from 30.0.0.2 and 30.0.0.3 (untrusted site) to the POP3 server (to retrieve mail) on the trusted site.

Procedure

Proceed as follows:

1. Go to **Expert Mode > Firewall > Policy**.
2. Select **MyLevel**.
3. Click **New**. The Policy Rule Properties form opens.
4. Select an index. Note that the lower index has the higher priority.
5. Provide the following information:
   - **Name:** “Share POP3 Server”.
   - **Source Interface:** “wan”. This allows traffic from the (untrusted WAN site).
   - **Source IP:** “30.0.0.[2-3]” (IP range)
   - **Service:** “pop3”. This allows only POP3 traffic from the WAN site.
6. Select the **Enable** and Log flags.
7. Select **accept** as Action to allow the specified kind of traffic.
8. Click **Apply** to add the rule to the security level.
9. Click **Save All** to save the configuration.

As with the previous example, this is also configurable via **Basic Mode > Toolbox > Game & Application Sharing**. The procedure is similar. However, you cannot limit access to the clients via **Games and Application** sharing.

5.4 Scenario 2: Portrange restrictions

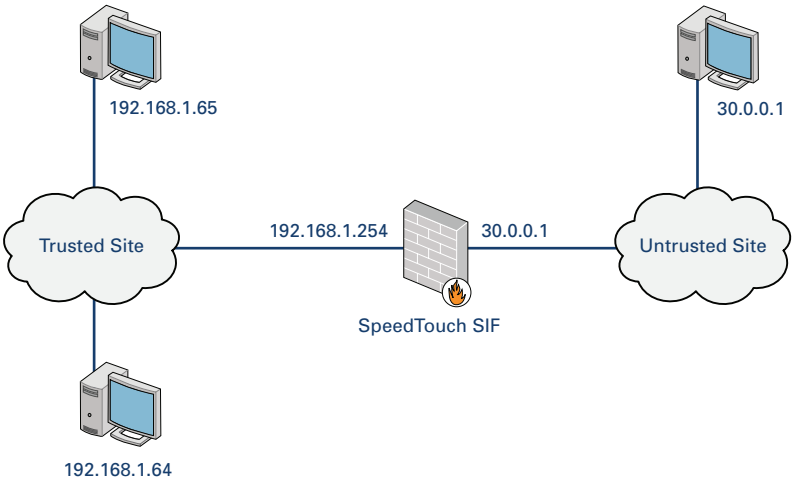
Introduction

This section will explain how to allow incoming connections from a specific portrange.

For this scenario we start with ***security level standard***. Security level standard allows all outgoing connections and blocks all incoming traffic. Game & Application sharing is allowed by the firewall.

Network setup

Following pictures shows the network setup:



Scenario Example

In this example, we will allow access from incoming TCP connections with port range 1 to 1023.

Procedure

Proceed as follows:

1. Go to **Expert Mode > Firewall > Policy**.
2. Create a new security level called **MyLevel**., derived from the ***Standard*** Security Level.
3. For more information, see "5.2 How to Create and Modify a Security Level" on page 34.
4. Create a service expression called **portrange** for TCP portrange 1 to 1023:
5. For more information on how to create expressions, see "5.1 How to Create an expression" on page 30.
6. Select **MyLevel** on the policy page and click **New**. The Policy Rule Properties form opens.
7. Select an index. Note that the lower index has the higher priority.
8. Provide the following information:
   - **Name:** "portrange filtering".
   - **Source Interface:** "wan". This allows traffic from the (untrusted WAN site).
   - **Source IP:** "30.0.0.[2-3]" (IP range)
   - **Destination IP:** Select "portrange".
9. Select the **Enable** and **Log** flags.
10. Select **accept** as Action to allow the specified kind of traffic.
11. Click **Apply** to add the rule to the security level.
12. Click **Save All** to save the configuration.

6 Firewall configurations via CLI

Overview

This chapter covers the following topics:

6.1 How to Configure the General Firewall Properties

About the firewall config command

The firewall config commands displays and sets controls the firewall's general settings. It has the following syntax:

```
=>firewall config [state = <{disabled|enabled}>]
                  [keep = <{disabled|enabled}>]
                  [tcpchecks = <{none|fast|exact}>]
                  [udpchecks = <{disabled|enabled}>]
                  [icmpchecks = <{disabled|enabled}>]
                  [logdefault = <{disabled|enabled}>]
                  [logthreshold = <{disabled|enabled}>]
                  [tcpwindow = <number{0-1073725440}>]
```

To view the configuration, use the command without any of its parameters:

```
=>firewall config
```

General firewall settings

Each of these parameters corresponds with a firewall setting:

Parameter	Setting
state	Disable or enable the firewall. Note that disabling the firewall poses a security risk.
keep	When enabled, this setting will cause the Thomson Gateway to keep the existing connections when firewall rules change.
tcpchecks	The level of TCP checks (no checks, fast checks or exact checks)
udpchecks	Disable or enable UDP checks
icmpchecks	Disable or enable ICMP checks
logdefault	Disable or enable logging of default firewall rules
logthreshold	Disable or enable log thresholding
tcpwindow	Modify the tcpwindow for fast TCP checks

Clear all firewall Settings

To clear all settings, use the following command:

```
=>firewall clear
```

Since the default behaviour of the SIF is to block, clearing all settings will block ALL traffic to and from the Thomson TG, including TELNET traffic.

6.2 How to Configure Firewall Rules

General Procedure

Proceed as follows to configure rules on the firewall:

1. Select the chain to which you want to add the rule. If necessary, create a new chain.
2. Add rules to the chain.

Overview

This section covers the following topics:

6.2.1 How to Select, Create or Remove a Chain

Available Chains

For more information about chains and hooks, refer to "4.1 Hook Points and Flows of the Thomson Gateway" on page 20.

To view a list of available chains, use the following CLI command:

```
=>firewall chain list
```

This produces the following output:

```
Chains
======
Name                                                Policy          Description

-------------------------------------------------------------------------------
sink                                                accept          system
forward                                             accept          system
source                                              accept          system
sink_fire                                           accept          system
forward_fire                                        accept          system
source_fire                                         accept          system
forward_timeofday                                   accept          system
forward_custom                                      accept          system
sink_system_service                                 accept          system
source_system_service                               accept          system
forward_level                                       accept          system
forward_host_service                                accept          system
forward_multicast                                   accept          system
forward_level_High                                  accept          system
forward_level_Medium                                accept          system
forward_level_Standard                              accept          system
forward_level_Low                                   accept          system
forward_level_Disabled                              accept          system
forward_level_BlockAll                              accept          system
forward_level_Test                                  accept          system
{Administrator}=>
```

When adding a rule, you will need the name of the chain to which you want to add it.

Creating a New Chain

It is also possible to create other chains using the following command:

```
=>firewall chain add chain <name of the chain>
```

Example

The following command:

```
=>firewall chain add chain Test
```

creates a chain called test. The list command produces the following output:

```
Chains
======
Name                                                Policy          Description

-------------------------------------------------------------------------------
sink                                                accept          system
forward                                             accept          system
source                                              accept          system
sink_fire                                           accept          system
forward_fire                                        accept          system
source_fire                                         accept          system
forward_timeofday                                   accept          system
forward_custom                                      accept          system
sink_system_service                                 accept          system
source_system_service                               accept          system
forward_level                                       accept          system
forward_host_service                                accept          system
forward_multicast                                   accept          system
forward_level_High                                  accept          system
forward_level_Medium                                accept          system
forward_level_Standard                              accept          system
forward_level_Low                                   accept          system
forward_level_Disabled                              accept          system
forward_level_BlockAll                              accept          system
forward_level_Test                                  accept          system
Test                                                accept          user
{Administrator}=>
```

Removing Chains

There are two options for removing chains:

- remove an individual chain: use the following command:

```
firewall chain delete <name of the chain>
```

- flush the entire list of chains: use the following command:

```
firewall chain flush
```

Since the default behaviour of the SIF is to block, clearing all settings will block ALL traffic to and from the Thomson TG, including TELNET traffic.

6.2.2 How to Add or Remove Rules to and from a Chain

Use the following command to add a rule to a chain:

```
firewall rule add
             chain = <chain name> [index = <number>] [name = <string>]
             [clink = <chain name>]
             [srcintf [!]= <{wan|local|lan|tunnel|dmz|guest}>]
             [srcip [!]= <{private|ssdp_ip|mdap_ip}>]
             [dstintf [!]= <{wan|local|lan|tunnel|dmz|guest}>]
             [dstip [!]= <{private|ssdp_ip|mdap_ip}>]
             [serv [!]= <{icmp|igmp|ftp|telnet|http|httpproxy|https|RPC|NBT|
                        SMB|imap|imap3|imap4-ssl|imaps|pop2|pop3|pop3s|smtp|
                        ssh|dns|nntp|ipsec|esp|ah|ike|DiffServ|sip|h323|dhcp|
                        rtsp|ssdp_serv|mdap_serv|syslog}>]
             [log = <{disabled|enabled}>] [state = <{disabled|enabled}>]
             action = <{accept|deny|drop|reset|count|link}>
```

This command uses the following parameters:

Parameter	Description
chain	Name of the chain which contains the rule
index	Index of the rule in the chain
clink	Name of the chain to be parsed when this rule applies (if the action is ‘link’)
srcintf	Name of the source interface expression
dstintf	Name of the destination interface expression
serv	Name of the service expression
log	Disable/Enable logging when this rule applies
action	The action to be taken when this rule applies (must be 'link' when clink is used)

When selecting interface or service expressions, it is possible to use the exclamation mark character to indicate a logical not.

Example: **serv=!dns** means everything but dns or “not dns”.

It is possible to combine several not-expressions in the same way that the expression itself is used. It is also possible to combine regular expressions and not-expressions

Changing existing rules

Use the following command to change an existing rule:

```
=>firewall rule modify
             chain = <chain name> [index = <number>] [name = <string>]
             [clink = <chain name>]
             [srcintf [!]= <{wan|local|lan|tunnel|dmz|guest}>]
             [srcip [!]= <{private|ssdp_ip|mdap_ip}>]
             [dstintf [!]= <{wan|local|lan|tunnel|dmz|guest}>]
             [dstip [!]= <{private|ssdp_ip|mdap_ip}>]
             [serv [!]= <{icmp|igmp|ftp|telnet|http|httpproxy|https|RPC|NBT|
                        SMB|imap|imap3|imap4-ssl|imaps|pop2|pop3|pop3s|smtp|
                        ssh|dns|nntp|ipsec|esp|ah|ike|DiffServ|sip|h323|dhcp|
                        rtsp|ssdp_serv|mdap_serv|syslog}>]
             [log = <{disabled|enabled}>] [state = <{disabled|enabled}>]
             action = <{accept|deny|drop|reset|count|link}>
```

This command uses the same parameters as the **add** command.

Removing rules

There are two options for removing rules:

- remove an individual rule: use the following command:

```
firewall rule delete chain=<name of the chain> index=<number of the rule in the chain>
```

- flush the entire list of rules: use the following command:

```
firewall rule flush
```

6.3 How to Configure Firewall Security Levels via CLI

About firewall security levels

For a description of firewall levels, refer to "4.3 Firewall Security Levels" on page 23.

Viewing the current security level

Use the following command to view the current security level:

```
=>firewall level set
```

List all available levels

Use the following command to list all available levels:

```
=>firewall level list
```

Change the active security level

Use the following command to change the current active security level:

```
=>firewall level set name=<security level name>
```

Create a new level

Use the following command to create a new security level:

```
=>firewall level add name = <string>
        [index = <number>]
        [readonly = <{disabled|enabled}>]
        [udptrackmode = <{strict|loose}>]
        [service = <{disabled|enabled}>] [proxy = <{disabled|enabled}>]
        [text = <quoted string>] [policy = <{default|drop|accept}>]
```

This command uses the following parameters:

Parameter	Description
name	The name of the security level to add
index	Index of the security level
readonly	Select whether the security level is readonly (i.e. cannot be modified)
udptrackmode	Select UDP connection tracking mode
service	Enable/Disable host service definitions for this security level
proxy	Enable/Disable proxy system services for this security level
text	Description of this security level
policy	Default policy of this security level

Modify an existing level

Use the following command to modify an existing security level:

```
=>firewall level modify
        [index = <number>]
        [readonly = <{disabled|enabled}>]
        [udptrackmode = <{strict|loose}>]
        [service = <{disabled|enabled}>] [proxy = <{disabled|enabled}>]
        [text = <quoted string>] [policy = <{default|drop|accept}>]
```

This command uses the same parameters as the **add** command

Delete a level

Use the following command to delete a level:

```
=>firewall level delete <security level name>
```

7 Intrusion Detection Systems

Introduction

Intrusion Detection is the art of detecting inappropriate, incorrect, or anomalous activity. Among other tools, an Intrusion Detection System (IDS) can be used to determine if a computer network or server has experienced an unauthorized intrusion.

An Intrusion Detection System provides much the same purpose as a burglar alarm system installed in a house. In case of a (possible) intrusion, the IDS system will issue some type of warning or alert. An operator will then tag events of interest for further investigation. After the initial response the event needs to be handled.

Overview

This chapter covers the following topics:

7.1 Methods

Introduction

Among the different methods used by the IDS for the most common are:

- Pattern matching
- Stateful pattern matching
- Protocol decode-based Analysis
- Heuristic-based Analysis
- Profile-based (anomaly) intrusion detection

Definitions

- A ***False positive*** is generated by the IDS represent a fired alarm or interruption of traffic when no real threat occurs.
- A ***False Negative*** occurs in case it the IDS fails to detect malicious network activity.

Pattern matching

Pattern matching is a mechanism that looks for a fixed sequence of bytes within a single packet. To filter traffic inspection, the pattern is also usually associated with a particular service and source or destination port.

Example

An example of pattern matching is firing an alarm if the packet is Internet Protocol version 4 (IPv4) and User Datagram Protocol (UDP), it has destination port 12570, and it contains the string "madison" in the payload.

However, many protocols and attacks don't make use of well-known ports, and pattern matching thus has difficulty detecting these kinds of attacks. Also, if the matching is based on a pattern that isn't so unique, a large number of false positives can result.

Stateful pattern matching

Stateful pattern matching looks for unique sequences that might be distributed across several packets within a stream. Stateful pattern matching could improve on the preceding example by firing an alarm if the string "mad" is detected in one packet and "ison" is detected in one of the subsequent packets. Stateful pattern matching, even though it's more specific than pattern matching, is still vulnerable to false positives. Modifications to an attack can also result in missed events or false negatives.

Protocol decode-based Analysis

Protocol decode-based signatures are an intelligent extension of pattern matching. With this type of signature, the IDS searches for protocol violations, as defined by Requests for Comment (RFCs), and might also incorporate pattern matches for a particular field.

For example, consider an attack that runs over a hypothetical Multicast over Satellite Protocol (MSP) and uses an illegal argument ***xyz*** in the **MSP Type** field. Suppose also that the MSP has an Options field for which the valid options are ***qrs***, ***tuv***, and ***xyz***. In the case of simple or stateful pattern matching, a high number of false positives would result because ***xyz*** is a valid value for the Options field. With protocol decode-based analysis, the IDS decodes MSP and only reports ***xyz*** values in the **Type** field.

Although this method is effective in reducing false positives for well-defined protocols, protocol violations are easily missed by the IDS if the protocol is ambiguous or loosely defined.

Heuristic-based Analysis

An heuristic-based signature uses an algorithm to determine whether an alarm should be fired. An example of this type of analysis and warning would be a signature that fires an alarm if a threshold number of unique ports are scanned on a particular host. The signature can also be limited to, say, SYN packets that are from a particular source, such as a perimeter router. Although heuristic-based signatures can be the only way to detect certain types of attacks, they require tuning and modification to better conform to their unique network environment. Moreover, heuristic scanning is CPU- and resource-intensive, so be sure to carefully weigh the benefits and drawbacks against your network security needs before implementing a large-scale heuristic-based solution.

Profile-based (anomaly) intrusion detection

Profile-based intrusion detection, also referred to as anomaly detection, detects activity that deviates from "normal" activity. Profile-based anomaly detection depends on the statistical definition of normal and can be prone to a large number of false positives.

Thomson Gateway methodologies

The Thomson Gateway uses protocol decoded-based analysis and heuristic-based analysis.

7.2 Signatures

Introduction

Data or logs are compared against conditions or a set of conditions known as attack signatures or simply 'signatures' that when met, indicates intrusion activity, then an attack response is triggered by the IDS.

Thomson Gateway signatures

The signatures of the Thomson Gateway are divided in 5 different parsers:

- Fragment signatures parser: checks on fragmentation.
- Scan signatures parser: checks TCP and UDP port scans.
- DoS signatures parser: recognizes Denial of Service attacks.
- Protocol signatures parser: checks on protocol level.
- Rate signatures: there is a threshold for every protocol. The rate parser checks whether the threshold is not exceeded.

Fragment signatures

- fragment sweep
- zero-length fragment size
- small fragment size
- fragment size overrun
- fragment overlap
- fragment out-of-order

Scan signatures

- ip protocol scan
- tcp port scan
- tcp syn scan
- stealth tcp null scan
- stealth tcp fin scan
- stealth tcp xmas scan
- stealth tcp full xmas scan
- stealth tcp vecna scan
- stealth tcp syn-fin scan
- udp port scan
- ping sweep scan

DoS signatures

- tcp syn flood
- udp flood
- ping flood

- icmp unreachable storm
- smurf broadcast attack
- smurf storm attack
- fraggle broadcast attack
- fraggle storm attack
- land attack
- spoofed packet

Protocol signatures

- tcp null port
- tcp data on syn segment
- tcp invalid urgent offset
- udp null port
- icmp type unknown
- icmp code unknown
- ip zero payload

Rate signatures

- tcp rate limiting
- udp rate limiting
- icmp rate limiting
- ip rate limiting

Interesting links

More information about IDS and signatures can be found on the following sites:

- http://www.insecure.org/
- http://searchsecurity.techtarget.com/
- http://www.iss.net/security_center/advice/Intrusions/
- http://www.cve.mitre.org
- http://www.cert.org

7.3 Configure IDS on the Thomson Gateway

Introduction

The Intrusion Detection System cannot be configured via the Thomson Gateway web interface; yet valuable statistics on detected intrusion attempts can be consulted.

The following can be configured on the CLI:

- Enable or disable a parser
- Enable or disable a signature

Enable or disable a parser

Proceed as follows:

1. Go to the command group **`:ids parser`**.
2. **`:ids parser list`** provides an overview of the ids parser configuration.

```
=>:ids parser list
parser                                  state
-----------------------------------------
fragment                                enabled
scan                                    enabled
dos                                     enabled
proto                                   enabled
rate                                    enabled
=>
```

All parsers are by default enabled.

3. Use the **`modify`** command to enable or disable the parsers:

```
=>:ids parser modify
[parser] = fragment
state = disabled
:ids parser modify parser=fragment state=disabled
=>
```

Use parameter...	To...
parser	Select the parser (fragment, scan, dos, proto or rate).
state	Select enabled or disabled.

4. Click **saveall** to save the changes to the configuration.

Enable or disable a signature

Proceed as follows:

1. Go to the command group **`:ids signature`**.

2 **:ids signature list** provides an overview of the ids parser configuration.

```
=>:ids signature list
signature                       parser            hits action               state
-------------------------------------------------------------------------------------
fragment_sweep                  fragment             0 log                  enabled
zero-length_fragment_size       fragment             0 log, drop            enabled
small_fragment_size             fragment             0 log, drop            enabled
fragment_size_overrun           fragment             0 log, drop            enabled
fragment_overlap                fragment             0 log, drop            enabled
fragment_out-of-order           fragment             0 log                  enabled
ip_protocol_scan                scan                 0 log                  enabled
tcp_port_scan                   scan                 0 log                  enabled
tcp_syn_scan                    scan                 0 log                  enabled
spoofed_packet                  fragment             0 log                  enabled
stealth_tcp_null_scan           scan                 0 log                  enabled
stealth_tcp_fin_scan            scan                 0 log                  enabled
stealth_tcp_xmas_scan           scan                 0 log                  enabled
stealth_tcp_full_xmas_scan      scan                 0 log                  enabled
stealth_tcp_vecna_scan          scan                 0 log                  enabled
stealth_tcp_syn-fin_scan        scan                 0 log                  enabled
udp_port_scan                   scan                 0 log                  enabled
ping_sweep_scan                 scan                 0 log                  enabled
tcp_syn_flo                     dos                  0 log                  enabled
=>
```

All signatures are by default enabled except “spoofed_packet”.

3 Use the **modify** command to enable or disable the parsers:

```
=>:ids signature modify signature=fragment_overlap state=disabled
=>
```

Use parameter...	To...
signature	Select the signature.
state	Select enabled or disabled.

4 Execute **saveall** to save your changes if needed.

Modify the IDS threshold

Proceed as follows:

1 Go to the command group **:ids threshold list**

```
=>:ids threshold list
index  name                        window           limit  scaling
-----------------------------------------------------------------
   1.  ids frag sweep                 1              10  disabled
   2.  ids scan                      20              20  enabled
   3.  ids flood                      2             100  disabled
   4.  ids tcp rate                   1             200  disabled
   5.  ids udp rate                   1             200  disabled
   6.  ids icmp rate                  1             200  disabled
   7.  ids ip rate                    1             200  disabled
```

2 Use the **modify** command to change the ids thresholds parameters:

```
=>:ids threshold modify index=1 window=30 limit=30 scaling=enabled
=>
```

Use parameter...	To specify...
index	The index of the Threshold.
window	The time window of the Threshold
limit	The limit (amount of packets) of the threshold.
scaling	whether scaling should be enabled or disabled. Scaling is an option to make IDS more sensitive by extending (=scaling) the time window and keeping the limit unchanged.

3 Verify the new configuration:

```
=>:ids threshold list
index  name                      window           limit  scaling
-------------------------------------------------------------------
   1.  ids frag sweep               30              30  enabled
   2.  ids scan                     20              20  enabled
   3.  ids flood                     2             100  disabled
   4.  ids tcp rate                  1             200  disabled
   5.  ids udp rate                  1             200  disabled
   6.  ids icmp rate                 1             200  disabled
   7.  ids ip rate                   1             200  disabled
=>
```

4 Execute **saveall** to save your changes if needed.

THOMSON Telecom Belgium
Prins Boudewijnlaan 47
2650 Edegem

www.thomson-broadband.com

E-DOC-CTC-20071115-0008 v2.0.

THOMSON
images & beyond