FORSCHUNGSZENTRUM JÜLICH GmbH
Jülich Supercomputing Centre
D-52425 Jülich, Tel. (02461) 61-6402

Technical Report

Next Generation Firewalls – Testing Cisco ASA-5580 10 Gb/s Firewall

Egon Grünter, Markus Meier

FZJ-JSC-IB-2008-10

June 2008

(last change: 15.12.2008)

Table of Contents

1. Introduction

The Internet is still growing up and almost any participant claims for high bandwidth and performance. Different users and organisations are connected using different technologies to fulfil the request of high bandwidth. A lot of organizations and research companies are running high speed networks based on 10Gb/s-Ethernet.

Furthermore the number of users grows and also an unreported number of users who use the Internet in a malicious way. Therefore firewalls are used to separate the private network from the public network.

Firewalls are in-band devices. Each network packet has to traverse the firewall. Based on a highly configurable set of rules the firewall decides whether a packet is dropped or forwarded. In fact each firewall that is linked to a network path has an impact on the network performance.

But security and high speed network must meet each other. Currently there are different solutions available on the market. Load balancing solutions have in common that an algorithm shares the load between a master and slaves. Thus it is possible to build a 10Gb/s-Firewall by building a cluster of firewalls with each single device having a lower performance. Unfortunately the load balancing algorithms are based on IP-Addresses and ports which means that each stream is running across one of the firewall units, i.e. the maximum throughput of a single firewall unit of the cluster is the maximum throughput for one single data stream.

In November 2007 Cisco Systems Inc. Jülich Supercomputing Centre has participated in a beta-test of a new firewall product. The Cisco ASA 5580-40 has been tested and the results are summarized in that report.

2. Hardware

The Cisco ASA 5580-40 firewall is a hardware appliance. The following figure shows the front of the box.

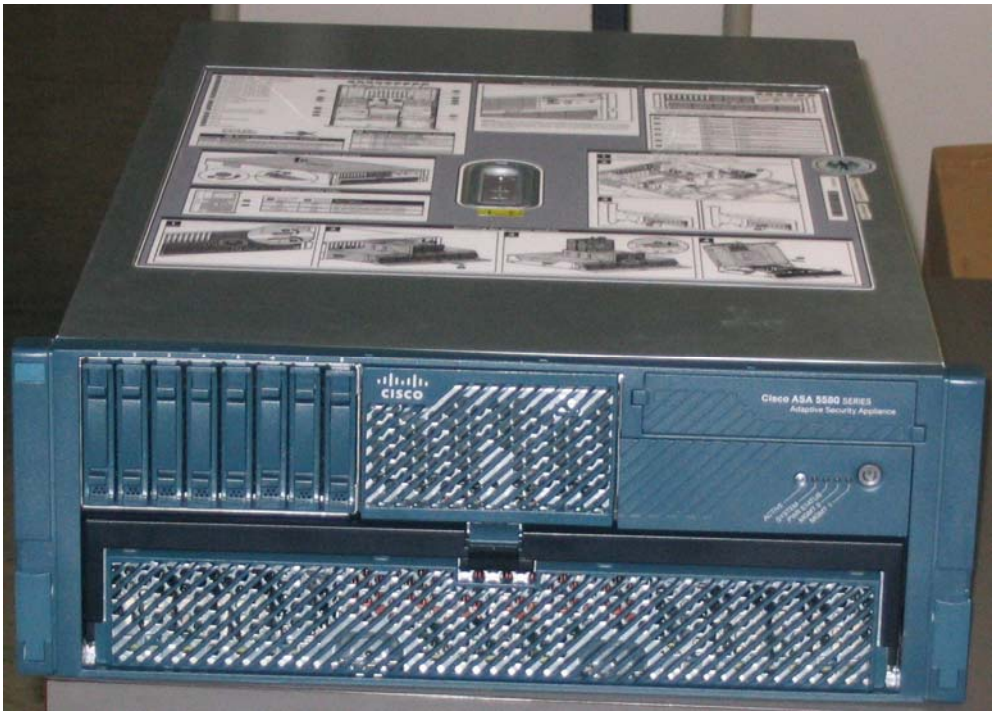


Figure 2-1 Cisco ASA 5580-40 Front

It has the following physical specifications:

Form Factor	4 RU, 19-in. rack-mountable
Dimensions (H x W x D)	17.6 x 48.3 x 67.3 cm
Weight (with Single Power Supply)	29.9 kg

At the upper left side there are eight slots to connect 2.5'' hard disks. Maybe they will be used in future to store configuration files or netflow information. In the middle of the figure we see a black handle, with which the lower part of box can be drawn out of the chassis. The next figure shows this part of the box with an open lid.

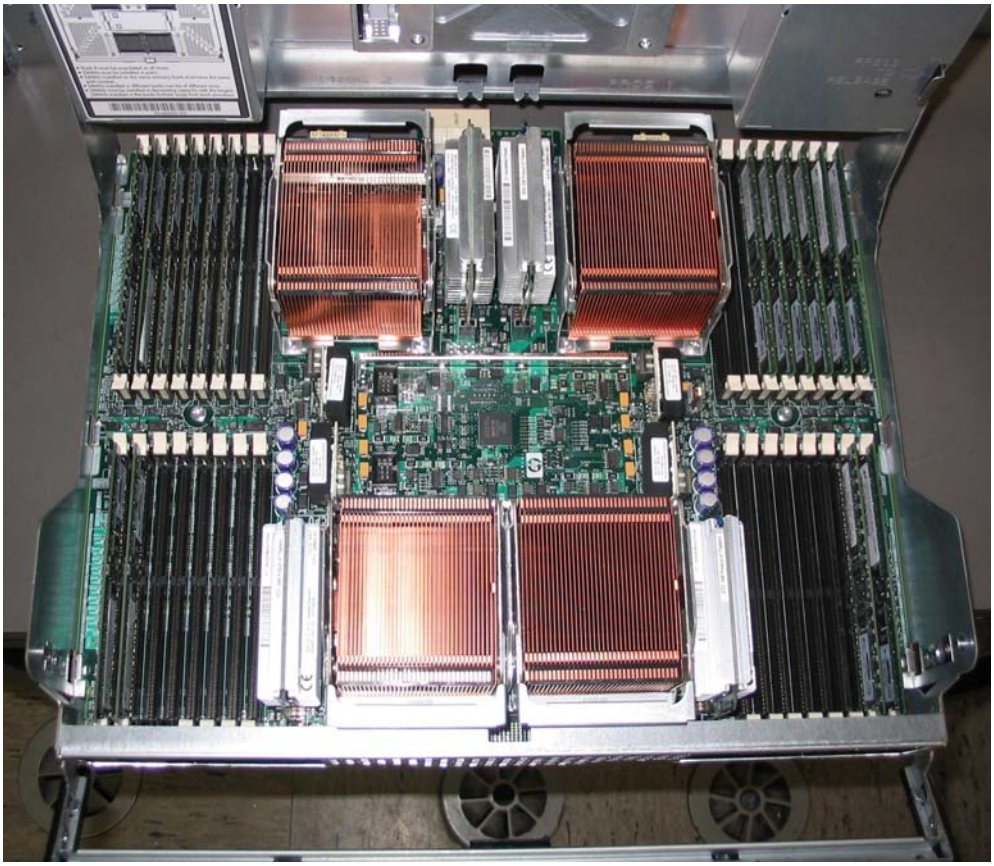


Figure 2-2 Cisco ASA 5580-40 Open lid

Figure 2-2 shows the 4 CPU 8 core architecture with 12 GB RAM. Only one core runs administrative tasks at a time just to guarantee that administrative tasks do not impact latency. However, each core can run the administrative functions. The 12 GB RAM can be found at the upper left and right side. The memory is shared between all the cores. Cisco ASA 5580-40 uses 1 GB of internal flash memory to store configuration files and software images.

The rear chassis illustrated in Figure 2-3 shows at the left and at the right side redundant hot swappable power supplies. From the right to left at the bottom you'll find the network ports (yellow area), a console port (blue) which can be used to manage the ASA from command line mode and two USB ports (black). As well the console port can be used to capture certain debug messages which will be printed only to the console.

In the middle there are 9 slots, numbered from the right to left beginning by 1. By default the ASA ships with a crypto accelerator connected to slot 1. Unfortunately a failure in the crypto hardware leads to system failure. Slot 2 is reserved for future use. Five 4-Port-10/100/1000 Ethernet cards are connected to slots 3 to 7. Slot 8 contains two 10 Gigabit-Ethernet-Ports (optical connectors). Slot 9 again is reserved for use with hard disk hardware which is currently not available. Slots 3 to 8 are customer available and ASA supports at least 12 (6*2) 10GE-Interfaces or 24 (6*4) GE-Interfaces.

Figure 2-3 Cisco ASA 5580-40 Rear chassis

The Cisco ASA 5580-40 uses two I/O controllers. Slots seven and eight are connected to the first I/O controller and both are high speed PCI Express (x8) buses with 18 Gbit/s full-duplex. Slots three, four, five, and six are connected to the second I/O controller. Slot five is another high speed PCI Express bus. Slots three, four, and six are medium PCI express buses (x4) with 10Gbit/s full-duplex. The crypto controller as well shares the I/O controller, but there is a separate bus for the crypto accelerator

3. Software

Some improvements to performance have been mentioned in chapter 2 Hardware. Memory is shared between all cores and only one core handles administrative functionalities at a time. According to Cisco documentation the leading step in performance can be found in software. Although the ASA product family has always been shipped with multi CPU based devices, the software architecture of the new software release 8.1 has been redesigned.

All cores run a 64 Bit SMP kernel. Because of the shared memory there is no flow affinity to one single core. This means, that any core can service I/O and any core can work at a flow but a single flow is always handled by one single core only. This features an ideal load balancing across the cores. In fact this means that most of the software features have been redesigned to be multi-core capable.

Netflow v9 support has been integrated into the new software because it performs much better than syslog in high performance environments. Because syslog is non-trivial in high performance environments Netflow performs much better. One single packet causes multiple Netflow events.

During the Beta-Test we discovered differences between the software images. Because Cisco ASA 5580-20 uses different hardware than Cisco ASA 5580-40 the images are not compatible.

4. Tests

4.1 Performance Tests

The first tests focused on the TCP-Performance of the Cisco ASA 5580-40. We used two hosts with dual AMD Opteron 256 processors and 2 GB RAM connected to a "TYAN Thunder K8WE S2895" motherboard. In order to achieve more than 1 Gb/s performance we operated with a Myricom 10 GE card in both hosts.

The tests are divided into two separate parts. First we measured the round trip time of a TCP-Segment. We used a tool called *tcppp* which is part of the visualization toolkit VISIT (http://www.fz-juelich.de/jsc/visit/). After the three way handshake has been done tcppp sends TCP segments of configurable sizes from the client to the server (TCP-Port 5001) and back. In order to compare the effect of an ASA 5580-40 we first measured the round trip time between the hosts connected via a Cisco Catalyst 6500 Series switch. The displayed numbers are the half of the round trip time.

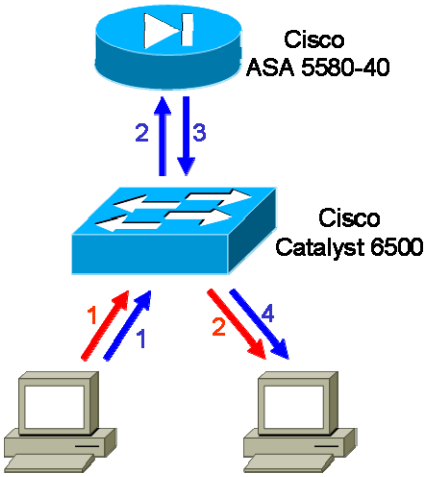


Figure 4-1Testbed

The Cisco Catalyst 6500 Series switch uses the following modules and submodules:

- CEF720 4 port 10-Gigabit Ethernet (WS-X6704-10GE)
  - Distributed Forwarding Card (WS-F6700-DFC3B)
- Supervisor Engine 720 (WS-SUP720-3B)
  - Policy Feature Card 3 (WS-F6K-PFC3B)
  - MSFC3 Daughterboard (WS-SUP720)

During each test we configured three packet sizes representing small, medium and big IP datagrams and sent one million TCP segments to get an acceptable average value.

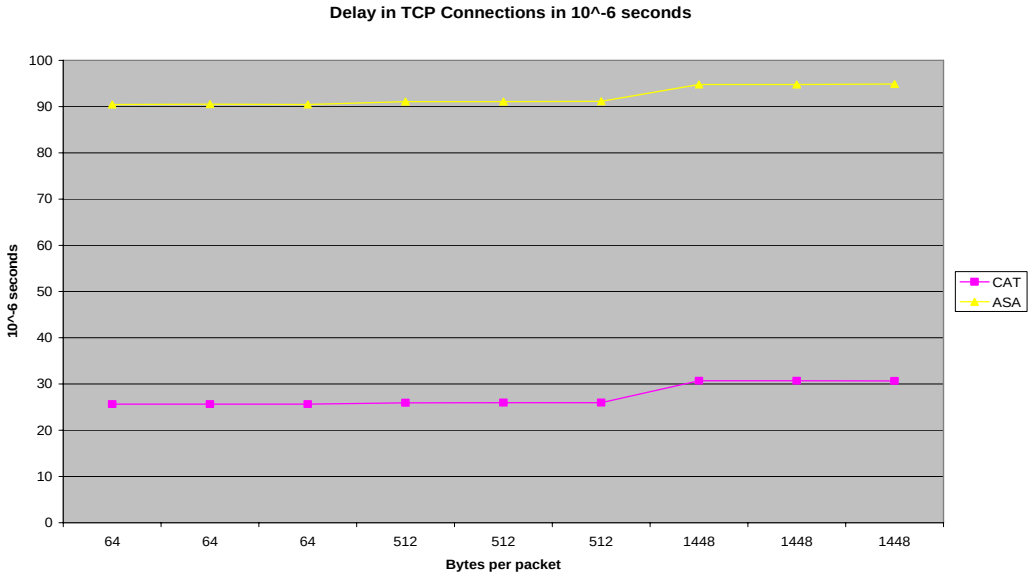


Figure 4-2 Delay in TCP connections

Figure 4-1 shows the results of the tests with the tcppp-routine. During the first tests without a Cisco ASA 5580-40 we discovered a medial latency of 25.65 microseconds if a 64 byte TCP segment has been sent. This latency increases to 25.95 microseconds if a 512 byte TCP segment has been sent and 30.70 microseconds if a 1448 byte TCP segment has been sent. It should be noted that the measured times are on user-level. This means they include time spent in the operation systems of the communication endpoints.

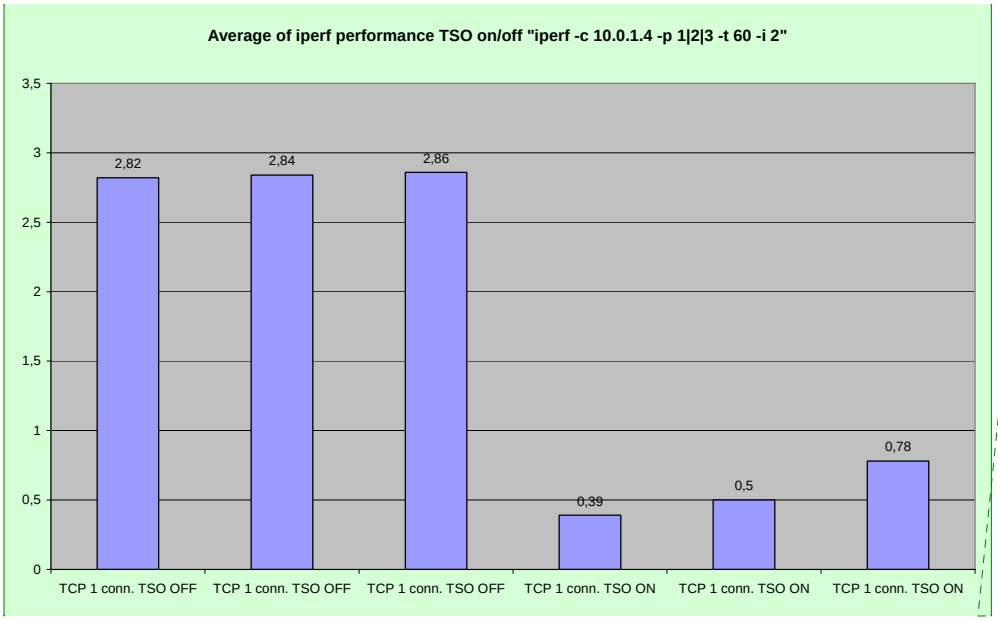
During the second tests the two hosts and the Cisco ASA 5580 have been connected via the Cisco Catalyst 6500 Series switch. Only one single access control list entry has been configured because the number of access control lists has an effect only during the connection set up. If a connection has been established the access control lists are used no longer. We configured the following commands:

access-list acl-outside permit ip any any

access-group acl-outside in interface outside

Except adjustments to the interface configuration no changes have been made so that the tests have been done with a standard configuration “out-of-the-box”. On the average the Cisco ASA 5580-40 increases the relative delay by a factor 3.38. The absolute growth is about 60 microseconds. For comparision only a packet takes 500 microseconds to cover a distance of 100 km.

During the next tests we used iperf version 2.0.2 to measure the throughput of a single TCP stream between the two hosts. We always used a simple iperf call: `iperf -c 10.0.1.4 -t 60 -i 10`.We discovered that the two hosts were the bottlenecks because the Cisco ASA 5580-40 has no effect on the performance if TCP segment offloading (TSO) is turned off at both hosts. If the network interfaces have TCP segment offloading enabled the performance decreased. During the tests Cisco provided a new software image which resolves this problem. After the installation the performance with TSO on achieved the same values as without the ASA. Figure 4-2 shows the result.



Kommentar [MM1]: Hast du die Grafik auch noch mit y-Achsenbeschreibung ?

Figure 4-3 iperf performance

After these test we did the same tests with jumbo frames but only single connection. Jumbo frames increased the performance up to 5.62 Gb/s.

At the end of the performance tests we focused on the VPN performance of the Cisco ASA 5580-40. During the tests we used the following hardware:

- 2 ThinkPad X60s CoreDuo 1.66
- 1 ThinkPad T60 Core 2 Duo 2.0
- 2 ThinkPad R52 Pentium M 2.0
- 1 ThinkPad T30 Pentium 4 M 2.4
- 1 ThinkPad T41 Pentium M 1.7
- 1 ThinkPad T41p Pentium M 1.7
- 1 ThinkPad T43p Pentium M 2.16
- 1 Fujitsu Lifebook S-Serie Core 2 Dip 1.8

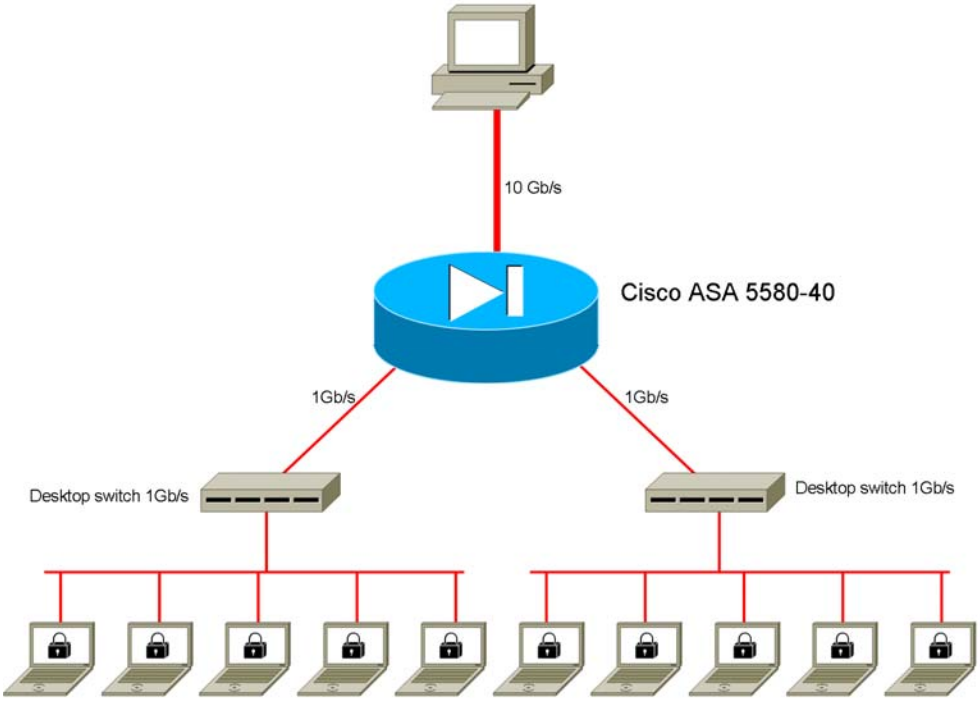


Figure 4-4VPN test setup

Figure 4-3 shows the VPN test setup. Five laptops were connected to a desktop switch which achieves a maximum throughput of 1 Gb/s. Each desktop switch has been connected via a 1 Gb/s link to a dedicated 1Gb/s port on the Cisco ASA 5580-40. The server in the internal network still used a 10Gb/s network link as it did during the performance tests described above. Summarized we achieved a throughput without any active VPN session of 1.81Gb/s.

After that we set up a single VPN session from each laptop to the dedicated ASA interface using 128 bit AES encryption and MD5 hashes. Figure 4-4 shows the results of these tests. It is obvious that 1Gb/s is the upper limit of the Cisco ASA 5580-40 VPN performance.

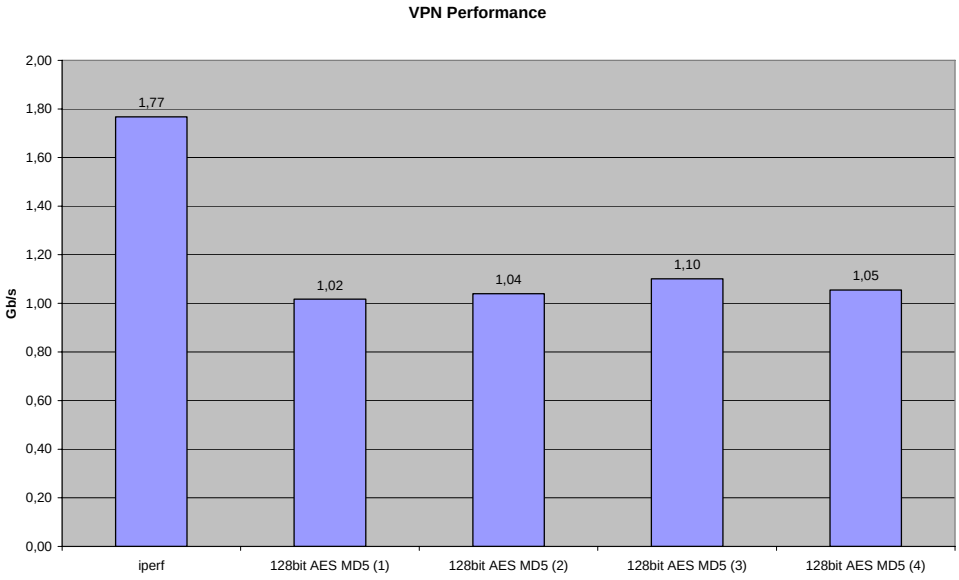


Figure 4-5 VPN Performance

Additionally the influence of access control lists (ACL) on the performance has been investigated. This has been done by generating an ACL with 1, 10, 100, 1000, 10000 and 100000 access list entries (ACE). It has been ensured that only the last entry in the access-list allows the communication that was needed for measurement tasks.

An ACL is only used when the first datagram of a connection arrives at a firewall interface. We measured the duration of the system-call *connect()* After *connect()* returns the connection setup has been done. 100 calls to *connect()* are averaged to 1 single measurement value. We carried out 100 measurement, i.e. 100000 calls to *connect()* have been measured. First we did that tests between the two 10GE hosts described above. After that the traffic has to cross the Cisco ASA 5580-40.

However, the results did not indicate any impact of the Cisco ASA 5580-40 on the performance.

4.2 Configuration and administration

During the second part of the tests we focussed on the configuration and administration of the Cisco ASA 5580-40. We used the command line interface (CLI) as well as the Adaptive Security Device Manager.

The command line interface is similar to the one of a Cisco Secure PIX Firewall and earlier versions of the operating system. The command line interface can be accessed via console, Telnet or SSH sessions. Multiple users are allowed to login simultaneously. The number of users and the access rights of the users can be defined via certain commands. After login via SSH or Telnet or after a console session has been launched the user receives a command prompt in an unprivileged mode. As with previous versions of PIX firewall users are allowed to access the enable mode via the *enable* command. After the password has been entered successfully the user reaches the enable mode. The modes differ from each other in the number of available commands. If there

are usernames and access rights configured the enable mode should be accessed via the *login* command. The user is asked for a username and password and if both of them are entered successfully the enable mode is reached. Depending on the access rights and their configuration different commands will be available. Users with highest privileges are allowed to enter the configuration mode by the *configure terminal* command. Online help is available for any command but in some places this help should be improved. File management of configurations and software images, configuration and administration tasks can be done via command line. For administration the command line interface offers some Unix-like tools, e.g. “include” or “exclude” which act as “grep” and “grep –v” commands.

As an alternative Cisco offers a GUI called ASDM (Adaptive Security Device Manager). It allows a configuration and administration via GUI. Before use the GUI the Cisco ASA 5580-40 has to be running an HTTPS server which is done by the *http server enable* command via command line interface.

The access via HTTPS can be done in two different ways. Windows clients could use the Cisco ASDM Launcher which is a small software that has to be installed. In addition this client has to run Java Runtime Environment in a compatible version (e.g. 1.6.0). Alternatively a standard web browser with Java enabled could be used to access the Cisco ASA 5580-40 via *https://asa.device.name*. In each case a Java applet is started.

After the applet has been started the first panel, called “Home”, shows an overview of the hardware, software versions, licenses, current resource usage for CPU and memory, interface states and one panel is reserved to show system log messages. A second panel is reserved for configuration settings and a third one for monitoring issues.

During configuration of the Cisco ASA 5580-40 via ASDM it turned out that it is helpful to activate the option “Preview commands before sending them to the device”. This forces ASDM to show the CLI-commands of the changes in configuration in a pop-up window and the administrator could check the commands again before sending it to the ASA.

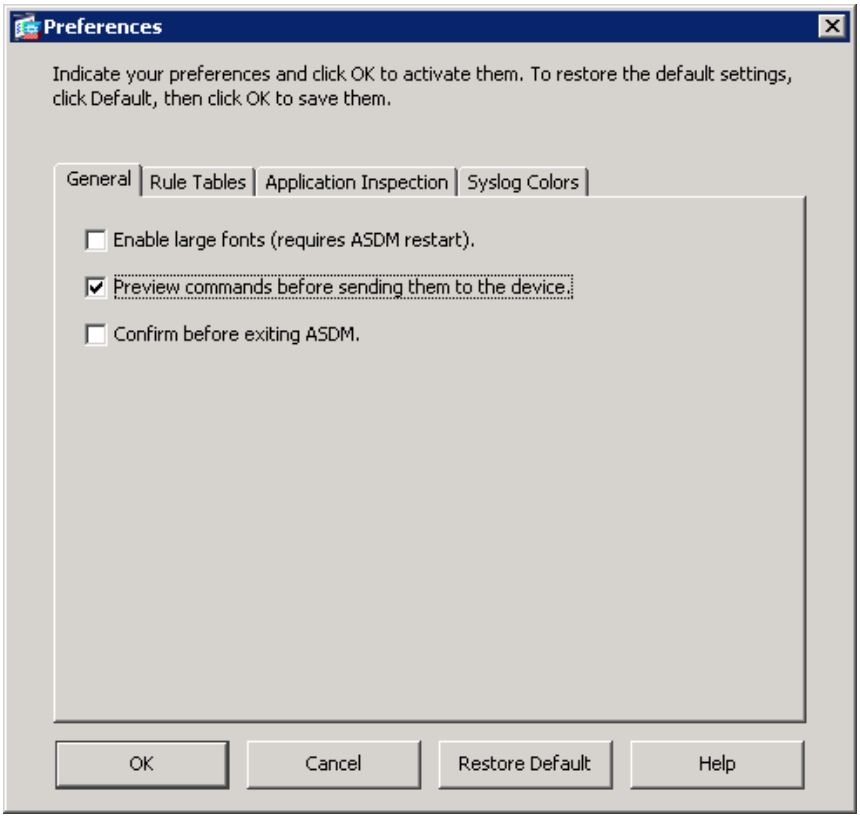


Figure 4-6 ASDM Preferences

Another useful tool is the packet tracer. Figure 4-6 shows a screenshot of the tool. Before the packet tracer starts an IP packet is to be set up. By clicking the start button the tool simulates the transfer of this certain packet through the ASA. This tool is very useful during troubleshooting because the administrator will find out which part of the adaptive security algorithm drops the packet.

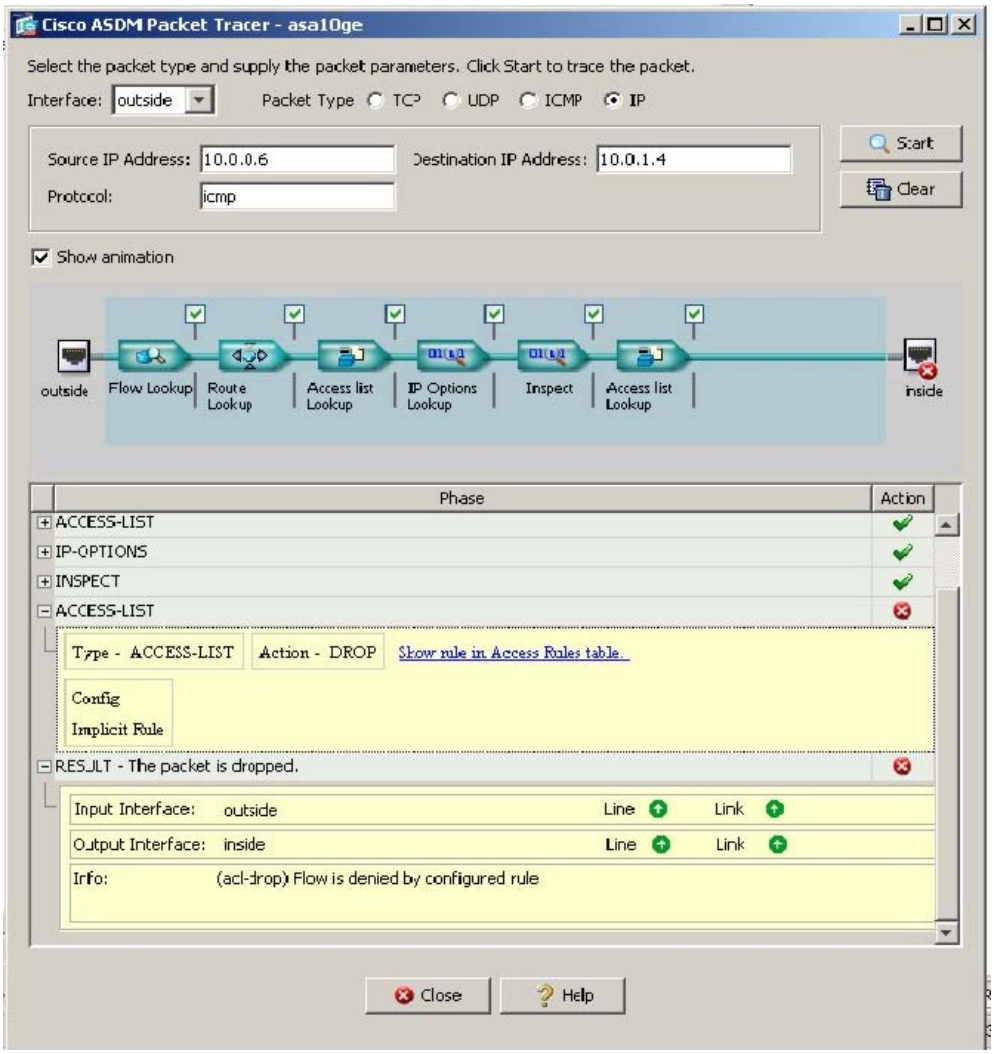


Figure 4-7 ASDM packet tracer

We encountered one of the biggest problems during configuration tests using ASDM and command line interface at the same time. If two administrators are logged in, one admin to the command line interface and the other one uses ASDM, and both are configuring the firewall there will be one configuration lost, i.e. the administrator who enters the *write memo*ry command first will lose the configuration changes. Maybe this will be improved by a future version by a pop-up window or a warning on CLI showing other users who are logged in, when entering the configuration mode.

Another problem we encountered in first ASDM version was that configuration changes could not be seen obviously. ASDM uses a refresh button that changes color from blue to red if the device configuration and the ASDM configuration is out of sync. During the tests we discovered that an administrator does not recognize the color of the button. Therefore Cisco added a pop-up window which indicates configuration changes as they take place.

Nevertheless Cisco Firewall admins will notice that the configuration of Cisco PIX Firewall is very similar to Cisco ASA 5580-40 configuration. The CLI is the same on

both hardware platforms. Only the ASDM-GUIs are different due to different hardware and software versions.

5. Summary

During the tests it has been figured out that the Cisco ASA 5580-40 is a high performance firewall. PIX firewall administrators find an intuitive environment improved by other features, that we did not pay attention to. The Juelich Supercomputing Centre therefore takes Cisco ASA 5580-40 into account to expand the network infrastructure.